DUMPSBOSS.

GIAC Information Security Professional

GIAC GISP

Version Demo

Total Demo Questions: 57

Total Premium Questions: 579

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security and Risk Management	44
Topic 2, Asset Security	32
Topic 3, Security Architecture and Engineering	78
Topic 4, Communication and Network Security	226
Topic 5, Identity and Access Management	72
Topic 6, Security Assessment and Testing	15
Topic 7, Security Operations	99
Topic 8, Software Development Security	12
Topic 9, Mix Questions	1
Total	579

QUESTION NO: 1

Which of the following is the rating for electronic or computer fires?

A. Class B

B. Class C

C. Class D

D. Class A

ANSWER: B

Explanation:

Class C is the correct fire classification for fires involving energized electrical equipment, including computers, electronic devices, wiring, circuit breakers, and other equipment that remains connected to an electrical power source. The defining safety consideration is that the extinguishing agent must not conduct electricity, because using a conductive agent on energized equipment could expose the person fighting the fire to electrical shock. Suitable agents commonly include carbon dioxide and clean-agent extinguishers; dry chemical extinguishers may also be rated for this use. Once electrical power is disconnected, the remaining burning material may be classified according to its fuel type, such as ordinary combustibles. For workplace fire safety, personnel should first activate the alarm, notify emergency responders, and attempt to use an extinguisher only when trained, when there is a safe escape route, and when the fire is small and contained. OSHA identifies Class C fires as those involving energized electrical equipment, and the National Fire Protection Association similarly defines Class C as fires involving energized electrical equipment. See OSHA's portable fire extinguisher guidance and NFPA fire extinguisher guidance.

QUESTION NO: 2

Which of the following are politically motivated threats that an organization faces?

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

A. Power distribution outages

B. Civil disobedience

C. Riot

D. Terrorist attacks

E. Vandalism

ANSWER: B C D E

Explanation:

Politically motivated threats are actions intended to influence government policy, advance an ideological cause, protest perceived injustice, or create social disruption in support of a political objective. **Civil disobedience** can directly affect an organization through demonstrations, blockades, sit-ins, or refusal to comply with laws or directions, particularly when an organization is associated with a contested policy or industry. A **riot** may create politically driven disorder that threatens personnel, facilities, operations, and physical assets. **Terrorist attacks** are a significant politically or ideologically motivated threat because they use or threaten violence to intimidate populations or coerce governments and other entities. **Vandalism** can also be politically motivated when property is damaged to communicate a protest message, target a symbolic organization, or disrupt its activities. These threats should be considered in organizational risk assessment and continuity planning because they can affect physical security, personnel safety, facility access, and service availability. The U.S. Department of Homeland Security discusses terrorism and targeted violence preparedness in its terrorism and homeland-security threats guidance, while the FBI provides resources concerning threats to businesses and critical infrastructure through its terrorism program.

QUESTION NO: 3

Which of the following statements about Secure Sockets Layer (SSL) are true?

Each correct answer represents a complete solution. Choose two.

A. It provides communication privacy, authentication, and message integrity.

B. It provides mail transfer service.

C. It provides connectivity between Web browser and Web server.

D. It uses a combination of public key and symmetric encryption for security of data.

ANSWER: A D

Explanation:

“It provides communication privacy, authentication, and message integrity.” is correct because SSL, and its modern successor TLS, was designed to protect data exchanged over an untrusted network. The protocol negotiates cryptographic parameters and establishes a protected session. Encryption provides confidentiality (communication privacy), certificate-based authentication enables a client to validate the identity asserted by the server, and cryptographic integrity protection detects unauthorized modification of protected records. These security services remain the core objectives of TLS as used for HTTPS and other application protocols.

“It uses a combination of public key and symmetric encryption for security of data.” is also correct. SSL/TLS uses asymmetric cryptography during authentication and key establishment, such as validating a server certificate and agreeing or deriving shared secret material. The resulting session keys are then used with symmetric encryption and integrity mechanisms to protect bulk application data efficiently. This hybrid approach combines the identity and key-establishment benefits of public-key cryptography with the performance of symmetric cryptography for ongoing communications. The historical SSL 3.0 protocol specification describes the handshake and record-layer model, while NIST provides current guidance for the TLS protocols that superseded SSL. See RFC 6101 and NIST SP 800-52 Rev. 2.

QUESTION NO: 4

Which of the following OSI model layers handles translation of data into standard format, data compression, and decompression?

A. Application

B. Physical

C. Presentation

D. Session

ANSWER: C

Explanation:

The **Presentation** layer is responsible for representing data in a format that communicating applications can understand. In the seven-layer OSI reference model, it sits between the Application and Session layers and acts as a syntax and format translator for application data. Its functions include converting character encodings and data formats, such as translating between different text representations or serializing structured data into an agreed form. It also handles data compression and decompression, which can reduce the amount of data sent across a network and restore it to its original form at the receiving end. Encryption and decryption are commonly associated with this layer as well, because they transform the representation of data while preserving its meaning for the application. These services help systems with differing internal data representations exchange information reliably. The OSI model is a conceptual framework, so modern protocol stacks do not always implement these functions as a distinct layer; nevertheless, translation, compression, and encryption remain the canonical responsibilities assigned to the Presentation layer. See the ISO OSI Basic Reference Model (ISO/IEC 7498-1) and the IBM overview of the OSI model.

QUESTION NO: 5

Where are user accounts and passwords stored in a decentralized privilege management environment?

A. On each server.

B. On a central authentication server.

C. On more than one server.

D. On a server configured for decentralized privilege management.

ANSWER: A

Explanation:

In a decentralized privilege management environment, user accounts and password information are maintained locally on each individual server or system. Each host therefore has its own account database and performs authentication using credentials stored on that host, rather than relying on a single, shared authentication authority. This model gives each system independent control over its local users and privileges, but it also requires administrators to provision, update, and remove accounts separately across all relevant servers. In practice, local account information on Unix-like systems is commonly represented through files such as `/etc/passwd` and protected password-hash storage such as `/etc/shadow`; Windows systems similarly maintain local accounts in the Security Accounts Manager database. Centralized identity services, by contrast, consolidate authentication data into a directory or identity provider. The distinction matters for access governance: decentralized management can increase administrative overhead and make consistent credential and privilege lifecycle management more difficult. NIST describes account management as the creation, enabling, modification, disabling, and removal of accounts, activities that must be performed for each locally managed system in this architecture. See NIST SP 800-53, Account Management and Linux passwd(5) documentation.

QUESTION NO: 6

Which of the following protocols allows Cisco devices to acquire and utilize digital certificates from Certification Authorities (CAs)?

A. Extensible Authentication Protocol (EAP)

B. Certificate Management Protocol (CMP)

C. Hypertext Transfer Protocol (HTTP)

D. Certificate Enrollment Protocol (CEP)

ANSWER: D

Explanation:

Certificate Enrollment Protocol (CEP) is correct. Cisco devices use CEP, commonly associated with the Simple Certificate Enrollment Protocol (SCEP), to automate interaction with a certification authority for public-key certificate operations. Through this enrollment process, a Cisco device can generate or submit a certificate-signing request, obtain an identity certificate issued by the CA, and retrieve CA certificate information needed to establish trust. The enrolled certificate and its corresponding private key can then support Cisco IOS PKI features and services that require certificate-based authentication or encryption, such as IPsec VPNs, SSL/TLS services, and secure device identity validation.

Cisco documentation describes configuring a PKI trustpoint with an enrollment URL using the `enrollment url` command, including the `http://.../cgi-bin/pkiclient.exe` format historically used for SCEP/CEP enrollment. This makes CEP the protocol specifically intended to let Cisco network devices request and receive certificates from a CA rather than merely transporting web content or performing an access-authentication exchange. The IETF's SCEP specification also defines the protocol's certificate-enrollment and CA-certificate-retrieval functions. See Cisco IOS PKI enrollment documentation and RFC 8894: Simple Certificate Enrollment Protocol.

QUESTION NO: 7

Which of the following encryption strengths is used to secure NTLM version 2 passwords?

A. 128-bit

B. 32-bit

C. 64-bit

D. 56-bit

ANSWER: A

Explanation:

128-bit is correct. NTLM version 2 strengthens the earlier NTLM authentication design by using a challenge-response process based on an NT password hash and a cryptographic response generated with HMAC-MD5. The resulting NTLMv2 response is 128 bits in length, which is why NTLMv2 is commonly described in security documentation and exam material as using 128-bit encryption strength. Importantly, NTLMv2 does not transmit a user's plaintext password across the network. Instead, the client proves knowledge of secret password-derived material by calculating a response to a server-provided challenge, with additional data such as a client challenge and timestamp helping resist replay attacks. Microsoft's NTLM protocol documentation describes the NTLMv2 response construction and identifies its 16-byte response fields, equivalent to 128 bits. Microsoft also documents NTLM as an authentication protocol used when Kerberos is unavailable or cannot be used. For implementation-level protocol details, see Microsoft's NTLM protocol specification. For Microsoft's overview of NTLM and its role in Windows authentication, see NTLM overview.

QUESTION NO: 8

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully performed the following steps of the preattack phase to check the security of the We-are-secure network:

•Gathering information

•Determining the network range

•Identifying active systems

Now, he wants to find the open ports and applications running on the network. Which of the following tools will he use to accomplish his task?

A. ARIN

B. APNIC

C. SuperScan

D. RIPE

ANSWER: C

Explanation:

SuperScan is correct because it is a network scanning utility designed to enumerate services exposed by target hosts. After defining the target range and identifying live systems, an ethical tester uses a port scanner to determine which TCP or UDP ports accept connections. Those open ports indicate network services that may be reachable, such as web, mail, file-sharing, or remote-administration services. SuperScan performs this reconnaissance function and can conduct port scans along with service-related enumeration, helping the tester build an accurate picture of the target attack surface. This information is essential before any authorized vulnerability validation, because testing must be directed at the services actually available on each discovered host. SuperScan is specifically described as a Windows TCP port scanner and is therefore aligned with the task of locating open ports and identifying running applications/services. Its role fits the active-

scanning stage that follows passive information gathering, network-range identification, and live-host discovery. See the SuperScan entry at SecTools and the Nmap port-scanning overview for the general security-testing principle that open-port discovery identifies reachable services.

QUESTION NO: 9

Which of the following tools was developed by the FBI and is used for keystroke logging in order to capture encryption keys and other information useful for deciphering transmissions?

A. Alchemy Remote Executor

B. Stealth Voice Recorder

C. KeyGhost USB keylogger

D. KeyGhost keylogger

E. Magic Lantern

ANSWER: E

Explanation:

Magic Lantern is correct. It is the name publicly associated with an FBI-developed software keystroke logger, sometimes described as a “computer and internet protocol address verifier” in discussions of lawful investigative monitoring. Its intended investigative value was to record a user’s keystrokes before encryption occurred. This can allow investigators, subject to appropriate legal authorization, to obtain plaintext communications, passphrases, or cryptographic keys at the endpoint rather than attempting to defeat strong encryption while data is in transit.

This endpoint-focused concept is important: encryption protects data as it travels or is stored, but a user must enter or otherwise make available a password or key to encrypt, decrypt, or access protected information. Keystroke logging can capture that information at the moment of entry. Contemporary reporting and privacy analysis identified Magic Lantern as an FBI keystroke-logging tool and discussed its relationship to court-authorized surveillance and encryption investigations. See the Electronic Privacy Information Center’s Magic Lantern overview and the FBI’s encryption information page for context on the investigative challenges posed by encrypted communications.

QUESTION NO: 10

Which of the following statements about the availability concept of Information security management is true?

A. It ensures that modifications are not made to data by unauthorized personnel or processes.

B. It determines actions and behaviors of a single individual within a system.

C. It ensures reliable and timely access to resources.

D. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.

ANSWER: C

Explanation:

“It ensures reliable and timely access to resources.” correctly describes availability, one of the three foundational objectives of information security alongside confidentiality and integrity. Availability means that authorized users can access information, systems, applications, and supporting infrastructure when they need them. The objective is not merely that a service is functioning at some point; it must remain dependable and accessible within the time frames required by the organization’s mission and business processes.

In practice, availability is supported through resilience and operational safeguards such as redundancy, backups, capacity management, system monitoring, preventive maintenance, incident response, and disaster recovery planning. These controls reduce the likelihood and impact of outages caused by equipment failures, software defects, human error,

environmental events, or denial-of-service conditions. Security practitioners assess availability in terms of service uptime, recovery objectives, and the ability to continue or restore essential operations following disruption. NIST defines availability as timely and reliable access to and use of information, which directly matches the statement. See the NIST CSRC definition of availability and the NIST glossary for the security-objective context.

QUESTION NO: 11

You work as a Web Developer for WebCrunch Inc. You create a web site that contains information about the company's products and services. The web site is to be used by the company's suppliers only. Which of the following options will you use to specify the nature of access to the web site?

A. Intranet

B. Internet and Intranet

C. Internet

D. Extranet

ANSWER: D

Explanation:

Extranet is the correct designation because the website is intended for a defined group outside WebCrunch Inc.—its suppliers—rather than solely for internal employees or for the unrestricted public. An extranet extends selected organizational information, services, or applications to authorized external parties such as suppliers, business partners, customers, or contractors. Access is typically controlled through authentication, authorization, and secure network connections, ensuring that suppliers can reach the resources needed for their business relationship while information remains protected from general Internet users.

This model supports common supplier-facing functions, including product documentation, ordering information, inventory visibility, support materials, and collaboration workflows. The organization determines which information each supplier role may access and enforces least privilege, ideally with account lifecycle controls and multifactor authentication where appropriate. NIST describes external users as a distinct access population that must be governed through access-control policy and authorization mechanisms; these principles directly support an extranet implementation. See NIST SP 800-53 Rev. 5 for access-control guidance and IBM's overview of extranets for the definition and common business use of an extranet.

QUESTION NO: 12

In which of the following attacks does an attacker send a spoofed TCP SYN packet in which the target's IP address is filled in both the source and destination fields?

A. Jolt DoS attack

B. Ping of death attack

C. Teardrop attack

D. Land attack

ANSWER: D

Explanation:

Land attack is correct because it uses a spoofed TCP SYN packet whose source IP address and destination IP address are both set to the victim's address. In the classic form of this denial-of-service technique, the attacker also uses the same TCP port as both the source and destination port. This causes the target to receive what appears to be a connection request from itself. Vulnerable TCP/IP implementations could enter an unstable processing condition while attempting to handle the self-referential connection, consuming resources or potentially causing a system crash. The defining characteristic is therefore

the intentional use of the target's own network address in both address fields, rather than merely sending a large, fragmented, or malformed packet. Although modern operating systems and network devices generally include protections against this historical attack, recognizing its packet construction remains important when interpreting attack terminology and reviewing suspicious packet captures. The CISA alert on the LAND attack vulnerability describes the use of identical source and destination addresses. Additional technical background appears in the TCP specification, RFC 793, which defines the TCP connection and segment fields targeted by this attack.

QUESTION NO: 13

Which of the following components come under the network layer of the OSI model?

Each correct answer represents a complete solution. Choose two.

A. Firewalls

B. Hub

C. Routers

D. MAC addresses

ANSWER: A C

Explanation:

Firewalls and **Routers** are the intended Network-layer components. The OSI Network layer, Layer 3, provides logical addressing and routing: it determines how packets are forwarded between separate networks. Routers are the canonical Layer 3 device because they examine destination IP addresses, consult routing information, and forward packets toward their destination network. Cisco's overview of routing describes routers as devices that connect networks and forward packets based on Layer 3 addressing.

Firewalls are often described as operating across multiple OSI layers, particularly in modern next-generation implementations. However, a traditional packet-filtering firewall is commonly classified at the Network layer because it evaluates Layer 3 information, such as source and destination IP addresses, and can enforce policy on IP traffic moving between networks. This classification is appropriate for the question's conventional OSI-device mapping. The Network layer's relationship to IP packet forwarding is described in the Internet Protocol requirements in RFC 1122, while Cisco provides a practical description of router functions and packet forwarding.

QUESTION NO: 14

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

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

A. Snort

B. SARA

C. Samhain

D. Tripwire

ANSWER: A C D

Explanation:

Snort, **Samhain**, and **Tripwire** can each support intrusion detection and alerting in a Linux environment. Snort is a network intrusion detection system that analyzes network traffic against rule sets and can generate alerts when it identifies suspicious

packets, known attack signatures, or policy violations. Its deployment is appropriate when the objective is to observe attempted attacks reaching or traversing the protected server's network segment.

Samhain is host-based intrusion-detection software. It monitors host security-relevant conditions, including file integrity, logs, processes, and other system-state information, and can report detected changes or suspicious events. Tripwire likewise provides host-based file integrity monitoring, establishing a trusted baseline and alerting when monitored files or system objects are modified unexpectedly. Unauthorized changes to executables, configuration files, or other critical assets are important indicators of a possible compromise. Using network-focused detection with Snort and host-focused detection with Samhain or Tripwire provides complementary visibility into hacking attempts and their effects on the server. See the Snort project and Tripwire Open Source documentation.

QUESTION NO: 15

Fill in the blank with the appropriate value.

Primary Rate Interface (PRI) of an ISDN connection contains _____ B channels and _____ D channel.

A. 23 B channels and 1 D channel

ANSWER: A

Explanation:

The appropriate value is **23 B channels and 1 D channel** for the conventional North American ISDN Primary Rate Interface. PRI is delivered over a T1 circuit, which provides 24 time slots of 64 Kbps each. Of those time slots, 23 are bearer (B) channels used to carry user traffic such as voice or data. The remaining slot is the data/signaling (D) channel, which carries call-control signaling for the associated B channels. This division is commonly expressed as 23B+D and provides an aggregate bearer capacity of 1.472 Mbps, with the 64-Kbps D channel reserved for signaling. This is the PRI format generally expected in U.S.-centric networking and security training material. PRI formats can vary by regional carrier infrastructure; for example, E1-based PRI deployments commonly use 30 bearer channels and one signaling channel. However, the T1-based 23B+D arrangement is the applicable completion when the question presents PRI without identifying an E1-based regional implementation. Cisco's ISDN overview describes PRI signaling and channel structures, while the ITU-T ISDN recommendation provides the underlying framework for integrated-services digital networks. See Cisco ISDN PRI documentation and ITU-T Recommendation I.430.

QUESTION NO: 16

Which of the following tools is used for breaking digital watermark?

A. TRACERT

B. Trin00

C. Fpipe

D. 2Mosaic

ANSWER: D

Explanation:

2Mosaic is the correct answer because it is associated with attacks against image watermarking schemes. Digital watermarks embed ownership or other identifying information into media while attempting to maintain the media's apparent quality. A watermark-breaking attack seeks to alter the image in a way that preserves enough visual usefulness for the image to remain valuable but disrupts the embedded watermark so that it cannot be reliably detected or decoded. Mosaic-based transformations are one technique used in research and testing of watermark robustness: they reorganize or reconstruct image content in a manner that can defeat watermark synchronization and detection mechanisms. Thus, 2Mosaic belongs in the category of tools or attack approaches used to challenge, remove, or invalidate digital watermarks. Understanding such attacks is important to evaluating whether a watermarking implementation remains resilient after realistic content transformations and malicious manipulation. Watermarking research commonly evaluates robustness

against signal-processing and geometric attacks, as documented by the University of Cambridge watermarking resources. The broader security objective of digital watermarking, including resistance to removal and tampering, is also discussed by the U.S. Copyright Office.

QUESTION NO: 17

Which of the following statements about the One Time Password (OTP) security system are true?

Each correct answer represents a complete solution. Choose two.

A. It requires a password only once to authenticate users.

B. It requires a new password every time a user authenticates himself.

C. It generates passwords by using either the MD4 or MD5 hashing algorithm.

D. It generates passwords by using Kerberos v5.

ANSWER: B C

Explanation:

“It requires a new password every time a user authenticates himself.” is correct because an OTP is intended to be valid for one authentication event only. After use, the value cannot be reused successfully, which prevents a captured credential from functioning as a replayable password. OTP systems may produce these values from a shared secret and a moving factor, such as a counter or time value, or from a chained sequence of cryptographic hash operations. This one-use property is the essential security characteristic of OTP authentication. NIST describes one-time passwords as secrets that are used only once and identifies OTP authenticators as a recognized authentication mechanism; see NIST SP 800-63B.

“It generates passwords by using either the MD4 or MD5 hashing algorithm.” is also correct in the context of the standardized S/KEY-style OTP system. RFC 2289 specifies an OTP scheme in which a secret passphrase is repeatedly hashed and includes MD4 and MD5 among its defined hash-function choices (as well as SHA-1). Thus, MD4 or MD5 can be used to generate the one-time password sequence in that OTP design. The protocol details and supported algorithms are documented in RFC 2289.

QUESTION NO: 18

Which of the following are examples of multifactor authentication?

Each correct answer represents a complete solution. Choose two.

A. A password and a one-time code from an authenticator application

B. A smart card and a PIN

C. Two different passwords

D. A username and a password

ANSWER: A B

Explanation:

Multifactor authentication requires authenticators from at least two different factor categories, such as something you know, something you have, and something you are. A password combined with a one-time code from an authenticator application combines a knowledge factor with a possession factor. A smart card combined with a PIN also combines possession and knowledge factors. Two passwords are not multifactor authentication because both are knowledge factors. NIST describes the authenticator categories and multifactor authentication requirements in NIST SP 800-63B.

QUESTION NO: 19

You work as a Network Administrator for Web World Inc. You want to host an e-commerce Web site on your network. You want to ensure that storage of credit card information is secure. Which of the following conditions should be met to accomplish this?

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

A. NT authentication should be required for all customers before they provide their credit card numbers.

B. The NTFS file system should be implemented on a client computer.

C. Strong encryption software should be used to store credit card information.

D. Limited and authorized access should be allowed on the stored credit card information.

ANSWER: C D

Explanation:

Strong encryption software should be used to store credit card information because payment-card data at rest must be rendered unreadable to anyone who obtains the underlying storage, backups, database exports, or files without authorization. Effective protection requires industry-accepted cryptography, secure key generation and storage, tightly controlled access to cryptographic keys, and procedures for key rotation and retirement. Encryption protects the confidentiality of stored account data even when another storage or system-level control fails.

Limited and authorized access should be allowed on the stored credit card information because access control is a core part of protecting cardholder data. Access should be restricted according to business need and least privilege, with unique identities, authentication, authorization, and logging sufficient to ensure that only approved personnel and services can retrieve or process the data. These controls also reduce the number of people and systems exposed to sensitive information, making monitoring and incident response more effective.

These practices align with PCI DSS requirements to protect stored account data using strong cryptography and to restrict access to system components and cardholder data based on business need to know. See the PCI Security Standards Council document library and NIST guidance on cryptographic key management.

QUESTION NO: 20

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

Each correct answer represents a complete solution. Choose three.

A. Integrity

B. Privacy

C. Confidentiality

D. Availability

ANSWER: A C D

Explanation:

The three fundamental principles are integrity, confidentiality, and availability, commonly called the CIA triad. Integrity means safeguarding information and systems against unauthorized or improper modification or destruction, so that information remains accurate, complete, and trustworthy. Confidentiality means preserving authorized restrictions on access and disclosure, ensuring sensitive information is accessible only to authorized people, processes, and systems. Availability means ensuring timely, reliable access to information and systems for authorized users when they need them. Together, these objectives provide a foundational model for identifying security requirements, selecting controls, assessing risks, and responding to security events. For example, access control and encryption primarily support confidentiality; change control, hashes, and digital signatures can support integrity; and redundancy, backups, patching, and resilience planning support

availability. These principles are explicitly defined as core information-security objectives in NIST guidance and are central to security governance and risk management. See NIST's confidentiality glossary entry and NIST's definition of information security.

QUESTION NO: 21

Which of the following are characteristics of a properly implemented public key infrastructure (PKI)?

Each correct answer represents a complete solution. Choose three.

A. A certificate authority issues signed certificates.

B. A private key must be protected by its owner.

C. Certificate status can be checked through a CRL or OCSP.

D. A public key must remain confidential.

ANSWER: A B C

Explanation:

A public key infrastructure manages certificates and the cryptographic keys associated with them. A certificate authority (CA) issues and signs certificates that bind a subject identity to a public key. Certificate revocation information, such as a certificate revocation list (CRL) or Online Certificate Status Protocol (OCSP) response, helps relying parties determine whether a certificate should no longer be trusted before its stated expiration date. The certificate subject must protect the associated private key because possession of that key enables the cryptographic operations associated with the certificate.

The public key may be distributed openly and is not required to remain confidential. It is specifically intended to be available to parties that need to validate signatures or establish encrypted communications with the key holder. RFC 5280 defines the X.509 certificate and CRL profile used in Internet PKI deployments. See RFC 5280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

QUESTION NO: 22

Which of the following statements about a fiber-optic cable are true?

Each correct answer represents a complete solution. Choose three.

A. It is immune to electromagnetic interference (EMI).

B. It can transmit undistorted signals over great distances.

C. It has eight wires twisted into four pairs.

D. It uses light pulses for signal transmission.

ANSWER: A B D

Explanation:

Fiber-optic cable transmits data as pulses of light through a glass or plastic core rather than as electrical current through metal conductors. Consequently, it is immune to electromagnetic interference (EMI), a major advantage in environments with electrical equipment, motors, radio-frequency sources, or nearby power cabling. Because optical fiber does not conduct electricity, it also avoids electrical noise coupling that can affect copper media.

Fiber supports high-bandwidth communications over substantially greater distances than typical copper Ethernet cabling while maintaining signal integrity. Although real-world fiber links are engineered around attenuation and dispersion budgets and may require optical transceivers or regeneration at long distances, fiber is specifically well suited to transmitting signals reliably across long runs. The light-pulse transmission method is the fundamental operating principle that enables these characteristics. Cisco's overview of fiber media discusses light propagation and its resistance to electromagnetic

interference: Cisco: What Is Fiber Optic Cable?. The U.S. National Institute of Standards and Technology also describes optical fiber as a communications medium that carries information using light: NIST: Optical Fiber Measurements.

QUESTION NO: 23

Which of the following security models deal only with integrity?

Each correct answer represents a complete solution. Choose two.

A. Biba

B. Bell-LaPadula

C. Biba-Wilson

D. Clark-Wilson

ANSWER: A D

Explanation:

Biba and **Clark-Wilson** are integrity-focused security models. The Biba Integrity Model was designed specifically to preserve the trustworthiness of information by preventing improper modification and contamination of data. Its core rules control information flow according to integrity levels: subjects should not read data at a lower integrity level, and they should not write data to a higher integrity level. These restrictions are intended to ensure that decisions and records are based on sufficiently trustworthy data.

The Clark-Wilson model also addresses integrity, but does so through well-formed transactions and separation of duties. It distinguishes constrained data items from unconstrained input, requires authorized transformation procedures to modify protected data, and uses integrity-verification procedures to confirm that data remains in a valid state. This makes the model especially applicable to commercial systems, such as financial and business-processing environments, where only controlled procedures should alter critical records. NIST describes integrity as guarding against improper information modification or destruction and ensuring information authenticity; both models directly implement that objective. See NIST's integrity definition and the NIST security handbook.

QUESTION NO: 24

Which of the following encryption algorithms are based on symmetric key cryptographic algorithms?

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

A. RC5

B. AES

C. DSA

D. Blowfish

E. IDEA

ANSWER: A B D E

Explanation:

RC5, AES, Blowfish, and IDEA are symmetric-key encryption algorithms. Symmetric cryptography uses one shared secret key for both encryption and decryption; consequently, parties must establish and protect that shared key before confidential data can be exchanged. NIST describes symmetric-key cryptography as cryptography in which the same secret key is used to perform both the cryptographic transformation and its inverse, subject to the algorithm's defined operation. See the NIST definition of symmetric-key cryptography.

AES is the modern NIST-standardized symmetric block cipher and is specified in FIPS 197. RC5 is a parameterized symmetric block cipher with variable word size, number of rounds, and key length. Blowfish is a symmetric 64-bit block cipher designed for use with a variable-length secret key. IDEA is also a symmetric block cipher, using a 128-bit key to encrypt 64-bit blocks. These algorithms therefore all rely on a shared secret rather than a public/private key pair. The AES design and approved key sizes are specified in NIST FIPS 197.

QUESTION NO: 25

Fill in the blanks with the appropriate values.

International Data Encryption Algorithm (IDEA) is a _____ -bit block cipher that uses a _____-bit key.

A. 64-bit block cipher that uses a 128-bit key.

ANSWER: A

Explanation:

International Data Encryption Algorithm (IDEA) is a 64-bit block cipher that uses a 128-bit key. The block size identifies the amount of plaintext processed in each encryption operation: IDEA divides data into 64-bit blocks and transforms each block using its round structure. Its 128-bit key is divided into subkeys that are used across the algorithm's eight full rounds and final output transformation. These values are defining technical characteristics of IDEA, rather than configurable choices. RFC 3058, which specifies the use of IDEA in OpenPGP, explicitly describes IDEA as operating on 64-bit blocks with 128-bit keys. The algorithm was designed by Xuejia Lai and James Massey and combines operations from different algebraic groups—XOR, addition modulo 2^{16}, and multiplication modulo $2^{16} + 1$—to provide confusion and diffusion. In the context of security fundamentals, distinguishing a cipher's block size from its key length is important: the former concerns the fixed unit of data transformed at once, while the latter determines the size of the secret key space. See RFC 3058: Use of the IDEA Encryption Algorithm in OpenPGP and the IETF Datatracker version of RFC 3058.

QUESTION NO: 26

Which of the following are used to suppress electrical and computer fires?

Each correct answer represents a complete solution. Choose two.

A. Halon

B. Soda acid

C. CO2

D. Water

ANSWER: A C

Explanation:

Halon and CO2 are appropriate clean-agent extinguishing media for energized electrical and computer-equipment fires because neither agent is electrically conductive and both suppress fire without applying water or foam directly to sensitive electronic equipment. Carbon dioxide works primarily by displacing oxygen around the fire and is recognized by OSHA as suitable for Class C fires involving energized electrical equipment. Once electrical equipment has been de-energized, the fire's underlying fuel class determines the appropriate extinguishing method, but CO2 is specifically useful while electrical energy remains present. Halon agents interrupt the combustion reaction and leave no residue, which historically made them especially valuable for computer rooms, telecommunications systems, and other areas containing delicate electronics. Although production of most halons has been phased out because of ozone-depletion impacts, existing halon systems may still be used under regulated conditions, and modern clean-agent systems provide comparable residue-free protection. The National Fire Protection Association identifies clean-agent fire-extinguishing systems as systems that use electrically nonconductive, volatile, or gaseous extinguishants that leave no residue. See OSHA's portable fire extinguisher guidance and NFPA's overview of clean-agent fire-extinguishing systems.

QUESTION NO: 27

Which of the following is an authentication protocol?

A. LDAP

B. PPTP

C. TLS

D. Kerberos

ANSWER: D

Explanation:

Kerberos is an authentication protocol designed to verify the identities of users and services across an untrusted network. It uses a trusted third party, the Key Distribution Center (KDC), to issue time-limited cryptographic tickets. After a user authenticates, Kerberos can provide tickets that let the user access authorized services without repeatedly transmitting a password. This ticket-based approach supports mutual authentication: the client can validate the service's identity and the service can validate the client's identity. Kerberos is widely used in enterprise identity environments, including Microsoft Active Directory domains, where domain controllers perform the KDC role. Its reliance on symmetric-key cryptography, ticket lifetimes, and synchronized clocks helps reduce credential exposure and limits the usefulness of captured authentication data. The Internet Engineering Task Force specifies the protocol in RFC 4120, which describes the Kerberos network authentication service and its ticket-granting workflow. Microsoft also documents Kerberos as the default authentication protocol for Windows domain environments. See RFC 4120: The Kerberos Network Authentication Service and Microsoft's Kerberos authentication overview.

QUESTION NO: 28

Which of the following processes removes data from the media so that it is difficult to restore?

A. Overwriting

B. Degaussing

C. Sanitization

D. Declassification

ANSWER: C

Explanation:

Sanitization is correct because it is the overall process of making data stored on media inaccessible and unrecoverable to an unauthorized party, using techniques appropriate to the media type and the required level of protection. In media-disposition practice, sanitization addresses the risk that residual information may remain after a device is reassigned, released from organizational control, repaired, or disposed of. The intended result is that data recovery is infeasible or impractical using the capabilities assumed in the organization's security requirements.

NIST defines media sanitization as a process that renders access to target data on the media infeasible for a given level of effort. The process is selected based on the sensitivity of the data, the storage technology, whether the media will remain in use, and the organization's risk tolerance. Depending on those factors, a sanitization method can include clearing, purging, cryptographic erase where applicable, or physical destruction. This broad process-oriented definition directly matches the question's description of removing data from media so that restoration is difficult. See NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization and the NIST security and privacy guidance resources.

QUESTION NO: 29

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

A. Patent

B. Snooping

C. Copyright

D. Utility model

ANSWER: A

Explanation:

Patent is correct because a patent is a government-granted intellectual-property right that gives an inventor, or a permitted assignee, the exclusive right to prevent others from making, using, offering for sale, selling, or importing the claimed invention for a limited statutory term. In return for this limited monopoly, the patent application must describe the invention sufficiently clearly and completely for a person skilled in the relevant field to make and use it. This disclosure requirement serves the public interest: once the patent term expires, the disclosed technical knowledge is available for public use.

In the United States, utility patents generally have a term of 20 years from the earliest effective filing date, subject to applicable adjustments or extensions and payment of required maintenance fees. Patent protection is territorial, meaning rights are granted and enforced under the laws of the particular country or region that issues the patent. This definition is consistent with the World Intellectual Property Organization's explanation that patents provide exclusive rights in exchange for public disclosure, as well as the U.S. Patent and Trademark Office's description of the rights conveyed by a patent. See WIPO: Patents and USPTO: Patent process overview.

QUESTION NO: 30

Which of the following languages enable programmers to store cookies on client computers?

Each correct answer represents a complete solution. Choose two.

A. Perl

B. DHTML

C. JavaScript

D. HTML

ANSWER: A C

Explanation:

Perl and **JavaScript** enable a programmer to cause cookies to be stored in a user's browser. A Perl application commonly runs on the web server and can generate an HTTP response containing a `Set-Cookie` header. When the browser receives a valid response header, it stores the cookie subject to its attributes, browser policy, and applicable privacy controls. Perl's CGI facilities specifically support constructing cookie values and emitting them as HTTP headers before the response body is returned.

JavaScript can create or update cookies available to the current page through the browser's `document.cookie` interface. Script-created cookies are constrained by browser-enforced scope and attributes, such as `Path`, `Domain`, `Expires` or `Max-Age`, `SameSite`, and `Secure`. JavaScript cannot set the `HttpOnly` attribute because that attribute intentionally prevents client-side script access. Cookie handling is ultimately performed by the browser, while Perl supplies server-side HTTP headers and JavaScript uses the browser's client-side cookie API. See the MDN document.cookie reference and the CGI::Cookie Perl documentation.

QUESTION NO: 31

Against which of the following does SSH provide protection?

Each correct answer represents a complete solution. Choose two.

A. DoS attack

B. Password sniffing

C. Broadcast storm

D. IP spoofing

ANSWER: B D

Explanation:

SSH protects remote-access sessions by creating an encrypted and integrity-protected channel between the client and server. “Password sniffing” is therefore protected against when SSH password authentication is used: the password is transmitted within the SSH transport’s encrypted connection rather than as readable cleartext on the network. SSH also protects against the security consequences of “IP spoofing” by relying on cryptographic server authentication, normally through host keys, rather than treating an IP address as proof of a server’s identity. The client verifies the server’s host key during key exchange, and the resulting session keys provide confidentiality and integrity for subsequent traffic. This means an attacker cannot successfully impersonate the legitimate SSH server merely by presenting a forged source IP address; the attacker would also need to satisfy the host-key authentication and cryptographic protocol checks. RFC 4253 specifies that the SSH Transport Layer Protocol provides server authentication, confidentiality, and integrity protection, while RFC 4252 describes SSH user-authentication methods, including password authentication conducted over the established secure transport. See RFC 4253: SSH Transport Layer Protocol and RFC 4252: SSH Authentication Protocol.

QUESTION NO: 32

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

A. RSA

B. Diffie-Hellman

C. Twofish

D. Blowfish

ANSWER: B

Explanation:

Diffie-Hellman is correct because its fundamental purpose is to let two parties derive a shared secret across an untrusted network without transmitting that secret directly. In its basic, unauthenticated form, however, the protocol does not establish the identities of the parties participating in the exchange. An active attacker positioned between the two endpoints can intercept each party’s public value and substitute values of their own. The attacker then establishes one shared secret with each endpoint, enabling the attacker to relay, inspect, or potentially alter traffic while each victim believes it is communicating directly with the other.

This is the classic man-in-the-middle weakness of unauthenticated Diffie-Hellman key exchange. Diffie-Hellman therefore must be paired with an authentication mechanism, such as digitally signed ephemeral key-exchange parameters, certificates, or a pre-shared-key-based authenticated protocol. Modern secure protocol designs commonly use authenticated ephemeral Diffie-Hellman to gain both peer authentication and forward secrecy. RFC 2631 explicitly notes that Diffie-Hellman alone does not provide authentication and describes authentication as a required associated service; see RFC 2631. NIST also specifies approved finite-field Diffie-Hellman key-establishment schemes and their security requirements in NIST SP 800-56A Rev. 3.

QUESTION NO: 33

At which of the following layers Structured Query Language (SQL) works?

A. Physical

B. Network

C. Transport

D. Session

E. Application

ANSWER: E

Explanation:

Structured Query Language (SQL) operates at the **Application** layer of the OSI model. SQL is a high-level language used by client applications, database tools, and services to request, manipulate, and administer data in relational database management systems. Statements such as `SELECT`, `INSERT`, `UPDATE`, and `DELETE` express application-level data operations; they do not define how bits are transmitted, how packets are routed, or how transport connections are established.

In a client-server database architecture, an application or database client submits SQL requests through a database protocol to a database server. Lower OSI layers support the communication path: transport services may provide reliable delivery, network services may route packets, and physical components carry signals. However, SQL's purpose and semantics remain application-facing, making the Application layer the appropriate classification. The OSI Application layer provides network services directly to end-user processes and application software, which aligns with SQL's role in interacting with database services. See the ISO OSI basic reference model and Oracle's SQL Language Reference.

QUESTION NO: 34

Which of the following technologies are forms of single sign-on (SSO)?

Each correct answer represents a complete solution. Choose three.

A. CoSign

B. SESAME

C. Kerberos

D. RADIUS

ANSWER: A B C

Explanation:

CoSign, SESAME, and Kerberos are forms of single sign-on because each is designed to let an authenticated user access multiple protected services without separately authenticating to every service. Single sign-on relies on an initial authentication event and then uses trusted credentials, tickets, or assertions that participating applications can accept. CoSign is an SSO approach that centrally manages a user's authentication and enables access to integrated systems after the initial sign-in. SESAME (Secure European System for Applications in a Multi-vendor Environment) was a security architecture that extended ticket-based authentication concepts for distributed environments and supported SSO across services. Kerberos is the best-known example: after a user obtains a ticket-granting ticket from the Key Distribution Center, the user can request service tickets for participating resources without repeatedly providing a password. This reduces password exposure while providing mutual-authentication capabilities when properly deployed. The MIT Kerberos documentation describes this ticket-based authentication model at MIT Kerberos. NIST also identifies federation and SSO as mechanisms through which one authentication event can support access to multiple relying parties; see NIST SP 800-63C.

QUESTION NO: 35

What is the hash value length of the Secure Hash Algorithm (SHA-1)?

A. 164-bit

B. 320-bit

C. 128-bit

D. 160-bit

ANSWER: D

Explanation:

SHA-1 produces a 160-bit message digest (hash value). Regardless of the size of the input message, the algorithm's output is fixed at 160 bits, conventionally represented as 40 hexadecimal characters because each hexadecimal character represents 4 bits. SHA-1 was specified in Federal Information Processing Standard (FIPS) 180-1 and later included in the Secure Hash Standard family. Understanding the output length distinguishes SHA-1 from related algorithms: for example, MD5 produces 128-bit digests, while SHA-256 produces 256-bit digests. Although 160-bit is the defined SHA-1 digest length, SHA-1 is no longer appropriate for security-sensitive uses requiring collision resistance. NIST formally deprecated SHA-1 for digital signatures, time stamping, and other applications after practical collision attacks demonstrated that its collision-resistance strength was insufficient. Modern systems should use SHA-256 or a stronger SHA-2/SHA-3 algorithm where a cryptographic hash is needed. The algorithm's original specification and output-length definition are documented by NIST in FIPS PUB 180-1; NIST's current Secure Hash Standard is available in FIPS PUB 180-4.

QUESTION NO: 36

Which of the following are data link layer components?

Each correct answer represents a complete solution. Choose three.

A. Switches

B. Bridges

C. MAC addresses

D. Hub

ANSWER: A B C

Explanation:

Switches, bridges, and MAC addresses are associated with the OSI data link layer, Layer 2. This layer provides node-to-node delivery over a local network segment and organizes transmitted data into frames. It also uses physical (MAC) addressing so that frames can be delivered to the intended network interface on the local LAN. A MAC address is the Layer 2 identifier carried in Ethernet frame headers as the source and destination address. Bridges operate at Layer 2 by examining MAC addresses and forwarding or filtering frames between LAN segments. Ethernet switches perform the same fundamental Layer 2 forwarding function, learning source MAC addresses to build a forwarding table and sending frames only to the appropriate port when possible. These functions reduce unnecessary traffic across segments while maintaining connectivity at the local-network level. The National Institute of Standards and Technology describes the data link layer as responsible for framing and local-link transmission functions, while Cisco's networking documentation describes switching decisions based on MAC address tables. See NIST's OSI model publication and Cisco's LAN switching overview.

QUESTION NO: 37

Which of the following works at the network layer and hides the local area network IP address and topology?

A. Hub

B. MAC address

C. Network address translation (NAT)

D. Network interface card (NIC)

ANSWER: C

Explanation:

Network address translation (NAT) is correct because it operates on Internet Protocol addressing, which is a network-layer function. A NAT-enabled gateway translates private internal IP addresses into one or more externally routable public IP addresses as traffic passes between a local network and an external network. To outside systems, connections appear to originate from the gateway's public address rather than from the individual private hosts behind it. This prevents external parties from directly seeing the internal addressing scheme and reduces exposure of the local network's IP-address structure. When port address translation is used, many internal devices can share a single public address, with the gateway tracking the associations needed to return response traffic to the appropriate internal device. NAT is consequently commonly deployed at network boundaries to conserve public IPv4 addresses and to provide address/topology obscurity as a secondary effect. It should not, however, be treated as a replacement for a firewall or other access-control mechanisms; its primary function is address translation. The Internet Engineering Task Force describes traditional NAT behavior and terminology in RFC 3022. For foundational networking-layer context, see the CISA overview of layered network models.

QUESTION NO: 38

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. SocketShield

B. Enum

C. KFSensor

D. Sheep dip

ANSWER: A C

Explanation:

SocketShield and **KFSensor** are security tools intended to help defend Windows hosts against malicious activity. SocketShield is designed to provide endpoint-oriented protection against malicious software, including threats such as spyware, viruses, Trojan activity, and keylogging-related malware. Its purpose is to identify and block suspicious or unauthorized activity before it can compromise the protected host.

KFSensor provides host-based intrusion-detection and deception capabilities. It deploys simulated services and monitors interactions with them, helping identify malware, worms, Trojan activity, and unauthorized attempts to access or compromise a computer. This allows administrators to detect hostile behavior directed at the system and respond before or during a compromise. Its alerting and logging functions also provide useful evidence for incident investigation and containment.

Both products therefore fit the question's broad requirement for tools that can be used to protect a computer system from malware-related threats and keylogger-associated compromise attempts. KFSensor describes its role as a host-based intrusion detection system and honeypot at KFSensor. More generally, CISA recommends using protective controls and security monitoring to prevent and detect malware activity; see CISA's malware guidance.

QUESTION NO: 39

SSH is a network protocol that allows data to be exchanged between two networks using a secure channel. Which of the following encryption algorithms can be used by the SSH protocol?

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

A. Blowfish

B. DES

C. RC4

D. IDEA

ANSWER: A B C D

Explanation:

Blowfish, DES, RC4, and IDEA can all be used by SSH in the broad, historical sense intended by this question. SSH negotiates an encryption algorithm as part of establishing its secure transport channel, and its protocol ecosystem has defined or implemented support for each of these ciphers. The SSH Transport Layer Protocol algorithm registry includes names for Blowfish, IDEA, and ARCFOUR (the SSH name for RC4); RFC 4253 documents these encryption algorithm identifiers and the process by which a client and server select a mutually supported cipher. See RFC 4253, SSH Transport Layer Protocol. DES was also supported by earlier SSH implementations and protocol versions, including SSH-1-era deployments. Consequently, all four are valid answers to a question about algorithms that can be used by SSH rather than algorithms that should be selected for a newly deployed SSH service. In current operational practice, these legacy ciphers are generally disabled or avoided because modern SSH configurations favor authenticated encryption or strong modern ciphers such as AES-GCM or ChaCha20-Poly1305. OpenSSH documents its available cipher configuration through its sshd_config Ciphers directive.

QUESTION NO: 40

Which of the following statements about Network Address Translation (NAT) is true?

A. It hides the public network from internal hosts.

B. It hides internal hosts from the public network.

C. It uses public IP addresses on an internal network.

D. It translates IP addresses into user friendly names.

ANSWER: B

Explanation:

It hides internal hosts from the public network. NAT commonly operates at the boundary between a private internal network and the Internet, replacing an internal source IP address with a public, routable address as traffic leaves the network. For connections initiated from inside, the NAT device maintains a translation entry that associates the internal address, and often the source port, with the public-facing address and port. Return traffic can then be mapped to the originating internal host without exposing that host's private address in Internet-routable packet headers. This address-concealment effect is a common benefit of NAT, particularly when private IPv4 address ranges are used internally and one or a limited pool of public IPv4 addresses is available externally. NAT itself is primarily an address/port translation mechanism rather than a complete security control; organizations should still enforce explicit firewall rules and other layered protections. The IETF describes traditional NAT behavior and terminology in RFC 3022, including translation between private and public address realms. For the private IPv4 address ranges commonly used behind NAT, see RFC 1918.

QUESTION NO: 41

Which of the following statements about buffer overflow are true?

Each correct answer represents a complete solution. Choose two.

A. It is a situation that occurs when a storage device runs out of space.

B. It can terminate an application.

C. It can improve application performance.

D. It is a situation that occurs when an application receives more data than it is configured to accept

ANSWER: B D

Explanation:

A buffer overflow occurs when a program writes data beyond the boundary of a memory buffer allocated to hold it. This condition commonly arises when an application receives more input than the relevant buffer is configured or coded to accept and does not correctly enforce bounds checking. The excess data can overwrite adjacent memory locations, corrupting program state, data, or control-flow information. Therefore, “It is a situation that occurs when an application receives more data than it is configured to accept” correctly expresses the fundamental condition that leads to a buffer overflow.

“It can terminate an application” is also correct because overwriting memory may trigger an access violation, segmentation fault, exception, or other abnormal program state from which the application cannot continue safely. The operational impact can range from a crash and denial of service to more serious security consequences when altered memory affects execution control. MITRE classifies this weakness as CWE-120, describing buffer-copy operations that do not sufficiently limit the size of copied data, and explains the potential for memory corruption. See MITRE CWE-120: Buffer Copy without Checking Size of Input and CISA: Understanding Buffer Overflows.

QUESTION NO: 42

Which of the following is the most secure policy for a firewall?

A. Passing all packets unless they are explicitly rejected.

B. Enabling all internal interfaces.

C. Blocking all packets unless they are explicitly permitted.

D. Disabling all external interfaces.

ANSWER: C

Explanation:

Blocking all packets unless they are explicitly permitted is the most secure firewall policy because it implements a default-deny, or implicit-deny, posture. Under this approach, traffic is rejected unless a rule specifically authorizes it according to the organization’s documented business and security requirements. This minimizes the network’s attack surface: unneeded services, ports, protocols, and communication paths are not reachable simply because an administrator overlooked them. Explicit allow rules can then be narrowly scoped by source and destination address, protocol, port, application, direction, and, where supported, user or device identity. The policy also makes firewall rule reviews more meaningful, since every permitted flow should have a defined purpose and owner. Default deny is consistent with the principle of least privilege, which limits access to only what is necessary to perform an approved function. NIST describes firewalls as enforcing policy through rules that permit or block traffic and recommends a restrictive rule set tailored to authorized communications. The Center for Internet Security likewise includes deny-by-default principles in secure network-device configuration guidance. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and CIS Controls: Network Monitoring and Defense.

QUESTION NO: 43

Which of the following allows an administrator to find weak passwords on the network?

A. Rainbow table

B. Back door

C. Worm

D. Access control list

ANSWER: A

Explanation:

Rainbow table is correct because it is a precomputed collection of password candidates and their corresponding hash values. When an administrator obtains password hashes during an authorized password audit, a rainbow table can be used to compare those hashes against precomputed results and rapidly identify passwords that are common, short, predictable, or otherwise weak. This makes it useful for assessing whether accounts are protected by passwords that could be feasibly recovered if the password database were exposed. The effectiveness of rainbow-table attacks against unsalted hashes also demonstrates why password-storage systems should use a unique salt for each password and a slow, password-specific hashing function. Salting ensures that the same password does not always produce the same stored value and prevents a single precomputed table from being reused effectively across many accounts. NIST's digital identity guidance requires salts and appropriately resistant password-verification mechanisms, while OWASP recommends modern password-hashing algorithms designed to make offline guessing costly. In an authorized administrative review, the ability to discover easily recovered credentials helps identify accounts that need password resets or stronger authentication controls. See NIST SP 800-63B and the OWASP Password Storage Cheat Sheet.

QUESTION NO: 44

John works as a professional Ethical Hacker. He has been assigned a project for testing the security of www.we-are-secure.com. He wants to corrupt an IDS signature database so that performing attacks on the server is made easy and he can observe the flaws in the We-are-secure server. To perform his task, he first of all sends a virus that continuously changes its signature to avoid detection from IDS. Since the new signature of the virus does not match the old signature, which is entered in the IDS signature database, IDS becomes unable to point out the malicious virus. Which of the following IDS evasion attacks is John performing?

A. Session splicing attack

B. Evasion attack

C. Insertion attack

D. Polymorphic shell code attack

ANSWER: D

Explanation:

Polymorphic shell code attack is correct because the defining behavior in the scenario is repeated modification of the malicious payload's detectable pattern while retaining its malicious function. Signature-based intrusion detection relies on recognizing known byte sequences, strings, hashes, or other stable indicators associated with threats. Polymorphic code changes its representation on each iteration—often through encoding, encryption, mutation engines, or altered instruction sequences—so a previously stored signature no longer reliably identifies the new instance. This frustrates simple signature matching and can permit the payload to pass a detector that has not been updated with behavior-based, heuristic, or more resilient detection logic. In practical security testing, this concept illustrates a limitation of purely signature-driven controls and the importance of layered detection, including endpoint telemetry, behavioral analytics, and anomaly detection. MITRE ATT&CK identifies polymorphic code as a form of obfuscated or compressed files and information used to hinder analysis and detection: MITRE ATT&CK: Polymorphic Code. Additional guidance on detecting and responding to malware is available from CISA Malware.

QUESTION NO: 45

Which of the following statements about DNSSEC are true?

Each correct answer represents a complete solution. Choose two.

A. It helps validate that DNS data has not been modified in transit.

B. It uses a chain of trust between DNS zones.

C. It encrypts DNS queries and responses.

D. It eliminates the need for DNS resolvers.

ANSWER: A B

Explanation:

DNS Security Extensions (DNSSEC) add origin authentication and data-integrity protection to DNS information through digital signatures. A validating resolver can verify that DNS records were signed by the appropriate zone and that the response has not been changed in transit. Therefore, DNSSEC helps protect against forged DNS responses and uses a chain of trust from a configured trust anchor, normally the DNS root, through signed delegations.

DNSSEC does not encrypt DNS queries or responses, so it does not provide confidentiality for DNS traffic. Encrypted DNS transports, such as DNS over TLS or DNS over HTTPS, address transport confidentiality but are separate from DNSSEC validation. See RFC 4033, DNS Security Introduction and Requirements and RFC 4035, Protocol Modifications for DNSSEC.

QUESTION NO: 46

Which of the following is a process of monitoring data packets that travel across a network?

A. Packet sniffing

B. Authentication

C. Network binding

D. Encryption

ANSWER: A

Explanation:

Packet sniffing is the process of capturing and inspecting packets as they traverse a network. A packet sniffer operates through a network interface and records packet headers and, where traffic is not protected, potentially the packet payload. Security professionals use packet sniffing for legitimate activities such as troubleshooting connectivity problems, investigating suspicious traffic, validating network configurations, and analyzing protocols. It provides visibility into information such as source and destination addresses, ports, protocols, flags, timing, and transmitted content. Because captured packets may contain sensitive information, packet-capture tools and stored capture files should be handled under appropriate authorization and access controls. NIST describes packet sniffers as tools that monitor and capture network traffic, and its incident-response guidance identifies packet capture as a valuable source of network-based evidence. For additional guidance, see NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems and the Wireshark documentation, which explains how packet capture and analysis are performed.

QUESTION NO: 47

Which of the following are the examples of administrative controls?

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

A. Data Backup

B. Auditing

C. Security policy

D. Security awareness training

ANSWER: B C D

Explanation:

Administrative controls, also called managerial controls, govern how an organization directs, manages, and verifies its security program through people, policy, process, and oversight. **Security policy** is an administrative control because it establishes management's security requirements, assigns responsibilities, and defines the rules personnel must follow. **Security awareness training** is administrative because it equips personnel to recognize their security responsibilities and apply required practices in their daily work. **Auditing** is also an administrative control when it is used to assess compliance with organizational policies, procedures, and security requirements; audit results provide management with evidence for oversight, corrective action, and risk decisions. These controls are fundamental to governance because they establish expected behavior and evaluate whether the security program is operating as intended, rather than directly enforcing a technical restriction. NIST identifies policy and procedures, awareness and training, and assessment activities as management-control areas within an information security program. See NIST SP 800-53 Rev. 5 and FIPS 200.

QUESTION NO: 48

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with a lot of requests. Which of the following tools can an attacker use to perform a DNS zone transfer?

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

A. Dig

B. NSLookup

C. DSniff

D. Host

ANSWER: A B D

Explanation:

DNS zone transfers use the AXFR DNS query type to synchronize a zone's resource records between authoritative primary and secondary servers. If an authoritative DNS server is misconfigured to permit transfers to arbitrary clients, a requester can obtain the zone data and enumerate records such as hostnames, IP addresses, name servers, mail exchangers, and potentially other internal naming details. This information is useful for reconnaissance because it can reveal systems and services associated with the organization.

Dig can explicitly request an AXFR transfer with syntax such as `dig @server example.com AXFR`. **NSLookup** supports zone-transfer attempts through its interactive `ls` command when querying a server that allows the operation. **Host** also supports a zone-listing mode, commonly invoked as `host -l example.com server`, which requests a zone transfer. In each case, success depends on the selected DNS server being authoritative for the target zone and allowing AXFR from the requesting client. Administrators should restrict zone transfers to authorized secondary DNS servers, preferably using explicit transfer ACLs and authenticated transfer mechanisms. See the dig manual page and the host manual page.

QUESTION NO: 49

You work as a Network Administrator for NetTech Inc. To ensure the security of files, you encrypt data files using Encrypting File System (EFS). You want to make a backup copy of the files and maintain security settings. You can backup the files either to a network share or a floppy disk. What will you do to accomplish this?

A. Copy the files to a network share on a FAT32 volume.

B. Copy the files to a network share on an NTFS volume.

C. Place the files in an encrypted folder. Then, copy the folder to a floppy disk.

D. Copy the files to a floppy disk that has been formatted using Windows 2000 Professional.

ANSWER: B

Explanation:

Copy the files to a network share on an NTFS volume. EFS is implemented through the NTFS file system: NTFS stores the metadata that identifies a file as encrypted and maintains the encrypted file-encryption key information needed for authorized users or recovery agents to access it. Therefore, an NTFS-formatted destination is required when making a copied backup that is intended to retain EFS protection. A network share can satisfy this requirement when its underlying destination volume is NTFS and supports EFS. The files remain protected at rest by EFS on that destination, so access continues to depend on the appropriate EFS certificate/private key or designated recovery capability. This is the appropriate choice whether the remote storage is used as a normal file-copy destination or as a backup location managed by the organization. Microsoft describes EFS as NTFS-based encryption and explains that EFS encrypts files and folders transparently for authorized users. The Windows file-encryption API documentation also identifies EFS as a file-system feature, reinforcing that the destination file system must support the feature for the encrypted state to be retained. See Microsoft File Encryption documentation and Microsoft documentation on encrypting files with EFS.

QUESTION NO: 50

Which of the following are examples of passive attacks?

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

A. Shoulder surfing

B. Dumpster diving

C. Placing a backdoor

D. Eavesdropping

ANSWER: A B D

Explanation:

Passive attacks obtain information without altering the target system, its data, or its normal operation. **Shoulder surfing** is passive because the attacker observes sensitive information, such as a password, authentication factor, screen contents, or documents, while the legitimate user enters or handles it. **Dumpster diving** is also passive: discarded papers, storage media, labels, and other materials can disclose useful information without the attacker needing to interact with or change an active system. **Eavesdropping** fits the same principle because it involves listening to or capturing communications in order to learn their contents or metadata rather than modifying the communication. These techniques are commonly associated with reconnaissance, information gathering, and social-engineering activity. The defining security concern is confidentiality: the victim may have no immediately visible indication that information has been observed or collected. NIST describes passive attacks as attacks that monitor or eavesdrop on communications, and its guidance emphasizes protecting sensitive information throughout its lifecycle, including when it exists in physical form or is discarded. See NIST CSRC: passive attack and NIST SP 800-53 Rev. 5.

QUESTION NO: 51

Which of the following functions are performed by a firewall?

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

A. It hides vulnerable computers that are exposed to the Internet.

B. It logs traffic to and from the private network.

C. It enhances security through various methods, including packet filtering, circuit-level filtering, and application filtering.

D. It blocks unwanted traffic.

ANSWER: A B C D

Explanation:

Firewalls enforce an organization's network-security policy at a boundary between networks with different trust levels, such as the Internet and a private network. By permitting only authorized inbound connections and limiting unnecessary externally reachable services, a firewall can hide or shield vulnerable internal computers from direct Internet exposure. Firewalls also create useful security records: their logging capabilities can capture allowed and denied connection attempts, traffic metadata, events, and policy violations for monitoring, incident investigation, and auditing. Their central security function is to block unwanted traffic according to defined rules, while allowing legitimate communications needed by the organization. This enforcement can be implemented through several firewall techniques and architectures, including packet filtering, circuit-level filtering or gateways, and application-layer filtering or proxies. Packet filtering evaluates network and transport characteristics, circuit-level controls validate or govern sessions, and application filtering can apply policy using application-specific awareness. Modern firewalls may combine these capabilities, but the underlying purpose remains controlled, policy-based traffic flow and visibility. NIST describes firewalls as devices or programs that control network traffic according to policy and documents the principal firewall technologies and capabilities in NIST SP 800-41 Rev. 1. Additional firewall-related security guidance is available from CISA.

QUESTION NO: 52

Which of the following statement about eavesdropping is true?

A. It is a type of password guessing attack.

B. It is a way of preventing electronic emissions that are generated from a computer or network.

C. It is known as network saturation attack or bandwidth consumption attack.

D. It is the process of hearing or listening in private conversations.

ANSWER: D

Explanation:

Eavesdropping is the unauthorized interception, monitoring, or listening to communications that were intended to be private. In information security, it commonly refers to a passive attack in which an adversary captures data moving across a network or listens to a communication channel without necessarily altering the data or disrupting the service. Examples include packet sniffing on an inadequately protected network, intercepting unencrypted wireless traffic, or capturing the contents of communications that lack effective transport encryption. The process of hearing or listening in private conversations accurately captures the core meaning of eavesdropping and applies both to ordinary spoken communications and to electronic communications. Security controls that help reduce this risk include strong encryption in transit, authenticated secure protocols, secure wireless configurations, network segmentation, and physical protection of communications infrastructure. NIST describes passive attacks as attempts to learn or make use of information from a system without affecting system resources, a category that includes the interception of communications. See NIST's definition of a passive attack and the CISA overview of denial-of-service attacks for related security terminology.

QUESTION NO: 53

Which of the following are default ports for the FTP service?

Each correct answer represents a complete solution. Choose two.

A. 443

B. 20

C. 21

D. 80

ANSWER: B C

Explanation:

FTP conventionally uses TCP port 21 for its control connection. This channel carries commands and server replies, including authentication, directory navigation, transfer requests, and session-management commands. The client initiates the control connection to the FTP server's listening port 21, which is why firewalls and network monitoring tools commonly identify FTP control traffic on that port.

TCP port 20 is the well-known FTP data port used by the server for an active-mode FTP data connection. FTP separates control traffic from file-transfer and directory-listing data; in active mode, the server establishes the data connection from source port 20 to the client endpoint negotiated through the control session. This traditional two-port behavior is the basis for recognizing ports 20 and 21 as FTP's default ports. Modern FTP can also use passive mode, where the server selects a negotiated high-numbered port for the data connection, but that does not change the standard assignment of port 20 for active-mode FTP data and port 21 for FTP control. The IANA service-name registry lists ftp-data as TCP port 20 and ftp as TCP port 21. See the IANA Service Name and Transport Protocol Port Number Registry and RFC 959.

QUESTION NO: 54

Which of the following terms refers to a steady lower voltage state without a complete loss of power?

A. Sag

B. Brownout

C. Blackout

D. Spike

ANSWER: B

Explanation:

Brownout is the correct term for a sustained condition in which electrical service remains available but is deliberately or incidentally supplied at a voltage below its normal level. In contrast to a complete interruption of electric service, a brownout preserves some power delivery, which is exactly what "without a complete loss of power" describes. Utilities may reduce voltage during periods of exceptionally high demand to help stabilize the electrical grid and avoid a more extensive outage. The reduced voltage can affect equipment differently depending on its design: lights may dim, motors can operate inefficiently or overheat, and sensitive electronic systems may require voltage regulation or uninterruptible power protection to continue operating reliably. From an information-security and business-continuity perspective, recognizing a brownout matters because it is a power-quality event that can impair availability and damage or disrupt IT equipment even though the facility has not lost power entirely. Dictionary references likewise define a brownout as a reduction in voltage rather than a full cessation of electrical service. See Merriam-Webster's definition of brownout and Encyclopaedia Britannica's brownout reference.

QUESTION NO: 55

Which of the following techniques are used to secure wireless networks?

Each correct answer represents a complete solution. Choose three.

A. MAC address filtering

B. SSID spoofing

C. IP spoofing

D. Closed network

E. WPA3-Personal with Simultaneous Authentication of Equals (SAE)

ANSWER: A D E

Explanation:

MAC address filtering, a closed network configuration, and WPA3-Personal with Simultaneous Authentication of Equals are wireless-network security measures. MAC address filtering is an access-control mechanism that allows an access point to restrict association attempts to devices whose configured hardware addresses appear on an allowlist. It is best used as a supplementary control, since MAC addresses can be observed and imitated, but it can still limit casual or unauthorized association attempts. A closed network configuration suppresses routine SSID advertisement and requires clients to be configured with the network name; this can reduce casual discovery, although it is not a replacement for strong authentication and encryption. WPA3-Personal provides the essential cryptographic protection: its SAE authentication exchange improves resistance to offline password-guessing attacks, and WPA3 protects wireless traffic using modern encryption. In practice, organizations should use WPA3 where client compatibility permits, select a strong unique passphrase, and retain MAC filtering or SSID suppression only as defense-in-depth measures. The Wi-Fi Alliance describes WPA3 and SAE at Wi-Fi Alliance: Wi-Fi security; NIST provides wireless-LAN security guidance at NIST SP 800-153.

QUESTION NO: 56

Which of the following port numbers is used by the HTTPS protocol for secure Web transmission?

A. 8080

B. 21

C. 110

D. 443

E. 80

F. 25

ANSWER: D

Explanation:

The correct answer is **443**. HTTPS (Hypertext Transfer Protocol Secure) uses TCP port 443 by default to provide encrypted web communications. HTTPS is HTTP carried over Transport Layer Security (TLS), which authenticates the server through its certificate and protects data in transit against eavesdropping and tampering. When a user visits a URL beginning with `https://` without specifying a port, the browser normally establishes its TLS-protected connection to the destination server on port 443. This default assignment is registered in the IANA Service Name and Transport Protocol Port Number Registry as `https` over TCP port 443. Security practitioners should recognize this convention when configuring firewalls, reviewing network flows, hardening web services, and investigating traffic, while also remembering that HTTPS can technically be configured to use a nondefault port when explicitly specified in a URL or service configuration. See the IANA service-name and port-number registry entry for HTTPS and the HTTP Semantics specification (RFC 9110), which identifies 443 as the default HTTPS port.

QUESTION NO: 57

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network.

You have configured a firewall on the network. A filter has been applied to block all the ports. You want to enable sending and receiving of *emails* on the network. Which of the following ports will you open?

Each correct answer represents a complete solution. Choose two.

A. 20

B. 80

C. 110

D. 25

ANSWER: C D

Explanation:

Port 25 and port 110 are the expected ports for basic email transmission and retrieval in the conventional TCP/IP mail model. Port 25 is assigned to SMTP (Simple Mail Transfer Protocol), which transfers outbound email from a mail client or server and relays messages between mail servers. Opening it permits the sending function referenced in the question. Port 110 is assigned to POP3 (Post Office Protocol version 3), which allows an email client to retrieve received messages from a mail server. Together, SMTP on port 25 and POP3 on port 110 support the stated ability to send and receive email. The Internet Assigned Numbers Authority lists TCP port 25 for SMTP and TCP port 110 for POP3 in its service-name and port-number registry. In modern production environments, administrators commonly use authenticated mail submission on TCP port 587 and encrypted POP3 on TCP port 995, but those alternatives are not included here and do not change the conventional port mappings tested by this question. See the IANA SMTP service-port registry entry and the IANA POP3 service-port registry entry.