312-50v11.VCEplus.premium.exam.125q

Number: 312-50v11
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

312-50v11

Certified Ethical Hacker v11 Exam

Version 1.0

Exam A

QUESTION 1
While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

A. Clickjacking
B. Cross-Site Scripting
C. Cross-Site Request Forgery
D. Web form input validation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2 Which service in a PKI will vouch for the identity of an individual or company?

A. KDC
B. CR
C. CBC
D. CA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3 Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

A. LDAP Injection attack
B. Cross-Site Scripting (XSS)
C. SQL injection attack
D. Cross-Site Request Forgery (CSRF)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

A. Application
B. Transport
C. Session
D. Presentation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

A. The WAP does not recognize the client's MAC address
B. The client cannot see the SSID of the wireless network
C. Client is configured for the wrong channel
D. The wireless client is not configured to use DHCP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
If you want to only scan fewer ports than the default scan using Nmap tool, which option would you use?

A. –r
B. –F
C. –P
D. –sP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7 Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

A. SOA
B. biometrics
C. single sign on
D. PKI

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

A. Social engineering
B. Piggybacking
C. Tailgating
D. Eavesdropping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

A. Traceroute
B. Hping
C. TCP ping
D. Broadcast ping

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10 Which is the first step followed by Vulnerability Scanners for scanning a network?

A. OS Detection
B. Firewall detection
C. TCP/UDP Port scanning
D. Checking if the remote host is alive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11 Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus
B. Multipart virus
C. Macro virus
D. Stealth virus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

A. Privilege Escalation
B. Shoulder-Surfing
C. Hacking Active Directory
D. Port Scanning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

A. The computer is not using a private IP address.
B. The gateway is not routing to a public IP address.
C. The gateway and the computer are not on the same network.
D. The computer is using an invalid IP address.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14 Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

A. 113
B. 69
C. 123
D. 161

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15 Due to a slowdown of normal network operations, the IT department decided to monitor internet traffic for all of the employees. From a legal standpoint, what would be troublesome to take this kind of measure?

A. All of the employees would stop normal work activities
B. IT department would be telling employees who the boss is
C. Not informing the employees that they are going to be monitored could be an invasion of privacy.
D. The network could still experience traffic slow down.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

A. Nikto
B. John the Ripper
C. Dsniff
D. Snort

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up. What is the most likely cause?

A. The network devices are not all synchronized.
B. Proper chain of custody was not observed while collecting the logs.
C. The attacker altered or erased events from the logs.
D. The security breach was a false positive.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.
What command is used to determine if the entry is present in DNS cache?

A. nslookup -fullrecursive update.antivirus.com
B. dnsnooping –rt update.antivirus.com
C. nslookup -norecursive update.antivirus.com
D. dns --snoop update.antivirus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19 Which of the following is an extremely common IDS evasion technique in the web world?

A. Spyware
B. Subnetting
C. Unicode Characters
D. Port Knocking

Correct Answer: C
Section: (none)

Explanation
Explanation/Reference:

QUESTION 20 John the Ripper is a technical assessment tool used to test the weakness of which of the following?

A. Passwords
B. File permissions
C. Firewall rulesets
D. Usernames

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning. What should Bob recommend to deal with such a threat?

A. The use of security agents in clients' computers
B. The use of DNSSEC
C. The use of double-factor authentication
D. Client awareness

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?

A. Circuit
B. Stateful
C. Application
D. Packet Filtering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23 By using a smart card and pin, you are using a two-factor authentication that satisfies

A. Something you are and something you remember
B. Something you have and something you know
C. Something you know and something you are
D. Something you have and something you are
Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
"........is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there." Fill in the blank with appropriate choice.

A. Evil Twin Attack
B. Sinkhole Attack
C. Collision Attack
D. Signal Jamming Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server. Based on this information, what should be one of your key recommendations to the bank?

A. Place a front-end web server in a demilitarized zone that only handles external web traffic
B. Require all employees to change their anti-virus program with a new one
C. Move the financial data to another server on the same IP subnet
D. Issue new certificates to the web servers from the root certificate authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Residual risk
B. Impact risk
C. Deferred risk
D. Inherent risk

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following is the best countermeasure to encrypting ransomwares?
A. Use multiple antivirus softwares
B. Pay a ransom

C. Keep some generation of off-line backup
D. Analyze the ransomware to get decryption key of encrypted data

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?

A. tcpsplice
B. Burp
C. Hydra
D. Whisker

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.

What is the best Nmap command you will use?

A. nmap -T4 -q 10.10.0.0/24
B. nmap -T4 -F 10.10.0.0/24
C. nmap -T4 -r 10.10.1.0/24
D. nmap -T4 -O 10.10.0.0/24

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization’s interest and your liabilities as a tester?

A. Service Level Agreement
B. Project Scope
C. Rules of Engagement
D. Non-Disclosure Agreement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31 Which of the following is the BEST way to defend against network sniffing?

A. Using encryption protocols to secure network communications
B. Register all machines MAC Address in a Centralized Database
C. Use Static IP Address
D. Restrict Physical Access to Server Rooms hosting Critical Servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

A. Iris patterns
B. Voice
C. Height and Weight
D. Fingerprints

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?

A. SFTP
B. Ipsec
C. SSL
D. FTPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

A. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
B. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
C. If (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permitD. If (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 35
Jim’s company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim’s company keeps the backup tapes in a safe in the office. Jim’s company is audited each year, and the results from this year’s audit show a risk because backup tapes are not stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

A. Encrypt the backup tapes and transport them in a lock box.
B. Degauss the backup tapes and transport them in a lock box.
C. Hash the backup tapes and transport them in a lock box.
D. Encrypt the backup tapes and use a courier to transport them.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL. What may be the problem?

A. Traffic is Blocked on UDP Port 53
B. Traffic is Blocked on TCP Port 80C. Traffic is Blocked on TCP Port 54
D. Traffic is Blocked on UDP Port 80

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Kismet
B. Abel
C. Netstumbler
D. Nessus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.

While monitoring the data, you find a high number of outbound connections. You see that IP’s owned by XYZ (Internal) and private IP’s are communicating to a Single Public IP. Therefore, the Internal IP’s are sending data to the Public IP.

After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.
What kind of attack does the above scenario depict?

A. Botnet Attack
B. Spear Phishing Attack
C. Advanced Persistent Threats

D. Rootkit Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Scenario1:
1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'.
3. Victim clicks to the interesting and attractive content URL.
4. Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' URL but actually he/she clicks to the content or URL that exists in thetransparent 'iframe' which is setup by the attacker.

What is the name of the attack which is mentioned in the scenario?

A. Session Fixation
B. HTML Injection
C. HTTP Parameter Pollution
D. Clickjacking Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The “ps” command shows that the “nc” file is running as process, and the netstat command shows the “nc” process is listening on a network port.

What kind of vulnerability must be present to make this remote attack possible?

A. File system permissions
B. Privilege escalation
C. Directory traversal
D. Brute force login

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41 Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?

Code:

```
#include <string.h> int main(){    char buffer[8];
strcpy(buffer, ““1111111111111111111111111111111””);} Output: Segmentation fault
```

A. C#

B. Python
C. Java
D. C++

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Internet Protocol Security IPsec is actually a suite pf protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.

A. Protect the payload and the headers
B. Encrypt
C. Work at the Data Link Layer
D. Authenticate

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

A. Make sure that legitimate network routers are configured to run routing protocols with authentication. B.
Disable all routing protocols and only use static routes
C. Only using OSPFv3 will mitigate this risk.
D. Redirection of the traffic cannot happen unless the admin allows it explicitly.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44 Which method of password cracking takes the most
time and effort?

A. Dictionary attack
B. Shoulder surfing
C. Rainbow tables
D. Brute force

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 45
An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gain access to the DNS server and redirect the direction www.google.com to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

A. MAC Flooding
B. Smurf Attack
C. DNS spoofing
D. ARP Poisoning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering that NMAP result below, which of the following is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

A. The host is likely a Linux machine.
B. The host is likely a printer.
C. The host is likely a router.
D. The host is likely a Windows machine.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

A. The amount of time and resources that are necessary to maintain a biometric system
B. How long it takes to setup individual user accounts
C. The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication informationD. The amount of time it takes to convert biometric data into a template on a smart card

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48 You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

A. nmap -A - Pn
B. nmap -sP -p-65535 -T5
C. nmap -sT -O -T0
D. nmap -A --host-timeout 99 -T1

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 49 What does the –oX flag do in
an Nmap scan?

A. Perform an eXpress scan
B. Output the results in truncated format to the screen
C. Output the results in XML format to a file
D. Perform an Xmas scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50 A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.
B. Determine the impact of enabling the audit feature.
C. Perform a cost/benefit analysis of the audit feature.
D. Allocate funds for staffing of audit log review.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51 Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?

A. Honeypots
B. Firewalls
C. Network-based intrusion detection system (NIDS)
D. Host-based intrusion detection system (HIDS)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52 The collection of potentially actionable, overt, and publicly available
information is known as

A. Open-source intelligence
B. Real intelligence
C. Social intelligence
D. Human intelligence

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

A. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
B. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
C. Symmetric encryption allows the server to security transmit the session keys out-of-band.
D. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
The change of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?

A. $1320
B. $440C. $100
D. $146

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55 What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

A. Man-in-the-middle attack
B. Meet-in-the-middle attack
C. Replay attack
D. Traffic analysis attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access. A camera captures people walking and identifies the individuals using Steve's approach.
After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:

A. Although the approach has two phases, it actually implements just one authentication factor
B. The solution implements the two authentication factors: physical object and physical characteristic
C. The solution will have a high level of false positives
D. Biological motion cannot be used to identify people

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
What is not a PCI compliance recommendation?

A. Use a firewall between the public network and the payment card data.
B. Use encryption to protect all transmission of card holder data over any public network.
C. Rotate employees handling credit card transactions on a yearly basis to different departments.
D. Limit access to card holder data to as few individuals as possible.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58 What is the minimum number of network connections in a multihomed firewall?

A. 3
B. 5
C. 4
D. 2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

A. Accept the risk
B. Introduce more controls to bring risk to 0%
C. Mitigate the risk
D. Avoid the risk

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?
A. All three servers need to be placed internally
B. A web server facing the Internet, an application server on the internal network, a database server on the internal network
C. A web server and the database server facing the Internet, an application server on the internal networkD. All three servers need to face the Internet so that they can communicate between themselves

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines.
Which one of the following tools the hacker probably used to inject HTML code?

A. Wireshark
B. Ettercap
C. Aircrack-ng
D. Tcpdump

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

A. ESP transport mode
B. ESP confidential
C. AH permiscuous
D. AH Tunnel mode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

A. Exploration
B. Investigation
C. Reconnaissance
D. Enumeration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 64 Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

A. Macro virus
B. Stealth/Tunneling virus

C. Cavity virus
D. Polymorphic virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65 The “Gray-box testing” methodology enforces what kind of restriction?

A. Only the external operation of a system is accessible to the tester.
B. The internal operation of a system in only partly accessible to the tester.
C. Only the internal operation of a system is known to the tester.
D. The internal operation of a system is completely known to the tester.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66 When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator’s Computer to update the router configuration. What type of an alert is this?

A. False negative
B. True negativeC. True positive
D. False positive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing – Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?

A. Paros Proxy
B. BBProxy
C. Blooover
D. BBCrack

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 68
When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?

A. http-methods
B. http enum
C. http-headers
D. http-git

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on behavioral attributes.
B. A biometric system that bases authentication decisions on physical attributes.
C. An authentication system that creates one-time passwords that are encrypted with secret keys.
D. An authentication system that uses passphrases that are converted into virtual passwords.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70 Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering
B. Eavesdropping
C. Scanning
D. Sniffing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS
B. CAPTCHA
C. IANA
D. IETF

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72 Why is a penetration test considered to be more thorough than vulnerability scan?

A. Vulnerability scans only do host discovery and port scanning by default.
B. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.
C. It is not – a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
D. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Bob received this text message on his mobile phone: “Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com”. Which statement below is true?

A. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
B. This is a scam because Bob does not know Scott.
C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.
D. This is probably a legitimate message as it comes from a respectable organization.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
env x=’(){ :;};echo exploit’ bash –c ‘cat/etc/passwd’

What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

A. Removes the passwd file
B. Changes all passwords in passwd
C. Add new user to the passwd file
D. Display passwd content to prompt

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75 Which of the following is assured by the use of a hash?

A. Authentication
B. Confidentiality
C. Availability
D. Integrity

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which results will be returned with the following Google search query? site:target.com – site:Marketing.target.com
accounting

A. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.
B. Results matching all words in the query.
C. Results for matches on target.com and Marketing.target.com that include the word “accounting”D. Results matching “accounting” in domain target.com but not on the site Marketing.target.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

A. OPPORTUNISTICTLS
B. UPGRADETLS
C. FORCETLS
D. STARTTLS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78 In the field of cryptanalysis, what is meant by a
“rubber-hose” attack?

A. Forcing the targeted keystream through a hardware-accelerated device such as an ASIC.
B. A backdoor placed into a cryptographic algorithm by its creator.
C. Extraction of cryptographic secrets through coercion or torture.
D. Attempting to decrypt ciphertext by making logical assumptions about the contents of the original plaintext.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

A. tcp.srcport= = 514 && ip.src= = 192.168.0.99
B. tcp.srcport= = 514 && ip.src= = 192.168.150
C. tcp.dstport= = 514 && ip.dst= = 192.168.0.99
D. tcp.dstport= = 514 && ip.dst= = 192.168.0.150

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80 What two conditions must a digital signature meet?

A. Has to be the same number of characters as a physical signature and must be unique.
B. Has to be unforgeable, and has to be authentic.
C. Must be unique and have special characters.
D. Has to be legible and neat.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access the user and password information stored in the company's SQL database.
B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
C. Attempts by attackers to access password stored on the user's computer without the user's knowledge.
D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82 What is correct about digital signatures?

A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
B. Digital signatures may be used in different documents of the same type.
C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 83
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
B. He will activate OSPF on the spoofed root bridge.
C. He will repeat this action so that it escalates to a DoS attack.
D. He will repeat the same attack against all L2 switches of the network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

A. John the Ripper
B. SET
C. CHNTPW
D. Cain & Abel

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
What does a firewall check to prevent particular ports and applications from getting packets into an organization?

A. Transport layer port numbers and application layer headers
B. Presentation layer headers and the session layer port numbers
C. Network layer headers and the session layer port numbers
D. Application layer port numbers and the transport layer headers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", the user is directed to a phishing site.

Which file does the attacker need to modify?

A. Boot.ini
B. Sudoers
C. Networks
D. Hosts

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 87 _________ is a set of extensions to DNS that provide the origin authentication of DNS data to DNS clients (resolvers) so as to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.

A. DNSSEC

B. Resource records
C. Resource transfer
D. Zone transfer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88 Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

A. Preparation phase
B. Containment phaseC. Identification phase
D. Recovery phase

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described?

A. Multi-cast mode
B. Promiscuous mode
C. WEM
D. Port forwarding

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90 A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems.

What is the best security policy concerning this setup?

A. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.
B. As long as the physical access to the network elements is restricted, there is no need for additional measures.
C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
D. The operator knows that attacks and down time are inevitable and should have a backup site.
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91 PGP, SSL, and IKE are all examples of which type of cryptography?

A. Digest
B. Secret Key
C. Public Key
D. Hash Algorithm

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?

A. Scanning
B. Footprinting
C. Enumeration
D. System Hacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer’s software and hardware without the owner’s permission. Their intention can either be to simply gain knowledge or to illegally make changes.
Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

A. White Hat
B. Suicide Hacker
C. Gray Hat
D. Black Hat

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.

What is this type of DNS configuration commonly called?
A. DynDNS
B. DNS Scheme
C. DNSSEC
D. Split DNS

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 95 What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment?

A. Behavioral based
B. Heuristics based
C. Honeypot based
D. Cloud based

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96 Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace
B. Nessus
C. OpenVAS
D. tcptraceroute

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packetfiltering of the firewall?

A. Session hijacking
B. Firewalking
C. Man-in-the middle attack
D. Network sniffing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following is not a Bluetooth attack?

A. Bluedriving
B. Bluesmacking
C. Bluejacking

D. Bluesnarfing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99 What is the role of test automation in security testing?

A. It is an option but it tends to be very expensive.
B. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.
C. Test automation is not usable in security due to the complexity of the tests.
D. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.

What should you do?

A. Confront the client in a respectful manner and ask her about the data.
B. Copy the data to removable media and keep it in case you need it.
C. Ignore the data and continue the assessment until completed as agreed.
D. Immediately stop work and contact the proper legal authorities.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
While using your bank’s online servicing you notice the following string in the URL bar:
“http: // www. MyPersonalBank. com/ account?id=368940911028389&Damount=10980&Camount=21”
You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflects the changes. Which type of vulnerability is present on this site?

A. Cookie Tampering
B. SQL Injection
C. Web Parameter Tampering
D. XSS Reflection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102 The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?

A. ACK
B. SYN
C. RST
D. SYN-ACK

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103 Which type of security feature stops vehicles from crashing through the doors of a building?

A. Bollards
B. Receptionist
C. Mantrap
D. Turnstile

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. Which of the following options can be useful to ensure the integrity of the data?

A. The CFO can use a hash algorithm in the document once he approved the financial statements B.
The CFO can use an excel file with a password
C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document D.
The document can be sent to the accountant using an exclusive USB for that document

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105 What is the purpose of a demilitarized zone on a network?

A. To scan all traffic coming through the DMZ to the internal network
B. To only provide direct access to the nodes within the DMZ and protect the network behind it
C. To provide a place to put the honeypot
D. To contain the network devices you wish to protect
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106 Which of the following Linux commands will resolve a domain name into IP address?

A. >host-t a hackeddomain.com
B. >host-t ns hackeddomain.com
C. >host -t soa hackeddomain.com
D. >host -t AXFR hackeddomain.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107 Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

A. Linux
B. Unix
C. OS X
D. Windows

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108 Which regulation defines security and privacy controls for Federal information systems and organizations?

A. HIPAA
B. EU Safe Harbor
C. PCI-DSS
D. NIST-800-53

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109 What is a “Collision attack” in cryptography?

A. Collision attacks try to get the public key
B. Collision attacks try to break the hash into three parts to get the plaintext value
C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key
D. Collision attacks try to find two inputs producing the same hash

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110 Which of the following tools can be used for passive OS fingerprinting?

A. nmap
B. tcpdump
C. tracert
D. ping

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111 Which of the following describes the characteristics of a Boot Sector Virus?

A. Modifies directory table entries so that directory entries point to the virus code instead of the actual program.
B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.
C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.
D. Overwrites the original MBR and only executes the new virus code.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool
B. Use a scan tool like Nessus
C. Check MITRE.org for the latest list of CVE findings
D. Create a disk image of a clean Windows installation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113 Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. nessus
B. tcpdump
C. ethereal
D. jack the ripper

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114 DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

A. Spanning tree
B. Dynamic ARP Inspection (DAI)
C. Port security
D. Layer 2 Attack Prevention Protocol (LAPP)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

A. Disable unused ports in the switches
B. Separate students in a different VLAN
C. Use the 802.1x protocol
D. Ask students to use the wireless network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
A company’s policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?

A. tcp.port = = 21
B. tcp.port = 23
C. tcp.port = = 21 | | tcp.port = =22
D. tcp.port ! = 21

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 117 You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration? alert tcp any any -> 192.168.100.0/24 21 (msg: ““FTP on the network!””;)

A. A firewall IPTable
B. FTP Server rule
C. A Router IPTable
D. An Intrusion Detection System

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following program infects the system boot sector and the executable files at the same time?

A. Polymorphic virus
B. Stealth virus
C. Multipartite VirusD. Macro virus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

A. Randomizing
B. Bounding
C. Mutating
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A. Protocol analyzer
B. Network sniffer
C. Intrusion Prevention System (IPS)
D. Vulnerability scanner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the Transport Layer Security (TLS) protocols defined in RFC6520.

What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A. Public
B. Private
C. Shared
D. Root

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122 Why should the security analyst disable/remove unnecessary ISAPI filters?

A. To defend against social engineering attacks
B. To defend against webserver attacks
C. To defend against jailbreaking
D. To defend against wireless attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123 Which of the following is a component of a risk assessment?

A. Administrative safeguards
B. Physical security
C. DMZ
D. Logical interface

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email message looks like this:

From: jim_miller@companyxyz.com
To: michelle_saunders@companyxyz.com
Subject: Test message
Date: 4/3/2017 14:37
The employee of CompanyXYZ receives your email message.

This proves that CompanyXYZ's email gateway doesn't prevent what?

A. Email Masquerading
B. Email Harvesting
C. Email Phishing
D. Email Spoofing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations. Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA. In this context, what can you say?

A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
B. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
C. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstationsD. Bob is partially right. DMZ does not make sense when a stateless firewall is available

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: