DUMPSBOSS.

Certified Ethical Hacker Exam

ECCouncil 312-50

Version Demo

Total Demo Questions: 58

Total Premium Questions: 667

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to Ethical Hacking	115
Topic 2, Footprinting and Reconnaissance	49
Topic 3, Scanning Networks	86
Topic 4, Enumeration	19
Topic 5, System Hacking	72
Topic 6, Malware Threats	19
Topic 7, Sniffing	32
Topic 8, Social Engineering	19
Topic 9, Denial of Service	8
Topic 10, Session Hijacking	9
Topic 11, Evading IDS, Firewalls, and Honeypots	58
Topic 12, Hacking Web Servers	10
Topic 13, Hacking Web Applications	41
Topic 14, SQL Injection	10
Topic 15, Hacking Wireless Networks	25
Topic 16, Hacking Mobile Platforms	1
Topic 17, Cryptography	83
Topic 18, Mix Questions	11
Total	667

QUESTION NO: 1

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

A. tcpdump

B. nmap

C. ping

D. tracert

ANSWER: A

Explanation:

tcpdump can be used for passive OS fingerprinting because it captures and displays packets that are already traversing a network interface, without sending discovery probes to the target. An analyst can inspect TCP/IP header characteristics exposed in captured traffic, such as the initial TTL value, TCP window size, TCP options and their ordering, the Don't Fragment flag, and related protocol behaviors. These values can be compared with known operating-system TCP/IP stack signatures to infer the likely operating system of the communicating host. This approach is passive because the assessment relies on observing normal traffic rather than generating traffic that could be logged by, or alert, the target. tcpdump's packet-capture filters also let an analyst focus on relevant traffic, such as initial TCP SYN packets, which are especially useful when collecting fingerprint attributes. The tcpdump manual documents its role as a utility for capturing and decoding network traffic: tcpdump manual. For background on passive fingerprinting based on observed TCP/IP stack behavior, see the p0f passive fingerprinting project.

QUESTION NO: 2

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

Explanation:

SNMPUtil, SNScan, and Solarwinds IP Network Browser are appropriate tools for performing SNMP-focused discovery and enumeration. SNMP enumeration involves querying SNMP-enabled hosts—typically using known or discovered community strings—to retrieve management information from Management Information Base objects. Useful results can include interface details, IP addressing, routing information, device descriptions, running services, system contact data, and other configuration information exposed through SNMP.

SNMPUtil is designed to send SNMP requests and retrieve object values, making it suitable for targeted queries against specific object identifiers. SNScan is intended to locate and query SNMP services across network ranges, supporting the discovery-oriented aspect of enumeration. Solarwinds IP Network Browser provides SNMP-based network discovery and browsing capabilities, allowing an administrator to identify devices and inspect management information exposed by those devices. These tools directly support the task of collecting SNMP data from reachable managed devices, which is the objective described in the question. For background on SNMP's role in monitoring and management, see RFC 3411; SolarWinds also describes SNMP-oriented network-management tooling at SolarWinds SNMP Tools.

QUESTION NO: 3

Which of the following are appropriate actions when preserving digital evidence from a running system? (Choose two.)

A. Document the system state and collection actions

B. Calculate cryptographic hashes of collected evidence

C. Modify file timestamps to simplify sorting

D. Delete temporary files before acquisition

E. Use the original evidence as the working copy

ANSWER: A B

Explanation:

Document the system state and collection actions and **Calculate cryptographic hashes of collected evidence** are correct. Detailed documentation records the time, personnel, tools, commands, system condition, and evidence-handling actions. This supports chain of custody and helps demonstrate that the evidence was collected in a controlled and repeatable manner.

Cryptographic hashes provide a means to verify evidence integrity. The hash should be calculated when evidence is acquired and verified again whenever the evidence is transferred or examined. Investigators should minimize unnecessary changes to the system and use validated collection procedures. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.

QUESTION NO: 4

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:

A DNS zone transfer retrieves DNS records for an entire zone from an authoritative DNS server, normally through the AXFR query type over TCP port 53. **NSLookup** can request a zone listing/transfer when connected to a DNS server that permits it; its interactive commands have historically included `ls` for this purpose. **Dig** explicitly supports AXFR requests, for example `dig @server example.com AXFR`, making it a standard choice for authorized DNS enumeration. **Sam Spade**, a legacy network-investigation utility commonly associated with CEH-era tooling, includes DNS-query capabilities and can request zone transfers. **Host** also supports zone transfers through its zone-listing functionality, such as `host -l example.com server`. Whether any of these requests succeeds depends on the authoritative server configuration: properly administered DNS servers restrict transfers to explicitly authorized secondary servers. The DNS utility documentation for dig describes query types and transfer behavior, while the host manual documents its zone-listing capability. In an authorized security assessment, these tools are used to determine whether a DNS server improperly exposes complete zone data.

QUESTION NO: 5

A circuit level gateway works at which of the following layers of the OSI Model?

A. Layer 5 – Session

B. Layer 4 – TCP

C. Layer 3 – Internet protocol

D. Layer 2 – Data link

ANSWER: A

Explanation:

Layer 5 – Session is correct. A circuit-level gateway is a proxy-based firewall mechanism that operates by establishing and monitoring communication sessions rather than inspecting the application payload in detail. It validates the legitimacy of a connection, commonly by evaluating session-establishment activity such as the TCP handshake, then creates a controlled virtual circuit between endpoints. This makes it associated with the OSI Session layer, whose role includes establishing, managing, and terminating dialogs or sessions between communicating systems.

In practical firewall terminology, descriptions can sometimes emphasize that circuit-level gateways monitor TCP connections, because TCP is involved in creating many of the sessions they control. That operational association does not change the conventional OSI-layer classification used for circuit-level gateways in security training: they are categorized at Layer 5, the Session layer. This contrasts with a gateway that understands and filters the commands or content of a particular application protocol, which would require application-layer awareness. Fortinet's overview describes circuit-level gateways as operating at the session layer, and Cloudflare's OSI model reference identifies Layer 5 as the Session layer. See Fortinet: Circuit-Level Gateway and Cloudflare: OSI Model.

QUESTION NO: 6

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

A. tcpdump

B. nessus

C. etherea

D. Jack the ripper

ANSWER: A

Explanation:

tcpdump is the correct command-line packet analyzer. It captures and displays network packets observed on a selected network interface, allowing an analyst to inspect traffic such as Ethernet frames, IP packets, TCP sessions, UDP datagrams, ICMP messages, and application-protocol exchanges. Like Wireshark, tcpdump relies on packet-capture facilities provided by libpcap on Unix-like systems and supports capture filters to focus collection on relevant hosts, networks, protocols, or ports. For example, an ethical hacker or network defender can use a filter such as `tcp port 443` to observe HTTPS-related TCP traffic or save captured packets to a file for subsequent analysis in Wireshark. Its terminal-based design makes it particularly useful on remote servers, minimal installations, incident-response systems, and environments without a graphical desktop. The tcpdump manual describes it as a tool that "prints out a description of the contents of packets on a network interface," while Wireshark documentation confirms that capture files and filtering concepts can be used across packet-analysis workflows. See the tcpdump manual page and Wireshark documentation.

QUESTION NO: 7

The "white box testing" methodology enforces what kind of restriction?

A. The internal operation of a system is completely known to the tester.

B. Only the external operation of a system is 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 only partly accessible to the tester.

ANSWER: A

Explanation:

White-box testing assumes that the tester has complete visibility into the system's internal implementation. Accordingly, "The internal operation of a system is completely known to the tester." is correct. This testing approach uses knowledge of source code, program logic, control flow, data flow, interfaces, configurations, and architecture to design and execute tests. The tester can inspect implementation details and construct test cases that exercise specific statements, branches, paths, conditions, error-handling routines, and security-relevant code paths.

In an ethical hacking or application-security context, this level of knowledge enables a more targeted and systematic assessment than one based solely on observable behavior. It supports identifying flaws that may not be readily discoverable from the outside, such as insecure input handling in a particular function, authorization checks omitted on a code path, or logic errors in internal workflows. The restriction inherent in the methodology is therefore not a limitation on access to internals; rather, its defining condition is that internal system knowledge is available to the tester. The ISTQB glossary defines white-box testing as testing based on analysis of internal structure, while OWASP describes code review and testing activities that rely on access to application implementation details. See the ISTQB white-box testing glossary entry and the OWASP Web Security Testing Guide.

QUESTION NO: 8

A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

A. Spoofing an IP address

B. Tunneling scan over SSH

C. Tunneling over high port numbers

D. Scanning using fragmented IP packets

ANSWER: B

Explanation:

Tunneling scan over SSH is the most efficient technique because an SSH tunnel provides an encrypted, authenticated channel to a system that already has access to the internal network. In an authorized penetration test, the tester can use that internal foothold or approved jump host as the scanning vantage point. The border device observes the permitted SSH session rather than the individual reconnaissance packets directed at internal systems, while the internal network receives traffic from a host within its trusted address space. This is both practical and reliable because SSH is designed to securely forward TCP connections through encrypted channels, making it a standard mechanism for controlled remote administration and for reaching otherwise inaccessible private-network services. The test scope and rules of engagement must explicitly authorize the tunnel, the internal source system, and the target subnet; defenders should also retain SSH session and endpoint telemetry so such activity is accountable. OpenSSH documents port forwarding and tunneling capabilities in its ssh manual. NIST's guidance on secure remote access also emphasizes using protected, managed remote-access mechanisms and appropriate monitoring controls; see NIST SP 800-46 Rev. 2.

QUESTION NO: 9

SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible? (Choose two.)

A. It used TCP as the underlying protocol.

B. It uses community string that is transmitted in clear text.

C. It is susceptible to sniffing.

D. It is used by all network devices on the market.

ANSWER: B C

Explanation:

“It uses community string that is transmitted in clear text.” and “It is susceptible to sniffing.” are correct because legacy SNMP deployments, particularly SNMPv1 and SNMPv2c, use a community string as a shared credential and do not provide cryptographic protection for that value or for the management data carried in the message. A party able to observe management traffic can therefore capture the community string and read useful device-management information, such as system details, interface data, routing-related values, and configuration-related objects exposed through the device’s Management Information Base.

This exposure is especially relevant because SNMP commonly uses UDP and management polling may traverse shared, switched, wireless, or otherwise observable network paths. Captured read communities can enable further unauthenticated enumeration where access controls permit it; captured write communities can be substantially more dangerous. RFC 1157 specifies the community-based SNMPv1 model, while RFC 3414 describes the User-based Security Model used by SNMPv3 to add authentication and privacy protections. In practice, defenders should migrate to SNMPv3 where feasible, restrict SNMP access with network controls, use strong credentials, and disable unnecessary SNMP services. See RFC 1157 and RFC 3414.

QUESTION NO: 10

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 Windows-oriented enumeration tools. USER2SID is used to resolve a known Windows user or account name to its Security Identifier (SID). SID2USER performs the reverse function, resolving a SID to an associated account name. These mappings are useful during enumeration because Windows access-control information, group memberships, and account relationships are commonly represented with SIDs rather than only friendly account names. Microsoft explains that a SID is a unique value used to identify a security principal such as a user or group, making SID resolution an important reconnaissance activity in Windows environments.

DumpSec is designed to collect and report security-relevant information from Windows systems, including users, groups, group memberships, share permissions, policies, and related account data. This type of collection directly supports enumeration: it transforms accessible system and domain information into actionable details about identities, privileges, and exposed resources. In an authorized assessment, these tools help establish the account and authorization landscape before attempting deeper validation. See Microsoft’s overview of security identifiers and SystemTools’ DumpSec product information.

QUESTION NO: 11

If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

A. Civil

B. International

C. Criminal

D. Common

ANSWER: A

Explanation:

Civil law applies when executives are held liable for failing to exercise appropriate care in protecting company assets and information systems. This type of liability generally arises from a duty of care owed to the organization, its shareholders, customers, or other affected parties. If decision-makers neglect reasonable security governance, risk management, oversight, or safeguards and that failure causes measurable harm, a civil action may seek remedies such as compensatory damages, recovery of losses, or equitable relief.

In information-security governance, executives and directors are expected to make informed, good-faith decisions and to provide reasonable oversight of material organizational risks, including cyber risk. A finding that they did not properly protect systems or information concerns accountability for harm and financial loss, which is characteristic of civil liability. The U.S. Securities and Exchange Commission describes directors' and officers' duties in the context of corporate governance and accountability, while the NIST Cybersecurity Framework emphasizes governance and organizational responsibility for managing cybersecurity risk. See the SEC corporate governance overview and the NIST Cybersecurity Framework.

QUESTION NO: 12

Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?

A. Preparation phase

B. Containment phase

C. Recovery phase

D. Identification phase

ANSWER: A

Explanation:

The **Preparation phase** is correct because effective incident handling begins before an incident is detected. During preparation, an organization establishes its incident-response policies, procedures, roles, responsibilities, communication and escalation paths, and the personnel needed to operate the response capability. It also prepares technical and operational resources, such as secure backups, forensic tools, logging, asset information, contact lists, and alternate business processes. Developing contingency or backup plans and exercising them through tabletop exercises, simulations, and technical tests helps ensure that the response team and the wider workforce can act quickly and consistently under pressure. These activities reduce uncertainty, preserve critical business operations, and make later response activities more effective. NIST describes preparation as establishing and maintaining an incident-response capability, including plans, policies, procedures, training, tools, and exercises. The incident-handling lifecycle presented in CEH-aligned material likewise places policy definition, team coordination, backup planning, and plan testing in preparation. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and CISA Incident Response resources.

QUESTION NO: 13

Windows LAN Manager (LM) hashes are known to be weak. Which of the following are known weaknesses of LM? (Choose three.)

A. Converts passwords to uppercase.

B. Hashes are sent in clear text over the network.

C. Makes use of only 32-bit encryption.

D. Effective length is 7 characters.

E. Does not use a salt, so identical passwords produce identical hashes.

ANSWER: A D E

Explanation:

LM hashing weakens password security by converting the password to uppercase before processing. This removes case sensitivity and substantially reduces the possible password search space. LM also processes a password as two independent 7-character blocks (after padding to its 14-character maximum). Consequently, a password longer than seven characters is not protected as one combined secret; each half can be attacked independently, which makes cracking much more practical. In addition, LM hashes do not use a salt. The same password therefore produces the same LM hash across systems, enabling precomputed lookup tables and allowing attackers to recognize password reuse. These design properties are why modern Windows environments should avoid storing LM hashes and should use stronger password-verification mechanisms such as NTLMv2 or Kerberos. Microsoft documents the legacy LM hash behavior and recommends preventing LM hash storage through the applicable security policy; see Microsoft's guidance on preventing LM hash storage. The independent seven-character treatment and uppercase conversion are also described in SANS's discussion of Windows password hashes.

QUESTION NO: 14

A possibly malicious sequence of packets that were sent to a web server has been captured by an Intrusion Detection System (IDS) and was saved to a PCAP file. As a network administrator, you need to determine whether this packets are indeed malicious. What tool are you going to use?

A. Intrusion Prevention System (IPS)

B. Vulnerability scanner

C. Protocol analyzer

D. Network sniffer

ANSWER: C

Explanation:

A protocol analyzer is the appropriate tool because the packet capture has already been collected in PCAP format and must now be examined at the packet and protocol levels. A protocol analyzer such as Wireshark can open a PCAP file, decode its constituent protocols, reconstruct conversations, inspect packet fields and payloads, follow TCP or HTTP streams, and apply display filters to isolate suspicious traffic. These capabilities let an administrator validate IDS findings by looking for concrete indicators of malicious activity, such as unusual request methods or parameters, exploit strings, malformed protocol fields, command-and-control patterns, suspicious redirects, or unexpected data transfers. Wireshark's documentation describes its core purpose as capturing and interactively browsing network traffic, including reading saved capture files and dissecting many protocols. Its filtering and stream-following functions are particularly useful when determining the context and impact of a sequence of packets directed at a web server. This is forensic analysis of recorded network traffic, rather than prevention or a new assessment of hosts. See the Wireshark User's Guide introduction and the Wireshark display-filter documentation.

QUESTION NO: 15

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” is correct because a standard SNMP access list commonly permits requests based on the packet’s source address. In an authorized assessment scenario, using an address within the permitted range demonstrates whether the device trusts unauthenticated source addressing in addition to the community string. A valid read-write SNMP community can be used with Cisco’s configuration-copy management objects to instruct the device to copy its running or startup configuration using TFTP. Cisco documents SNMP support and its use for managing device operations at Cisco IOS SNMP Support.

“Run a network sniffer and capture the returned traffic with the configuration file from the router” is also correct because traditional TFTP transfers carry configuration data in cleartext. Once the router has been instructed to perform a configuration copy, a tester positioned where the relevant traffic is visible can capture and reconstruct the TFTP data packets containing the configuration. TFTP’s simple UDP-based transfer behavior is defined in RFC 1350. Together, the spoofed SNMP SET request bypasses a source-address-based ACL check, while packet capture obtains the configuration sent during the resulting copy operation.

QUESTION NO: 16

Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2f%2e%2e%2f = ../ ../ ../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

A. Configure the Web Server to deny requests involving "hex encoded" characters

B. Create rules in IDS to alert on strange Unicode requests

C. Use SSL authentication on Web Servers

D. Enable Active Scripts Detection at the firewall and routers

ANSWER: B

Explanation:

Create rules in IDS to alert on strange Unicode requests is the appropriate protection for an obstructed-URL attack because these attacks rely on alternative encodings to disguise dangerous path characters and evade simple, literal request matching. Unicode and other noncanonical encodings can cause different components in the request path—such as a proxy, web server, or application—to interpret the same URL differently. This may permit an attacker to conceal traversal sequences or attempts to access sensitive server-side resources.

An IDS rule set should inspect HTTP requests for suspicious Unicode representations, encoded directory-separator characters, multiple decoding layers, and traversal patterns after normalization. Alerting on these indicators enables defenders to identify reconnaissance and exploitation attempts, investigate the originating client, and correlate activity with web-server logs. Effective detection depends on canonicalizing request paths before applying signatures and maintaining current signatures for web-server attacks. OWASP describes path traversal as an attack in which manipulated file-path input can access files outside the intended web root: OWASP Path Traversal. Guidance on detecting encoded HTTP evasion techniques is also available in the Snort HTTP inspection documentation.

QUESTION NO: 17

Which of these options is the most secure procedure for storing backup tapes?

A. In a climate controlled facility offsite

B. On a different floor in the same building

C. Inside the data center for faster retrieval in a fireproof safe

D. In a cool dry environment

ANSWER: A

Explanation:

The most secure procedure is storing backup tapes *in a climate controlled facility offsite*. A resilient backup strategy must protect not only the confidentiality and integrity of backup media, but also its availability after a major incident. Keeping copies at a geographically separate location prevents a single event affecting the primary site—such as fire, flooding, power loss, structural damage, or a localized disaster—from destroying both production systems and the backups needed to recover them.

Climate control is also important for tape media because excessive heat, humidity, dust, and abrupt environmental changes can degrade media and reduce the reliability of restoration. A suitable offsite storage provider should apply physical access controls, inventory and chain-of-custody procedures, environmental monitoring, and secure transport. Encryption and documented key management further ensure that a lost or improperly accessed tape does not expose protected data.

This approach aligns with contingency-planning guidance that calls for storing backup copies at an alternate or offsite location and ensuring they remain protected and recoverable. NIST discusses alternate storage and system backup considerations in SP 800-34 Rev. 1. NARA also provides preservation guidance on appropriate environmental conditions for magnetic media in its magnetic tape storage and care guidance.

QUESTION NO: 18

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 it takes to convert biometric data into a template on a smart card.

B. The amount of time and resources that are necessary to maintain a biometric system.

C. The amount of time it takes to be either accepted or rejected when an individual provides identification and authentication information.

D. How long it takes to setup individual user accounts.

ANSWER: C

Explanation:

“The amount of time it takes to be either accepted or rejected when an individual provides identification and authentication information” correctly describes biometric processing speed. In an operational biometric system, a presented biometric sample is captured, processed into features, and compared with a stored reference template to produce a match or non-match decision. Processing speed therefore concerns the response time experienced during the authentication transaction: how quickly the system can complete its analysis and return an accept/reject result after the user presents the biometric characteristic.

This measurement is important when selecting a biometric solution because authentication delays directly affect usability, queueing, and the system’s ability to support expected transaction volumes. A system may have sound matching accuracy but still be unsuitable for a busy access-control location if the capture, feature extraction, comparison, and decision workflow takes too long. NIST describes biometric verification as comparing a captured biometric sample with an enrolled biometric reference to determine whether they match, while its biometric guidance also emphasizes the practical performance characteristics of presentation and matching systems. See NIST SP 800-63B: Digital Identity Guidelines and NIST’s definition of biometric verification.

QUESTION NO: 19

Which type of firewall operates by examining the state of active network connections before allowing or denying traffic?

A. Stateful inspection firewall

B. Packet sniffer

C. Network hub

D. Content delivery network

ANSWER: A

Explanation:

A stateful inspection firewall is correct because it maintains a state table for active communications and evaluates packets in the context of an established connection. For example, after an internal host initiates an approved TCP connection, the firewall can permit returning traffic that matches the connection state without requiring a separate broad inbound rule.

A stateless packet-filtering firewall evaluates packets independently using criteria such as source address, destination address, protocol, and port. Stateful inspection adds awareness of connection state, which generally permits more precise rule enforcement. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy.

QUESTION NO: 20

Which of the following controls help protect an organization against SQL injection attacks? (Choose two.)

A. Use parameterized queries.

B. Perform server-side allow-list input validation.

C. Concatenate user input into SQL statements.

D. Use client-side validation only.

E. Grant application accounts database administrator privileges.

ANSWER: A B

Explanation:

Parameterized queries are a primary protection against SQL injection because they separate SQL code from supplied data. The database driver sends parameter values independently of the query structure, preventing user-controlled input from being interpreted as additional SQL syntax.

Server-side allow-list input validation is also an appropriate control. It verifies that input conforms to the expected format, length, type, and permitted character set for the particular field. Input validation does not replace parameterized queries, but it reduces malicious and malformed input and supports secure application behavior. OWASP recommends parameterized queries as the preferred defense and identifies allow-list validation as an additional security measure. See the OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 21

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 reflect the changes.

Which type of vulnerability is present on this site?

A. Web Parameter Tampering

B. Cookie Tampering

C. XSS Reflection

D. SQL injection

ANSWER: A

Explanation:

Web Parameter Tampering is present because application-relevant values are supplied in the URL query string and can be altered by the client before the request reaches the server. In this case, the `Damount` and `Camount` parameters appear to represent amounts used by the banking application. The observed behavior—that changing those parameter values causes the displayed data to change—demonstrates that the application accepts client-controlled input for values that should be validated and, where security- or business-critical, derived from trusted server-side records.

HTTP query parameters are inherently untrusted because a browser user, proxy, script, or interception tool can modify them. Secure applications must enforce authorization, integrity, and business rules on the server for every request; they must not rely on URL parameters as immutable evidence of transaction values or account state. OWASP's Web Security Testing Guide describes testing for parameter tampering by modifying request parameters and checking whether the application improperly accepts the changed values. CWE-472 also classifies this pattern as external control of an assumed-immutable web parameter. See the OWASP Web Security Testing Guide and CWE-472.

QUESTION NO: 22

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:

Recommended DNS security practices include hardening DNS servers, using split-horizon DNS, restricting zone transfers, and deploying authoritative DNS servers with subnet diversity. Hardening reduces the DNS server's attack surface through prompt patching, minimal installed services, secure configuration, controlled administrative access, logging, and monitoring. Split-horizon operation separates internal DNS responses from public-facing responses, so internal names and addressing details are not unnecessarily exposed externally. Zone transfers should be restricted to explicitly authorized secondary servers, preferably protected with transaction signatures (TSIG) where supported, because zone data can reveal valuable details about hosts and network structure. Subnet diversity places redundant authoritative DNS servers on distinct network prefixes and paths. This helps preserve name-resolution availability if a routing failure, network outage, or targeted denial-of-service event affects one network segment. These controls support confidentiality of internal naming data, integrity of DNS administration, and resilient DNS availability. Guidance on securing authoritative DNS infrastructure and limiting zone transfers is available from CISA DNS Best Practices and the DNS operational requirements described in RFC 2182.

QUESTION NO: 23

When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

A. A bottom-up approach

B. A top-down approach

C. A senior creation approach

D. An IT assurance approach

ANSWER: B

Explanation:

A top-down approach is correct because the security program is driven by senior management's authority, support, and enforcement of organizational security policy. In this model, executives establish security objectives, approve policies, allocate budget and personnel, define accountability, and require business units to comply. Their visible sponsorship gives the program the organizational authority needed to apply security requirements consistently across departments, systems, and personnel.

This approach also aligns security governance with business goals and risk-management decisions. Senior leaders set the organization's risk appetite and ensure that security responsibilities are assigned, measured, and reviewed. Security teams then translate those management-approved directives into standards, procedures, technical controls, awareness activities, and monitoring processes. Effective governance therefore begins with leadership commitment rather than relying solely on individual technical teams or informal operational initiatives. NIST describes organizational leadership as responsible for establishing and maintaining an information-security program and supporting the policies and resources necessary for it. See NIST FIPS 200 and NIST SP 800-53.

QUESTION NO: 24

Which of the following is a protocol specifically designed for transporting event messages?

A. SYSLOG

B. SMS

C. SNMP

D. ICMP

ANSWER: A

Explanation:

SYSLOG is correct because it is the standardized protocol and message format used to convey system and application event records from a generating device or application to a logging collector. These event messages can record operational conditions, security-relevant activity, authentication events, service failures, configuration changes, and other auditable occurrences. A syslog architecture separates the originator that creates an event, a relay that may forward it, and a collector that receives and stores messages, allowing centralized logging across hosts, network devices, and security tools.

Syslog messages include structured metadata that helps recipients interpret and prioritize the event. In the modern syslog standard, the priority value combines a facility, identifying the general source category, with a severity level that indicates the event's urgency. This consistent representation makes syslog especially useful for monitoring, incident detection, correlation, alerting, and forensic investigation. Syslog is commonly transported over UDP port 514, while TCP and TLS-based transports can be used where more reliable delivery and protected transmission are needed. The IETF specification defines syslog as a protocol for conveying event notification messages, directly matching the question's requirement. See RFC 5424: The Syslog Protocol and the RFC 5426 syslog UDP transport specification.

QUESTION NO: 25

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 established password-auditing and password-recovery tools that can be used during an authorized security assessment to evaluate the strength of password hashes. L0phtCrack is historically associated with auditing Windows account passwords and supports techniques such as dictionary and brute-force attacks against obtained password-hash material. Its purpose in a legitimate engagement is to identify weak credentials so an organization can remediate them through stronger password policies, multifactor authentication, and secure hash storage.

John the Ripper is a widely used, cross-platform password-cracking suite. It supports numerous hash formats and can conduct wordlist, rule-based, incremental, and other cracking modes. In ethical hacking, a tester uses it only with explicit authorization and appropriately acquired hashes to demonstrate whether passwords are vulnerable to practical guessing attacks. The tool's official documentation describes its password-hash cracking capabilities and supported usage. L0phtCrack likewise identifies itself as a password-auditing and recovery application. References: Openwall: John the Ripper password cracker and L0phtCrack.

QUESTION NO: 26

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 spoofing works by sending forged ARP messages that associate an attacker-controlled MAC address with another device's IP address, commonly the default gateway. **Use port security on his switches.** is appropriate because switch-port security can restrict which MAC addresses are permitted on an access port and can take a protective action when an unauthorized MAC address is observed. This reduces the opportunity for an unauthorized device to join the LAN and inject spoofed ARP traffic. Cisco describes port-security configuration and violation actions in its Port Security Configuration Guide.

Use a tool like ARPwatch to monitor for strange ARP activity. provides an important detection control. ARPwatch maintains IP-to-MAC mappings and reports changes, allowing an administrator to investigate unexpected address changes quickly and limit the duration and impact of an attempted poisoning attack. Its purpose and behavior are documented in the arpwatch manual page.

If you have a small network, use static ARP entries. is also a valid preventive measure for critical hosts because fixed IP-to-MAC mappings prevent those systems from dynamically accepting a forged mapping for the specified peer. Static entries require careful maintenance, so they are most practical in small, stable environments or for high-value infrastructure endpoints.

QUESTION NO: 27

Which of the following are security advantages provided by using SSH instead of Telnet for remote administration? (Choose two.)

A. Encrypts the remote session

B. Supports server authentication

C. Uses UDP for reliable delivery

D. Eliminates the need for user authentication

E. Uses port 23 by default

ANSWER: A B

Explanation:

Encrypts the remote session and **supports server authentication** are correct. SSH protects the confidentiality and integrity of an administrative session by encrypting traffic between the client and server. This prevents a party that captures the network traffic from directly reading commands, passwords, and returned output.

SSH also supports server authentication, usually through host keys, allowing the client to verify the identity of the system it is contacting. Telnet transmits session data, including credentials, in cleartext and does not provide equivalent cryptographic peer authentication. See RFC 4251, The Secure Shell Protocol Architecture and CISA guidance on protecting network services.

QUESTION NO: 28

Which of the following is the primary objective of a rootkit?

A. It opens a port to provide an unauthorized service

B. It creates a buffer overflow

C. It replaces legitimate programs

D. It provides an undocumented opening in a program

ANSWER: C

Explanation:

A rootkit's defining purpose is to maintain covert, privileged access by modifying or substituting trusted operating-system components and programs. Therefore, *It replaces legitimate programs* is the best answer in this set. Rootkits commonly alter system utilities, libraries, drivers, or kernel components so that routine administration and security tools no longer accurately display malicious files, processes, network connections, user accounts, or other attacker activity. This replacement capability supports persistence and concealment: an attacker can retain elevated access while making the compromise difficult for users and defenders to detect.

The term does not describe merely gaining access; it describes the mechanisms used after compromise to hide that access and control. In host-based incidents, defenders should treat suspected rootkit activity as a high-severity integrity failure because the operating system and its normal reporting tools may no longer be trustworthy. NIST describes rootkits as tools that attackers use to conceal their presence, while MITRE ATT&CK documents rootkit techniques involving kernel modules, drivers, and other components that hide adversary behavior. See NIST's Rootkit definition and MITRE ATT&CK: Rootkit.

QUESTION NO: 29

A newly discovered flaw in a software application would be considered which kind of security vulnerability?

A. Input validation flaw

B. HTTP header injection vulnerability

C. 0-day vulnerability

D. Time-to-check to time-to-use flaw

ANSWER: C

Explanation:

A newly discovered flaw in a software application is generally classified as a **0-day vulnerability** when it is unknown to the software vendor or has no vendor-provided patch available at the time of discovery. The term "zero-day" reflects the fact that defenders have had zero days to prepare a corrective update before the vulnerability may be exposed to attack. Such flaws can arise in any application component and may permit outcomes such as unauthorized access, code execution, information disclosure, or denial of service, depending on the defect and affected environment.

In security operations, a zero-day requires prompt risk assessment and compensating controls while a permanent vendor fix is developed, tested, and deployed. Appropriate temporary measures can include restricting exposure, applying network filtering, disabling the affected feature, increasing monitoring, and following vendor incident guidance. CISA describes zero-day vulnerabilities as flaws that are unknown to the vendor or for which no patch is available, and emphasizes reducing exposure through timely vulnerability management and mitigations. See CISA: Understanding Zero-Day Vulnerabilities and NIST Cybersecurity Framework.

QUESTION NO: 30

An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

A. Timing attack

B. Replay attack

C. Memory trade-off attack

D. Chosen plain-text attack

ANSWER: D

Explanation:

Chosen plain-text attack is the applicable attack model because public-key encryption intentionally makes the public encryption key available to anyone, including an attacker. The attacker can select plaintext values, encrypt them with the

target's public key, and study the resulting ciphertexts in relation to the captured ciphertext. This capability is especially relevant when evaluating whether an encryption implementation leaks information through deterministic encryption, predictable message formats, weak padding, or an improperly designed cryptosystem.

In cryptographic terminology, a secure public-key encryption scheme should be resistant to chosen-plaintext attack (CPA), commonly expressed as indistinguishability under chosen-plaintext attack (IND-CPA). Such resistance means that even though an attacker can obtain encryptions of plaintexts of their choosing, they should not be able to determine meaningful information about a separate intercepted ciphertext. NIST identifies chosen-plaintext attack resistance as a fundamental security property for encryption schemes, while modern public-key encryption designs use appropriate randomized padding and encoding to provide it. See NIST's definition of a chosen-plaintext attack and its IND-CPA glossary entry.

QUESTION NO: 31

Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

A. NMAP

B. Metasploit

C. Nessus

D. BeEF

ANSWER: C

Explanation:

Nessus is correct because it is a vulnerability assessment platform designed to scan networked systems and identify security weaknesses, missing patches, insecure configurations, and known vulnerabilities. It performs credentialed or non-credentialed scans against hosts and services, then correlates the discovered software and configuration details with its regularly updated vulnerability knowledge base. This enables security teams to prioritize remediation based on the findings and their severity.

In addition to vulnerability detection, Nessus supports configuration and compliance assessment through audit policies. These checks can evaluate systems against recognized security configuration baselines and regulatory or organizational requirements, helping assess whether deployed systems conform to required controls. The resulting reports provide actionable evidence for vulnerability-management processes and compliance-audit activities. Tenable describes Nessus as a vulnerability assessment solution that provides broad vulnerability coverage and configuration assessment capabilities. Further product details and supported compliance auditing functions are available from Tenable Nessus and in the Tenable Nessus Compliance Checks documentation.

QUESTION NO: 32

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

A. BA810DBA98995F1817306D272A9441BB

B. 44EFCE164AB921CQAAD3B435B51404EE

C. 0182BD0BD4444BF836077A718CCDF409

D. CEC52EB9C8E3455DC2265B23734E0DAC

E. B757BF5C0D87772FAAD3B435B51404EE

F. E52CAC67419A9A224A3B108F3FA6CB6D

ANSWER: B E

Explanation:

LM hashing converts a password to uppercase, pads it to 14 bytes, and divides it into two independent seven-byte portions. Each portion produces a 16-hexadecimal-character value, yielding the familiar 32-character LM hash. If the original password has fewer than eight characters, the second seven-byte portion contains only padding. Its resulting fixed LM value is `AAD3B435B51404EE`. Therefore, the values `44EFCE164AB921CQAAD3B435B51404EE` and `B757BF5C0D87772FAAD3B435B51404EE` are the intended selections because both end with that empty-second-half marker. The first of those displayed strings contains `Q`, which is not a hexadecimal character and is evidently a transcription error; nevertheless, its final 16-character field is the standard marker used by this question to indicate a password shorter than eight characters. This behavior follows directly from the LM one-way-function construction, which splits the 14-byte password buffer into two seven-byte DES inputs. See Microsoft's NTLM protocol documentation and RFC 2433's description of the LM hash calculation at RFC 2433, section 8.3.

QUESTION NO: 33

Name two software tools used for OS guessing? (Choose two.)

A. Nmap

B. Snadboy

C. Queso

D. UserInfo

E. NetBus

ANSWER: A C

Explanation:

Nmap and **Queso** are tools used for operating-system guessing, more commonly called OS fingerprinting. OS fingerprinting estimates the remote host's operating system by examining characteristics of its TCP/IP stack and responses to deliberately crafted network probes. This is useful during reconnaissance because the identified OS helps an authorized tester select relevant enumeration methods and assess applicable security controls.

Nmap provides active OS detection through its `-O` capability. It sends a series of probes to target ports, evaluates response details such as TCP flags, window sizes, IP behavior, and ICMP responses, and compares the resulting fingerprint against its OS database. Nmap documentation describes this process and notes that reliable detection generally benefits from having at least one open and one closed TCP port available for probing. See the Nmap OS Detection documentation.

Queso is also an active TCP/IP stack fingerprinting utility. It sends crafted packets and analyzes the target's replies to infer the likely operating system or network stack implementation. Queso is a classic example of a dedicated OS-identification tool and is cataloged in the Security Tools Queso entry.

QUESTION NO: 34

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 a DNS replication mechanism used to copy DNS zone data from an authoritative primary server to an authorized secondary server. Therefore, “A zone transfer is accomplished with the DNS” is correct: the transfer is a DNS operation, not a capability of a separate “nslookup service.” A full zone transfer, commonly called AXFR, transfers the complete set of resource records for the requested zone, which makes “A zone transfer passes all zone information that a DNS server maintains” correct in the context of that zone. This behavior is why unrestricted zone transfers can expose hostnames, addressing, mail-routing records, and other information useful for reconnaissance.

DNS zone-transfer requests and responses use TCP port 53. Consequently, blocking inbound TCP port 53 connections prevents external systems from initiating TCP-based AXFR or IXFR transfers to that DNS server. In operational environments, the preferred approach is to permit TCP/53 only from explicitly authorized secondary DNS servers, rather than broadly exposing zone-transfer access. RFC 5936 defines AXFR as a DNS zone-transfer protocol and specifies TCP as its transport. DNS server guidance also recommends restricting transfers to approved hosts. See RFC 5936: DNS Zone Transfer Protocol (AXFR) and the BIND 9 allow-transfer documentation.

QUESTION NO: 35

The "gray box testing" methodology enforces what kind of restriction?

A. The internal operation of a system is only partly accessible to the tester.

B. The internal operation of a system is completely known to the tester.

C. Only the external operation of a system is accessible to the tester.

D. Only the internal operation of a system is known to the tester.

ANSWER: A

Explanation:

Gray-box testing means the tester has limited or partial knowledge of the target system’s internal implementation. Therefore, “The internal operation of a system is only partly accessible to the tester.” is correct. This approach occupies the middle ground between testing entirely from an external perspective and testing with full access to source code, architecture, and implementation details. In practical security testing, partial access may include selected design documents, API specifications, data-flow information, user roles, network diagrams, or limited source-code visibility. That information helps the tester create more informed test cases and focus on high-risk areas while still evaluating the application much as an external user or attacker would. Gray-box testing is useful because it combines knowledge-driven assessment of internal trust boundaries and logic with validation of observable behavior at interfaces. The OWASP Web Security Testing Guide describes testing approaches in which the tester may have differing levels of knowledge about an application, including partial knowledge that supports targeted assessment. NIST also recognizes that testing methods and the information made available to assessors should be defined as part of the assessment process. See the OWASP Web Security Testing Guide and NIST SP 800-115: Technical Guide to Information Security Testing and Assessment.

QUESTION NO: 36

What does a type 3 code 13 represent? (Choose two.)

A. Echo request

B. Destination unreachable

C. Network unreachable

D. Administratively prohibited

E. Port unreachable

F. Time exceeded

ANSWER: B D

Explanation:

In ICMP for IPv4, the Type field identifies the broad error-message category and the Code field supplies the specific reason within that category. A value of type 3 is the ICMP “Destination Unreachable” message category. Therefore, “Destination unreachable” correctly identifies the meaning of the type value. Within that category, code 13 denotes “Communication Administratively Prohibited,” commonly described as “Administratively prohibited.” This is generated when a router or firewall policy blocks forwarding or communication to the destination—for example, because an access-control rule prohibits the traffic. The distinction is important during network troubleshooting and security assessment: the host or router is explicitly reporting a policy-based denial, rather than simply being unable to find a route. The IANA ICMP Parameters registry lists type 3 as Destination Unreachable and maps code 13 to Communication Administratively Prohibited. RFC 1812 likewise specifies that routers use code 13 when communication with the destination is administratively prohibited. See the IANA ICMP Parameters registry and RFC 1812, section 5.2.7.1.

QUESTION NO: 37

Which of the following processes evaluates the adherence of an organization to its stated security policy?

A. Vulnerability assessment

B. Penetration testing

C. Risk assessment

D. Security auditing

ANSWER: D

Explanation:

Security auditing is correct because an audit is a systematic, independent evaluation of an organization’s controls, procedures, configurations, and operational practices against defined requirements. In this case, the stated security policy supplies the baseline: the audit gathers evidence to determine whether personnel, systems, and processes are actually complying with the policy’s requirements. Typical audit activities include reviewing policy and procedure documents, examining access-control settings and account records, sampling change-management evidence, checking logs, interviewing responsible personnel, and documenting findings for management. The result identifies compliance status, control gaps, and corrective actions needed to bring operations into alignment with the organization’s approved policy. This function is central to governance and assurance because a policy has value only when its requirements are implemented and consistently followed. NIST describes assessment as the process of evaluating implemented controls to determine the extent to which they are correctly implemented, operating as intended, and producing the desired outcome. ISO’s auditing guidance likewise frames audits as a systematic process for obtaining objective evidence and evaluating it against audit criteria. See NIST SP 800-53A and ISO 19011 auditing guidelines.

QUESTION NO: 38

What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

A. Blue Book

B. ISO 26029

C. Common Criteria

D. The Wassenaar Agreement

ANSWER: C

Explanation:

Common Criteria is the correct answer. Formally published as ISO/IEC 15408, the Common Criteria framework provides internationally recognized criteria for evaluating the security properties of IT products and systems. It establishes a common vocabulary and structured requirements for security functionality, called Security Functional Requirements, and for the assurance activities used to establish confidence that those functions are correctly designed and implemented, called Security Assurance Requirements.

Under Common Criteria, a product evaluation is performed against a defined Protection Profile or Security Target. The result helps customers, government procurement programs, and other relying parties compare evaluated products on a consistent basis and understand the scope and assurance level of the security claims. Evaluation Assurance Levels provide a progressively stronger scale of assurance, reflecting the rigor of the evidence and evaluation rather than a guarantee that a product is invulnerable. This standardized, requirements-based evaluation approach is precisely what creates a baseline of confidence in IT security functionality. The Common Criteria portal provides an overview of the framework and its recognition arrangements at Common Criteria Portal. ISO describes ISO/IEC 15408 as the standard for evaluating the security properties of IT products at ISO/IEC 15408-1.

QUESTION NO: 39

Which of the following are common characteristics of a buffer overflow vulnerability? (Choose two.)

A. Writing data beyond the bounds of an allocated buffer

B. Potential modification of control data in memory

C. Use of a cryptographically strong hash function

D. Encryption of all network traffic

E. Validation of every input length before copying

ANSWER: A B

Explanation:

Writing data beyond the bounds of an allocated buffer and **Potential modification of control data in memory** are correct. A buffer overflow occurs when software writes more data to a memory buffer than the buffer was allocated to hold. Depending on memory layout and protections, the excess data can overwrite adjacent variables, pointers, return addresses, or other control information.

Exploitation may allow a program crash, denial of service, information disclosure, or code execution. Defenses include memory-safe languages where appropriate, bounds checking, compiler hardening, address space layout randomization, data execution prevention, and secure coding review. See CWE-120: Buffer Copy without Checking Size of Input and CISA secure design guidance.

QUESTION NO: 40

What are two things that are possible when scanning UDP ports? (Choose two.)

A. A reset will be returned

B. An ICMP message will be returned

C. The four-way handshake will not be completed

D. An RFC 1294 message will be returned

E. Nothing

ANSWER: B E

Explanation:

UDP is connectionless, so a UDP port scan generally sends a UDP datagram to a target port and interprets any response, or lack of response. “An ICMP message will be returned” is correct because a closed UDP port commonly causes the target host to send an ICMP Destination Unreachable, Port Unreachable response. This is the strongest conventional indication that the scanned UDP port is closed. Firewalls and filtering devices may also generate other ICMP unreachable responses, which can help characterize packet filtering behavior.

“Nothing

” is also correct because an open UDP service will often accept the probe silently, and an open|filtered port may likewise produce no response when a firewall drops the packet or its reply. Therefore, silence is an expected and meaningful UDP scanning outcome, although it is inherently ambiguous: it does not conclusively distinguish an open port from one filtered by a packet filter. Scanner implementations typically retry UDP probes and consider the absence of any reply in their state assessment. Nmap’s UDP scan documentation describes ICMP port-unreachable replies as evidence of a closed port and no response as the usual basis for an open|filtered result. See Nmap Network Scanning: UDP Scan and RFC 1122.

QUESTION NO: 41

Which of the following are characteristics of a distributed denial-of-service attack? (Choose two.)

A. Traffic originates from multiple attacking systems.

B. It attempts to exhaust target resources.

C. It requires physical access to the target server.

D. It can occur only through TCP port 80.

E. It requires a valid administrative password.

ANSWER: A B

Explanation:

A distributed denial-of-service attack uses many systems to generate traffic or requests against a target. The attacking systems may be compromised hosts controlled as a botnet, allowing the attacker to create greater aggregate traffic volume and make simple source-based blocking less effective.

The goal is commonly to exhaust a target resource, such as available bandwidth, connection state, CPU capacity, memory, or application-worker capacity. DDoS attacks do not require successful authentication to the target, and they are not limited to a single protocol or source address. CISA describes denial-of-service attacks as attempts to make systems or networks unavailable by overwhelming resources, including attacks originating from multiple systems. See CISA guidance on denial-of-service attacks.

QUESTION NO: 42

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

A. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

B. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR

C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program

D. Overwrites the original MBR and only executes the new virus code

ANSWER: B

Explanation:

“Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR” correctly describes a common boot-sector virus infection technique. The Master Boot Record is located in the first sector of a bootable disk and is executed early in the startup sequence, before the operating system loads. By preserving the legitimate boot record elsewhere on the disk while placing malicious code at the original boot location, the virus can gain control when the system starts. Its code can then execute its payload and transfer control to the relocated legitimate boot information so the computer may continue booting normally, helping the infection remain less immediately apparent to the user.

This placement is particularly significant because firmware reads the initial boot code directly from the boot device. Historic boot-sector malware commonly spread through removable media and infected systems when they booted from infected disks. Understanding the boot process and the role of the Master Boot Record is essential when assessing this type of malware. See Microsoft’s overview of MBR-based disk architecture and the MITRE ATT&CK Bootkit technique for related boot-level persistence context.

QUESTION NO: 43

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:

NetBIOS-related Windows networking should be filtered at the firewall using the NetBIOS Name Service, NetBIOS Datagram Service, and NetBIOS Session Service ports. **137 and 138** cover NetBIOS name-resolution and datagram traffic, normally carried over UDP. Blocking them prevents NetBIOS name announcements, name queries, and datagram services from crossing the firewall boundary. **139** is the TCP NetBIOS Session Service port, historically used by Windows systems for session-oriented file and printer sharing over NetBIOS.

445 should also be blocked when the objective is to prevent exposure of the associated Windows file-sharing service. Modern Windows systems can use direct-hosted SMB on TCP 445 instead of encapsulating SMB in a NetBIOS session. Consequently, filtering 445 along with the NetBIOS ports prevents SMB/file-sharing access from bypassing the NetBIOS transport controls. Microsoft’s Windows port-requirements guidance identifies UDP 137 and 138, TCP 139, and TCP 445 as relevant ports for these Windows networking services. Apply the restrictions in the needed inbound and outbound firewall directions, allowing exceptions only where an explicitly required, secured service path exists. See Microsoft’s service overview and network port requirements and Microsoft guidance for securing SMB traffic.

QUESTION NO: 44

A security administrator notices that the log file of the company’s webserver contains suspicious entries:

\[20/Mar/2011:10:49:07\] "GET /login.php?user=test'+oR+3>2%20-- HTTP/1.1" 200 9958
\[20/Mar/2011:10:51:02\] "GET /login.php?user=admin';%20-- HTTP/1.1" 200 9978

The administrator decides to further investigate and analyze the source code of login.php file:

```
php
include('../../config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = mysql_query($sql) or die ("couldn't execute query");

if (mysql_num_rows($result) != 0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to

A. command injection.

B. SQL injection.

C. directory traversal.

D. LDAP injection.

ANSWER: B

Explanation:

SQL injection. is correct because a login script becomes vulnerable to SQL injection when it incorporates attacker-controlled login data directly into a database query rather than treating that data strictly as parameter values. Suspicious web-server log entries associated with a login endpoint commonly reveal crafted input intended to alter a query's syntax or logic, such as quote characters, SQL operators, comments, or tautological conditions. During source-code analysis, this conclusion is supported when request parameters are concatenated into a SQL statement used to retrieve or validate account records. In that situation, the supplied value can change the meaning of the query and potentially bypass authentication or expose database data.

The appropriate secure implementation is to use parameterized queries (prepared statements), so the database separates the fixed SQL command structure from untrusted values. Input validation can complement parameterization, but it does not replace it. OWASP describes SQL injection as occurring when untrusted data is sent to an interpreter as part of a command or query and recommends prepared statements as a primary defense. See the OWASP SQL Injection overview and the OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 45

In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?

A. Implementing IPv4 security in a dual-stack network offers protection from IPv6 attacks too.

B. Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.

C. Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addresses.

D. Vulnerabilities in the application layer are greatly different from IPv4.

ANSWER: B

Explanation:

“Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.” is correct because moving from IPv4 to IPv6 does not inherently change the fundamental security weaknesses in applications. Application-layer flaws arise primarily from application logic, insecure authentication and session handling, improper input validation, insecure deserialization, authorization failures, and implementation defects. These weaknesses exist above the IP layer, so an application that is vulnerable when reached over IPv4 generally remains vulnerable when it is reached over IPv6.

Accordingly, common attack patterns—such as injection, credential attacks, cross-site scripting, malicious file handling, and exploitation of insecure APIs—continue to apply. The core defensive practices also remain the same: secure design and coding, patch management, strong authentication, least privilege, input validation, logging, monitoring, web application protection, and vulnerability testing. Security teams should ensure that these controls, asset inventories, monitoring systems, and testing processes operate over both IP versions. IPv6 can introduce network-layer operational and configuration considerations, but it does not eliminate or fundamentally transform typical application-layer vulnerability classes. NIST’s IPv6 security guidance discusses the need to address IPv6 alongside existing security controls, while OWASP documents the application-focused risks that are largely protocol-independent. See NIST SP 800-119 and the OWASP Top 10.

QUESTION NO: 46

The company ABC recently contracted 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. What of the following options can be useful to ensure the integrity of the data?

A. The document can be sent to the accountant using an exclusive USB for that document.

B. The CFO can use a hash algorithm in the document once he approved the financial statements.

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 it is the same document.

D. The CFO can use an excel file with a password.

ANSWER: B

Explanation:

The CFO can use a hash algorithm in the document once he approved the financial statements. A cryptographic hash function produces a fixed-length digest that is uniquely tied, for practical purposes, to the contents of the approved financial statements. The CFO can calculate the hash value at approval time and provide that expected value to the accountant through a trusted channel or alongside the document. When the accountant receives the file, they calculate its hash using the same algorithm and compare the result with the CFO’s approved hash. Matching values provide strong assurance that the received data is identical to the data that was approved; even a very small alteration to the document produces a different digest.

For an operationally stronger implementation, the CFO should digitally sign the hash with their private key. This preserves the integrity-verification benefit while also allowing the accountant to validate that the approval originated with the CFO. Current guidance recommends modern cryptographic hash algorithms, such as SHA-256 or stronger, rather than deprecated algorithms such as MD5 or SHA-1. NIST describes approved hash functions and their security properties in FIPS 180-4: Secure Hash Standard. For the role of digital signatures in detecting modification and validating origin, see FIPS 186-5: Digital Signature Standard.

QUESTION NO: 47

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 positive

B. False negative

C. True positive

D. True negative

ANSWER: A

Explanation:

False positive is correct because the IDS generated a positive detection event—an alert—but the underlying activity was authorized and benign. In this scenario, the system administrator used their own computer to access the external router for the legitimate operational purpose of updating its configuration. Although router-management access can resemble suspicious activity to an IDS, particularly if it matches a rule for administrative protocols, remote management, or a sensitive network device, there is no actual malicious action described.

In intrusion-detection terminology, a false positive occurs when a security tool reports an attack, policy violation, or otherwise suspicious event even though the observed activity is legitimate. Reviewing alert context, including the source host, authorized administrator identity, approved maintenance activity, time window, and change records, allows the administrator to classify this event correctly. This classification can also guide IDS rule tuning or allowlisting so that approved administrative work generates fewer unnecessary alerts while monitoring remains effective. NIST defines a false positive as an alert indicating malicious activity when none occurred; see the NIST CSRC glossary. Additional IDS analysis and tuning guidance is available in NIST SP 800-94.

QUESTION NO: 48

How do employers protect assets with security policies pertaining to employee surveillance activities?

A. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.

B. Employers use informal verbal communication channels to explain employee monitoring activities to employees.

C. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.

D. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.

ANSWER: D

Explanation:

Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences. This is the appropriate policy-based approach because a written surveillance or acceptable-use policy formally notifies personnel about what organizational systems and activities may be monitored, the purposes for which monitoring is performed, the limits that apply, and the consequences of violations. Clear written notice supports consistent enforcement, helps establish that users understood the conditions of using company assets, and creates an auditable record of acknowledgement. From an information-security perspective, such a policy helps protect organizational assets by setting expectations for authorized use and by enabling monitoring necessary to detect misuse, data loss, insider threats, and security incidents. It should be distributed to employees, incorporated into onboarding and periodic awareness training, and reviewed with legal and human-resources stakeholders to account for applicable privacy, labor, and jurisdictional requirements. NIST's guidance identifies rules of behavior as a documented set of user responsibilities and expected conduct for information systems; acknowledgment is an important component of communicating those rules. See NIST SP 800-53 Rev. 5 and the related NIST control assessment guidance.

QUESTION NO: 49

Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

A. UDP 123

B. UDP 541

C. UDP 514

D. UDP 415

ANSWER: C

Explanation:

UDP 514 is the traditional network port used by the Syslog protocol to transmit log messages from devices, hosts, and applications to a centralized log collector or log-analysis tool. When the collector is located behind a firewall, the firewall may need an inbound rule permitting UDP traffic to destination port 514 from the authorized logging sources. Syslog is widely used for centralized event collection because network devices, servers, security appliances, and many applications can forward operational and security logs in this format. The Internet Assigned Numbers Authority registers port 514 for the Syslog service over UDP, reflecting this conventional transport configuration. Although modern deployments may instead use TCP, TLS, or a vendor-specific port to improve delivery reliability and protect log data in transit, UDP port 514 is the expected answer for the standard Syslog forwarding scenario described. Firewall rules should be limited to known source systems and the designated collector where possible, since log messages may contain security-relevant information. See the IANA Service Name and Port Number Registry and RFC 5426: Transmission of Syslog Messages over UDP.

QUESTION NO: 50

Which of the following are benefits of network segmentation? (Choose two.)

A. It can limit lateral movement after a compromise.

B. It permits security policies to differ by network zone.

C. It eliminates the need for authentication controls.

D. It guarantees that malware cannot enter the network.

E. It removes the need to patch systems.

ANSWER: A B

Explanation:

Network segmentation limits lateral movement by separating systems into distinct security zones and controlling communications between those zones. If an attacker compromises a workstation in one segment, filtering and access controls can prevent direct access to sensitive servers, management networks, or other protected segments.

Segmentation also allows organizations to apply different security policies based on system function and risk. For example, guest wireless clients, payment systems, user workstations, and administrative interfaces can be placed in separate segments with only the explicitly required traffic permitted between them. NIST describes network segmentation as a means of separating systems and limiting communications to reduce exposure in NIST SP 800-125B. CISA also recommends segmentation as a defense against lateral movement. See CISA Cybersecurity Performance Goals.

QUESTION NO: 51

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

A. Public Key

B. Secret Key

C. Hash Algorithm

D. Digest

ANSWER: A

Explanation:

Public Key is correct because PGP, SSL, and IKE use public-key (asymmetric) cryptography as a core part of establishing secure communications. In public-key cryptography, each participant has a mathematically related key pair: a public key that can be distributed and a private key that must remain secret. This arrangement supports essential security functions such as authentication, digital signatures, and secure exchange or establishment of symmetric session keys.

PGP uses public-key operations to protect messages and to create or verify digital signatures. SSL, the predecessor to TLS, uses public-key certificates and asymmetric cryptography to authenticate endpoints and negotiate protected session material. IKE is the key-management protocol used with IPsec; it authenticates peers and establishes shared security associations and keys, commonly using public-key techniques such as digital signatures or public-key certificates. Although these protocols also use symmetric encryption and hash functions for particular tasks, their common cryptographic classification in this context is public-key cryptography. See the OpenPGP Message Format and Internet Key Exchange Protocol Version 2 (IKEv2).

QUESTION NO: 52

One of your team members has asked you to analyze the following SOA record. What is the version?

Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

A. 200303028

B. 3600

C. 604800

D. 2400

E. 60

F. 4800

G. 200302028

ANSWER: G

Explanation:

The SOA record version is **200302028**. In DNS terminology, the field described informally as the SOA "version" is the *serial number*. It is the first numeric value in the parenthesized timing and control fields following the primary authoritative name server and the responsible party's mailbox. In the presented record, the relevant sequence begins `(200302028 3600 3600 604800 2400)`, making `200302028` the serial value.

The serial number identifies the current version of a DNS zone for zone-transfer purposes. Secondary authoritative DNS servers compare their locally held SOA serial with the primary server's serial; when the primary value is greater under DNS serial arithmetic, the secondary knows that it should request a zone transfer to obtain the updated zone data. Administrators commonly format serials using a date-based convention, but DNS treats the value as an unsigned 32-bit serial number rather than requiring a particular human-readable format. The other numeric fields are operational timers for refresh, retry, expiry, and negative caching behavior, not the zone version. See RFC 1035, SOA record format and RFC 1982, Serial Number Arithmetic.

QUESTION NO: 53

Which of the following practices reduce the risk of wireless evil twin attacks? (Choose two.)

A. Validate the authentication server certificate.

B. Train users to avoid unapproved wireless networks.

C. Disable encryption on the corporate SSID.

D. Use a shared default administrator password on access points.

E. Configure clients to accept any certificate warning.

ANSWER: A B

Explanation:

Using WPA2-Enterprise or WPA3-Enterprise with certificate validation helps reduce evil twin risk because the client can authenticate the legitimate enterprise authentication server. A rogue access point that presents an untrusted or incorrect certificate should not be accepted by a properly configured client.

Training users not to join unapproved wireless networks is also important. Evil twin attacks frequently rely on a deceptive SSID that resembles a legitimate network and on users accepting unexpected sign-in prompts or certificate warnings. Wireless monitoring can provide additional detection, but user and device configuration remain key controls. NIST discusses enterprise wireless security and authentication considerations in NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks.

QUESTION NO: 54

You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.

What tool will help you with the task?

A. Metagoofil

B. Armitage

C. Dimitry

D. cdpsnarf

ANSWER: A

Explanation:

Metagoofil is the appropriate choice because it is an information-gathering tool designed to locate public documents associated with a target and extract useful embedded metadata from them. Its primary use in a penetration-testing reconnaissance workflow is identifying documents such as PDF and Microsoft Office files, downloading them, and parsing metadata that may reveal usernames, author names, software or operating-system details, document paths, server names, and other infrastructure clues. These details can help a tester build an understanding of the target environment and identify areas for further authorized investigation.

Metagoofil automates an otherwise repetitive process: finding exposed documents through search engines, retrieving them, extracting their metadata through supporting libraries, and presenting the results in a report. This directly matches the stated objective of performing metadata analysis during information gathering. While metadata capabilities vary by file format and tool version, Metagoofil is the CEH-associated reconnaissance utility specifically intended for harvesting metadata from publicly available target documents. The project documentation describes its document-searching and metadata-extraction purpose: Metagoofil GitHub repository. Kali Linux also provides package information for the tool: Kali Tools: Metagoofil.

QUESTION NO: 55

Which of the following practices help reduce the risk of sensitive information being exposed through error messages in a web application? (Choose two.)

A. Display generic error messages to users

B. Log detailed errors securely on the server

C. Display database exception details in the browser

D. Enable debug mode in production

E. Include stack traces in all HTTP responses

ANSWER: A B

Explanation:

Display generic error messages to users and **Log detailed errors securely on the server** are correct. Generic client-facing errors avoid disclosing implementation details such as stack traces, database names, file paths, software versions, and internal hostnames. Such information can help an attacker map the application and identify likely weaknesses.

Detailed diagnostic information remains valuable for administrators and developers, but it should be retained in protected server-side logs with appropriate access control and monitoring. Production applications should disable debug output and implement centralized exception handling. See the OWASP Improper Error Handling guidance and CWE-209: Generation of Error Message Containing Sensitive Information.

QUESTION NO: 56

Which of the following measures help protect against password spraying attacks? (Choose two.)

A. Require multifactor authentication

B. Monitor failed authentication attempts across many accounts

C. Use the same password for all service accounts

D. Disable all authentication logging

E. Increase the number of permitted failed logons

ANSWER: A B

Explanation:

Require multifactor authentication and **monitor failed authentication attempts across many accounts** are correct. Password spraying attempts a small number of commonly used passwords against many accounts to avoid triggering lockout thresholds associated with repeated failures against one account. Multifactor authentication reduces the value of a guessed password because possession of the password alone is insufficient for access.

Monitoring authentication failures across multiple accounts can identify the distributed pattern characteristic of password spraying, such as one source attempting the same password against many usernames. Strong password policies, disabling legacy authentication, conditional access controls, and alerting on unusual login patterns further reduce exposure. See MITRE ATT&CK Password Spraying and NIST SP 800-63B.

QUESTION NO: 57

Which of the following are common indicators of a successful ARP poisoning attack? (Choose two.)

A. The default gateway IP address maps to a new MAC address.

B. Multiple IP addresses map to the same unexpected MAC address.

C. DNS zone transfers begin using UDP port 53.

D. All TCP ports return a SYN-ACK response.

E. The DHCP server assigns only static addresses.

ANSWER: A B

Explanation:

An unexpected change in the MAC address associated with the default gateway is an important indicator of ARP poisoning. In a typical attack, an attacker sends forged ARP replies that cause a victim to associate the gateway IP address with the attacker-controlled MAC address. Traffic intended for the gateway can then be redirected through the attacker.

Multiple IP addresses resolving to the same MAC address can also indicate suspicious ARP activity. Although some legitimate configurations may use shared or virtual MAC addresses, this condition should be investigated when it appears unexpectedly on an ordinary switched LAN. ARPwatch and switch security features can help identify anomalous IP-to-MAC mappings. See RFC 826, Address Resolution Protocol and the arpwatch manual page.

QUESTION NO: 58

You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account.

What should you do?

A. Report immediately to the administrator

B. Do not report it and continue the penetration test.

C. Transfer money from the administrator's account to another account.

D. Do not transfer the money but steal the bitcoins.

ANSWER: A

Explanation:

Report immediately to the administrator is the appropriate response because a penetration test is an authorized security assessment, not permission to access, use, disclose, or alter sensitive personal financial data beyond what is necessary to validate the finding. Credentials for a bank account and a Bitcoin account represent highly sensitive information and may create an immediate risk of financial loss or unauthorized account access. The tester should stop any further interaction with those accounts, preserve only the minimum evidence needed to document the exposure, and promptly notify the designated client contact through the engagement's agreed escalation process. In this scenario, reporting to the administrator enables rapid credential rotation, account review, and incident-response actions while maintaining the tester's professional and legal obligations. The finding should be recorded accurately in the final report, including the affected location, the access path that exposed it, the business impact, and remediation guidance, while avoiding unnecessary inclusion of the actual credentials. NIST's technical guide for security testing emphasizes planning, rules of engagement, documentation, and careful handling of results throughout an assessment. See NIST SP 800-115: Technical Guide to Information Security Testing and Assessment and the Penetration Testing Execution Standard Rules of Engagement.