# PrepKing

Number: JKO-018
Passing Score: 750
Time Limit: 120 min
File Version: 8.0

*PrepKing-JKO-018*

## Exam A

**QUESTION 1**
Which of the following elements of PKI are found in a browser's trusted root CA?

A. Private key
B. Symmetric key
C. Recovery key
D. Public key

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 2**
Which of the following protocols only encrypts password packets from client to server?

A. XTACACS
B. TACACS
C. RADIUS
D. TACACS+

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 3**
Where are revoked certificates stored?

A. Recovery agent
B. Registration
C. Key escrow
D. CRL

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 4**
DRPs should contain which of the following?

A. Hierarchical list of non-critical personnel
B. Hierarchical list of critical systems
C. Hierarchical access control lists
D. Identification of single points of failure

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 5**
A system administrator could have a user level account and an administrator account to prevent:

A. password sharing.
B. escalation of privileges.
C. implicit deny.
D. administrative account lockout.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 6**
Which of the following is the BEST way to mitigate data loss if a portable device is compromised?

A. Full disk encryption
B. Common access card
C. Strong password complexity
D. Biometric authentication

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 7**
Which of the following protocols should be blocked at the network perimeter to prevent host enumeration by sweep devices?

A. HTTPS
B. SSH
C. IPv4
D. ICMP

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 8**
Which of the following is specific to a buffer overflow attack?

A. Memory addressing
B. Directory traversal
C. Initial vector
D. Session cookies

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 9**
Which of the following asymmetric encryption keys is used to encrypt data to ensure only the intended recipient can decrypt the ciphertext?

A. Private
B. Escrow
C. Public
D. Preshared

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 10**
Which of the following should a security administrator implement to prevent users from disrupting network connectivity, if a user connects both ends of a network cable to different switch ports?

A. VLAN separation
B. Access control
C. Loop protection
D. DMZ

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 11**
A new enterprise solution is currently being evaluated due to its potential to increase the company's profit margins. The security administrator has been asked to review its security implications. While evaluating the product, various vulnerability scans were performed. It was determined that the product is not a threat but has the potential to introduce additional vulnerabilities. Which of the following assessment types should the security administrator also take into consideration while evaluating this product?

A. Threat assessment
B. Vulnerability assessment
C. Code assessment
D. Risk assessment

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 12**
Which of the following requires special handling and explicit policies for data retention and data distribution?

A. Personally identifiable information
B. Phishing attacks
C. Zero day exploits
D. Personal electronic devices

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 13**
Centrally authenticating multiple systems and applications against a federated user database is an example of:

A. smart card.
B. common access card.
C. single sign-on.
D. access control list.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 14**
WEP is seen as an unsecure protocol based on its improper use of which of the following?

A. RC6
B. RC4

C. 3DES

D. AES

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 15**
Which of the following should be performed if a smartphone is lost to ensure no data can be retrieved from it?

A. Device encryption

B. Remote wipe

C. Screen lock

D. GPS tracking

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 16**
In an 802.11n network, which of the following provides the MOST secure method of both encryption and authorization?

A. WEP with 802.1x

B. WPA Enterprise

C. WPA2-PSK

D. WPA with TKIP

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 17**
Which of the following methods of access, authentication, and authorization is the MOST secure by default?

A. Kerberos

B. TACACS

C. RADIUS

D. LDAP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 18**
Which of the following facilitates computing for heavily utilized systems and networks?

A. Remote access
B. Provider cloud
C. VPN concentrator
D. Telephony

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 19**
With which of the following is RAID MOST concerned?

A. Integrity
B. Confidentiality
C. Availability
D. Baselining

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 20**
Which of the following reduces the likelihood of a single point of failure when a server fails?

A. Clustering
B. Virtualization
C. RAID
D. Cold site

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 21**
A user downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?

A. Logic bomb

B. Worm

C. Trojan

D. Adware

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 22**
Which of the following is used in conjunction with PEAP to provide mutual authentication between peers?

A. LEAP

B. MSCHAPv2

C. PPP

D. MSCHAPv1

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 23**
A targeted email attack sent to the company's Chief Executive Officer (CEO) is known as which of the following?

A. Whaling

B. Bluesnarfing

C. Vishing

D. Dumpster diving

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 24**
Which of the following uses TCP port 22 by default?

A. SSL, SCP, and TFTP

B. SSH, SCP, and SFTP

C. HTTPS, SFTP, and TFTP

D. TLS, TELNET, and SCP

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 25**
Actively monitoring data streams in search of malicious code or behavior is an example of:

A. load balancing.
B. an Internet proxy.
C. URL filtering.
D. content inspection.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 26**
A user is no longer able to transfer files to the FTP server. The security administrator has verified the ports are open on the network firewall. Which of the following should the security administrator check?

A. Anti-virus software
B. ACLs
C. Anti-spam software
D. NIDS

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 27**
A Human Resource manager is assigning access to users in their specific department performing the same job function. This is an example of:

A. role-based access control.
B. rule-based access control.
C. centralized access control.
D. mandatory access control.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 28**

Which of the following BEST describes the process of key escrow?

A. Maintains a copy of a user's public key for the sole purpose of recovering messages if it is lost
B. Maintains a secured copy of a user's private key to recover the certificate revocation list
C. Maintains a secured copy of a user's private key for the sole purpose of recovering the key if it is lost
D. Maintains a secured copy of a user's public key in order to improve network performance

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 29**
Which of the following network devices would MOST likely be used to detect but not react to suspicious behavior on the network?

A. Firewall
B. NIDS
C. NIPS
D. HIDS

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 30**
Which of the following is an example of allowing a user to perform a self-service password reset?

A. Password length
B. Password recovery
C. Password complexity
D. Password expiration

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 31**
Which of the following wireless attacks uses a counterfeit base station with the same SSID name as a nearby intended wireless network?

A. War driving
B. Evil twin
C. Rogue access point
D. War chalking

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 32**
A security administrator finished taking a forensic image of a computer's memory. Which of the following should the administrator do to ensure image integrity?

A. Run the image through AES128.
B. Run the image through a symmetric encryption algorithm.
C. Compress the image to a password protected archive.
D. Run the image through SHA256.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 33**
Which of the following BEST explains the security benefit of a standardized server image?

A. All current security updates for the operating system will have already been applied.
B. Mandated security configurations have been made to the operating system.
C. Anti-virus software will be installed and current.
D. Operating system license use is easier to track.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 34**
Which of the following is the primary purpose of using a digital signature? (Select TWO).

A. Encryption
B. Integrity
C. Confidentiality
D. Non-repudiation
E. Availability

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 35**
Which of the following must a security administrator do when the private key of a web server has been compromised by an intruder?

A. Submit the public key to the CRL.
B. Use the recovery agent to revoke the key.
C. Submit the private key to the CRL.
D. Issue a new CA.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 36**
The security administrator often observes that an employee who entered the datacenter does not match the owner of the PIN that was entered into the keypad. Which of the following would BEST prevent this situation?

A. Multifactor authentication
B. Username and password
C. Mandatory access control
D. Biometrics

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 37**
A programmer allocates 16 bytes for a string variable, but does not adequately ensure that more than 16 bytes cannot be copied into the variable. This program may be vulnerable to which of the following attacks?

A. Buffer overflow
B. Cross-site scripting
C. Session hijacking
D. Directory traversal

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 38**
An administrator is updating firmware on routers throughout the company. Where should the administrator document this work?

A. Event Viewer

B. Router's System Log

C. Change Management System

D. Compliance Review System

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 39**
The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses:

A. multiple keys for non-repudiation of bulk data.

B. different keys on both ends of the transport medium.

C. bulk encryption for data transmission over fiber.

D. the same key on each end of the transmission medium.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 40**
Which of the following allows a user to have a one-time password?

A. Biometrics

B. SSO

C. PIV

D. Tokens

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 41**
Which of the following allows a security administrator to set device traps?

A. SNMP

B. TLS

C. ICMP

D. SSH

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 42**
Which of the following is the BEST way to secure data for the purpose of retention?

A. Off-site backup
B. RAID 5 on-site backup
C. On-site clustering
D. Virtualization

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 43**
In which of the following locations would a forensic analyst look to find a hooked process?

A. BIOS
B. Slack space
C. RAM
D. Rootkit

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 44**
Several classified mobile devices have been stolen. Which of the following would BEST reduce the data leakage threat?

A. Use GPS tracking to find the devices.
B. Use stronger encryption algorithms.
C. Immediately inform local law enforcement.
D. Remotely sanitize the devices.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 45**
Which of the following is an example of requiring users to have a password of 16 characters or more?

A. Password recovery requirements

B. Password complexity requirements
C. Password expiration requirements
D. Password length requirements

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 46**
Which of the following devices provides storage for RSA or asymmetric keys and may assist in user authentication? (Select TWO).

A. Trusted platform module
B. Hardware security module
C. Facial recognition scanner
D. Full disk encryption
E. Encrypted USB

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 47**
A small company needs to invest in a new expensive database. The company's budget does not include the purchase of additional servers or personnel. Which of the following solutions would allow the small company to save money on hiring additional personnel and minimize the footprint in their current datacenter?

A. Allow users to telecommute
B. Setup a load balancer
C. Infrastructure as a Service
D. Software as a Service

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 48**
A security administrator needs to implement a site-to-site VPN tunnel between the main office and a remote branch. Which of the following protocols should be used for the tunnel?

A. RTP
B. SNMP
C. IPSec
D. 802.1X

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 49**
When examining HTTP server logs the security administrator notices that the company's online store crashes after a particular search string is executed by a single external user. Which of the following BEST describes this type of attack?

A. Spim
B. DDoS
C. Spoofing
D. DoS

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 50**
Which of the following MUST a programmer implement to prevent cross-site scripting?

A. Validate input to remove shell scripts
B. Validate input to remove hypertext
C. Validate input to remove batch files
D. Validate input to remove Java bit code

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 51**
Which of the following is seen as non-secure based on its ability to only store seven uppercase characters of data making it susceptible to brute force attacks?

A. PAP
B. NTLMv2
C. LANMAN
D. CHAP

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 52**
Which of the following should be used to help prevent device theft of unused assets?

A. HSM device
B. Locking cabinet
C. Device encryption
D. GPS tracking

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 53**
Which of the following security practices should occur initially in software development?

A. Secure code review
B. Patch management
C. Fuzzing
D. Penetration tests

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 54**
Which of the following uses tickets to identify users to the network?

A. RADIUS
B. LDAP
C. TACACS+
D. Kerberos

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 55**
Which of the following file transfer protocols is an extension of SSH?

A. FTP
B. TFTP
C. SFTP

D. FTPS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 56**
Due to sensitive data concerns, a security administrator has enacted a policy preventing the use of flash drives. Additionally, which of the following can the administrator implement to reduce the risk of data leakage?

A. Enact a policy that all work files are to be password protected.
B. Enact a policy banning users from bringing in personal music devices.
C. Provide users with unencrypted storage devices that remain on-site.
D. Disallow users from saving data to any network share.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 57**
The security administrator implemented privacy screens, password protected screen savers, and hired a secure shredding and disposal service. Which of the following attacks is the security administrator trying to mitigate? (Select TWO).

A. Whaling
B. Dumpster diving
C. Shoulder surfing
D. Tailgating
E. Impersonation

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 58**
Performing routine security audits is a form of which of the following controls?

A. Preventive
B. Detective
C. Protective
D. Proactive

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 59**
Which of the following web application security weaknesses can be mitigated by preventing the use of HTML tags?

A. LDAP injection
B. SQL injection
C. Error and exception handling
D. Cross-site scripting

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 60**
Which of the following access control technologies provides a rolling password for one-time use?

A. RSA tokens
B. ACL
C. Multifactor authentication
D. PIV card

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 61**
Which of the following would be the BEST action to perform when conducting a corporate vulnerability assessment?

A. Document scan results for the change control board.
B. Organize data based on severity and asset value.
C. Examine the vulnerability data using a network analyzer.
D. Update antivirus signatures and apply patches.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 62**
Which of the following would allow traffic to be redirected through a malicious machine by sending false hardware address updates to a switch?

A. ARP poisoning
B. MAC spoofing
C. pWWN spoofing
D. DNS poisoning

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 63**
Which of the following devices would be installed on a single computer to prevent intrusion?

A. Host intrusion detection
B. Network firewall
C. Host-based firewall
D. VPN concentrator

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 64**
Which of the following is a policy that would force all users to organize their areas as well as help in reducing the risk of possible data theft?

A. Password behaviors
B. Clean desk policy
C. Data handling
D. Data disposal

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 65**
A penetration test shows that almost all database servers were able to be compromised through a default database user account with the default password. Which of the following is MOST likely missing from the operational procedures?

A. Application hardening
B. OS hardening
C. Application patch management
D. SQL injection

**Correct Answer:** A

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 66**
Isolation mode on an AP provides which of the following functionality types?

A. Segmentation of each wireless user from other wireless users

B. Disallows all users from communicating directly with the AP

C. Hides the service set identifier

D. Makes the router invisible to other routers

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 67**
Which of the following secure protocols is MOST commonly used to remotely administer Unix/Linux systems?

A. SSH

B. SCP

C. SFTP

D. SNMP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 68**
Which of the following is MOST likely to be the last rule contained on any firewall?

A. IP allow any any

B. Implicit deny

C. Separation of duties

D. Time of day restrictions

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 69**
During the analysis of malicious code, a security analyst discovers JavaScript being used to send random data to another service on the same system. This is MOST likely an example of which of the following?

A. Buffer overflow
B. XML injection
C. SQL injection
D. Distributed denial of service

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 70**
Which of the following is true about hardware encryption? (Select TWO).

A. It must use elliptical curve encryption.
B. It requires a HSM file system.
C. It only works when data is not highly fragmented.
D. It is faster than software encryption.
E. It is available on computers using TPM.

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 71**
Which of the following is an example of verifying new software changes on a test system?

A. User access control
B. Patch management
C. Intrusion prevention
D. Application hardening

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 72**
Which of the following is a technical control?

A. System security categorization requirement
B. Baseline configuration development
C. Contingency planning
D. Least privilege implementation

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 73**
Public keys are used for which of the following?

A. Decrypting wireless messages
B. Decrypting the hash of an electronic signature
C. Bulk encryption of IP based email traffic
D. Encrypting web browser traffic

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 74**
Which of the following penetration testing types is performed by security professionals with limited inside knowledge of the network?

A. Passive vulnerability scan
B. Gray box
C. White box
D. Black box

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 75**
Which of the following devices BEST allows a security administrator to identify malicious activity after it has occurred?

A. Spam filter
B. IDS
C. Firewall
D. Malware inspection

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 76**
Which of the following cloud computing concepts is BEST described as providing an easy-to- configure OS and on-demand computing for customers?

A. Platform as a Service
B. Software as a Service
C. Infrastructure as a Service
D. Trusted OS as a Service

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 77**
A security administrator wants to prevent users in sales from accessing their servers after 6:00

A. m., and prevent them from accessing accounting's network at all times. Which of the following should the administrator implement to accomplish these goals? (Select TWO).
B. Separation of duties
C. Time of day restrictions
D. Access control lists
E. Mandatory access control
F. Single sign-on

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 78**
Which of the following environmental controls would BEST be used to regulate cooling within a datacenter?

A. Fire suppression
B. Video monitoring
C. EMI shielding

D. Hot and cold aisles

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 79**
Which of the following is used when performing a quantitative risk analysis?

A. Focus groups
B. Asset value
C. Surveys
D. Best practice

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 80**
Which of the following BEST describes the function of TPM?

A. High speed secure removable storage device
B. Third party certificate trust authority
C. Hardware chip that stores encryption keys
D. A trusted OS model

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 81**
Which of the following PKI implementation element is responsible for verifying the authenticity of certificate contents?

A. CRL
B. Key escrow
C. Recovery agent
D. CA

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 82**
Which of the following describes a passive attempt to identify weaknesses?

A. Vulnerability scanning
B. Zero day attack
C. Port scanning
D. Penetration testing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 83**

The security administrator is getting reports from users that they are accessing certain websites and are unable to download anything off of those sites. The security administrator is also receiving several alarms from the IDS about suspicious traffic on the network. Which of the following is the MOST likely cause?

A. NIPS is blocking activities from those specific websites.
B. NIDS is blocking activities from those specific websites.
C. The firewall is blocking web activity.
D. The router is denying all traffic from those sites.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 84**
Which of the following should be enabled to ensure only certain wireless clients can access the network?

A. DHCP
B. SSID broadcast
C. MAC filtering
D. AP isolation

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 85**
Which of the following is the BEST choice for encryption on a wireless network?

A. WPA2-PSK
B. AES
C. WPA
D. WEP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 86**

Which of the following will educate employees about malicious attempts from an attacker to obtain bank account information?

A. Password complexity requirements
B. Phishing techniques
C. Handling PII
D. Tailgating techniques

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 87**
If a user wishes to receive a file encrypted with PGP, the user must FIRST supply the:

A. public key.
B. recovery agent.
C. key escrow account.
D. private key.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 88**
Which of the following is a reason to perform a penetration test?

A. To passively test security controls within the enterprise
B. To provide training to white hat attackers
C. To identify all vulnerabilities and weaknesses within the enterprise
D. To determine the impact of a threat against the enterprise

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 89**
Which of the following methods BEST describes the use of hiding data within other files?

A. Digital signatures
B. PKI
C. Transport encryption
D. Steganography

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 90**
Which of the following BEST describes the proper method and reason to implement port security?

A. Apply a security control which ties specific ports to end-device MAC addresses and prevents additional devices from being connected to the network.
B. Apply a security control which ties specific networks to end-device IP addresses and prevents new devices from being connected to the network.
C. Apply a security control which ties specific ports to end-device MAC addresses and prevents all devices from being connected to the network.
D. Apply a security control which ties specific ports to end-device IP addresses and prevents
mobile devices from being connected to the network.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 91**
Which of the following attacks is manifested as an embedded HTML image object or JavaScript image tag in an email?

A. Exception handling
B. Adware
C. Cross-site request forgery
D. Cross-site scripting

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 92**
Which of the following is MOST likely to result in data loss?

A. Accounting transferring confidential staff details via SFTP to the payroll department.
B. Back office staff accessing and updating details on the mainframe via SSH.
C. Encrypted backup tapes left unattended at reception for offsite storage.
D. Developers copying data from production to the test environments via a USB stick.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 93**
A security administrator has discovered through a password auditing software that most passwords can be discovered by cracking the first seven characters and then cracking the second part of the password. Which of the following is in use by the company?

A. LANMAN
B. MD5

C. WEP
D. 3DES

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 94**
Which of the following concepts ensures that the data is only viewable to authorized users?

A. Availability
B. Biometrics
C. Integrity
D. Confidentiality

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 95**
Which of the following BEST describes an intrusion prevention system?

A. A system that stops an attack in progress.
B. A system that allows an attack to be identified.
C. A system that logs the attack for later analysis.
D. A system that serves as a honeypot.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 96**
A user reports that their 802.11n capable interface connects and disconnects frequently to an access point that was recently installed. The user has a Bluetooth enabled laptop. A company in the next building had their wireless network breached last month. Which of the following is MOST likely causing the disconnections?

A. An attacker inside the company is performing a bluejacking attack on the user's laptop.

B. Another user's Bluetooth device is causing interference with the Bluetooth on the laptop.

C. The new access point was mis-configured and is interfering with another nearby access point.

D. The attacker that breached the nearby company is in the parking lot implementing a war driving attack.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 97**
Risk can be managed in the following ways EXCEPT:

A. mitigation.

B. acceptance.

C. elimination.

D. transference.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 98**
A web application has been found to be vulnerable to a SQL injection attack. Which of the following BEST describes the required remediation action?

A. Change the server's SSL key and add the previous key to the CRL.

B. Install a host-based firewall.

C. Install missing security updates for the operating system.

D. Add input validation to forms.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 99**
While browsing the Internet, an administrator notices their browser behaves erratically, appears to download something, and then crashes. Upon restarting the PC, the administrator notices performance is extremely slow and there are hundreds of outbound connections to various websites. Which of the following BEST describes what has occurred?

A. The PC has become part of a botnet.

B. The PC has become infected with spyware.

C. The PC has become a spam host.

D. The PC has become infected with adware.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 100**
Which of the following is a best practice when securing a switch from physical access?

A. Disable unnecessary accounts
B. Print baseline configuration
C. Enable access lists
D. Disable unused ports

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 101**
A security administrator is asked to email an employee their password. Which of the following account policies MUST be set to ensure the employee changes their password promptly?

A. Password expiration
B. Account lockout
C. Password recovery
D. Account enablement

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 102**
Data can potentially be stolen from a disk encrypted, screen-lock protected, smartphone by which of the following?

A. Bluesnarfing
B. IV attack
C. Honeynet
D. SIM cloning

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 103**
A purpose of LDAP authentication services is:

A. to implement mandatory access controls.
B. a single point of user management.
C. to prevent multifactor authentication.
D. to issue one-time hashed passwords.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 104**
Which of the following allows an attacker to identify vulnerabilities within a closed source software application?

A. Fuzzing
B. Compiling
C. Code reviews
D. Vulnerability scanning

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 105**
Which of the following should the security administrator look at FIRST when implementing an AP to gain more coverage?

A. Encryption methods
B. Power levels
C. SSID
D. Radio frequency

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 106**
Which of the following would an administrator do to ensure that an application is secure and all unnecessary services are disabled?

A. Baselining
B. Application hardening
C. Secure application coding

D. Patch management

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 107**
Which of the following security threats does shredding mitigate?

A. Shoulder surfing
B. Document retention
C. Tailgating
D. Dumpster diving

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 108**
A thumbprint scanner is used to test which of the following aspects of human authentication?

A. Something a user did

B. Something a user has
C. Something a user is
D. Something a user knows

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 109**
Which of the following protocols requires the use of a CA based authentication process?

A. FTPS implicit
B. FTPS explicit
C. MD5
D. PEAP-TLS

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 110**

Which of the following malware types is an antivirus scanner MOST unlikely to discover? (Select TWO).

A. Trojan
B. Pharming
C. Worms
D. Virus
E. Logic bomb

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 111**
An existing application has never been assessed from a security perspective. Which of the following is the BEST assessment technique in order to identify the application's security posture?

A. Baseline reporting
B. Protocol analysis
C. Threat modeling
D. Functional testing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 112**
A security administrator with full administrative rights on the network is forced to change roles on a quarterly basis with another security administrator. Which of the following describes this form of access control?

A. Job rotation
B. Separation of duties
C. Mandatory vacation
D. Least privilege

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 113**
In order to access the network, an employee must swipe their finger on a device. Which of the following describes this form of authentication?

A. Single sign-on
B. Multifactor

C. Biometrics
D. Tokens

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 114**
MAC filtering is a form of which of the following?

A. Virtualization
B. Network Access Control
C. Virtual Private Networking
D. Network Address Translation

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 115**
Which of the following tools provides the ability to determine if an application is transmitting a password in clear-text?

A. Protocol analyzer
B. Port scanner
C. Vulnerability scanner
D. Honeypot

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 116**
A certificate that has been compromised should be published to which of the following?

A. AES
B. CA
C. CRL
D. PKI

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 117**
NTLM is an improved and substantially backwards compatible replacement for which of the following?

A. 3DES
B. LANMAN
C. PGP
D. passwd

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 118**
A security administrator is implementing a solution that can integrate with an existing server and provide encryption capabilities. Which of the following would meet this requirement?

A. Mobile device encryption
B. Full disk encryption
C. TPM
D. HSM

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 119**
A security administrator working for a health insurance company needs to protect customer data by installing an HVAC system and a mantrap in the datacenter. Which of the following are being addressed? (Select TWO).

A. Integrity
B. Recovery
C. Clustering
D. Confidentiality
E. Availability

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 120**
Which of the following can a security administrator implement to help identify smurf attacks?

A. Load balancer
B. Spam filters
C. NIDS
D. Firewall

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 121**
The security administrator notices a number of TCP connections from the development department to the test network segregation. Large volumes of data are being transmitted between the two networks only on port 22. Which of the following is MOST likely occurring?

A. The development team is transferring data to test systems using FTP and TFTP.
B. The development team is transferring data to test systems using SCP and TELNET.
C. The development team is transferring data to test systems using SFTP and SCP.
D. The development team is transferring data to test systems using SSL and SFTP.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 122**
A company that purchases insurance to reduce risk is an example of which of the following?

A. Risk deterrence
B. Risk acceptance
C. Risk avoidance
D. Risk transference

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 123**
Which of the following are the BEST reasons to use an HSM? (Select TWO).

A. Encrypt the CPU L2 cache
B. Recover keys
C. Generate keys
D. Transfer keys to the CPU

E. Store keys

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 124**
Which of the following is a reason to perform user awareness and training?

A. To enforce physical security requirements by staff
B. To minimize the organizational risk posed by users
C. To comply with law and vendor software best practices
D. To identify the staff's personally owned electronic devices

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 125**
When configuring multiple computers for RDP on the same wireless router, it may be necessary to do which of the following?

A. Forward to different RDP listening ports.
B. Turn off port forwarding for each computer.
C. Enable DMZ for each computer.
D. Enable AP isolation on the router.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 126**
Used in conjunction, which of the following are PII? (Select TWO).

A. Marital status
B. Favorite movie
C. Pet's name
D. Birthday
E. Full name

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 127**
Which of the following can prevent an unauthorized employee from entering a datacenter? (Select TWO).

A. Failsafe
B. Video surveillance
C. Bollards
D. Security guard
E. Proximity reader

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 128**
The security administrator is tasked with authenticating users to access an encrypted database. Authentication takes place using PKI and the encryption of the database uses a separate cryptographic process to decrease latency. Which of the following would describe the use of encryption in this situation?

A. Private key encryption to authenticate users and private keys to encrypt the database
B. Private key encryption to authenticate users and public keys to encrypt the database
C. Public key encryption to authenticate users and public keys to encrypt the database
D. Public key encryption to authenticate users and private keys to encrypt the database

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 129**
A proximity card reader is used to test which of the following aspects of human authentication?

A. Something a user knows
B. Something a user is
C. Something a user did
D. Something a user has

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 130**
Which of the following wireless security controls can be easily and quickly circumvented using only a network sniffer? (Select TWO).

A. MAC filtering
B. Disabled SSID broadcast
C. WPA2-Enterprise
D. EAP-TLS
E. WEP with 802.1x

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 131**
Which of the following would need to be configured correctly to allow remote access to the network?

A. ACLs
B. Kerberos
C. Tokens
D. Biometrics

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 132**
Which of the following attacks would password masking help mitigate?

A. Shoulder surfing
B. Brute force
C. Tailgating
D. Impersonation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 133**
A technician needs to limit the wireless signal from reaching outside of a building. Which of the following actions should the technician take?

A. Disable the SSID broadcast on the WAP
B. Place the WAP antenna on the exterior wall of the building
C. Decrease the power levels on the WAP
D. Enable MAC filtering in the WAP

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 134**
A security administrator has been receiving support tickets for unwanted windows appearing on user's workstations. Which of the following can the administrator implement to help prevent this from happening?

A. Pop-up blockers
B. Screen locks
C. Host-based firewalls
D. Antivirus

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 135**
On-going annual awareness security training should be coupled with:

A. succession planning.
B. implementation of security controls.
C. user rights and permissions review.
D. signing of a user agreement.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 136**
Employees are required to come up with a passphrase of at least 15 characters to access the corporate network. Which of the following account policies does this exemplify?

A. Password expiration
B. Password complexity
C. Password lockout
D. Password length

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 137**
Which of the following would an administrator apply to mobile devices to BEST ensure the confidentiality of data?

A. Screen locks
B. Device encryption
C. Remote sanitization
D. Antivirus software

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 138**
Which of the following functions is MOST likely performed by a web security gateway?

A. Protocol analyzer
B. Content filtering
C. Spam filtering
D. Flood guard

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 139**
An administrator identifies a security issue on the corporate web server, but does not attempt to exploit it. Which of the following describes what the administrator has done?

A. Vulnerability scan
B. Penetration test
C. Social engineering
D. Risk mitigation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 140**
An administrator who wishes to block all database ports at the firewall should include which of the following ports in the block list?

A. 445
B. 1433

C. 1501

D. 3389

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 141**
Which of the following devices is often used to cache and filter content?

A. Proxies

B. Firewall

C. VPN

D. Load balancer

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 142**
Which of the following is the primary difference between a virus and a worm?

A. A worm is undetectable

B. A virus is typically larger

C. A virus is easily removed

D. A worm is self-replicating

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 143**
Which of the following describes when forensic hashing should occur on a drive?

A. After the imaging process and before the forensic image is captured

B. Before the imaging process and then after the forensic image is created

C. After the imaging process and after the forensic image is captured

D. Before and after the imaging process and then hash the forensic image

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 144**
Which of the following would be considered multifactor authentication?

A. Pin number and a smart card
B. ACL entry and a pin number
C. Username and password
D. Common access card

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 145**
Which of the following is a security vulnerability that can be disabled for mobile device users?

A. Group policy
B. Remote wipe
C. GPS tracking
D. Pop-up blockers

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 146**
Which of the following threats corresponds with an attacker targeting specific employees of a company?

A. Spear phishing
B. Phishing
C. Pharming
D. Man-in-the-middle

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 147**

An application log shows that the text "test; rm -rf /etc/passwd" was entered into an HTML form. Which of the following describes the type of attack that was attempted?

A. Session hijacking
B. Command injection

C. Buffer overflow

D. SQL injection

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 148**
When a user first moves into their residence, the user receives a key that unlocks and locks their front door. This key is only given to them but may be shared with others they trust. Which of the following cryptography concepts is illustrated in the example above?

A. Asymmetric key sharing

B. Exchange of digital signatures

C. Key escrow exchange

D. Symmetric key sharing

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 149**
Which of the following does a TPM allow for?

A. Cloud computing

B. Full disk encryption

C. Application hardening

D. Input validation

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 150**

If a security administrator wants to TELNET into a router to make configuration changes, which of the following ports would need to be open by default?

A. 23

B. 135

C. 161

D. 3389

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 151**
Logs from an IDS show that a computer has been compromised with a botnet and is actively communicating with a command and control server. If the computer is powered off, which of the following data types will be unavailable for later investigation?

A. Swap files, system processes, and master boot record
B. Memory, temporary file system, and archival storage
C. System disk, email, and log files
D. Memory, network processes, and system processes

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 152**
A security administrator ensures that certain characters and commands entered on a web server are not interpreted as legitimate data and not passed on to backend servers. This is an example of which of the following?

A. Error and exception handling
B. Input validation
C. Determining attack surface
D. Data execution prevention

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 153**
An administrator has implemented a policy that passwords expire after 60 days and cannot match their last six previously used passwords. Users are bypassing this policy by immediately changing their passwords six times and then back to the original password. Which of the following can the administrator MOST easily employ to prevent this unsecure practice, with the least administrative effort?

A. Create a policy that passwords must be no less than ten characters.
B. Monitor user accounts and change passwords of users found to be doing this.
C. Create a policy that passwords cannot be changed more than once a day.
D. Monitor user accounts and lock user accounts that are changing passwords excessively.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 154**
Which of the following will provide the HIGHEST level of wireless network security?

A. WPA2
B. SSH
C. SSID
D. WEP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 155**
Which of the following is a requirement when implementing PKI if data loss is unacceptable?

A. Web of trust
B. Non-repudiation
C. Key escrow
D. Certificate revocation list

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 156**
Which of the following is an unauthorized wireless router that allows access to a secure network?

A. Interference
B. War driving
C. Evil twin
D. Rogue access point

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 157**
The server log shows 25 SSH login sessions per hour. However, it is a large company and the administrator does not know if this is normal behavior or if the network is under attack. Where should the administrator look to determine if this is normal behavior?

A. Change management
B. Code review

C. Baseline reporting
D. Security policy

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 158**
Which of the following cryptography types provides the same level of security but uses smaller key sizes and less computational resources than logarithms which are calculated against a finite field?

A. Elliptical curve
B. Diffie-Hellman
C. Quantum
D. El Gamal

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 159**
Two systems are being designed. System A has a high availability requirement. System B has a high security requirement with less emphasis on system uptime. Which of the following configurations BEST fits the need for each system?

A. System A fails open. System B fails closed.
B. System A and System B both fail closed.
C. System A and System B both fail open.
D. System A fails closed. System B fails open.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 160**
Which of the following MUST be implemented in conjunction with password history, to prevent a user from re-using the same password?

A. Maximum age time
B. Lockout time
C. Minimum age time
D. Expiration time

**Correct Answer:** C
**Section: (none)**

**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 161**
Which of the following protocols would be the MOST secure method to transfer files from a host machine?

A. SFTP

B. WEP
C. TFTP
D. FTP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 162**
A user receives an automated call which appears to be from their bank. The automated recording provides details about the bank's privacy policy, security policy and requests that the user clearly state their name, birthday and enter the banking details to validate the user's identity. Which of the following BEST describes this type of attack?

A. Phishing
B. Spoofing
C. Vishing
D. Pharming

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 163**
Which of the following software should a security administrator implement if several users are stating that they are receiving unwanted email containing advertisements?

A. Host-based firewalls
B. Anti-spyware
C. Anti-spam
D. Anti-virus

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 164**
Which of the following is a technique designed to obtain information from a specific person?

A. Smurf attack
B. Spear phishing
C. DNS poisoning

D. Pharming

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 165**
The BEST way to protect the confidentiality of sensitive data entered in a database table is to use:

A. hashing.
B. stored procedures.
C. encryption.
D. transaction logs.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 166**
Reviewing an access control list on a firewall reveals a Drop All statement at the end of the rules. Which of the following describes this form of access control?

A. Discretionary
B. Time of day restrictions
C. Implicit deny
D. Mandatory

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 167**
An employee stores their list of passwords in a spreadsheet on their local desktop hard drive. Which of the

following encryption types would protect this information from disclosure if lost or stolen?

A. Database
B. Removable media

C. File and folder level
D. Mobile device

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 168**
Which of the following is MOST commonly a part of routine system audits?

A. Job rotation
B. Business impact analysis
C. User rights and permissions reviews
D. Penetration testing

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 169**
Which of the following represents the complexity of a password policy which enforces lower case password using letters from 'a' through 'z' where 'n' is the password length?

A. n26
B. 2n * 26
C. 26n
D. n2 * 26

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 170**
In order to provide flexible working conditions, a company has decided to allow some employees remote access into corporate headquarters. Which of the following security technologies could be used to provide remote access? (Select TWO).

A. Subnetting

B. NAT
C. Firewall

D. NAC
E. VPN

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 171**
Which of the following is a form of photo identification used to gain access into a secure location?

A. Token
B. CAC
C. DAC
D. Biometrics

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 172**
Several staff members working in a datacenter have reported instances of tailgating. Which of the following could be implemented to prevent this security concern?

A. Proximity readers
B. Mantraps
C. Video surveillance
D. Biometric keypad

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 173**
By default, which of the following stops network traffic when the traffic is not identified in the firewall ruleset?

A. Access control lists
B. Explicit allow
C. Explicit deny
D. Implicit deny

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 174**
A security administrator is tasked with ensuring that all servers are highly available and that hard drive failure will not affect an individual server. Which of the following configurations will allow for high availability? (Select TWO).

A. Hardware RAID 5
B. Load sharing
C. Server clustering
D. Software RAID 1
E. Load balancing

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 175**
When granting access, which of the following protocols uses multiple-challenge responses for authentication, authorization and audit?

A. TACACS
B. TACACS+
C. LDAP
D. RADIUS

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 176**
Which of the following port numbers is used for SCP, by default?

A. 22
B. 69
C. 80
D. 443

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 177**
Which of the following devices is used to optimize and distribute data workloads across multiple computers or

networks?

A. Load balancer
B. URL filter
C. VPN concentrator
D. Protocol analyzer

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 178**
A business-critical application will be installed on an Internet facing server. Which of the following is the BEST security control that should be performed in conjunction with updating the application to the MOST current version?

A. The firewall should be configured to allow the application to auto-update.
B. The firewall should be configured to prevent the application from auto-updating.
C. A port scan should be run against the application's server.
D. Vendor-provided hardening documentation should be reviewed and applied.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 179**
Which of the following is a trusted OS implementation used to prevent malicious or suspicious code from executing on Linux and UNIX platforms?

A. SELinux
B. vmlinuz
C. System File Checker (SFC)
D. Tripwire

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 180**
Which of the following assists in identifying if a system was properly handled during transport?

A. Take a device system image
B. Review network traffic and logs
C. Track man hours and incident expense

D. Chain of custody

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 181**
Penetration testing should only be used during controlled conditions with express consent of the system owner because:

A. white box penetration testing cannot identify zero day exploits.
B. vulnerability scanners can cause massive network flooding during risk assessments.
C. penetration testing passively tests policy controls and can identify vulnerabilities.
D. penetration testing actively tests security controls and can cause system instability.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 182**
Which of the following risks may result from improper use of social networking and P2P software?

A. Shoulder surfing

B. Denial of service
C. Information disclosure
D. Data loss prevention

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 183**
Which of the following is true about PKI? (Select TWO).

A. When encrypting a message with the public key, only the public key can decrypt it.
B. When encrypting a message with the private key, only the private key can decrypt it.
C. When encrypting a message with the public key, only the CA can decrypt it.
D. When encrypting a message with the public key, only the private key can decrypt it.
E. When encrypting a message with the private key, only the public key can decrypt it.

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 184**
Users of specific systems are reporting that their data has been corrupted. After a recent patch update to those systems, the users are still reporting issues of data being corrupt. Which of the following assessment techniques need to be performed to identify the issue?

A. Hardware baseline review
B. Vulnerability scan
C. Data integrity check
D. Penetration testing

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 185**
A company has remote workers with laptops that house sensitive data. Which of the following can be implemented to recover the laptops if they are lost?

A. GPS tracking
B. Whole disk encryption
C. Remote sanitation
D. NIDS

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 186**
A company needs to reduce the risk of employees emailing confidential data outside of the company. Which of the following describes an applicable security control to mitigate this threat?

A. Install a network-based DLP device
B. Prevent the use of USB drives
C. Implement transport encryption
D. Configure the firewall to block port 110

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 187**
A visitor plugs their laptop into the network and receives a warning about their antivirus being out- of-date along with various patches that are missing. The visitor is unable to access the Internet or any network resources.

Which of the following is the MOST likely cause?

A. The IDS detected that the visitor's laptop did not have the right patches and updates so the IDS blocked access to the network.
B. The security posture is disabled on the network but remediation must take place before access is given to the visitor on that laptop.
C. The security posture is enabled on the network and remediation must take place before access is given to the visitor on that laptop.
D. The IPS detected that the visitor's laptop did not have the right patches and updates so it prevented its access to the network.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 188**
Upon investigation, an administrator finds a suspicious system-level kernel module which modifies file system operations. This is an example of which of the following?

A. Trojan
B. Virus
C. Logic bomb
D. Rootkit

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 189**
Which of the following is a best practice to identify fraud from an employee in a sensitive position?

A. Acceptable usage policy
B. Separation of duties
C. False positives
D. Mandatory vacations

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 190**
Which of the following is another name for a malicious attacker?

A. Black hat
B. White hat

C. Penetration tester

D. Fuzzer

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 191**
A security administrator is in charge of a datacenter, a hot site and a cold site. Due to a recent disaster, the administrator needs to ensure that their cold site is ready to go in case of a disaster. Which of the following does the administrator need to ensure is in place for a cold site?

A. Location with all required equipment loaded with all current patches and updates

B. Location with duplicate systems found in the datacenter

C. Location near the datacenter that meets power requirements

D. Location that meets power and connectivity requirements

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 192**
Which of the following is used when performing a qualitative risk analysis?

A. Exploit probability

B. Judgment

C. Threat frequency

D. Asset value

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 193**
A security administrator performs several war driving routes each month and recently has noticed a certain area with a large number of unauthorized devices. Which of the following attack types is MOST likely occurring?

A. Interference

B. Rogue access points

C. IV attack

D. Bluejacking

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 194**
A security administrator is setting up a corporate wireless network using WPA2 with CCMP but does not want to use PSK for authentication. Which of the following could be used to support 802.1x authentication?

A. LDAP
B. RADIUS
C. Kerberos
D. Smart card

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 195**
Which of the following is the MOST secure method of utilizing FTP?

A. FTP active
B. FTP passive
C. SCP
D. FTPS

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 196**
An administrator is taking an image of a server and converting it to a virtual instance. Which of the following BEST describes the information security requirements of a virtualized server?

A. Virtual servers require OS hardening but not patching or antivirus.
B. Virtual servers have the same information security requirements as physical servers.
C. Virtual servers inherit information security controls from the hypervisor.
D. Virtual servers only require data security controls and do not require licenses.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 197**
Webmail is classified under which of the following cloud-based technologies?

A. Demand Computing
B. Infrastructure as a Service (IaaS)
C. Software as a Service (SaaS)
D. Platform as a Service (PaaS)

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 198**
Based on logs from file servers, remote access systems, and IDS, a malicious insider was stealing data using a personal laptop while connected by VPN. The affected company wants access to the laptop to determine loss, but the insider's lawyer insists the laptop cannot be identified. Which of the following would BEST be used to identify the specific computer used by the insider?

A. IP address
B. User profiles
C. MAC address
D. Computer name

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 199**
A security administrator with full administrative rights on the network is forced to temporarily take time off of their duties. Which of the following describes this form of access control?

A. Separation of duties
B. Discretionary
C. Mandatory vacation
D. Least privilege

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 200**
A security engineer is troubleshooting a server in the DMZ, which cannot be reached from the Internet or the internal network. All other servers on the DMZ are able to communicate with this server. Which of the following is the MOST likely cause?

A. The server is configured to reject ICMP packets.
B. The server is on the external zone and it is configured for DNS only.

C. The server is missing the default gateway.
D. The server is on the internal zone and it is configured for DHCP only.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 201**
The recovery agent is used to recover the:

A. root certificate.
B. key in escrow.
C. public key.
D. private key.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 202**
Which of the following logical controls does a flood guard protect against?

A. Spanning tree
B. Xmas attacks
C. Botnet attack
D. SYN attacks

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 203**
Which of the following is a detective security control?

A. CCTV
B. Firewall
C. Design reviews
D. Bollards

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 204**
Which of the following ports would a security administrator block if the administrator wanted to stop users from accessing outside SMTP services?

A. 21
B. 25
C. 110
D. 143

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 205**
Which of the following is a method to prevent ad-hoc configuration mistakes?

A. Implement an auditing strategy
B. Implement an incident management strategy
C. Implement a patch management strategy
D. Implement a change management strategy

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 206**
Proper wireless antenna placement and radio power setting reduces the success of which of the following reconnaissance methods?

A. Rogue APs
B. War driving
C. Packet analysis
D. RF interference

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 207**
An IT administrator wants to provide 250 staff with secure remote access to the corporate network. Which of the following BEST achieves this requirement?

A. Software based firewall
B. Mandatory Access Control (MAC)

C. VPN concentrator
D. Web security gateway

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 208**
Applying detailed instructions to manage the flow of network traffic at the edge of the network, including allowing or denying traffic based on port, protocol, address, or direction is an implementation of which of the following?

A. Virtualization
B. Port security
C. IPSec
D. Firewall rules

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 209**
Which of the following is an example of allowing another user physical access to a secured area without validation of their credentials?

A. Evil twin
B. Tailgating
C. Impersonation
D. Shoulder surfing

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 210**
Which of the following identifies some of the running services on a system?

A. Determine open ports
B. Review baseline reporting
C. Review honeypot logs
D. Risk calculation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 211**
Which of the following protocols can be implemented to monitor network devices?

A. IPSec
B. FTPS
C. SFTP
D. SNMP

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 212**
Which of the following can cause hardware based drive encryption to see slower deployment?

A. A lack of management software
B. USB removable drive encryption
C. Role/rule-based access control
D. Multifactor authentication with smart cards

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 213**
Which of the following is the MOST secure way of storing keys or digital certificates used for decryption/ encryption of SSL sessions?

A. Database
B. HSM
C. Key escrow
D. Hard drive

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 214**
Which of the following should be reviewed periodically to ensure a server maintains the correct security configuration?

A. NIDS configuration

B. Firewall logs
C. User rights
D. Incident management

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 215**
Which of the following is MOST relevant to a buffer overflow attack?

A. Sequence numbers
B. Set flags
C. IV length
D. NOOP instructions

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 216**
A bulk update process fails and writes incorrect data throughout the database. Which of the following concepts describes what has been compromised?

A. Authenticity
B. Integrity
C. Availability
D. Confidentiality

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 217**
A network consists of various remote sites that connect back to two main locations. The security administrator needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

A. Block port 23 on the L2 switch at each remote site.
B. Block port 23 on the network firewall.
C. Block port 25 on the L2 switch at each remote site.
D. Block port 25 on the network firewall.

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 218**
Which of the following is a removable device that may be used to encrypt in a high availability clustered environment?

A. Cloud computer
B. HSM
C. Biometrics
D. TPM

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 219**
The company encryption policy requires all encryption algorithms used on the corporate network to have a key length of 128-bits. Which of the following algorithms would adhere to company policy?

A. DES
B. SHA
C. 3DES
D. AES

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 220**
Which of the following attacks is BEST described as the interruption of network traffic accompanied by the insertion of malicious code?

A. Spoofing
B. Man-in-the-middle
C. Spear phishing

D. DoS

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 221**

Which of the following may cause a user, connected to a NAC-enabled network, to not be prompted for credentials?

A. The user's PC is missing the authentication agent.
B. The user's PC is not fully patched.
C. The user's PC is not at the latest service pack.
D. The user's PC has out-of-date antivirus software.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 222**
Which of the following environmental variables reduces the potential for static discharges?

A. EMI
B. Temperature
C. UPS
D. Humidity

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 223**
A security administrator is tasked with revoking the access of a terminated employee. Which of the following account policies MUST be enacted to ensure the employee no longer has access to the network?

A. Account disablement
B. Account lockout

C. Password recovery
D. Password expiration

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 224**
Which of the following protocols would an administrator MOST likely use to monitor the parameters of network devices?

A. SNMP
B. NetBIOS
C. ICMP
D. SMTP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 225**
Which of the following is true about the CRL?

A. It should be kept public
B. It signs other keys
C. It must be kept secret
D. It must be encrypted

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 226**
When decommissioning old hard drives, which of the following is the FIRST thing a security engineer should do?

A. Perform bit level erasure or overwrite
B. Flash the hard drive firmware

C. Format the drive with NTFS
D. Use a waste disposal facility

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 227**
Recovery Point Objectives and Recovery Time Objectives directly relate to which of the following BCP concepts?

A. Succession planning
B. Remove single points of failure
C. Risk management
D. Business impact analysis

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 228**
A remote office is reporting they are unable to access any of the network resources from the main office. The security administrator realizes the error and corrects it. The administrator then tries to ping the router at the remote office and receives no reply; however, the technician is able to telnet to that router. Which of the following is the MOST likely cause of the security administrator being unable to ping the router?

A. The remote switch is turned off.
B. The remote router has ICMP blocked.
C. The remote router has IPSec blocked.
D. The main office's router has ICMP blocked.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 229**
Upper management decides which risk to mitigate based on cost. This is an example of:

A. qualitative risk assessment.
B. business impact analysis.
C. risk management framework.
D. quantitative risk assessment.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 230**
Which of the following would be implemented to allow access to services while segmenting access to the internal network?

A. IPSec
B. VPN
C. NAT
D. DMZ

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 231**
Which of the following authentication services would be used to authenticate users trying to access a network device?

A. SSH

B. SNMPv3

C. TACACS+

D. TELNET

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 232**
The security administrator wants to ensure messages traveling between point A and point B are encrypted and authenticated. Which of the following accomplishes this task?

A. MD5

B. RSA

C. Diffie-Hellman

D. Whole disk encryption

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 233**
Which of the following should be considered when trying to prevent somebody from capturing network traffic?

A. Video monitoring

B. Hot aisles

C. HVAC controls

D. EMI shielding

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 234**
Which of the following is the MAIN reason to require data labeling?

A. To ensure that staff understands what data they are handling and processing

B. To ensure that new viruses do not transfer to removable media

C. To ensure that all media sanitization requirements are met

D. To ensure that phishing attacks are identified and labeled properly

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 235**
Which of the following has a programmer MOST likely failed to consider if a user entering improper input is able to crash a program?

A. SDLM
B. CRC
C. Data formatting
D. Error handling

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 236**
Which of the following is the MOST efficient way to combat operating system vulnerabilities?

A. Anti-spam
B. Locking cabinets
C. Screen locks
D. Patch management

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 237**
Which of the following is the MOST likely cause of a single computer communicating with an unknown IRC server and scanning other systems on the network?

A. Worm
B. Spyware
C. Botnet
D. Rootkit

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 238**
Instead of giving a security administrator full administrative rights on the network, the administrator is given rights only to review logs and update security related network devices. Additional rights are handed out to

network administrators for the areas that fall within their job description. Which of the following describes this form of access control?

A. Mandatory vacation
B. Least privilege
C. Discretionary
D. Job rotation

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 239**
A security administrator is implementing a solution that encrypts an employee's newly purchased laptop but does not require the company to purchase additional hardware or software. Which of the following could be used to meet this requirement?

A. Mobile device encryption
B. HSM
C. TPM
D. USB encryption

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 240**
During incident response, which of the following procedures would identify evidence tampering by outside entities?

A. Hard drive hashing
B. Annualized loss expectancy
C. Developing audit logs
D. Tracking man hours and incident expenses

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 241**
A security administrator needs to separate two departments. Which of the following would the administrator implement to perform this?

A. Cloud computing
B. VLAN
C. Load balancer
D. MAC filtering

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 242**
When a certificate issuer is not recognized by a web browser, which of the following is the MOST common reason?

A. Lack of key escrow
B. Self-signed certificate
C. Weak certificate pass-phrase
D. Weak certificate cipher

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 243**
A security administrator wants to determine what data is allowed to be collected from users of the corporate Internet-facing web application. Which of the following should be referenced?

A. Privacy policy
B. Human Resources policy
C. Appropriate use policy
D. Security policy

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 244**
A security administrator wants to know which systems are more susceptible to an attack compared to other systems on the network. Which of the following assessment tools would be MOST effective?

A. Network design review
B. Vulnerability scanner
C. Baseline review
D. Port scanner

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 245**
A file has been encrypted with an employee's private key. When the employee leaves the company, their account is deleted. Which of the following are the MOST likely outcomes? (Select TWO).

A. Recreate the former employee's account to access the file.
B. Use the recovery agent to decrypt the file.
C. Use the root user account to access the file.
D. The data is not recoverable.
E. Decrypt the file with PKI.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 246**
A company needs to be able to prevent entry, at all times, to a highly sensitive area inside a public building. In order to ensure the BEST type of physical security, which of the following should be implemented?

A. Intercom system
B. Video surveillance
C. Nightly guards
D. Mantrap

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 247**

Which of the following is the default rule found in a corporate firewall's access control list?

A. Anti-spoofing
B. Permit all
C. Multicast list
D. Deny all

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 248**
Which of the following is a security control that is lost when using cloud computing?

A. Logical control of the data
B. Access to the application's administrative settings
C. Administrative access to the data
D. Physical control of the data

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 249**
A rogue access point with the same SSID as the production wireless network is found. Which of the following BEST describes this attack?

A. Evil twin
B. Vishing
C. War driving
D. Bluesnarfing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 250**
Which of the following should be installed to prevent employees from receiving unsolicited emails?

A. Pop-up blockers
B. Virus definitions
C. Spyware definitions
D. Spam filters

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 251**
Which of the following are the default ports for HTTP and HTTPS protocols? (Select TWO).

A. 21
B. 80
C. 135
D. 443

E. 445

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 252**
Which of the following would provide the MOST reliable proof that a datacenter was accessed at a certain time of day?

A. Video surveillance

B. Security log

C. Entry log

D. Proximity readers

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 253**
Which of the following describes the purpose of chain of custody as applied to forensic image retention?

A. To provide proof the evidence has not been tampered with or modified

B. To provide verification that the forensic examiner is qualified

C. To provide documentation as to who has handled the evidence

D. To provide a baseline reference

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 254**
Which of the following is a hardening step of an application during the SDLC?

A. Disabling unnecessary accounts

B. Application patch management schedule

C. Secure coding concepts

D. Disabling unnecessary services

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 255**
A security firm has been engaged to assess a software application. A production-like test environment, login details, production documentation and source code have been provided. Which of the following types of testing is being described?

A. White box
B. Gray box
C. Black box
D. Red teaming

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 256**
Which of the following should be performed on a computer to protect the operating system from malicious software? (Select TWO).

A. Disable unused services
B. Update NIDS signatures
C. Update HIPS signatures
D. Disable DEP settings
E. Install a perimeter firewall

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 257**
A critical system in the datacenter is not connected to a UPS. The security administrator has coordinated an authorized service interruption to resolve this issue. This is an example of which of the following?

A. Fault tolerance
B. Continuity of operations
C. Succession planning
D. Data handling error

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 258**
Which of the following is a management control type?

A. Vulnerability scanning
B. Least privilege implementation
C. Baseline configuration development
D. Session locks

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 259**
Which of the following is BEST used to prevent ARP poisoning attacks across a network?

A. VLAN segregation
B. IPSec
C. IP filters
D. Log analysis

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 260**
In order to ensure high availability of all critical servers, backups of the main datacenter are done in the middle of the night and then the backup tapes are taken to an offsite location. Which of the following would ensure the minimal amount of downtime in the case of a disaster?

A. Having the offsite location of tapes also be the standby server
B. Having the offsite location of tapes also be the warm site
C. Having the offsite location of tapes also be the cold site
D. Having the offsite location of tapes also be the hot site

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 261**
Which of the following malware types is MOST commonly installed through the use of thumb drives to compromise systems and provide unauthorized access?

A. Trojans
B. Botnets
C. Adware
D. Logic bomb

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 262**
The detection of a NOOP sled is an indication of which of the following attacks?

A. SQL injection
B. Buffer overflow
C. Cross-site scripting
D. Directory transversal

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 263**
Which of the following devices would allow a technician to view IP headers on a data packet?

A. NIDS
B. Protocol analyzer
C. VPN switch
D. Firewall

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 264**
A network administrator is implementing a network addressing scheme that uses a long string of both numbers and alphanumeric characters to create addressing options and avoid duplicates. Which of the following describes a protocol built for this purpose?

A. IPv6
B. ICMP
C. IGMP
D. IPv4

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 265**
Which of the following should a security administrator implement to prevent users from disrupting network connectivity, if a user connects both ends of a network cable to different switch ports?

"Pass Any Exam. Any Time." - 100% Pass Guarantee 4

A. VLAN separation
B. Access control
C. Loop protection
D. DMZ

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 266**
Which of the following is a trusted OS implementation used to prevent malicious or suspicious code from executing on Linux and UNIX platforms?

"Pass Any Exam. Any Time." - 100% Pass Guarantee 61

A. SELinux
B. vmlinuz
C. System File Checker (SFC)
D. Tripwire

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 267**
A network administrator is implementing a network addressing scheme that uses a long string of both numbers and alphanumeric characters to create addressing options and avoid duplicates. Which of the following describes a protocol built for this purpose?

A. IPv6
B. ICMP
C. IGMP
D. IPv4

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 268**
Which of the following is specific to a buffer overflow attack?

A. Memory addressing
B. Directory traversal
C. Initial vector
D. Session cookies

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 269**
Which of the following methods of access, authentication, and authorization is the MOST secure by default?

A. Kerberos
B. TACACS
C. RADIUS
D. LDAP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 270**
Actively monitoring data streams in search of malicious code or behavior is an example of:

A. load balancing.
B. an Internet proxy.
C. URL filtering.
D. content inspection.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation: