PassQueen
a.k.a dumpsqueen.com

Hacker Tools, Techniques, Exploits and Incident Handling

SANS SEC504

Version Demo

Total Demo Questions: 38

Total Premium Questions: 380

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Incident Handling and Cyber Investigation	33
Topic 2, Computer and Network Hacker Exploits	259
Topic 3, Endpoint Detection and Response	10
Topic 4, Network Detection and Response	22
Topic 5, Defending Against Web Application Attacks	45
Topic 6, Mix Questions	11
Total	380

QUESTION NO: 1

Which of the following tools can be used as penetration tools in the Information system auditing process?

Each correct answer represents a complete solution. Choose two.

A. Nmap

B. Snort

C. SARA

D. Nessus

ANSWER: C D

Explanation:

SARA and Nessus are appropriate tools for the vulnerability-assessment and penetration-testing activities that support an information-system audit. SARA (Security Auditor's Research Assistant) is a vulnerability scanner that performs checks against discovered systems and services to identify known weaknesses and configuration exposures. Nessus is likewise a widely used vulnerability-assessment scanner that identifies vulnerabilities, missing patches, insecure configurations, and exposure details. In an authorized audit, the findings from these tools give the assessor evidence to validate, prioritize, and report technical risk; they also provide targets for carefully scoped follow-up testing. This use must be governed by explicit authorization, defined scope, safe scanning settings, and procedures for validating findings before reporting them as confirmed issues. NIST's technical security-testing guidance identifies vulnerability scanning as a core testing technique and emphasizes planning, execution, analysis, and mitigation reporting. Nessus documentation similarly describes using scan results to identify vulnerabilities and configuration issues across assessed assets. See NIST SP 800-115, Technical Guide to Information Security Testing and Assessment and Tenable Nessus documentation.

QUESTION NO: 2

You want to measure the number of heaps used and overflows occurred at a point in time. Which of the following commands will you run to activate the appropriate monitor?

A. UPDATE DBM CONFIGURATION USING DFT_MON_TABLE

B. UPDATE DBM CONFIGURATION DFT_MON_TIMESTAMP

C. UPDATE DBM CONFIGURATION USING DFT_MON_BUFPOOL

D. UPDATE DBM CONFIGURATION USING DFT_MON_SORT ON

ANSWER: D

Explanation:

`UPDATE DBM CONFIGURATION USING DFT_MON_SORT ON` enables the default sort-monitor switch at the database-manager level. This is the appropriate monitor because sort monitoring collects statistics about sort activity, including sort heap use and sort overflows. A sort overflow occurs when a sort cannot be completed entirely in its allocated sort memory and must use temporary disk space; this is an important performance indicator because frequent overflows can point to insufficient sort memory or inefficient query activity. Enabling the switch in the database-manager configuration establishes the default monitoring behavior for subsequently activated databases. The explicit `ON` value is required to activate the parameter. IBM documents `DFT_MON_SORT` as the default monitoring switch for sort information, and its documentation identifies sort-related counters such as total sorts and sort overflows as monitor data used to evaluate sorting behavior. See IBM's DFT_MON_SORT parameter documentation and the UPDATE DATABASE MANAGER CONFIGURATION command reference.

QUESTION NO: 3

You are concerned about rootkits on your network communicating with attackers outside your network. Without using an IDS how can you detect this sort of activity?

A. By examining your domain controller server logs.

B. You cannot, you need an IDS.

C. By examining your firewall logs.

D. By setting up a DMZ.

ANSWER: C

Explanation:

By examining your firewall logs is correct because a perimeter firewall records connections crossing the network boundary, including outbound sessions initiated by potentially compromised internal systems. Rootkits commonly maintain command-and-control access by making periodic outbound connections, using unusual destination addresses or ports, generating recurring beacon-like traffic, or creating unexpected connections from systems that should not normally access the Internet. Reviewing allowed outbound traffic—not only denied traffic—can therefore reveal communication patterns requiring investigation. Useful indicators include connections to rare external IP addresses, outbound traffic from servers with narrowly defined functions, repeated short sessions at regular intervals, unexpected encrypted connections, and activity outside an endpoint's normal operational baseline. Firewall logs also provide key pivot data such as internal source address, destination, protocol, port, timestamp, and action, enabling an incident handler to identify the suspected host and correlate the event with endpoint, DNS, proxy, and authentication evidence. This is a practical network-monitoring control even when a dedicated intrusion detection system is unavailable. NIST incident-handling guidance identifies firewall and network-device logs as valuable sources of incident evidence and recommends centralized logging and analysis for detection and response. See NIST SP 800-61 Rev. 2 and CISA guidance on monitoring and reducing attack exposure.

QUESTION NO: 4

The IT administrator wants to implement a stronger security policy. What are the four most important security priorities for PassGuide Software Systems Pvt. Ltd.?

A. Providing secure communications between the overseas office and the headquarters.

B. Implementing Certificate services on Texas office.

C. Protecting employee data on portable computers.

D. Providing two-factor authentication.

E. Ensuring secure authentication.

F. Preventing unauthorized network access.

G. Providing secure communications between Washington and the headquarters office.

H. Preventing denial-of-service attacks.

ANSWER: A C E F

Explanation:

The key priorities are "Providing secure communications between the overseas office and the headquarters," "Protecting employee data on portable computers," "Ensuring secure authentication," and "Preventing unauthorized network access." Together, these address foundational security objectives: protecting information in transit, safeguarding data on mobile endpoints, verifying user identity before access is granted, and restricting network access to authorized users and devices. Secure interoffice communications protect confidentiality and integrity when business data crosses untrusted networks. Portable-computer protection is essential because laptops are susceptible to loss, theft, and use outside managed office environments. Secure authentication ensures that access decisions are based on trustworthy identity verification, while network-access controls enforce those decisions at the organizational boundary and within internal environments. These priorities align with NIST's guidance that security programs should manage access control, identification and authentication,

communications protection, and system and information integrity as core control areas. NIST also identifies mobile-device security as requiring protections for data stored on and transmitted by enterprise mobile devices. See the NIST SP 800-53 control catalog and NIST SP 800-124 mobile-device security guidance.

QUESTION NO: 5

Which of the following techniques does an attacker use to sniff data frames on a local area network and modify the traffic?

A. MAC spoofing

B. IP address spoofing

C. Email spoofing

D. ARP spoofing

ANSWER: D

Explanation:

ARP spoofing is correct because it enables a machine on the same Ethernet LAN to position itself between communicating systems. The Address Resolution Protocol maps an IPv4 address to a local MAC address so that hosts can place frames on the network. An attacker sends forged ARP replies that associate the attacker-controlled MAC address with the IP address of a legitimate peer, commonly the default gateway. Victims then send frames intended for that peer to the attacker instead. By forwarding the received traffic to its legitimate destination, the attacker can maintain connectivity while acting as a man-in-the-middle. This position permits capture of unencrypted traffic and, where protocol protections do not detect changes, alteration or injection of traffic before it is relayed. ARP was designed for trusted local networks and does not authenticate ARP replies, which makes this attack feasible on susceptible LANs. Defensive controls include switch features such as Dynamic ARP Inspection, static bindings where appropriate, network segmentation, and use of encrypted, integrity-protected protocols so intercepted traffic cannot be read or changed. Cisco's overview of ARP operation describes how ARP resolves IP addresses to MAC addresses, and the CISA guidance on network attacks provides relevant defensive context for protecting network communications.

QUESTION NO: 6

Which of the following can be used as a countermeasure against the SQL injection attack?

Each correct answer represents a complete solution. Choose two.

A. mysql_real_escape_string()

B. session_regenerate_id()

C. mysql_escape_string()

D. Prepared statement

ANSWER: A D

Explanation:

`mysql_real_escape_string()` can mitigate SQL injection in legacy PHP/MySQL code when it is used correctly on every untrusted string value before that value is incorporated into a quoted SQL literal. Unlike generic escaping, it accounts for the active database connection's character set, which is essential for correct escaping behavior. Its use is historically recognized as a defensive control for applications built with the old MySQL extension, although that extension is obsolete and should be replaced in maintained applications.

A prepared statement is the preferred modern defense because it sends the SQL structure separately from parameter data. The database parses the statement template as code and treats bound values strictly as data, even if a value contains quote characters or text resembling SQL syntax. This protection applies consistently when all externally supplied values are bound

as parameters and dynamic SQL identifiers are handled through an appropriate allowlist. PHP's documentation recommends prepared statements for parameterized queries and notes their benefits for security. See the PHP documentation for mysql_real_escape_string() and MySQLi prepared statements.

QUESTION NO: 7

Which of the following statements are true about firewalking?

Each correct answer represents a complete solution. Choose all that apply.

A. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall.

B. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.

C. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.

D. Firewalking works on the UDP packets.

ANSWER: A B C D

Explanation:

Firewalking is a reconnaissance technique for mapping a filtering device's policy from an external position. It generally starts by identifying the hop distance to the firewall or filtering gateway and uses a reachable system beyond that device as the probe destination. This supplies the network path information needed to place the probe's time-to-live precisely. A probe is crafted so that, if the firewall permits its selected transport protocol and destination port, it passes through the firewall and expires at the next routed hop. That downstream router then returns an ICMP Time Exceeded message, revealing that the tested traffic was allowed through the firewall. Repeating this process with different port and protocol combinations can identify services or protocol types permitted by the filter. Although descriptions often demonstrate the technique with TCP probes, firewalking is not limited to TCP: UDP probes can also be used, provided routing and ICMP responses permit the necessary observations. The Firewalk tool documentation specifically describes support for TCP and UDP scanning, while router requirements for generating ICMP Time Exceeded messages when a packet's TTL reaches zero are described in RFC 1812. See the Kali Firewalk tool documentation and RFC 1812.

QUESTION NO: 8

In which of the following steps of the incident handling processes does the Incident Handler make sure that all business processes and functions are back to normal and then also wants to monitor the system or processes to ensure that the system is not compromised again?

A. Eradication

B. Lesson Learned

C. Recovery

D. Containment

ANSWER: C

Explanation:

Recovery is the incident-handling phase in which the organization safely returns affected systems and business operations to normal service. After containment and eradication have addressed the immediate threat and its cause, the incident handler restores systems from known-good backups or rebuilds them as appropriate, validates that business functions operate correctly, and returns services to production in a controlled manner. Recovery is not simply turning systems back on: it includes heightened monitoring, logging, and validation to detect signs that an attacker retained access, that malware remains, or that the original vulnerability is being exploited again. The duration and depth of this monitoring should reflect the incident's severity, the attacker's capabilities, and the organization's risk tolerance. NIST's incident-response lifecycle

explicitly identifies recovery as the stage for restoring normal operations and confirming that remediated systems are functioning as intended, while continued observation helps ensure the incident does not recur. This directly matches the requirement to verify normal business processes and monitor for renewed compromise. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and the SANS SEC504 course overview.

QUESTION NO: 9

Which of the following statements about a Trojan horse are true?

Each correct answer represents a complete solution. Choose two.

A. It is a macro or script that attaches itself to a file or template.

B. The writers of a Trojan horse can use it later to gain unauthorized access to a computer.

C. It is a malicious software program code that resembles another normal program.

D. It infects the boot record on hard disks and floppy disks.

ANSWER: B C

Explanation:

A Trojan horse is malicious software that masquerades as, or is embedded within, something that appears legitimate or useful to persuade a user to execute it. Therefore, “It is a malicious software program code that resembles another normal program.” correctly captures the defining deception characteristic of a Trojan. The apparent normality of the software is what distinguishes the social-engineering delivery aspect of a Trojan from malware that primarily spreads by independently replicating.

“The writers of a Trojan horse can use it later to gain unauthorized access to a computer.” is also correct because Trojans commonly establish a backdoor, remote-access capability, or another persistence mechanism after execution. This enables an attacker to return to the affected host, issue commands, steal data, deploy additional payloads, or move further into an environment without authorized user approval. In incident handling, a suspected Trojan should be treated as a potential compromise of host integrity and credentials, since its visible behavior may not reveal all attacker access mechanisms. CISA describes Trojan malware as software that misleads users about its true intent, while Microsoft’s security documentation identifies remote-access Trojans as malware used to control compromised devices. See CISA: Understanding Malware and Microsoft: What is malware?.

QUESTION NO: 10

Which of the following techniques can be used to map 'open' or 'pass through' ports on a gateway?

A. Traceport

B. Tracefire

C. Tracegate

D. Traceroute

ANSWER: A

Explanation:

Traceport is the correct technique because it applies traceroute-style TTL probing to TCP traffic aimed at a selected destination port. Rather than only identifying the network path, this approach can help determine whether a gateway or firewall permits packets for that port to pass toward the target. By varying packet TTL values and observing responses such as ICMP Time Exceeded messages, TCP reset packets, or the absence of a response, an analyst can infer where filtering occurs and identify services whose traffic is allowed through the gateway. This makes it useful during authorized perimeter assessment and incident analysis when the goal is to understand exposed paths through a filtering device, not merely to enumerate ports directly on a host. The underlying behavior relies on IP TTL expiration and ICMP reporting, described in

RFC 1812. The broader security-testing principle of using carefully selected probe characteristics to evaluate firewall behavior is also covered in the Nmap Network Scanning Reference Guide. Results must be interpreted cautiously because modern stateful firewalls, NAT, ICMP rate limiting, and filtering policies can suppress or alter the responses on which traceport-style analysis depends.

QUESTION NO: 11

Which of the following protocols uses only User Datagram Protocol (UDP)?

A. POP3

B. FTP

C. ICMP

D. TFTP

ANSWER: D

Explanation:

TFTP is correct because it is a lightweight file-transfer protocol specified to use UDP as its transport protocol. A TFTP client sends its initial read or write request to UDP port 69 on the server. After the server accepts the request, the transfer proceeds using UDP datagrams, typically from a server-selected transient port. Rather than relying on TCP for connection establishment, ordered delivery, retransmission, or flow control, TFTP implements the limited reliability it needs at the application layer: data is sent in numbered blocks, and the recipient acknowledges each block. If an expected acknowledgment is not received within a timeout period, the sender retransmits the relevant packet. This simple UDP-based design keeps TFTP small and easy to implement, which is why it has traditionally been useful for tasks such as network-device bootstrapping and transferring configuration or firmware files in controlled environments. The normative TFTP specification explicitly states that it is implemented on top of UDP; see RFC 1350. IANA's service-name registry also identifies the well-known `tftp` service on UDP port 69: IANA Service Name and Port Number Registry.

QUESTION NO: 12

You are the Administrator for a corporate network. You are concerned about denial of service attacks.

Which of the following would be the most help against Denial of Service (DOS) attacks?

A. Packet filtering firewall

B. Network surveys.

C. Honey pot

D. Stateful Packet Inspection (SPI) firewall

ANSWER: D

Explanation:

Stateful Packet Inspection (SPI) firewall is the most helpful choice because it maintains context about active network connections and applies policy based on connection state, rather than evaluating each packet in isolation. At the network perimeter, this enables the firewall to discard unsolicited packets that do not belong to an established or permitted connection, helping reduce exposure to common connection-based denial-of-service attempts, malformed traffic, and spoofed packets. Stateful inspection also permits more precise rules for inbound services and can log connection behavior that supports detection and incident response. NIST describes stateful inspection as a core firewall capability that tracks the state of communications and uses that information when making filtering decisions; see NIST SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy. A stateful firewall is not a complete solution for a large-scale volumetric event that exhausts an Internet connection before traffic reaches the organization. Effective resilience should also include upstream provider support, traffic scrubbing or mitigation services, capacity planning, monitoring, and a practiced incident-response process.

CISA provides practical guidance on preparing for and responding to denial-of-service events at Understanding Denial-of-Service Attacks.

QUESTION NO: 13

Which of the following commands is used to access Windows resources from Linux workstation?

A. mutt

B. scp

C. rsync

D. smbclient

ANSWER: D

Explanation:

`smbclient` is the appropriate command because it is Samba's command-line SMB/CIFS client for accessing shared resources exposed by Windows systems from a Linux workstation. Windows file and printer sharing commonly uses the Server Message Block protocol, and `smbclient` lets an analyst authenticate to an SMB server, enumerate available shares, connect to a selected share, browse directories, and transfer files interactively or through scripted commands. For example, an investigator can use `smbclient -L //server -U username` to list available shares and then connect to a specific share with `smbclient //server/share -U username`. This makes it particularly useful during incident response, validation of access controls, and authorized assessment of Windows-hosted network resources. Samba documents `smbclient` as an FTP-like client for SMB/CIFS resources, including Microsoft Windows shares. Its support for SMB authentication and share operations directly addresses access to Windows network resources from Linux. See the Samba smbclient manual and the Samba documentation.

QUESTION NO: 14

Victor wants to send an encrypted message to his friend. He is using certain steganography technique to accomplish this task. He takes a cover object and changes it accordingly to hide information. This secret information is recovered only when the algorithm compares the changed cover with the original cover.

Which of the following Steganography methods is Victor using to accomplish the task?

A. The distortion technique

B. The spread spectrum technique

C. The substitution technique

D. The cover generation technique

ANSWER: A

Explanation:

The distortion technique is correct because it embeds a secret by making controlled modifications to an existing cover object, such as an image, audio file, or other digital media. Its defining characteristic is that successful extraction depends on having access to the original, unmodified cover as well as the altered version. The recovery process compares the two objects, identifies the deliberate changes introduced during embedding, and interprets those changes as the hidden message. This directly matches the stated requirement that the secret information can be recovered only by comparing the changed cover with its original version. In steganographic terminology, the original cover serves as a reference that allows the recipient to distinguish message-bearing distortions from the cover's ordinary content. This model can provide reliable decoding when the original object is shared securely, although that requirement also makes cover management an important operational consideration. A useful overview of steganography concepts, including cover objects and embedding approaches, is

available from NIST's overview of steganography in digital media. Additional technical background on information hiding and steganographic methods is available through IEEE's survey of information hiding.

QUESTION NO: 15

Adam works as a Senior Programmer for Umbrella Inc. A project has been assigned to him to write a short program to gather user input for a Web application. He wants to keep his program neat and simple. His chooses to use printf(str) where he should have ideally used printf("%s", str).

What attack will his program expose the Web application to?

A. Format string attack

B. Cross Site Scripting attack

C. SQL injection attack

D. Sequence++ attack

ANSWER: A

Explanation:

Format string attack is correct because `printf(str)` treats attacker-controlled input in `str` as the format-string argument rather than as ordinary text. The `printf` family parses format directives such as `%x`, `%p`, `%s`, and `%n`. If an attacker supplies these directives, the program can unintentionally disclose values from process memory, dereference unintended addresses, or, in conditions where writable targets can be reached, write values through the `%n` directive. This can lead to information disclosure, crashes, and potentially more serious memory-corruption consequences.

Using `printf("%s", str)` establishes a fixed, developer-controlled format string. In that form, the contents of `str` are passed as data for the `%s` conversion and are printed literally, so percent signs within user input are not interpreted as formatting commands. Secure coding guidance therefore requires that format strings be static or otherwise trusted, especially when outputting user-provided data. See the MITRE CWE-134: Use of Externally-Controlled Format String entry and the printf(3) manual page for the behavior of format directives.

QUESTION NO: 16

Which of the following steps can be taken as countermeasures against sniffer attacks?

Each correct answer represents a complete solution. Choose all that apply.

A. Use encrypted protocols for all communications.

B. Use switches instead of hubs since they switch communications, which means that information is delivered only to the predefined host.

C. Use tools such as StackGuard and Immunix System to avoid attacks.

D. Reduce the range of the network to avoid attacks into wireless networks.

ANSWER: A B D

Explanation:

Using encrypted protocols for all communications is a primary defense against packet sniffing because an interceptor may capture traffic but cannot readily read the protected contents without the required cryptographic keys. This should include encryption for web traffic, remote administration, email transport where applicable, and wireless authentication and data protection. CISA emphasizes that encryption protects the confidentiality of data, including data in transit: CISA—Understanding Encryption.

Using switches instead of hubs also reduces ordinary wired-network sniffing exposure. A hub repeats received frames to every connected port, whereas a switch learns MAC-address locations and normally forwards unicast frames only through the port associated with the intended destination. This limits passive observation opportunities and is strengthened operationally through switch security features such as port security and protections against address-table manipulation. Cisco documents port-security capabilities for restricting access to switch ports: Cisco—Configuring Port Security.

Reducing the range of a wireless network is also a useful countermeasure because it decreases the physical area from which an attacker can receive and capture radio transmissions. Appropriate access-point placement, transmit-power management, directional antennas where suitable, and limiting signal leakage beyond controlled areas reduce the opportunity for wireless packet collection.

QUESTION NO: 17

Which of the following tools can be used for steganography?

Each correct answer represents a complete solution. Choose all that apply.

A. Image hide

B. Stegbreak

C. Snow.exe

D. Anti-x

ANSWER: A C

Explanation:

Image hide and **Snow.exe** are tools used to conceal information through steganography. Image Hide is designed to embed a hidden payload within an image file, allowing the image to remain a plausible-looking carrier while containing data that can be recovered using the appropriate tool or credentials. This is a classic example of image-based steganography, where the carrier's visual content is altered in a way intended to be difficult for a casual observer to notice.

Snow.exe is the Windows executable form of SNOW, a well-known text steganography utility. SNOW hides messages in the trailing whitespace of text lines, and it can use compression and password-based encryption before embedding the payload. Because trailing spaces and tabs generally do not visibly change displayed text, the resulting carrier can appear ordinary unless it is inspected with whitespace-aware analysis tools. The SNOW project documentation describes its purpose as concealing messages in ASCII text using whitespace: SNOW: A White Space Steganography Program. More broadly, NIST defines steganography as concealing information within other data to avoid detection: NIST CSRC Glossary: Steganography.

QUESTION NO: 18

OutGuess is used for _____ attack.

A. Steganography

B. Web password cracking

C. SQL injection

D. Man-in-the-middle

ANSWER: A

Explanation:

OutGuess is used for steganography: the practice of concealing information within another, seemingly ordinary file. In particular, OutGuess is a steganographic tool designed to embed hidden data in JPEG image files while attempting to preserve statistical properties that could otherwise make the hidden content easier to detect. In a security-testing or incident-

handling context, understanding tools such as OutGuess matters because attackers may use steganography to conceal commands, malware payloads, configuration data, or exfiltrated information within benign-looking media. Conversely, defenders can use knowledge of these techniques when investigating suspicious image files, anomalous file transfers, or potential covert channels. The tool's historical documentation describes its purpose as universal steganographic extraction and notes its operation on JPEG images. For technical background, see the Kali Linux OutGuess tool page and the original OutGuess research paper, which discusses hiding and extracting data in JPEG images.

QUESTION NO: 19

Which of the following hacking tools provides shell access over ICMP?

A. John the Ripper

B. Nmap

C. Nessus

D. Loki

ANSWER: D

Explanation:

Loki provides shell access over ICMP by using ICMP messages as a covert command-and-control transport. Rather than relying on a conventional TCP or UDP service, a Loki client and server exchange command data and shell output within ICMP traffic, allowing an interactive remote shell where outbound ICMP is permitted. This behavior is an example of using a non-application-layer protocol for command and control, a technique defenders should recognize because ICMP is commonly allowed for diagnostic purposes and can blend with expected ping-related traffic. In incident handling, suspicious indicators can include unusually frequent ICMP packets, atypical payload sizes, payloads that do not resemble normal echo-request and echo-reply behavior, or ICMP communication with unexpected external systems. MITRE ATT&CK documents this type of command-and-control behavior under Non-Application Layer Protocol and specifically notes that ICMP may be used for C2 communications: MITRE ATT&CK: Non-Application Layer Protocol. Network monitoring and egress controls should therefore treat ICMP as a protocol requiring visibility and policy enforcement, not merely as harmless diagnostic traffic. Additional detection context is available from SANS Reading Room.

QUESTION NO: 20

Which of the following statements are true about tcp wrappers?

Each correct answer represents a complete solution. Choose all that apply.

A. tcp wrapper provides access control, host-address-spoofing checks, client username lookups, etc.

B. When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server program directly.

C. tcp wrapper allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens to filter for access control purposes.

D. tcp wrapper protects a Linux server from IP address spoofing.

ANSWER: A B C

Explanation:

tcp_wrappers is a host-based access-control mechanism historically used with network services launched by inetd and with applications linked against the libwrap library. When configured through inetd, inetd invokes the tcpd wrapper first; tcpd evaluates the connection against the access rules and then starts the requested server daemon when access is permitted. This creates a consistent control point before the protected service handles the client connection.

The wrapper's rules can use client host addresses, network or subnet specifications, host names, and daemon names. tcpd also supports optional username information obtained through the IDENT protocol, allowing ident replies to be considered in rules where that functionality is enabled. In addition, tcp_wrappers performs hostname and address verification: it compares name-service results with the peer address and can identify suspicious name/address mismatches associated with host-address spoofing attempts. These capabilities support the corrected statement describing host-address-spoofing checks, rather than implying that spoofing itself is a feature provided to users.

See the tcpd manual page and the hosts_access manual page for the tcpd invocation model, access tokens, and hostname/address verification behavior.

QUESTION NO: 21

Your IDS discovers that an intruder has gained access to your system. You immediately stop that access, change passwords for administrative accounts, and secure your network. You discover an odd account (not administrative) that has permission to remotely access the network. What is this most likely?

A. An example of privilege escalation.

B. A normal account you simply did not notice before. Large networks have a number of accounts; it is hard to track them all.

C. A backdoor the intruder created so that he can re-enter the network.

D. An example of IP spoofing.

ANSWER: C

Explanation:

A backdoor the intruder created so that he can re-enter the network is the most likely finding. Attackers commonly establish persistence after obtaining access, so they retain a path back into an environment if the initial access method is detected, blocked, or its credentials are changed. Creating or modifying a non-administrative account with remote-access permissions is a practical persistence mechanism: it can appear less conspicuous than use of a highly privileged account while still allowing the intruder to reconnect and continue reconnaissance, escalate privileges, or move laterally. During incident handling, the account should be treated as potentially malicious until its owner, business purpose, creation source, authentication activity, assigned groups, remote-logon rights, and related endpoint or directory logs have been validated. Containment should include disabling the account or removing its remote-access authorization in accordance with the organization's response procedures, preserving relevant evidence, and hunting for related persistence mechanisms or unauthorized account changes. MITRE ATT&CK identifies account creation as a persistence technique and notes that adversaries may create accounts to maintain access; see MITRE ATT&CK: Create Account. Guidance on containment, eradication, and recovery is also provided by NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

QUESTION NO: 22

Which of the following practices come in the category of denial of service attack?

Each correct answer represents a complete solution. Choose three.

A. Performing Back door attack on a system

B. Disrupting services to a specific computer

C. Sending thousands of malformed packets to a network for bandwidth consumption

D. Sending lots of ICMP packets to an IP address

ANSWER: B C D

Explanation:

Denial-of-service activity is intended to impair the availability of a host, network, or service for legitimate users. "Disrupting services to a specific computer" directly describes the availability impact that defines a denial-of-service attack. "Sending

thousands of malformed packets to a network for bandwidth consumption" is also a denial-of-service technique: high-volume traffic can exhaust network capacity, while malformed traffic may consume processing resources or trigger faults in vulnerable network stacks and services. "Sending lots of ICMP packets to an IP address" describes an ICMP flood (often called a ping flood), in which excessive ICMP Echo Request traffic consumes available bandwidth and/or target processing capacity. Whether the traffic originates from one system or many systems, the relevant outcome is resource exhaustion and degraded or unavailable service. These practices align with incident-handling guidance that treats unusually high traffic volumes, flooding, and resource exhaustion as availability attacks requiring detection, filtering, and mitigation. See the CISA denial-of-service attack overview and the IETF RFC 4732: Internet Denial-of-Service Considerations for technical context on flooding and resource-exhaustion attacks.

QUESTION NO: 23

Which of the following statements are true about a SYN flood attack?

Each correct answer represents a complete solution. Choose all that apply.

A. It attempts to exhaust resources allocated for incomplete TCP connections.

B. It may use spoofed source IP addresses.

C. SYN cookies can help mitigate the attack.

D. It requires the attacker to complete the TCP three-way handshake.

ANSWER: A B C

Explanation:

A SYN flood attempts to exhaust the resources used by a target to maintain incomplete TCP connection state. The attacker sends many TCP SYN packets, often using spoofed source addresses, and does not complete the TCP three-way handshake after the target replies with SYN/ACK packets. If enough half-open connections accumulate, legitimate clients may be unable to establish new connections.

SYN cookies are a recognized mitigation because they allow a server to avoid allocating normal connection state until it receives the final ACK from the client. Rate limiting, upstream filtering, increased backlog capacity, and DDoS protections may also reduce impact. A SYN flood does not require an attacker to authenticate successfully, and it is not an attack on application-layer session cookies. See RFC 4987, TCP SYN Flooding Attacks and Common Mitigations.

QUESTION NO: 24

When you conduct the XMAS scanning using Nmap, you find that most of the ports scanned do not give a response. What can be the state of these ports?

A. Filtered

B. Open

C. Closed

D. Open or filtered

ANSWER: D

Explanation:

The correct result is **Open or filtered**. An XMAS scan sends a TCP probe with the FIN, PSH, and URG flags set. Under the TCP behavior described in RFC 793, a closed port should respond to an unexpected probe with a TCP RST packet. In contrast, an open port commonly ignores this type of probe and sends no response. However, a firewall, packet filter, or other filtering device can also silently discard the probe, producing the same observable result: no response arrives at the scanner. Because Nmap cannot reliably distinguish an open port that ignored the packet from a filtered port whose response

was suppressed, it reports this result using the combined `open|filtered` state rather than asserting that the port is definitely open or definitely filtered. This distinction is important during reconnaissance and incident handling because it accurately communicates uncertainty and helps guide follow-up validation, such as a SYN scan, service detection, or testing from another network position. Nmap documents that FIN, NULL, and XMAS scans classify nonresponsive ports as `open|filtered`; see the Nmap Network Scanning reference on NULL, FIN, and XMAS scans and the Nmap port-state definitions.

QUESTION NO: 25

Which of the following are the limitations for the cross site request forgery (CSRF) attack?

Each correct answer represents a complete solution. Choose all that apply.

A. The attacker must determine the right values for all the form inputs.

B. The attacker must target a site that doesn't check the referrer header.

C. The target site should have limited lifetime authentication cookies.

D. The target site should authenticate in GET and POST parameters, not only cookies.

ANSWER: A B

Explanation:

CSRF relies on a victim's browser automatically attaching credentials, such as session cookies, to a request sent to an application where the victim is already authenticated. Therefore, *The attacker must determine the right values for all the form inputs.* is a practical limitation: the forged request must match the target endpoint's expected method, parameter names, and valid values. If the operation requires an unpredictable, session-bound anti-CSRF token or another value that an external site cannot read, the attacker cannot construct a valid request.

The attacker must target a site that doesn't check the referrer header. is also a limitation in the intended sense. Origin or Referer-header validation can allow an application to verify that a state-changing request originated from its own trusted site rather than an attacker-controlled origin. A reliable validation implementation can therefore reject cross-site forged requests. Modern guidance treats Origin validation and anti-CSRF tokens as complementary defenses, since header behavior can vary due to privacy controls and browser policies. OWASP recommends synchronizer or signed double-submit CSRF tokens for state-changing requests and describes Origin/Referer verification as defense in depth. See the OWASP CSRF overview and the OWASP CSRF Prevention Cheat Sheet.

QUESTION NO: 26

Fill in the blank with the appropriate term.

_____ is a free Unix subsystem that runs on top of Windows.

A. Cygwin

ANSWER: A

Explanation:

Cygwin is the appropriate term. It is a free, open-source environment that provides a substantial collection of GNU and Open Source tools for Windows, along with a POSIX-compatible runtime DLL. This combination enables many Unix and Linux-oriented command-line utilities, shell scripts, and tools to run on Windows with a familiar Unix-style interface. In the context of security operations and the SEC504 toolset, Cygwin can be useful when an analyst or responder needs Unix-like utilities and scripting capabilities on a Windows host, particularly where native Windows commands do not provide the desired workflow. The Cygwin Project describes the software as providing functionality similar to a Linux distribution on Windows

while running natively rather than requiring a separate virtual machine. Its runtime layer translates POSIX-oriented program expectations to underlying Windows functionality, which is why it is commonly characterized as a Unix subsystem or Unix-like environment running on top of Windows. See the official Cygwin Project site and its FAQ documentation for details about the environment, supported packages, and Windows integration.

QUESTION NO: 27

Which of the following can be used as a Trojan vector to infect an information system?

Each correct answer represents a complete solution. Choose all that apply.

A. NetBIOS remote installation

B. Any fake executable

C. Spywares and adware

D. ActiveX controls, VBScript, and Java scripts

ANSWER: A B C D

Explanation:

A Trojan is malware that masquerades as legitimate or desirable software, or that is delivered through a trusted-looking mechanism, to induce execution on a target system. NetBIOS remote installation can be a delivery vector when exposed Windows file-sharing and administrative services are used to copy or remotely launch a malicious program. A fake executable is a classic Trojan delivery method because it can appear to be a useful application, document-related utility, installer, or update while executing malicious code. Spyware and adware may also function as Trojan delivery mechanisms when bundled with seemingly legitimate software or used to install additional unwanted or malicious payloads. Browser-delivered active content—including ActiveX controls and scripts such as VBScript and JavaScript—can be used to persuade a user to run code, exploit vulnerable components, or retrieve a payload. These mechanisms all rely on execution, installation, or delivery paths that can place a Trojan on a host. CISA recommends treating unexpected software, attachments, downloads, and prompts as potential malware-delivery mechanisms and maintaining protections that limit unauthorized execution. See CISA: Understanding Malware and Its Threats and MITRE ATT&CK: SMB/Windows Admin Shares.

QUESTION NO: 28

Which of the following programming languages are NOT vulnerable to buffer overflow attacks?

Each correct answer represents a complete solution. Choose two.

A. C

B. Java

C. C++

D. Perl

ANSWER: B D

Explanation:

Java and Perl are the correct selections because their standard execution environments use managed memory rather than exposing ordinary application code to unrestricted direct memory access. Java arrays perform runtime bounds checking: an attempt to access an array index outside its valid range raises an exception instead of overwriting adjacent memory. Java also has automatic garbage collection and does not expose pointer arithmetic in normal Java code. The Java Language Specification defines array-access behavior and the resulting `ArrayIndexOutOfBoundsException` at the Java Language Specification.

Perl similarly manages string and scalar storage internally and does not provide the C-style, unchecked buffer manipulation model in ordinary Perl programs. Its runtime controls allocation and object/string representation, so application-level operations do not normally permit writing past an allocated buffer into adjacent process memory. This makes conventional stack- and heap-based buffer-overflow exploitation associated with unsafe native code inapplicable to typical Java and Perl source. Perl's memory-management model and its use of dynamically allocated scalar values are described in perlguts. This classification concerns the languages' standard managed-language semantics; native extensions, unsafe foreign-function interfaces, or vulnerabilities in an interpreter or virtual machine can still introduce native-memory risks.

QUESTION NO: 29

John works as a Network Security Professional. He is assigned a project to test the security of

www.we-are-secure.com. He establishes a connection to a target host running a Web service with netcat and sends a bad html request in order to retrieve information about the service on the host.

Which of the following attacks is John using?

A. Sniffing

B. Eavesdropping

C. War driving

D. Banner grabbing

ANSWER: D

Explanation:

Banner grabbing is correct because John is actively connecting to a web service with Netcat and sending a deliberately malformed HTTP/HTML request to provoke an error response. Web servers commonly include identifying details in response headers or generated error pages, such as the server software name, version, enabled modules, and sometimes operating-system-related information. Collecting this service-identification information is banner grabbing, an enumeration activity used during authorized security testing to understand the exposed technology stack and identify software that may require further review or patch verification.

For HTTP services, a response to a request can include headers such as `Server`, which may disclose the web server product and version. A malformed request can also produce a distinctive error page that reveals implementation details. Netcat is suitable for this type of manual interaction because it permits a tester to establish a raw TCP connection and send custom HTTP request text directly. The HTTP semantics and response-header structure are defined in RFC 9110: HTTP Semantics. For defensive guidance, OWASP recommends minimizing unnecessary server and framework information disclosure in its Error Handling Cheat Sheet.

QUESTION NO: 30

Which of the following functions can be used as a countermeasure to a Shell Injection attack?

Each correct answer represents a complete solution. Choose all that apply.

A. escapeshellarg()

B. mysql_real_escape_string()

C. regenerateid()

D. escapeshellcmd()

ANSWER: A D

Explanation:

`escapeshellarg()` is designed to safely encode one value that will be passed as a shell-command argument. It wraps the value as a single shell argument and escapes characters that could otherwise terminate that argument or gain shell syntax meaning. This is appropriate when an application must construct a command and user-controlled data is intended to occupy one argument position. PHP documents that the function adds single quotes around the argument and escapes embedded single quotes, preventing the supplied value from being interpreted as additional shell syntax.

`escapeshellcmd()` is intended to escape shell metacharacters in an entire command string before it is passed to a shell-executing function. It provides a defensive control against command separators, redirection operators, and related metacharacters being interpreted as shell control syntax. When command execution is unavoidable, it should be used according to its intended scope, while command names and permitted arguments should also be tightly controlled through application design and allowlisting. PHP's security guidance emphasizes treating external input carefully when executing programs. See the PHP references for escapeshellarg() and escapeshellcmd().

QUESTION NO: 31

Rick works as a Computer Forensic Investigator for BlueWells Inc. He has been informed that some confidential information is being leaked out by an employee of the company. Rick suspects that someone is sending the information through email. He checks the emails sent by some employees to other networks. Rick finds out that Sam, an employee of the Sales department, is continuously sending text files that contain special symbols, graphics, and signs. Rick suspects that Sam is using the Steganography technique to send data in a disguised form. Which of the following techniques is Sam using?

Each correct answer represents a part of the solution. Choose all that apply.

A. Linguistic steganography

B. Perceptual masking

C. Technical steganography

D. Text Semagrams

ANSWER: A D

Explanation:

Linguistic steganography and **Text Semagrams** correctly describe the suspected method. Linguistic steganography hides a message through the representation and arrangement of language-related material rather than by modifying the binary data of a digital carrier such as an image or audio file. It can use words, formatting, symbols, or other textual conventions to communicate information that is not apparent to an ordinary reader. A semagram conveys information through visual signs, objects, symbols, or graphical arrangements. In particular, text semagrams use symbols, signs, graphics, and other visible textual elements to encode or signal a concealed message. The scenario explicitly identifies text files containing special symbols, graphics, and signs, which is characteristic of text semagrams and places the technique within the broader linguistic-steganography category. During an investigation, this would justify preserving the original messages and reviewing character choices, symbol placement, ordering, whitespace, fonts, and repeated visual patterns, including comparison

across multiple emails to identify a consistent encoding scheme. NIST describes steganography as concealing information within another medium in its Computer Security Resource Center glossary; background on semagrams is available from Wikipedia's semagram overview.

QUESTION NO: 32

Which of the following languages are vulnerable to a buffer overflow attack?

Each correct answer represents a complete solution. Choose all that apply.

A. Java

B. C++

C. C

D. Action script

ANSWER: B C

Explanation:

C++ and **C** are vulnerable to buffer-overflow attacks because both languages permit direct memory manipulation and use constructs that do not inherently enforce array bounds at runtime. In C, developers commonly work with raw pointers, fixed-size buffers, and library functions whose safe use depends on correctly calculating and validating lengths. Writing beyond an allocated buffer can corrupt adjacent memory, alter program control flow, disclose data, or cause a crash. C++ retains these capabilities through raw arrays, pointers, manual memory management, and interoperability with C-style APIs. Although modern C++ offers safer abstractions such as `std::array`, `std::vector`, and bounds-checked access through `at()`, the language still allows code that accesses memory outside a buffer's valid bounds. Therefore, secure development and incident-handling practice must treat native C and C++ applications as potentially exposed to memory-corruption flaws when input validation, length handling, and memory-safe APIs are not used consistently. MITRE classifies classic buffer overflows under CWE-120 and identifies the failure to verify buffer size before copying input as the core condition. See MITRE CWE-120: Buffer Copy without Checking Size of Input and SEI CERT C Coding Standard.

QUESTION NO: 33

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server. The output of the scanning test is as follows:

C:\whisker.pl -h target_IP_address

-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - =

= Host: target_IP_address

= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1

mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22

+ 200 OK: HEAD /cgi-bin/printenv

John recognizes /cgi-bin/printenv vulnerability ('Printenv' vulnerability) in the We_are_secure server. Which of the following statements about 'Printenv' vulnerability are true?

Each correct answer represents a complete solution. Choose all that apply.

A. This vulnerability helps in a cross site scripting attack.

B. 'Printenv' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.

C. The countermeasure to 'printenv' vulnerability is to remove the CGI script.

D. With the help of 'printenv' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

ANSWER: A C D

Explanation:

The `/cgi-bin/printenv` program is a diagnostic CGI script that displays environment variables supplied to the CGI process. These variables can incorporate request-controlled values, including HTTP request headers and request metadata. If the script presents those values in an HTML response without context-appropriate output encoding, a tester may place HTML or script payloads in a crafted request or link and have that content reflected in the resulting page. This makes the exposed diagnostic endpoint useful in a cross-site scripting attack, particularly where an authenticated user can be induced to visit the crafted URL or where request headers are reflected by the script.

The appropriate remediation is to remove the CGI script when it is not strictly required. Diagnostic programs should not be exposed in production because they reveal implementation and configuration details, and legacy CGI output frequently lacks the output handling expected of modern web applications. If temporary diagnostic functionality is necessary, it should be access-restricted, protected by authentication, and ensure that every untrusted value is safely encoded before it is included in an HTML response. Apache's CGI documentation describes how request information is passed to CGI programs through environment variables, while OWASP explains the need for output encoding to prevent reflected script execution: Apache HTTP Server CGI tutorial and OWASP Cross-Site Scripting Prevention Cheat Sheet.

QUESTION NO: 34

Which of the following is designed to protect the Internet resolvers (clients) from forged DNS data created by DNS cache poisoning?

A. Stub resolver

B. BINDER

C. Split-horizon DNS

D. Domain Name System Extension (DNSSEC)

ANSWER: D

Explanation:

Domain Name System Extension (DNSSEC) is designed to let DNS resolvers authenticate DNS data and detect forged responses, including data injected through DNS cache-poisoning attacks. DNSSEC adds cryptographic signatures to DNS records. A validating resolver uses the DNS trust chain, beginning with a configured trust anchor and continuing through signed delegations, to verify that the received record set was signed by the authoritative zone and was not altered in transit. If signature validation fails, or if the answer cannot be securely validated where DNSSEC is expected, the resolver treats the data as bogus rather than caching and returning it as trustworthy information. This directly addresses the core cache-poisoning problem: an attacker may be able to send a response that appears to be from a legitimate source, but cannot produce a valid signature for the authoritative zone's records. DNSSEC also provides authenticated denial of existence through signed denial records, helping resolvers verify claims that a name or record does not exist. It does not encrypt DNS queries or responses; its relevant protection here is data-origin authentication and integrity validation. See the DNS Security Introduction and Requirements (RFC 4033) and the ICANN DNSSEC overview.

QUESTION NO: 35

You run the following PHP script:

$password = mysql_real_escape_string($_POST["password"]); ?>

What is the use of the mysql_real_escape_string() function in the above script.

Each correct answer represents a complete solution. Choose all that apply.

A. It can be used to mitigate a cross site scripting attack.

B. It can be used as a countermeasure against a SQL injection attack.

C. It escapes all special characters from strings $_POST["name"] and $_POST["password"] except ' and ".

D. It escapes the null byte, newline, carriage return, backslash, single quote, double quote, and control-Z character in these strings for the current MySQL connection.

ANSWER: B D

Explanation:

`mysql_real_escape_string()` was designed to escape data before it is interpolated into a MySQL query string. In this script, applying it to submitted name and password values helps prevent those values from terminating a quoted SQL literal or introducing SQL syntax. It is therefore a legacy countermeasure against SQL injection when used with the same active database connection and with correctly quoted SQL values. The function escapes the characters MySQL treats specially in string literals: the null byte, newline, carriage return, backslash, single quote, double quote, and the control-Z character. Its behavior is connection-aware because character-set handling matters when escaping data for MySQL.

For modern PHP applications, this function should not be used: the original MySQL extension, including `mysql_real_escape_string()`, was removed in PHP 7. Prepared statements with parameter binding are the preferred approach because query structure and user-supplied data remain separate. Nevertheless, for the legacy code shown, escaping the specified MySQL string-literal characters and using the function as a SQL-injection countermeasure accurately describe its purpose. See the PHP manual and the OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 36

The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook's preview pane. The Klez worm gathers email addresses from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?

A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

C. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"

D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

ANSWER: C

Explanation:

`HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"` is the relevant value because it records the path to the current user's Windows Address Book file. Klez used the Windows Address Book as a source of recipient addresses for its mass-mailing behavior. During incident analysis of an affected legacy Windows system, this value lets an examiner determine which WAB file the logged-on user was using and then inspect that address-book data in the context of Klez's address-harvesting activity. This is especially useful when reconstructing the worm's execution and propagation scope, because the WAB can contain the contacts from which Klez selected email targets. The value is user-specific, so the appropriate user hive must be examined rather than assuming a machine-wide address-book location. This behavior aligns with historical Klez analysis describing its collection of recipient addresses from Windows Address Book data. See CISA's historical Klez Worm alert and Microsoft's Windows Address Book documentation for background on the worm and the legacy WAB subsystem.

QUESTION NO: 37

John works as a Penetration Tester in a security service providing firm named you-are-secure Inc. Recently, John's company has got a project to test the security of a promotional Website www.missatlanta.com and assigned the pen-testing

work to John. When John is performing penetration testing, he inserts the following script in the search box at the company home page:

After pressing the search button, a pop-up box appears on his screen with the text - "Hi, John." Which of the following attacks can be performed on the Web site tested by john while considering the above scenario?

A. Replay attack

B. CSRF attack

C. Buffer overflow attack

D. XSS attack

ANSWER: D

Explanation:

XSS attack is correct because the application accepted user-supplied HTML/JavaScript from the search field and caused the browser to execute it. The `<script>alert('Hi, John')</script>` payload producing an alert demonstrates that untrusted input was included in a response without effective context-appropriate output encoding or sanitization. In this search-result scenario, the behavior is most consistent with reflected cross-site scripting: the submitted value is returned in the page and immediately interpreted by the client browser as active script.

Successful script execution in the application's origin is significant because a real attacker could substitute the harmless alert with JavaScript that interacts with page content, makes requests as the current user where browser protections permit, or attempts to obtain sensitive data exposed to scripts. The finding should be documented with the affected parameter, request, response context, proof of execution, and remediation advice. Effective remediation includes applying output encoding appropriate to the HTML, attribute, JavaScript, URL, or CSS context; avoiding unsafe DOM insertion APIs; and using a restrictive Content Security Policy as defense in depth. OWASP describes XSS and its prevention approaches in its Cross Site Scripting guidance and XSS Prevention Cheat Sheet.

QUESTION NO: 38 - (SIMULATION)

Fill in the blank with the appropriate term.

_____ is a free Unix subsystem that runs on top of Windows.

ANSWER: See the explanation for the answer

Explanation:

Answer: `Cygwin`

Cygwin is a free Unix-like environment/subsystem for Windows, providing Unix tools and a POSIX compatibility layer on top of the Windows operating system.