QUESTION 801
The difference between a vulnerability assessment and a penetration test is that a vulnerability assessment:

- A. searches and checks the infrastructure to detect vulnerabilities, whereas penetration testing intends to exploit the vulnerabilities to probe the damage that could result from the vulnerabilities.
- B. and penetration tests are different names for the same activity.
- C. is executed by automated tools, whereas penetration testing is a totally manual process.
- D. is executed by commercial tools, whereas penetration testing is executed by public processes.

Correct Answer: A
Explanation: A vulnerability assessment is designed to identify and report vulnerabilities in a system without actively exploiting them, while penetration testing actively tries to exploit the vulnerabilities to determine the extent of potential damage. The two are distinct processes, with different goals and techniques, but both can be performed using automated or manual tools.

QUESTION 802
The most common problem in the operation of an intrusion detection system (IDS) is:

- A. the detection of false positives.
- B. receiving trap messages.
- C. reject-error rates.
- D. denial-of-service attacks.

Correct Answer: A
Explanation: The most common issue with IDSs is the generation of false positives, where legitimate activity is incorrectly identified as a security threat. This can lead to alert fatigue and make it harder to identify real attacks. Trap messages are part of SNMP and not specific to IDS, reject-error rates relate to biometrics, and denial-of-service attacks are a type of threat, not an operational problem for IDS.

QUESTION 803
Which of the following provides nonrepudiation services for e-commerce transactions?

- A. Public key infrastructure (PKI)
- B. Data Encryption Standard (DES)
- C. Message authentication code (MAC)
- D. Personal identification number (PIN)

Correct Answer: A
Explanation: PKI provides nonrepudiation services by using digital certificates and digital signatures, ensuring that the sender of a message cannot deny their identity. DES is a symmetric encryption algorithm, MAC provides message integrity, and a PIN verifies identity but does not ensure nonrepudiation.

QUESTION 804
While copying files from a floppy disk, a user introduced a virus into the network. Which of the following would MOST effectively detect the existence of the virus?

- A. A scan of all floppy disks before use
- B. A virus monitor on the network file server
- C. Scheduled daily scans of all network drives
- D. A virus monitor on the user's personal computer

Correct Answer: C
Explanation: Scheduled daily scans of all network drives will detect any viruses that may have been introduced into the system. Scanning all floppy disks before use or using virus monitors on personal computers or servers are preventive measures but do not guarantee detection after infection.

QUESTION 805

Which of the following message services provides the strongest evidence that a specific action has occurred?

- A. Proof of delivery
- B. Nonrepudiation
- C. Proof of submission
- D. Message origin authentication

Correct Answer: B

Explanation: Nonrepudiation provides strong evidence that a specific action occurred, typically through digital signatures. It ensures that the sender of a message cannot deny sending it, providing stronger proof than delivery or submission confirmations or message origin authentication.

QUESTION 806

The PRIMARY objective of Secure Sockets Layer (SSL) is to ensure:

- A. only the sender and receiver are able to encrypt/decrypt the data.
- B. the sender and receiver can authenticate their respective identities.
- C. the alteration of transmitted data can be detected.
- D. the ability to identify the sender by generating a one-time session key.

Correct Answer: A

Explanation: SSL's main goal is to secure communication by encrypting data between the sender and receiver, ensuring that only they can decrypt it. Although SSL supports authentication and data integrity, its primary purpose is to provide confidentiality by encrypting the transmitted data.

QUESTION 807

The role of the certificate authority (CA) as a third party is to:

- A. provide secured communication and networking services based on certificates.
- B. host a repository of certificates with the corresponding public and secret keys issued by that CA.
- C. act as a trusted intermediary between two communication partners.
- D. confirm the identity of the entity owning a certificate issued by that CA.

Correct Answer: D

Explanation: The primary role of a CA is to verify the identity of an entity before issuing a digital certificate. This ensures that the entity's public key is correctly associated with its identity. The CA does not provide communication services or store secret keys, and while it helps with trust, it is not involved in direct communication.

QUESTION 808

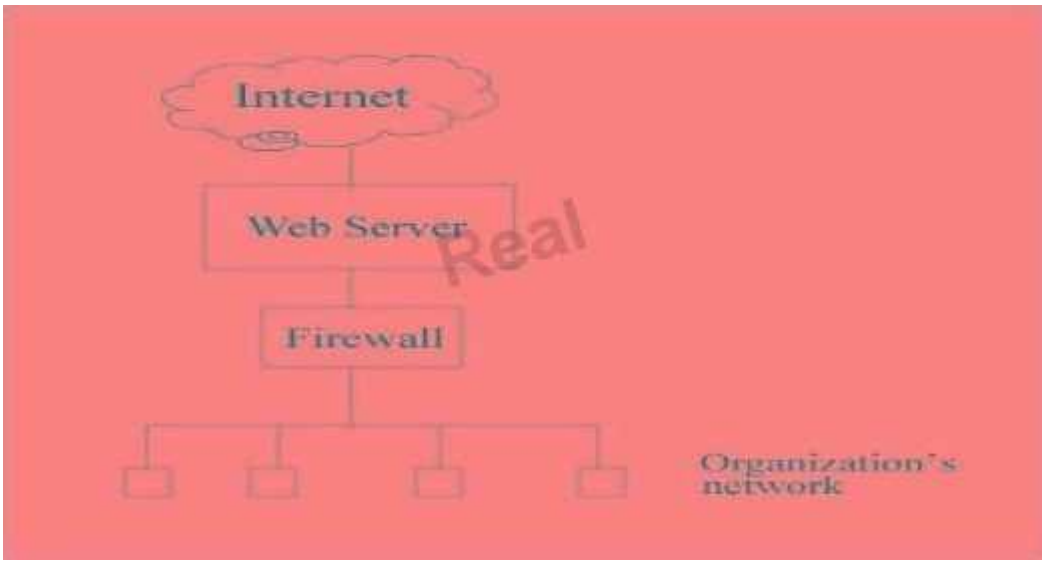
Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?

- A. The buyer is assured that neither the merchant nor any other party can misuse their credit card data.
- B. All personal SET certificates are stored securely in the buyer's computer.
- C. The buyer is liable for any transaction involving his/her personal SET certificates.
- D. The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

Correct Answer: C

Explanation: In SET, the cardholder assumes responsibility for any use of their personal SET certificates. While SET improves security for credit card transactions, the buyer is still liable for any transactions made with their certificates. The protocol does not eliminate the need to handle credit card information or guarantee that certificates are securely stored.

QUESTION 809
E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network.



The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

- A. alert the appropriate staff.
- B. create an entry in the log.
- C. close firewall-2.
- D. close firewall-1.

Correct Answer: C
Explanation: If traffic that bypasses the mail gateway is detected, firewall-1 may have been compromised. The first priority is to close firewall-2 to protect the internal network from unauthorized traffic. Closing firewall-1 might not be possible if it has already been compromised. Logging the incident or alerting staff is secondary to immediately securing the network.

QUESTION 810
An IS auditor should be MOST concerned with what aspect of an authorized honeypot?

- A. The data collected on attack methods
- B. The information offered to outsiders on the honeypot
- C. The risk that the honeypot could be used to launch further attacks on the organization's infrastructure
- D. The risk that the honeypot would be subject to a distributed denial-of-service attack

Correct Answer: C
Explanation: The primary concern is that the honeypot could be used by attackers to infiltrate the organization's systems and launch further attacks. While honeypots gather valuable information about attack methods, they can also become a liability if not properly isolated from critical infrastructure.

QUESTION 811

Which of the following should be a concern to an IS auditor reviewing a wireless network?

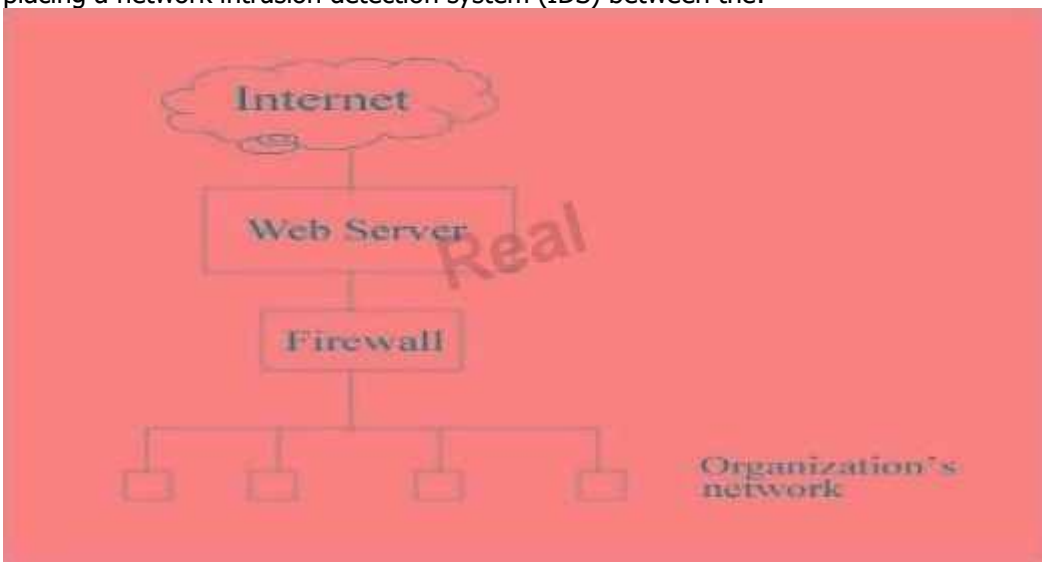
- A. 128-bit static-key WEP (Wired Equivalent Privacy) encryption is enabled.
- B. SSID (Service Set Identifier) broadcasting has been enabled.
- C. Antivirus software has been installed in all wireless clients.
- D. MAC (Media Access Control) access control filtering has been deployed.

Correct Answer: B

Explanation: SSID broadcasting should be disabled to prevent unauthorized users from easily discovering the wireless network. Enabling SSID broadcasting makes the network more vulnerable to unauthorized access. WEP, while not highly secure, adds some protection, and antivirus and MAC filtering strengthen security.

QUESTION 812

To detect attack attempts that the firewall is unable to recognize, an IS auditor should recommend placing a network intrusion detection system (IDS) between the:



- A. Firewall and the organization's network.
- B. Internet and the firewall.
- C. Internet and the web server.
- D. Web server and the firewall.

Correct Answer: A

Explanation: Placing a network-based IDS between the firewall and the organization's network ensures that any attacks that bypass the firewall will still be detected. This setup monitors all traffic that reaches the internal network, enhancing the ability to detect potential intrusions that the firewall may miss.

QUESTION 813

Which of the following ensures a sender's authenticity and an e-mail's confidentiality?

- A. Encrypting the hash of the message with the sender's private key and thereafter encrypting the hash of the message with the receiver's public key
- B. The sender digitally signing the message and thereafter encrypting the hash of the message with the sender's private key
- C. Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key
- D. Encrypting the message with the sender's private key and encrypting the message hash with the receiver's public key.

Correct Answer: C

Explanation: To ensure both authenticity and confidentiality, the message should be encrypted first with the sender's private key (ensuring authenticity) and then with the receiver's public key (ensuring confidentiality). This double encryption process ensures that the message remains private and that its origin is verified.

QUESTION 814
An efficient use of public key infrastructure (PKI) should encrypt the:

- A. entire message.
- B. private key.
- C. public key.
- D. symmetric session key.

Correct Answer: D
Explanation: PKI systems are computationally intensive, so they are often used to exchange symmetric session keys, which are then used to encrypt and decrypt the actual message. Symmetric encryption is faster and more efficient for bulk data encryption, while PKI handles the secure exchange of the session keys.

QUESTION 815
Which of the following cryptographic systems is MOST appropriate for bulk data encryption and small devices such as smart cards?

- A. DES
- B. AES
- C. Triple DES
- D. RSA

Correct Answer: B
Explanation: AES (Advanced Encryption Standard) is well-suited for bulk data encryption and can run efficiently on a variety of platforms, including small devices like smart cards. DES is no longer considered secure, Triple DES is slower, and RSA is more suited for encrypting small amounts of data.

QUESTION 816
Disabling which of the following would make wireless local area networks more secure against unauthorized access?

- A. MAC (Media Access Control) address filtering
- B. WPA (Wi-Fi Protected Access Protocol)
- C. LEAP (Lightweight Extensible Authentication Protocol)
- D. SSID (service set identifier) broadcasting

Correct Answer: D
Explanation: Disabling SSID broadcasting makes it harder for unauthorized users to find and access the wireless network. Enabling MAC address filtering, WPA, and LEAP enhances security, but SSID broadcasting should be turned off to add an additional layer of security by making the network less visible.

QUESTION 817
Which of the following is BEST suited for secure communications within a small group?

- A. Key distribution center
- B. Certification authority
- C. Web of trust
- D. Kerberos Authentication System

Correct Answer: C
Explanation: A web of trust is ideal for secure communications in a small group. It allows users to verify each other’s public keys through trusted relationships. In contrast, a key distribution center and certification authority are better suited for larger organizations or formal communications, while Kerberos is used to manage authentication in a larger network environment.

QUESTION 818
Which of the following is the MOST important action in recovering from a cyberattack?
- A. Creation of an incident response team
- B. Use of cyberforensic investigators
- C. Execution of a business continuity plan
- D. Filing an insurance claim

Correct Answer: C
Explanation: The execution of a business continuity plan (BCP) is crucial in recovering from a cyberattack, as it ensures that critical business functions can continue while the attack is addressed. The creation of an incident response team and the use of cyberforensics are preventive and investigative measures, but BCP is the key to minimizing the impact of the attack.

QUESTION 819
What method might an IS auditor utilize to test wireless security at branch office locations?
- **A.** War dialing
- **B.** Social engineering
- **C.** War driving
- **D.** Password cracking

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
War driving is a technique used for locating and accessing wireless networks by moving around a building with a wireless-enabled device. This helps to identify unsecured or weakly protected wireless networks. War dialing is used for gaining access to a network by dialing multiple phone numbers. Social engineering is about exploiting human weaknesses to gain access to systems. Password cracking attempts to guess users' passwords but does not specifically target wireless network security.

QUESTION 820
In a public key infrastructure, a registration authority:
- **A.** Verifies information supplied by the subject requesting a certificate.
- **B.** Issues the certificate after the required attributes are verified and the keys are generated.
- **C.** Digitally signs a message to achieve nonrepudiation of the signed message.
- **D.** Registers signed messages to protect them from future repudiation.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
A registration authority (RA) is responsible for verifying the identity and legitimacy of a requestor before a certificate is issued. The certification authority (CA), not the RA, is responsible for issuing certificates. The RA does not sign messages or register signed messages.

QUESTION 821
Confidentiality of the data transmitted in a wireless LAN is BEST protected if the session is:
- **A.** Restricted to predefined MAC addresses.
- **B.** Encrypted using static keys.
- **C.** Encrypted using dynamic keys.
- **D.** Initiated from devices that have encrypted storage.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Dynamic encryption keys, which change regularly, provide better confidentiality than static keys. Limiting access to predefined MAC addresses is not sufficient to ensure confidentiality. Static encryption keys are

more vulnerable to being compromised. Encryption of device storage does not protect the data transmitted over the network.

QUESTION 822
Which of the following provides the MOST relevant information for proactively strengthening security settings?

- **A.** Bastion host
- **B.** Intrusion detection system
- **C.** Honeypot
- **D.** Intrusion prevention system

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
A honeypot is designed to lure attackers, providing valuable information about attack strategies and methods, which can be used to proactively strengthen security settings. A bastion host does not provide detailed insights into attackers' methods. Intrusion detection and prevention systems are focused on identifying and stopping attacks in progress rather than proactively gathering intelligence.

QUESTION 823
Over the long term, which of the following has the greatest potential to improve the security incident response process?

- **A.** A walkthrough review of incident response procedures
- **B.** Postevent reviews by the incident response team
- **C.** Ongoing security training for users
- **D.** Documenting responses to an incident

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Postevent reviews provide valuable insights into how incidents were handled, identifying gaps and opportunities for improvement. While walkthrough reviews, training, and documentation are important, postevent reviews have the greatest potential to improve the response process over time by learning from real-world incidents.

QUESTION 824
When reviewing an intrusion detection system (IDS), an IS auditor should be MOST concerned about which of the following?

- **A.** Number of nonthreatening events identified as threatening
- **B.** Attacks not being identified by the system
- **C.** Reports/logs being produced by an automated tool
- **D.** Legitimate traffic being blocked by the system

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The greatest concern is the failure of the IDS to identify attacks, as these could lead to significant security breaches. False positives (nonthreatening events identified as threats) are a problem but are generally known and can be managed. Legitimate traffic being blocked is not as critical as missing real attacks. Automated tools generating reports are a normal feature and not a concern.

QUESTION 825
Distributed denial-of-service (DDOS) attacks on Internet sites are typically evoked by hackers using which of the following?

- **A.** Logic bombs

- **B.** Phishing
- **C.** Spyware
- **D.** Trojan horses

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Trojan horses are malicious software that can allow attackers to take control of multiple computers. These compromised computers can then be used in a DDOS attack to flood a target website with traffic, overwhelming its servers. Logic bombs are timed attacks, phishing aims to trick users into giving up sensitive information, and spyware collects data from an infected device but does not directly cause DDOS attacks.

QUESTION 826
Validated digital signatures in an e-mail software application will:

- **A.** Help detect spam.
- **B.** Provide confidentiality.
- **C.** Add to the workload of gateway servers.
- **D.** Significantly reduce available bandwidth.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Validated digital signatures in email help ensure that the sender is legitimate, which can aid in detecting spam or malicious emails. Digital signatures do not inherently provide confidentiality, as they do not encrypt the content. Their impact on server workload and bandwidth is minimal.

QUESTION 827
In transport mode, the use of the Encapsulating Security Payload (ESP) protocol is advantageous over the Authentication Header (AH) protocol because it provides:

- **A.** Connectionless integrity.
- **B.** Data origin authentication.
- **C.** Antireplay service.
- **D.** Confidentiality.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
ESP provides confidentiality by encrypting the payload of the communication, which AH does not do. Both ESP and AH offer connectionless integrity, data origin authentication, and antireplay services, but ESP additionally provides encryption for confidentiality.

QUESTION 828
An IS auditor notes that IDS log entries related to port scanning are not being analyzed. This lack of analysis will MOST likely increase the risk of success of which of the following attacks?

- **A.** Denial-of-service
- **B.** Replay
- **C.** Social engineering
- **D.** Buffer overflow

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Port scanning is often used as a precursor to a denial-of-service (DoS) attack. By identifying open ports and vulnerabilities, attackers can launch DoS attacks. A replay attack involves re-sending captured data, social engineering targets human vulnerabilities, and buffer overflow exploits flaws in code.

QUESTION 829
IS management recently replaced its existing wired local area network (LAN) with a wireless infrastructure to accommodate the increased use of mobile devices within the organization. This will increase the risk of which of the following attacks?

- **A.** Port scanning
- **B.** Back door
- **C.** Man-in-the-middle
- **D.** War driving

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
War driving involves scanning for wireless networks, often by moving around with a device that can detect wireless signals. This attack becomes a greater risk with a wireless LAN infrastructure. Port scanning is more common with wired networks, back doors are vulnerabilities in software, and man-in-the-middle attacks are a different type of network interception.

QUESTION 830
Which of the following encryption techniques will BEST protect a wireless network from a man-in-the-middle attack?

- **A.** 128-bit wired equivalent privacy (WEP)
- **B.** MAC-based pre-shared key (PSK)
- **C.** Randomly generated pre-shared key (PSK)
- **D.** Alphanumeric service set identifier (SSID)

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
A randomly generated pre-shared key (PSK) offers stronger protection because it is difficult to predict and less susceptible to brute-force attacks. WEP has known weaknesses, and using a MAC-based PSK is less secure because MAC addresses can be spoofed. The SSID is not a security measure, as it is often broadcast in plaintext.

QUESTION 831
The IS management of a multinational company is considering upgrading its existing virtual private network (VPN) to support voice-over IP (VoIP) communications via tunneling. Which of the following considerations should be PRIMARILY addressed?

- **A.** Reliability and quality of service (QoS)
- **B.** Means of authentication
- **C.** Privacy of voice transmissions
- **D.** Confidentiality of data transmissions

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
While the existing VPN likely handles authentication and confidentiality through tunneling, the primary consideration when implementing VoIP is the reliability and quality of service (QoS). VoIP requires low latency and consistent delivery of packets, which makes QoS a crucial concern. Privacy and confidentiality are typically addressed by the VPN protocols already in place.

QUESTION 832
Which of the following antispam filtering techniques would BEST prevent a valid, variable-length email message containing a heavily weighted spam keyword from being labeled as spam?

- **A.** Heuristic (rule-based)
- **B.** Signature-based

- **C.** Pattern matching
- **D.** Bayesian (statistical)

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Bayesian filtering applies statistical modeling to messages by performing a frequency analysis on each word and evaluating the message as a whole. It can ignore suspicious keywords if the overall content appears legitimate. Heuristic filtering might require additional rules for new exceptions, and signature-based filtering fails with variable-length messages. Pattern matching is a less effective rule-based method that operates at the word level.

QUESTION 833
Which of the following public key infrastructure (PKI) elements provides detailed descriptions for dealing with a compromised private key?

- **A.** Certificate revocation list (CRL)
- **B.** Certification practice statement (CPS)
- **C.** Certificate policy (CP)
- **D.** PKI disclosure statement (PDS)

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The Certification Practice Statement (CPS) provides instructions on handling key compromises. The Certificate Revocation List (CRL) simply lists revoked certificates. The Certificate Policy (CP) sets general requirements, and the PKI Disclosure Statement (PDS) outlines legal responsibilities.

QUESTION 834
Active radio frequency ID (RFID) tags are subject to which of the following exposures?

- **A.** Session hijacking
- **B.** Eavesdropping
- **C.** Malicious code
- **D.** Phishing

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Like other wireless devices, active RFID tags can be subject to eavesdropping. They transmit signals that can be intercepted, but they are not directly vulnerable to session hijacking, malicious code, or phishing attacks.

QUESTION 835
When conducting a penetration test of an organization's internal network, which of the following approaches would BEST enable the conductor of the test to remain undetected on the network?

- **A.** Use the IP address of an existing file server or domain controller.
- **B.** Pause the scanning every few minutes to allow thresholds to reset.
- **C.** Conduct the scans during evening hours when no one is logged in.
- **D.** Use multiple scanning tools since each tool has different characteristics.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Pausing scans helps avoid exceeding traffic thresholds that might trigger alerts. Using the IP address of an existing server risks detection due to address conflicts, scanning during off-hours increases chances of detection, and multiple scanning tools could trigger alerts more easily.

QUESTION 836
Two-factor authentication can be circumvented through which of the following attacks?
- **A.** Denial-of-service
- **B.** Man-in-the-middle
- **C.** Keylogging
- **D.** Brute force

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
A man-in-the-middle attack intercepts communication between the user and the system, enabling the attacker to capture authentication details. Keylogging and brute force attacks can compromise single-factor authentication but are less effective against two-factor authentication.

QUESTION 837
An organization can ensure that the recipients of emails from its employees can authenticate the identity of the sender by:
- **A.** Digitally signing all email messages.
- **B.** Encrypting all email messages.
- **C.** Compressing all email messages.
- **D.** Password-protecting all email messages.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Digital signatures ensure that the recipient can verify the sender's identity. Encryption ensures confidentiality but does not authenticate the sender. Compressing and password-protecting messages do not provide authentication.

QUESTION 838
Sending a message and a message hash encrypted by the sender's private key will ensure:
- **A.** Authenticity and integrity.
- **B.** Authenticity and privacy.
- **C.** Integrity and privacy.
- **D.** Privacy and nonrepudiation.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Encrypting the message and hash with the sender's private key ensures authenticity (proving the sender's identity) and integrity (the message was not altered). Encrypting with the sender's private key alone does not ensure privacy because anyone with the sender's public key can decrypt the message.

QUESTION 839
Which of the following is a passive attack on a network?
- **A.** Message modification
- **B.** Masquerading
- **C.** Denial-of-service
- **D.** Traffic analysis

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Traffic analysis is a passive attack where the attacker observes and analyzes the communication patterns between network devices. Message modification, masquerading, and denial-of-service are active attacks, as they involve directly altering or interfering with the communication.

QUESTION 840
An organization has a mix of access points that cannot be upgraded to stronger security and newer access points having advanced wireless security. An IS auditor recommends replacing the nonupgradeable access points. Which of the following would BEST justify the IS auditor's recommendation?

- **A.** The new access points with stronger security are affordable.
- **B.** The old access points are poorer in terms of performance.
- **C.** The organization's security would be as strong as its weakest points.
- **D.** The new access points are easier to manage.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The organization’s security is compromised by the weakest access points, making it vulnerable to attacks. Affordability, performance, and manageability are secondary to the security risks posed by the old access points.

QUESTION 841
An investment advisor e-mails periodic newsletters to clients and wants reasonable assurance that no one has modified the newsletter. This objective can be achieved by:

- encrypting the hash of the newsletter using the advisor's private key.
- encrypting the hash of the newsletter using the advisor's public key.
- digitally signing the document using the advisor's private key.
- encrypting the newsletter using the advisor's private key.

Correct Answer: A
Explanation: The objective is to assure recipients that the newsletter has not been modified (message integrity). By encrypting the hash of the newsletter using the advisor's private key, recipients can decrypt it with the public key to verify that the newsletter is unaltered. Encrypting the newsletter using a private key would not be appropriate, as it would also involve confidentiality, which is not the main concern in this case.

QUESTION 842
An IS auditor reviewing wireless network security determines that the Dynamic Host Configuration Protocol (DHCP) is disabled at all wireless access points. This practice:

- reduces the risk of unauthorized access to the network.
- is not suitable for small networks.
- automatically provides an IP address to anyone.
- increases the risks associated with Wireless Encryption Protocol (WEP).

Correct Answer: A
Explanation: Disabling DHCP reduces the risk of unauthorized access by requiring devices to use static IP addresses. This makes it harder for unauthorized devices to connect. DHCP is suitable for small networks, and its absence means IP addresses are not automatically assigned, reducing certain risks. Disabling DHCP does not increase the risks associated with WEP.

QUESTION 843
A virtual private network (VPN) provides data confidentiality by using:

- Secure Sockets Layer (SSL)
- Tunneling
- Digital signatures
- Phishing

Correct Answer: B

Explanation: VPNs provide data confidentiality by encapsulating and encrypting data through a process called tunneling. SSL is used for securing browser-server communication, digital signatures are used for authentication, and phishing is a social engineering attack, not related to VPNs.

QUESTION 844
In auditing a web server, an IS auditor should be concerned about the risk of individuals gaining unauthorized access to confidential information through:

- common gateway interface (CGI) scripts.
- enterprise Java beans (EJBs).
- applets.
- web services.

Correct Answer: A
Explanation: CGI scripts are executable programs that run on the server, which can introduce vulnerabilities. Bugs in CGI scripts may allow unauthorized access to the server, potentially compromising confidential data. Applets, EJBs, and web services have different security considerations but are controlled differently than CGI scripts.

QUESTION 845
An IS auditor reviewing access controls for a client-server environment should FIRST:

- evaluate the encryption technique.
- identify the network access points.
- review the identity management system.
- review the application-level access controls.

Correct Answer: B
Explanation: In a client-server environment, identifying network access points is crucial as they represent potential vulnerabilities. Encryption techniques, identity management, and application-level access controls should be reviewed later, but securing network access points is the priority.

QUESTION 846
To prevent IP spoofing attacks, a firewall should be configured to drop a packet if:

- the source routing field is enabled.
- it has a broadcast address in the destination field.
- a reset flag (RST) is turned on for the TCP connection.
- dynamic routing is used instead of static routing.

Correct Answer: A
Explanation: IP spoofing attacks exploit the source-routing option in the IP protocol, allowing an attacker to insert a false source IP address. A firewall should drop packets with this option enabled to prevent such attacks. The other options are unrelated to IP spoofing.

QUESTION 847
An IS auditor reviewing the implementation of an intrusion detection system (IDS) should be MOST concerned if:

- IDS sensors are placed outside of the firewall.
- a behavior-based IDS is causing many false alarms.
- a signature-based IDS is weak against new types of attacks.
- the IDS is used to detect encrypted traffic.

Correct Answer: D
Explanation: An IDS cannot detect attacks within encrypted traffic. While false alarms and weaknesses in signature-based systems are common, the primary concern is if the IDS is expected to detect threats in encrypted communications, as it is not designed for this purpose.

QUESTION 848
Which of the following BEST describes the role of a directory server in a public key infrastructure (PKI)?

- Encrypts the information transmitted over the network
- Makes other users' certificates available to applications
- Facilitates the implementation of a password policy
- Stores certificate revocation lists (CRLs)

Correct Answer: B
Explanation: A directory server in a PKI is primarily responsible for making users' certificates available to applications. Encryption of data and storage of certificate revocation lists are roles of a security server, while password policies are not part of PKI.

QUESTION 849
An organization is using symmetric encryption. Which of the following would be a valid reason for moving to asymmetric encryption? Symmetric encryption:

- provides authenticity.
- is faster than asymmetric encryption.
- can cause key management to be difficult.
- requires a relatively simple algorithm.

Correct Answer: C
Explanation: Symmetric encryption can complicate key management since each pair of users needs a unique key. This issue is resolved in asymmetric encryption. Symmetric encryption does not provide authenticity and is generally faster but more challenging to manage due to the number of keys involved.

QUESTION 850
Which of the following would provide the BEST protection against the hacking of a computer connected to the Internet?

- A remote access server
- A proxy server
- A personal firewall
- A password-generating token

Correct Answer: C
Explanation: A personal firewall provides the best protection against hacking by filtering network traffic based on rules. While remote access servers, proxy servers, and password tokens have their uses, they do not provide the same level of direct protection against hacking attempts.

QUESTION 851
When installing an intrusion detection system (IDS), which of the following is MOST important?

- Properly locating it in the network architecture
- Preventing denial-of-service (DoS) attacks
- Identifying messages that need to be quarantined
- Minimizing the rejection errors

Correct Answer: A
Explanation: Proper placement of an IDS in the network is critical to ensure that it can monitor the right areas. A poorly positioned IDS might leave key network segments unprotected. Other factors like DoS prevention, message identification, and minimizing errors are secondary concerns to proper placement.

QUESTION 852
In a public key infrastructure (PKI), which of the following may be relied upon to prove that an online transaction was authorized by a specific customer?

- Nonrepudiation
- Encryption
- Authentication
- Integrity

Correct Answer: A
Explanation:
Nonrepudiation, achieved through the use of digital signatures, ensures that the sender of a message cannot later deny having sent it, providing proof that an online transaction was authorized by the customer. Encryption protects data, but does not prove authorization. Authentication establishes identity, and integrity ensures accuracy, but neither provides nonrepudiation.

QUESTION 853
Which of the following ensures confidentiality of information sent over the Internet?

- Digital signature
- Digital certificate
- Online Certificate Status Protocol
- Private key cryptosystem

Correct Answer: D
Explanation:
A private key cryptosystem ensures confidentiality by encrypting information sent over the Internet. Digital signatures assure data integrity, authentication, and nonrepudiation, but not confidentiality. A digital certificate binds a public key with an identity, but does not address confidentiality. Online Certificate Status Protocol (OCSP) checks the revocation status of a digital certificate.

QUESTION 854
To protect a VoIP infrastructure against a denial-of-service (DoS) attack, it is MOST important to secure the:

- Access control servers
- Session border controllers
- Backbone gateways
- Intrusion detection system (IDS)

Correct Answer: B
Explanation:
Session border controllers enhance security by hiding user addresses and controlling the access and bandwidth of VoIP traffic. They are crucial in preventing DoS attacks. While access control servers, backbone gateways, and IDSs also play roles in security, session border controllers directly mitigate DoS attack risks.

QUESTION 855
Which of the following attacks targets the Secure Sockets Layer (SSL)?

- Man-in-the-middle
- Dictionary
- Password sniffing
- Phishing

Correct Answer: A
Explanation:
A man-in-the-middle attack involves an attacker intercepting SSL traffic between the user and the server, compromising secure communication. Dictionary attacks aim to crack passwords, and phishing attacks target users rather than SSL. Password sniffing does not affect SSL because SSL traffic is encrypted.

QUESTION 856
Which of the following potentially blocks hacking attempts?

- Intrusion detection system
- Honeypot system
- Intrusion prevention system
- Network security scanner

Correct Answer: C
Explanation:
An intrusion prevention system (IPS) actively detects and blocks hacking attempts, as it is deployed in-line. An intrusion detection system (IDS) only detects attacks but does not prevent them. A honeypot lures attackers to a fake target, and a network security scanner identifies vulnerabilities without stopping them.

QUESTION 857
A web server is attacked and compromised. Which of the following should be performed FIRST to handle the incident?

- Dump the volatile storage data to a disk
- Run the server in a fail-safe mode
- Disconnect the web server from the network
- Shut down the web server

Correct Answer: C
Explanation:
The first action should be to disconnect the compromised server from the network to contain the attack and prevent further damage. Dumping volatile storage data and shutting down the server can be part of the investigation process but may cause loss of valuable information. Running the server in fail-safe mode may still allow the attack to continue.

QUESTION 858
To address a maintenance problem, a vendor needs remote access to a critical network. The MOST secure and effective solution is to provide the vendor with a:

- Secure Shell (SSH-2) tunnel for the duration of the problem
- Two-factor authentication mechanism for network access
- Dial-in access
- Virtual private network (VPN) account for the duration of the vendor support contract

Correct Answer: A
Explanation:
A Secure Shell (SSH-2) tunnel provides secure, temporary access for the vendor while minimizing the risk of unauthorized access. Two-factor authentication and VPN would provide broader access, which may be unnecessary. Dial-in access is less secure and more difficult to monitor than SSH-2.

QUESTION 859
What is the BEST approach to mitigate the risk of a phishing attack?

- Implement an intrusion detection system (IDS)
- Assess website security
- Strong authentication
- User education

Correct Answer: D
Explanation:
Phishing primarily exploits users by tricking them into divulging sensitive information. Educating users on how to recognize and avoid phishing attacks is the most effective mitigation. An IDS can detect attacks, but not all phishing attacks target systems directly. Website security and strong authentication can help, but user awareness is the best defense.

QUESTION 860
A sender of an e-mail message applies a digital signature to the digest of the message. This action provides assurance of the:

- Date and time stamp of the message
- Identity of the originating computer
- Confidentiality of the message's content

- Authenticity of the sender

Correct Answer: D

Explanation:

A digital signature verifies the authenticity of the sender by binding the sender's identity to the message. It does not provide the date or time stamp, identity of the originating computer, or ensure confidentiality, as the message content itself is not encrypted.

QUESTION 861

The BEST filter rule for protecting a network from being used as an amplifier in a denial-of-service (DoS) attack is to deny all:

- Outgoing traffic with IP source addresses external to the network
- Incoming traffic with discernible spoofed IP source addresses
- Incoming traffic with IP options set
- Incoming traffic to critical hosts

Correct Answer: A

Explanation:

By denying outgoing traffic with an external IP source address, you prevent the network from being used in DoS attacks where attackers spoof the source address to make it appear as though the attack is coming from within the network. Other options do not specifically address this issue.

QUESTION 862

The network of an organization has been the victim of several intruders' attacks. Which of the following measures would allow for the early detection of such incidents?

- Antivirus software
- Hardening the servers
- Screening routers
- Honeypots

Correct Answer: D

Explanation:

Honeypots are designed to attract and capture the attention of intruders, allowing administrators to gather data on attack trends and techniques. Since they are isolated and serve no legitimate business function, any activity directed toward them is considered suspicious, making them useful for early detection of attacks. Other options do not provide direct indications of potential attacks.

QUESTION 863

A company has decided to implement an electronic signature scheme based on public key infrastructure. The user's private key will be stored on the computer's hard drive and protected by a password. The MOST significant risk of this approach is:

- Use of the user's electronic signature by another person if the password is compromised.
- Forgery by using another user's private key to sign a message with an electronic signature.
- Impersonation of a user by substitution of the user's public key with another person's public key.
- Forgery by substitution of another person's private key on the computer.

Correct Answer: A

Explanation:

If the password protecting the user's private key is compromised, an attacker could use the user's electronic signature, representing a significant risk. Other options involve more complex scenarios that are less likely to occur.

QUESTION 864

An IS auditor selects a server for a penetration test that will be carried out by a technical specialist. Which of the following is MOST important?

- The tools used to conduct the test
- Certifications held by the IS auditor
- Permission from the data owner of the server
- An intrusion detection system (IDS) is enabled

Correct Answer: C

Explanation:

Obtaining permission from the data owner is crucial to ensure that the penetration test is authorized and that the risks are understood. Other choices, while important, do not supersede the necessity of permission from the data owner.

QUESTION 865

After observing suspicious activities in a server, a manager requests a forensic analysis. Which of the following findings should be of MOST concern to the investigator?

- Server is a member of a workgroup and not part of the server domain
- Guest account is enabled on the server
- Recently, 100 users were created in the server
- Audit logs are not enabled for the server

Correct Answer: D

Explanation:

Audit logs are essential for conducting forensic investigations as they provide evidence of activities and can help trace the steps of an attacker. The other findings, while concerning, do not directly impact the ability to conduct a thorough investigation.

QUESTION 866

Which of the following would be the GREATEST cause for concern when data are sent over the Internet using HTTPS protocol?

- Presence of spyware in one of the ends
- The use of a traffic sniffing tool
- The implementation of an RSA-compliant solution
- A symmetric cryptography is used for transmitting data

Correct Answer: A

Explanation:

Spyware on an end-user's device can capture data before it is encrypted by HTTPS, making it the greatest risk. Other options pertain to encryption techniques that are generally secure against interception.

QUESTION 867

A firewall is being deployed at a new location. Which of the following is the MOST important factor in ensuring a successful deployment?

- Reviewing logs frequently
- Testing and validating the rules
- Training a local administrator at the new location
- Sharing firewall administrative duties

Correct Answer: B

Explanation:

Testing and validating the rules before deployment is critical to ensure that the firewall is secure. Incorrect rules can lead to vulnerabilities. Other actions are also important but do not have the same immediate impact on security during deployment.

QUESTION 868

The human resources (HR) department has developed a system to allow employees to enroll in benefits via a web site on the corporate Intranet. Which of the following would protect the confidentiality of the data?

- SSL encryption
- Two-factor authentication
- Encrypted session cookies
- IP address verification

Correct Answer: A

Explanation:

SSL encryption is essential for protecting the confidentiality of data transmitted over the Internet. While the other options help with security, they do not specifically address data confidentiality during transmission.

QUESTION 869

What is the MOST prevalent security risk when an organization implements remote virtual private network (VPN) access to its network?

- Malicious code could be spread across the network
- VPN logon could be spoofed
- Traffic could be sniffed and decrypted
- VPN gateway could be compromised

Correct Answer: A

Explanation:

The most significant risk is the spread of malicious code from remote clients to the organization's network. Although other options are valid concerns, mature VPN technology effectively mitigates these risks.

QUESTION 870

The use of digital signatures:

- Requires the use of a one-time password generator.
- Provides encryption to a message.
- Validates the source of a message.
- Ensures message confidentiality.

Correct Answer: C

Explanation:

Digital signatures serve to validate the identity of the sender, ensuring the integrity and authenticity of the message. They do not inherently encrypt the message or ensure confidentiality.

QUESTION 871

The FIRST step in a successful attack to a system would be:

- Gathering information.
- Gaining access.
- Denying services.
- Evading detection.

Correct Answer: A

Explanation:

The initial phase of a successful attack involves gathering information about the target to identify vulnerabilities, making it the most critical step in the attack process.

QUESTION 872

The sender of a public key would be authenticated by a:

- Certificate authority.
- Digital signature.
- Digital certificate.

- Registration authority.

Correct Answer: C
Explanation:
A digital certificate authenticates the sender of a public key, indicating that the key holder is who they claim to be. The certificate authority issues these certificates, while digital signatures ensure message integrity.

QUESTION 873
An IS auditor finds that conference rooms have active network ports. Which of the following is MOST important to ensure?

- The corporate network is using an intrusion prevention system (IPS)
- This part of the network is isolated from the corporate network
- A single sign-on has been implemented in the corporate network
- Antivirus software is in place to protect the corporate network

Correct Answer: B
Explanation:
Isolating the conference room network from the corporate network is vital to prevent unauthorized access. An IPS and other measures are important, but isolating networks is a primary security concern.

QUESTION 874
What is the BEST action to prevent loss of data integrity or confidentiality in the case of an e-commerce application running on a LAN, processing electronic fund transfers (EFT) and orders?

- Using virtual private network (VPN) tunnels for data transfer
- Enabling data encryption within the application
- Auditing the access control to the network
- Logging all changes to access lists

Correct Answer: A
Explanation:
Using VPN tunnels for data transfer provides strong encryption, protecting both confidentiality and integrity during communication over the network. Other options are beneficial practices but do not directly provide the same level of protection during transmission.

QUESTION 875
When conducting a penetration test of an IT system, an organization should be MOST concerned with:

- The confidentiality of the report.
- Finding all possible weaknesses on the system.
- Restoring all systems to the original state.
- Logging all changes made to the production system.

Correct Answer: C
Explanation:
The ability to restore all systems to their original state after a penetration test is paramount to ensure business continuity and security. While the other items are important, they are secondary to the need for restoration.

QUESTION 876
Which of the following penetration tests would MOST effectively evaluate incident handling and response capabilities of an organization?

- Targeted testing
- External testing
- Internal testing

- Double-blind testing

Correct Answer: D

Explanation:

In a double-blind test, both the administrator and security staff are unaware of the test, allowing for a realistic assessment of the organization's incident handling and response capabilities. Other testing types involve prior notification, which may skew the results.

QUESTION 877

When protecting an organization's IT systems, which of the following is normally the next line of defense after the network firewall has been compromised?

- Personal firewall
- Antivirus programs
- Intrusion detection system (IDS)
- Virtual local area network (VLAN) configuration

Correct Answer: C

Explanation:

An Intrusion Detection System (IDS) is crucial after a firewall compromise, as it can detect abnormal activities and help identify and respond to security incidents.

QUESTION 878

In wireless communication, which of the following controls allows the device receiving the communications to verify that the received communications have not been altered in transit?

- Device authentication and data origin authentication
- Wireless intrusion detection (IDS) and prevention systems (IPS)
- The use of cryptographic hashes
- Packet headers and trailers

Correct Answer: C

Explanation:

Cryptographic hashes enable verification that data has not been altered during transmission. This method effectively prevents message modification attacks, ensuring data integrity.

QUESTION 879

An organization is planning to replace its wired networks with wireless networks. Which of the following would BEST secure the wireless network from unauthorized access?

- Implement Wired Equivalent Privacy (WEP)
- Permit access to only authorized Media Access Control (MAC) addresses
- Disable open broadcast of service set identifiers (SSID)
- Implement Wi-Fi Protected Access (WPA) 2

Correct Answer: D

Explanation:

Wi-Fi Protected Access (WPA) 2 provides robust security through the Advanced Encryption Standard (AES), making it the best option for securing a wireless network. Other methods, such as WEP, are outdated and vulnerable.

QUESTION 880

An IS auditor is reviewing a software-based firewall configuration. Which of the following represents the GREATEST vulnerability? The firewall software:

- Is configured with an implicit deny rule as the last rule in the rule base.
- Is installed on an operating system with default settings.
- Has been configured with rules permitting or denying access to systems or networks.
- Is configured as a virtual private network (VPN) endpoint.

Correct Answer: B

Explanation:

Using default settings poses significant risks as they are well-known and can be easily exploited by attackers. A hardened operating system is crucial for firewall security.

QUESTION 881
The GREATEST risk posed by an improperly implemented intrusion prevention system (IPS) is:

- That there will be too many alerts for system administrators to verify.
- Decreased network performance due to IPS traffic.
- The blocking of critical systems or services due to false triggers.
- Reliance on specialized expertise within the IT organization.

Correct Answer: C
Explanation:
The most significant risk is the possibility of false triggers that may block critical systems or services, potentially leading to disruptions in business operations.

QUESTION 882
The MOST effective control for reducing the risk related to phishing is:

- Centralized monitoring of systems.
- Including signatures for phishing in antivirus software.
- Publishing the policy on antiphishing on the intranet.
- Security training for all users.

Correct Answer: D
Explanation:
Security training for users is the most effective measure against phishing, as it helps employees recognize and avoid social engineering attacks.

QUESTION 883
When reviewing a digital certificate verification process, which of the following findings represents the MOST significant risk?

- There is no registration authority (RA) for reporting key compromises.
- The certificate revocation list (CRL) is not current.
- Digital certificates contain a public key that is used to encrypt messages and verify digital signatures.
- Subscribers report key compromises to the certificate authority (CA).

Correct Answer: B
Explanation:
An outdated certificate revocation list (CRL) poses a significant risk, as it may allow the use of compromised certificates that have not been revoked.

QUESTION 884
When using a digital signature, the message digest is computed:

- Only by the sender.
- Only by the receiver.
- By both the sender and the receiver.
- By the certificate authority (CA).

Correct Answer: C
Explanation:
Both the sender and the receiver compute the message digest to verify the integrity of the message, ensuring that it has not been altered during transmission.

QUESTION 885
Which of the following would effectively verify the originator of a transaction?

- Using a secret password between the originator and the receiver
- Encrypting the transaction with the receiver's public key

- Using a portable document format (PDF) to encapsulate transaction content
- Digitally signing the transaction with the source's private key

Correct Answer: D

Explanation:

Digitally signing the transaction with the source's private key provides authentication of the originator and ensures the integrity of the transaction content.

QUESTION 886

A perpetrator looking to gain access to and gather information about encrypted data being transmitted over the network would use:

- Eavesdropping.
- Spoofing.
- Traffic analysis.
- Masquerading.

Correct Answer: C

Explanation:

Traffic analysis involves observing the patterns and characteristics of encrypted data transmissions, allowing an attacker to infer information without decrypting the data itself.

QUESTION 887

Upon receipt of the initial signed digital certificate, the user will decrypt the certificate with the public key of the:

- Registration authority (RA).
- Certificate authority (CA).
- Certificate repository.
- Receiver.

Correct Answer: B

Explanation:

The user decrypts the digital certificate using the public key of the Certificate Authority (CA), which signed the certificate to verify its authenticity.

QUESTION 888

IS management is considering a Voice-over Internet Protocol (VoIP) network to reduce telecommunication costs and management asked the IS auditor to comment on appropriate security controls. Which of the following security measures is MOST appropriate?

- Review and, where necessary, upgrade firewall capabilities
- Install modems to allow remote maintenance support access
- Create a physically distinct network to handle VoIP traffic
- Redirect all VoIP traffic to allow clear text logging of authentication credentials

Correct Answer: A

Explanation:

Reviewing and upgrading firewall capabilities is crucial to ensure that firewalls can adequately handle VoIP traffic and protect against associated vulnerabilities.

QUESTION 889

Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?

- Statistical-based
- Signature-based
- Neural network
- Host-based

Correct Answer: A

Explanation:

Statistical-based IDSs, which rely on defined norms of expected behavior, are prone to flagging normal activities as suspicious, leading to false alarms.

QUESTION 890
When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

- Hardware is protected against power surges.
- Integrity is maintained if the main power is interrupted.
- Immediate power will be available if the main power is lost.
- Hardware is protected against long-term power fluctuations.

Correct Answer: A
Explanation:
A voltage regulator protects hardware against short-term power surges, helping to prevent damage from sudden fluctuations in power supply.

QUESTION 891
Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?

- Halon gas
- Wet-pipe sprinklers
- Dry-pipe sprinklers
- Carbon dioxide gas

Correct Answer: C
Explanation:
Water sprinklers with an automatic power shutoff system are efficient and environmentally friendly. Dry-pipe sprinklers prevent leakage risks, while Halon is effective but environmentally damaging. Carbon dioxide is less efficient for occupied areas due to safety concerns.

QUESTION 892
Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

- Power line conditioners
- Surge protective devices
- Alternative power supplies
- Interruptible power supplies

Correct Answer: A
Explanation:
Power line conditioners manage voltage fluctuations and protect equipment from peaks and valleys in power supply. Other options serve different purposes, like protecting against surges or providing backup power for longer durations.

QUESTION 893
An IS auditor inspected a windowless room containing phone switching and networking equipment and documentation binders. The room was equipped with two handheld fire extinguishers—one filled with CO2, the other filled with halon. Which of the following should be given the HIGHEST priority in the auditor's report?

- The halon extinguisher should be removed because halon has a negative impact on the atmospheric ozone layer.
- Both fire suppression systems present a risk of suffocation when used in a closed room.
- The CO2 extinguisher should be removed because CO2 is ineffective for suppressing fires involving solid combustibles (paper).

- The documentation binders should be removed from the equipment room to reduce potential risks.

  Correct Answer: B

  Explanation:

  Protecting lives is the top priority in fire suppression. Both CO2 and halon reduce oxygen levels and can pose suffocation risks in closed spaces. While halon may be environmentally harmful, the immediate concern is personal safety.

QUESTION 894

Which of the following would be BEST prevented by a raised floor in the computer machine room?

- Damage of wires around computers and servers
- A power failure from static electricity
- Shocks from earthquakes
- Water flood damage

  Correct Answer: A

  Explanation:

  A raised floor allows for cable management, reducing the risk of damage caused by improperly placed cables. It does not effectively prevent static electricity, earthquakes, or water damage from overhead sources.

QUESTION 895

A penetration test performed as part of evaluating network security:

- Provides assurance that all vulnerabilities are discovered.
- Should be performed without warning the organization's management.
- Exploits the existing vulnerabilities to gain unauthorized access.
- Would not damage the information assets when performed at network perimeters.

  Correct Answer: C

  Explanation:

  Penetration tests actively seek to exploit vulnerabilities to assess security measures, simulating a real attack. They can potentially damage information assets and do not guarantee all vulnerabilities will be found.

QUESTION 896

Users are issued security tokens to be used in combination with a PIN to access the corporate virtual private network (VPN). Regarding the PIN, what is the MOST important rule to be included in a security policy?

- Users should not leave tokens where they could be stolen.
- Users must never keep the token in the same bag as their laptop computer.
- Users should select a PIN that is completely random, with no repeating digits.
- Users should never write down their PIN.

  Correct Answer: D

  Explanation:

  Writing down a PIN poses a security risk if the token is stolen. The effectiveness of two-factor authentication relies on both components being kept secret, regardless of whether the PIN is random.

QUESTION 897

Which of the following fire suppression systems is MOST appropriate to use in a data center environment?

- Wet-pipe sprinkler system
- Dry-pipe sprinkler system
- FM-200 system

- Carbon dioxide-based fire extinguishers

Correct Answer: C

Explanation:

FM-200 is a clean agent effective for gaseous fire suppression, making it suitable for sensitive equipment. Water-based extinguishers can cause damage, and carbon dioxide may not provide rapid enough protection.

QUESTION 898

During the review of a biometrics system operation, an IS auditor should FIRST review the stage of:

- Enrollment.
- Identification.
- Verification.
- Storage.

Correct Answer: A

Explanation:

Enrollment is the first step in biometric systems, where user characteristics are captured and converted into a template for future identification and verification.

QUESTION 899

An accuracy measure for a biometric system is:

- System response time.
- Registration time.
- Input file size.
- False-acceptance rate.

Correct Answer: D

Explanation:

The false-acceptance rate (FAR) is a critical measure of accuracy in biometric systems, indicating how often unauthorized users are incorrectly accepted.

QUESTION 900

What is a risk associated with attempting to control physical access to sensitive areas such as computer rooms using card keys or locks?

- Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.
- The contingency plan for the organization cannot effectively test controlled access practices.
- Access cards, keys, and pads can be easily duplicated allowing easy compromise of the control.
- Removing access for those who are no longer authorized is complex.

Correct Answer: A

Explanation:

Piggybacking, where unauthorized individuals follow authorized personnel into restricted areas, poses a significant security risk in physical access control.