PassQueen
a.k.a dumpsqueen.com

GIAC Information Security Fundamentals

GIAC GISF

Version Demo

Total Demo Questions: 36

Total Premium Questions: 367

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	153
Topic 2, Volume B	153
Topic 3, Volume C	41
Total	367

QUESTION NO: 1

Which of the following statements are true about UDP?

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

A. UDP is an unreliable protocol.

B. FTP uses a UDP port for communication.

C. UDP is a connectionless protocol.

D. TFTP uses a UDP port for communication.

E. UDP works at the data-link layer of the OSI model.

ANSWER: A C D

Explanation:

UDP is an unreliable protocol, in the networking sense that it provides no mechanism to guarantee delivery, retransmit lost datagrams, preserve ordering, or prevent duplicate delivery. Its checksum can detect corruption (when used), but UDP does not perform recovery when a datagram is lost or damaged. This low-overhead design is useful where timeliness and application-level control are more important than transport-level reliability.

UDP is a connectionless protocol because endpoints do not establish or maintain a transport-layer session before datagrams are sent. Each UDP datagram is handled independently and includes the addressing information needed for delivery. This makes UDP efficient for applications that need lightweight request/response exchanges, streaming, or their own reliability logic.

TFTP uses a UDP port for communication. TFTP initially receives requests on UDP port 69, then transfers occur through UDP using negotiated ephemeral ports. The protocol is deliberately simple and implements its own application-layer acknowledgments and retransmissions to support basic file transfers. UDP is a transport-layer protocol, as specified by the IETF in RFC 768; TFTP's use of UDP is specified in RFC 1350.

QUESTION NO: 2

Which of the following statements about Public Key Infrastructure (PKI) are true?

Each correct answer represents a complete solution. Choose two.

A. It is a digital representation of information that identifies users.

B. It uses asymmetric key pairs.

C. It provides security using data encryption and digital signature.

D. It uses symmetric key pairs.

ANSWER: B C

Explanation:

Public Key Infrastructure uses asymmetric key pairs. Each entity has a mathematically related public key and private key: the public key can be distributed for others to use, while the private key must remain under the owner's exclusive control. PKI also establishes the operational trust model around those keys, including certificates, certificate authorities, registration processes, certificate status validation, and key-management practices. This structure allows a recipient to associate a public key with an identified subject when relying on a certificate issued under an appropriate trust chain.

Public Key Infrastructure provides security using data encryption and digital signature. A sender can use a recipient's public key to protect information so that only the holder of the corresponding private key can decrypt it. Conversely, a signer uses their private key to generate a digital signature, and relying parties validate that signature with the signer's public key. Digital signatures provide integrity and origin authentication and can support nonrepudiation when the surrounding identity

validation, private-key protection, and policy controls are appropriately implemented. Certificate-based PKI is therefore a foundational mechanism for secure communications, authenticated services, signed software, and secure email. See the NIST PKI reference framework and NIST guidance on cryptographic key management.

QUESTION NO: 3 - (SIMULATION)

Fill in the blank with the appropriate layer name.

The Network layer of the OSI model corresponds to the_____ layer of the TCP/IP model.

ANSWER: See the explanation for the answer

Explanation:

Answer: Internet layer

In the TCP/IP model, the OSI Network layer maps to the **Internet** layer. This layer handles logical addressing and routing, including protocols such as IP.

QUESTION NO: 4

You have decided to implement an intrusion detection system on your network. You primarily are interested in the IDS being able to recognized known attack techniques. Which type of IDS should you choose?

A. Signature Based

B. Passive

C. Active

D. Anomaly Based

ANSWER: A

Explanation:

Signature Based is the appropriate choice when the primary requirement is recognizing known attack techniques. A signature-based intrusion detection system compares observed network or host activity against a library of predefined signatures, rules, or patterns that represent previously identified malicious activity. Those patterns can include recognizable byte sequences, protocol-field values, exploit payloads, command sequences, or other indicators associated with established threats. When traffic or events match a signature, the IDS can generate an alert, allowing security personnel to identify and investigate activity that corresponds to a known technique.

This detection approach is especially useful where an organization wants reliable identification of threats for which indicators and detection rules are already available. Its effectiveness depends on maintaining current signature content, because new signatures are needed as attackers introduce new malware, exploits, and techniques. NIST describes signature-based detection as identifying attacks through known patterns of malicious activity and emphasizes the need to keep detection signatures current. See NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems. The MITRE ATT&CK knowledge base also provides a structured catalog of known adversary techniques that can inform detection-rule development and signature coverage: MITRE ATT&CK.

QUESTION NO: 5

Which of the following can be used to prevent routing loops in distance vector routing protocols?

Each correct answer represents a complete solution. Choose two.

A. Split horizon

B. Link-state advertisement

C. Spanning Tree Protocol

D. Hold-down timers

ANSWER: A D

Explanation:

Split horizon and hold-down timers are standard loop-avoidance and loop-mitigation mechanisms used by distance-vector routing protocols. Split horizon prevents a router from advertising a route back out through the same interface on which it learned that route. This limits the opportunity for neighboring routers to incorrectly re-learn each other's routes and form a routing loop. A common related implementation, split horizon with poison reverse, advertises the learned route back toward its source with an unreachable metric, making the route explicitly unusable in that direction.

Hold-down timers help stabilize routing after a route fails or becomes unreachable. During the hold-down period, the router resists accepting potentially stale or inferior updates that claim the route is available again. This gives failure information time to propagate through the network and reduces the likelihood of the count-to-infinity behavior associated with distance-vector convergence. Together, these controls address the delayed and neighbor-by-neighbor exchange of routing knowledge inherent in distance-vector algorithms. Cisco documents split horizon, route poisoning, and hold-down timers as distance-vector loop-prevention techniques in its RIP configuration and troubleshooting guidance; see also the RIPv2 specification for distance-vector route metrics and update behavior.

QUESTION NO: 6

Which of the following is a correct sequence of different layers of Open System Interconnection (OSI) model?

A. Physical layer, data link layer, network layer, transport layer, presentation layer, session layer, and application layer

B. Physical layer, network layer, transport layer, data link layer, session layer, presentation layer, and application layer

C. application layer, presentation layer, network layer, transport layer, session layer, data link layer, and physical layer

D. Physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer

ANSWER: D

Explanation:

The correct sequence is **Physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer**. This lists the seven OSI layers from the lowest layer, closest to the transmission medium and hardware, through to the highest layer, closest to the user-facing network services. The Physical layer handles signaling and media; the Data Link layer provides local-link framing and addressing; and the Network layer supports logical addressing and routing between networks. The Transport layer provides end-to-end transport functions, including reliability and flow control where applicable. Above it, the Session layer manages communication dialogs, the Presentation layer handles data representation functions such as formatting and encryption transformations, and the Application layer provides network services used by applications. Knowing the ordered model is useful in security because it helps analysts identify where a control, protocol, device, or failure belongs and supports systematic troubleshooting. Cisco's OSI overview presents these layers in this bottom-to-top order: Cisco: What Is a Network Switch?. A concise layer-by-layer reference is also available from Cloudflare: OSI model.

QUESTION NO: 8

Which of the following statements are true about security risks? Each correct answer represents a complete solution. Choose three.

A. They are considered an indicator of threats coupled with vulnerability.

B. They can be mitigated by reviewing and taking responsible actions based on possible risks.

C. They can be removed completely by taking proper actions.

D. They can be analyzed and measured by the risk analysis process.

ANSWER: A B D

Explanation:

Security risk is appropriately understood in relation to threats and vulnerabilities: a threat may exploit a vulnerability, creating the potential for an adverse effect on an organization's operations, assets, or individuals. Thus, identifying threats together with relevant weaknesses is a fundamental way to identify and characterize risk. Risk management also requires responsible, risk-informed action. Organizations mitigate risk by selecting and implementing safeguards, changing processes, accepting risk within approved tolerances, transferring aspects of risk where appropriate, and continuously monitoring the environment. These actions reduce likelihood, impact, or both; they support informed management of the organization's remaining exposure. Finally, risk analysis provides a structured means to analyze and measure risk. It evaluates potential adverse impacts and the likelihood that particular threat events could exploit identified vulnerabilities, allowing risks to be prioritized for treatment. This supports repeatable decisions rather than relying solely on intuition. NIST describes risk as a function of the likelihood of a threat event and its potential adverse impacts in NIST SP 800-30 Rev. 1. The broader life-cycle activities of framing, assessing, responding to, and monitoring risk are defined in NIST SP 800-37 Rev. 2.

QUESTION NO: 9

You work as a Network Administrator for Tech Perfect Inc. The company has recruited a large number of fresh employees. You have been asked to give them a presentation on data protection and confidentiality to ensure a secure wireless communication between the employees. What types of information require confidentiality? Each correct answer represents a complete solution. Choose all that apply.

A. Information that is public

B. Information that reveals technical data

C. Information that may reveal systems relationships

D. Information that may reveal organizational relationships

ANSWER: B C D

Explanation:

Information that reveals technical data requires confidentiality because details such as network configurations, wireless settings, infrastructure designs, software versions, and security-control implementation information can help an unauthorized party understand the environment and target it more effectively. Protecting this information supports the confidentiality objective: preventing unauthorized disclosure of information and limiting access to personnel with a valid business need.

Information that may reveal systems relationships also requires confidentiality. Knowledge of trust relationships, network connectivity, dependencies, authentication flows, administrative boundaries, and connections between systems can expose paths through an environment. Even where individual technical details appear harmless, their combination can create a useful map for reconnaissance or attack planning.

Information that may reveal organizational relationships should likewise be safeguarded. Reporting structures, business partnerships, employee roles, privileged contacts, and internal ownership relationships can be used to identify high-value targets or craft convincing social-engineering attempts. Effective protection therefore includes classifying such information appropriately, restricting access, and avoiding unnecessary disclosure over wireless or other communications channels. NIST describes confidentiality as preserving authorized restrictions on information access and disclosure in its confidentiality glossary definition; related safeguards are addressed by the NIST SP 800-53 security and privacy controls.

QUESTION NO: 10

Victor works as a network administrator for DataSecu Inc. He uses a dual firewall Demilitarized Zone (DMZ) to insulate the rest of the network from the portions, which is available to the Internet. Which of the following security threats may occur if DMZ protocol attacks are performed?

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

A. Attacker can exploit any protocol used to go into the internal network or intranet of the com pany.

B. Attacker managing to break the first firewall defense can access the internal network without breaking the second firewall if it is different.

C. Attacker can gain access to the Web server in a DMZ and exploit the database.

D. Attacker can perform Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network.

ANSWER: A C D

Explanation:

A dual-firewall DMZ provides an intermediary network for Internet-facing services, but it does not eliminate the risk that a compromised DMZ system can be used as a foothold for further attacks. An attacker who compromises an exposed host may attempt to exploit permitted protocols and connections that traverse from the DMZ toward internal systems. Security policy must therefore strictly limit, authenticate, and monitor every allowed service flow between the DMZ and intranet. This is why an attacker can exploit any protocol used to go into the internal network or intranet of the com pany is a valid threat scenario.

Likewise, a Web server in a DMZ commonly needs controlled access to a back-end database or application service. Compromising that Web server can enable abuse of its authorized database connection, application credentials, or vulnerable queries; therefore, attacker can gain access to the Web server in a DMZ and exploit the database describes a realistic impact. Finally, Internet-facing DMZ services are potential delivery points for previously unknown exploits. A malicious payload not recognized by signature-based detection can evade those controls, making attacker can perform Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network a valid threat. See NIST SP 800-41 Rev. 1 and CISA's zero-day vulnerability guidance.

QUESTION NO: 11

Which of the following statements are TRUE regarding asymmetric encryption and symmetric encryption? Each correct answer represents a complete solution. Choose all that apply.

A. Data Encryption Standard (DES) is a symmetric encryption key algorithm.

B. In symmetric encryption, the secret key is available only to the recipient of the message.

C. Symmetric encryption is commonly used when a message sender needs to encrypt a large amount of data.

D. Asymmetric encryption uses a public key and a private key pair for data encryption.

ANSWER: A C D

Explanation:

Data Encryption Standard (DES) is a symmetric-key encryption algorithm: the same shared secret key is used to transform plaintext into ciphertext and to recover the plaintext. Although DES is now obsolete for modern protection because its effective 56-bit key length is vulnerable to exhaustive key-search attacks, its classification as a symmetric algorithm is correct. NIST formally withdrew DES as an approved encryption algorithm, while retaining its historical definition in its cryptographic publications.

Symmetric encryption is commonly used for large amounts of data because symmetric ciphers are computationally efficient and are designed for bulk confidentiality. Modern protocols commonly establish or protect a symmetric session key using public-key cryptography, then use that symmetric key to encrypt the actual data stream. This combines efficient bulk encryption with practical key distribution.

Asymmetric encryption uses a mathematically related public and private key pair. The public key can be used for encryption so that only the holder of the corresponding private key can decrypt the protected data. Public-key systems also support authentication-related uses, such as digital signatures, through the same paired-key concept. See NIST's FIPS 46-3 publication for DES and its public-key cryptography glossary definition.

QUESTION NO: 12

Which of the following network connectivity devices translates one protocol into another and is used to connect dissimilar network technologies?

A. Hub

B. Firewall

C. Bridge

D. Gateway

ANSWER: D

Explanation:

Gateway is correct because a gateway connects networks or systems that use dissimilar communications protocols, architectures, or data formats. Unlike devices that primarily forward, filter, or repeat traffic within a common networking framework, a gateway can perform protocol conversion so that devices using different technologies can exchange information. This translation can occur at multiple layers of the network stack, depending on the gateway's purpose. For example, an application gateway may translate between application protocols or mediate communications between systems with incompatible formats, while a network gateway can provide the connection point between separate networks and apply the required conversion or encapsulation functions. In security and networking terminology, "default gateway" often refers to the router that provides a path out of a local subnet; however, the broader definition of a gateway is a device or software component that enables interoperability between otherwise dissimilar networks. This makes gateway the best match for the description's emphasis on translating one protocol into another and connecting different network technologies. Cisco's networking glossary describes a gateway as a device that connects networks using different protocols, while IBM similarly defines gateways in terms of connecting networks that may use different protocols or architectures. See Cisco's networking overview and IBM documentation on gateways.

QUESTION NO: 13

Which of the following is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy?

A. Disaster Invocation Guideline

B. Business Continuity Strategy

C. Index of Disaster-Relevant Information

D. Availability/ ITSCM/ Security Testing Schedule

ANSWER: B

Explanation:

Business Continuity Strategy is correct because it is developed from the business perspective to establish how the organization will maintain or restore its prioritized products, services, activities, and resources following a disruptive event. It reflects business requirements such as recovery priorities, recovery time objectives, acceptable levels of disruption, alternate operating arrangements, and resource needs. IT Service Continuity Management then uses those business-defined requirements as the basis for its IT Service Continuity Strategy. This ensures that IT recovery capabilities are designed to support the organization's required continuity outcomes, rather than being based solely on technical preferences or available infrastructure. In practical terms, the business continuity strategy identifies what the business must continue or recover and

to what level; the IT service continuity strategy determines the technology, systems, data, facilities, and recovery measures needed to meet those commitments. This business-led dependency is a core continuity-management principle: IT continuity is aligned with, and supports, wider business continuity planning. The ISO business-continuity standard describes establishing continuity strategies and solutions based on the organization's continuity requirements: ISO 22301:2019. ITIL guidance similarly treats service continuity as ensuring that services can meet agreed business continuity requirements: AXELOS ITIL.

QUESTION NO: 14

Which of the following tools are used to determine the hop counts of an IP packet?

Each correct answer represents a complete solution. Choose two.

A. Netstat

B. Ping

C. TRACERT

D. IPCONFIG

ANSWER: B C

Explanation:

Ping and **TRACERT** can be used to assess the number of network hops involved in reaching a destination. TRACERT is specifically designed for this purpose: it sends packets with progressively increasing IP Time to Live values and records the routers that return ICMP Time Exceeded messages. Each displayed route entry therefore corresponds to a hop, enabling an administrator to identify the path and count the intervening routers. Microsoft documents that tracert works by incrementing the TTL value to discover each router along the route.

Ping can also provide hop-count information through the TTL value in ICMP Echo Reply packets. A responding system includes a TTL value in its reply, and, when the sender knows or can reasonably infer the responder's initial TTL convention, the difference between that initial value and the received TTL indicates the approximate number of routed hops traversed. This is useful as a quick diagnostic indicator, although it is less explicit than the hop-by-hop output produced by TRACERT. ICMP Echo and Time Exceeded behavior are defined in the ICMP specification, while TTL processing is defined by IPv4. See Microsoft's tracert documentation and RFC 791, Internet Protocol.

QUESTION NO: 15

Which of the following can be used to protect a computer system from malware, viruses, spyware, and various types of keyloggers? Each correct answer represents a complete solution. Choose all that apply.

A. KFSensor

B. Sheep dip

C. Enum

D. SocketShield

ANSWER: B D

Explanation:

Sheep dip is a defensive malware-control practice in which potentially untrusted media, files, or systems are examined in an isolated, dedicated environment before they are allowed to reach a production computer or network. The sheep-dip environment can use updated antimalware scanning and analysis controls to identify viruses, spyware, keyloggers, and other malicious content before exposure occurs. This supports the broader security principle of scanning potentially malicious content at a controlled boundary. NIST's guidance on malware incident prevention and handling emphasizes maintaining

protective technologies and scanning mechanisms to prevent malicious code from executing in enterprise environments; see NIST SP 800-83 Rev. 1.

SocketShield is designed as endpoint protection against spyware and keylogging activity, including methods intended to capture keystrokes or otherwise monitor user activity. Such protection is relevant because keyloggers are commonly deployed as spyware or as part of broader malware infections, and endpoint controls can reduce the risk of credential and sensitive-data capture. Its use complements core malware-prevention practices such as maintaining updated antimalware protections, restricting untrusted software, and monitoring systems for suspicious activity. CISA provides additional practical guidance on recognizing and reducing malware risk at CISA's Malware resource page.

QUESTION NO: 16

Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using?

A. Risk acceptance

B. Risk transfer

C. Risk avoidance

D. Risk mitigation

ANSWER: B

Explanation:

Risk transfer is correct because the company is using an insurance policy to shift the financial consequences of specified information-security events to an insurer. The organization still owns and must manage the underlying operational risk: systems can still be attacked, assets can still be damaged, and the organization remains responsible for implementing appropriate safeguards and meeting policy conditions. However, in exchange for premiums and subject to coverage limits, exclusions, deductibles, and claim requirements, the insurer agrees to bear defined monetary losses or liabilities. This is the standard risk-management meaning of transfer: allocating some financial impact of a risk to another party through a contractual arrangement. Cyber-liability and property-liability insurance are common examples because they can cover costs such as incident response, legal liability, restoration, notification, or physical-loss claims, depending on the policy. NIST describes risk framing and risk response as organizational activities that include considering risk-sharing arrangements, while insurance is a widely recognized contractual mechanism for transferring financial exposure. See NIST SP 800-39, Managing Information Security Risk and CISA guidance on cybersecurity insurance.

QUESTION NO: 17

A company would like your consulting firm to review its current network and suggest changes that will increase its efficiency and optimize the business processes.

To design such a network, you prepare a case study.

Which of the following policies should be implemented through a group policy that is associated with the netperfect.com domain?

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

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

A. Account lockout policy.

B. Password policy.

C. Limit computers that can access production schedule software.

D. Assign MS Office suite to appropriate users.

ANSWER: A B D

Explanation:

Account lockout policy and **Password policy** are domain account policies. They apply to domain user accounts and therefore should be configured in a Group Policy Object linked at the domain level, such as the Default Domain Policy or another appropriately managed domain-linked GPO. This ensures that the required password characteristics, password lifetime, failed-sign-in threshold, lockout duration, and related account protections are consistently enforced for accounts in the netperfect.com domain. Microsoft documents that password policy and account lockout policy settings are domain-level account-policy settings when configured through Group Policy: Microsoft password policy settings and Microsoft account lockout policy.

Assign MS Office suite to appropriate users can also be implemented using a domain-associated GPO. Group Policy Software Installation supports assigning software to users, and the deployment can be scoped so that only the intended users receive the application, such as through security-group filtering. Linking the GPO to the domain makes the policy available within the domain while the applicable user scope controls which appropriate users receive the Office assignment. Microsoft's Group Policy guidance describes using Group Policy to manage software deployment: Use Group Policy to install software.

QUESTION NO: 18

A firewall is a combination of hardware and software, used to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. IPChains

B. OpenSSH

C. Stunnel

D. IPTables

ANSWER: D

Explanation:

IPTables is correct because it is the user-space command-line utility used to configure the Linux kernel's Netfilter packet-filtering framework, which was introduced with the Linux 2.4 kernel series. Through iptables rules, an administrator can define filtering policies for inbound, outbound, and forwarded network traffic. Rules can match characteristics such as source and destination IP addresses, transport protocols, and TCP or UDP port numbers, then apply actions such as accepting, dropping, rejecting, or logging packets. This directly supports the firewall functions described in the question: controlling traffic crossing the boundary between internal and external networks and enforcing a defined access policy. Netfilter performs the in-kernel packet processing, while iptables supplies the administrative interface for viewing, creating, changing, and deleting the rules that govern that processing. The Netfilter project's packet-filtering documentation identifies iptables as the tool for configuring these packet-filtering rules and describes its built-in chains for traffic entering, leaving, and traversing a host. See the Netfilter Packet Filtering HOWTO and the iptables manual page.

QUESTION NO: 19

Which of the following is the main purpose of using OODA loops?

A. Providing economic balance

B. Making decisions and taking action faster than an adversary

C. Information welfare

D. Creating advanced military weapons

ANSWER: B

Explanation:

Making decisions and taking action faster than an adversary is the main purpose of an OODA loop. OODA stands for Observe, Orient, Decide, and Act. Developed by U.S. Air Force Colonel John Boyd, it describes a repeating decision cycle in which a person or organization gathers observations, interprets them in context, selects a response, acts, and then observes the changed environment again. Its value is not merely faster transmission of information; it is faster, better-informed adaptation. In security operations, for example, analysts observe an alert, orient it using asset, threat, and business context, decide on containment or escalation, and act. Repeating the cycle quickly helps defenders adjust as an incident develops and can disrupt an attacker's ability to execute a plan. The objective is to create a tempo advantage: decisions and actions occur quickly enough that the opposing party is reacting to an environment that has already changed. This idea is widely applied beyond military contexts, including incident response and competitive decision-making. The U.S. Air Force's discussion of Boyd's concepts provides background on the decision-cycle model, while the NIST incident-response guidance illustrates the importance of iterative analysis, containment, and recovery in operational security work. See Air University's overview of John Boyd's work and NIST SP 800-61 Rev. 2.

QUESTION NO: 20

Which of the following U.S.C. laws is governs the fraudulent activities associated with computers?

A. 18 U.S.C. 2251

B. 18 U.S.C. 3771

C. 18 U.S.2257

D. 18 U.S.C. 1030

ANSWER: D

Explanation:

18 U.S.C. 1030 is the Computer Fraud and Abuse Act (CFAA), the principal U.S. federal statute addressing computer-related fraud and unauthorized access. It establishes criminal offenses for intentionally accessing protected computers without authorization, or exceeding authorized access, in circumstances involving fraud, theft of information or value, damage to systems or data, extortion, and related conduct. A "protected computer" includes computers used in or affecting interstate or foreign commerce or communication, which gives the statute broad applicability to modern networked systems and Internet-connected business environments. The statute also provides for penalties that vary based on the conduct, harm, prior offenses, and other aggravating factors, and it includes a civil cause of action in specified situations. For information-security professionals, this law is foundational because improper access, misuse of credentials, data theft, and intentional system damage can create both security incidents and potential CFAA exposure. The authoritative statutory text is available through the U.S. House Office of the Law Revision Counsel. The Department of Justice also provides guidance on the CFAA and computer crime enforcement in its Computer Crime and Intellectual Property Section resources.

QUESTION NO: 21

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 domainbased network. The network has three Windows Server 2008 member servers and 150 Windows Vista client computers. According to the company's security policy, you apply Windows firewall setting to the computers on the network. Now, you are troubleshooting a connectivity problem that might be caused by Windows firewall. What will you do to identify connections that Windows firewall allows or blocks?

A. Configure Network address translation (NAT).

B. Disable Windows firewall logging.

C. Configure Internet Protocol Security (IPSec).

D. Enable Windows firewall logging.

ANSWER: D

Explanation:

Enable Windows firewall logging. Windows Firewall logging records firewall activity in a log file, providing evidence that is useful when diagnosing whether traffic is being permitted or denied. In the Windows Server 2008 and Windows Vista firewall implementation, logging settings are configured per firewall profile, such as Domain, Private, or Public. An administrator can choose to log dropped packets and successful connections, then review the resulting log entries for source and destination IP addresses, ports, protocol information, and the action recorded. This allows the administrator to correlate an affected application or client connection with firewall activity and determine whether the firewall is involved in the connectivity issue. For a domain-based network, the active profile will commonly be the Domain profile while devices can authenticate to the domain, so logging should be enabled and reviewed for the profile currently applied to the affected system. Logging is an important troubleshooting and audit capability because it produces a record of observed firewall decisions without broadly weakening the host's protection. Microsoft documents that Windows Firewall with Advanced Security can log both dropped packets and successful connections, and that the log location and settings are configurable per profile. See Microsoft's Windows Firewall configuration guidance and Microsoft's command-line firewall configuration documentation.

QUESTION NO: 23

Which of the following are the goals of the cryptographic systems?

Each correct answer represents a complete solution. Choose three.

A. Availability

B. Authentication

C. Confidentiality

D. Integrity

ANSWER: B C D

Explanation:

Authentication, confidentiality, and integrity are core security goals that cryptographic systems are designed to provide. Confidentiality protects information from unauthorized disclosure, commonly through encryption that makes data intelligible only to parties holding the appropriate decryption key. Integrity provides assurance that information has not been modified, inserted, deleted, or otherwise altered without detection; cryptographic hashes, message authentication codes, and digital signatures are common mechanisms used to support this goal. Authentication establishes confidence in the identity of a communicating party or in the origin of data. For example, digital signatures can authenticate the signer while also protecting the signed content's integrity, and message authentication codes can authenticate a message's source to parties sharing a secret key. These services are often used together: an encrypted, authenticated communication protocol can protect the secrecy of transmitted data while confirming its origin and detecting tampering. NIST describes cryptographic mechanisms and key management as foundational means of protecting information and supporting security services such as confidentiality, integrity, and authentication. See NIST SP 800-57 Part 1 and the NIST definition of authentication.

QUESTION NO: 24

Which of the following protocols are used by Network Attached Storage (NAS)?

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

A. Apple Filing Protocol (AFP)

B. Server Message Block (SMB)

C. Network File System (NFS)

D. Distributed file system (Dfs)

ANSWER: A B C

Explanation:

Network Attached Storage provides file-level storage over a network, so clients access shared files and directories through network file-sharing protocols. Apple Filing Protocol (AFP) is a file-sharing protocol historically used by Apple systems and supported by NAS platforms that provide compatibility with legacy macOS environments. Server Message Block (SMB) is the standard network file-sharing protocol used broadly by Windows clients and is a common NAS service for shared folders, file access, and authenticated access control. Network File System (NFS) provides equivalent network file-sharing functionality in UNIX, Linux, and many mixed-platform environments, and is likewise a core protocol offered by NAS devices. These protocols enable client systems to mount or browse storage hosted by the NAS while the NAS manages the underlying disks, permissions, and file system. In practice, a single NAS appliance can expose the same stored data through SMB, NFS, and, where needed, AFP to serve heterogeneous client environments. For protocol background, see the Microsoft SMB overview and the NFS version 4.1 specification.

QUESTION NO: 25

You are concerned about outside attackers penetrating your network via your company Web server.

You wish to place your Web server between two firewalls

One firewall between the Web server and the outside world

The other between the Web server and your network

What is this called?

A. IDS

B. SPI firewall

C. DMZ

D. Application Gateway firewall

ANSWER: C

Explanation:

DMZ is correct. A demilitarized zone is a separately isolated network segment used for systems that must be reachable from untrusted networks, such as a public web server. In the described architecture, the internet-facing firewall controls inbound traffic from the outside world to the web server, while the internal firewall restricts traffic between that server and the organization's trusted internal network. This segmentation limits the ability of an attacker who compromises the public-facing server to move directly into internal systems.

A DMZ is a defense-in-depth design: services exposed to the internet are placed in a less-trusted zone rather than on the internal LAN. Firewall policy should allow only the required web traffic from the internet to the server and only narrowly defined, necessary connections from the DMZ to internal resources. Logging, monitoring, patching, and hardened server configuration remain important because a DMZ reduces exposure and lateral-movement opportunities but does not eliminate compromise risk. NIST describes DMZs as perimeter-network segments that provide additional protection for internal networks, and CISA recommends network segmentation to contain attacks and reduce their impact. See NIST SP 800-41 Rev. 1 and CISA guidance on network segmentation.

QUESTION NO: 26

You are the project manager of the HHH Project. The stakeholders for this project are scattered across the world and you need a method to promote interaction. You determine that a Web conferencing software would be the most cost effective solution. The stakeholders can watch a slide show while you walk them through the project details. The stakeholders can hear you, ask questions via a chat software, and post concerns. What is the danger in this presentation?

A. 55 percent of all communication is nonverbal and this approach does not provide non-verbal communications.

B. The technology is not proven as reliable.

C. The stakeholders won't really see you.

D. The stakeholders are not required to attend the entire session.

ANSWER: A

Explanation:

55 percent of all communication is nonverbal and this approach does not provide non-verbal communications. is the correct answer because the described session provides presentation visuals, spoken words, and text chat, but does not state that participants can see one another through video. Consequently, the project manager loses a major source of communication feedback: facial expressions, posture, gestures, and other observable reactions. Stakeholders may be confused, hesitant, disengaged, or concerned without those signals being readily visible to the presenter. This makes it harder to assess whether the audience understands the material, recognizes a risk, or needs the discussion to slow down or change direction. The often-cited 55-percent figure comes from Albert Mehrabian's research on the relative contribution of nonverbal cues in communicating feelings and attitudes; it should be understood in that context rather than as a universal measurement for every project discussion. Even so, the core project-management concern remains sound: communication channels should be selected with awareness of the feedback they preserve or remove. For important stakeholder interactions, incorporating video, explicit check-ins, and follow-up mechanisms can help compensate for reduced nonverbal feedback. See the original research record at the American Psychological Association DOI record and PMI's discussion of communication practices at Project Management Institute.

QUESTION NO: 27

You work as a SharePoint Administrator for TechWorld Inc. You must protect your SharePoint server farm from viruses that are accidentally uploaded to the SharePoint libraries. You have installed antivirus software that is designed for use with Windows SharePoint server. You have logged on to the Central Administration site.

How can you configure the SharePoint site so that the document libraries are protected?

A. SharePoint does not support antivirus solutions.

B. Restrict users to read only on document libraries.

C. Choose the Scan documents on upload option in the antivirus settings.

D. Require all documents to be scanned on the local PC before uploading to the SharePoint sit e.

ANSWER: C

Explanation:

Choose the Scan documents on upload option in the antivirus settings. This is the appropriate Central Administration setting for a SharePoint farm that has a SharePoint-compatible antivirus product installed. When enabled, SharePoint sends a document to the registered antivirus scanner as part of the upload process, before the uploaded content becomes available in the library. This provides server-side enforcement at the point where potentially unsafe files enter SharePoint, rather than depending on a user's local workstation configuration or behavior.

SharePoint Server's antivirus integration is specifically designed to let administrators control scan behavior centrally for the farm. In addition to scanning on upload, administrators can configure related protections such as scanning documents on download and defining the action to take when a virus is detected. The upload scan setting directly addresses the stated requirement: preventing accidental uploads from introducing infected documents into SharePoint document libraries. It should be enabled only after confirming that the antivirus solution is compatible with and registered for SharePoint's antivirus interface, so that SharePoint can invoke the scanner during content processing.

Microsoft describes these farm-level controls in its Configure antivirus settings for SharePoint Server guidance and provides related deployment information in Plan antivirus protection for SharePoint Server.

QUESTION NO: 28

John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail. Which of the following techniques is he performing to accomplish his task?

A. Web ripping

B. Email spoofing

C. Steganography

D. Social engineering

ANSWER: C

Explanation:

Steganography is the practice of concealing information within another, apparently ordinary file or communication so that the existence of the hidden information is not readily apparent. In this scenario, the confidential file is embedded inside an image using an image-hiding tool. The resulting image can look like a normal photograph while carrying an additional concealed payload, allowing the sender to transmit sensitive data without placing the secret content visibly in the email body or as an obvious document attachment. This matches the central goal of steganography: hiding the presence of a message rather than merely protecting its readability. A mail gateway that only performs basic filtering based on file type, visible content, or conventional attachment signatures may treat the item as an ordinary image unless it performs content inspection, steganalysis, or enforces controls that restrict outbound image attachments. NIST describes steganography as hiding information within other data, and its glossary distinguishes the concept from cryptography, which focuses on rendering information unintelligible to unauthorized parties. Organizations can reduce this data-exfiltration risk through egress filtering, data-loss-prevention controls, attachment inspection, and monitoring of outbound communications. See the NIST definition of steganography and NIST's data exfiltration glossary entry.

QUESTION NO: 29

Availability Management allows organizations to sustain the IT service availability to support the business at a justifiable cost. Which of the following elements of Availability Management is used to perform at an agreed level over a period of time?

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

A. Maintainability

B. Resilience

C. Error control

D. Recoverability

E. Reliability

F. Security

G. Serviceability

ANSWER: A B D E F G

Explanation:

Availability Management sustains agreed service levels by addressing several related service-quality characteristics together. **Reliability** is the characteristic most directly associated with performing an agreed function without interruption for a specified period. It therefore expresses whether a service continues to deliver the required level of operation over time. **Maintainability**, **Serviceability**, and **Recoverability** support that sustained operation by ensuring that faults can be

repaired, supplier support can be obtained, and service operation can be restored within agreed targets. **Resilience** supports continued delivery when components, dependencies, or operating conditions fail or are disrupted. **Security** is also integral to availability because security events and inadequate safeguards can prevent legitimate users from accessing or using a service at its agreed level. These characteristics are considered collectively when designing, measuring, and improving service availability at a cost justified by business requirements. Service-management guidance describes Availability Management as ensuring that services deliver agreed availability levels, while resilience engineering emphasizes the ability to anticipate, withstand, recover from, and adapt to disruption. See ServiceNow's Availability Management overview and NIST SP 800-160, Systems Security Engineering.

QUESTION NO: 30

You work as the Security Administrator for Prodotxiss Inc. You want to ensure the security of your Wi-Fi enterprise network against the wireless snooping attacks. Which of the following measures will you take over the site network devices of the network?

A. Apply firewalls at appropriate spots.

B. Download and install new firmware patch for the router.

C. Disable the SSID broadcast feature of the router.

D. Apply a standard ACL on the router.

E. Configure WPA3-Enterprise Wi-Fi security with 802.1X authentication and strong encryption.

ANSWER: E

Explanation:

Configure WPA3-Enterprise (or WPA2-Enterprise where WPA3 is not supported) with strong encryption and 802.1X authentication to protect a wireless enterprise network from snooping. Wireless traffic is transmitted over radio frequencies and can be captured by anyone within range, so the essential protection is cryptographic confidentiality of the frames, not simply making the network less visible. Enterprise Wi-Fi authentication uses an authentication server and unique credentials or certificates for users, rather than a single shared passphrase. This also enables centralized access control and makes it practical to revoke an individual user's access without changing credentials for every device. WPA3-Enterprise provides stronger protections and, when available, is the preferred modern choice; WPA2-Enterprise remains a widely deployed secure baseline when properly configured. Administrators should use protected management frames where supported, select strong authentication methods such as certificate-based EAP-TLS, and ensure legacy insecure wireless security modes are not permitted. The Wi-Fi Alliance describes WPA3 security capabilities at https://www.wi-fi.org/discover-wi-fi/security, and the National Institute of Standards and Technology provides enterprise WLAN security guidance in NIST SP 800-153.

QUESTION NO: 31

Which of the following concepts represent the three fundamental principles of information security?

Each correct answer represents a complete solution. Choose three.

A. Privacy

B. Availability

C. Integrity

D. Confidentiality

ANSWER: B C D

Explanation:

The fundamental principles of information security are confidentiality, integrity, and availability, commonly called the CIA triad. **Confidentiality** means protecting information from unauthorized access or disclosure, so that only authorized people, processes, and systems can view sensitive data. **Integrity** means preserving the accuracy, completeness, and authorized state of information and systems; data must not be altered, destroyed, or manipulated improperly. **Availability** means ensuring that authorized users can access information and related systems when they need them. This includes resilience against outages, failures, denial-of-service events, and other conditions that could prevent legitimate access. Together, these principles provide a foundational model for identifying security requirements, evaluating risks, and selecting safeguards. A security control can support one or more of these principles—for example, access controls support confidentiality, hashing can help verify integrity, and redundancy supports availability. The National Institute of Standards and Technology identifies security objectives that directly align with this model in its information-security guidance. See NIST's definition of confidentiality and NIST's definition of integrity.

QUESTION NO: 32

You work as a Network Administrator for McRoberts Inc. You are required to upgrade a client computer on the company's network to Windows Vista Ultimate. During installation, the computer stops responding, and the screen does not change. What is the most likely cause?

A. Teardrop attack

B. Replay attack

C. Denial-of-Service (DoS) attack

D. Polymorphic shell code attack

ANSWER: C

Explanation:

Denial-of-Service (DoS) attack is correct because a DoS condition is defined by the loss of availability of a system or service. In this scenario, the client computer becomes unresponsive during the operating-system upgrade: it no longer processes the installation normally and the display remains unchanged. That observable loss of responsiveness is consistent with a resource-exhaustion or availability-disruption event, which is the core effect associated with denial of service. A DoS attack may consume processing capacity, memory, network bandwidth, or other system resources to the point that legitimate work cannot continue. Availability is one of the fundamental security objectives addressed in information-security practice, and preventing or recovering from disruptions that make a system unavailable is central to maintaining it. The U.S. Cybersecurity and Infrastructure Security Agency describes DoS attacks as actions that prevent users from accessing systems, networks, or other resources, while NIST's glossary similarly characterizes denial of service in terms of preventing authorized access to resources. These definitions align with the computer's apparent inability to continue the installation process. See CISA: Understanding Denial-of-Service Attacks and NIST CSRC: Denial of Service.

QUESTION NO: 33

Which of the following types of virus is capable of changing its signature to avoid detection?

A. Stealth virus

B. Boot sector virus

C. Macro virus

D. Polymorphic virus

ANSWER: D

Explanation:

Polymorphic virus is correct because it modifies its detectable code pattern, or signature, as it replicates or infects additional files. Typically, the virus encrypts or otherwise transforms its payload and changes the associated decryption

routine, producing many distinct byte sequences while retaining the same malicious function. This variation makes simple signature-based antivirus detection less reliable, since a static pattern observed in one instance may not appear in the next. Security tools therefore supplement traditional signatures with heuristic analysis, behavioral monitoring, emulation, and machine-learning or reputation-based detections to identify suspicious actions despite code changes. The technique is specifically intended to evade detection mechanisms that depend on recognizing known malware patterns. The UK National Cyber Security Centre describes how malware can use obfuscation and packing to make static analysis and detection more difficult, concepts closely related to the code-changing behavior used by polymorphic malware: NCSC Malware Analysis. MITRE also documents obfuscated or compressed files and information as a defense-evasion technique used to conceal malicious content from security tools: MITRE ATT&CK T1027.

QUESTION NO: 34

Which of the following refers to the ability to ensure that the data is not modified or tampered with?

A. Availability

B. Integrity

C. Confidentiality

D. Non-repudiation

ANSWER: B

Explanation:

Integrity is the security property that ensures information remains accurate, complete, and unaltered except through authorized and intended changes. In the CIA triad, integrity applies both to stored data and to data in transit: an organization must be able to detect or prevent unauthorized modification, deletion, insertion, or corruption. Common controls that support integrity include cryptographic hashes, message authentication codes, digital signatures, access controls, file-permission management, database constraints, audit logging, and version control. For example, a recipient can calculate a hash of a downloaded file and compare it with a trusted published hash; a mismatch indicates that the file may have been changed. Digital signatures additionally provide cryptographic evidence that a signed message has not been altered since it was signed. The National Institute of Standards and Technology defines integrity as guarding against improper information modification or destruction, including assurance of information non-repudiation and authenticity in some contexts. This makes **Integrity** the term that directly describes protection against data being modified or tampered with. See the NIST CSRC definition of integrity and the CISA overview of confidentiality, integrity, and availability.

QUESTION NO: 35

You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company. The suspected employee is using an online e-mail system such as Hotmail or Yahoo. Which of the following folders on the local computer will you review to accomplish the task?

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

A. Cookies folder

B. Temporary Internet Folder

C. Download folder

D. History folder

ANSWER: A B D

Explanation:

"Cookies folder," "Temporary Internet Folder," and "History folder
" are appropriate locations to review when investigating use of web-based email from a local computer. A browser history

database can establish that the employee visited a particular webmail provider, identify relevant URLs, and help construct a timeline of webmail activity. Cached web content, historically stored in the Temporary Internet Files area and now commonly held in browser cache directories, can preserve downloaded attachments, images, page resources, and remnants of viewed web content. Cookies can identify webmail domains used by the browser and may contain account-related identifiers, preference data, or session artifacts that assist correlation with other evidence. Together, these browser artifacts can support an investigation by showing access to online email services and guiding collection of associated local artifacts. Examiners should preserve the system state where appropriate, acquire data using forensically sound procedures, and document timestamps and paths because browser data is subject to deletion, expiration, and overwrite. NIST's guidance on collecting and preserving digital evidence is available in NIST SP 800-86. The CISA Digital Forensics and Incident Response resources also provide relevant evidence-handling context.

QUESTION NO: 36

Which of the following is an organization that defines standards for anti-virus software?

A. ICSA

B. IETF

C. IIS

D. IEEE

ANSWER: A

Explanation:

ICSA is correct. The International Computer Security Association, through ICSA Labs, was a recognized security-product testing and certification organization. Its anti-virus certification program established criteria that products had to meet for capabilities such as detecting malware, disinfecting infected files where applicable, and maintaining reliable operation. Vendors could submit anti-virus products for independent evaluation against these published requirements, making ICSA a standards and certification body in the anti-virus product ecosystem. In the context of foundational security terminology and legacy certification material, "ICSA" commonly refers to this role: defining testing criteria and validating whether security products conform to them. This is distinct from simply developing a technology or operating an Internet service; the essential point is the organization's product-assurance and certification function. ICSA Labs' historical materials and certification information are available through its ICSA Labs website. For broader context on malware defenses and the importance of anti-malware protections within an organizational security program, see NIST's guidance on malware incident prevention and handling.