DUMPSARENA

GIAC Security Leadership Certification (GSLC)

GIAC GSLC

Version Demo

Total Demo Questions: 59

Total Premium Questions: 591

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	160
Topic 2, Volume B	153
Topic 3, Volume C	156
Topic 4, Volume D	102
Total	591

QUESTION NO: 1

A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides an attacker unauthorized access to a computer. Which of the following tools can an attacker use to perform war dialing?

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

A. Wingate

B. ToneLoc

C. THC-Scan

D. NetStumbler

ANSWER: B C

Explanation:

ToneLoc and **THC-Scan** are tools associated with war dialing. War dialing automates calls across a defined range of telephone numbers, records which calls answer, and identifies lines that present characteristics of modems, fax systems, remote-access services, or other dial-up-capable devices. This was particularly relevant where organizations operated remote-access modem pools or standalone maintenance modems, because an externally reachable dial-in service could become an unmonitored access path.

ToneLoc is a well-known historical wardialing utility designed to systematically dial number ranges and log responses for subsequent review. THC-Scan is likewise used for scanning and identifying dial-up or modem-accessible systems in the context of telephone-number enumeration. In a security assessment, the results of such scanning should be treated as evidence to validate authorized remote-access inventory, disable unneeded dial-in services, require strong authentication, and monitor any remaining legacy access paths. NIST defines war dialing as using software to dial a range of telephone numbers in order to locate modems or other computer systems; see the NIST CSRC war dialing glossary entry. Additional historical context on ToneLoc and wardialing is available from SecTools' ToneLoc entry.

QUESTION NO: 2

Which of the following is the best encryption algorithm to encrypt and decrypt messages?

A. AES

B. DES

C. RSA

D. TripleDES

ANSWER: A

Explanation:

AES is the appropriate choice among these algorithms for protecting message content because it is the current, broadly accepted symmetric encryption standard and supports efficient, strong encryption with 128-, 192-, or 256-bit keys. In practical systems, messages are commonly encrypted with AES because symmetric encryption is efficient enough for data of arbitrary length. AES should normally be used through an authenticated-encryption mode, such as GCM, so the recipient can both decrypt the message and verify that it was not altered in transit. AES-GCM combines confidentiality with integrity and authenticity checks when used correctly with unique initialization values.

NIST specifies AES as a Federal Information Processing Standard and identifies it as a symmetric block cipher for protecting sensitive information. NIST also defines GCM as an authenticated-encryption mode for block ciphers, making it a suitable construction for secure message protection. Real-world secure messaging designs may use public-key cryptography to establish or wrap an AES session key, but AES performs the bulk encryption and decryption of the message itself. See NIST FIPS 197: Advanced Encryption Standard and NIST SP 800-38D: GCM and GMAC.

QUESTION NO: 3

In which of the following Person-to-Person social engineering attacks does an attacker pretend to be an outside contractor, delivery person, etc., in order to gain physical access to the organization?

A. In person attack

B. Third-party authorization attack

C. Important user posing attack

D. Impersonation attack

ANSWER: D

Explanation:

Impersonation attack is correct because it relies on an attacker assuming a believable identity to exploit human trust and bypass physical security controls. By posing as a contractor, courier, maintenance technician, vendor, or other expected visitor, the attacker creates a plausible reason to be near restricted areas, ask an employee to hold a door, obtain a visitor badge, or gain entry through a reception area. The objective is usually unauthorized physical access, which may then enable theft, device tampering, placement of malicious hardware, observation of sensitive information, or access to internal systems.

Effective defenses combine people, process, and physical controls: staff should verify visitor identities and work orders, escorts should be required in sensitive locations, badges should be visibly displayed, and employees should avoid granting access merely because someone appears to have an operational role. CISA identifies impersonation and pretext-based approaches as social-engineering tactics that manipulate a target into providing access or information. NIST also emphasizes visitor management and physical access authorization as important elements of organizational security programs. See CISA guidance on avoiding social-engineering attacks and NIST SP 800-53 physical and personnel security controls.

QUESTION NO: 4

You are responsible for security on your network. One particular concern is the theft of sensitive data. You want to make sure that end users do not (purposefully or accidentally) take data off the premises. Which of the following should you be concerned about?

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

A. Cell Phones

B. Individual scanners

C. USB Drives

D. Individual printers

ANSWER: A B C D

Explanation:

Cell Phones, Individual scanners, USB Drives, and Individual printers are all relevant data-loss and data-exfiltration concerns because each can move sensitive information outside controlled organizational systems or turn it into a portable form. Cell Phones can capture documents or displays with cameras and can transmit files through wireless communications. Individual scanners can convert paper records into digital files that may then be copied or transmitted. USB Drives provide a compact removable-media path for copying large quantities of information without using approved network-sharing mechanisms. Individual printers can create hard-copy records that a user can remove from the facility, including documents that might otherwise remain within protected applications or storage locations. Effective protection therefore requires controls spanning removable media, printing, imaging, mobile devices, physical removal, monitoring, and policy enforcement—not merely network controls. NIST guidance identifies the need to control removable media and restrict the use of organizationally

owned portable storage devices; see NIST SP 800-53 Rev. 5. NIST's data-loss-prevention guidance also describes protecting sensitive data across endpoints, removable media, and output channels; see NIST SP 800-92.

QUESTION NO: 5

Which of the following password authentication schemes enables a user with a domain account to log on to a network once, using a password or smart card, and to gain access to multiple computers in the domain without being prompted to log in again?

A. Single Sign-On

B. Dynamic

C. One-time password

D. Kerberos

ANSWER: A

Explanation:

Single Sign-On is correct because it describes the authentication capability in which a user establishes an authenticated session once and then accesses multiple authorized systems or services without repeatedly entering credentials. In a domain environment, the initial sign-in may use a password or smart card; after that successful authentication, the identity infrastructure can provide or validate credentials for access to additional domain resources. This reduces repeated credential prompts while maintaining centralized identity management and access control.

Single Sign-On is an authentication experience and architectural capability rather than a specific cryptographic protocol. In many enterprise domains, it is commonly implemented through interoperable identity services and ticket-based authentication, allowing a user's initial domain authentication to be reused for access to computers, applications, and network services within the authorized scope. Microsoft describes this user experience as accessing resources after a single sign-in, and NIST recognizes single sign-on as a mechanism supporting authentication across relying parties. See Microsoft Kerberos authentication and NIST Digital Identity Guidelines.

QUESTION NO: 6

Which of the following programs can be used to detect stealth port scans performed by a malicious hacker?

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

A. portsentry

B. nmap

C. scanlogd

D. libnids

ANSWER: A C D

Explanation:

`portsentry`, `scanlogd`, and `libnids` can be used to identify the network activity associated with stealth port scanning. PortSentry is an intrusion-detection tool designed to monitor specified TCP and UDP ports and generate alerts or take configured response actions when it observes scan activity. This makes it appropriate for detecting attempts to identify accessible services without establishing normal application connections.

Scanlogd was specifically designed to detect port scans, including stealth techniques that may use fragmented, spoofed, or incomplete TCP packets to avoid conventional logging. It analyzes packet and connection information to recognize suspicious scan patterns rather than relying solely on successful TCP connections. Its documentation describes its purpose as detecting port scans and discusses support for stealth-scan-related detection considerations.

Libnids is a network intrusion-detection development library that captures and processes network traffic, including TCP stream reassembly and IP-fragment handling. Those capabilities enable an IDS or monitoring program built with libnids to inspect packet patterns and implement reliable stealth-port-scan detection logic. See the Scanlogd project documentation and the libnids project repository.

QUESTION NO: 7

Which of the following is responsible for assuring the quality of the deliverables in a project?

A. Quality assurance (QA) manager

B. Quality control (QC) manager

C. Stakeholder

D. Project manager

ANSWER: A

Explanation:

The **Quality assurance (QA) manager** is responsible for establishing confidence that project deliverables will meet defined quality requirements. This responsibility includes developing and maintaining the quality-management approach, defining applicable standards and acceptance criteria, ensuring that suitable processes are used throughout delivery, and performing reviews or audits to verify that those processes are being followed. In a project environment, quality assurance is preventive: it builds quality into planning and execution rather than treating quality as an activity performed only after work is complete.

By maintaining a documented, repeatable quality process, the QA manager helps ensure that deliverables are consistently produced in conformance with stakeholder requirements, organizational policies, contractual obligations, and relevant standards. The QA role also provides objective evidence that the project's methods are capable of producing acceptable results and identifies process improvements before defects propagate into completed deliverables. The American Society for Quality describes quality assurance as the planned and systematic activities used to provide confidence that quality requirements will be fulfilled: ASQ: Quality Assurance vs. Quality Control. This aligns with ISO's quality-management principles, which emphasize process-based management and continual improvement: ISO Quality Management.

QUESTION NO: 8

Which of the following types of attacks cannot be prevented by a firewall?

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

A. Ping flood attack

B. Phishing attack

C. Shoulder surfing attack

D. URL obfuscation attack

ANSWER: B C D

Explanation:

Phishing attack, shoulder surfing attack, and URL obfuscation attack are correct because they primarily exploit people, physical access, or deceptive content rather than a network connection that a conventional firewall can reliably block. Phishing persuades a recipient to disclose information, open a harmful attachment, or follow a deceptive link; firewall policy alone cannot ensure that a user recognizes and rejects the fraud. The CISA phishing guidance emphasizes user awareness and verification practices as important protections.

Shoulder surfing consists of observing sensitive information directly from a nearby physical position, such as watching a user enter a password. Preventing this requires physical and procedural safeguards, including privacy screens, secure workspace practices, and user awareness, rather than network traffic filtering.

URL obfuscation disguises a destination through misleading text, encoding, redirects, shortened links, or similar techniques intended to defeat a user's inspection of a link. A basic firewall generally evaluates network traffic and access rules, not whether a displayed or delivered URL is deceptive. Effective defense therefore combines user education with email and web security controls, URL reputation filtering, and browser protections. The NIST Cybersecurity Framework resources support using layered safeguards across technical, organizational, and human-risk areas.

QUESTION NO: 9

You have detected what appears to be an unauthorized wireless access point on your network. However this access point has the same MAC address as one of your real access points and is broadcasting with a stronger signal. What is this called?

A. Buesnarfing

B. DOS

C. The evil twin attack

D. WAP cloning

ANSWER: C

Explanation:

The evil twin attack is correct because it involves an unauthorized wireless access point impersonating a legitimate access point in order to attract clients. An attacker commonly copies identifying characteristics of the trusted wireless network, such as its SSID and, in some scenarios, the access point's MAC address (BSSID). Broadcasting a stronger signal makes the fraudulent access point more attractive to nearby devices, which may associate with it instead of the genuine infrastructure.

Once a client connects, the attacker can potentially observe traffic, capture credentials through a counterfeit authentication portal, perform man-in-the-middle activity, or otherwise exploit the victim's trust in the familiar network identity. The defining feature is therefore deceptive impersonation of a real Wi-Fi service, not merely the presence of an unapproved wireless device. Wireless security monitoring should detect duplicate or suspicious BSSIDs, unexpected signal-strength changes, and unauthorized radios, while strong mutual authentication such as WPA2/WPA3-Enterprise with certificate validation helps clients distinguish legitimate infrastructure from impostors. NIST discusses wireless threats and recommended WLAN security controls in SP 800-153, and Cloudflare provides an overview of evil twin attacks.

QUESTION NO: 10

You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

A. Quantitative risk analysis

B. Seven risk responses

C. Qualitative risk analysis

D. A risk probability-impact matrix

ANSWER: C

Explanation:

Qualitative risk analysis is the correct answer because it provides a rapid, prioritized assessment of identified risks by evaluating their relative probability of occurrence and potential effect on project objectives. The project team commonly applies defined rating scales, such as low, medium, and high, along with expert judgment, to assess each risk. This creates a practical view of which risks require prompt attention, further analysis, an assigned owner, or a planned response.

The result is usually documented in the risk register and may include an overall risk score, urgency, categorization, and watch-list status. This high-level prioritization is especially useful early in planning and throughout project execution because it helps leaders focus limited time and resources on the risks most likely to affect scope, schedule, cost, quality, or other objectives. A probability-impact matrix can be used as a tool during this process, but qualitative risk analysis is the overall analysis process that delivers the quick, high-level review described in the question. PMI describes qualitative risk analysis as prioritizing individual project risks for further analysis or action by assessing their probability and impacts. See PMI's qualitative risk analysis guidance and the PMBOK Guide overview.

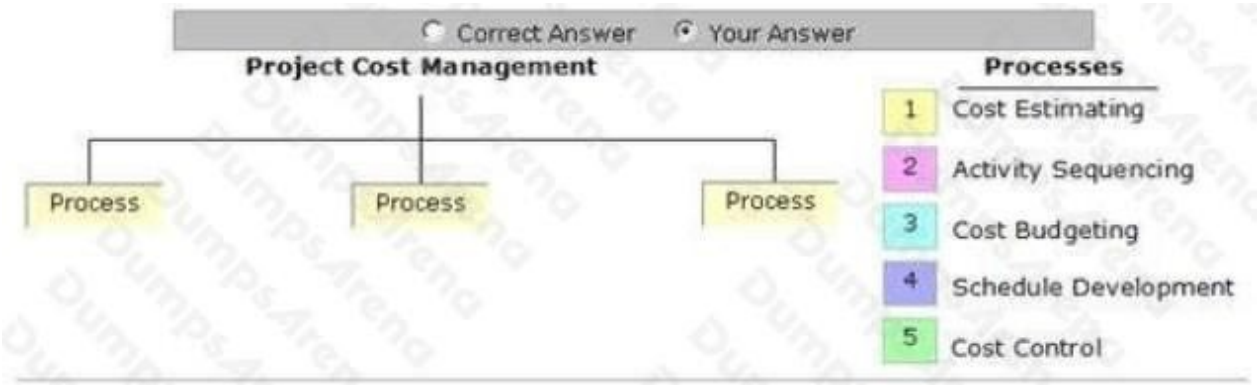
QUESTION NO: 11 - (DRAG DROP)

DRAG DROP

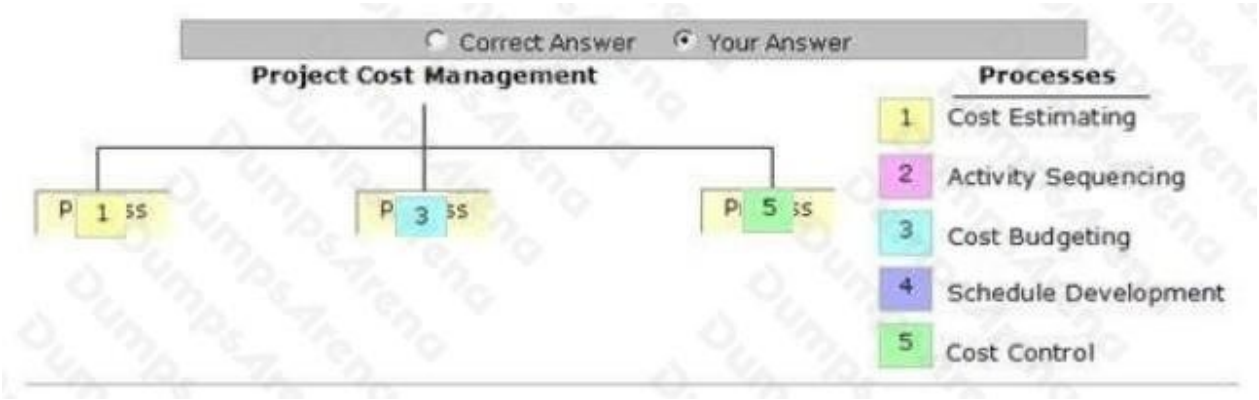
Place the processes that are grouped under the Project Cost Management Knowledge Area in the image below.

Drag an item from the item list and drop it on the appropriate spot. To remove an item, drag and drop it anywhere on the window.

Select and Place:



ANSWER:



Explanation:

Project Cost Management contains the processes used to plan, estimate, establish, finance, manage, and control project costs so that the project can be completed within its approved budget. In the process model used by this question, the applicable processes are Cost Estimating, Cost Budgeting, and Cost Control. Cost Estimating establishes an informed approximation of the monetary resources needed for the project's activities, work packages, or deliverables. Those estimates provide the basis for determining how much funding the work is likely to require.

Cost Budgeting follows by aggregating the approved estimates and assigning them across the project work to create the authorized cost baseline. The budget is important because it becomes the approved financial reference point for the project. It supports funding decisions and gives the project team a measurable standard against which actual spending and performance can be assessed.

Cost Control is the continuing management process that uses the approved cost baseline to monitor project cost performance, identify variances, manage changes that affect cost, and help keep expenditures aligned with authorized funding. Together, these processes form a practical lifecycle: determine expected cost, establish the authorized budget, and monitor and control cost performance throughout execution. This is why the visual sequence of Cost Estimating, Cost Budgeting, and Cost Control correctly represents Project Cost Management. PMI provides an overview of project cost management concepts in its Project Cost Management resource, including the importance of estimating, budgeting, and controlling costs against an approved baseline.

QUESTION NO: 12

Which type of attack is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs?

A. Bluesnarfing

B. Bluebugging

C. Blue Jacking

D. Bluecast

ANSWER: A

Explanation:

Bluesnarfing is the unauthorized acquisition of data from a Bluetooth-enabled device by exploiting weaknesses in its Bluetooth implementation or configuration. The term specifically describes gaining access to information stored on, or available through, a nearby device without the owner's authorization. Depending on the affected device and vulnerability, exposed information can include contacts, calendar entries, messages, files, device identifiers, or other personal and organizational data. The attack is associated with Bluetooth's short-range wireless communications, meaning proximity is generally relevant, although practical range can vary based on radio hardware, antennas, and environmental conditions.

This definition directly matches the question's focus on unauthorized access to information from devices such as phones, laptops, desktops, and personal digital assistants through a Bluetooth connection. Security leaders should treat Bluetooth as an attack surface: maintain current device firmware and operating-system updates, disable Bluetooth when it is not needed, avoid discoverable mode in public environments, and require secure pairing practices. NIST's glossary identifies bluesnarfing as unauthorized access to information from a wireless device through a Bluetooth connection. Additional Bluetooth security guidance is available from NIST's mobile-device security resources.

References: NIST CSRC: Bluesnarfing; NIST SP 800-124 Rev. 2.

QUESTION NO: 13

You are a Web Administrator of Millennium Inc. The company has hosted its Web site within its network. The management wants the company's vendors to be able to connect to the corporate site from their locations through the Internet. As a public network is involved in this process, you are concerned about the security of data transmitted between the vendors and the corporate site. Which of the following can help you?

A. Smart card

B. EAP

C. VPN

D. WEP

ANSWER: C

Explanation:

A virtual private network (VPN) is appropriate because it protects communications between remote vendors and the corporate network while traffic traverses the public Internet. A VPN establishes an encrypted tunnel between endpoints, providing confidentiality for transmitted data and, depending on the VPN protocol and configuration, integrity protection and peer authentication as well. This allows authorized vendor users to access required internal web resources without exposing the contents of their sessions to parties monitoring or intercepting Internet traffic. For this use case, the organization can deploy a remote-access VPN for individual vendor users or a site-to-site VPN if vendors connect from managed networks. Security leadership should also require strong authentication, least-privilege authorization, current cryptographic settings, logging, and periodic access reviews for third-party accounts. The U.S. Cybersecurity and Infrastructure Security Agency describes VPNs as encrypted connections over less secure networks, and NIST provides guidance on secure remote-access technologies and their management. See CISA's overview of VPNs and NIST SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and BYOD Security.

QUESTION NO: 14

Which of the following types of security will be the cause of concern if the server has been stolen from the organization's premises?

A. Information security

B. Operational security

C. Physical security

D. User authentication

ANSWER: C

Explanation:

Physical security is correct because the theft of a server from an organization's premises represents a failure, or potential failure, of protections intended to safeguard tangible assets and restrict unauthorized physical access. Physical security encompasses controls such as secured server rooms and data centers, locks, access badges, guards, CCTV, asset tracking, visitor management, and procedures for securely mounting or storing equipment. These controls are designed to prevent unauthorized removal, tampering, and destruction of hardware.

A stolen server can create serious downstream business and security consequences, particularly if it contains sensitive data or cryptographic material. However, the event described—an individual removing an organizational server from its location—most directly concerns the protection of the physical asset and the premises in which it was housed. Effective security leadership treats physical controls as part of a defense-in-depth program, aligning facility safeguards with asset inventory, incident-response processes, and data-protection controls. NIST describes physical and environmental protection as safeguards for physical access to systems, equipment, and operating environments. See NIST SP 800-53 Physical and Environmental Protection controls and the CISA physical security guidance.

QUESTION NO: 15

In which of the following social engineering attacks does an attacker first damage any part of the target's equipment and then advertise himself as an authorized person who can help fix the problem.

A. Impersonation attack

B. In person attack

C. Important user posing attack

D. Reverse social engineering attack

ANSWER: D

Explanation:

Reverse social engineering attack is correct because the attacker engineers a situation in which the target initiates contact and requests assistance. The attack commonly begins with a deliberate disruption, such as disabling equipment, interfering with a service, or otherwise creating a plausible technical problem. The attacker then presents themself as an authorized support professional or makes their supposed support service known to the victim. Because the victim is motivated to restore normal operations, they are more likely to trust the apparent helper and voluntarily disclose credentials, provide access, install software, or follow instructions that compromise the organization.

This technique exploits trust in authority and the urgency created by an operational outage. Its distinguishing feature is that the attacker does not merely approach the victim with a pretext; instead, the attacker creates the need and positions themself as the solution. This can reduce suspicion because the victim believes they are seeking legitimate help. NIST defines social engineering as techniques that manipulate people into performing actions or divulging confidential information, a description that directly fits this trust-based scenario. CISA likewise emphasizes verifying support requests and identities through trusted, independently obtained contact channels. See the NIST social engineering glossary entry and CISA guidance on avoiding social-engineering attacks.

QUESTION NO: 16

What is the major difference between a worm and a Trojan horse?

A. A worm is a form of malicious program, while a Trojan horse is a utility.

B. A Trojan horse is a malicious program, while a worm is an anti-virus software.

C. A worm is self replicating, while a Trojan horse is not.

D. A worm spreads via e-mail, while a Trojan horse does not.

ANSWER: C

Explanation:

A worm is self replicating, while a Trojan horse is not. This is the key behavioral distinction: a computer worm is standalone malicious code that can make copies of itself and propagate between systems, commonly by exploiting network-accessible vulnerabilities or using other automated propagation mechanisms. Its ability to replicate without attaching itself to another program enables infections to spread rapidly with little or no action from a user.

A Trojan horse, by contrast, is malware that presents itself as legitimate or desirable software in order to persuade a user to install or run it. Although a Trojan may perform harmful actions after execution—such as stealing data, opening remote access, or downloading additional malware—deception rather than autonomous self-replication is its defining characteristic. A Trojan can be delivered by email or can lead to a worm being installed, but those delivery or payload details do not make it self-replicating. The distinction is important to security leaders because worms often require urgent containment through network segmentation and patching, while Trojan defenses emphasize trusted software controls, user awareness, and endpoint detection. See the CISA overview of malware threats and the MITRE ATT&CK Spearphishing guidance.

QUESTION NO: 17

You work in an enterprise as a Network Engineer. Your enterprise has a secure internal network. You want to apply an additional network packet filtering device that is intermediate to your enterprise's internal network and the outer network (internet). Which of the following network zones will you create to accomplish this task?

A. Border network area

B. Autonomous system area (AS)

C. Demilitarized zone (DMZ)

D. Site network area

ANSWER: C

Explanation:

A demilitarized zone (DMZ) is the appropriate network zone for placing systems or controls between a trusted internal network and an untrusted external network such as the Internet. A DMZ creates a separate security boundary, typically enforced by firewalls or packet-filtering devices, so that traffic entering from the Internet does not directly reach internal systems. The filtering controls can apply distinct rules for Internet-to-DMZ, DMZ-to-internal, internal-to-DMZ, and outbound connections. This segmentation supports defense in depth by limiting exposure and ensuring that services needing external access, such as web, mail, or DNS services, are isolated from the enterprise's private network. A DMZ may be implemented with separate external and internal firewalls, or with logically separate firewall interfaces and tightly controlled policy rules. NIST describes firewall architectures that use a DMZ to separate public-facing systems from protected internal networks and to provide an additional layer of protection. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and the CISA guidance on firewall and DMZ security.

QUESTION NO: 18

Which of the following security policies will you implement to keep safe your data when you connect your Laptop to the office network over IEEE 802.11 WLANs? Each correct answer represents a complete solution. Choose two.

A. Using personal firewall software on your Laptop.

B. Using an IPSec enabled VPN for remote connectivity.

C. Using portscanner like nmap in your network.

D. Using a protocol analyzer on your Laptop to monitor for risks.

ANSWER: A B

Explanation:

Using personal firewall software on your Laptop is an appropriate endpoint-security control for wireless use. A properly managed host firewall applies rules to inbound and outbound traffic, limits exposure of local services, and helps prevent unauthorized connections from other devices sharing the wireless environment. This is especially important when a laptop may encounter networks whose devices and traffic cannot be fully trusted. NIST's wireless-network guidance identifies host-based protections as a valuable layer of defense for WLAN clients; see NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks.

Using an IPSec enabled VPN for remote connectivity is also a sound policy because IPsec provides authenticated, encrypted protection for traffic carried across the wireless network before it reaches organizational resources. A VPN reduces the risk that wireless traffic is read or altered by an unauthorized party and can enforce access through the organization's controlled remote-access gateway. IPsec is designed to protect IP communications through security associations that provide confidentiality, integrity, and peer authentication. NIST describes these protections and IPsec deployment considerations in NIST SP 800-77 Rev. 1, Guide to IPsec VPNs. Together, these measures protect both the laptop's exposed network services and data in transit.

QUESTION NO: 19

What is a stakeholder analysis chart?

A. It is a matrix that identifies who must communicate with whom.

B. It is a matrix that identifies all of the stakeholders and to whom they must report to.

C. It is a matrix that documents stakeholders' threats, perceived threats, and communication needs.

D. It is a matrix that documents the stakeholders' requirements, when the requirements were created, and when the fulfillment of the requirements took place.

ANSWER: C

Explanation:

A stakeholder analysis chart is a structured matrix used to identify relevant stakeholders and document the security-related factors that affect how each stakeholder should be engaged. In this context, the chart captures stakeholders' threats, their perceived threats, and their communication needs. This gives security leadership a practical view of both actual risk concerns and the concerns that influence stakeholder support, resistance, decision-making, and required communications. Recording communication needs helps ensure that security information is provided to the appropriate parties in a form, frequency, and level of detail they can use. Capturing perceived threats is equally important because stakeholders may prioritize risks differently depending on their responsibilities, business objectives, and exposure to consequences. The resulting analysis supports risk-informed governance and enables a security leader to tailor engagement and reporting throughout an initiative or security program. NIST describes risk management as an organization-wide activity involving senior leaders and other stakeholders, with communication and shared risk understanding as essential elements. See NIST SP 800-39, Managing Information Security Risk. For additional stakeholder-management context, see the Project Management Institute stakeholder management guidance.

QUESTION NO: 20

The 3-way handshake method is used by the TCP protocol to establish a connection between a client and the server. It involves three steps:

1. In the first step, a SYN message is sent from a client to the server.

2. In the second step, a SYN/ACK message is sent from the server to the client.

3. In the third step, an ACK (usually called SYN-ACK-ACK) message is sent from the client to theserver. At this point, both the client and the server have received acknowledgements of the TCP connection. If the Initial Sequence Numbers of the client and server were 241713111 and 241824111 respectively at the time when the client was sending the SYN message in the first step of the TCP 3-way handshake method, what will be the value of the acknowledgement number field of the server's packet when the server was sending the SYN/ACK message to the client in the second step of the TCP 3-way handshake method?

A. 241824111

B. 241713112

C. 241824112

D. 241713111

ANSWER: B

Explanation:

The correct acknowledgement number is **241713112**. In TCP, the acknowledgement field identifies the next sequence number the sender expects to receive from its peer. The client begins the handshake by transmitting a SYN segment with an initial sequence number of 241713111. Although the SYN does not carry application payload, it consumes one position in TCP sequence-number space. Therefore, when the server responds with its SYN/ACK segment, it acknowledges the client's SYN by setting its acknowledgement number to the client's initial sequence number plus one: 241713111 + 1 = 241713112.

The server simultaneously chooses and sends its own initial sequence number, 241824111, in the *sequence number* field of that SYN/ACK packet. That server sequence number does not determine the acknowledgement number in this direction; the acknowledgement specifically confirms receipt of the client's SYN. The client then completes the handshake by acknowledging the server's SYN with an acknowledgement number of 241824112. This sequence-space behavior is specified in the TCP standard: a SYN consumes one sequence number even when no data is present. See RFC 9293, TCP connection establishment and RFC 9293, TCP sequence numbers.

QUESTION NO: 21

Which of the following are the examples of administrative controls?

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

A. Security policy

B. Auditing

C. Security awareness training

D. Data Backup

ANSWER: A B C

Explanation:

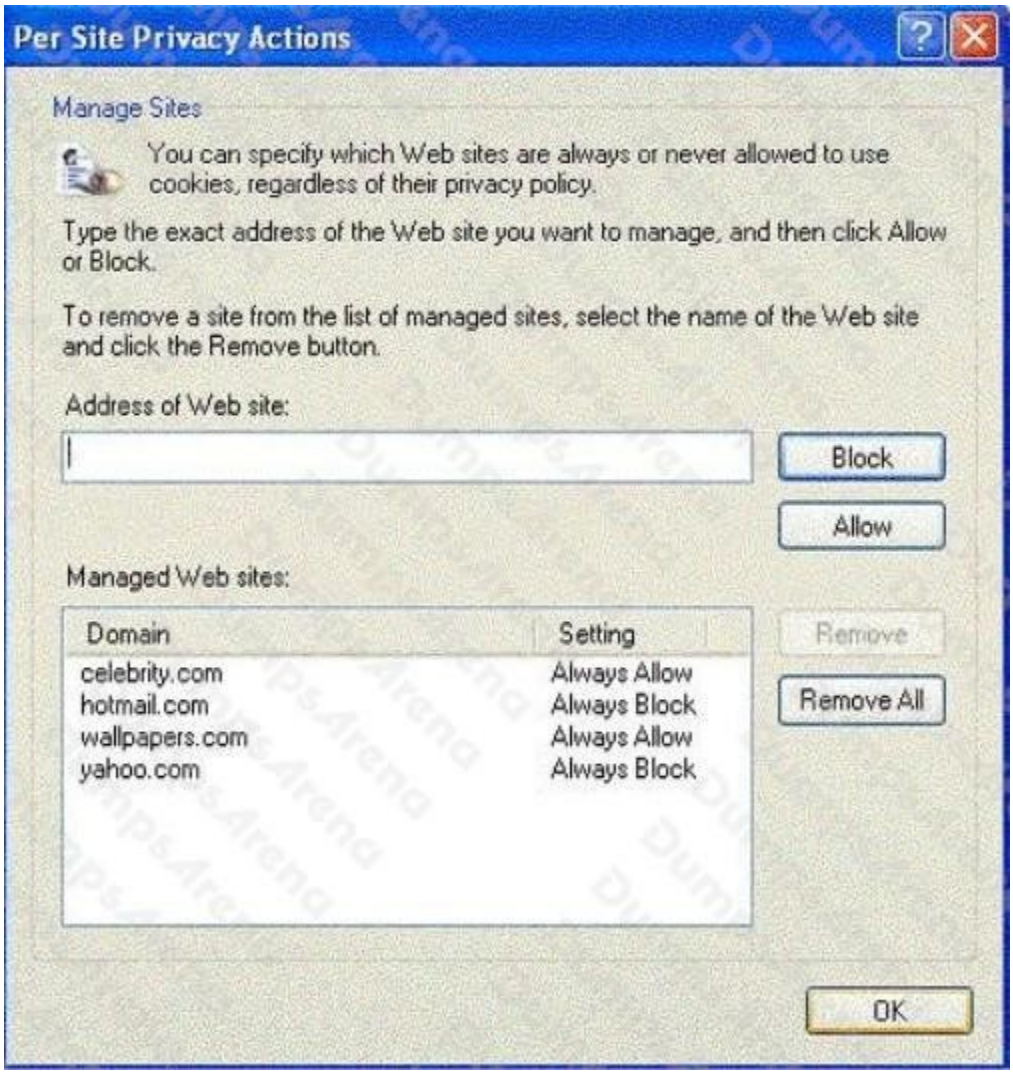
Administrative controls, also called managerial controls, govern how an organization directs, manages, and oversees security through people, processes, and documented expectations. **Security policy** is an administrative control because it establishes management-approved security requirements, responsibilities, and rules for organizational behavior. **Security awareness training** is administrative because it equips personnel to follow those requirements and recognize their security responsibilities. **Auditing** is also an administrative control when used as a governance and oversight activity: it evaluates whether policies, procedures, and security requirements are being followed, identifies gaps, and supports management accountability and corrective action.

This classification is consistent with NIST's use of management controls, which focus on managing risk and establishing security governance, including policy, training, assessment, and oversight activities. Auditing provides evidence for those management decisions and for ongoing compliance monitoring. See NIST SP 800-53 Rev. 5, especially its Program Management and Assessment, Authorization, and Monitoring control families: NIST SP 800-53 Rev. 5. NIST also describes awareness and training as an essential organizational security function: NIST Awareness and Training.

QUESTION NO: 22

John works as a Website Administrator in ABC Inc. The users of the company always use Internet Explorer for Web browsing. One of the users opens the Privacy tab page in the Internet Options dialog box and configures the privacy settings for the Internet zone as displayed in the following images:


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Move the slider to select a privacy setting for the Internet zone.
Medium High
- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your explicit consent
- Blocks first-party cookies that use personally identifiable information without implicit consent
Import...
Advanced...
Default
Web Sites
To override cookie handling for individual Web sites, click the Edit button.
Edit...
OK
Cancel
Apply



Which of the following statements regarding the configurations are true?

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

A. John has specifically blocked some websites from using cookies.

B. John has set a privacy policy for websites in the Internet zone.

C. John has specifically allowed some websites to use cookies.

D. Hotmail.com and Yahoo.com will not use cookies regardless of their privacy policy.

ANSWER: A B C D

Explanation:

The displayed Internet Explorer Privacy-tab configuration combines a zone-wide cookie policy with site-specific exceptions. The Internet-zone privacy setting is a policy applied to websites by default, so it constitutes a configured privacy policy for sites in that zone. Internet Explorer's Privacy settings control how cookies are handled, including cookies with compact privacy policies and cookies lacking a suitable policy.

The per-site settings shown in the images explicitly create exceptions for named domains. A site entered with the Block action is specifically prevented from using cookies, while a site entered with the Allow action is specifically permitted to use cookies. These exceptions are evaluated as direct administrator or user choices for the listed sites rather than relying solely on the site's declared privacy behavior.

Because Hotmail.com and Yahoo.com are listed as blocked sites in the displayed per-site privacy configuration, their cookies are blocked regardless of what privacy policy either site publishes. This is the practical purpose of the per-site exception list: it permits explicit cookie decisions for individual domains while retaining a general privacy policy for all other Internet-zone

websites. Microsoft describes cookie controls and per-site cookie exceptions in its Internet Explorer privacy documentation: Manage cookies in Internet Explorer and Internet Explorer privacy settings reference.

QUESTION NO: 23

Which of the following processes is described in the statement below?

"This is the process of numerically analyzing the effect of identified risks on overall project objectives."

A. Identify Risks

B. Perform Quantitative Risk Analysis

C. Monitor and Control Risks

D. Perform Qualitative Risk Analysis

ANSWER: B

Explanation:

Perform Quantitative Risk Analysis is correct because it evaluates identified project risks using numerical methods to determine their potential effect on project objectives, such as cost, schedule, scope, or performance. This process commonly applies probability distributions, expected monetary value, decision-tree analysis, sensitivity analysis, simulation, or quantitative modeling to estimate the likelihood and magnitude of risk outcomes. The resulting analysis gives leadership objective, measurable information for prioritizing risk responses, establishing contingency reserves, and making informed decisions where uncertainty could materially affect the project.

The wording in the question closely matches the Project Management Institute definition: quantitative risk analysis is the process of numerically analyzing the combined effect of identified individual project risks and other sources of uncertainty on overall project objectives. Unlike an initial descriptive assessment, this process produces numerical estimates that support planning and governance decisions. See PMI's overview of project risk management at PMI: Project Risk Management and the risk-analysis guidance from the U.S. Government Accountability Office at GAO Cost Estimating and Assessment Guide.

QUESTION NO: 24

What does noise in a power line indicate?

A. Power degradation that is low and less than normal

B. Interference superimposed onto the power line

C. Momentary high voltage

D. Prolonged loss of power

ANSWER: B

Explanation:

Noise in a power line indicates unwanted electrical interference superimposed on the normal power signal. Rather than representing an intended change in the supply voltage, this interference consists of irregular electrical disturbances that can be introduced by sources such as switching equipment, motors, radio-frequency emissions, nearby electrical circuits, or lightning-related effects. In an information-security and continuity context, power-line noise matters because sensitive electronic equipment may interpret or be affected by these disturbances, potentially causing data errors, communications problems, unexpected behavior, or equipment damage when protection is inadequate.

Power-quality terminology distinguishes noise from events such as sags, surges, and outages based on the nature and duration of the disturbance. The U.S. Department of Energy describes electrical noise as unwanted disturbances that affect electrical systems and equipment, while NIST guidance recognizes the need for power conditioning and electromagnetic-interference controls to protect information-system components. Appropriate mitigations can include properly selected

uninterruptible power supplies, line conditioners, surge protective devices, filtering, grounding, and shielding, chosen according to the operational environment and the criticality of the systems being protected. See the U.S. Department of Energy power-quality overview and NIST SP 800-53 Rev. 5.

QUESTION NO: 25

Joseph works as a Network Administrator for WebTech Inc. He has to set up a centralized area on the network so that each employee can share resources and documents with one another. Which of the following will he configure to accomplish the task?

A. VPN

B. Intranet

C. Extranet

D. WEP

ANSWER: B

Explanation:

Intranet is correct because it is a private network environment intended for use within an organization. It provides employees with a centralized internal location to access, publish, and share organizational resources, such as documents, policies, internal applications, team sites, announcements, and collaboration tools. Access is normally limited to authorized personnel through corporate network connectivity and identity-based authentication, allowing the organization to apply consistent permissions and security controls.

For WebTech Inc., an intranet directly meets the requirement to make resources and documents available among employees. A network administrator can implement it using an internal web portal, document-management platform, file-sharing service, or collaboration system, while managing access through groups and role-based permissions. This creates a controlled workspace that supports internal communication and information sharing without making those materials generally available to external users. NIST's glossary describes an intranet as a private network based on Internet technologies that is accessible only to authorized users: NIST Computer Security Resource Center. Microsoft's guidance on SharePoint also illustrates a common intranet implementation for sharing organizational content and resources: Microsoft Support.

QUESTION NO: 26

Which of the following are the countermeasures against a man-in-the-middle attack? Each correct answer represents a complete solution. Choose all that apply.

A. Using Off-channel verification.

B. Using Secret keys for authentication.

C. Using basic authentication.

D. Using public key infrastructure authentication.

ANSWER: A B D

Explanation:

A man-in-the-middle attack succeeds when an attacker can impersonate one endpoint to the other, alter exchanged messages, or establish separate sessions while appearing to be a trusted party. **Using Off-channel verification.** is a countermeasure because parties can validate a certificate fingerprint, public-key fingerprint, or session-verification value through a separate trusted path, such as an authenticated phone call or in-person comparison. This prevents reliance solely on the channel that may be under interception.

Using Secret keys for authentication. provides a countermeasure when the communicating parties use a pre-shared secret in a cryptographically secure authentication protocol, such as a message authentication code or authenticated key exchange. The attacker cannot successfully impersonate a party without possession of that secret.

Using public key infrastructure authentication. counters interception by binding a public key to an authenticated identity through certificates and validating the certificate chain, identity, validity period, and revocation status as appropriate. TLS uses this model to authenticate endpoints and establish protected sessions. NIST describes authenticated key establishment and the role of key confirmation in preventing impersonation in SP 800-56A Rev. 3. For practical TLS certificate validation requirements, see RFC 5280.

QUESTION NO: 27

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. John notices that the We-are-secure network is vulnerable to a man-inthe-middle attack since the key exchange process of the cryptographic algorithm it is using does not authenticate participants. Which of the following cryptographic algorithms is being used by the Weare-secure server?

A. RSA

B. Diffie-Hellman

C. Twofish

D. Blowfish

ANSWER: B

Explanation:

Diffie-Hellman is correct because its basic key-agreement protocol lets two parties derive a shared secret over an untrusted network without inherently verifying either party's identity. An active attacker positioned between the endpoints can establish one Diffie-Hellman exchange with each endpoint, creating separate shared secrets and relaying or modifying traffic. This is the classic man-in-the-middle risk associated with unauthenticated Diffie-Hellman key exchange. Authentication must therefore be added through a mechanism such as digital signatures, certificates, or a pre-shared authentication method. In modern TLS, ephemeral Diffie-Hellman key agreement is normally authenticated by the server's certificate and signature; the key exchange alone is not the identity proof. The NIST guidance on key-establishment schemes describes Diffie-Hellman-style schemes and the role of key confirmation and authentication in securely establishing keys. RFC 2631 also specifies Diffie-Hellman key agreement and notes that unauthenticated exchanges are susceptible to active attacks. See NIST SP 800-56A Rev. 3 and RFC 2631: Diffie-Hellman Key Agreement Method.

QUESTION NO: 28

Which of the following work as traffic monitoring tools in the Linux operating system?

Each correct answer represents a complete solution. Choose two.

A. IPTraf

B. Hotspotter

C. Ntop

D. John the Ripper

ANSWER: A C

Explanation:

IPTraf and Ntop are Linux-capable network-traffic monitoring tools. IPTraf is an interactive, console-based utility for observing IP traffic in real time. It provides views such as per-interface traffic statistics, TCP and UDP connection information, packet counts, and protocol-level activity. This makes it useful to an administrator or security analyst who needs

to inspect current network behavior directly from a Linux host. The maintained IPTraf-ng project describes itself as an IP traffic monitoring tool and documents these operational monitoring capabilities at IPTraf-ng on GitHub.

Ntop is designed for network observation and traffic analysis, presenting network usage and flow information in a more comprehensive interface. Its modern implementation, ntopng, monitors traffic, analyzes flows, identifies active hosts and protocols, and provides web-based reporting that supports operational visibility and security monitoring. These capabilities make Ntop appropriate for monitoring traffic traversing or observed by a Linux system. The ntop project documentation describes its traffic-monitoring and flow-analysis functionality at ntopng User's Guide. Together, IPTraf and Ntop represent established tools for inspecting and monitoring network traffic on Linux.

QUESTION NO: 29

Which of the following refers to the process of verifying the identity of a person, network host, or system process?

A. Auditing

B. Packet filtering

C. Authentication

D. Hacking

ANSWER: C

Explanation:

Authentication is the process of verifying that a claimed identity is genuine. A person may authenticate with something they know, such as a password or PIN; something they have, such as a hardware token or smart card; or something they are, such as a biometric characteristic. The same concept applies to technical entities: a network host or system process can prove its identity through mechanisms such as cryptographic keys, digital certificates, signed tokens, or mutual Transport Layer Security authentication.

Authentication establishes confidence in *who* or *what* is attempting to access a resource. It is a foundational security control because subsequent decisions, including authorization and accountability, depend on a reliably established identity. In practice, strong authentication commonly combines independent factors and protects authentication exchanges using secure, cryptographically sound protocols. NIST defines authentication as the process of determining the validity of one or more credentials used to claim a digital identity; its Digital Identity Guidelines describe these concepts and associated assurance considerations. See NIST SP 800-63-3: Digital Identity Guidelines and NIST CSRC: Authentication.

QUESTION NO: 30

Which of the following is a complete indexed set of records of the procurement process incorporated into the administrative closure process?

A. Contract file

B. Required resources and skills

C. Required actions to complete the project scope

D. Description of the work packages

ANSWER: A

Explanation:

Contract file is the correct answer because it is the organized, indexed repository of records created and maintained throughout a procurement. It normally contains the procurement documentation needed to demonstrate how the supplier was selected, what was agreed, how the contract was administered, what changes were approved, and how performance and acceptance were documented. Typical contents include the procurement statement of work, source-selection

documentation, the signed contract and amendments, correspondence, invoices and payment records, inspection or acceptance records, and dispute-resolution documentation.

During administrative closure, these records are reviewed to verify that all contractual obligations have been fulfilled, outstanding claims or issues have been resolved, final acceptance has been obtained, and the procurement can be formally closed. Maintaining a complete contract file supports auditability, legal defensibility, financial accountability, lessons learned, and organizational record-retention requirements. This aligns with the project-procurement practice of retaining complete procurement records through contract closure and with federal acquisition guidance requiring agencies to establish and maintain contract files containing the records of contractual actions. See the Federal Acquisition Regulation, 4.801—Contract Files and the PMI PMBOK Guide and Standards resources.

QUESTION NO: 31

You work as a Network Administrator for McNeil Inc. The company has a Windows Active Directorybased single domain single forest network. The functional level of the forest is Windows Server 2003. The company's management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks:

□□The wireless network communication should be secured.

□□The laptop users should be able to use smart cards for getting authenticated.

In order to accomplish the tasks, you take the following steps:

□□Configure 802.1x and WEP for the wireless connections.

□□Configure the PEAP-MS-CHAP v2 protocol for authentication

What will happen after you have taken these steps?

A. Both tasks will be accomplished.

B. The wireless network communication will be secured.

C. None of the tasks will be accomplished.

D. The laptop users will be able to use smart cards for getting authenticated.

ANSWER: B

Explanation:

The wireless network communication will be secured. IEEE 802.1X supplies port-based access control for the wireless connection: the client must successfully authenticate through the authentication infrastructure before normal network access is granted. When 802.1X is used with WEP in this Windows Server 2003-era design, the authentication process can provide dynamically generated WEP keys rather than relying solely on one static, manually shared key. This delivers protected wireless communications and helps limit access to authenticated wireless clients.

PEAP provides a protected TLS tunnel between the wireless client and authentication server, and PEAP with MS-CHAP v2 uses credentials within that tunnel. Thus, the stated configuration implements authenticated, protected wireless access. Microsoft’s documentation describes PEAP as a method that creates a protected channel for an inner authentication method, including MS-CHAP v2, and identifies its use in network access authentication. See Microsoft Learn: NPS certificate management and Microsoft Learn: Manage Network Access Protection.

QUESTION NO: 32

Ned is the program manager for his organization and he's considering some new materials for his program. He and his team have never worked with these materials before and he wants to ask the vendor for some additional information, a demon, and even some samples. What type of a document should Ned send to the vendor?

A. IFB

B. RFI

C. RFP

D. RFQ

ANSWER: B

Explanation:

RFI is correct because Ned is still conducting preliminary market research rather than soliciting a binding offer or selecting a supplier. A Request for Information is used to obtain general information from potential vendors about available products, capabilities, technical approaches, and market practices. In this situation, the team has not previously worked with the materials and needs to improve its understanding before defining detailed requirements or making a procurement decision. Asking for additional product information, a demonstration, and samples is consistent with this information-gathering stage. Vendor responses can help Ned assess whether the materials are suitable, identify feasible specifications, compare available capabilities, and shape a later acquisition strategy. In government and commercial procurement practice, RFIs support market research and planning; they are generally not requests for priced proposals and do not create an award commitment. The Federal Acquisition Regulation describes agencies' use of market research to determine what products and capabilities are available before developing requirements, including contacts with knowledgeable industry sources. See FAR 10.002—Procedures for Conducting Market Research. The General Services Administration likewise describes an RFI as a market-research tool used to collect information from industry before issuing a formal solicitation: GSA Market Research.

QUESTION NO: 33

You see the career section of a company's Web site and analyze the job profile requirements. You conclude that the company wants professionals who have a sharp knowledge of Windows server 2003 and Windows active directory installation and placement. Which of the following steps are you using to perform hacking?

A. Covering tracks

B. Scanning

C. Gaining access

D. Reconnaissance

ANSWER: D

Explanation:

Reconnaissance is correct because reviewing a company's publicly accessible careers page is a passive information-gathering activity performed before attempting to interact with, probe, or access its systems. Job postings can reveal useful organizational and technical context, such as operating systems, directory services, enterprise platforms, cloud providers, security products, development languages, and the skills associated with teams that operate particular environments. In this case, references to Windows Server 2003 and Active Directory installation and placement indicate that the organization may operate, support, or have legacy familiarity with Microsoft Windows domain infrastructure. This kind of open-source intelligence helps a security professional understand the target environment, identify areas that may warrant authorized assessment, and build an initial profile without sending traffic to the organization's infrastructure. It is therefore part of the early reconnaissance phase commonly described in penetration-testing and adversary-emulation methodologies. The MITRE ATT&CK technique for Search Open Websites/Domains specifically recognizes gathering information from publicly available websites as a reconnaissance activity. Ethical security work must ensure that any follow-on testing occurs only with explicit authorization and within the defined scope of engagement. See MITRE ATT&CK: Search Open Websites/Domains and NIST SP 800-115: Technical Guide to Information Security Testing and Assessment.

QUESTION NO: 34

Which of the following are based on malicious code?

Each correct answer represents a complete solution. Choose two.

A. Trojan horse

B. Worm

C. Biometrics

D. Denial-of-Service (DoS)

ANSWER: A B

Explanation:

Trojan horse and worm are both categories of malicious code, commonly called malware. A Trojan horse is malicious software that presents itself as legitimate or useful software in order to induce a user to run it. Its harmful functionality is therefore delivered through code executed on the target system. A worm is also malicious code, but it is distinguished by its ability to self-replicate and spread across systems or networks, typically without requiring a user to attach it to another program or manually distribute it. Both threats can be used to compromise confidentiality, integrity, or availability, including by installing additional payloads, stealing information, altering systems, or enabling unauthorized access. The U.S. Cybersecurity and Infrastructure Security Agency describes malware as software intentionally designed to cause damage or gain unauthorized access and identifies Trojans and worms among common malware forms. NIST similarly defines malicious code as software or firmware intended to perform an unauthorized process that adversely affects confidentiality, integrity, or availability. See CISA's malware guidance and NIST's definition of malicious code.

QUESTION NO: 36

Which of the following tools can be used for stress testing of a Web server? Each correct answer represents a complete solution. Choose two.

A. Internet bots

B. Spyware

C. Anti-virus software

D. Scripts

ANSWER: A D

Explanation:

Internet bots and scripts can both be used to perform authorized Web-server stress testing because they automate repeated HTTP requests and can simulate many concurrent clients. A bot is an automated Internet client; when configured and used with explicit authorization, it can repeatedly crawl, request, or interact with Web resources at controlled rates. This helps a test team observe how the server, application, network path, and supporting services behave as request volume and concurrency increase.

Scripts provide an especially flexible way to generate test traffic. They can issue requests, maintain sessions, submit forms, vary parameters, introduce delays, and run multiple workers in parallel. A script may also be used to drive dedicated load-testing software or cloud-based test runners. The important governance requirement is that testing has defined scope, rate limits, monitoring, and written authorization, since uncontrolled automated traffic can disrupt production services. Modern testing platforms such as Apache JMeter support scripted test plans, concurrent virtual users, and HTTP request generation; see the Apache JMeter User Manual. OWASP also identifies availability and resilience testing as an important security-testing consideration; see the OWASP Web Security Testing Guide.

QUESTION NO: 37

Which of the following statements about IPSec are true?

Each correct answer represents a complete solution. Choose two.

A. It uses Internet Protocol (IP) for data integrity.

B. It uses Authentication Header (AH) for data integrity.

C. It uses Password Authentication Protocol (PAP) for user authentication.

D. It uses Encapsulating Security Payload (ESP) for data confidentiality.

ANSWER: B D

Explanation:

"It uses Authentication Header (AH) for data integrity." is correct because AH is an IPsec protocol designed to provide connectionless integrity and data-origin authentication for protected IP packets. AH accomplishes this by applying an integrity check over the applicable packet content, enabling a receiving system to detect unauthorized modification in transit. In an IPsec security architecture, integrity protection is negotiated and applied through Security Associations, with algorithms and keys selected under the relevant IPsec policy and key-management arrangements.

"It uses Encapsulating Security Payload (ESP) for data confidentiality." is also correct because ESP provides confidentiality by encrypting the protected payload. ESP can be used in transport mode to protect upper-layer data or in tunnel mode to protect an entire inner IP packet, making it fundamental for encrypted VPN traffic. ESP also supports optional integrity and authentication services, but its defining security service in this statement is encryption-based confidentiality. The IPsec architecture identifies AH and ESP as the protocols used to provide these packet-level security services. See the IETF's Security Architecture for the Internet Protocol and IP Encapsulating Security Payload.

QUESTION NO: 38

John works as a professional Ethical Hacker. He has been assigned the task of testing the security of www.we-are-secure.com. He installs a sniffer on the We-are-secure server thinking that the following protocols of the We-are-secure server are being used in the network:

- HTTP
- SSL
- SSH
- IPSec

Considering the above factors, which of the following types of packets can he expect to see captured in encrypted form when he checks the sniffer's log file?

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

A. SSH

B. SSL

C. HTTP

D. IPSec

ANSWER: A B D

Explanation:

Packets associated with SSH, SSL, and IPSec can be expected to appear encrypted in a network sniffer capture because these technologies are designed to provide confidentiality for data in transit. SSH establishes an encrypted channel for remote administration, command execution, tunneling, and file-transfer-related traffic after its cryptographic negotiation completes. SSL—now generally deployed as TLS—encrypts application traffic carried inside the established TLS session, such as protected web traffic. IPSec applies cryptographic protection at the network layer; its Encapsulating Security Payload mechanism commonly provides encryption of the protected IP payload, while the precise visible packet structure depends on tunnel or transport mode. A sniffer can still capture packet headers, session negotiation metadata, and encrypted ciphertext, but it cannot recover protected content without appropriate session keys or a successful decryption capability. In contrast, ordinary HTTP does not itself encrypt its request and response contents; protection for web traffic

requires HTTP to be carried over TLS, commonly called HTTPS. These distinctions are central when assessing which protocols protect confidentiality against passive packet capture. See the SSH Transport Layer Protocol specification and NIST's Guide to IPsec VPNs.

QUESTION NO: 40

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to use Kismet as a wireless sniffer to sniff the We-are-secure network. Which of the following IEEE-based traffic can be sniffed with Kismet?

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

A. 802.11g

B. 802.11a

C. 802.11b

D. 802.11n

ANSWER: A B C D

Explanation:

Kismet is a passive wireless detection and packet-capture platform that supports monitoring IEEE 802.11 Wi-Fi traffic when it is used with a compatible wireless adapter and the adapter is configured for monitor mode. Therefore, 802.11a, 802.11b, 802.11g, and 802.11n traffic can all be sniffed by Kismet. These standards cover the major legacy and high-throughput Wi-Fi PHY families across the 2.4 GHz and 5 GHz bands. Kismet can identify wireless networks, observe management and control activity, collect packets, and save captures for subsequent analysis. Practical capture capability depends on the radio hardware, installed driver, supported frequency bands, channel width, and monitor-mode support; for example, a 2.4 GHz-only adapter cannot capture a 5 GHz 802.11a network. That hardware constraint does not change Kismet's support for the listed IEEE 802.11 traffic types when suitable capture hardware is available. Kismet's documentation describes its Wi-Fi capture architecture and the need for supported capture sources, while its supported-hardware guidance explains that available features depend on the specific chipset and driver. See the Kismet introduction documentation and Kismet Linux Wi-Fi capture-source documentation.

QUESTION NO: 41

Which of the following statements are true about MS-CHAPv2?

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

A. It can be replaced with EAP-TLS as the authentication mechanism for PPTP.

B. It provides an authenticator-controlled password change mechanism.

C. It is subject to offline dictionary attacks.

D. It is a connectionless protocol.

ANSWER: A B C

Explanation:

MS-CHAPv2 is a challenge-response authentication protocol commonly used with PPP-based access technologies. PPTP transports PPP frames, allowing PPP authentication to be negotiated independently of the tunneling mechanism. Consequently, EAP-TLS can be used in place of MS-CHAPv2 for PPTP authentication where the client and server support certificate-based EAP authentication. EAP-TLS provides mutual certificate authentication and derives keying material as part of the EAP exchange.

MS-CHAPv2 also defines an authenticator-controlled password-change capability. The protocol includes password-change packets and procedures that allow a user to change an expired password during authentication rather than requiring a separate, completed session before changing it. This capability is specified in the MS-CHAPv2 protocol definition.

Finally, captured MS-CHAPv2 exchanges can be subjected to offline password-guessing or dictionary attacks, particularly when user passwords are weak. The challenge, response, and account identifier provide material an attacker can test against candidate passwords without continually interacting with the authenticating server. This risk is why modern security guidance generally favors stronger, phishing-resistant authentication such as certificate-based methods.

See RFC 2759: Microsoft PPP CHAP Extensions, Version 2 and RFC 2637: Point-to-Point Tunneling Protocol.

QUESTION NO: 42

Which of the following federal laws are related to hacking activities? Each correct answer represents a complete solution. Choose three.

A. 18 U.S.C. 2510

B. 18 U.S.C. 1029

C. 18 U.S.1028

D. 18 U.S.C. 1030

ANSWER: A B D

Explanation:

18 U.S.C. 2510 is related to hacking because it begins the federal statutory framework governing interception of wire, oral, and electronic communications. Unauthorized interception or capture of electronic communications is a common component of intrusion and surveillance activity addressed by federal computer-crime investigations. The definitions and framework are available in the U.S. House Office of the Law Revision Counsel text of 18 U.S.C. 2510.

18 U.S.C. 1029 addresses fraud and related activity involving access devices, including unauthorized access devices and related trafficking or fraudulent use. Compromised payment-card data, account credentials, and other access-device information can result from or be used in hacking activity, making this provision relevant to such offenses.

18 U.S.C. 1030 is the principal federal computer-crime statute, commonly called the Computer Fraud and Abuse Act. It prohibits specified unauthorized access to protected computers, obtaining information through unauthorized access, computer-related fraud, damage, and related conduct. Its scope directly covers core hacking behaviors and is set out in the current statutory text for 18 U.S.C. 1030.

QUESTION NO: 43 - (SIMULATION)

Fill in the blank with the appropriate word.

_____ is also used to refer to any attempt to circumvent the security of other types of cryptographic algorithms and protocols in general, and not just encryption.

ANSWER: See the explanation for the answer

Explanation:

Answer: `Cryptanalysis`

Cryptanalysis refers broadly to attempts to defeat or circumvent the security of cryptographic algorithms and protocols, not only to breaking encryption.

QUESTION NO: 45

Which of the following is NOT an input of the Administer Procurements process?

A. Contract

B. Requirements traceability matrix

C. Procurement management plan

D. Procurement documents

E. Work performance information

ANSWER: E

Explanation:

Work performance information is correct because it is produced by the Administer Procurements process rather than supplied to it. Administer Procurements involves managing the buyer-seller relationship, monitoring contract performance, handling contract changes, and documenting procurement activities. The process analyzes available performance data—such as information about deliverable status, schedule progress, costs, and technical performance—and turns that analysis into work performance information for communication and decision-making. This information can then support project monitoring and control, stakeholder reporting, and necessary change actions.

This distinction reflects PMI's input/output model: data are raw observations and measurements available to a process, whereas information is the analyzed and contextualized result of processing that data. In the PMBOK process model that uses the name "Administer Procurements," work performance data are an input, while work performance information is an output. PMI's current standards have evolved toward principle- and performance-domain-based guidance, but this terminology remains important when interpreting process-based exam questions. See PMI's PMBOK Guide and Standards overview and the PMI Lexicon of Project Management Terms for PMI terminology.

QUESTION NO: 46

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

Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company's headquarters is located at Los Angeles. A branch office of the company is located at Denver. You are about to send a message to Rick who is a Network Administrator at Denver. You want to ensure that the message cannot be read by anyone but the recipient. Which of the following keys will you use to encrypt the message?

A. The recipient's public key

B. Your private key

C. The recipient's private key

D. Your public key

ANSWER: A

Explanation:

The recipient's public key is used to encrypt a confidential message intended solely for that recipient. Public-key cryptography uses a mathematically related key pair: a public key that can be distributed to senders and a private key that remains under the recipient's exclusive control. When the sender encrypts message content with the recipient's public key, only the corresponding recipient private key can decrypt it. This provides the required confidentiality even when the message traverses networks or mail systems that other users or administrators may access.

In an Active Directory environment, certificates and public keys can be published through directory services or obtained from a trusted certification authority. This lets the sender locate and validate the recipient's encryption certificate before protecting the message. In practice, email encryption systems commonly use hybrid encryption: the sender encrypts the message with

a temporary symmetric content-encryption key, then encrypts that temporary key with the recipient's public key. The essential asymmetric-key principle remains the same: access to the recipient's private key is required to recover the protected content. NIST describes the distinct confidentiality roles of public and private keys in its Key Management Guidelines. Microsoft also documents certificate-based encryption concepts in Understanding Public Key Infrastructure.

QUESTION NO: 47

Which of the following statements about Digest authentication are true? Each correct answer represents a complete solution. Choose two.

A. Digest authentication is a more secure authentication method as compared to Basic authentication.

B. In Digest authentication, passwords are sent across a network as clear text, rather than as a has value.

C. Digest authentication is used by wireless LANs, which follow the IEEE 802.11 standard.

D. In Digest authentication, a hash-based digest response is sent across the network rather than the password as clear text.

ANSWER: A D

Explanation:

Digest authentication is more secure than Basic authentication because it does not transmit a user's password in directly decodable Base64 form with every request. Instead, the client proves knowledge of the password by calculating a digest response using inputs such as the username, realm, server nonce, request method, requested URI, and a password-derived value. The server validates that response without receiving the plaintext password over the network. This challenge-response design also lets the server issue a nonce, helping tie the authentication response to a specific challenge and reducing straightforward replay exposure when the protocol is implemented appropriately.

The statement that passwords are sent as a hash value rather than as clear text is correct in the intended sense: HTTP Digest authentication sends a calculated digest response, not the plaintext password. More precisely, the transmitted value is a hash-based response derived from password-related material and request-specific challenge data; it is not simply a standalone hash of the password. RFC 7616 defines this Digest access authentication framework and its challenge-response calculations. Modern deployments should still protect HTTP traffic with TLS, since Digest authentication alone does not provide full confidentiality or comprehensive protection for all request content. See RFC 7616: HTTP Digest Access Authentication and MDN Web HTTP authentication.

QUESTION NO: 48 - (SIMULATION)

SIMULATION

Fill in the blank with the appropriate word.

A_____ is a computer system on the Internet that is expressly set up to attract and trap people who attempt to penetrate other people's computer systems.

ANSWER: See the explanation for the answer

Explanation:

Answer: `honeypot`

A honeypot is a deliberately deployed computer system or service designed to attract, detect, and trap unauthorized attackers attempting to penetrate systems.

QUESTION NO: 50

Which of the following are outputs of the Direct and Manage Project Execution process? Each correct answer represents a complete solution. Choose all that apply.

A. Change requests

B. Deliverables

C. Project staff assignments

D. Work performance information

ANSWER: A B D

Explanation:

In the PMBOK process model that uses the name “Direct and Manage Project Execution,” **Change requests**, **Deliverables**, and **Work performance information** are outputs of the process. Directing and managing execution produces the completed products, services, or results identified by the project scope; these are the deliverables provided for review, acceptance, or transition. As work is carried out, the project team also collects and organizes execution results into work performance information, allowing project leadership to understand how the work is progressing and to support subsequent monitoring and controlling activities.

The execution process may also identify needed modifications to scope, schedule, cost, quality, resources, or other controlled project elements. Those requested modifications are formally recorded as change requests and routed through the project’s integrated change-control approach. These outputs reflect the central purpose of execution: perform authorized work, create the planned results, communicate meaningful performance status, and initiate controlled changes when necessary. PMI’s historical process terminology and process-group framework are documented in its PMBOK® Guide—Fifth Edition; PMI’s current standards resources are available through the PMI Standards and Publications page.

QUESTION NO: 51

Which of the following statements are true about WPA?

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

A. WPA provides better security than WEP.

B. Shared-key WPA is vulnerable to password cracking attacks if a weak passphrase is used.

C. WPA-PSK converts the passphrase into a 256-bit key.

D. WPA-PSK requires a user to enter an 8-character to 63-character passphrase into a wireless client.

ANSWER: A B C D

Explanation:

WPA provides better security than WEP because it was introduced as an interim improvement over WEP’s fundamentally weak protection model. WPA uses the Temporal Key Integrity Protocol to provide per-packet key mixing, a message-integrity mechanism, replay protection, and periodic rekeying. These measures significantly improve the protection of a wireless network compared with WEP’s static-key design.

Shared-key WPA is vulnerable to password cracking attacks if a weak passphrase is used because WPA-Personal derives authentication material from the network name and passphrase. An attacker that captures the applicable authentication exchange can make offline passphrase guesses; consequently, a long, unique, high-entropy passphrase is essential. WPA-PSK derives a 256-bit pairwise master key from the passphrase by using PBKDF2. For a text passphrase, WPA-Personal accepts an ASCII passphrase from 8 through 63 characters; implementations may also permit direct entry of a 64-hex-character preshared key. These details are specified in the Wi-Fi Alliance’s Wi-Fi security overview and discussed in NIST’s Guidelines for Securing Wireless Local Area Networks.

QUESTION NO: 52

Jacob is worried about sniffing attacks and wants to protect his SMTP transmissions from this attack. What can he do to accomplish this?

A. Use an SSL certificate.

B. Use EFS.

C. Use a proxy server.

D. Use a firewall.

ANSWER: A

Explanation:

Use an SSL certificate. In practice, SMTP servers use a certificate as part of TLS encryption, commonly negotiated through the STARTTLS SMTP extension or configured as implicit TLS. TLS establishes an encrypted channel between the sending client or mail server and the receiving mail server, so a person capturing packets on the network cannot read SMTP commands, message headers, credentials, or message content transmitted within that protected connection. The certificate also lets the connecting system authenticate the mail server's identity, helping ensure that the encryption is being established with the intended server rather than an impersonator.

For SMTP, the relevant modern terminology is TLS rather than the obsolete SSL protocol name; however, a certificate is the essential credential used by the SMTP TLS deployment described in the answer. RFC 3207 specifies the STARTTLS extension for SMTP and explains that it provides a means to start a TLS session over an SMTP connection. Proper protection requires configuring the server to offer TLS, using a valid certificate, and requiring or verifying TLS where policy supports it. See RFC 3207: SMTP Service Extension for Secure SMTP over Transport Layer Security and RFC 8314: Cleartext Considered Obsolete.

QUESTION NO: 53

Which of the following are the tools and techniques of the Plan Procurements process? Each correct answer represents a complete solution. Choose all that apply.

A. Contract types

B. Expert judgment

C. Probability and impact matrix

D. Make-or-buy analysis

ANSWER: A B D

Explanation:

In the PMBOK framework that uses the process name "Plan Procurements," **Contract types**, **Expert judgment**, and **Make-or-buy analysis** are procurement-planning tools and techniques. Contract types support selection of an appropriate contractual arrangement and allocation of responsibility and risk between the buyer and seller. The selected type—such as fixed-price, cost-reimbursable, or time-and-materials—must suit the scope's clarity, the degree of uncertainty, and the desired balance of cost and performance risk. Expert judgment brings relevant commercial, legal, technical, financial, and procurement experience into planning so that procurement decisions and documentation are realistic and compliant. Make-or-buy analysis is the structured assessment of whether the project team should obtain a product, service, or result externally or perform the work internally, considering capability, capacity, cost, schedule, risk, and strategic considerations. Together, these practices enable the project to define a viable procurement approach before soliciting sellers or awarding agreements. PMI's standards resources provide the broader process-group and knowledge-area context for procurement management; see the PMI standards and PMBOK Guide resources and PMI's project procurement management practices overview.

QUESTION NO: 54

Victor works as a professional Ethical Hacker for SecureNet Inc. He wants to use the Steganographic file system method to encrypt and hide some secret information. Which of the following disk spaces will he use to store this secret information?

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

A. Hidden partition

B. Dumb space

C. Slack space

D. Unused sectors

ANSWER: A C D

Explanation:

A steganographic file system conceals information by placing encrypted content in disk locations that are not normally presented as ordinary, visible files. **Hidden partition** is appropriate because a partition can be excluded from routine user views or use a non-obvious configuration, providing a separate area in which protected data can be stored. **Slack space** is also suitable: it is the residual space in the final allocated cluster of a file after the file's logical end. This area may contain data not displayed through ordinary file access, making it a traditional location for concealed information. **Unused sectors** can likewise hold hidden encrypted data because sectors that are not allocated to active filesystem objects are not ordinarily accessed as part of a user's files. The technique relies on recording both the encrypted payload and sufficient metadata or a recovery mechanism to locate its fragments later. These locations are relevant to forensic examinations because data can persist outside the logical contents of active files. NIST discusses the distinction between data residing in allocated and unallocated storage and the importance of handling residual data in NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization. The NIST Guide to Integrating Forensic Techniques into Incident Response also provides context on preserving and analyzing storage artifacts during investigations.

QUESTION NO: 55

Ryan wants to create an ad hoc wireless network so that he can share some important files with another employee of his company. Which of the following wireless security protocols should he choose for setting up an ad hoc wireless network?

Each correct answer represents a part of the solution. Choose two.

A. WEP

B. WPA-PSK

C. WPA2 -EAP

D. WPA-EAP

ANSWER: A B

Explanation:

WEP and WPA-PSK are the applicable choices for the ad hoc scenario described. An ad hoc wireless network is a peer-to-peer connection in which participating devices communicate directly, rather than through an access point-managed infrastructure. WEP was historically supported by ad hoc wireless implementations and uses a shared WEP key configured on every participating device. Although it is now cryptographically obsolete and should not be used when a stronger alternative is available, it is a valid legacy protocol choice in the context of this question.

WPA-PSK is also appropriate because it uses a pre-shared passphrase that both employees can configure locally before establishing the connection. This avoids the need for centralized account-based authentication and permits the two peers to protect traffic with a mutually configured secret. For practical use, the passphrase should be long, unique, and exchanged through a trusted channel. NIST describes the risks of WEP and recommends stronger wireless protections in its Guide to Securing Legacy IEEE 802.11 Wireless Networks. Microsoft's wireless-security guidance also distinguishes pre-shared-key authentication from centrally managed enterprise authentication: Network access authentication and EAP.

QUESTION NO: 56

Which of the following are examples of administrative controls that involve all levels of employees within an organization and determine which users have access to what resources and information?

Each correct answer represents a complete solution. Choose three.

A. Training and awareness

B. Employee registration and accounting

C. Network authentication

D. Encryption

E. Disaster preparedness and recovery plans

ANSWER: A B E

Explanation:

Administrative controls are management-directed safeguards implemented through policies, procedures, planning, personnel practices, and organizational governance. They rely on people following defined processes and therefore apply throughout the organization, from leadership to individual staff members. Training and awareness is an administrative control because it establishes the knowledge and expected behaviors employees need to protect information, recognize security responsibilities, and follow access-related policies. Employee registration and accounting supports administrative access management by ensuring that personnel are formally identified, assigned appropriate responsibilities, and tracked through organizational processes; this helps connect access decisions to an accountable individual. Disaster preparedness and recovery plans are also administrative controls because they document management-approved responsibilities, communications, recovery priorities, and actions for maintaining or restoring business operations following a disruptive event. These plans require coordinated participation across business, technical, and leadership functions. Together, these controls establish the governance and procedures through which access and information-handling responsibilities are administered. NIST describes awareness and training as an organizational security-control family and identifies contingency planning as a management control area; see NIST SP 800-53 Rev. 5. Personnel accountability and access governance are also consistent with the access-control and personnel-security principles in NIST Cybersecurity Framework 2.0.

QUESTION NO: 57

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. SARA

B. Snort

C. Tripwire

D. Samhain

ANSWER: B C D

Explanation:

Snort, **Tripwire**, and **Samhain** can each provide intrusion-detection capability on a Linux system, although they monitor different security-relevant events. Snort is widely deployed as a network intrusion detection system (NIDS). It inspects network traffic against rules and signatures and can generate alerts when observed packets or flows match known attack patterns, suspicious activity, or policy violations. Its alerting and rule-driven inspection model make it suitable for detecting attempted attacks directed at services on the protected environment.

Tripwire provides host-based intrusion detection through file-integrity monitoring. It establishes a trusted baseline for monitored files, directories, and system objects, then detects and alerts on unauthorized or unexpected changes. Such changes can be important indicators of compromise, including modified system binaries, altered configurations, or persistence mechanisms. Samhain is also a host-based intrusion detection system for Unix-like platforms. It supports integrity checking, centralized logging and alerting, and monitoring intended to identify suspicious changes on protected hosts. Together, these tools represent valid IDS approaches: network-event detection with Snort and host-integrity detection with Tripwire and Samhain. See the Snort project and the Tripwire file integrity monitoring overview.

QUESTION NO: 58

In which of the following attacks does an attacker create the IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system?

A. Polymorphic shell code attack

B. IP address spoofing

C. Cross-site request forgery

D. Rainbow attack

ANSWER: B

Explanation:

IP address spoofing is the correct answer because it specifically describes the deliberate creation or alteration of an IP packet so that its source-address field claims to be an address other than the system that actually transmitted the packet. This can conceal the sender's identity, make traffic appear to originate from a trusted host, or support certain denial-of-service and network reconnaissance techniques. The defining technical feature is manipulation of the source IP address in the network-layer packet header.

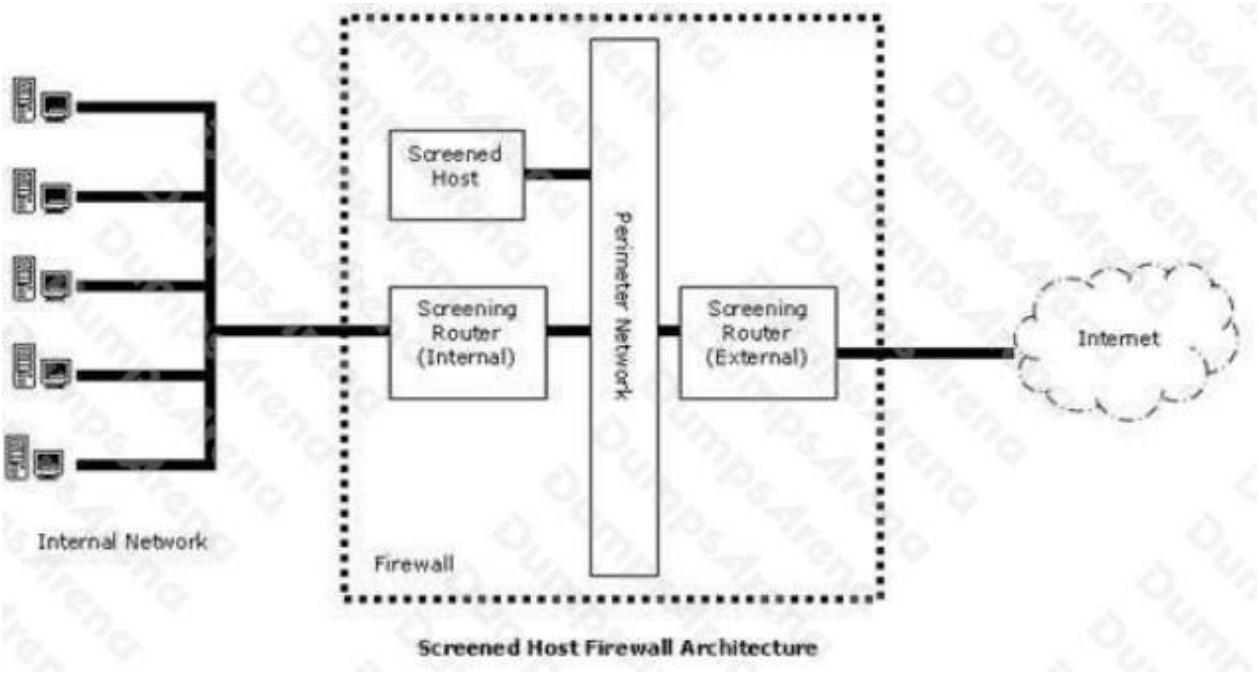
IP spoofing is particularly relevant where systems make trust decisions based on source addresses or where connectionless protocols permit packets to be sent without a completed handshake. Although modern networks commonly apply ingress and egress filtering to reduce spoofed traffic, organizations should still treat source IP information as potentially untrusted unless it is corroborated through appropriate network controls and protocol-level authentication. The Internet Engineering Task Force's guidance in BCP 38 describes filtering practices intended to prevent packets with forged source addresses from leaving networks. MITRE also documents IP spoofing-related adversary behavior as a technique used to obscure or manipulate the apparent origin of network communications.

QUESTION NO: 59 - (HOTSPOT)

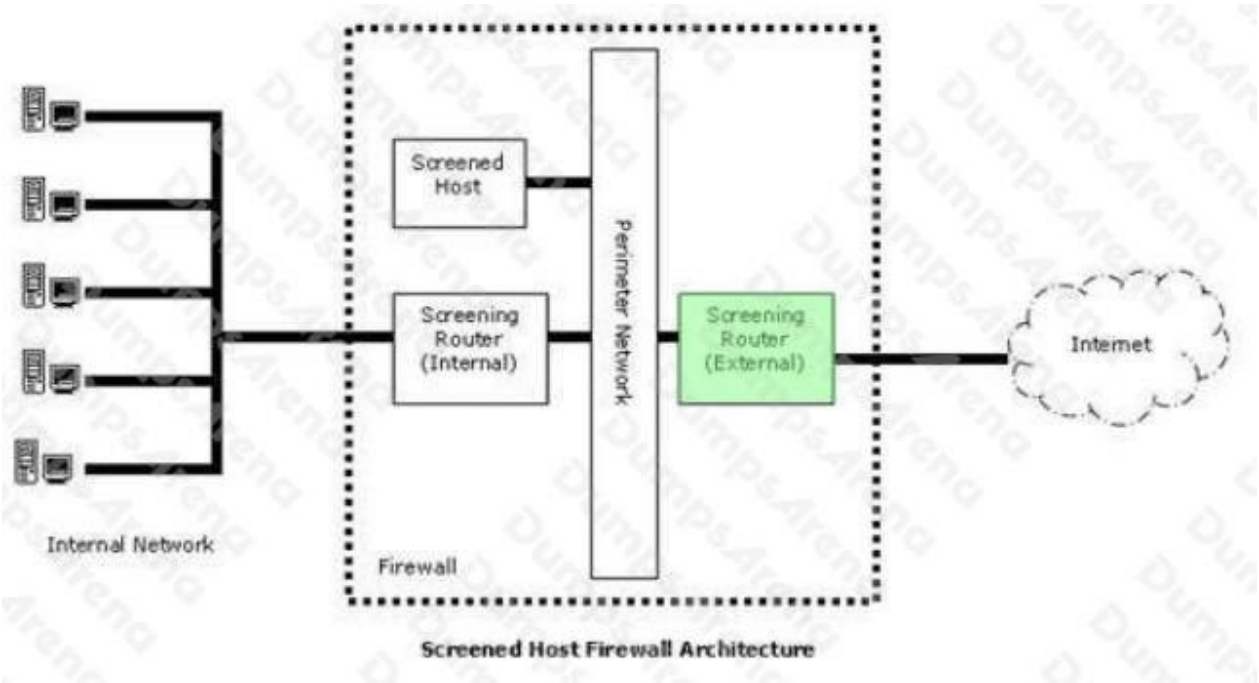
HOTSPOT

In the image of the Screened Host Firewall Architecture given below, select the element that is commonly known as the access router.

Hot Area:



ANSWER:



Explanation:

The access router in this screened host firewall diagram is the Internet-facing screening router. It is the network device positioned directly between the public Internet connection and the organization's perimeter network. Its role is to provide the external network access path while enforcing routing and packet-filtering policy at the boundary. In practical firewall architecture terminology, this router is often called the access router because it is the router through which external traffic accesses the protected environment.

Placing this device at the outer edge supports a layered-defense design. Traffic originating from the Internet encounters the access router first, allowing basic filtering rules to be applied before traffic is allowed toward the perimeter network, screened host, or internal network. This separation is important because it establishes a controlled ingress and egress point and limits which communications can proceed deeper into the architecture. The router's external placement also makes it the natural connection point for the organization's upstream Internet service.

The selected "Screening Router (External)" is therefore the correct component because it is visibly connected to the Internet cloud and serves as the outside boundary device for the screened host firewall architecture. NIST describes boundary

protection as monitoring and controlling communications at external boundaries; the Internet-facing access router contributes to that boundary-control function. See NIST's Boundary Protection glossary entry and NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy for firewall and network-boundary context.