PassQueen
a.k.a dumpsqueen.com

EC-Council Certified Security Specialist (ECSS) v10

ECCouncil ECSS

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, Information Security Fundamentals	152
Topic 2, Network Security Fundamentals	161
Topic 3, Computer Forensics Fundamentals	66
Topic 4, Mix Questions	1
Total	380

QUESTION NO: 1

Bob, a professional hacker, targeted an organization to launch attacks. Bob gathered information such as network topology and a list of live hosts. Based on the collected information, he launched further attacks over the organization's network.

Identify the type of network attack Bob initiated on the target organization in the above scenario.

A. Session hijacking

B. Buffer overflow

C. Data modification

D. Enumeration

ANSWER: D

Explanation:

Enumeration is correct because the activity described consists of actively identifying and cataloging accessible systems and network characteristics before conducting additional attacks. Building a list of live hosts reveals which IP addresses are currently responding and therefore represent potential targets. Collecting network-topology information further helps an attacker understand how systems are arranged, which segments may be reachable, and where to direct later reconnaissance or exploitation efforts. This is a core early-stage attacker activity: information gathered through host discovery and network-service discovery is used to refine the attack surface and select targets and techniques for subsequent operations. MITRE ATT&CK documents these closely related discovery behaviors as Remote System Discovery and Network Service Discovery. In penetration-testing methodology, discovery and enumeration are likewise used to identify live systems and collect technical details that enable later testing; NIST describes information gathering and discovery as important components of technical security assessment planning and execution in NIST SP 800-115. Thus, the attacker's collection of live-host and topology data is network enumeration.

QUESTION NO: 2

Which of the following networks relies on the tunneling protocol?

A. Wide Area Network (WAN)

B. Virtual Private Network (VPN)

C. Local Area Network (LAN)

D. Wireless Network

ANSWER: B

Explanation:

Virtual Private Network (VPN) is correct because a VPN creates a protected logical connection, commonly called a tunnel, across an untrusted or public network such as the internet. Tunneling encapsulates traffic from one protocol inside packets used by another protocol, allowing private network communications to traverse intermediary networks while remaining logically separated from other traffic. In typical remote-access and site-to-site VPN deployments, the tunnel is also protected with cryptographic controls that provide confidentiality, integrity, and peer authentication. For example, IPsec-based VPNs use encapsulation and security associations to protect IP traffic, while TLS-based VPNs establish encrypted remote-access connections through TLS. The term "virtual" reflects that endpoints communicate as though they were connected through a private network even though the underlying transport may be a shared public WAN. This tunneling capability is a defining VPN characteristic and supports secure access to internal resources for remote users and connections between geographically separated sites. The National Institute of Standards and Technology describes IPsec as a suite for protecting IP communications, including VPN use cases: NIST SP 800-77 Rev. 1. A practical overview of VPN tunneling and protocols is available from the Internet Engineering Task Force's IPsec architecture specification: RFC 4301.

QUESTION NO: 3

Andrew works as a Forensic Investigator for Passguide Inc. The company has a Windowsbased environment. The company's employees use Microsoft Outlook Express as their email client program. E-mails of some employees have been deleted due to a virus attack on the network.

Andrew is therefore assigned the task to recover the deleted mails. Which of the following tools can Andrew use to accomplish the task?

Each correct answer represents a complete solution. Choose two.

A. FINALeMAIL

B. eMailTrackerPro

C. EventCombMT

D. R-mail

ANSWER: A D

Explanation:

FINALeMAIL and **R-mail** are appropriate tools for recovering deleted Outlook Express email. Outlook Express stores mail folders in DBX mailbox files. When messages are deleted, their contents may remain recoverable within the mailbox database or from the underlying storage until they are overwritten; a virus incident can therefore require specialized mail-recovery utilities rather than simply opening the email client.

FINALeMAIL is designed to locate, repair, and recover email from damaged or deleted email-store files, including Outlook Express mail. This makes it suitable where the virus has deleted or damaged the user's mail data. Its recovery workflow can extract messages from the affected store and save recovered mail in accessible formats. The product's supported recovery capabilities are described by FINALeMAIL.

R-mail is also designed for email recovery and supports recovery of deleted messages from Outlook Express mailbox files. It can scan the relevant mail-store data and restore recoverable messages, making it a complete solution for the stated forensic recovery task. R-TT's documentation for R-Mail for Outlook Express describes its Outlook Express recovery use case. Before recovery, an investigator should preserve forensic copies of the affected DBX files and work from those copies to avoid altering evidence.

QUESTION NO: 4

John, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled.

Which of the following attacks is John performing?

A. Replay attack

B. DoS attack

C. ARP spoofing

D. Rainbow attack

ANSWER: B

Explanation:

DoS attack is correct because the described activity deliberately exhausts the router's available resources by creating a large number of simultaneous open connections. Network devices must maintain state and allocate processing capacity, memory, and connection-table entries for active sessions. When those finite resources are consumed, the router can no longer reliably process or forward legitimate traffic. Consequently, hosts whose connectivity depends on that router are denied access to network services, which is the defining objective of a denial-of-service attack.

The scenario describes a single malicious actor generating the resource-consuming traffic, so it is specifically a denial-of-service condition rather than requiring the distributed component associated with a DDoS attack. Flooding connection capacity is a common availability attack pattern and is often associated with TCP connection or SYN-flood-style exhaustion, depending on the exact packets and state involved. The essential security impact is loss of availability for legitimate users and systems behind the affected router. NIST defines denial of service as preventing or impairing authorized access to systems or network resources; see NIST's Denial of Service glossary entry. Further technical context on TCP SYN flood resource exhaustion is available from Cloudflare's SYN flood overview.

QUESTION NO: 5

Which of the following two cryptography methods are used by NTFS Encrypting File

System (EFS) to encrypt the data stored on a disk on a file-by-file basis?

A. Twofish

B. Digital certificates

C. Public key

D. RSA

ANSWER: B C

Explanation:

NTFS Encrypting File System uses public-key cryptography together with a user's digital certificate to protect encrypted files on a per-file basis. When EFS encrypts a file, it first creates a unique, randomly generated File Encryption Key (FEK) and uses that key for the actual bulk encryption of the file data. EFS then protects the FEK using the public key associated with the authorized user's EFS certificate. The resulting encrypted FEK is stored with the encrypted file, allowing only an account holding the corresponding private key to recover the FEK and decrypt the file.

Digital certificates are therefore integral to EFS operation because they bind the user's identity to the public key used to protect the FEK and provide the associated private key material needed for decryption. Public key cryptography provides the asymmetric protection and key-distribution mechanism that lets EFS securely share access with designated recovery agents or additional authorized users without exposing the underlying file-encryption key. Microsoft's EFS overview and key-management documentation describe this certificate- and public-key-based design: Microsoft EFS documentation and EFS overview.

QUESTION NO: 6

You are using the dsniff tool to intercept communications between two entities and establish credentials with both sides of the connections. These entities do not notice that you were retrieving the information between these two. Which of the following attacks are you performing?

A. Session hijacking

B. DoS

C. ARP poisoning

D. Man-in-the-middle

ANSWER: D

Explanation:

Man-in-the-middle is correct because the described activity places the attacker transparently between two communicating entities, allowing the attacker to intercept traffic while maintaining a separate, apparently legitimate connection with each endpoint. Each party believes it is communicating directly with the other, while the intermediary can observe and potentially alter the exchanged data. This is the defining characteristic of a man-in-the-middle attack.

The dsniff suite includes tools used for network-traffic inspection and credential collection, such as password sniffing utilities. In a switched Ethernet environment, an attacker may first arrange for traffic to traverse the attacker's machine, then capture credentials or other unprotected information during the relayed communication. The key detail in the question is not merely packet capture, but the covert establishment of communications with both sides, which describes the intermediary position central to a man-in-the-middle attack. EC-Council's coverage of network attacks identifies man-in-the-middle attacks as interception attacks in which an adversary sits between communicating parties. See EC-Council's overview of man-in-the-middle attacks and Kali Linux documentation for dsniff.

QUESTION NO: 7

Which of the following algorithms is used by the Advanced Encryption Standard (AES)?

A. Rijndael

B. 3 DES

C. Twofish

D. Blowfish

ANSWER: A

Explanation:

AES is based on the Rijndael cipher, designed by Joan Daemen and Vincent Rijmen. Following a public evaluation and selection process, the U.S. National Institute of Standards and Technology selected Rijndael as the algorithm for the Advanced Encryption Standard in 2000. AES specifies a symmetric-key block cipher that processes 128-bit data blocks and supports key sizes of 128, 192, and 256 bits. Rijndael was designed with variable block and key sizes, while the AES standard adopts the Rijndael design with a fixed 128-bit block size and the three standardized key lengths. In practical security implementations, AES performs a series of substitution, permutation, and key-dependent transformation rounds to provide confidentiality for data. The formal AES specification is published in NIST Federal Information Processing Standard 197, which identifies the algorithm as Rijndael and defines its approved parameters. See NIST FIPS 197: Advanced Encryption Standard and NIST's AES development archive.

QUESTION NO: 8

Which of the following technologies is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet?

A. Demilitarized zone (DMZ)

B. Intrusion detection system (IDS)

C. Firewall

D. Packet filtering

ANSWER: B

Explanation:

Intrusion detection system (IDS) is correct because its purpose is to monitor hosts and/or network traffic for indicators of unauthorized access, misuse, malicious activity, or policy violations. An IDS analyzes events such as login attempts, system and application logs, file changes, protocol activity, and network packets. It can operate as a host-based IDS, which observes activity on an individual endpoint, or as a network-based IDS, which monitors traffic moving across network segments. This enables detection of suspicious attempts originating locally as well as attempts received through the Internet or an organizational intranet.

IDS technology typically identifies activity through signature-based detection, which recognizes known attack patterns, and anomaly-based detection, which identifies deviations from an established baseline of normal behavior. When suspicious

activity is detected, the system generates alerts for security personnel or forwards event data to centralized monitoring tools for investigation and response. This detection and alerting capability is a core part of defense in depth and supports timely incident handling. NIST describes intrusion detection as the process of monitoring events in information systems and networks and analyzing them for signs of possible incidents. See NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems and CISA Cyber Threats and Advisories.

QUESTION NO: 9

An attacker wants to launch an attack on a wired Ethernet. He wants to accomplish the following tasks:

· Sniff data frames on a local area network.

· Modify the network traffic.

· Stop the network traffic frequently.

Which of the following techniques will the attacker use to accomplish the task?

A. ARP spoofing

B. IP spoofing

C. Eavesdropping

D. Session hijacking

ANSWER: A

Explanation:

ARP spoofing is correct because it can place an attacker in the traffic path between devices on the same Ethernet LAN. ARP maps an IPv4 address to a link-layer MAC address, allowing a host to deliver an Ethernet frame to its intended local destination. An attacker can send forged ARP replies that associate the attacker's MAC address with the IP address of a gateway, victim, or both. Systems that accept those forged mappings then transmit traffic to the attacker rather than directly to the legitimate peer.

Once positioned as a man-in-the-middle, the attacker can capture frames forwarded through that device, selectively alter packets before relaying them, or discard packets instead of forwarding them. Dropping forwarded traffic produces repeated disruption or denial of service, while forwarding it preserves the attacker's ability to observe and manipulate communications. This directly satisfies all three stated goals: local traffic sniffing, traffic modification, and frequent interruption of traffic flow.

The underlying ARP behavior is defined in RFC 826. A practical defensive control is Dynamic ARP Inspection, which validates ARP packets and is described in Cisco's Dynamic ARP Inspection documentation.

QUESTION NO: 10

Which of the following statements are true about session hijacking?

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

A. TCP session hijacking is when a hacker takes over a TCP session between two machines.

B. It is used to slow the working of victim's network resources.

C. Use of a long random number or string as the session key reduces session hijacking.

D. It is the exploitation of a valid computer session to gain unauthorized access to informationor services in a computer system.

ANSWER: A C D

Explanation:

TCP session hijacking is when an attacker assumes control of an established TCP communication session between two systems. This can involve predicting or desynchronizing TCP sequence numbers, injecting packets into the session, or otherwise impersonating one endpoint after the connection has been established. At the web-application level, session hijacking similarly occurs when an attacker obtains or successfully guesses a valid session identifier and reuses it to act as the authenticated user. As a result, it is accurately described as exploiting a valid computer session to obtain unauthorized access to information or services.

Using a long, unpredictable, cryptographically strong random value as the session key substantially reduces the chance that an attacker can guess a valid active session identifier. Secure session management also requires protecting the identifier in transit and at rest in the browser, commonly through HTTPS plus Secure and HttpOnly cookie attributes, and renewing identifiers at appropriate authentication or privilege-change events. OWASP recommends that session identifiers be meaningless, unique, and generated with sufficient entropy to resist brute-force prediction. See the OWASP Session Management Cheat Sheet and OWASP's session hijacking overview.

QUESTION NO: 11

Which of the following measures help prevent SQL injection attacks in Web applications?

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

A. Use parameterized queries or prepared statements.

B. Validate input on the server using allow lists.

C. Use a database account with minimum required privileges.

D. Concatenate all user input directly into SQL statements.

E. Rely only on client-side input validation.

ANSWER: A B C

Explanation:

Parameterized queries, also called prepared statements, are a primary defense against SQL injection because they keep user-supplied values separate from the SQL command structure. The database interprets supplied input as data rather than executable query syntax. Server-side allow-list input validation is also useful because it restricts accepted input to expected formats, types, lengths, and values.

Using a database account with only the permissions required by the application limits the impact if an injection flaw is discovered. Error messages should not disclose detailed database information to users because such details can assist an attacker in refining malicious input. Client-side validation alone is insufficient because an attacker can bypass browser controls and submit modified requests directly. OWASP provides detailed prevention guidance in its SQL Injection Prevention Cheat Sheet.

QUESTION NO: 12

Which of the following Linux rootkits allows attackers to hide files, processes, and network connections?

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

A. Phalanx2

B. Adore

C. Knark

D. Beastkit

ANSWER: B C

Explanation:

Adore and Knark are Linux kernel rootkits associated with stealth capabilities that conceal multiple types of operating-system artifacts. Their kernel-level operation enables the rootkit to intercept or alter the results returned through system interfaces used to enumerate directory entries, running tasks, and active network sockets. As a result, a local administrator or monitoring utility may receive a filtered view that omits attacker-selected files, processes, and connections, even though those artifacts remain active on the host.

This is a significant incident-response concern because ordinary inspection commands often depend on kernel-provided process, filesystem, and networking information. A rootkit that controls those views can make persistence mechanisms, command shells, packet listeners, and malicious executables difficult to discover through routine host checks. MITRE ATT&CK identifies rootkits as a mechanism for hiding artifacts and modifying system behavior: Rootkit (T1014). Linux kernel security documentation also explains the kernel-level security architecture in which loadable components and security controls operate: Linux Security Module documentation. Therefore, Adore and Knark meet all three stated concealment requirements.

QUESTION NO: 13

Which of the following software can be used to protect a computer system from external threats (viruses, worms, malware, or Trojans) and malicious attacks?

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

A. Employee monitoring software

B. Burp Suite

C. Antivirus

D. Firewall

ANSWER: C D

Explanation:

Antivirus and **Firewall** are complementary endpoint-security controls that help protect systems against malware and malicious external activity. Antivirus software detects, blocks, quarantines, and removes malicious code such as viruses, worms, Trojans, and other malware. Modern antivirus products commonly use a combination of signature-based detection, heuristic analysis, and behavior monitoring, so protection can extend beyond known malware samples. Microsoft describes how antivirus protection helps detect and remediate threats through its Microsoft Defender Antivirus documentation.

A firewall provides a network boundary control by applying rules to inbound and outbound traffic. It can block unsolicited connection attempts, restrict access to unnecessary ports and services, and limit communications to approved networks or applications. This reduces the attack surface exposed to external attackers and can prevent or contain malicious network activity. The U.S. Cybersecurity and Infrastructure Security Agency explains the protective role of firewalls in its Understanding Firewalls guidance. Used together, antivirus addresses malicious files and endpoint behavior, while a firewall controls potentially hostile network traffic, making both part of a defense-in-depth solution.

QUESTION NO: 14

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows

Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest domain-based network. The company has recently provided fifty laptops to its sales team members. You are required to configure an 802.11 wireless network for the laptops. The sales team members must be able to use their data placed at a server in a cabled network. The planned network should be able to handle the threat of unauthorized access and data interception by an unauthorized user. You are also required to prevent the sales team members from communicating directly to one another. Which of the following actions will you perform to accomplish the task?

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

A. Implement the open system authentication for the wireless network.

B. Implement the IEEE 802.1X authentication for the wireless network.

C. Configure the wireless network to use WEP encryption for the data transmitted over a wireless network.

D. Using group policies, configure the network to allow the wireless computers to connect to the infrastructure networks only.

E. Using group policies, configure the network to allow the wireless computers to connect to the ad hoc networks only.

F. Configure the wireless network to use WPA2-Enterprise encryption with IEEE 802.1X authentication.

ANSWER: B D F

Explanation:

Implementing the IEEE 802.1X authentication for the wireless network provides port-based access control and supports centrally managed, identity-based authentication through an authentication server such as NPS/RADIUS integrated with Active Directory. This ensures that only authorized sales users and managed devices can join the protected WLAN. WPA2-Enterprise must be used with 802.1X because it supplies modern wireless encryption and per-session cryptographic keys, protecting wireless traffic against interception while users access resources on the wired server network. Microsoft documents the use of 802.1X with WPA2-Enterprise for authenticated, protected wireless access in its WPA2-Enterprise and RADIUS guidance. Configuring wireless computers through Group Policy to connect only to infrastructure networks prevents users from forming ad hoc, peer-to-peer wireless connections directly with one another. Infrastructure mode directs wireless clients through the access point, where authentication, encryption, and network access controls can be enforced. This design also allows the organization to centrally deploy the required wireless profile and prohibit less controlled network types. The Wi-Fi Alliance identifies WPA2-Enterprise as an enterprise security approach based on 802.1X authentication in its wireless security overview.

QUESTION NO: 15

An Anti-Virus software is used to prevent, detect, and remove malware from a system, including computer viruses, worms, and Trojan horses. Which of the following companies are the providers of Anti-virus softwares?

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

A. Symantec Corporation

B. F-Secure Corporation

C. AVG Technologies

D. Kaspersky Lab

E. McAfee Inc.

ANSWER: A B C D E

Explanation:

All listed organizations have provided antivirus or endpoint-security products designed to detect, prevent, quarantine, and remediate malicious software. Symantec Corporation is widely associated with the Norton antivirus product line and enterprise endpoint protection. F-Secure Corporation provides consumer and business security products that include malware and virus protection. AVG Technologies developed AVG AntiVirus, a well-known endpoint antivirus product. Kaspersky Lab provides endpoint-security products with antivirus, anti-malware, behavioral detection, and threat-remediation capabilities. McAfee Inc. has long supplied consumer and enterprise antivirus and endpoint-protection software.

The names in the question reflect companies and brands commonly used in security training materials; corporate ownership, product branding, and organizational structures can change over time, but each named organization has been an antivirus-software provider. Antivirus remains a foundational endpoint control because it uses signatures, heuristics, behavioral analysis, and cloud-assisted threat intelligence to identify malware and support its removal or containment. For general

guidance on selecting and using anti-malware protections, see the CISA Secure Our World guidance and the NIST Guide to Malware Incident Prevention and Handling.

QUESTION NO: 16

Which two security components should you implement on the sales personnel portable computers to increase security?

(Click the Exhibit button on the toolbar to see the case study.)

Each correct answer represents a complete solution. Choose two.

A. Encrypting File System (EFS)

B. L2TP over IPSec

C. PPTP

D. Remote access policy

E. Remote Authentication Dial-In User Service (RADIUS)

ANSWER: A B

Explanation:

Encrypting File System (EFS) protects sensitive files stored locally on a salesperson's portable computer. This is particularly valuable for mobile systems because laptops can be lost or stolen outside the organization's physical security perimeter. EFS encrypts files at the NTFS file-system level and associates decryption with the authorized user's credentials, helping ensure that offline data remains protected from unauthorized access. Microsoft describes EFS as a file-encryption technology for protecting confidential data stored on NTFS volumes: Microsoft File Encryption documentation.

L2TP over IPSec provides a protected VPN connection when sales personnel use remote or untrusted networks. L2TP supplies the tunneling mechanism, while IPSec provides authentication, integrity protection, and encryption for the traffic carried through the tunnel. This combination protects business communications between the portable computer and corporate resources from interception or tampering during transit. Microsoft's VPN protocol guidance identifies L2TP/IPsec as a VPN protocol that uses IPsec security mechanisms: Microsoft VPN deployment documentation. Together, local file encryption and encrypted remote connectivity address the principal data-at-rest and data-in-transit risks associated with mobile sales devices.

QUESTION NO: 17

Net Spy Pro is the latest network monitoring software. This program helps a user to know what the others are doing on their computers. What are the features of this program?

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

A. PC administration

B. Remote control

C. Activity filtering

D. Activity monitoring

ANSWER: A B C D

Explanation:

Net Spy Pro combines observation and management functions for computers on a monitored network. **PC administration** is a core capability because an administrator can perform routine management actions on connected client systems from a central console. **Remote control** is also a feature: it permits the administrator to view and interact with a remote user's

desktop when assistance, supervision, or an operational intervention is necessary. **Activity filtering** supports policy enforcement by allowing the administrator to control or limit monitored user activity according to configured rules. Finally, **Activity monitoring** is fundamental to the product's purpose, enabling the collection and review of user-computer activity across the network. Together, these functions provide both visibility into endpoint use and the ability to administer endpoints remotely, which is consistent with the stated objective of learning what users are doing on their computers. Historical product documentation for Net Spy Pro identifies monitoring, filtering, remote-control, and administration capabilities; see the archived Net Spy Pro product site. More generally, centralized endpoint monitoring and remote administration are established security-management practices described in NIST SP 800-53 Rev. 5.

QUESTION NO: 18

Which of the following statements are TRUE about Demilitarized zone (DMZ)?

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

A. The purpose of a DMZ is to add an additional layer of security to the Local Area Network

of an organization.

B. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet.

C. Hosts in the DMZ have full connectivity to specific hosts in the internal network.

D. Demilitarized zone is a physical or logical sub-network that contains and exposes external services of an organization to a larger un-trusted network.

ANSWER: A B D

Explanation:

A DMZ provides a separated network segment that adds a protective layer between an organization's trusted local network and an untrusted network such as the Internet. It is used to place systems that must accept externally initiated connections—such as public web, email, DNS, or proxy services—outside the internal LAN while still allowing security controls to govern traffic. This separation helps limit the exposure of internal assets if an internet-facing service is compromised.

In a typical DMZ design, the organization's LAN systems remain behind firewall controls rather than being directly exposed to the public network. Firewalls or equivalent filtering devices enforce distinct rules for Internet-to-DMZ, DMZ-to-internal-network, and internal-network-to-DMZ traffic. This architecture supports controlled publication of external services without placing the broader LAN at the same level of risk. The definition of a DMZ as a physical or logical subnetwork that exposes selected organizational services to a larger untrusted network accurately describes its core security role. See CISA's firewall guidance and Cloudflare's DMZ overview.

QUESTION NO: 19

A chkrootkit is a toolkit that checks whether a rootkit is installed in the Linux operating system or not. Which of the following tools are contained in chkrootkit?

A. chkproc.c

B. chklastlog.c

C. chkdsk

D. ifpromisc.c

E. chkwtmp.c

ANSWER: A B D E

Explanation:

`chkproc.c`, `chklastlog.c`, `ifpromisc.c`, and `chkwtmp.c` are source components supplied with chkrootkit. The toolkit uses several small utilities to inspect different system areas that can reveal indicators of compromise. `chkproc.c` examines process-related information for signs of hidden processes or suspicious behavior. `chklastlog.c` checks the lastlog database, while `chkwtmp.c` examines wtmp login-accounting data; these checks help identify possible tampering with records of user sessions and logins. `ifpromisc.c` checks network interfaces for promiscuous-mode operation, which can be relevant when detecting packet sniffers. These programs are compiled or invoked as part of chkrootkit's collection of host-based checks rather than being standalone disk-management utilities. The chkrootkit manual describes its purpose as locally checking a system for signs of known rootkits, and its distributed source tree includes these named components. See the chkrootkit manual page and the chkrootkit source repository for the toolkit's checks and source files.

QUESTION NO: 20

John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He is working on the Linux operating system and wants to install an Intrusion Detection System on the We-are-secure server so that he can receive alerts about any hacking attempts. Which of the following tools can John use to accomplish the task?

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

A. Samhain

B. Tripwire

C. Snort

D. SARA

ANSWER: A B C

Explanation:

Samhain, Tripwire, and Snort can each be used as part of an intrusion-detection solution on a Linux system. Samhain is a host-based intrusion detection system that performs file-integrity checking, detects unauthorized changes to important files and directories, and can generate alerts or reports when monitored system state changes. Tripwire likewise provides host-based file-integrity monitoring: it establishes a trusted baseline for files and compares subsequent filesystem state against that baseline, helping administrators identify possible tampering after an attack attempt. These tools are particularly useful for detecting unauthorized modification of operating-system files, application binaries, configurations, and logs on the protected server.

Snort provides network intrusion detection capabilities. It inspects network traffic using rules and signatures and can alert when traffic patterns indicate suspicious activity, exploit attempts, scanning, policy violations, or other known attack behavior. Deploying Snort alongside host-based monitoring gives the administrator visibility into both traffic reaching or leaving the server and changes occurring on the server itself. This aligns with the layered use of network-based and host-based IDS technologies described in NIST guidance. See NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems and the Snort overview.

QUESTION NO: 21

Which of the following types of firewall examines the state of active network connections before allowing or denying traffic?

A. Packet-filtering firewall

B. Stateful inspection firewall

C. Proxy auto-configuration firewall

D. Static routing firewall

ANSWER: B

Explanation:

A **stateful inspection firewall** is correct because it maintains information about established connections in a state table. When a packet arrives, the firewall can evaluate not only source and destination addresses, ports, and protocol, but also whether the packet belongs to a legitimate existing session. This allows return traffic for approved connections to be handled appropriately while unsolicited or invalid traffic can be blocked.

A packet-filtering firewall generally evaluates packets independently against configured rules and does not maintain the same connection-state awareness. NIST discusses stateful inspection firewall capabilities in SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy.

QUESTION NO: 22

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

Which of the following tools is John using to crack the wireless encryption keys?

A. AirSnort

B. Kismet

C. PsPasswd

D. Cain

ANSWER: A

Explanation:

AirSnort is the correct tool because it was specifically designed to recover Wired Equivalent Privacy (WEP) encryption keys from captured wireless traffic. It operates passively by monitoring 802.11 packets and collecting initialization vectors (IVs) associated with WEP-encrypted frames. Once it has captured a sufficient number of packets containing vulnerable or weak IV patterns, AirSnort applies known statistical weaknesses in the WEP RC4 key-scheduling process to derive the shared WEP key. This purpose directly matches a description or interface indicating wireless packet capture, IV collection, and WEP key recovery.

WEP is no longer considered secure because its short IV and RC4 implementation permit IV reuse and enable practical key-recovery attacks when enough traffic is available. AirSnort is a historically important example of a WEP-cracking utility and is therefore the expected identification in a security-training question focused on wireless encryption key cracking. The AirSnort project describes it as a wireless LAN WEP encryption-cracking tool at AirSnort on SourceForge. For background on the IEEE 802.11 security weaknesses that led to WEP replacement, see NIST SP 800-97.

QUESTION NO: 23

Which of the following is a name, symbol, or slogan with which a product is identified?

A. Copyright

B. Trademark

C. Trade secret

D. Patent

ANSWER: B

Explanation:

Trademark is correct because a trademark is an intellectual-property identifier used to distinguish the source of goods or services in the marketplace. It can consist of a word, name, phrase, symbol, design, logo, slogan, or a combination of these elements. A product name and its associated logo, for example, allow consumers to recognize that products originate from a particular company and differentiate them from competing products. Trademark protection therefore focuses on brand identity and the consumer association between a mark and its source, rather than protecting the underlying technical invention or the expressive content of a work. In security and business contexts, trademarks are important assets because unauthorized use of a protected brand can enable impersonation, fraud, counterfeit sales, and reputational damage. The United States Patent and Trademark Office describes a trademark as protecting words, phrases, symbols, and designs that identify the source of goods; it also notes that service marks identify the source of services. The World Intellectual Property Organization similarly explains that trademarks distinguish one enterprise's goods or services from those of other enterprises. See the USPTO trademark overview and WIPO trademark resources.

QUESTION NO: 24

Which of the following is a network worm that exploits the RPC sub-system vulnerability present in the Microsoft Windows operating system?

A. WMA/TrojanDownloader.GetCodec

B. Win32/PSW.OnLineGames

C. Win32/Agent

D. Win32/Conflicker

ANSWER: D

Explanation:

Win32/Conflicker is intended to refer to the Conficker worm, also known as Downadup. Conficker is a self-propagating Windows network worm that exploited the Microsoft Windows Server service vulnerability addressed by security bulletin MS08-067. This flaw is a remote-code-execution issue involving the handling of RPC requests: an unauthenticated attacker could send a specially crafted RPC request to a vulnerable system and execute code remotely. Once a host was compromised, Conficker could scan for other reachable Windows machines and use the same vulnerability to spread across networks, making it a prominent example of a worm using an RPC-related Windows vulnerability. Microsoft's MS08-067 bulletin documents the affected Server service and describes the vulnerability as one that could permit remote code execution through specially crafted RPC requests. Microsoft also published detailed guidance on the Conficker threat and its network propagation behavior. See Microsoft Security Bulletin MS08-067 and Microsoft's Conficker worm guidance.

QUESTION NO: 25

You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack. Which of the following logs will you review to accomplish the task?

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

A. Web server logs

B. Event logs

C. Program logs

D. System logs

ANSWER: B C D

Explanation:

Event logs, Program logs, and System logs are appropriate evidence sources because they collectively record the operating-system and application activity that commonly accompanies exploitation attempts and their effects. Event logs can preserve

security, application, and system events, including process failures, service errors, access activity, auditing records, and exception-related entries. These records help an investigator establish a timeline and correlate suspicious activity with the affected host. Microsoft describes Windows Event Log as the service that manages event logs and supports the recording of system, security, and application events: Windows Event Log.

Program logs are particularly valuable for identifying application crashes, unhandled exceptions, abnormal requests, diagnostic messages, and application-specific authentication or session activity. Such records can show whether a vulnerable process behaved unexpectedly during a suspected buffer-overflow incident. System logs provide complementary host-level evidence, such as service starts and stops, kernel or driver messages, resource failures, and system stability events. Reviewing and correlating these sources supports reliable incident reconstruction, preserves context around the suspected attack time, and helps identify affected processes and accounts. NIST's incident-handling guidance emphasizes collecting and analyzing relevant logs and other evidence during investigation: NIST SP 800-61 Rev. 2.

QUESTION NO: 26

Sarah was accessing confidential office files from a remote location via her personal computer connected to the public Internet. Accidentally, a malicious file was downloaded onto Sarahâ€™s computer without her knowledge. This download might be due to the free Internet access and the absence of network defense solutions.

Identify the Internet access policy demonstrated in the above scenario.

A. Promiscuous policy

B. Paranoid policy

C. Permissive policy

D. Prudent policy

ANSWER: C

Explanation:

Permissive policy is correct because the scenario describes broadly unrestricted access to the public Internet from a personally owned remote computer, combined with no effective network-defense controls. A permissive Internet-access approach emphasizes availability and user freedom over strict restrictions on destinations, downloads, applications, or content categories. Consequently, a user may reach untrusted sites and download material without preventative filtering or inspection stopping the transfer. In this case, the accidental download of a malicious file is the expected type of exposure created when Internet access is freely available and protective controls are absent or insufficient.

For remote access to confidential organizational resources, security practice requires that access decisions account for the risks of unmanaged endpoints and public-network connectivity. NIST explains that remote-access security should protect organizational systems and data through appropriate technical and policy controls, including controls for remote client devices and communications. CISA similarly recommends protective measures that reduce exposure to malicious downloads and unsafe Internet activity. These principles support identifying the described unrestricted, lightly controlled access model as a permissive policy. See NIST SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and BYOD Security and CISA: Malware.

QUESTION NO: 27

A digital signature is a type of public key cryptography. Which of the following statements are true about digital signatures?

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

A. In order to digitally sign an electronic record, a person must use his/her public key.

B. In order to verify a digital signature, the signer's private key must be used.

C. In order to verify a digital signature, the signer's public key must be used.

D. In order to digitally sign an electronic record, a person must use his/her private key.

ANSWER: C D

Explanation:

A digital signature is created using the signer's private key. Typically, the signing process first computes a cryptographic hash of the electronic record and then applies the signer's private key to produce the signature value. Because the private key must remain under the signer's exclusive control, this process supports evidence of origin and helps provide nonrepudiation when the associated key-management and certificate practices are sound.

Verification uses the signer's corresponding public key. A verifier obtains the public key—commonly from the signer's digital certificate—validates the signature mathematically, and compares the result with a newly calculated hash of the received record. A successful verification demonstrates that the record has not changed since it was signed and that the signature was generated with the private key corresponding to the supplied public key. NIST describes digital signatures as mechanisms that provide authentication, data integrity, and non-repudiation support through private-key signing and public-key verification. See NIST FIPS 186-5, Digital Signature Standard and NIST Digital Signature Standard.

QUESTION NO: 28

In which of the following techniques does an attacker take network traffic coming towards a host at one port and forward it from that host to another host?

A. Snooping

B. UDP port scanning

C. Port redirection

D. Firewalking

ANSWER: C

Explanation:

Port redirection is correct. This technique uses a compromised or attacker-controlled host as an intermediary that listens for traffic arriving on a designated local port, then relays that traffic to a port and service on another system. For example, traffic sent to a host on a particular TCP port can be forwarded through that host to an internal system that is not directly reachable by the attacker. This creates a pivot path through the intermediary and can expose services across network boundaries without requiring the attacker to connect to the destination host directly from their original machine.

Port redirection is commonly implemented with tunneling, proxying, or port-forwarding functionality. In security testing and incident response, understanding these relays is important because they can be used to traverse segmented environments and create concealed communication channels. The MITRE ATT&CK technique for Proxy describes how adversaries may route communications through an intermediate system, including port redirection, to reach target infrastructure or obscure the source of communications. See MITRE ATT&CK: Proxy and the SOCKS Protocol (RFC 1928) for a standard proxying model that relays client traffic to requested destinations.

QUESTION NO: 29

Which of the following is a technique of attacks in which the attacker secretly listens to the private conversation between victims?

A. Eavesdropping

B. Denial of service

C. Dialler attack

D. Intrusion

ANSWER: A

Explanation:

Eavesdropping is the technique in which an attacker covertly intercepts or listens to private communications without the participants' authorization. In cybersecurity, the term applies to capturing information while it is transmitted or communicated, such as network traffic, voice calls, wireless signals, messages, or other data exchanged between parties. The objective is typically to obtain sensitive information—such as credentials, financial details, confidential business information, or personal data—while remaining undetected.

Eavesdropping can occur through passive monitoring of unencrypted network communications or through interception methods that place the attacker in a position to observe traffic. Strong encryption for data in transit, secure wireless configurations, authenticated connections, and the use of protocols such as HTTPS reduce the risk because intercepted data is significantly more difficult to read or use. The UK National Cyber Security Centre describes encryption as protecting data from unauthorized access, including when data is transmitted, at NCSC guidance. OWASP also identifies the protection of data in transit as an essential application-security practice in its OWASP Top 10.

QUESTION NO: 30

Adam works as a Security Analyst for Umbrella Inc. He is retrieving large amount of log data from syslog servers and network devices such as Router and switches. He is facing difficulty in analyzing the logs that he has retrieved. To solve this problem, Adam decides to use software called Sawmill. Which of the following statements are true about Sawmill?

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

A. It is used to analyze any device or software package, which produces a log file such as Web servers, network devices (switches & routers etc.), syslog servers etc.

B. It incorporates real-time reporting and real-time alerting.

C. It comes only as a software package for user deployment.

D. It is a software package for the statistical analysis and reporting of log files.

ANSWER: A B D

Explanation:

Sawmill is a log-analysis and reporting platform intended to turn raw event records into searchable, aggregated, and visualized operational or security information. Its core purpose is the statistical analysis and reporting of log files: it parses records, extracts fields, applies filters, and produces reports that help an analyst identify activity patterns and investigate events. Sawmill is not limited to web-server logs. Its log-processing model and available formats/parsers support data generated by many sources, including network infrastructure and syslog-producing systems, so it is appropriate when router, switch, server, and other device logs must be reviewed together.

Real-time reporting and alerting are also relevant capabilities. Rather than requiring an analyst to wait for a purely manual, end-of-day review, Sawmill can continuously process incoming log data and use report or alerting functions to provide timely visibility into conditions of interest. This supports monitoring workflows in which large volumes of device and syslog events need to be summarized and acted on quickly. The product documentation describes Sawmill as a universal log-analysis solution and identifies reporting, log processing, and alert-related capabilities. See the Sawmill product site and the Sawmill documentation.

QUESTION NO: 31

Which of the following is true for XSS, SQL injection, and RFI?

A. These are Trojans.

B. These are hacking tools.

C. These are viruses.

D. These are types of Web application vulnerabilities.

ANSWER: D

Explanation:

These are types of Web application vulnerabilities. Cross-site scripting (XSS) occurs when an application includes untrusted input in a web page without appropriate validation or output encoding, enabling attacker-controlled script to execute in a victim's browser. SQL injection occurs when an application constructs database queries using untrusted input in an unsafe manner, allowing an attacker to alter the intended query or access data. Remote file inclusion (RFI) arises when an application dynamically includes a file based on user-controlled input without sufficient validation, potentially causing the server to retrieve and execute attacker-controlled remote content. These issues share a common web-application security theme: the application accepts input across a trust boundary and processes it in a dangerous context without effective validation, parameterization, allowlisting, or encoding. Security testing should therefore examine all input vectors, enforce server-side controls, and use secure coding patterns appropriate to each interpreter or execution context. OWASP describes XSS and injection as important application-security risks and provides prevention guidance for each. See the OWASP Cross Site Scripting Prevention guidance and the OWASP SQL Injection page.

QUESTION NO: 32

Which of the following OSI layers is used for routers?

A. Application layer

B. Network layer

C. Physical layer

D. Transport layer

ANSWER: B

Explanation:

Routers primarily operate at the **Network layer** of the OSI model, also called Layer 3. Their core function is to forward packets between separate networks by examining logical network addresses, most commonly Internet Protocol addresses. A router uses its routing table and routing information learned through configured routes or routing protocols to select an appropriate next hop and outgoing interface for each packet. This Layer 3 role enables communication beyond a single local network and is fundamental to segmentation, inter-network connectivity, and controlling paths through an IP network.

In practice, a router receives a frame on one interface, processes the encapsulated IP packet to make a forwarding decision based on its destination IP address, then encapsulates that packet into a suitable Layer 2 frame for the next network segment. While routers necessarily use lower-layer interfaces to transmit and receive traffic, routing itself—the decision to move packets across IP networks—belongs to the Network layer. Cisco's overview of the OSI model identifies routing and logical addressing as Layer 3 functions, and RFC 1812 defines requirements for IPv4 routers. See Cisco's networking overview and RFC 1812: Requirements for IP Version 4 Routers.

QUESTION NO: 33

Which of the following parameters are required to be followed on receiving a suspicious mail according to the Department of Justice?

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

A. Call

B. Look

C. Identify

D. Stop

ANSWER: A B D

Explanation:

The required actions are **Stop**, **Look**, and **Call**, which form a practical response sequence for a suspicious email. Stop means pausing before clicking links, opening attachments, replying, or providing information; this prevents an impulsive action from turning a suspected phishing message into a security incident. Look means carefully inspecting the message for indicators such as an unexpected request, unusual urgency, mismatched sender details, unfamiliar links, or attachment-related warnings. This review helps a recipient recognize that an email may be impersonating a trusted person or organization. Call means independently verifying the request through a trusted channel, such as calling the sender using a known phone number or contacting the organization's help desk or security team. Verification must not rely on contact information supplied in the suspicious message itself. Together, these steps support the Department of Justice's cybersecurity-awareness approach by ensuring that recipients pause, assess the message, and verify authenticity before taking action. The DOJ provides cybersecurity resources through its Cybersecurity page, and the same cautious handling and reporting principles are reinforced in CISA's phishing-recognition guidance.

QUESTION NO: 34

Who among the following are security experts who specialize in penetration testing and other testing methodologies to ensure that their company's information systems are secure?

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

A. Black hat hackers

B. White hat hackers

C. Script Kiddies

D. Ethical hackers

ANSWER: B D

Explanation:

White hat hackers and ethical hackers are authorized security professionals who use penetration testing and related assessment methodologies to identify, validate, and help remediate security weaknesses before those weaknesses can be exploited maliciously. In common security terminology, "white hat hacker" and "ethical hacker" describe the same essential role: a tester who operates with explicit permission, a defined scope, and rules of engagement established by the organization that owns the systems. Their work can include reconnaissance, vulnerability assessment, controlled exploitation, post-exploitation validation, and clear reporting of findings and recommended fixes. This testing provides an organization with evidence of real-world attack paths and helps prioritize risk treatment based on demonstrated impact. Authorization and responsible handling of findings are fundamental because even technically valid testing must protect the confidentiality, integrity, and availability of business systems and data. EC-Council's Certified Ethical Hacker program describes ethical hacking as using hacker techniques lawfully to identify vulnerabilities and improve an organization's security posture. The National Institute of Standards and Technology likewise describes penetration testing as a security assessment method that simulates attacks to identify and validate vulnerabilities. See EC-Council Certified Ethical Hacker and NIST SP 800-115, Technical Guide to Information Security Testing and Assessment.

QUESTION NO: 35

Which of the following tools is used to catch someone installing a rootkit or running a packet sniffer?

A. chkrootkit

B. rkhunter

C. Blue Pill

D. OSSEC

ANSWER: D

Explanation:

OSSEC is correct because it is a host-based intrusion detection system designed to continuously monitor endpoints and generate alerts for suspicious security-relevant activity. Its capabilities include rootkit detection, file-integrity monitoring, log analysis, active response, and real-time alerting. These functions can identify indicators associated with a rootkit installation, such as unauthorized changes to system binaries, hidden files or processes, suspicious kernel-level artifacts, and modifications to monitored configuration files.

OSSEC can also help detect packet-sniffing activity through host monitoring and log correlation. A packet sniffer commonly requires elevated privileges and may place a network interface into promiscuous mode; these events, related process activity, and associated system or audit-log entries can be monitored and alerted on by an HIDS deployment. Unlike a point-in-time scanner, OSSEC is intended to provide ongoing endpoint visibility, making it suitable for catching an attempted or active compromise as it occurs. The OSSEC project describes its platform as an open-source host-based intrusion detection system with rootkit detection and real-time alerting capabilities. See the OSSEC documentation and the OSSEC project overview.

QUESTION NO: 36

Linux traffic monitoring tools are used to monitor and quickly detect faults in the network or a system. Which of the following tools are used to monitor traffic of the Linux operating system?

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

A. PsExec

B. IPTraf

C. MRTG

D. PsLogList

E. Ntop

ANSWER: B C E

Explanation:

IPTraf, **MRTG**, and **Ntop** are established tools for observing network activity on Linux systems. IPTraf is an interactive, console-based network monitor that presents real-time information such as interface traffic, packet counts, protocol activity, TCP and UDP connections, and LAN-station statistics. This makes it useful for directly examining traffic on a host or interface during troubleshooting. The maintained IPTraf-ng project documents its purpose as a console-based network statistics utility for Linux: IPTraf-ng project.

MRTG (Multi Router Traffic Grapher) collects traffic counters, commonly through SNMP, stores historical measurements, and produces graphs showing bandwidth utilization over time. Its trend reporting supports capacity planning and the detection of persistent or recurring traffic anomalies rather than only immediate packet-level inspection. MRTG is designed to monitor network links and related measured values, as described in the official MRTG documentation.

Ntop is a traffic-monitoring and analysis tool that captures and summarizes network flows, protocols, hosts, and throughput. It provides visibility into which systems and applications generate traffic, helping administrators investigate congestion, unusual communication patterns, and network faults. Together, these tools cover interactive traffic inspection, historical graphing, and flow-oriented network visibility.

QUESTION NO: 37

Which of the following proxy servers is used to retrieve web pages?

A. FTP proxy server

B. NAT proxy server

C. HTTP proxy server

D. Socks proxy server

ANSWER: C

Explanation:

HTTP proxy server is correct because it is specifically designed to handle web traffic using the Hypertext Transfer Protocol (HTTP), the application-layer protocol browsers use to request web pages and related resources. Rather than a client connecting directly to a website, the browser sends its HTTP request to the proxy. The proxy then retrieves the requested page from the destination web server and returns the response to the client. This intermediary role can support web-access control, request logging, content filtering, caching of frequently requested resources, and hiding internal client addresses from external web servers. HTTP proxies can also process HTTPS connections using the HTTP CONNECT method, which establishes a tunnel to the requested secure web service. The HTTP semantics involved in requests and responses are defined by the Internet Engineering Task Force's HTTP Semantics standard: RFC 9110. Mozilla's networking documentation also describes an HTTP proxy as a proxy configuration used for HTTP web requests and identifies the proxy as the server through which those requests are sent: Firefox HTTP Proxy documentation.

QUESTION NO: 38

Which of the following is a valid IP address for class B Networks?

A. 212.136.45.8

B. 172.157.88.3

C. 225.128.98.7

ANSWER: B

Explanation:

172.157.88.3 is a valid class B IPv4 address under traditional classful addressing rules. In classful IPv4 addressing, the address class is determined by the value of the first octet. Class B addresses have a first octet from 128 through 191, which corresponds to a leading binary pattern of `10`. The first octet in 172.157.88.3 is 172, placing it squarely within that class B range.

Class B networks historically used the default subnet mask 255.255.0.0 (/16). This leaves the first two octets as the network identifier and the final two octets as the host identifier. With that default mask, 172.157.88.3 has a nonzero host portion and is structurally usable as a host address. Although modern networks use classless inter-domain routing and subnet masks rather than relying on address classes for routing decisions, classful ranges remain important foundational knowledge for IPv4 addressing questions. The IETF's original IPv4 specification describes the class-based address structure, and IANA maintains the authoritative IPv4 address-space registry: RFC 791 and IANA IPv4 Address Space Registry.