PassQueen
a.k.a dumpsqueen.com

Certified Ethical Hacker Exam (CEH v11)

ECCouncil 312-50v11

Version Demo

Total Demo Questions: 66

Total Premium Questions: 662

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Information Security and Ethical Hacking Overview	94
Topic 2, Reconnaissance Techniques	117
Topic 3, System Hacking Phases and Attack Techniques	109
Topic 4, Network and Perimeter Hacking	111
Topic 5, Web Application Hacking	82
Topic 6, Wireless Network Hacking	39
Topic 7, Mobile Platform, IoT, and OT Hacking	29
Topic 8, Cloud Computing	22
Topic 9, Cryptography	59
Total	662

QUESTION NO: 1

Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

A. [inurl:]

B. [info:]

C. [site:]

D. [related:]

ANSWER: D

Explanation:

The correct operator is **[related:]**. When it is followed by a target website address, such as `related:example.com`, Google uses the supplied URL as a point of comparison and returns websites it considers similar or related. In reconnaissance, this can help an ethical hacker identify organizations in the same market, competitors, affiliated services, alternative providers, or sites with comparable subject matter. Those results can provide useful context about the target's public-facing ecosystem and may suggest additional domains or technologies worth investigating within an authorized assessment scope.

This use aligns directly with the question's requirement to locate sites similar to a specified URL, rather than merely locating pages containing a term or restricting results to a particular domain. Google provides an Advanced Search interface for refining and targeting searches at Google Advanced Search. For practical documentation of the `related:` search operator and its URL-based similarity function, see Ahrefs' overview of Google search operators: Google Advanced Search Operators. As with all reconnaissance techniques, searches should be conducted only against targets and information-gathering activities explicitly authorized by the system owner.

QUESTION NO: 2 - (SIMULATION)

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

ANSWER: See the explanation for the answer

Explanation:

Correct answer: B. `nmap -T4 -F 10.10.0.0/24`

This scans the local `10.10.0.0/24` network using aggressive timing (`-T4`) and Nmap's fast scan option (`-F`), which checks a reduced set of common ports. It is the best choice for quickly discovering/enumerating systems on that subnet.

`-T4`: faster/aggressive timing template.
`-F`: fast mode; scans fewer, commonly used ports.
`10.10.0.0/24`: includes hosts in the same subnet as `10.10.0.5`.

The other choices are unsuitable: `-q` is not the intended fast discovery option, `-r` only disables port randomization and targets the wrong subnet, and `-O` performs slower OS detection.

QUESTION NO: 3

In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details. Ignorant users usually fall prey to this scam.

Which of the following statement is incorrect related to this attack?

A. Do not reply to email messages or popup ads asking for personal or financial information

B. Do not trust telephone numbers in e-mails or popup ads

C. Review credit card and bank account statements regularly

D. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks

E. Do not send credit card numbers, and personal or financial information via e-mail

ANSWER: D

Explanation:

The scenario describes phishing: an attacker impersonates a trusted organization, such as PayPal, and uses an urgent account-related message to persuade the recipient to disclose payment-card details, PINs, or other sensitive information. The incorrect statement is “Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks” because phishing is primarily a social-engineering attack, not necessarily a malware infection or a network intrusion that endpoint security software can reliably identify. Although modern security products and email gateways may flag some malicious messages, URLs, attachments, or known fraudulent domains, they cannot very easily or consistently recognize every deceptive message—especially newly created or carefully tailored phishing emails. Detection also depends on reputation data, signatures, content analysis, and user reporting, all of which can be bypassed or delayed. Effective phishing defense therefore requires cautious user behavior, independent verification of account requests, and avoiding the disclosure of credentials or financial information in response to unsolicited communications. PayPal specifically advises users to forward suspicious emails to its phishing-reporting address and not to provide account information through suspicious links. See PayPal’s guidance for reporting suspicious messages and the FTC’s phishing-scam guidance.

QUESTION NO: 4

According to the NIST cloud deployment reference architecture, which of the following provides connectivity and transport services to consumers?

A. Cloud connector

B. Cloud broker

C. Cloud carrier

D. Cloud provider

ANSWER: C

Explanation:

Cloud carrier is correct. In the NIST Cloud Computing Reference Architecture, the cloud carrier is the intermediary responsible for providing the connectivity and transport that enables a cloud consumer to access cloud services delivered by a cloud provider. This role covers the communications path between consumer and provider, such as telecommunications networks, internet connectivity, and associated transport arrangements. The carrier may supply network access directly or through other network providers, but its essential function is to move cloud-service traffic reliably between the parties.

NIST distinguishes this transport role from the entities that offer, consume, manage, or aggregate cloud services. The definition is therefore based on the carrier’s responsibility for the network connection and delivery path, rather than ownership or operation of the cloud application, platform, or infrastructure itself. In practical terms, a consumer’s ability to reach a hosted cloud environment depends on the connectivity services represented by the cloud carrier role. NIST’s reference architecture explicitly identifies the cloud carrier as the party that provides connectivity and transport of cloud services from providers to consumers. See NIST SP 500-292: Cloud Computing Reference Architecture and the NIST publication record.

QUESTION NO: 5

An ethical hacker is preparing a final report after completing an authorized penetration test. Which section should provide management with a high-level description of the most important findings, associated business risk, and overall security posture?

A. Executive summary

B. Chain of custody

C. Rules of Engagement

D. Packet capture appendix

ANSWER: A

Explanation:

Executive summary is correct because it presents the assessment results in business-oriented language for decision makers. It summarizes the overall scope, major findings, risk implications, and key recommendations without requiring management to review detailed exploit evidence, raw scan output, or technical reproduction steps.

A technical findings section contains the detailed vulnerabilities, affected assets, evidence, severity ratings, and remediation guidance needed by security and system administrators. The rules of engagement defines the testing boundaries before the assessment, while a chain-of-custody record documents handling of evidence. NIST identifies reporting as an important phase of security testing and recommends communicating assessment results in a form appropriate to stakeholders. See NIST SP 800-115, Technical Guide to Information Security Testing and Assessment.

QUESTION NO: 6

Shiela is an information security analyst working at HiTech Security Solutions. She is performing service version discovery using Nmap to obtain information about the running services and their versions on a target system.

Which of the following Nmap options must she use to perform service version discovery on the target host?

A. -sN

B. -sV

C. -sX

D. -sF

ANSWER: B

Explanation:

The correct Nmap option is `-sV`. This option enables service and version detection, causing Nmap to probe open ports and analyze service responses to identify the application protocol, product name, version, and sometimes additional details such as the device type or operating system family. For example, when an open port is commonly associated with a web server, Nmap can send protocol-specific probes and use the returned banner or response characteristics to distinguish products and versions. This information is important during authorized reconnaissance because known service versions can be correlated with vendor advisories, patch status, and potential security exposure. Nmap's service detection is configurable through options such as `--version-intensity`, which controls the breadth of probes used, but `-sV` is the primary switch that activates version detection. The Nmap Reference Guide documents `-sV` as the option for probing open ports to determine service and version information. See the Nmap service and version detection reference and the Nmap Reference Guide for the official syntax and operational details.

QUESTION NO: 7

Which Intrusion Detection System is 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)

ANSWER: C

Explanation:

Network-based intrusion detection system (NIDS) is the appropriate choice because it monitors packets and network activity traversing a defined network location rather than operating only on an individual endpoint. In a large environment, sensors can be placed at high-value observation points, such as network boundaries, data-center uplinks, demilitarized zones, or segments containing critical systems. This placement gives defenders visibility into communications involving many devices and enables scrutiny of traffic entering, leaving, or moving through sensitive segments.

A NIDS analyzes observed traffic for suspicious signatures, protocol anomalies, and behavioral indicators that may reveal reconnaissance, exploitation attempts, command-and-control activity, or lateral movement. Its segment-oriented visibility makes it particularly useful when the protection objective is to watch a critical portion of the network as a whole. Effective deployment includes selecting locations where the sensor can see the relevant traffic, ensuring encrypted-traffic monitoring is addressed where appropriate, and integrating alerts with incident-response processes. NIST describes intrusion-detection technologies and deployment considerations in its Guide to Intrusion Detection and Prevention Systems (IDPS); further practical network-monitoring context is provided by CISA's attack-surface management resources.

QUESTION NO: 8

During an authorized assessment, an ethical hacker sends a TCP SYN packet to a target port and receives a SYN/ACK response. Instead of completing the TCP three-way handshake, the tester sends an RST packet. Which type of Nmap scan uses this behavior?

A. TCP connect scan

B. TCP SYN scan

C. TCP ACK scan

D. UDP scan

ANSWER: B

Explanation:

TCP SYN scan is correct because it sends a SYN packet and determines that a port is open when a SYN/ACK is received. Nmap then terminates the connection with an RST rather than completing the handshake. This is commonly called a half-open scan and is implemented with the `-sS` option. Nmap documents SYN scanning in its TCP SYN scan reference.

QUESTION NO: 9

Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules. Which of the following types of firewalls can protect against SQL injection attacks?

A. Data-driven firewall

B. Packet firewall

C. Web application firewall

D. Stateful firewall

ANSWER: C

Explanation:

Web application firewall is correct because it operates at the HTTP/HTTPS application layer and is designed to inspect web requests and responses for patterns associated with attacks against web applications. SQL injection occurs when untrusted input is incorporated into a database query in a way that changes the query's intended meaning. A web application firewall can apply rule sets, signatures, protocol validation, and anomaly detection to identify and block suspicious SQL syntax or injection payloads in parameters, form fields, cookies, and request bodies before they reach the application and its database. This makes it a valuable compensating control for publicly exposed web applications, particularly while application-level fixes are being deployed. It is not a substitute for secure development: the primary defense remains parameterized queries (prepared statements), along with server-side input validation and least-privilege database accounts. OWASP identifies web application firewalls as an additional defense that can help detect and block common injection attempts, while emphasizing that applications must prevent injection through safe query construction. See the OWASP Web Application Firewall guidance and OWASP's SQL Injection Prevention Cheat Sheet.

QUESTION NO: 10

Which of the following are well known password-cracking programs?

A. L0phtcrack

B. NetCat

C. Jack the Ripper

D. Netbus

E. John the Ripper

ANSWER: A E

Explanation:

L0phtcrack and **John the Ripper** are well-known password-auditing and password-recovery tools that may be used by authorized security professionals to assess password strength. L0phtCrack is historically associated with auditing Windows password hashes, including the recovery or cracking of weak passwords from captured hash data. Its purpose in an authorized engagement is to identify credentials that are vulnerable because of weak, reused, or easily guessed passwords, allowing an organization to improve password policy and account security.

John the Ripper is a widely used open-source password-security auditing tool. It supports multiple hash formats and uses methods such as dictionary-based guessing, rules, and brute-force-style candidate generation to test whether password hashes can be recovered. This makes it useful for demonstrating the real-world impact of inadequate password choices and for validating password-hardening controls. Both tools should only be used against systems, hashes, and accounts for which explicit authorization has been obtained. The official project resources describe John the Ripper as a fast password cracker and provide documentation on its supported use: Openwall: John the Ripper password cracker. L0phtCrack product information and its Windows password-auditing focus are available at L0phtCrack.

QUESTION NO: 11

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes Wi-Fi sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, even after the device is out of the communication zone.

Which of the following attacks is performed by Clark in the above scenario?

A. Man-in-the-disk attack

B. iOS jailbreaking

C. iOS trustjacking

D. Exploiting SS7 vulnerability

ANSWER: C

Explanation:

iOS trustjacking is correct because the scenario centers on an attacker-controlled computer becoming a trusted synchronization endpoint for an iPhone. Trustjacking is a technique in which a victim connects and authorizes an iOS device with a malicious or compromised computer, then enables iTunes Wi-Fi synchronization. Once the computer has that trust relationship, it can continue interacting with the device wirelessly after the USB cable is removed, subject to the relevant Wi-Fi connectivity and synchronization conditions. This trusted connection can expose sensitive device information and permit monitoring or access through the compromised host.

The essential indicators are the initial physical connection to a hostile public computer, establishment of device trust, and activation of iTunes Wi-Fi sync. These actions create the persistent trusted pairing relationship exploited in trustjacking; the attack does not depend on compromising cellular signaling or merely modifying application storage. Symantec's research describes how iTunes Wi-Fi sync can be abused after a device is paired with an attacker's computer: Symantec Threat Intelligence: Trustjacking. Apple also documents the device-sync feature and its wireless-sync behavior in Apple iTunes User Guide.

QUESTION NO: 12

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, PUT, DELETE, 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

ANSWER: A

Explanation:

`http-methods` is the Nmap Scripting Engine script specifically designed to enumerate the HTTP methods supported by a web server. It sends an `OPTIONS` request to the target path and reports the methods returned by the server, such as GET, POST, HEAD, PUT, DELETE, TRACE, CONNECT, or others. This is valuable during web-server reconnaissance because enabled methods define the operations a client may request and can reveal an unnecessarily broad or risky server configuration. In particular, discovering support for PUT or DELETE warrants further authorized testing of the server's access controls and WebDAV-related behavior, since the methods may permit modification or removal of resources when permissions are improperly configured. The script can be run against HTTP services with a command such as `nmap --script http-methods -p 80,443 target`; the script also supports arguments for the request path and for restricting displayed methods. Nmap's official NSE documentation lists `http-methods` as the script that performs HTTP method enumeration and describes its OPTIONS-based approach. See the official http-methods NSE script documentation and the Nmap Scripting Engine guide.

QUESTION NO: 13

Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS

B. A zone transfer is accomplished with the nslookup service

C. A zone transfer passes all zone information that a DNS server maintains

D. A zone transfer passes all zone information that a nslookup server maintains

E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections

F. Zone transfers cannot occur on the Internet

ANSWER: A C E

Explanation:

“A zone transfer is accomplished with the DNS” is correct because a zone transfer is a DNS protocol operation used to replicate authoritative zone data between DNS servers, commonly from a primary server to authorized secondary servers. The standardized full-zone transfer mechanism is AXFR, while IXFR can transfer only incremental changes. RFC 5936 defines AXFR as a DNS transaction that transfers the contents of a DNS zone and specifies that the transfer uses TCP, normally on DNS port 53. See RFC 5936: DNS Zone Transfer Protocol.

“A zone transfer passes all zone information that a DNS server maintains” is correct in the context of a full AXFR transfer. AXFR provides the complete set of resource records for the requested authoritative zone, allowing a secondary authoritative server to obtain a synchronized copy of that zone’s data. This can include host, mail-routing, name-server, and other records published within the zone.

“A zone transfer can be prevented by blocking all inbound TCP port 53 connections” is correct for preventing remote systems from initiating zone-transfer requests to the protected DNS server. Since AXFR uses TCP, filtering inbound TCP port 53 blocks that request path. In operational environments, administrators generally combine network filtering with DNS-server transfer authorization controls, allowing transfers only to specifically approved secondary servers. BIND documents this practice through its zone-transfer access-control configuration, such as `allow-transfer`; see BIND 9 Administrator Reference Manual.

QUESTION NO: 14

These hackers have limited or no training and know how to use only basic techniques or tools.

What kind of hackers are we talking about?

A. Black-Hat Hackers A

B. Script Kiddies

C. White-Hat Hackers

D. Gray-Hat Hacker

ANSWER: B

Explanation:

Script Kiddies is the correct classification. This term describes inexperienced individuals with limited technical knowledge who typically rely on readily available scripts, exploit kits, automated scanners, and publicly released tools rather than developing exploits or techniques themselves. They may be able to launch attacks by following tutorials or copying commands, but commonly have little understanding of the underlying vulnerabilities, network protocols, payload behavior, or operational consequences. In ethical-hacking training, recognizing this attacker profile helps defenders understand that even relatively unsophisticated adversaries can create real risk when powerful tools and published proof-of-concept exploits are easily accessible. Effective defense therefore requires timely patching, secure configuration, endpoint monitoring, and detection of known malicious tool behavior—not merely protection against highly advanced custom attacks. EC-Council’s CEH materials categorize script kiddies as hackers who have limited or no training and use basic techniques or tools. This is

also consistent with the broader security-industry definition of the term as an unskilled attacker using scripts created by others. See EC-Council's overview of hacker types and the CISA guidance on understanding cyber threats.

QUESTION NO: 15

Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands. Which of the following commands was used by Clark to hijack the connections?

A. btlejack-f 0x129f3244-j

B. btlejack -c any

C. btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s

D. btlejack -f 0x9c68fd30 -t -m 0x1 fffffffff

ANSWER: D

Explanation:

`btlejack -f 0x9c68fd30 -t -m 0x1 fffffffff` is the command used in the BTLEJack hijacking workflow. BTLEJack targets Bluetooth Low Energy connections by first recovering connection parameters, including the Access Address, and then following the target connection. In this command, `-f` supplies the recovered Access Address to follow, while the remaining parameters configure the takeover operation and the channel-map information required to remain synchronized with the BLE connection. Once synchronization and connection parameters have been established, BTLEJack can inject packets that take over the connection, enabling interception of application data exchanged by the connected devices. This is the operational objective described by a Btlejacking attack: gaining control of an existing BLE link rather than merely discovering nearby BLE advertising activity. The BTLEJack project documentation describes connection recovery, following, and hijacking capabilities and provides the tool's command-line workflow. BLE connection behavior, including use of an Access Address and channel map, is defined by the Bluetooth Core Specification. See the BTLEJack project documentation and the Bluetooth Core Specification.

QUESTION NO: 16

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

A. 110

B. 135

C. 139

D. 161

E. 445

F. 1024

G. 137 and 138

ANSWER: C E G

Explanation:

For a firewall policy intended to stop NetBIOS-related Windows file-sharing and discovery traffic, TCP port 139, TCP port 445, and UDP ports 137 and 138 should be blocked at the network perimeter. NetBIOS Session Service uses TCP 139 for session-oriented connections, including traditional SMB-over-NetBIOS communication. TCP 445 carries SMB directly over

TCP/IP and is therefore essential to block when preventing exposure of Windows file-sharing services, even when NetBIOS-over-TCP/IP is not being used. NetBIOS Name Service uses UDP 137 for name registration and resolution, while NetBIOS Datagram Service uses UDP 138 for connectionless datagram traffic such as browser and discovery communications. Blocking this complete set prevents the principal NetBIOS name, datagram, session, and related SMB paths from traversing the firewall. Microsoft's port-requirements documentation identifies UDP 137 and 138, TCP 139, and TCP 445 as the relevant NetBIOS/SMB ports: Microsoft service overview and network port requirements. Microsoft also documents the relationship between NetBIOS name services and Windows name resolution in its NetBIOS name-resolution guidance.

QUESTION NO: 17

_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

A. Trojan

B. RootKit

C. DoS tool

D. Scanner

E. Backdoor

ANSWER: B

Explanation:

RootKit is correct because a rootkit is specifically designed to conceal malicious activity and maintain covert, privileged access on a compromised system. Its concealment mechanisms can manipulate operating-system views and system-call results so that malicious processes do not appear in normal process listings and associated files or configuration artifacts, including Windows Registry entries, are not readily visible to users or security tools. Rootkits may operate in user mode, kernel mode, boot components, or firmware, with lower-level implementations generally providing deeper control over what the operating system reports. A rootkit can also incorporate surveillance functionality such as keystroke interception, allowing an attacker to capture credentials and other sensitive input while remaining difficult to detect. This combination of stealth, persistence, and system-level manipulation is the defining behavior described in the question. The U.S. National Institute of Standards and Technology defines rootkits as software designed to obtain and maintain privileged access while hiding its presence; see NIST's rootkit glossary entry. Additional technical context on detecting rootkits is available from MITRE ATT&CK: Rootkit.

QUESTION NO: 18

A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output:

HTTP/1.1 200 OK

Server: Microsoft-IIS/6

Expires: Tue, 17 Jan 2011 01:41:33 GMT

Date: Mon, 16 Jan 2011 01:41:33 GMT

Content-Type: text/html

Accept-Ranges: bytes

Last Modified: Wed, 28 Dec 2010 15:32:21 GMT

ETag:"b0aac0542e25c31:89d"

Content-Length: 7369

Which of the following is an example of what the engineer performed?

A. Banner grabbing

B. SQL injection

C. Whois database query

D. Cross-site scripting

ANSWER: A

Explanation:

Banner grabbing is the correct answer. Banner grabbing is an enumeration technique in which an assessor connects to a network service and examines the response information it exposes. In this case, connecting to TCP port 80 with netcat and receiving an HTTP response reveals a service banner: `Server: Microsoft-IIS/6`. This identifies the web-server software and its version, while the additional HTTP headers disclose useful operational details such as content type, modification time, entity tag, supported byte ranges, and response length.

This is valuable during authorized reconnaissance because product and version information helps the engineer build an accurate asset profile, identify applicable security advisories, and determine whether further validation is appropriate. HTTP response headers are a common source of service-identification data, particularly when a server has not been configured to minimize version disclosure. Microsoft documents that IIS can add server-related HTTP response headers and provides configuration guidance for managing them. Netcat is also commonly used to make manual TCP connections and inspect application-layer responses.

References: Microsoft IIS Request Filtering documentation; Ncat documentation.

QUESTION NO: 19

In this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstalls the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values.

What is this attack called?

A. Evil twin

B. Chop chop attack

C. Wardriving

D. KRACK

ANSWER: D

Explanation:

KRACK is correct. KRACK, short for Key Reinstallation Attack, is a family of attacks against the WPA2 protocol's cryptographic handshakes. It exploits the fact that, during the WPA2 four-way handshake, a retransmitted handshake message can be manipulated or replayed to cause a vulnerable client to reinstall a key that it has already installed. Reinstalling that key resets associated state, including nonce and packet-number values used to prevent replay and to ensure that encryption keystreams are not reused. This can permit replay, decryption, or—in certain configurations—packet forgery, depending on the cipher suite and implementation involved. The attack is not a flaw in a user's Wi-Fi password; it targets implementation behavior in WPA2 clients and access points. Mitigation requires applying vendor patches to affected wireless clients, access points, and embedded devices, because properly patched implementations prevent reinstallation of an already-in-use key. The original KRACK disclosure describes the key reinstallation condition and its effect on transmit and receive packet counters in detail. See the KRACK Attacks disclosure site and CERT/CC's WPA2 key reinstallation vulnerability advisory.

QUESTION NO: 20

Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds

B. USER2SID

C. Cheops

D. SID2USER

E. DumpSec

ANSWER: B D E

Explanation:

USER2SID, **SID2USER**, and **DumpSec** are enumeration tools because they collect or translate information that helps identify Windows accounts, groups, and security relationships. USER2SID is used to derive a Windows Security Identifier (SID) associated with an account name, while SID2USER performs the reverse lookup, resolving a known SID to its associated user or group name. These lookups are valuable during Windows and Active Directory enumeration because SIDs are the underlying identifiers Windows uses for security principals; understanding their mappings can reveal account naming and privilege-related information. Microsoft explains the role and structure of SIDs in its Security identifiers documentation and documents how Windows security principals are represented in the Security principals reference. DumpSec is designed to enumerate and report Windows security information, including users, groups, permissions, policies, and related account details. In an authorized assessment, these tools support the enumeration phase by transforming accessible system or directory information into an organized view of identities and security configuration that can be reviewed for exposure and privilege relationships.

QUESTION NO: 21

Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

A. BA810DBA98995F1817306D272A9441BB

B. 44EFCE164AB921C0AAD3B435B51404EE

C. 0182BD0BD4444BF836077A718CCDF409

D. CEC52EB9C8E3455DC2265B23734E0DAC

E. B757BF5C0D87772FAAD3B435B51404EE

F. E52CAC67419A9A224A3B108F3FA6CB6D

ANSWER: B E

Explanation:

LM hashing processes passwords as two independent seven-character portions after converting the password to uppercase and padding it to 14 characters. When a password contains fewer than eight characters, the second seven-character portion contains only padding. Its resulting, well-known LM hash value is `AAD3B435B51404EE`. Therefore, an LM hash whose final 16 hexadecimal characters equal that value identifies a password that has no characters in the second LM portion and is consequently fewer than eight characters long. Both `44EFCE164AB921C0AAD3B435B51404EE` and `B757BF5C0D87772FAAD3B435B51404EE` have this characteristic. The first value in each hash is the hash of the populated first portion, while the common trailing value represents the empty padded second portion. This behavior is a direct consequence of the legacy LM one-way-function design, which splits a password into two seven-character blocks rather than hashing the password as one complete value. Microsoft's NTLM protocol specification describes the LM one-way function and its password-padding behavior: MS-NLMP documentation. A practical description of the LM hash format and the empty-half marker is also available in Samba documentation.

QUESTION NO: 22

Which definition among those given below best describes a covert channel?

A. A server program using a port that is not well known.

B. Making use of a protocol in a way it is not intended to be used.

C. It is the multiplexing taking place on a communication link.

D. It is one of the weak channels used by WEP which makes it insecure

ANSWER: B

Explanation:

Making use of a protocol in a way it is not intended to be used is the best description of a covert channel. A covert channel is an unauthorized or unintended communications path that enables information transfer in a manner outside the system's designed security policy or normal communication semantics. Rather than using an explicitly permitted data field or application function for its intended purpose, a sender can encode information into incidental protocol characteristics, such as packet timing, ordering, padding, header values, or deliberately selected field values. A receiver who knows the encoding method can observe those characteristics and reconstruct the hidden message.

This behavior is especially important in ethical hacking and security assessments because it can bypass monitoring and data-loss controls that focus only on expected application content. The key characteristic is not merely that a network protocol is present, but that a feature, resource, or observable property is repurposed to carry information contrary to its intended design. NIST defines a covert channel as a communications channel not intended for information transfer at all, while RFC 4949 similarly describes it as an unintended or unauthorized communications path. See the NIST Computer Security Resource Center definition of covert channel and the Internet Security Glossary, Version 2 (RFC 4949).

QUESTION NO: 23

A friend of yours tells you that he downloaded and executed a file that was sent to him by a coworker. Since the file did nothing when executed, he asks you for help because he suspects that he may have installed a trojan on his computer.

What tests would you perform to determine whether his computer is infected?

A. Upload the file to VirusTotal.

B. You do not check; rather, you immediately restore a previous snapshot of the operating system.

C. Use ExifTool and check for malicious content.

D. Use netstat and check for outgoing connections to strange IP addresses or domains.

ANSWER: D

Explanation:

Use netstat and check for outgoing connections to strange IP addresses or domains. is the most appropriate test because a trojan that appears to do nothing may be running silently in the background and communicating with a command-and-control server. Examining active network connections can reveal unexpected remote endpoints, unusual listening ports, or persistent outbound sessions created by the malicious process. A responder should collect connection information, identify the owning process and its process identifier, then validate whether the destination and application are expected for that system. On Windows, `netstat -abno` can associate connections with executables and process IDs; this evidence can then be correlated with Task Manager, Process Explorer, endpoint telemetry, DNS logs, and firewall logs. This is a practical initial infection check because command-and-control communication is a common operational characteristic of remote-access trojans. Microsoft documents Netstat's ability to display active TCP connections, listening ports, executable involvement, and process IDs at Microsoft Learn: netstat. For incident handling context, NIST recommends identifying and analyzing indicators and relevant system/network evidence during incident response; see NIST SP 800-61 Rev. 2.

QUESTION NO: 24

Miley, a professional hacker, decided to attack a target organization's network. To perform the attack, she used a tool to send fake ARP messages over the target network to link her MAC address with the target system's IP address. By performing this, Miley received messages directed to the victim's MAC address and further used the tool to intercept steal, modify, and block sensitive communication to the target system.

What is the tool employed by Miley to perform the above attack?

A. Wireshark

B. BetterCAP

C. DerpNSpoof

D. Gobbler

ANSWER: B

Explanation:

BetterCAP is correct because it is a network reconnaissance and man-in-the-middle framework that supports ARP spoofing, also called ARP poisoning. In this attack, the attacker transmits forged ARP replies on a local network so that another host associates an IP address with the attacker-controlled MAC address. This can redirect traffic intended for a victim or gateway through the attacker's system, placing the attacker in a position to observe and potentially manipulate communications. BetterCAP includes an ARP-spoofing capability designed for this type of local-network MITM scenario, along with packet capture, traffic inspection, and extensible modules that can support interception and modification workflows. The described behavior—sending fake ARP messages to bind the attacker's MAC address to a target IP address, then receiving traffic intended for the victim—is the defining mechanism of ARP spoofing. BetterCAP's official documentation specifically identifies its ARP spoofing module and describes its use in man-in-the-middle attacks. For further technical details, see the BetterCAP ARP spoofing documentation and the ARP protocol specification (RFC 826).

QUESTION NO: 25

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

A. Data collection and vulnerability scanning

B. Interviewing employees and network engineers

C. Reviewing the firewalls configuration

D. Source code review

ANSWER: A

Explanation:

Data collection and vulnerability scanning is the appropriate preparation activity because it provides an evidence-based view of the organization's actual technical environment before the formal assessment begins. Collecting asset data—such as host identifiers, operating systems, installed software, network addresses, ownership, and configuration details—allows the analyst to reconcile discovered systems and services with the records in the secure asset database. That reconciliation identifies unmanaged, missing, duplicated, or incorrectly described assets that could otherwise be omitted from the assessment scope.

Vulnerability scanning then evaluates those discovered assets for missing patches, insecure services, weak configurations, and known vulnerabilities. The scan results can be compared with the organization's defined minimum security baseline to establish whether each system meets required hardening and patch-management expectations. This combination supports accurate scoping, prioritization, and repeatable assessment planning, while producing documented findings that can be validated during the formal engagement. NIST describes technical security testing, including vulnerability scanning, as a core

activity for identifying vulnerabilities and assessing security posture in SP 800-115. Asset identification and vulnerability assessment are also central practical areas in EC-Council's Certified Ethical Hacker program.

QUESTION NO: 26

Which of the following tools can be used to perform a zone transfer?

A. NSLookup

B. Finger

C. Dig

D. Sam Spade

E. Host

F. Netcat

G. Neotrace

ANSWER: A C D E

Explanation:

NSLookup, Dig, Sam Spade, and Host can perform DNS zone-transfer requests when the authoritative DNS server permits them. A zone transfer is a DNS replication mechanism in which a secondary server obtains an entire zone's records from the primary server, usually through an AXFR request over TCP port 53. From an assessment perspective, an allowed AXFR transfer can disclose valuable DNS intelligence, including hostnames, address records, mail-routing records, and internal naming conventions.

NSLookup supports zone-transfer functionality through its interactive `ls` command in implementations that retain this capability. Dig can explicitly request a full transfer with an `AXFR` query type. Host provides the `-l` option to list a zone by requesting a transfer. Sam Spade is a legacy network-investigation utility that includes DNS-query and zone-transfer capabilities. In each case, successful retrieval depends on the target DNS server's transfer-access controls; properly configured servers restrict transfers to authorized secondary name servers. DNS AXFR is specified by the DNS standards, and common command-line tool documentation describes the relevant query capabilities. See RFC 5936: DNS Zone Transfer Protocol and the dig manual page.

QUESTION NO: 27

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

ANSWER: A

Explanation:

`http-methods` is the appropriate Nmap Scripting Engine (NSE) script because it discovers the HTTP methods that a web server reports as supported. The script sends an HTTP `OPTIONS` request and evaluates the methods returned by the target,

typically in the `Allow` header. This provides an efficient way to enumerate methods such as `GET`, `POST`, `HEAD`, `PUT`, `DELETE`, and `TRACE` during web-server reconnaissance. Identifying enabled methods is important because the available HTTP verb set directly affects the server's exposed functionality and attack surface. In particular, methods that permit resource creation, modification, or removal should be validated against the application's intended configuration and authorization controls. The script can be run against a web service with a command such as `nmap -p 80,443 --script http-methods target.example`; use `-sV` where service/version detection is useful for identifying HTTP services on nonstandard ports. Nmap's official script documentation describes `http-methods` as performing HTTP method enumeration, and its NSE documentation explains how scripts are selected and executed. See Nmap: http-methods NSE script documentation and Nmap Reference Guide: NSE.

QUESTION NO: 28

Attacker Simon targeted the communication network of an organization and disabled the security controls of NetNTLMvl by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic. He then extracted all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks. What is the type of attack performed by Simon?

A. Internal monologue attack

B. Combinator attack

C. Rainbow table attack

D. Dictionary attack

ANSWER: A

Explanation:

Internal monologue attack is correct. This technique abuses Windows' local NTLM authentication behavior to obtain NTLM challenge-response material for accounts represented by token-bearing processes, without requiring the attacker to interact with a remote service or capture traffic over the network. The attacker first weakens relevant NTLM protections through registry policy values, then enumerates usable process tokens and causes local authentication attempts under those security contexts. The resulting NetNTLM material can be cracked offline to recover credentials, enabling the attacker to impersonate a legitimate account and pursue subsequent actions.

The details in the scenario closely match the defining workflow of Internal Monologue: modifying NTLM-related settings such as `LMCompatibilityLevel`, `NTLMMinClientSec`, and `RestrictSendingNTLMTraffic`, followed by extracting and using non-network logon tokens from active processes. Microsoft documents the NTLM security-policy controls and their impact on NTLM negotiation in its LAN Manager authentication level policy reference. The technique's implementation and its use of local tokens are also described by the original Internal-Monologue project.

QUESTION NO: 29

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.

ANSWER: B

Explanation:

Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials is correct because HTTP cookies commonly store session identifiers or authentication tokens. After a user signs in, a website can issue a session cookie that the browser returns with later requests, allowing the site to recognize the authenticated session without requiring the user to submit credentials again. If such a cookie remains on a shared, lost, compromised, or otherwise accessible computer after the browser closes, an attacker may copy and replay it to impersonate the user at the trusting website. This is generally known as session hijacking or session sidejacking, depending on how the token is obtained. Automatically deleting cookies when the browser terminates reduces the persistence window for these session artifacts, particularly for cookies without an appropriate expiration setting or in environments where multiple people could access the same endpoint. Cookie deletion is therefore a client-side control that helps limit reuse of retained authentication state. OWASP describes session identifiers as credentials that must be protected throughout their lifecycle and recommends secure session-management practices, including suitable expiration and invalidation behavior. For related browser cookie controls, see the OWASP Session Management Cheat Sheet and MDN's HTTP cookie documentation.

QUESTION NO: 30

Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection.

What is the APT lifecycle phase that Harry is currently executing?

A. Initial intrusion

B. Persistence

C. Cleanup

D. Preparation

ANSWER: A

Explanation:

Initial intrusion is correct because the described activity is the attacker's first successful entry into the target environment. In an APT operation, preparation occurs before engaging the target and includes planning, target research, and developing or obtaining the necessary infrastructure and tools. Here, that preparatory work has already occurred. The attacker is now using spear-phishing and exploitation of publicly exposed systems to gain an initial foothold.

Deploying malware that establishes an outbound connection is also consistent with obtaining that foothold: it gives the attacker a channel through which the compromised host can communicate with attacker-controlled infrastructure, enabling subsequent control and follow-on activity. Spear-phishing is a well-established initial-access technique, while exploiting an internet-facing application or server is another common means of entering an organization's network. MITRE ATT&CK documents these behaviors under Phishing and Exploit Public-Facing Application. The successful compromise and malware deployment therefore place the activity in the initial intrusion phase of the APT lifecycle.

QUESTION NO: 31

Which of the following statements is FALSE with respect to Intrusion Detection Systems?

A. Intrusion Detection Systems can be configured to distinguish specific content in network packets

B. Intrusion Detection Systems can easily distinguish a malicious payload in encrypted traffic

C. Intrusion Detection Systems require constant update of the signature library

D. Intrusion Detection Systems can examine the contents of the data n context of the network protocol

ANSWER: B

Explanation:

Intrusion Detection Systems can easily distinguish a malicious payload in encrypted traffic is the false statement. A network IDS generally inspects packet headers and payloads that are visible on the wire. Encryption protects the application payload from intermediate devices, so an IDS that does not have access to the decrypted session cannot directly inspect that payload for exploit signatures, malware content, commands, or other indicators of compromise. TLS interception or decryption at an appropriate trusted inspection point can make plaintext available to a security control, but this requires deliberate architecture, certificate and key-management considerations, and careful handling of privacy and operational risks. Even when payloads remain encrypted, IDS technologies can still provide useful detection based on metadata and behavior, such as source and destination addresses, ports, TLS handshake attributes, certificate information, traffic volume, timing, protocol anomalies, and correlations with other telemetry. Those methods do not mean the IDS can easily identify a malicious encrypted payload itself. This limitation is central to network monitoring because modern application traffic commonly uses TLS. For further guidance on the visibility and inspection implications of encrypted traffic, see CISA's SSL/TLS inspection guidance and the TLS recommendations in RFC 9325.

QUESTION NO: 32

While testing a web application in development, you notice that the web server does not properly ignore the "dot dot slash" (../) character string and instead returns the file listing of a folder structure of the server.

What kind of attack is possible in this scenario?

A. Cross-site scripting

B. Denial of service

C. SQL injection

D. Directory traversal

ANSWER: D

Explanation:

Directory traversal is possible because the `../` sequence is a relative-path notation that instructs a filesystem to move up one directory level. When a web server or application accepts user-controlled path input and fails to normalize and validate it before accessing a file, an attacker can repeatedly use this sequence to escape the intended web root or application directory. The resulting requests may expose directory listings and permit access to files outside the location that the application was meant to serve, subject to the permissions of the web-server process. This issue is also commonly called path traversal. Secure implementations prevent it by treating file names as untrusted input, canonicalizing paths, enforcing that the resolved path remains beneath an allowed base directory, and avoiding direct use of user input in filesystem paths. OWASP classifies this as Path Traversal and demonstrates how `../` can be used to reach sensitive filesystem locations when validation is absent. See the OWASP Path Traversal guidance and the CWE-22: Path Traversal entry for the underlying weakness and recommended mitigations.

QUESTION NO: 33

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network.

Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

A. SNMPUtil

B. SNScan

C. SNMPScan

D. Solarwinds IP Network Browser

E. NMap

ANSWER: A B D E

Explanation:

SNMPUtil, **SNScan**, **Solarwinds IP Network Browser**, and **NMap** can be used for SNMP-focused discovery and enumeration. SNMPUtil is a command-line utility designed to query SNMP-enabled devices and retrieve management information exposed through SNMP object identifiers. SNScan is purpose-built to locate SNMP services and query devices, making it suitable for identifying responsive hosts and available SNMP information. Solarwinds IP Network Browser provides network discovery capabilities and can use SNMP to identify and collect details about managed network devices. Nmap can enumerate SNMP when UDP SNMP ports are targeted and relevant Nmap Scripting Engine scripts are used. For example, the `snmp-info` script queries a target's SNMP service for system information, while additional SNMP scripts can gather interfaces, processes, software, and routing-related data where access permits. Nmap's official NSE documentation describes the SNMP information script and its usage at Nmap: snmp-info NSE script. Nmap's broader SNMP script collection is documented at Nmap NSE SNMP category. In an authorized assessment, the available results depend on reachable UDP services, the SNMP version in use, valid community strings or credentials, and the access controls configured on the target device.

QUESTION NO: 34

Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about DNS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names, IP addresses, DNS records, and network Whois records. He further exploited this information to launch other sophisticated attacks.

What is the tool employed by Gerard in the above scenario?

A. Towelroot

B. Knative

C. zANTI

D. Bluto

ANSWER: D

Explanation:

Bluto is the correct tool because it is an automated DNS-footprinting and reconnaissance utility designed to collect DNS-related information about a target. Its enumeration capabilities align directly with the scenario: it can obtain domain and host names, associated IP addresses, DNS record information, zone-related data, and network registration/WHOIS details. This type of collection helps an assessor or attacker build a picture of an organization's externally visible infrastructure, identify naming conventions and potential hosts, and map systems that may be relevant to later testing phases. DNS is particularly useful during reconnaissance because DNS resource records associate names with services and network addresses; the IETF's DNS specifications describe DNS as the distributed database used to map domain names and other resource data. WHOIS/RDAP-style registration data can additionally provide registration and contact information useful for understanding an Internet resource's public ownership context. Therefore, the described combination of DNS zone-data retrieval, host discovery, record enumeration, and network WHOIS lookup identifies Bluto. See the IETF DNS Concepts and Facilities specification and the ICANN WHOIS and RDAP overview.

QUESTION NO: 35

A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted. Which cryptography attack is the student attempting?

A. Man-in-the-middle attack

B. Brute-force attack

C. Dictionary attack

D. Session hijacking

ANSWER: C

Explanation:

The correct answer is **Dictionary attack**. A dictionary attack attempts authentication guesses using a prepared collection of likely passwords, such as common passwords, words, names, leaked credentials, or password variants. Here, the script iterates through a list of commonly used passwords and tests each candidate against the password-protected PDF. That use of a predefined, targeted wordlist is the defining characteristic of a dictionary attack. The attack may succeed quickly when a document owner has selected a predictable password, because such passwords are more likely to appear in commonly used-password lists. Password-recovery and auditing tools can apply this approach to protected files, including PDFs, by trying candidate entries from a wordlist until one successfully opens the document or the list is exhausted. Secure password practices reduce this risk: passwords should be long, unique, and randomly generated rather than chosen from recognizable words or frequently used patterns. NIST recommends screening new passwords against lists of commonly used, expected, or compromised values, which directly addresses the kind of password selection weakness exploited by dictionary guessing. See NIST SP 800-63B: Digital Identity Guidelines and OWASP password attack guidance.

QUESTION NO: 36

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

ANSWER: B

Explanation:

To defend against webserver attacks is correct because ISAPI filters are native extensions that run inside the IIS web-server process and can inspect, modify, or otherwise participate in processing HTTP requests and responses. Each enabled filter therefore increases the server's attack surface and may introduce vulnerabilities through flawed code, unsafe parsing, insecure configuration, or outdated components. A filter that is not required for the server's intended function provides no compensating operational value, yet it remains code that can potentially be reached by remote requests or abused after a compromise.

Removing or disabling unnecessary filters follows the principle of least functionality: expose only the services and extensions needed to deliver the application. This reduces opportunities for exploitation, simplifies patching and monitoring, and limits the number of modules that execute within a sensitive web-server environment. Microsoft's IIS guidance describes ISAPI filters as components that can alter request and response processing, which illustrates why their use should be deliberate and tightly controlled. Security hardening guidance similarly recommends removing unnecessary roles, features, and components to reduce attack surface. See Microsoft's ISAPI Filters Overview and Microsoft guidance for securing IIS.

QUESTION NO: 37

You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

```
invictus@victim_server.~$ nmap -T4 -O 10.10.0.0/24 TCP/IP
fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!
```

What seems to be wrong?

A. The nmap syntax is wrong.

B. This is a common behavior for a corrupted nmap application.

C. The outgoing TCP/IP fingerprinting is blocked by the host firewall.

D. OS Scan requires root privileges.

ANSWER: D

Explanation:

OS Scan requires root privileges. Nmap operating-system detection, typically invoked with `-O`, relies on TCP/IP stack fingerprinting. To build an OS fingerprint, Nmap sends specially crafted probes and analyzes subtle characteristics of responses, such as TCP flags, sequence behavior, window sizes, and ICMP response details. On Unix-like systems, performing this type of raw-packet operation requires elevated privileges, normally root access (or the relevant raw-socket capabilities). A shell on a compromised system does not necessarily provide those privileges; it may be running under a restricted user account. Therefore, attempting an OS scan without elevation produces the expected privilege-related failure rather than completing host fingerprinting. The appropriate action in an authorized assessment is to obtain approved elevated access or run the scan from an authorized system/account that has the necessary packet-capture and raw-packet permissions. Nmap documents that OS detection requires privileges because it uses raw sockets, and its reference guide identifies `-O` as the OS-detection feature. See the Nmap OS Detection documentation and the Nmap Reference Guide.

QUESTION NO: 38

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

A. Use the same machines for DNS and other applications

B. Harden DNS servers

C. Use split-horizon operation for DNS servers

D. Restrict Zone transfers

E. Have subnet diversity between DNS servers

ANSWER: B C D E

Explanation:

Harden DNS servers, **Use split-horizon operation for DNS servers**, **Restrict Zone transfers**, and **Have subnet diversity between DNS servers** are sound DNS-security recommendations. DNS server hardening reduces the exposed attack surface by applying timely patches, disabling unnecessary services, using secure administrative access, limiting recursion to authorized clients, and maintaining secure configuration and logging. Split-horizon DNS separates answers intended for internal users from records exposed externally, helping prevent unnecessary disclosure of internal hostnames, addressing structure, and services. Restricting zone transfers to explicitly authorized secondary servers is essential because zone data can reveal an organization's systems and provide valuable reconnaissance information. Authorization is typically enforced with source restrictions and transaction signatures where supported. Subnet diversity improves DNS availability and resilience: authoritative or recursive DNS servers should not share a single network dependency that could be disrupted by a routing failure, denial-of-service event, or localized compromise. Deploying redundant servers across independent network segments, and preferably separate locations or providers, supports continued name resolution during incidents. These controls align with CISA guidance on securing DNS infrastructure and NIST recommendations for secure DNS

deployment and operation. See CISA DNS Amplification Attacks guidance and NIST SP 800-81-2, Secure Domain Name System Deployment Guide.

QUESTION NO: 39

What is the least important information when you analyze a public IP address in a security alert?

A. DNS

B. Whois

C. Geolocation

D. ARP

ANSWER: D

Explanation:

ARP is the least important information for analysis of a public IP address in a security alert because ARP is a Layer 2, local-network protocol. Its role is to resolve an IPv4 address to a MAC address on the same broadcast domain; ARP requests are not routed across the Internet. Consequently, an analyst investigating an externally observed public address ordinarily cannot use ARP to establish useful attribution, reputation, ownership, geographic context, or remote-host identity for that address. ARP data can be highly valuable during an internal investigation when the analyst has access to the relevant LAN, switch infrastructure, DHCP records, or endpoint telemetry. In that local context, a historical IP-to-MAC mapping can help identify the device that used an address. However, that information is inherently scoped to the local segment and is not meaningful public-IP enrichment. The protocol's original specification describes ARP as translating protocol addresses into local network hardware addresses, and operational guidance likewise treats ARP as a local-link mechanism. See RFC 826: An Ethernet Address Resolution Protocol and Cisco's ARP overview.

QUESTION NO: 40

The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

You are hired to conduct security testing on their network.

You successfully brute-force the SNMP community string using a SNMP crack tool.

The access-list configured at the router prevents you from establishing a successful connection.

You want to retrieve the Cisco configuration from the router. How would you proceed?

A. Use the Cisco's TFTP default password to connect and download the configuration file

B. Run a network sniffer and capture the returned traffic with the configuration file from the router

C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address

D. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0

ANSWER: B D

Explanation:

"Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0" and "Run a network sniffer and capture the returned traffic with the configuration file from the router" work together when the router's SNMP access control list trusts addresses from that internal range. A source address that matches the permitted management network can cause the router to accept an otherwise blocked SNMP request. In a controlled assessment, the tester can use SNMP write access to invoke Cisco configuration-copy functionality, directing the router to transfer its running or startup configuration through a supported copy mechanism. Because a spoofed source address generally prevents replies from being delivered directly to the tester, packet capture is needed at a location where the resulting traffic can be observed.

Capturing the configuration transfer or associated response provides the configuration contents while avoiding dependence on receiving a normal routed reply at the tester's actual address. This scenario illustrates why IP-based SNMP ACLs are not sufficient protection by themselves: SNMP should be restricted to dedicated management paths and protected with SNMPv3 authentication and privacy. The SNMP protocol's message and request model is specified in RFC 1157, and Cisco documents SNMP configuration and security guidance in its IOS XE SNMP Configuration Guide.

QUESTION NO: 41

Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script. After infecting the victim's device, Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self-extracting RAR file, to retrieve information related to network resources such as writable share drives.

What is the tool employed by Mason in the above scenario?

A. NetPass.exe

B. Outlook scraper

C. WebBrowserPassView

D. Credential enumerator

ANSWER: D

Explanation:

Credential enumerator is the correct tool. Emotet campaigns have used a credential-enumeration component distributed as a self-extracting RAR archive. Once executed, this component collects credentials and discovers network resources that can support onward propagation, including accessible and writable network shares. Identifying writable shares is especially valuable to an attacker because they can be used to copy malicious files to systems or locations reachable by other users, increasing the malware's opportunity to spread through an organization.

This behavior aligns with the network-share discovery activity documented in the MITRE ATT&CK knowledge base. Attackers enumerate network shares to identify accessible resources and determine where they may be able to place payloads or obtain further information. In the scenario, the defining details are the Emotet context, the self-extracting RAR packaging, and discovery of writable share drives; together, these identify the Credential enumerator utility rather than a standalone password-recovery or email-harvesting utility. See MITRE ATT&CK's description of Network Share Discovery and CISA's advisory on Emotet Malware.

QUESTION NO: 42

A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.

A. Use port security on his switches.

B. Use a tool like ARPwatch to monitor for strange ARP activity.

C. Use a firewall between all LAN segments.

D. If you have a small network, use static ARP entries.

E. Use only static IP addresses on all PC's.

ANSWER: A B D

Explanation:

ARP poisoning works by sending forged ARP replies that associate an attacker-controlled MAC address with a legitimate IP address, often the default gateway. **Use port security on his switches.** is a valuable Layer 2 control because switch ports

can be limited to an expected number of MAC addresses and, where appropriate, configured with secure or statically assigned MAC addresses. This reduces the opportunity for an unauthorized host to attach or to present unexpected MAC identities on an access port. **Use a tool like ARPwatch to monitor for strange ARP activity.** provides an important detection control: it observes IP-to-MAC bindings and can alert administrators when a host's Ethernet address changes unexpectedly. Rapid alerts allow the administrator to investigate, isolate the relevant switch port, and restore correct mappings before a spoofing event causes significant interception or disruption. **If you have a small network, use static ARP entries.** directly prevents a host from dynamically accepting a forged mapping for the configured peer, such as the default gateway, because the critical IP-to-MAC association is manually fixed. Static entries are operationally practical only in limited, stable environments, but they are effective for protecting key ARP relationships. Together, access-port controls, ARP-change monitoring, and static mappings where manageable provide complementary prevention and response coverage. See Cisco's port-security documentation and the ARPwatch project documentation.

QUESTION NO: 43

While testing a web application in development, you notice that the web server does not properly ignore the "dot dot slash" (../) character string and instead returns the file listing of a folder higher up in the folder structure of the server.

What kind of attack is possible in this scenario?

A. Cross-site scripting

B. SQL injection

C. Denial of service

D. Directory traversal

ANSWER: D

Explanation:

Directory traversal is possible because the `../` sequence is a relative-path token that directs a filesystem path resolver to move from the current directory to its parent directory. If the application accepts user-controlled path input and fails to normalize, validate, and constrain that path to an approved base directory, an attacker can use repeated traversal sequences to reach folders outside the intended web-accessible location. The reported ability to obtain a listing of a higher-level folder is direct evidence that the server is resolving the supplied traversal token rather than safely rejecting it. Depending on the account permissions of the web server process and the endpoint's behavior, this weakness can expose application source files, configuration files, logs, credentials, or other sensitive filesystem content. Secure implementations canonicalize the requested path, enforce that its resolved location remains beneath a designated directory, and avoid exposing directory listings. OWASP identifies this issue as path traversal and notes that attackers can manipulate file-path variables with sequences such as `../` to access files and directories stored outside the intended web root. See the OWASP Path Traversal overview and the MITRE CWE-22 definition.

QUESTION NO: 44

Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a Dos attack, and as a result, legitimate employees were unable to access the clients network. Which of the following attacks did Abel perform in the above scenario?

A. VLAN hopping

B. DHCP starvation

C. Rogue DHCP server attack

D. STP attack

ANSWER: B

Explanation:

DHCP starvation is correct because the described activity deliberately exhausts the DHCP server's available address pool. In this attack, the tester sends a large volume of DHCP requests, commonly using spoofed or randomized MAC addresses so that each request appears to originate from a different client. The DHCP server allocates leases to those apparent clients until its configured scope has no addresses remaining. Consequently, legitimate systems cannot obtain an IP configuration, such as an IP address, default gateway, and DNS server, and are denied network access.

This is a denial-of-service condition at the network-addressing layer. The defining feature is consumption of all available leases, rather than merely impersonating a DHCP server or modifying network-switching behavior. DHCP starvation can also be used as a preliminary step for interception attacks: after legitimate DHCP service is exhausted, an attacker may attempt to provide fraudulent network configuration to clients. However, the scenario specifically identifies the lease-exhaustion action and resulting inability of users to connect, which is DHCP starvation.

Network administrators can reduce this risk with switch-port controls such as DHCP snooping, port security, rate limiting, and appropriately sized, monitored DHCP scopes. See Cisco DHCP Snooping documentation and RFC 2131: Dynamic Host Configuration Protocol.