PassQueen
a.k.a dumpsqueen.com

GIAC Security Essentials

GIAC GSEC

Version Demo

Total Demo Questions: 41

Total Premium Questions: 419

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Access Controls and Password Management	30
Topic 2, Active Defense	41
Topic 3, Cloud Security	11
Topic 4, Computer Networking	75
Topic 5, Cryptography	39
Topic 6, Cybersecurity Laws and Regulations	3
Topic 7, Incident Response	14
Topic 8, Linux Security	56
Topic 9, Network Security	57
Topic 10, Security Policy	34
Topic 11, Windows Security	53
Topic 12, Mix Questions	6
Total	419

QUESTION NO: 1

You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e-mails. Which of the following will you use to accomplish this?

A. PPTP

B. IPSec

C. PGP

D. NTFS

ANSWER: C

Explanation:

PGP is the appropriate choice because it is designed specifically to protect email content using public-key cryptography. A sender encrypts a message using the recipient's public key, and only the recipient who possesses the corresponding private key can decrypt it. PGP can also digitally sign email: the sender signs with a private key and recipients validate the signature using the sender's public key. This provides authentication, message integrity, and nonrepudiation in addition to confidentiality. In practice, OpenPGP is the open standard that defines interoperable PGP-style message encryption and signatures, including formats commonly used for email attachments and inline email protection. The Internet Engineering Task Force's OpenPGP standard describes how public-key-encrypted and signed data are represented and processed: RFC 9580: OpenPGP. The Electronic Frontier Foundation also provides practical background on using PGP to encrypt communications and verify identities through cryptographic keys and fingerprints: EFF: Introduction to Public-Key Cryptography and PGP. Therefore, PGP directly fulfills the company's requirement to encrypt email messages.

QUESTION NO: 2 - (SIMULATION)

Fill in the blank with the correct answer to complete the statement below.

The permission is the minimum required permission that is necessary for a user to enter a directory and list its contents.

ANSWER: See the explanation for the answer

Explanation:

The required directory permission is `read and execute` (`r-x`, numeric value `5`).

`r` allows the user to list the directory's contents.
`x` allows the user to enter/traverse the directory.

Therefore, the minimum permission to both enter a directory and list its contents is `r-x`.

QUESTION NO: 3

Which of the following statements about Hypertext Transfer Protocol Secure (HTTPS) are true? Each correct answer represents a complete solution. Choose two.

A. It uses TCP port 443 as the default port.

B. It is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure site.

C. It is a protocol used to provide security for a database server in an internal network.

D. It uses TCP port 80 as the default port.

ANSWER: A B

Explanation:

HTTPS uses TCP port 443 as its registered default port. The HTTPS URI scheme specifies that, when an explicit port is not included in the URL, the client connects using port 443. This conventional default lets browsers, proxies, firewalls, and web servers identify and route HTTPS traffic consistently. HTTPS is also the scheme used at the beginning of a web address—such as `https://www.example.com`—to indicate that the HTTP exchange is protected by Transport Layer Security (TLS). TLS authenticates the server through its certificate and provides confidentiality and integrity protection for data exchanged between the browser and the website, assuming certificate validation succeeds and a secure TLS configuration is used. In normal web use, entering or following an `https` URL directs the client to establish a TLS-protected connection before sending HTTP requests. The HTTPS URI scheme and its default port are defined by the HTTP standards, while browser documentation describes HTTPS as HTTP sent over TLS to secure communication with a website. See RFC 9110, HTTPS URI scheme and MDN Web Docs: HTTPS.

QUESTION NO: 4

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He wants to change the startup shell of Maria from bash to tcsh. Which of the following commands will John use to accomplish the task?

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

A. usermod -s /bin/tcsh maria

B. chage

C. usermod -u

D. useradd -s

E. chsh -s /bin/tcsh maria

ANSWER: A E

Explanation:

Changing an existing account's startup, or login, shell requires updating the shell field associated with that account in the local account database. `usermod -s /bin/tcsh maria` does this directly: the `-s` argument sets the user's login shell to the specified executable path. The shell should be installed and listed in `/etc/shells` where that policy is enforced. The `usermod` manual documents `-s, --shell SHELL` specifically as the setting that defines a user's new login shell. See usermod(8).

`chsh -s /bin/tcsh maria` is also a complete solution. The `chsh` utility is designed to change a user's login shell, and when run by root it can target Maria's account by name. Both commands persist the selected shell for future login sessions; they do not merely start an interactive tcsh process for the current terminal. The change takes effect when Maria begins a new login session. The expected behavior and syntax are described in the chsh(1) documentation.

QUESTION NO: 5

What database can provide contact information for Internet domains?

A. dig

B. who

C. who is

D. ns look up

ANSWER: C

Explanation:

The correct answer is **who is**, referring to the WHOIS service and its registration-record databases. WHOIS has historically provided query access to domain-registration data maintained by registries and registrars. Depending on the top-level domain, a WHOIS query may return information such as the sponsoring registrar, registration and expiration dates, authoritative name servers, domain status codes, and registrant, administrative, technical, or abuse contact details. This makes it useful during security investigations, incident response, asset discovery, and basic domain attribution, because analysts can identify the organization or registrar associated with a domain and find relevant points of contact.

Modern privacy regulations and registrar privacy/proxy services often limit the personally identifying contact information displayed in public results. Nevertheless, WHOIS remains the traditional term for this source of domain-registration information. Registration Data Access Protocol is increasingly used as the standardized successor to WHOIS and can provide similar registration data through structured web queries. ICANN explains the purpose and availability of registration data through its Registration Data resources, while the Internet Engineering Task Force defines the modern RDAP protocol.

QUESTION NO: 6

At what point in the Incident Handling process should an organization determine its approach to notifying law enforcement?

A. When performing analysis

B. When preparing policy

C. When recovering from the incident

D. When reacting to an incident

ANSWER: B

Explanation:

When preparing policy is correct because decisions about whether, when, and how to involve law enforcement must be established before an incident occurs. This preparation-stage planning gives the organization a documented, repeatable escalation path that accounts for legal obligations, contractual requirements, privacy concerns, evidence preservation, executive authority, and communications responsibilities. It also identifies the appropriate law-enforcement contacts and defines who is authorized to make notification decisions or communicate externally. Establishing these details in incident-response policy helps responders act quickly under pressure without making inconsistent or unauthorized disclosures during an active event. NIST describes incident-response policy as defining the organization's approach to incident response, including roles, responsibilities, and reporting requirements. Its incident-response guidance also emphasizes preparation activities that enable coordinated handling and communication. A well-defined policy should therefore address the criteria and process for contacting external parties, including law enforcement, before responders need to use it. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and the CISA information-sharing guidance.

QUESTION NO: 7

Which of the following protocols are used to provide secure communication between a client and a server over the Internet?

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

A. SSL

B. HTTP

C. TLS

D. SNMP

ANSWER: A C

Explanation:

SSL and **TLS** are protocols designed to establish protected communications between networked endpoints, including a client and a server on the Internet. They provide authentication through digital certificates, confidentiality through encryption, and integrity protection that detects unauthorized modification of data in transit. SSL established the original widely deployed model for securing client-server sessions, while TLS is its modern successor and is the protocol family used by current secure services such as HTTPS, secure mail transport, and many VPN or application protocols. Although legacy SSL versions must not be enabled in production because of known weaknesses, SSL remains a correct historical protocol answer in the context of identifying protocols created for secure client-server communication. TLS should be configured using currently supported versions, particularly TLS 1.2 or TLS 1.3, with appropriate certificate validation and secure cipher-suite choices. The Internet Engineering Task Force defines TLS 1.3 and its security properties in RFC 8446. For practical deployment guidance, the U.S. National Institute of Standards and Technology recommends using TLS to protect data in transit and provides configuration guidance in NIST SP 800-52 Revision 2.

QUESTION NO: 8

You work as a Network Administrator for Tech2tech Inc. You have configured a network-based IDS for your company. You have physically installed sensors at all key positions throughout the network such that they all report to the command console.

What will be the key functions of the sensors in such a physical layout?

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

A. To collect data from operating system logs

B. To notify the console with an alert if any intrusion is detected

C. To analyze for known signatures

D. To collect data from Web servers

ANSWER: B C

Explanation:

In a network-based intrusion detection system, deployed sensors observe traffic at strategically selected network locations and send their findings to a centralized management or command console. “To notify the console with an alert if any intrusion is detected” is correct because the sensor or its associated detection component generates event and alert information when observed activity meets configured detection criteria; the console receives this information for correlation, investigation, and response. “To analyze for known signatures” is also correct because signature-based detection compares observed network activity against patterns associated with known attacks, exploits, protocol misuse, and other suspicious behaviors. This is a core detection method for network IDS deployments, alongside anomaly- and stateful-protocol-based approaches. NIST describes network-based IDPS sensors as monitoring network traffic and using detection methodologies such as signature-based analysis, with alerts commonly reported to centralized management infrastructure. Strategic placement allows the organization to observe relevant network segments, ingress and egress points, and other high-value traffic paths while preserving centralized visibility. See NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems and CISA’s overview of intrusion detection systems.

QUESTION NO: 9

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He wants to change the modified date and time of the file private.txt to 11 Nov 2009 02:59:58 am. Which of the following commands will John use to accomplish his task?

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

A. rm private.txt #11 Nov 2009 02:59:58 am

B. touch -d "11 Nov 2009 02:59:58 am" private.txt

C. touch private.txt #11 Nov 2009 02:59:58 am

D. touch -t 200911110259.58 private.txt

ANSWER: B D

Explanation:

`touch -d "11 Nov 2009 02:59:58 am" private.txt` is correct because the `-d` option accepts a human-readable date string. GNU `touch` parses the supplied date and uses it as the timestamp to apply to the target file. Because neither `-a` nor `-m` is specified, `touch` updates both the access and modification timestamps; consequently, the requested modification timestamp is set to 02:59:58 on 11 November 2009.

`touch -t 200911110259.58 private.txt` is also correct. The `-t` option uses the explicit timestamp format `[[CC]YY]MMDDhhmm[.ss]`. Here, `2009` is the year, `11` the month, `11` the day, `02` the hour, `59` the minute, and `.58` the seconds. This precisely represents 11 November 2009 at 02:59:58. Both commands are complete Linux solutions for assigning the requested modification time to an existing file. Root access may permit the operation regardless of ordinary file-permission constraints, but the timestamp-setting syntax itself is provided by `touch`. See the GNU Coreutils touch documentation and the touch(1) manual page.

QUESTION NO: 10

What is the name of the registry key that is used to manage remote registry share permissions for the whole registry?

A. regkey

B. regmng

C. winreg

D. rrsreg

ANSWER: C

Explanation:

winreg is the correct answer. Windows exposes the registry remotely through the Remote Registry service and the named-pipe interface commonly called `winreg`. Permissions governing remote access to the registry as a whole are configured through the `winreg` registry key, specifically under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`. The security descriptor on this key controls which users and groups can connect to and access the registry remotely, making it a significant hardening and administrative-control point.

Microsoft documents that remote registry access is subject to both the Remote Registry service and access controls associated with the registry's remote-management interface. Administrators can use the key's permissions to limit remote registry connections to authorized principals, following least-privilege practice. Because registry data often contains security settings, service configuration, installed-software information, and other sensitive system details, controlling this interface helps reduce the attack surface and prevents unauthorized remote enumeration or modification. Further technical context on remote registry operations is available in Microsoft's Remote Registry documentation and its Registry Key Security and Access Rights documentation.

QUESTION NO: 11

Which of the following statements about DMZ are true?

Each correct answer represents a complete solution. Choose two.

A. It is the boundary between the Internet and a private network.

B. It is an anti-virus software that scans the incoming traffic on an internal network.

C. FTP servers.

D. It contains an access control list (ACL).

ANSWER: A C

Explanation:

A DMZ is a separately controlled network segment positioned between the untrusted Internet and an organization's trusted private network. It provides a security boundary zone for systems that must be reachable from external networks while limiting direct exposure of internal assets. Traffic between the Internet, the DMZ, and the internal network is normally constrained by firewall policy, with only explicitly required services and connections permitted. This architecture reduces the likelihood that compromise of an Internet-facing system immediately provides unrestricted access to the internal network.

FTP servers can be placed in a DMZ when they need to accept connections or transfers from external parties. As an Internet-facing service, an FTP server is a common example of a host that benefits from DMZ placement: external clients can reach the service through narrowly defined firewall rules, while the server remains segregated from sensitive internal systems. Secure operational practice also requires tightly limiting allowed protocols, ports, administrative access, and any permitted connections from the DMZ into internal networks. NIST describes DMZs as perimeter network segments that isolate public-facing services from internal networks; see NIST SP 800-41 Rev. 1. Cisco likewise describes a DMZ as a network area for publicly accessible servers, including FTP services: Cisco DMZ overview.

QUESTION NO: 12

Which of the following statements about a RAID 1 disk configuration are true?

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

A. It stores duplicate copies of data on mirror members.

B. It can tolerate the failure of one disk in a two-disk mirror.

C. It eliminates the need for backups.

D. It uses distributed parity to protect data.

ANSWER: A B

Explanation:

RAID 1 maintains mirrored copies of data on two or more disks. Because data is duplicated, a RAID 1 set can continue operating after the failure of one member disk, provided another current mirror member remains available. It can also improve read performance in some implementations because reads may be distributed between mirror members.

RAID 1 is not a substitute for backups. Accidental deletion, ransomware encryption, application corruption, and malicious changes can be replicated to every mirror member. RAID 1 also does not provide parity-based capacity efficiency; usable capacity is generally limited to the capacity of one disk in a two-disk mirror. See NIST SP 800-111 for storage-protection context and Microsoft Storage Spaces overview for mirrored storage concepts.

QUESTION NO: 13

While using Wire shark to investigate complaints of users being unable to login to a web application, you come across an HTTP POST submitted through your web application. The contents of the POST are listed below. Based on what you see below, which of the following would you recommend to prevent future damage to your database?

```
POST /samplelogin.cfm HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (X11; U; en-US;) Gecko/200910 Ubuntu/8.4
Firefox/2.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.example.com/
Cookie: SID=026DCB9CBBF2339C2CBFAEBA8F1DD656;
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
username='a'&password=DROP+TABLE+members;+--
```

A. Use ssh to prevent a denial of service attack

B. Sanitize user inputs to prevent injection attacks

C. Authenticate users to prevent hackers from using your database

D. Use https to prevent hackers from inserting malware

ANSWER: B

Explanation:

Sanitize user inputs to prevent injection attacks is the appropriate recommendation because a suspicious login POST containing database-query syntax or control characters indicates an attempt to cause the application to interpret supplied data as part of a command rather than as ordinary username or password data. This is a classic injection-risk pattern. The essential defensive control is to ensure that user-controlled values are never concatenated into database queries. Applications should use parameterized queries (prepared statements), with database drivers binding submitted values as data. Input validation should also enforce expected formats, lengths, and character sets for fields such as usernames, while output handling and error controls should avoid exposing database details to clients.

These measures directly protect the database even when an attacker submits crafted values through a normal web form. The Open Worldwide Application Security Project identifies injection as a major web-application risk and recommends parameterized interfaces as the primary defense. Its SQL Injection Prevention Cheat Sheet provides implementation guidance, including prepared statements and allow-list input validation: OWASP SQL Injection Prevention Cheat Sheet. More broadly, OWASP's injection guidance explains why applications must keep commands and untrusted data separate: OWASP Injection Flaws.

QUESTION NO: 14

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:

IPsec uses the Authentication Header (AH) to provide connectionless integrity and data-origin authentication for IP packets. AH protects the packet against undetected modification by calculating an integrity check over protected portions of the packet, including the payload and applicable immutable IP-header fields. This allows a recipient to verify that the protected traffic was not altered in transit and came from a party holding the relevant security association keys. The IETF definition of AH and its integrity-processing requirements is specified in RFC 4302.

IPsec uses the Encapsulating Security Payload (ESP) to provide data confidentiality. ESP encrypts its protected payload using the encryption algorithm negotiated for the IPsec security association, preventing unauthorized parties from reading the protected traffic. Depending on the configured algorithms and security association, ESP can also provide integrity and origin authentication, but its core IPsec role for this question is confidentiality through encryption. ESP may operate in transport mode, protecting an upper-layer payload, or tunnel mode, protecting an entire original IP packet within a new IP packet. The protocol's confidentiality service and packet format are defined by the IETF in RFC 4303.

QUESTION NO: 15

Which of the following statements about Hypertext Transfer Protocol Secure (HTTPS) are true? Each correct answer represents a complete solution. Choose two.

A. It uses TCP port 443 as the default port.

B. It is a protocol used in the Uniform Resource Locator (URL) address line to connect to a secure site.

C. It is a protocol used to provide security for a database server in an internal network.

D. It uses TCP port 80 as the default port.

ANSWER: A B

Explanation:

HTTPS is HTTP communicated over a TLS-secured connection, providing authentication of the intended server (when certificate validation succeeds), confidentiality, and integrity protection for HTTP traffic in transit. "It uses TCP port 443 as the default port" is correct because the registered default port for the `https` URI scheme is 443. A client can use another explicitly specified port, but 443 is the conventional and scheme-defined default when no port appears in the URL. The IETF HTTP Semantics specification identifies port 443 as the default for HTTPS URIs; see RFC 9110, Section 4.2.2.

"It is a protocol used in the Uniform Resource Locator (URL) address line to connect to a secure site" is also correct. The `https://` scheme at the beginning of a URL tells the user agent to access the resource using HTTPS rather than cleartext HTTP. In normal browser use, this causes the browser to establish TLS before exchanging HTTP application data and to validate the site's certificate against the requested hostname. The URL Standard defines HTTPS as a special URL scheme and specifies its default port as 443; see the WHATWG URL Standard's special-scheme table.

QUESTION NO: 16

What is the purpose of notifying stakeholders prior to a scheduled vulnerability scan?

A. Risk of system crashes and security alerts.

B. Risk of deletion of backup files.

C. Risk of modified application configuration files.

D. Risk of applying untested patches.

ANSWER: A

Explanation:

The purpose is to prepare affected teams for the possibility of system instability and security alerts generated by the scan. Although vulnerability scans are ordinarily designed to be non-destructive, active probing can create measurable load on hosts, applications, network devices, and fragile legacy services. In some environments, this activity can contribute to performance degradation, service interruptions, or even crashes. Scan traffic may also resemble reconnaissance or attack behavior to intrusion detection systems, endpoint tools, web application firewalls, and security operations personnel.

Advance notification gives system owners, operations staff, and security monitoring teams the scan scope, schedule, source addresses, and escalation contacts. They can monitor important services, distinguish authorized scanning from an actual incident, and respond quickly if an unexpected operational impact occurs. It also supports change-management practices and ensures that appropriate personnel are available during the approved maintenance window. NIST describes planning and coordination as essential activities for security testing, including vulnerability scanning, so that testing is authorized and operational risks are managed. See NIST SP 800-115, Technical Guide to Information Security Testing and Assessment and CISA Cybersecurity Performance Goals.

QUESTION NO: 17

Which of the following services resolves host name to IP Address?

A. Computer Browser

B. DHCP

C. DNS

D. WINS

ANSWER: C

Explanation:

DNS is the service that resolves host names, such as `www.example.com`, to IP addresses that network clients use to locate and communicate with hosts. A client typically sends a DNS query to a configured recursive resolver, which either returns a matching record from its cache or performs the necessary lookups through the DNS hierarchy. For forward name resolution, the relevant record is commonly an IPv4 `A` record or IPv6 `AAAA` record. This translation is fundamental because people can use readable, stable names while network protocols route traffic using numerical IP addresses. DNS can also provide related information, including mail-server records, aliases, and reverse lookups; however, its core function in this question is mapping a host name to an IP address. The Internet Engineering Task Force's DNS terminology document describes DNS as a distributed database that maps domain names to data, including IP addresses, and its DNS concepts document explains the resolver and authoritative-server roles involved in answering queries. See RFC 9499: DNS Terminology and RFC 1034: Domain Names—Concepts and Facilities.

QUESTION NO: 18

Which of the following authentication methods are used by Wired Equivalent Privacy (WEP)? Each correct answer represents a complete solution. Choose two.

A. Anonymous authentication

B. Mutual authentication

C. Open system authentication

D. Shared key authentication

ANSWER: C D

Explanation:

WEP defines two IEEE 802.11 authentication modes: **Open system authentication** and **Shared key authentication**. Open system authentication is a basic authentication exchange in which a wireless client can request association without proving

knowledge of a secret. In a WEP network, access control and confidentiality may still be configured through WEP encryption after association, but the open-system authentication transaction itself does not validate a shared credential.

Shared key authentication uses a challenge-response process. The access point sends a challenge text to the client, and the client encrypts that challenge using the configured WEP key and returns it. The access point decrypts and compares the result to verify that the client possesses the shared WEP key. These are the two authentication algorithms specified for legacy WEP-capable 802.11 deployments. NIST describes WEP's support for open-system and shared-key authentication, as well as the security limitations of these legacy mechanisms, in NIST SP 800-48. Cisco also documents these two WEP authentication choices in its WEP configuration guide.

QUESTION NO: 19

What advantage would an attacker have in attacking a web server using the SSL protocol?

A. The web server trusts the client because they are using the same secret key.

B. The attacker needs to generate just one encryption key for all his requests.

C. The Client can cause the ssl web server to use a weak encryption algorithm.

D. The encrypted session makes It harder for an Intrusion Detection System to detect.

ANSWER: D

Explanation:

The encrypted session makes It harder for an Intrusion Detection System to detect. TLS, historically called SSL, encrypts the application-layer contents exchanged between the client and web server. A network-based intrusion detection system positioned outside the TLS endpoint can still observe metadata such as source and destination addresses, ports, packet sizes, timing, certificate details, and connection behavior. However, it generally cannot inspect the protected HTTP requests, responses, parameters, payloads, or commands that would reveal an attack signature. This reduced visibility can make malicious activity carried within an encrypted web session more difficult to identify using conventional signature-based network inspection. An attacker may therefore benefit when exploit delivery, command traffic, or data transfer blends into legitimate encrypted web traffic. Effective monitoring of such traffic commonly requires controls at a decryption point, such as a reverse proxy, web application firewall, endpoint telemetry, server-side logging, or carefully managed TLS inspection. NIST notes that encrypted traffic limits the content available to network monitoring technologies and may require monitoring at endpoints or other locations where traffic is available in plaintext. See NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems and CISA guidance on HTTPS and certificates.

QUESTION NO: 20

You are an Intrusion Detection Analyst and the system has alerted you to an Event of Interest (EOI) that appears to be activity generated by a worm. You investigate and find that the network traffic was normal. How would this type of alert be categorized?

A. False Positive

B. True Negative

C. True Positive

D. False Negative

ANSWER: A

Explanation:

False Positive is correct because the intrusion detection system generated an alert suggesting worm-related activity, but the analyst's investigation established that the observed network traffic was normal and no malicious activity was actually present. In detection terminology, a "positive" is an alert or detection produced by the security control, while "false" means

the alert does not correspond to a real security event. Therefore, this is a false positive: the IDS indicated a threat when there was no worm activity to validate.

False positives are an important operational concern because they consume analyst time, can create alert fatigue, and may obscure genuinely malicious events among benign detections. Analysts should document the validation outcome and, where appropriate, refine IDS signatures, thresholds, baselines, or contextual enrichment so that routine legitimate traffic is less likely to trigger the same alert in the future. This tuning should be performed carefully and supported by evidence, since overly broad suppression can reduce detection coverage. NIST describes intrusion detection as monitoring events and analyzing them for signs of possible incidents, which necessarily requires analyst validation of alerts. See NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems and the CISA Cyber Threats and Advisories resources.

QUESTION NO: 21

Which of the following are security benefits of using a properly configured virtual private network (VPN) for remote access?

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

A. It can encrypt traffic across an untrusted network.

B. It can authenticate remote users or devices.

C. It eliminates the need for endpoint security controls.

D. It automatically grants every remote user administrator access.

ANSWER: A B

Explanation:

A VPN can provide confidentiality for traffic carried across an untrusted network by encrypting the protected communications. It can also authenticate remote users or devices before allowing them access to protected internal resources. These protections are especially valuable when users connect through networks that the organization does not control.

A VPN does not remove the need for endpoint security, authorization controls, or monitoring. Once a remote device is connected, its permitted access must still be restricted according to least privilege, and a compromised endpoint can still pose risk. NIST describes VPN technologies as establishing protected communication channels and identifies authentication and encryption as central security functions. See NIST SP 800-77 Rev. 1.

QUESTION NO: 22

Which of the following statements about S/MIME are true?

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

A. It can provide digital signatures for email messages.

B. It can encrypt MIME message content for intended recipients.

C. It uses X.509 certificates to support public-key operations.

D. It replaces SMTP for transferring mail between mail servers.

E. It guarantees that every message is delivered to its recipient.

ANSWER: A B C

Explanation:

S/MIME is a standard for securing MIME data, including email messages, through cryptographic signing and encryption. A sender can digitally sign a message to provide integrity protection and support authentication of the signer. A recipient can validate the signature using the sender's certificate and public key, subject to certificate validation and trust decisions.

S/MIME can also encrypt message content for one or more recipients. The sender uses recipient certificate information to protect the content-encryption key, allowing only holders of the appropriate recipient private keys to decrypt the message. S/MIME does not replace SMTP as the mail-transfer protocol and does not inherently guarantee that an email was delivered. S/MIME message specifications are defined in RFC 8551.

QUESTION NO: 23

Which of the following are the types of access controls?

Each correct answer represents a complete solution. Choose three.

A. Physical

B. Administrative

C. Automatic

D. Technical

ANSWER: A B D

Explanation:

Physical, Administrative, and Technical are the three commonly taught categories of access controls. Physical controls protect facilities, equipment, and people through tangible safeguards such as locks, fences, security guards, badges, and secure entry points. These measures establish and enforce the physical boundary around systems and information assets. Administrative controls, also called managerial controls, define the governance and human processes that direct secure behavior. Typical examples include security policies, standards, procedures, awareness training, personnel screening, and risk-management decisions. Technical controls are safeguards implemented through technology to enforce security requirements on systems and data. Authentication mechanisms, authorization rules, encryption, firewalls, endpoint protections, and audit logging are all examples of this category. Used together, these categories provide defense in depth: organizational direction establishes expectations, physical safeguards protect the environment, and technical mechanisms enforce protections within information systems. NIST describes security controls as safeguards or countermeasures used to protect the confidentiality, integrity, and availability of information systems and organizations; see NIST's Security Control glossary entry. Additional access-control concepts and implementation guidance are available in NIST SP 800-53 Rev. 5.

QUESTION NO: 24

Which of the following is the key point to consider in the recovery phase of incident handling?

Which of the following is the key point to consider in the recovery phase of incident handling?

A. Isolating the source of the compromise

B. Shutting down the system

C. Ensuring that vulnerable code is not being restored

D. Preparing the jump bag

ANSWER: C

Explanation:

Ensuring that vulnerable code is not being restored is the key recovery-phase consideration. Recovery is the controlled process of returning affected systems and services to normal operation after the incident has been contained and eradicated. Before restoring from backups, redeploying applications, or returning hosts to production, responders must verify

that the original weakness has been remediated. Otherwise, the organization can restore the same vulnerable software, configuration, credentials, or malicious persistence mechanism that enabled the incident, resulting in rapid reinfection or recurrence. Recovery therefore includes applying security patches, correcting insecure configurations, rebuilding systems from known-good images where appropriate, validating backup integrity, resetting compromised credentials, and monitoring restored assets for suspicious activity. NIST's incident-response guidance identifies recovery as restoring affected systems and confirms that recovery activities should include remediating vulnerabilities and implementing safeguards to prevent similar incidents. The updated NIST incident-response framework also emphasizes integrating recovery with vulnerability management and continuous improvement. These steps allow services to be restored with confidence that the environment is not merely operational again, but is operating in a remediated and monitored state. See NIST SP 800-61 Rev. 2 and the NIST Cybersecurity Framework.

QUESTION NO: 25

You have been hired to design a TCP/IP-based network that will contain both Unix and Windows computers. You are planning a name resolution strategy. Which of the following services will best suit the requirements of the network?

A. APIPA

B. LMHOSTS

C. DNS

D. DHCP

E. WINS

ANSWER: C

Explanation:

DNS is the appropriate name-resolution service for a mixed TCP/IP network containing Unix and Windows computers. The Domain Name System provides a distributed, hierarchical mechanism for translating human-readable host names, such as `server.example.com`, into IP addresses and for performing reverse lookups where needed. DNS is a standards-based Internet protocol and is supported natively by both Unix-like operating systems and supported Windows versions, making it suitable for interoperable host and service discovery across the environment. A well-designed DNS namespace can support forward and reverse lookup zones, delegation, redundancy through multiple authoritative servers, and integration with dynamic updates where appropriate. This makes DNS scalable and manageable as the network grows, rather than requiring each host-to-address mapping to be maintained separately. DNS is specified in the IETF's core DNS standards, including the concepts and operation of domain names and name servers in RFC 1034. Microsoft also documents DNS as the name-resolution service that maps names to IP addresses and supports Windows network environments in its DNS overview.

QUESTION NO: 26

You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely reasons for the clustering?

Each correct answer represents a complete solution. Choose two.

A. Reduce power consumption

B. Ease of maintenance

C. Load balancing

D. Failover

ANSWER: C D

Explanation:

Load balancing and failover are core reasons to deploy clustered server services in a Microsoft-based environment. Load balancing distributes incoming client requests or workloads across multiple servers, preventing an individual server from becoming a bottleneck and helping the organization maintain responsive application performance as demand increases. Microsoft Network Load Balancing, for example, distributes traffic among hosts in a cluster while presenting a virtual service to clients. This supports availability and scalability for suitable stateless services such as web applications. See Microsoft's Network Load Balancing documentation.

Failover clustering is intended to preserve service availability when a participating server or component fails, or when planned maintenance is required. Cluster nodes monitor the health of the clustered workload and can move a clustered role to another available node. Clients can then continue accessing the service with minimized interruption, rather than waiting for a failed server to be repaired. This design is especially important for critical workloads that require continuity of operations. Microsoft describes the architecture, health monitoring, and role failover behavior in its Failover Clustering overview.

QUESTION NO: 27

Which of the following statements about asymmetric cryptography are true?

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

A. It uses a public key and a private key.

B. A recipient can decrypt data encrypted with the recipient's public key by using the corresponding private key.

C. It requires all users to protect the same shared secret key.

D. A digital signature is created with the signer's public key.

ANSWER: A B

Explanation:

Asymmetric cryptography uses a mathematically related key pair consisting of a public key and a private key. A public key may be distributed to other parties, while the corresponding private key must be protected by its owner. This key-pair design supports functions such as encryption and digital signatures.

When a sender encrypts information for a recipient using the recipient's public key, the corresponding private key is required to decrypt it. For digital signatures, the signer uses a private key to create the signature, and relying parties use the corresponding public key to verify it. Asymmetric cryptography does not require every communicating party to share the same secret key in advance; that describes symmetric cryptography. See NIST's public key cryptography glossary entry and FIPS 186-5.

QUESTION NO: 28

You work as a Linux technician for Tech Perfect Inc. You have lost the password of the root. You want to provide a new password. Which of the following steps will you take to accomplish the task?

A. The password of the root user cannot be changed.

B. Reboot the computer.

C. At the bash# prompt, run the PASSWD root command.

D. Use INIT=/bin/sh as a boot option.

ANSWER: D

Explanation:

Use INIT=/bin/sh as a boot option. This boot parameter directs the Linux kernel to start `/bin/sh` as the initial process rather than launching the normal init system and its authentication services. It provides a maintenance shell from which an administrator can regain control of the local system when the root password is unavailable. In the traditional recovery

workflow, the administrator starts the system with this parameter, ensures that the root filesystem is mounted read-write if necessary, runs `passwd root` to set the replacement password, and then safely reboots. This procedure must be performed only by an authorized administrator with console or otherwise approved recovery access, since physical boot access can provide powerful administrative recovery capabilities. Modern distributions may provide equivalent rescue, emergency, or boot-loader recovery procedures, and systems using SELinux may also require filesystem relabeling before the next normal boot. Red Hat documents booting into emergency/rescue environments for password recovery and related maintenance tasks in its root-password recovery guidance. Kernel boot parameters, including the init program selection mechanism, are described in the Linux kernel parameter documentation.

QUESTION NO: 29

Which of the following are network connectivity devices?

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

A. Network analyzer

B. Bridge

C. Brouter

D. Firewall

E. Repeater

F. Hub

ANSWER: B C E F

Explanation:

Bridge, Brouter, Repeater, and Hub are network connectivity devices because each provides a mechanism for linking, extending, or forwarding traffic between network segments. A bridge operates at the data-link layer and connects LAN segments while making forwarding decisions based on MAC addresses. A brouter combines bridge and router behavior: it can route protocols that are routable and bridge traffic for protocols that are not. A repeater regenerates or retimes signals so that a network segment can extend beyond the physical limits of the original medium. A hub is a multiport physical-layer device that connects attached hosts into a shared Ethernet segment and repeats received signals to its ports. These devices are commonly categorized as connectivity or internetworking hardware because their primary function is enabling communication across or within network segments. The layer responsibilities of repeaters, hubs, and bridges are described in the Cloudflare OSI model overview; Cisco also describes bridging and Layer 2 forwarding concepts in its LAN switching documentation.

QUESTION NO: 30

Which of the following processes Is used to prove a user Is who they claim to be based upon something they know, have, are, and/or their physical location?

A. Authorization

B. Accounting

C. Administration

D. Authentication

E. Identification

ANSWER: D

Explanation:

Authentication is the process of verifying that a user, device, or other entity is genuinely the identity it claims to be. It relies on one or more authentication factors: something the user knows, such as a password or PIN; something the user has, such as a smart card, hardware token, or authenticator application; something the user is, such as a fingerprint or facial biometric; and, in some contexts, somewhere the user is, determined through location-related signals. Requiring factors from different categories creates multifactor authentication, which provides substantially stronger assurance than relying on a password alone. Authentication occurs after an identity has been claimed and before access decisions are made, because a system must establish confidence in the claimant's identity before applying permissions or recording activity. NIST describes authentication as establishing confidence that a claimant controls one or more authenticators associated with a given identity, and its digital identity guidance details the use of different authenticator types and assurance levels. See NIST SP 800-63B: Digital Identity Guidelines—Authentication and Lifecycle Management and NIST Computer Security Resource Center: Authentication.

QUESTION NO: 31

Which of the following is an UDP based protocol?

A. telnet

B. SNMP

C. IMAP

D. LDAP

ANSWER: B

Explanation:

SNMP is the correct choice because the Simple Network Management Protocol commonly uses the User Datagram Protocol for lightweight, connectionless communication between network-management systems and managed devices. Standard SNMP requests and responses use UDP port 161, while SNMP notifications—traps and informs—use UDP port 162. UDP is well suited to routine monitoring because it has low overhead and does not require a connection to be established before a manager polls an agent for values such as interface status, bandwidth counters, or device health. SNMP itself includes request identifiers, error-status fields, retries, and timeout handling that allow the management application to handle missed datagrams when reliability is needed. SNMPv3 can additionally provide message authentication, integrity protection, and privacy, which are important when management traffic crosses untrusted networks. The Internet Assigned Numbers Authority registers SNMP at UDP port 161 and SNMP trap messages at UDP port 162: IANA Service Name and Port Number Registry. RFC 3417 specifies the transport mappings for SNMP and identifies UDP as the preferred transport mapping: RFC 3417.

QUESTION NO: 32

Which of the following protocols implements VPN using IPSec?

A. SLIP

B. PPP

C. L2TP

D. PPTP

ANSWER: C

Explanation:

L2TP is the correct answer when referring to the widely deployed L2TP/IPsec VPN architecture. Layer Two Tunneling Protocol provides the tunneling mechanism used to carry Layer 2 traffic, while IPsec supplies the security services that protect the packets crossing an untrusted network. In this arrangement, IPsec provides peer authentication, integrity protection, anti-replay protection, and encryption; L2TP then carries PPP frames through the protected tunnel. This

combination is commonly described as an L2TP/IPsec VPN and has historically been supported by many operating systems and VPN gateways.

The formal standards describe this relationship directly. RFC 3193 specifies using IPsec transport mode to secure L2TP traffic, including use of Encapsulating Security Payload and Internet Key Exchange for security association establishment. The IETF's L2TP specification also defines the protocol as a tunneling method that can be used with security mechanisms such as IPsec. Therefore, in the context of a question asking which listed protocol implements a VPN using IPsec, L2TP identifies the tunneling protocol paired with IPsec for the VPN solution. References: RFC 3193: Securing L2TP using IPsec and RFC 2661: Layer Two Tunneling Protocol.

QUESTION NO: 33

What dots Office 365 use natively for authentication?

A. Microsoft CHAP

B. Exchange Online

C. Azure Active Directory

D. Central Authentication Service

E. Extensible Authentication Protocol

ANSWER: B C

Explanation:

Office 365's cloud identity and sign-in foundation is Azure Active Directory, now named Microsoft Entra ID. It authenticates users, enforces Conditional Access and multifactor authentication policies, issues tokens, and provides single sign-on to Microsoft 365 services. Microsoft documents that Microsoft 365 uses Microsoft Entra ID as its identity platform, including for user authentication and authorization.

Exchange Online is also a native Microsoft 365 service involved in authenticated access to cloud-hosted email, calendars, and related Exchange workloads. When a user accesses an Exchange Online mailbox through Outlook, Outlook on the web, mobile clients, or service APIs, Exchange Online participates in the access flow and accepts identity tokens issued through the Microsoft 365 identity platform. Therefore, Azure Active Directory provides the central identity authentication capability, while Exchange Online is the native workload service that delivers authenticated mailbox access within Office 365.

For Microsoft's current terminology and architecture, see Microsoft 365 identity models and Exchange Online documentation.

QUESTION NO: 34

Which of the following defines the communication link between a Web server and Web applications?

A. CGI

B. PGP

C. Firewall

D. IETF

ANSWER: A

Explanation:

CGI (Common Gateway Interface) defines a standard interface through which a web server communicates with external applications, commonly called CGI programs or scripts. When a client sends an HTTP request for dynamic content, the web server can invoke the relevant application and provide request data through CGI-defined environment variables and standard input. The application processes that information—potentially querying a database or performing other server-side

work—and returns its output to the web server through standard output. The web server then formats and delivers the result as an HTTP response to the client. This separation lets a web server support dynamic, executable web functionality without embedding each application directly in the server itself. CGI was an important foundational mechanism for interactive web applications and remains useful for understanding the boundary between web-server request handling and server-side application execution. The IETF's CGI specification, RFC 3875, describes CGI as an interface between an information server and gateway programs, including the request metadata and response behavior used in that communication. See RFC 3875: The Common Gateway Interface (CGI) Version 1.1 and the W3C CGI resources.

QUESTION NO: 35

How is confidentiality disabled in the IPSec Encapsulated Security Payload protocol?

A. Selecting no algorithm for encryption or authentication

B. Selecting the NULL authentication algorithm

C. Selecting both NULL algorithms

D. Selecting the NULL encryption algorithm

ANSWER: D

Explanation:

Selecting the NULL encryption algorithm disables confidentiality for an IPsec Encapsulating Security Payload security association because encryption is the ESP service that provides payload secrecy. The NULL encryption transform intentionally performs no encryption: the protected payload remains readable to a party that can observe the packets. This is useful in limited designs where ESP's packet format and optional integrity/authentication protections are desired but encryption is not required or permitted. Importantly, choosing NULL encryption is a specific cryptographic-transform decision in the security association; it does not inherently determine whether integrity protection is used. ESP can therefore be configured with the NULL encryption transform while still using an integrity mechanism, depending on the negotiated IPsec policy and implementation. RFC 2410 defines the NULL encryption algorithm for IPsec and states that it does not encrypt data. RFC 4303 describes ESP as supporting confidentiality through encryption algorithms negotiated for a security association. See RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec and RFC 4303: IP Encapsulating Security Payload (ESP).

QUESTION NO: 36

You work as a Network Administrator for Net World Inc. The company has a Linux-based network. You want to mount an SMBFS share from a Linux workstation. Which of the following commands can you use to accomplish the task?

Each correct answer represents a complete solution. Choose two.

A. smbmount

B. mount smb

C. smbfsmount

D. mount -t smbfs

ANSWER: A D

Explanation:

`smbmount` is the Samba-provided utility historically used to mount an SMB/CIFS network share through the SMBFS client. It accepts a UNC-style share name and a local mount point, along with authentication and mount options, and performs the SMBFS mount operation. Samba's documentation describes `smbmount` specifically as mounting an SMBFS filesystem. The equivalent generic Linux mount form is `mount -t smbfs`, which explicitly selects the SMBFS filesystem type and supplies the remote share and local mount point as mount arguments. Thus, either command is a complete way to mount a share

when the system supports the legacy SMBFS client discussed in the question. These are historical commands: current Linux systems generally use the CIFS kernel client and the `mount.cifs` helper instead, but that does not change the expected answer for an SMBFS-focused question. See the Samba smbmount manual page and the Linux mount(8) manual page for the mount utility's filesystem-type behavior.

QUESTION NO: 37

Which of the following are used to suppress gasoline and oil fires? Each correct answer represents a complete solution. Choose three.

A. Halon

B. CO2

C. Soda acid

D. Water

E. Foam

ANSWER: A B E

Explanation:

Gasoline and oil fires are Class B fires because they involve flammable liquids. Halon is an effective clean-agent extinguishing medium for Class B fires: it suppresses combustion chemically and is especially useful where avoiding residue is important. Although new Halon production is prohibited because of its ozone-depleting effects, recycled Halon remains in certain legacy and critical-use fire-protection systems. CO2 is also appropriate because it displaces oxygen around the burning liquid and leaves no residue, making it useful for flammable-liquid hazards and energized equipment. Foam is a primary Class B extinguishing agent because it forms a vapor-suppressing blanket across the liquid surface, separating fuel vapors from oxygen and helping prevent re-ignition. OSHA identifies Class B hazards as flammable liquids and specifies appropriate extinguishing agents, including carbon dioxide and foam. The EPA also recognizes Halon as a fire-suppression agent while regulating its use due to environmental concerns. See OSHA's portable fire extinguisher standard and the EPA's Halon fire-extinguisher guidance.

QUESTION NO: 38

In preparation to do a vulnerability scan against your company's systems. You've taken the steps below:

You've notified users that there will be a system test.

You've priontized and selected your targets and subnets.

You've configured the system to do a deep scan.

You have a member of your team on call to answer questions.

Which of the following is a necessary step to take prior to starting the scan?

A. Placing the incident response team on call.

B. Clear relevant system log files.

C. Getting permission to run the scan.

D. Scheduling the scan to run before OS updates.

ANSWER: C

Explanation:

Getting permission to run the scan is necessary before initiating vulnerability-scanning activity, even when the systems are owned by the company. A deep scan can generate substantial network traffic, trigger security controls, temporarily affect availability, or interact unexpectedly with fragile applications and services. Explicit authorization establishes that the activity is approved, defines its scope, identifies permitted targets and testing windows, and confirms who is accountable if the scan causes an operational issue. Written authorization also helps distinguish legitimate scanner activity from an unauthorized attack when it is observed by monitoring personnel or security tools.

Authorization should be obtained from the asset owners and the individuals or teams with authority over the environment, and it should document operational boundaries such as in-scope networks, excluded critical systems, credentials if applicable, scan intensity, and escalation contacts. This is a foundational engagement-planning practice for vulnerability assessment and penetration testing. NIST's technical guidance describes obtaining authorization and defining rules of engagement before testing, while CISA emphasizes coordinating and gaining approval before conducting assessment activities. See NIST SP 800-115: Technical Guide to Information Security Testing and Assessment and CISA Penetration Testing guidance.

QUESTION NO: 39

What is a recommended defense against SQL injection, OS injection, and buffer overflows?

A. Put in an application layer

B. Validate user input

C. Use a secure protocol like HTTPS

D. Use stored procedures

ANSWER: B

Explanation:

Validate user input is the recommended defense because untrusted input is the common source of SQL injection, operating-system command injection, and many buffer-overflow conditions. Applications should treat all externally supplied data—including form fields, URL parameters, API values, cookies, uploaded-file metadata, and interprocess inputs—as untrusted. Input validation should use an allowlist approach wherever practical: define the expected type, character set, format, range, and maximum length, then reject input that does not meet those requirements. Enforcing strict length limits is particularly important for reducing buffer-overflow exposure, while type and format validation helps prevent data from being interpreted as SQL syntax or command syntax. Validation belongs at every trust boundary and should be complemented by safe implementation practices, such as parameterized database queries and APIs that avoid invoking a command shell. OWASP identifies allowlist input validation as a primary defense and explains that it helps reduce attack surface before data reaches interpreters or unsafe operations. For SQL-specific handling, OWASP also recommends parameterized queries so input remains data rather than executable query structure. See the OWASP Input Validation Cheat Sheet and the OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 40

Which of the following languages enable programmers to store cookies on client computers? Each correct answer represents a complete solution. Choose two.

A. DHTML

B. Perl

C. HTML

D. JavaScript

ANSWER: B D

Explanation:

Perl and **JavaScript** can both be used to cause a browser to store cookies on a client computer, although they do so in different execution contexts. A Perl-based web application commonly runs on the server and sends an HTTP `Set-Cookie` response header to the browser. The browser receives that header and stores the cookie subject to its attributes, such as `Path`, `Domain`, `Secure`, expiration, and `HttpOnly`. Perl CGI libraries have historically provided cookie-related functions that construct these response headers. See the CGI Perl module cookie documentation.

JavaScript executes in the browser and can create or update cookies available to the current site through the `document.cookie` interface. This supports client-side state management, provided browser cookie policies permit it. Cookies marked `HttpOnly` are intentionally inaccessible to JavaScript, which is an important security control, but JavaScript can still set ordinary applicable cookies. The browser behavior and the `document.cookie` API are documented by MDN Web Docs.

QUESTION NO: 41

Which port category does the port 110 fall into?

A. Well known port

B. Dynamic port

C. Private port

D. Application port

ANSWER: A

Explanation:

Well known port is correct because TCP/UDP port 110 is within the well-known port range, which spans port numbers 0 through 1023. This range is managed by the Internet Assigned Numbers Authority (IANA) and includes standard services that are commonly recognized across networks. Port 110 is assigned to the Post Office Protocol version 3 (POP3), a protocol traditionally used by email clients to retrieve messages from a mail server. Categorizing ports by their numerical range is useful in security operations because well-known ports often identify the type of network service exposed or observed in traffic. For example, a connection to port 110 commonly indicates POP3 activity, although analysts should validate the actual protocol rather than relying solely on a port number. IANA lists POP3 with service name “pop3” and port number 110 in its Service Name and Transport Protocol Port Number Registry. The range definitions are also published by IANA: well-known ports are 0–1023, registered ports are 1024–49151, and dynamic/private ports are 49152–65535. See the IANA registry entry for port 110 and IANA’s service-name and port-number registry.