ECSAv10.prepaway.premium.exam.150q

Number: ECSAv10
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

ECSAv10

EC-Council Certified Security Analyst

Version 1.0

Exam A

QUESTION 1
Irin is a newly joined penetration tester for XYZ Ltd. While joining, as a part of her training, she was instructed about various legal policies and information securities acts by her trainer. During the training, she was informed about a specific information security act related to the conducts and activities like it is illegal to perform DoS attacks on any websites or applications, it is illegal to supply and own hacking tools, it is illegal to access unauthorized computer material, etc.
To which type of information security act does the above conducts and activities best suit?

A. Police and Justice Act 2006
B. Data Protection Act 1998
C. USA Patriot Act 2001
D. Human Rights Act 1998

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Adam is an IT administrator for Syncan Ltd. He is designated to perform various IT tasks like setting up new user accounts, managing backup/restores, security authentications and passwords, etc. Whilst performing his tasks, he was asked to employ the latest and most secure authentication protocol to encrypt the passwords of users that are stored in the Microsoft Windows OS-based systems.
Which of the following authentication protocols should Adam employ in order to achieve the objective?

A. LANMAN
B. Kerberos
C. NTLM
D. NTLMv2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Michael, a Licensed Penetration Tester, wants to create an exact replica of an original website, so he can browse and spend more time analyzing it.
Which of the following tools will Michael use to perform this task?

A. VisualRoute
B. NetInspector
C. BlackWidow
D. Zaproxy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A hacker initiates so many invalid requests to a cloud network host that the host uses all its resources responding to invalid requests and ignores the legitimate requests.
Identify the type of attack

A. Denial of Service (DoS) attacks
B. Side Channel attacks
C. Man-in-the-middle cryptographic attacks
D. Authentication attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Thomas is an attacker and he skimmed through the HTML source code of an online shopping website for the presence of any vulnerabilities that he can exploit. He already knows that when a user makes any selection of items in the online shopping webpage, the selection is typically stored as form field values and sent to the application as an HTTP request (GET or POST) after clicking the Submit button. He also knows that some fields related to the selected items are modifiable by the user (like quantity, color, etc.) and some are not (like price). While skimming through the HTML code, he identified that the price field values of the items are present in the HTML code. He modified the price field values of certain items from $200 to $2 in the HTML code and submitted the request successfully to the application.
Identify the type of attack performed by Thomas on the online shopping website?

A. Session poisoning attack
B. Hidden field manipulation attack
C. HTML embedding attack
D. XML external entity attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Steven is performing a wireless network audit. As part of the engagement, he is trying to crack a WPA-PSK key. Steven has captured enough packets to run aircrack-ng and discover the key, but aircrack-ng did not yield any result, as there were no authentication packets in the capture.
Which of the following commands should Steven use to generate authentication packets?

A. aireplay-ng --deauth 11 -a AA:BB:CC:DD:EE:FF
B. airmon-ng start eth0
C. airodump-ng --write capture eth0
D. aircrack-ng.exe -a 2 -w capture.cap

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Sam was asked to conduct penetration tests on one of the client's internal networks. As part of the testing process, Sam performed enumeration to gain information about computers belonging to a domain, list of shares on the individual hosts in the network, policies and passwords.
Identify the enumeration technique.

A. NTP Enumeration
B. NetBIOS Enumeration
C. DNS Enumeration
D. SMTP Enumeration

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Jason is working on a pen testing assignment. He is sending customized ICMP packets to a host in the target network. However, the ping requests to the target failed with "ICMP Time Exceeded Type = 11" error messages.
What can Jason do to overcome this error?

A. Set a Fragment Offset
B. Increase the Window size in the packets
C. Increase the TTL value in the packets
D. Increase the ICMP header length

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Joseph, a penetration tester, was hired by Xsecurity Services. Joseph was asked to perform a pen test on a client's network. He was not provided with any information about the client organization except the company name.
Identify the type of testing Joseph is going to perform for the client organization?

A. White-box Penetration Testing
B. Black-box Penetration Testing
C. Announced Testing
D. Grey-box Penetration Testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
An organization deployed Microsoft Azure cloud services for running their business activities. They appointed Jamie, a security analyst for performing cloud penetration testing. Microsoft prohibits certain tests to be carried out on their platform.
Which of the following penetration testing activities Jamie cannot perform on the Microsoft Azure cloud service?

A. Post scanning
B. Denial-of-Service
C. Log monitoring
D. Load testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Sandra, a wireless network auditor, discovered her client is using WEP. To prove the point that the WEP encryption is very weak, she wants to decrypt some WEP packets. She successfully captured the WEP data packets, but could not reach the content as the data is encrypted.
Which of the following will help Sandra decrypt the data packets without knowing the key?

A. Fragmentation Attack
B. Chopchop Attack
C. ARP Poisoning Attack
D. Packet injection Attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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:

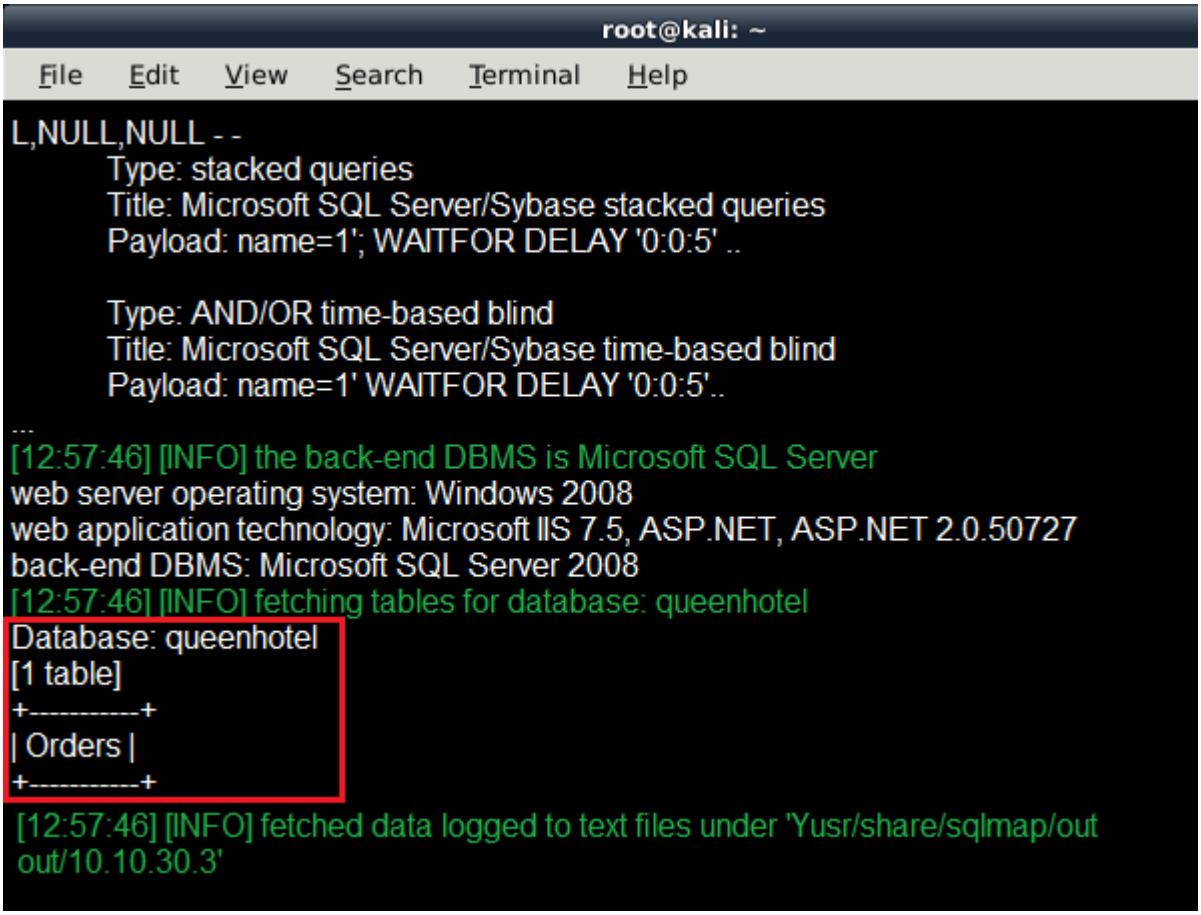
QUESTION 13
Richard, a penetration tester was asked to assess a web application. During the assessment, he discovered a file upload field where users can upload their profile pictures. While scanning the page for vulnerabilities, Richard found a file upload exploit on the website. Richard wants to test 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 14
Richard is working on a web app pen testing assignment for one of his clients. After preliminary information, gathering and vulnerability scanning Richard runs the SQLMAP tool to extract the database information.
Which of the following commands will give Richard an output as shown in the screenshot?

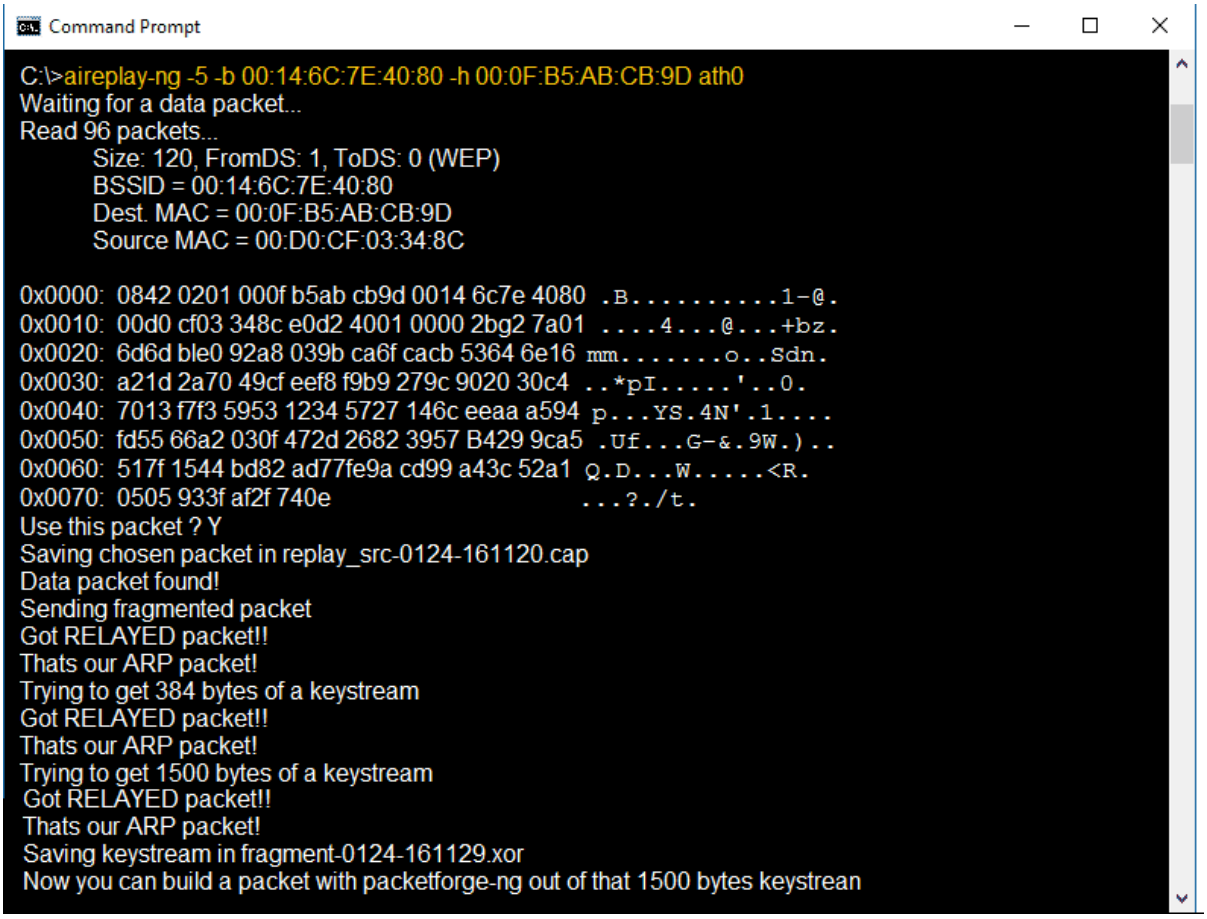


A. sqlmap –url http://quennhotel.com/about.aspx?name=1 –D queenhotel --tables
B. sqlmap –url http://quennhotel.com/about.aspx?name=1 –dbs
C. sqlmap –url http://quennhotel.com/about.aspx?name=1 –D queenhotel –T --columns
D. sqlmap –url http://quennhotel.com/about.aspx?name=1 –database queenhotel –tables

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Identify the PRGA from the following screenshot:



A. replay_src-0124-161120.cap
B. fragment-0124-161129.xor
C. 0505 933f af2f 740e
D. 0842 0201 000f b5ab cd9d 0014 6c7e 4080

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
James is an attacker who wants to attack XYZ Inc. He has performed reconnaissance over all the publicly available resources of the company and identified the official company website http://xyz.com. He scanned all the pages of the company website to find for any potential vulnerabilities to exploit. Finally, in the user account login page of the company's website, he found a user login form which consists of several fields that accepts user inputs like username and password. He also found than any non-validated query that is requested can be directly communicated to the active directory and enable unauthorized users to obtain direct access to the databases. Since James knew an employee named Jason from XYZ Inc., he enters a valid username "jason" and injects "jason)(&))" in the username field. In the password field, James enters "blah" and clicks Submit button. Since the complete URL string entered by James becomes "(&(USER=jason)(&))(PASS=blah))," only the first filter is processed by the Microsoft Active Directory, that is, the query "(&(USER=jason)(&))" is processed. Since this query always stands true, James successfully logs into the user account without a valid password of Jason.
In the above scenario, identify the type of attack performed by James?

A. LDAP injection attack
B. HTML embedding attack
C. Shell injection attack
D. File injection attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
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 18
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 19
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 20
Alisa is a Network Security Manager at Aidos Cyber Security. During a regular network audit, she sent specially crafted ICMP packet fragments with different offset values into the network, causing a system crash.
Which attack Alisa is trying to perform?

A. Ping-of-death attack
B. Fraggle attack
C. Session hijacking
D. Smurf attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following roles of Microsoft Windows Active Directory refers to the ability of an active directory to transfer roles to any domain controller (DC) in the enterprise?

A. Master Browser (MB)
B. Global Catalog (GC)
C. Flexible Single Master Operation (FSMO)
D. Rights Management Services (RMS)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A user unknowingly installed a fake malicious banking app in his Android mobile. This app includes a configuration file that consists of phone numbers of the bank. When the user makes a call to the bank, he is automatically redirected to the number being used by the attacker. The attacker impersonates as a banking official. Also, the app allows the attacker to call the user, then the app displays fake caller ID on the user's mobile resembling call from a legitimate bank.
Identify the attack being performed on the Android mobile user?

A. Tailgating

B. SMiShing
C. Vishing
D. Eavesdropping

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
How does OS Fingerprinting help you as a pen tester?

A. It defines exactly what software the target has installed
B. It doesn't depend on the patches that have been applied to fix existing security holes
C. It opens a security-delayed window based on the port being scanned
D. It helps to research vulnerabilities that you can use to exploit on a target system

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
While scanning a server, you found rpc, nfs and mountd services running on it. During the investigation, you were told that NFS Shares were mentioned in the /etc/exports list of the NFS server. Based on this information, which among the following commands would you issue to view the NFS Shares running on the server?

A. showmount
B. nfsenum
C. mount
D. rpcinfo

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
SecGlobal Corporation hired Michael, a penetration tester. Management asked Michael to perform cloud penetration testing on the company's cloud infrastructure. As a part of his task, he started checking all the agreements with cloud service provider and came to a conclusion that it is not possible to perform penetration testing on the cloud services that are being used by the organization due to the level of responsibilities between company and the Cloud Service Provider (CSP).
Identify the type of cloud service deployed by the organization?

A. Platform as a service (PaaS)
B. Software as a service (SaaS)
C. Anything as a service (XaaS)
D. Infrastructure as a service (IaaS)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

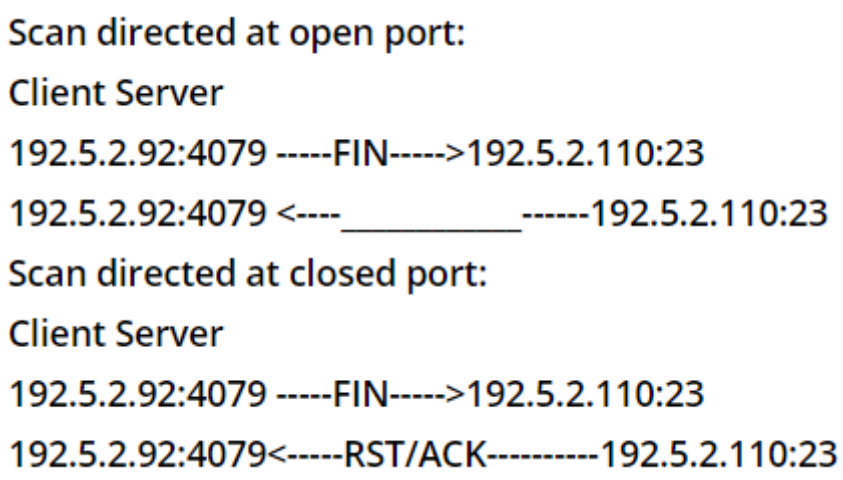
QUESTION 26
A team of cyber criminals in Germany has sent malware-based emails to workers of a fast-food center which is having multiple outlets spread geographically. When any of the employees click on the malicious email, it will give backdoor access to the point of sale (POS) systems located at various outlets. After gaining access to the POS systems, the criminals will be able to obtain credit card details of the fast-food center's customers.
In the above scenario, identify the type of attack being performed on the fast-food center?

A. Phishing
B. Vishing
C. Tailgating
D. Dumpster diving

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
As a part of the pen testing process, James performs a FIN scan as given below:



What will be the response if the port is open?

A. No response
B. FIN/RST
C. FIN/ACK
D. RST

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 28
Peter works as a lead penetration tester in a security service firm named Xsecurity. Recently, Peter was assigned a white-box pen test assignment testing the security of an IDS system deployed by a client. During the preliminary information gathering, Peter discovered the TTL to reach the IDS system from his end is 30. Peter created a Trojan and fragmented it in to 1-character packets using the Colasoft packet builder tool. He then used a packet flooding utility to bombard the IDS with these fragmented packets with the destination address of a target host behind the IDS whose TTL is 35.
What is Peter trying to achieve?

A. Peter is trying to bypass the IDS system using a Trojan
B. Peter is trying to bypass the IDS system using the broadcast address
C. Peter is trying to bypass the IDS system using the insertion attack
D. Peter is trying to bypass the IDS system using inconsistent packets

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Robert is a network admin in XYZ Inc. He deployed a Linux server in his enterprise network and wanted to share some critical and sensitive files that are present in the Linux server with his subordinates. He wants to set the file access permissions using chmod command in such a way that his subordinates can only read/view the files but cannot edit or delete the files.
Which of the following chmod commands can Robert use in order to achieve his objective?

A. chmod 666
B. chmod 644
C. chmod 755
D. chmod 777

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Tecty Motors Pvt. Ltd. has recently deployed RFID technology in the vehicles which allows the car owner to unlock the car with the exchange of a valid RFID signal between a reader and a tag. Jamie, on the other hand, is a hacker who decided to exploit this technology with the aim of stealing the target vehicle. To perform this attack on the target vehicle, he first used an automated tool to intercept the signals between the reader and the tag to capture a valid RFID signal and then later used the same signal to unlock and steal the victim's car.
Which of the following RFID attacks Jamie has performed in the above scenario?

A. RFID cloning
B. Replay attack
C. DoS attack

D. Power analysis attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
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 40
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 41
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 42
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 43
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 44
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 45
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 46
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 47
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 48
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 49
Moses, a professional hacker, attempts to overwhelm the target victim computer by transmitting TCP connection requests faster than the computer can process them. He started sending multiple SYN packets of size between 800 and 900 bytes with spoofed source addresses and port numbers. The main intention of Moses behind this attack is to exhaust the server resources and saturate the network of the target organization.
Identify the type of attack being performed by Moses?

A. VTP attack
B. DoS attack
C. ARP attack
D. HSRP attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
What is the purpose of the Traceroute command?

A. For extracting information about the network topology, trusted routers, and firewall locations
B. For extracting information about closed ports
C. For extracting information about the server functioning
D. For extracting information about opened ports

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which port does DHCP use for client connections?

A. UDP port 67
B. UDP port 68
C. UDP port 69
D. UDP port 66

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Rebecca, a security analyst, was auditing the network in her organization. During the scan, she found a service running on a remote host, which helped her to enumerate information related to user accounts, network interfaces, network routing and TCP connections.
Which among the following services allowed Rebecca to enumerate the information?

A. NTP
B. SNMP
C. SMPT
D. SMB

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
In delivering penetration testing report, which of the following steps should NOT be followed?

A. Always send the report by email or CD-ROM
B. Always deliver the report to approved stakeholders in the company in person
C. Always ask for a signed acknowledgment after submitting the report
D. Report must be presented in a PDF format, unless requested otherwise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
AB Cloud services provide virtual platform services for the users in addition to storage. The company offers users with APIs, core connectivity and delivery, abstraction and hardware as part of the service.
What is the name of the service AB Cloud services offer?

A. Web Application Services
B. Platform as a service (PaaS)
C. Infrastructure as a service (IaaS)
D. Software as a service (SaaS)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Jason is a penetration tester, and after completing the initial penetration test, he wanted to create a final penetration test report that consists of all activities performed throughout the penetration testing process. Before creating the final penetration testing report, which of the following reports should Jason prepare in order to verify if any crucial information is missed from the report?

A. Activity report
B. Host report
C. User report
D. Draft report

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
The penetration testers are required to follow predefined standard frameworks in making penetration testing reporting formats.
Which of the following standards does NOT follow the commonly used methodologies in penetration testing?

A. National Institute of Standards and Technology (NIST)
B. Information Systems Security Assessment Framework (ISSAF)
C. Open Web Application Security Project (OWASP)
D. American Society for Testing Materials (ASTM)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
You have implemented DNSSEC on your primary internal DNS server to protect it from various DNS attacks. Network users complained they are not able to resolve domain names to IP addresses at certain times. What could be the probable reason?

A. DNSSEC does not provide protection against Denial of Service (DoS) attacks
B. DNSSEC does not guarantee authenticity of a DNS response during an attack
C. DNSSEC does not protect the integrity of a DNS response
D. DNSSEC does not guarantee the non-existence of a domain name or type

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Ross performs security test on his company's network assets and creates a detailed report of all the findings.

In his report, he clearly explains the methodological approach that he has followed in finding the loopholes in the network. However, his report does not mention about the security gaps that can be exploited or the amount of damage that may result from the successful exploitation of the loopholes. The report does not even mention about the remediation steps that are to be taken to secure the network.
What is the type of test that Ross has performed?

A. Penetration testing
B. Vulnerability assessment
C. Risk assessment
D. Security audit

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
JUA Networking Solutions is a group of certified ethical hacking professionals with a large client base. Stanley works as a penetrating tester at this firm. Future group approached JUA for an internal pen test. Stanley performs various penetration testing test sequences and gains information about the network resources and shares, routing tables, audit and service settings, SNMP and DNS details, machine names, users and groups, applications and banners.
Identify the technique that gave Stanley this information.

A. Enumeration
B. Sniffing
C. Ping sweeps
D. Port scanning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Frank is a senior security analyst at Roger Data Systems Inc. The company asked him to perform a database penetration test on its client network to determine whether the database is vulnerable to attacks or not. The client did not reveal any information about the database they are using.
As a pen tester Frank knows that each database runs on its own default port. So he started database port scanning using the Nmap tool and tried different commands using default port numbers and succeeded with the following command.
nmap -sU –p 1521 <client ip-address>
Identify the database used by the company?

A. MySQL
B. Microsoft SQL Server
C. SQLite
D. Oracle

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
William, a penetration tester in a pen test firm, was asked to get the information about the SMTP server on a target network.
What does William need to do to get the SMTP server information?

A. Send an email message to a non-existing user of the target organization and check for bounced mail header
B. Examine the session variables
C. Examine TCP sequence numbers
D. Look for information available in web page source code

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
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:

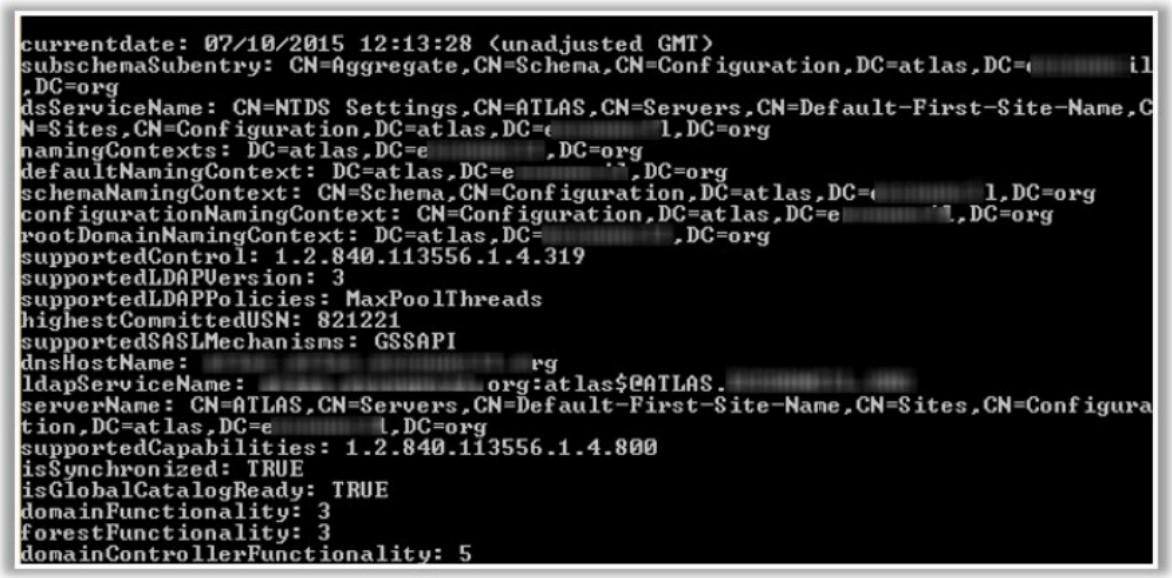
QUESTION 63
Nick is a penetration tester in Stanbiz Ltd. As a part of his duty, he was analyzing the network traffic by using various filters in the Wireshark tool. While sniffing the network traffic, he used "tcp.port==1433" Wireshark filter for acquiring a specific database related information since 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 64
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 65
Sam is a penetration tester and network admin at McLaren & McLaren, based out of Washington. The company has recently deployed IPv6 in their network. Sam found problems with the protocol implementation and tried to redeploy IPv6 over IPv4. This time, he used the tunneling mechanism while deploying the IPv6 network.
How does the tunneling mechanism work?

A. It encapsulates IPv6 packets in IPv4 packets
B. It transfers IPv4 first and the IPv6
C. It splits the IPv4 packets and provides a way to IPv6
D. It replaces IPv4 with IPv6

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

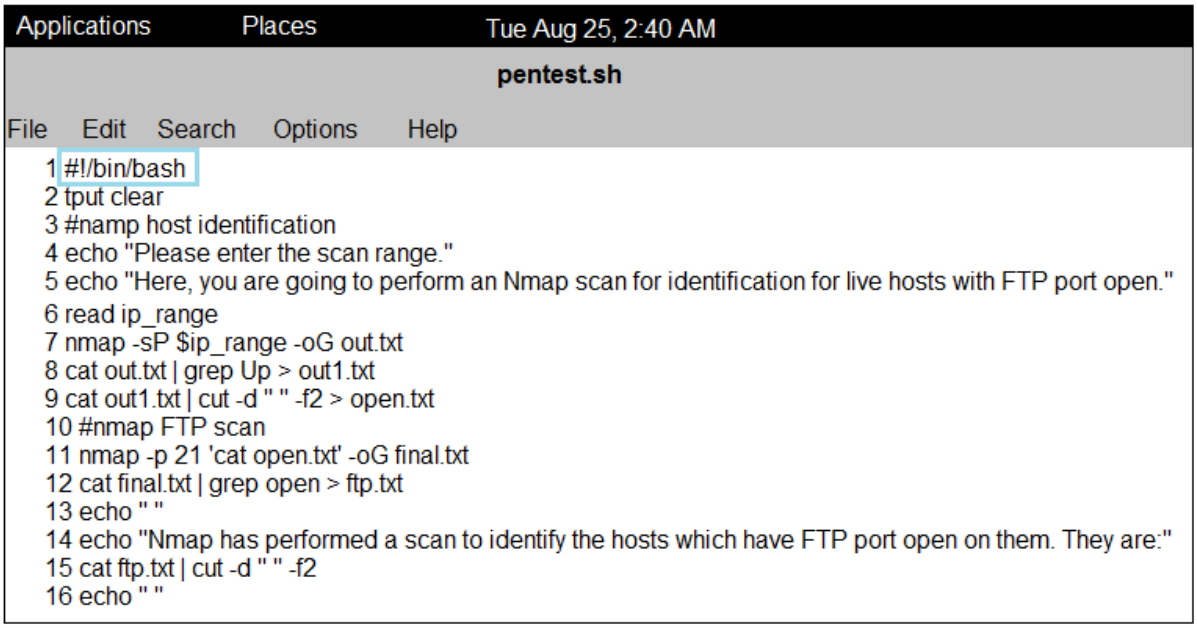
QUESTION 66
Dale is a network admin working in Zero Faults Inc. Recently the company's network was compromised and is experiencing very unusual traffic. Dale checks for the problem that compromised the network. He performed a penetration test on the network's IDS and identified that an attacker sent 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 67
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 68
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 69
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 70
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 71
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 72
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 73
An employee is trying to access the internal website of his company. When he opened a webpage, he received an error message notifying "Proxy Authentication Required." He approached the IT department in the company and reported the issue. The IT staff explained him that this is an HTTP error indicating that the server is unable to process the request due to lack of appropriate client's authentication credentials for a proxy server that is processing the requests between the clients and the server.
Identify the HTTP error code corresponding to the above error message received by the employee?

A. 415
B. 417
C. 407
D. 404

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
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 75
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 76
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 77
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 78
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 79
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 80
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 81
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 82
Russel, a penetration tester after performing the penetration testing, wants to create a report so that he can

provide details of the testing process and findings of the vulnerabilities to the management. Russel employs the commonly available vulnerability scoring framework called Common Vulnerability Scoring System (CVSS) v3.0 ratings for grading the severity and risk level of identified vulnerabilities in the report. For a specific SMB-based vulnerability, Russel assigned a score of 8.7.
What is the level of risk or level of severity of the SMB vulnerability as per CVSS v3.0 for the assigned score?

A. Critical
B. Low
C. Medium
D. High

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Lee has established a new startup where they develop android applications. In order to meet memory requirements of the company, Lee has hired a Cloud Service Provider, who offered memory space along with virtual systems. Lee was dissatisfied with their service and wanted to move to another CSP, but was denied as a part of the contract, which reads that the user cannot switch to another CSP.
What is this condition called?

A. Virtualization
B. Lock-in
C. Resource Isolation
D. Lock-up

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Jeffry, a penetration tester in Repotes Solutions Pvt. Ltd., is facing a problem in testing the firewall. By consulting other penetration testers and considering other penetration testing approaches, he was able to take critical decisions on how to test the firewall; he was finally successful in testing the firewall for vulnerabilities.
In which of the following sections of penetration testing report will Jeffry mention the above situation?

A. Timeline
B. Evaluation purpose
C. Assumptions
D. System description

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85

WallSec Inc. has faced several network security issues in the past and hired Williamson, a professional pentester, to audit its information systems. Before starting his work, Williamson, with the help of his legal advisor, signed an agreement with his client. This agreement states that confidential information of the client should not be revealed outside of the engagement.
What is the name of the agreement that Williamson and his client signed?

A. Non-disclosure agreement
B. TPOC agreement
C. Engagement letter
D. Authorization letter

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Tom is a networking manager in XYZ Inc. He and his team were assigned the task to store and update the confidential files present on a remote server using Network File System (NFS) client-server application protocol. Since the files are confidential, Tom was asked to perform this operation in a secured manner by limiting the access only to his team. As per the instructions provided to him, to use NFS securely, he employed the process of limiting the superuser access privileges only to his team by using authentication based on the team personnel identity.
Identify the method employed by Tom for securing access controls in NFS?

A. Root Squashing
B. nosuid
C. noexec
D. Suid

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
David is a penetration tester and he is attempting to extract password hashes from the Oracle database. Which of the following utilities should Dave employ in order to brute-force password hashes from Oracle databases?

A. TNS
B. Orabf
C. Opwg
D. OAT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following tasks is done after submitting the final pen testing report?

A. Kick-off meeting
B. System patching and hardening
C. Exploiting vulnerabilities
D. Mission briefing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Sam is auditing a web application for SQL injection vulnerabilities. During the testing, Sam discovered that the web application is vulnerable to SQL injection. He starts fuzzing the search field in the web application with UNION based SQL queries, however, he realized that the underlying WAF is blocking the requests. To avoid this, Sam is trying the following query:
UNION/**/SELECT/**/'/**/OR/**/1/**/=/**/1
Which of the following evasion techniques is Sam using?

A. Sam is using char encoding to bypass WAF
B. Sam is using obfuscated code to bypass WAF
C. Sam is using inline comments to bypass WAF
D. Sam is manipulating white spaces to bypass WAF

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Stanley, a pen tester needs to perform various tests to detect SQL injection vulnerabilities. He has to make a list of all input fields whose values could be used in crafting a SQL query. This includes the hidden fields of POST requests and then test them separately, attempting to interfere with the query and cause an error to generate as a result.
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. Dynamic Testing
B. Static Testing
C. Function Testing
D. Source Code Testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91

During the reconnaissance phase of a penetration test, you discovered that the client has deployed a firewall that only checks the TCP header information.
Which of the following techniques would you use to bypass the firewall?

A. Bypassing the firewall using tiny fragments
B. Bypassing the firewall by manipulating the IPID sequence number
C. Bypassing the firewall source routing
D. Bypassing the firewall using the IP address in place of an URL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
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:

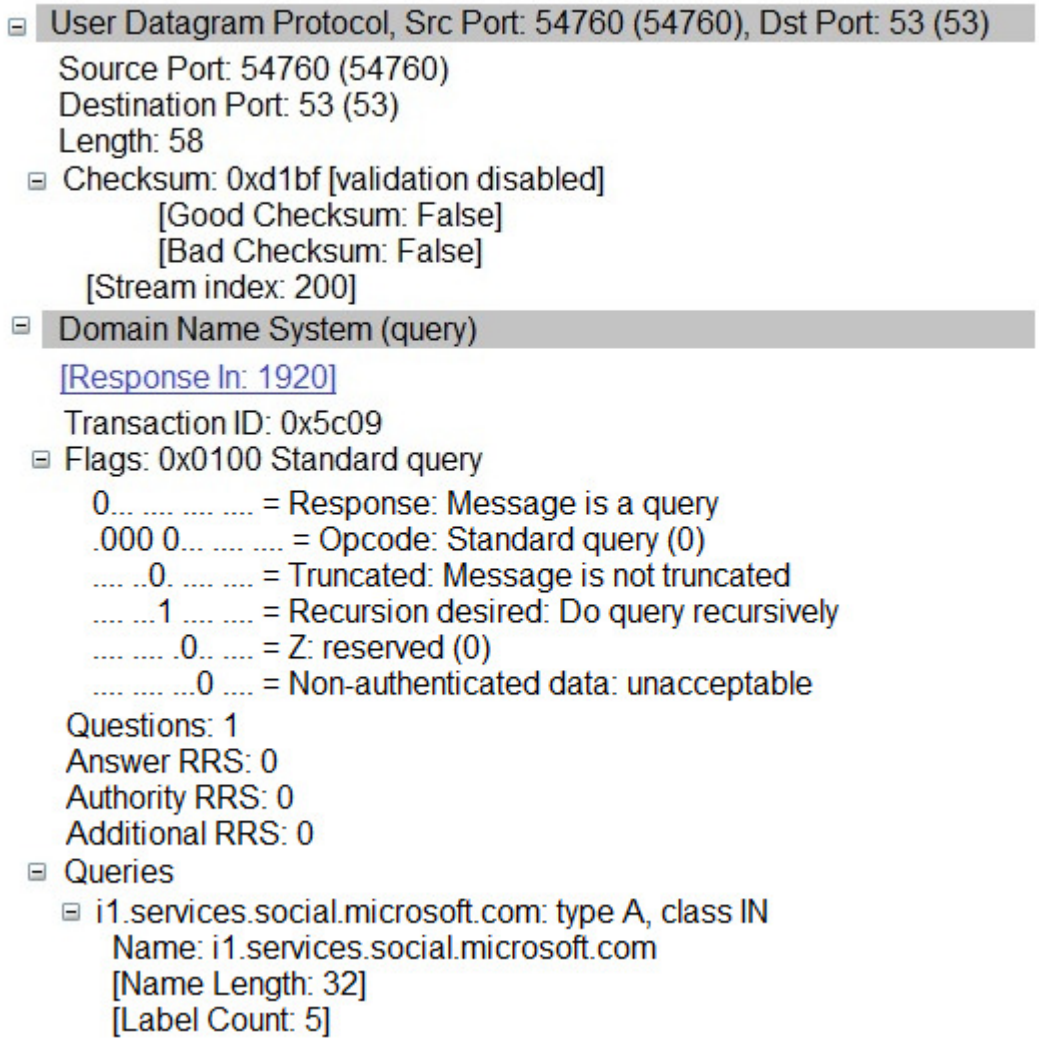
QUESTION 93
HDC Networks Ltd. is a leading security services company. Matthew works as a penetrating tester with this firm. He was asked to gather information about the target company. Matthew begins with social engineering by following the steps:
I. Secretly observes the target to gain critical information
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 94
Analyze the packet capture from Wireshark below and mark the correct statement.



A. It is an invalid DNS query
B. It is a DNS response message
C. It is an answer to the iterative query from Microsoft.com DNS server
D. It is Host (A record) DNS query message

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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 96
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 97
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 98
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 99
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 100
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 101
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 102
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 103
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 104
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 105
John is a penetration tester who wants to perform port scan on the DNS Server (IP address: 192.168.0.124) deployed in the perimeter. In his primary research, he identified that the DNS server is configured with default settings.
Since he is employing Nmap tool to perform port scanning, which of the following Nmap commands should John execute to port scan the DNS Server?

A. nmap -sS -sU –p 80 192.168.0.124
B. nmap -sS -sU –p 69 192.168.0.124
C. nmap -sS -sU –p 123 192.168.0.124
D. nmap -sS -sU –p 53 192.168.0.124

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
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 107
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 108
James, a penetration tester, found a SQL injection vulnerability in the website http://www.xsecurity.com. He used sqlmap and extracted the website's databases from the sql server, one of them being "offices." Which among the following sqlmap queries does James issue in order to extract the tables related to the database "offices"?

A. sqlmap -u "www.xsecurity.com" --dbs offices -T
B. sqlmap -u "www.xsecurity.com" --dbs offices --T
C. sqlmap -u "www.xsecurity.com" --dbs offices -tables
D. sqlmap -u "www.xsecurity.com" --dbs offices --tables

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Which of the following information security acts enables to ease the transfer of financial information between institutions and banks while making the rights of the individual through security requirements more specific?

A. The Digital Millennium Copyright Act (DMCA)
B. Sarbanes Oxley Act (SOX)
C. Computer Misuse Act 1990
D. Gramm-Leach-Bliley Act (GLBA)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
A security analyst at Techsoft Solutions is performing penetration testing on the critical IT assets of the company. As part of this process, he is simulating the methodologies and techniques of a real attacker because he is provided with limited or zero information about the company and its assets.
Identify the type of testing performed by the security analyst?

A. Announced testing
B. Blind testing
C. White-box testing
D. Unannounced testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
John is a newly appointed penetration testing manager in ABC Ltd. He is assigned a task to build a penetration testing team and asked to justify the return on investment (ROI).
To assess and predict the ROI of the team by considering the parameters like expected returns from the team and cost of investment, how can John calculate the ROI?

A. ROI = (Cost of investment – Expected returns)/Expected returns
B. ROI = (Expected returns – Cost of investment)/Cost of investment
C. ROI = (Expected returns + Cost of investment)/Cost of investment
D. ROI = (Cost of investment + Expected returns)/Expected returns

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
A penetration tester at Trinity Ltd. is performing IoT device testing. As part of this process, he is checking the IoT devices for open ports using port scanners such as Nmap. After identifying the open ports, he started using automated tools to check each open port for any exploitable vulnerabilities.
Identify the IoT security issues the penetration tester is trying to uncover?

A. Insecure software/firmware
B. Lack of transport encryption
C. Insecure network services
D. Insufficient security configurability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Peter is working on a pen testing assignment. During the reconnaissance phase, Peter discovered that the client's SYSLOG systems are taken off for four hours on the second Saturday of every month for maintenance. He wants to analyze the client's web pages for sensitive information without triggering their logging mechanism. There are hundreds of pages on the client's website and it is difficult to analyze all the information in just four hours.
What will Peter do to analyze all the web pages in a stealthy manner?

A. Use HTTrack to mirror the complete website
B. Use WayBackMachine
C. Perform reverse DNS lookup
D. Search the Internet, newsgroups, bulletin boards, and negative websites for information about the client

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
SecInfo is a leading cyber security provider who recently hired Andrew, a security analyst. He was assigned the task of identifying vulnerabilities in the NFC devices by performing an attack on them. In this process, he was present with his device in the close proximity with the NFC devices that are sharing data so that he can eavesdrop on the data and at the same time block the transmission to the receiver. He then manipulated the captured data and further relayed the data to the receiver.
Identify the type of attack performed by Andrew on the target NFC devices?

A. Ticket cloning
B. MITM attack
C. DoS attack
D. Virus attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Joe works as an engagement team lead with Xsecurity Inc. His pen testing team follows all the standard pentesting procedures, however, one of the team members inadvertently deletes a document containing the client's sensitive information. The client is suing Xsecurity for damages.
Which part of the Penetration Testing Contract should Joe have written better to avoid this lawsuit?

A. Objective of the penetration test
B. Indemnification clause
C. Fees and project schedule
D. Non-disclosure clause

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
A recent study from HyThech Technologies found that three of the most popular websites are having most commonly exploitable flaw in their web applications. Using this vulnerability, an attacker may inject malicious code that can be executed on a user's machine. Also, the study revealed that most sensitive target of this vulnerability is stealing session cookies. This helps attackers to duplicate the user session and access anything the user can perform on a website like manipulating personal information, creating fake social media posts, stealing credit card information and performing unauthorized financial transactions, etc.
Identify the vulnerability revealed by HyThech Technologies?

A. DoS vulnerability
B. Buffer overflow vulnerability

C. Insecure decentralization vulnerability
D. XSS vulnerability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
Stuart is a database penetration tester working with Regional Server Technologies. He was asked by the company to identify the vulnerabilities in its SQL database. Stuart wanted to perform a SQL penetration by passing some SQL commands through a web application for execution and succeeded with a command using a wildcard attribute indicator.
Which of the following strings is a wildcard attribute indicator?

A. ?Param1=foo&Param2=bar
B. %
C. @variable
D. @@variable

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
A web application developer is writing code for validating the user input. His aim is to verify the user input against a list of predefined negative inputs to ensure that the received input is not one among the negative conditions.
Identify the input filtering mechanism being implemented by the developer?

A. Black listing
B. White listing
C. Authentication
D. Authorization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
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 120
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 121
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 122
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 123
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 124
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 125
Adam is working as a senior penetration tester at Eon Tech Services Ltd. The company asked him to perform penetration testing on their database. The company informs Adam they use Microsoft SQL Server. As a part of the penetration testing, Adam wants to know the complete information about the company’s database. He uses

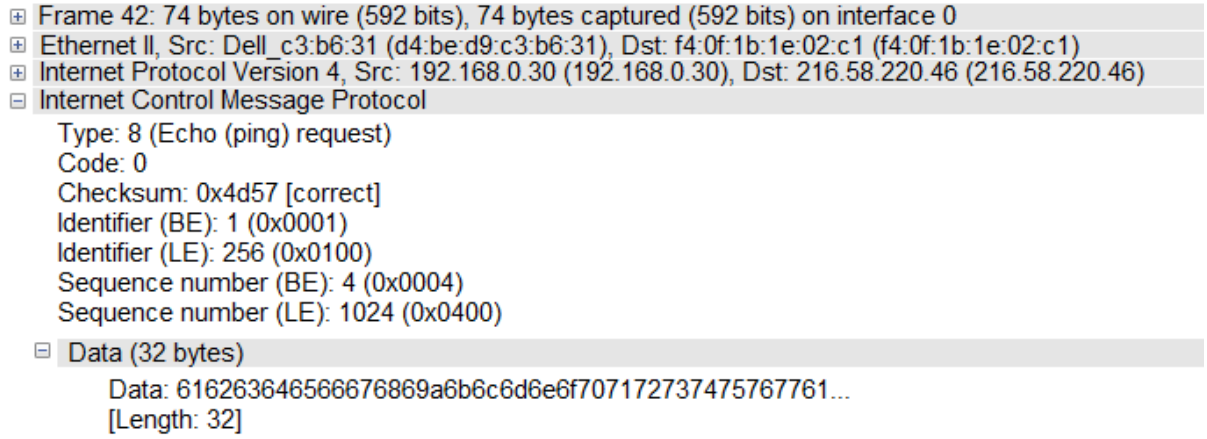
the Nmap tool to get the information.
Which of the following Nmap commands will Adam use to get the information?

A. nmap -p2051 --script ms-sql-info
B. nmap -p1801 --script ms-sql-info
C. nmap -p1443 --script ms-sql-info
D. nmap -p1521 --script ms-sql-info

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Analyze the ICMP packet below and mark the correct statement.

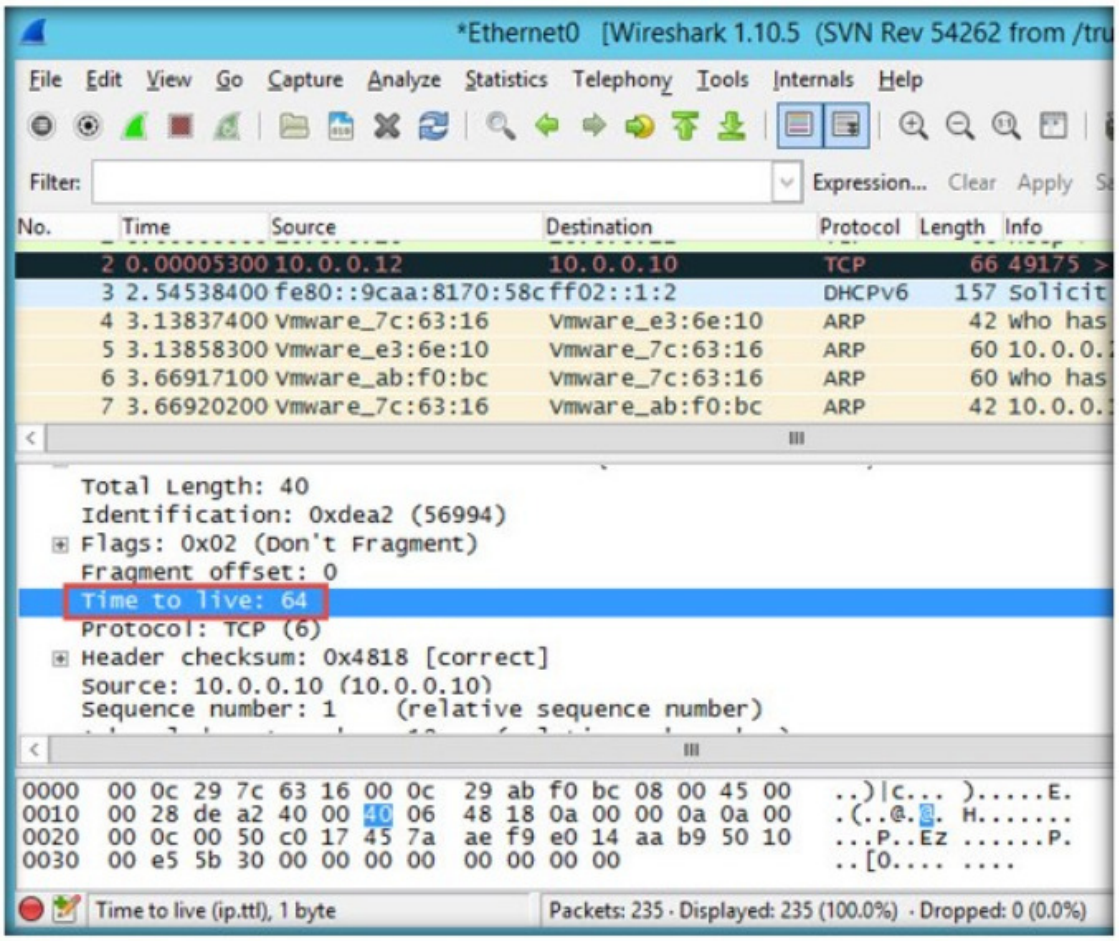


A. It is a ping packet that requires fragmentation, but the Don't Fragment flag is set
B. It is a ping request, but the destination port is unreachable
C. It is a ping response, when the destination host is unknown
D. It is a ping request, but the destination network is unreachable

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
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 128
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 129
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 130
Charles, a network penetration tester, is part of a team assessing the security of perimeter devices of an organization. He is using the following Nmap command to bypass the firewall:
nmap -D 10.10.8.5, 192.168.168.9, 10.10.10.12
What Charles is trying to do?

A. Packet Fragmentation
B. Cloaking a scan with decoys
C. Spoofing source address
D. Spoofing source port number

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
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 132
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 133
Rock is a disgruntled employee of XYZ Inc. He wanted to take revenge. For that purpose, he created a malicious software that automatically visits every page on the company's website, checks pages for important links to other content recursively, and indexes them in a logical flow. By using this malicious software, he gathered a lot of crucial information that is required to exploit the organization.
What is the type of software that Rock developed?

A. Web spider
B. Web fuzzer
C. Web scanner
D. Web proxy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
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:

QUESTION 135
As a normal three-way handshake mechanism system A sends an ACK packet to system B. However, system A does not send an ACK packet to system B. In this case, client B is waiting for an ACK packet from client A. What is the status of client B?

A. "Half-open"
B. "Filtered"
C. "Half-closed"
D. "Full-open"

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
GenSec Inc, a UK-based company, uses Oracle database to store all its data. The company also uses Oracle DataBase Vault to restrict users access to specific areas of their database. GenSec hired a senior penetration tester and security auditor named Victor to check the vulnerabilities of the company's Oracle DataBase Vault. He was asked to find all the possible vulnerabilities that can bypass the company's Oracle DB Vault. Victor tried different kinds of attacks to penetrate into the company's Oracle DB Vault and succeeded.
Which of the following attacks can help Victor to bypass GenSec's Oracle DB Vault?

A. Man-in-the-Middle Attack
B. Denial-of-Service Attack
C. Replay Attack
D. SQL Injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Michael, a penetration tester of Rolatac Pvt. Ltd., has completed his initial penetration testing and now he needs to create a penetration testing report for company's client, management, and top officials for their reference. For this, he created a report providing a detailed summary of the complete penetration testing process of the project that he has undergone, its outcomes, and recommendations for future testing and exploitation.
In the above scenario, which type of penetration testing report has Michael prepared?

A. Host report
B. Activity report
C. User report
D. Executive report

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
John is working as a cloud security analyst in an organization. The management instructed him to implement a technology in the cloud infrastructure which allows the organization to share the underlying cloud resources such as server, storage devices, and network.
Which of the following technologies John must employ?

A. VoIP technology
B. Virtualization technology
C. RFID technology
D. Site technology

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
The security team found the network switch has changed its behavior to learning mode and is functioning like a hub. The CAM table of the switch was filled with unnecessary traffic. Someone tried to penetrate into the network space by attacking the network switches. They wrote a report and submitted to higher authorities.
What kind of an attack did the attackers perform against the network switch?

A. DNS Poisoning
B. MITM Attack
C. MAC Flooding
D. ARP Poisoning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Which of the following pre-engagement documents identifies the systems to be tested, types of tests, and the depth of the testing?

A. Draft Report
B. Letter of Intent
C. Rule of Engagement
D. Authorization Letter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
George works at 3D-Networks Ltd as a Network Admin. He received an email from one of his clients stating that the client's company website has some flaws and they are receiving continuous emails from customers about the inconveniencies. While checking the web servers, he found loopholes with the DNS servers and he installed DNSSEC-Aware lookups. This made the site functional and the client was happy with the outcome. What problem does a Non-DNSSEC-Aware site face?

A. The users will get more information than they desired.
B. The user's commands will be delayed and the information they requested may be not delivered.
C. The site becomes slow and vulnerable
D. A mischievous Internet user can cut off the request and send back incorrect information by spoofing the response.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Which type of penetration testing will require you to send the Internal Control Questionnaires (ICQ) to the client?

A. White-box testing
B. Black-box testing
C. Blind testing
D. Unannounced testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
During a DHCP handshake in an IPv4 network, which of the following messages contains the actual IP addressing information for the clients to use?

A. DHCPDISCOVER
B. DHCPACK
C. REPLY
D. SOLICIT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
Depp Networks is a leader in providing ethical hacking services. They were tasked to examine the strength of a client network. After using a wide range of tests, they finally zeroed in on ICMP tunneling to bypass the firewall. What factor makes ICMP tunneling appropriate to bypass the firewall?

A. Deep packet inspection
B. Firewalls can not inspect ICMP packets
C. Firewalls can not handle the fragmented packets
D. The payload portion is arbitrary and not examined by most firewalls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
Gibson, a security analyst at MileTech Solutions, is performing cloud penetration testing. As part of this process, he needs to check for any governance and compliance issues against cloud services.
Which of the following documents helps Gibson in checking whether the CSP is regularly audited and certified for compliance issues?

A. Service level agreement
B. Data use agreement
C. ROE agreement
D. Nondisclosure agreement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
StarMotel is a prominent chain of hotels in the world that uses high-tech solutions to ease the stay of their guests. In those high-tech solutions, they deployed RFID cards using which a guest can get access to the allocated hotel room. Keeping an eye on the RFID technology and with an objective of exploiting it, John, a professional hacker, decided to hack it in order to obtain access to any room in the target hotel. In this process, he first pulled an RFID keycard from the trash of the target hotel and identified the master keycard code in several tries using an RFID card reading and writing tool. Then, he created its clone using a new RFID card that gave him free reign to roam in any hotel room in the building.
Identify the RFID attack John has performed on the target hotel?

A. RFID spoofing attack
B. Reverse engineering attack
C. RFID replay attack
D. Power analysis attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
An attacker impersonated himself as a pizza delivery boy and is waiting outside the target company. He observed that an employee of the company is gaining security approval to enter the campus. When the employee is opening the entrance door of the company, the attacker requested the employee to hold the door open to enter into the company.
In the above scenario, identify the technique used by the attacker to enter into the company?

A. Dumpster diving
B. Vishing
C. Tailgating
D. Phishing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
A disgruntled employee Robert targeted to acquire business secrets of the organization he is working in and wants to sell the same to a competing organization for some financial gain. He started gathering information about the organization and somehow came to know that the organization is conducting a meeting to discuss future business plans. To collect the information about the organization's business plans, he had built a listening device housed in his bag and arrived the meeting location wearing a suit and tie. One of the employees of the organization thought he was a senior executive from other branch who came to attend the meeting and readily took him to the meeting room. Robert waited until that employee left the meeting room and planted listening devices at multiple places in the room. Then, he went outside the building and started listening and recorded all the conversations in the meeting.
Identify the type of attack being performed by Robert on the target organization?

A. Vishing
B. Phishing
C. Shoulder surfing
D. Eavesdropping

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
A company identified critical vulnerability in its hyperconverged infrastructure that provides services such as computing, networking, and storage resources in a single system. Also, the company identified that this vulnerability may lead to various injection attacks that allow the attackers to execute malicious commands as the root users. The company decided to immediately implement appropriate countermeasure to defend against such attacks.
Which of the following defensive mechanisms should the company employ?

A. Data correlation
B. Patch management
C. Input validation
D. Session management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
Karen was running port scans on each machine of her network in order to identify suspicious ports on the target machines. She observed the following results during the port scan of a particular machine.
I. Some of the ports were not being acknowledged, i.e. no acknowledgment from the target machine
II. Some ports were responding with SYN + ACK packets
III. Some ports were responding with an RST packet

What should she interpret for the ports that did not return the acknowledgement?

A. She should that those ports as Closed ports
B. She should that those ports as Open ports
C. She should that those ports as Stealth ports
D. She should that those ports as Half Open ports

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: