Microsoft JK0-015 Questions $ Answers

Number: JK0-015
Passing Score: 800
Time Limit: 120 min
File Version: 34.1

http://www.gratisexam.com/

Microsoft JK0-015 Questions $ Answers

Exam Name: CompTIA E2C Security+ (2008 Edition) Exam

Examsoon

QUESTION 1
Which of the following logical access control methods would a security administrator need to modify in order to control network traffic passing through a router to a different network?

A. Configuring VLAN 1
B. ACL
C. Logical tokens
D. Role-based access control changes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following tools limits external access to the network?

A. IDS
B. VLAN
C. Firewall
D. DMZ

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following tools was created for the primary purpose of reporting the services that are open for connection on a networked workstation?

A. Protocol analyzer
B. Port scanner
C. Password crackers
D. Vulnerability scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Upon opening the browser, a guest user is redirected to the company portal and asked to agree to the acceptable use policy. Which of the following is MOST likely causing this to appear?

A. NAT
B. NAC

C. VLAN
D. DMZ

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
USB devices with a virus delivery mechanism are an example of which of the following security threats?

A. Adware
B. Trojan
C. Botnets
D. Logic bombs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Cell phones with network access and the ability to store data files are susceptible to which of the following risks?

A. Input validation errors
B. SMTP open relays
C. Viruses

D. Logic bombs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest?

A. MD5
B. SHA-1

C. LANMAN
D. NTLM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following technologies is used to verily that a file was not altered?

A. RC5
B. AES
C. DES
D. MD5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following uses an RC4 key that can be discovered by eavesdropping on plain text initialization vectors?

A. WEP
B. TKIP
C. SSH
D. WPA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
A user reports that each time they attempt to go to a legitimate website, they are sent to an inappropriate website. The security administrator suspects the user may have malware on the computer, which manipulated some of the user's files. Which of the following files on the user's system would need to be checked for unauthorized changes?

A. SAM
B. LMhosts
C. Services
D. Hosts

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
The security administrator needs to make a change in the network to accommodate a new remote location. The new location will be connected by a serial interface, off the main router, through a commercial circuit. This remote site will also have traffic completely separated from all other traffic. Which of the following design elements will need to be implemented to accommodate the new location?

A. VLANs need to be added on the switch but not the router.
B. The NAT needs to be re-configured to allow the remote location.
C. The current IP scheme needs to be subnetted.
D. The switch needs to be virtualized and a new DMZ needs to be created

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Mitigating security risks by updating and applying hot fixes is part of:

A. patch management.
B. vulnerability scanning.
C. baseline reporting.
D. penetration testing.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is the MAIN difference between a hotfix and a patch?

A. Hotfixes follow a predetermined release schedule while patches do not.
B. Hotfixes are smaller than patches.
C. Hotfixes may be released at anytime and will later be included in a patch.
D. Patches can only be applied after obtaining proper approval, while hotfixes do not need management approval

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A vulnerability assessment was conducted against a network. One of the findings indicated an out-dated version of software. This is an example of weak:

A. security policies.
B. patch management.
C. acceptable use policies.
D. configuration baselines.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following tools can execute a ping sweep?

A. Protocol analyzer
B. Anti-virus scanner
C. Network mapper
D. Password cracker

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following is a newer version of SSL?

A. SSH
B. IPSec
C. TLS
D. L2TP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
A technician visits a customer site which prohibits portable data storage devices. Which of the following items would be prohibited? (Select TWO).

A. USB Memory key

B. Bluetooth-enabled cellular phones
C. Wireless network detectors
D. Key card

E. Items containing RFID chips

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Exploitation of security vulnerabilities is used during assessments when which of the following is true?

A. Security testers have clear and written authorization to conduct vulnerability scans.
B. Security testers are trying to document vulnerabilities without impacting network operations.
C. Network users have permissions allowing access to network devices with security weaknesses.
D. Security testers have clear and written authorization to conduct penetration testing.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following should a technician deploy to detect malicious changes to the system and configuration?

A. Pop-up blocker
B. File integrity checker
C. Anti-spyware
D. Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
In order to prevent data loss in case of a disk error which of the following options would an administrator MOST

likely deploy?

A. Redundant connections
B. RAID
C. Disk striping
D. Redundant power supplies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A technician has installed security software; shortly thereafter the response time slows considerably. Which of the following can be used to determine the effect of the new software?

A. Event logs
B. System monitor
C. Performance monitor
D. Protocol analyzer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
After installing database software the administrator must manually change the default administrative password, remove a default database, and adjust permissions on specific files. These actions are BEST described as:

A. vulnerability assessment.
B. mandatory access control.
C. application hardening.
D. least privilege

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following is the BEST mitigation method to implement when protecting against a discovered OS exploit?

A. NIDS
B. Patch
C. Antivirus update

D. HIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following is the primary concern of governments in terms of data security?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following is BEST used to change common settings for a large number of deployed computers?

A. Group policies
B. Hotfixes
C. Configuration baselines
D. Security templates

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following solutions would a company be MOST likely to choose if they wanted to conserve rack space in the data center and also be able to manage various resources on the servers?

A. Install a manageable, centralized power and cooling system
B. Server virtualization
C. Different virtual machines on a local workstation
D. Centralize all blade servers and chassis within one or two racks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28

A rogue wireless network is showing up in the IT department. The network appears to be coming from a printer that was installed. Which of the following should have taken place, prior to this printer being installed, to prevent this issue?

A. Installation of Internet content filters to implement domain name kiting.
B. Penetration test of the network to determine any further rogue wireless networks in the area.
C. Conduct a security review of the new hardware to determine any possible security risks.
D. Implement a RADIUS server to authenticate all users to the wireless network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following characteristics distinguishes a virus from a rootkit, spyware, and adware?

A. Eavesdropping
B. Process hiding
C. Self-replication
D. Popup displays

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following is used to generate keys in PKI?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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:

QUESTION 32
When used to encrypt transmissions, which of the following is the MOST resistant to brute force attacks?

A. SHA
B. MD5
C. 3DES
D. AES256

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
A user visits their normal banking website. The URL is correct and the website is displayed in the browser, but the user gets an SSL warning that the SSL certificate is invalid as it is signed by an unknown authority. Which of the following has occurred?

A. Domain name kiting
B. Privilege escalation
C. Replay attack
D. Man-in-the-middle attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A technician reviews the system log entries for an internal DNS server. Which of the following entries MOST warrants further investigation?

A. DNS query from a source outside the organization
B. DNS query from a source inside the organization
C. Zone transfer to a source inside the organization
D. Zone transfer to a source outside the organization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Monitoring a computer's logs and critical files is part of the functionality of a

A. NIPS.
B. HIDS.

C. firewall.
D. honeypot.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Continuously documenting state and location of hardware from collection to disposition during a forensic investigation is known as:

A. risk mitigation.
B. data handling.
C. chain of custody.
D. incident response.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following is an example of two factor authentication?

A. PIN and password
B. Smartcard and token
C. Smartcard and PIN
D. Fingerprint and retina scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following uses a three-way-handshake for authentication and is commonly used in PPP connections?

A. MD5
B. CHAP

C. Kerberos
D. SLIP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following transmission types would an attacker most likely use to try to capture data packets?

A. Shielded twisted pair
B. Fiberoptic
C. Bluesnarfing
D. Wireless

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following describes a port that is left open in order to facilitate access at a later date?

A. Honeypot
B. Proxy server
C. Open relay
D. Backdoor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following is often bundled with freely downloaded software?

A. Cookies
B. Logic bomb
C. Adware
D. Spam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
An administrator believes a user is secretly transferring company information over the Internet. The network logs do not show any non-standard traffic going through the firewall. Which of the following tools would allow the administrator to better evaluate the contents of the network traffic?

A. Vulnerability scanner
B. Network anomaly detection
C. Protocol analyzer
D. Proxy server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A company has just recovered from a major disaster. Which of the following should signify the completion of a disaster recovery?

A. Verify all servers are back online and working properly.
B. Update the disaster recovery plan based on lessons learned.
C. Conduct post disaster recovery testing.
D. Verify all network nodes are back online and working properly.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A user tries to plug their laptop into the company's network and receives a warning that their patches and virus definitions are out-of-date. This is an example of which of the following mitigation techniques?

A. NAT
B. Honeypot
C. NAC
D. Subnetting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
A file has been compromised with corrupt data and might have additional information embedded within it. Which of the following actions should a security administrator follow in order to ensure data integrity of the file on that host?

A. Disable the wireless network and copy the data to the next available USB drive to protect the data

B. Perform proper forensics on the file with documentation along the way.
C. Begin chain of custody for the document and disallow access.
D. Run vulnerability scanners and print all reports of all diagnostic results.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
To ensure users are logging into their systems using a least privilege method, which of the following should be done?

A. Create a user account without administrator privileges.
B. Employ a BIOS password that differs from the domain password.
C. Enforce a group policy with the least amount of account restrictions.
D. Allow users to determine their needs and access to resources.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A recent security audit shows an organization has been infiltrated with a former administrator's credentials. Which of the following would be the BEST way to mitigate the risk of this vulnerability?

A. Conduct periodic audits of disaster recovery policies.
B. Conduct periodic audits of password policies.
C. Conduct periodic audits of user access and rights.
D. Conduct periodic audits of storage and retention policies.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A security administrator is analyzing the packet capture from an IDS triggered filter. The packet capture shows the following string:

<scrip>source=http://www.evilsite.jp/evil.js</script>

Which of the following attacks is occurring?

A. SQL injection
B. Redirection attack
C. Cross-site scripting
D. XLM injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
A user wants to edit a file that they currently have read-only rights to; however, they are unable to provide a business justification, so the request is denied. This is the principle of:

A. separation of duties.
B. job-based access control
C. least privilege.
D. remote access policy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following concepts addresses the threat of data being modified without authorization?

A. Integrity
B. Key management
C. Availability
D. Non-repudiation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
An attacker sends packets to a host in hopes of altering the host's MAC table. Which of the following is the attacker attempting to do?

A. Port scan
B. Privilege escalation
C. DNS spoofing

D. ARP poisoning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following is a best practice for organizing users when implementing a least privilege model?

A. By function
B. By department
C. By geographic location
D. By management level

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following describes how long email messages are available in case of a subpoena?

A. Backup procedures
B. Retention policy
C. Backup policy
D. Email server configuration

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Management would like to know if anyone is attempting to access files on the company file server. Which of the following could be deployed to BEST provide this information?

A. Software firewall
B. Hardware firewall
C. HIDS
D. NIDS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following is the correct risk assessment equation?

A. Risk = exploit x number of systems x cost of asset
B. Risk = infections x number of days infected x cost of asset
C. Risk = threat x vulnerability x cost of asset
D. Risk = vulnerability x days unpatched x cost of asset

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following is of the GREATEST concern in regard to a rogue access point?

A. Rogue access points are hard to find and remove from the network.
B. Rogue access points can scan the company's wireless networks and find other unencrypted and rouge access points
C. The radio signal of the rogue access point interferes with company approved access points.
D. Rogue access points can allow unauthorized users access the company's internal networks.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
The process of validating a user's claimed identity is called

A. identification.
B. authorization.
C. validation.
D. repudiation.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following is a benefit of utilizing virtualization technology?

A. Lowered cost of the host machine
B. Less overhead cost of software licensing
C. Streamline systems to a single OS
D. Fewer systems to monitor physical access

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
The security administrator wants to increase the cipher strength of the company's internal root certificate.

Which of the following would the security administer use to sign a stronger root certificate?

A. Certificate authority
B. Registration authority
C. Key escrow
D. Trusted platform module

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following describes a semi-operational site that in the event of a disaster, IT operations can be migrated?

A. Hot site
B. Warm site
C. Mobile site
D. Cold site

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following devices hooks into a LAN and captures traffic?

A. Protocol analyzer
B. Protocol filter
C. Penetration testing tool
D. Vulnerability assessment tool

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
When assessing a network containing resources that require near 100% availability, which of the following techniques should be employed to assess overall security?

A. Penetration testing

B. Vulnerability scanning
C. User interviews
D. Documentation reviews

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following would MOST likely contain a <SCRIPT> tag?

A. Cookies
B. XSS
C. DOS
D. Buffer overflow

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which of the following is a reason why wireless access points should not be placed near a building's perimeter?

A. Rouge access points
B. Vampire taps
C. Port scanning
D. War driving

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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:

QUESTION 66
Which of the following tools BEST identifies the method an attacker used after they have entered into a network?

A. Input validation
B. NIDS
C. Port scanner
D. HIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following is a major risk associated with cloud computing?

A. Loss of physical control over data
B. Increased complexity of qualitative risk assessments
C. Smaller attack surface
D. Data labeling challenges

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which of the following is MOST likely the reason why a security administrator would run a Nessus report on an important server?

A. To analyze packets and frames
B. To report on the performance of the system
C. To scan for vulnerabilities
D. To enumerate and crack weak system passwords

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which of the following BEST describes how the mandatory access control (MAC) method works?

A. It is an access policy based on a set of rules.

B. It is an access policy based on the role that the user has in an organization.
C. It is an access policy based on biometric technologies.

D. It is an access policy that restricts access to objects based on security clearance.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Using a smartcard and a physical token is considered how many factors of authentication?

A. One
B. Two
C. Three
D. Four

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following protocols is considered more secure than SSL?

A. TLS
B. WEP
C. HTTP
D. Telnet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A NIDS monitoring traffic on the public-side of a firewall provides which of the following?

A. Faster alerting to internal compromises
B. Intelligence about external threats
C. Protection of the external firewall interface
D. Prevention of malicious traffic

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following is an important part of disaster recovery training?

A. Schemes
B. Storage locations
C. Chain of custody
D. Table top exercises

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following would a network administrator implement to control traffic being routed between networks or network segments in an effort to preserve data confidentiality?

A. NAT
B. Group policies
C. Password policies
D. ACLs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
The security administrator wants each user to individually decrypt a message but allow anybody to encrypt it. Which of the following MUST be implemented to allow this type of authorization?

A. Use of digital certificates
B. Use of public keys only
C. Use of private keys only
D. Use of public and private keys

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A security administrator is analyzing the packet capture from an IDS triggered filter. The packet capture shows the following string:

a or1 ==1--

Which of the following attacks is occurring?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following has been implemented if several unsuccessful login attempts were made in a short period of time denying access to the user account, and after two hours the account becomes active?

A. Account lockout
B. Password expiration
C. Password disablement
D. Screen lock

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
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:

QUESTION 79
In the event of a disaster, in which the main datacenter is immediately shutdown, which of the following would a company MOST likely use with a minimum Recovery Time Objective?

A. Fault tolerance
B. Hot site
C. Cold site
D. Tape backup restoration

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 80
Which of the following methods involves placing plain text data within a picture or document?

A. Steganography
B. Digital signature
C. Transport encryption
D. Stream cipher

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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:

QUESTION 82
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following is a reason to implement Kerberos over local system authentication?

A. Authentication to multiple devices

B. Centralized file integrity protection
C. Non-repudiation
D. Greater password complexity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following should a security administrator implement to ensure there are no security holes in the OS?

A. Encryption protocols
B. Firewall definitions
C. Patch management
D. Virus definitions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following cipher types is used by AES?

A. Block
B. Fourier
C. Stream
D. Turing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following control systems is used to maintain proper environmental conditions in a datacenter?

A. HVAC
B. Bollards
C. CCTV
D. Mantrap

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
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:

QUESTION 89
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
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:

QUESTION 91
Which of the following is a reason to use TACACS+ over RADIUS?

A. Combines authentication and authorization
B. Encryption of all data between client and server
C. TACACS+ uses the UDP protocol
D. TACACS+ has less attribute-value pairs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A customer has called a company to report that all of their computers are displaying a rival company's website when the user types the correct URL into the browser. All of the other websites the user visits work correctly and other customers are not having this issue. Which of the following has MOST likely occurred?

A. The website company has a misconfigured firewall.
B. The customer has a virus outbreak.
C. The customer's DNS has been poisoned.
D. The company's website has been attacked by the rival company

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
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:

QUESTION 94
Which of the following describes an attack technique by which an intruder gains physical access by following an authorized user into a facility before the door is closed?

A. Shoulder surfing
B. Tailgating
C. Escalation
D. Impersonation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following is true when a user browsing to an HTTPS site receives the message: a Site name mismatch'?

A. The certificate CN is different from the site DNS A record.
B. The CA DNS name is different from the root certificate CN.
C. The certificate was issued by the intermediate CA and not by the root CA.
D. The certificate file name is different from the certificate CN.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which of the following will contain a list of unassigned public IP addresses?

A. TCP port
B. 802.1x
C. Loop protector
D. Firewall rule

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
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:

QUESTION 99
Which of the following access control methods provides the BEST protection against attackers logging on as authorized users?

A. Require a PIV card
B. Utilize time of day restrictions
C. Implement implicit deny
D. Utilize separation of duties

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Several PCs are running extremely slow all of a sudden. Users of the PCs report that they do a lot of web browsing and explain that a disgruntled employee from their department was recently fired. The security administrator observes that all of the PCs are attempting to open a large number of connections to the same destination. Which of the following is MOST likely the issue?

A. A logic bomb has been installed by the former employee
B. A man-in-the-middle attack is taking place.
C. The PCs have downloaded adware.
D. The PCs are being used in a botnet

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
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:

QUESTION 102
In the event of a disaster resulting in the loss of their data center, a company had determined that they will need to be able to be back online within an hour or two, with all systems being fully up to date. Which of the following would BEST meet their needs?

A. Off-site storage of backup tapes
B. A hot backup site
C. A cold backup site
D. A warm backup site

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Which of the following has a programmer MOST likely failed to consider if a user entering improper input is able to compromise the integrity of data?

A. SDLM
B. Error handling
C. Data formatting
D. Input validation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Which of the following provides EMI protection?

A. STP
B. UTP
C. Grounding
D. Anti-static wrist straps

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
A user reports that a web browser stopped working after it was updated. Which of the following BEST describes a probable cause of failure?

A. The browser was previously compromised and corrupted during the update.
B. Anti-spyware is preventing the browser from accessing the network.
C. A faulty antivirus signature has identified the browser as malware.
D. A network based firewall is blocking the browser as it has been modified.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Which of the following devices is MOST likely to be installed to prevent malicious attacks?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
Which of the following protocols uses UDP port 69 by default?

A. Kerberos
B. TFTP
C. SSH
D. DNS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Which of the following would a security administrator use to diagnose network issues?

A. Proxy
B. Host-based firewall
C. Protocol analyzer
D. Gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
A user wishes to encrypt only certain files and folders within a partition. Which of the following methods should a technician recommend?

A. EFS
B. Partition encryption
C. Full disk
D. BitLocker

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
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:

QUESTION 112
Which of the following characteristics distinguishes a virus from a rootkit, spyware, and adware?

A. Eavesdropping
B. Process hiding
C. Self-replication
D. Popup displays

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
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:

QUESTION 114
Which of the following forensic artifacts is MOST volatile?

A. CD-ROM
B. Filesystem
C. Random access memory
D. Network topology

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
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:

QUESTION 116
Risk can be managed in the following ways EXCEPT:

A. mitigation.
B. acceptance.
C. elimination.
D. transference.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
A security administrator needs to implement a wireless system that will only be available within a building. Which of the following configurations can the administrator modify to achieve this? (Select TWO).

A. Proper AP placement
B. Disable SSID broadcasting
C. Use CCMP
D. Enable MAC filtering
E. Reduce the power levels

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
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:

QUESTION 119
A user reports that the spreadsheet they use for the department will not open. The spreadsheet is located on a server that was recently patched. Which of the following logs would the technician review FIRST?

A. Access
B. Firewall
C. Antivirus
D. DNS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Which of the following helps prevent a system from being fingerprinted?

A. Personal firewall
B. Complex passwords
C. Anti-spam software
D. OS patching

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
An attacker captures valid wireless traffic in hopes of transmitting it repeatedly to generate enough traffic to discover the encryption key. Which of the following is the attacker MOST likely using?

A. War driving
B. Replay attack
C. Bluejacking
D. DNS poisoning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Which of the following is an authentication method that uses symmetric key encryption and a key distribution center?

A. MS-CHAP
B. Kerberos
C. 802.1x
D. EAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which of the following is a preventative physical security measure?

A. Video surveillance
B. External lighting
C. Physical access log
D. Access control system

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
An employee keeps getting pop-ups from a program on their computer stating it blocked an attacking IP address. Which of the following security applications BEST explains this behavior?

A. Antivirus
B. Anti-spam
C. Personal firewall
D. Pop-up blocker

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
A Maintenance Manager requests that a new group be created for a new development project, concerning

power distribution, in order to email and setup conference meetings to the whole project team. Which of the following group types would need to be created?

A. Default power users
B. Restricted group
C. Distribution
D. Security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Which of the following is an example of data obfuscation within a data stream?

A. Cryptography
B. Steganography
C. Hashing
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Which of the following concepts is applied FIRST when a user logs into a domain?

A. Virealization
B. Non-repudiation
C. Authorization
D. Identification

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
Which of the following tools will allow a technician to detect devices and associated IP addresses on the network?

A. Network intrusion detection software
B. Network mapping software
C. Port scanner
D. Protocol analyzers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
Which of the following attacks involves sending unsolicited contact information to Bluetooth devices configured in discover mode?

A. Impersonation
B. Bluejacking
C. War driving
D. Bluesnarfing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
Which of the following has the capability to perform onboard cryptographic functions?

A. Smartcard
B. ACL
C. RFID badge
D. Proximity badge

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Shielded communications media is MOST often used to prevent electrical emanations from being detected and crosstalk between which of the following?

A. Networks
B. Cables
C. VLANs
D. VPNs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Which of the following measures ensures unauthorized users cannot access a WAP in a user's home?

A. Proper WAP placement
B. Turn off the computers when not in use
C. Set the SSID to hidden
D. Change the administrator password on the computer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
Which of the following BEST describes where L2TP is used?

A. VPN encryption
B. Authenticate users using CHAP
C. Default gateway encryption
D. Border gateway protocol encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
The president of the company is trying to get to their bank's website, and the browser is displaying that the webpage is being blocked by the system administrator. Which of the following logs would the technician review?

A. DNS
B. Performance
C. System
D. Content filter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
Which of the following should a technician run to find user accounts that can be easily compromised?

A. NMAP
B. SNORT
C. John the Ripper

D. Nessus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
Which of the following defines the role of a root certificate authority (CA) in PKI?

A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
B. The CA stores the user's hash value for safekeeping.
C. The CA is the trusted root that issues certificates.
D. The root CA is used to encrypt email messages to prevent unintended disclosure of data

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Which of the following malicious programs compromises system security by exploiting system access through a virtual backdoor?

A. Virus
B. Trojan
C. Spam
D. Adware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
Which of the following BEST represents why a system administrator should download security patches from the manufacturer's website directly?

A. Maintain configuration baseline
B. Implement OS hardening
C. Ensure integrity of the patch
D. Ensure patches are up-to-date

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
While responding to a confirmed breach of the organization's web server, the security administrator determines the source of the attack was from a rival organization's IP address range. Which of the following should the security administer do with this information?

A. Notify the Help Desk
B. Notify ICANN
C. Notify management
D. Notify the rival organization's IT department

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
The BEST location for a spam filter is

A. on the local LAN.
B. on a proxy server.
C. behind the firewall.
D. in front of the mail relay server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Biometrics is an example of which of the following type of user authentication?

A. Something the user is
B. Something the user has
C. Something the user does
D. Something the user knows

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Which of the following contains a database of users and passwords used for authentication?

A. CHAP
B. SAM

C. TPM
D. DNS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Mandatory Access Control (MAC) allows:

A. access rights indicated by the role of the individual
B. access associated with the classification of data.
C. a system administrator to centralize policy.
D. rights to be assigned by the data owner.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
The accounting group, clinical group and operations group only have access to their own applications. The company often needs auditors to have access to all three groups' applications with little notice. Which of the following would simplify the process of granting auditors permissions to all the applications?

A. Create an auditors group and merge the members of the accounting, clinical and operations groups.
B. Create an auditors group and add each user to the accounting, clinical and operations groups individually.
C. Create an auditors group and add each of the accounting, clinical and operations groups to the auditors group

D. Create an auditors group and add the group to each of the accounting, clinical and operations groups.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
Which of the following solutions would an administrator MOST likely perform in order to keep up-to-date with various fixes on different applications?

A. Service pack installation
B. Patch management
C. Different security templates
D. Browser hotfixes

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 146
Attackers may be able to remotely destroy critical equipment in the datacenter by gaining control over which of the following systems?

A. Physical access control
B. Video surveillance
C. HVAC
D. Packet sniffer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
Which of the following situations applies to disaster recovery exercises?

A. Vulnerability scans should be performed after each exercise.
B. Separation of duties should be implemented after each exercise.
C. Passwords should be changed after each exercise.
D. Procedures should be updated after each exercise.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
The administrator needs to require all users to use complex passwords. Which of the following would be the BEST way to do this?

A. Set a local password policy on each workstation and server
B. Set a domain password policy
C. Set a group policy to force password changes
D. Post a memo detailing the requirement of the new password complexity requirements

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
Purchasing insurance on critical equipment is an example of which of the following types of risk mitigation techniques?

A. Risk avoidance
B. Risk transfer
C. Risk retention
D. Risk reduction

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
Which of the following would be used to eliminate the need for an administrator to manually configure passwords on each network device in a large LAN?

A. RADIUS
B. OVAL
C. RAS
D. IPSec VPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
A security administrator responds to a report of a web server that has been compromised. The security administrator observes the background has been changed to an image of an attacker group. Which of the following would be the FIRST step in the incident response process?

A. Run an antivirus scan
B. Disable the network connection

C. Power down the server
D. Print a copy of the background

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
After completing a forensic image of a hard drive, which of the following can be used to confirm data integrity?

A. Chain of custody
B. Image compression
C. AES256 encryption
D. SHA512 hash

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
A security administrator wants to prevent corporate users from being infected with viruses from flash based advertisements while using web browsers at work. Which of the following could be used to mitigate this threat?

A. Content filter
B. Firewall
C. IDS
D. Protocol analyzer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
Which of the following tools provides the MOST comprehensive view of the network's security?

A. Vulnerability assessment
B. Network anomaly detection
C. Penetration test
D. Network mapping program

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
Which of the following practices improves forensic analysis of logs?

A. Ensuring encryption is deployed to critical systems.
B. Ensuring SNMP is enabled on all systems.
C. Ensuring switches have a strong management password.
D. Ensuring the proper time is set on all systems.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
A user is concerned about threats regarding social engineering and has asked the IT department for advice. One suggestion offered might be to:

A. install a removable data backup device for portability ease.
B. verily the integrity of all data that is accessed across the network.
C. ensure that passwords are not named after relatives.
D. disallow all port 80 inbound connection attempts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
When disposing of old or damaged computer systems, which of the following is the primary security concern?

A. Integrity of company HR information
B. Compliance with industry best practices
C. Confidentiality of proprietary information
D. Adherence to local legal regulations

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
Which of the following is performed during a security assessment?

A. Remediate the machines with incorrectly configured controls.
B. Quarantine the machines that have no controls in place.
C. Calculate the cost of bringing the controls back into compliance.
D. Determine the extent to which controls are implemented correctly

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
The root certificate for the CA for a branch in a city was generated by the CA in a city in another country. Which of the following BEST describes this trust model?

A. Chain of trust
B. Linear trust
C. Hierarchical trust
D. Web of trust

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
The security administrator needs to determine whether common words and phrases are being used as passwords on the company server. Which of the following attacks would MOST easily accomplish this task?

A. NTLM hashing
B. Dictionary
C. Brute force
D. Encyclopedia

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
Conducting periodic user rights audits can help an administrator identity:

A. new user accounts that have been created.
B. users who are concurrently logged in under different accounts.
C. unauthorized network services.
D. users who can view confidential information.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
Which of the following has a 128-bit message digest?

A. NTLM

B. MD5
C. SHA
D. 3DES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Which of the following BEST describes a security benefit of a virtualization farm?

A. Increased anomaly detection
B. Stronger authentication

C. Stronger encryption
D. Increased availability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
The company president wants to replace usernames and passwords with USB security tokens for company systems. Which of the following authentication models would be in use?

A. Two factor
B. Form factor
C. Physical factor
D. Single factor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
A security administrator wants to detect and prevent attacks at the network perimeter. Which of the following security devices should be installed to address this concern?

A. NIPS
B. IDS
C. HIPS
D. NDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
Which of the following presents the GREATEST security risk to confidentiality of proprietary corporate data when attackers have physical access to the datacenter?

A. Solid state drives
B. Cell phone cameras
C. USB drives
D. NAS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
Which of the following allows a systems administrator to regain lost keys within a PKI?

A. Recovery agent
B. One time pad
C. CRL
D. Asymmetric keys

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
A vulnerable service is required between two systems on a network. Which of the following should an administrator use to prevent an attack on that service from outside the network?

A. Proxy server
B. NIDS
C. Firewall
D. HIDS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
A technician needs to validate that a sent file has not been modified in any way. A co-worker recommends that a thumbprint be taken before the file is sent. Which of the following should be done?

A. Take an AES hash of the file and send the receiver both the hash and the original file in a signed and encrypted email.

B. Take a MD5 hash of the file and send the receiver both the hash and the original file in a signed and encrypted email.
C. Take a NTLM hash of the file and send the receiver both the hash and the original file in a signed and encrypted email.
D. Take a LANMAN hash of the file and send the receiver both the hash and the original file in a signed and encrypted email.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170

A technician needs to setup a secure room to enable a private VTC system. Which of the following should be installed to prevent devices from listening to the VTC?

A. Shielding
B. HIDS
C. HVAC
D. MD5 hashing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
Which of the following is a primary effect of allowing P2P connections on a network?

A. Increased amount of spam
B. Input validation on web applications
C. Possible storage of illegal materials
D. Tracking cookies on the website

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
Which of the following services should be turned off on a printer to prevent malicious reconnaissance attempts?

A. FTP
B. Spooler
C. SNMP
D. IP printing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
Environmental monitoring includes which of the following? (Select TWO]

A. EMI shielding
B. Redundancy
C. Video monitoring
D. Humidity controls
E. Load balancing

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
Which of the following is the security concept that describes a user who only has enough access to complete their work?

A. Least privilege
B. Single sign-on
C. Explicit allow
D. Implicit deny

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
A security administrator wants to ensure that only authorized personnel are able to gain entry into a secure area. There is currently no physical security other than a badge reader. Which of the following would MOST likely be installed to regulate right of entry?

A. Security alarms
B. Video surveillance
C. Access list
D. Proximity readers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
Which of the following can be a risk of consolidating servers onto a single virtual host?

A. Data emanation
B. Non-repudiation
C. Environmental control
D. Availability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
Which of the following is a security best practice that allows a user to have one ID and password for all

systems?

A. SSO
B. PIV
C. Trusted OS
D. Token

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
An administrator is explaining the conditions under which penetration testing is preferred over vulnerability testing. Which of the following statements correctly describes these advantages?

A. Identifies surface vulnerabilities and can be run on a regular basis
B. Proves that the system can be compromised
C. Safe for even inexperienced testers to conduct
D. Can be fairly fast depending on number of hosts

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
An employee is not able to receive email from a specific user at a different organization; however, they can receive emails from other users. Which of the following would the administrator MOST likely check to resolve the user's issue?

A. Browser pop-up settings
B. Spam folder settings
C. User local antivirus settings

D. The local firewall settings

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
Which of the following encryption schemes can be configured as the LEAST secure?

A. RC4
B. Twofish
C. 3DES
D. DES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
Which of the following security precautions needs to be implemented when securing a wireless network? (Select THREE)

A. Enable data encryption on all wireless transmissions using WPA2.
B. Enable the lowest power setting necessary to broadcast to the targeted range.
C. Enable the highest power setting possible to make sure the broadcast reaches the targeted range.
D. Enable data encryption on all wireless transmissions using WEP.
E. Authentication should take place using a pre-shared key (PSK) of no more than six characters.
F. Enable the ability to verily credentials on an authentication server.

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
Which of the following is reversible when encrypting data?

A. A private key
B. A public key
C. A hashing algorithm
D. A symmetric key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
Which of the following can be exploited for session hijacking while accessing the Internet?

A. P2P
B. Browser history
C. Cookies
D. SQL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
A large amount of continuous small transmissions are originating from multiple external hosts to the corporate web server, which is also inaccessible to users. Which of the following attacks is MOST likely the cause?

A. Spoofing
B. DNS poisoning
C. DDoS
D. DoS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
Which of the following asymmetric algorithms was designed to provide both encryption and digital signatures?

A. Diffie-Hellman
B. DSA
C. SHA
D. RSA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
Which of the following can cause data leakage from web based applications?

A. Device encryption
B. Poor error handling
C. Application hardening
D. XML

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
Which of the following describes a design element that requires unknown computers connecting to the corporate network to be automatically part of a specific VLAN until certain company requirements are met?

A. RAS
B. NAC
C. NAT

D. RADIUS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
The benefit of using software whole disk encryption is:

A. the data can be retrieved easier if the disk is damaged
B. the disk's MBR is encrypted as well.
C. unauthorized disk access is logged in a separate bit.
D. the entire file system is encrypted in case of theft.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
Which of the following organizational disaster recovery types would provide a building and network equipment but not current application data?

A. Warm site
B. Field site
C. Cold site
D. Hot site

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
Which of the following best practices would a security administrator implement in order to prevent one user from having too many administrative rights?

A. Complex passwords
B. Least privilege
C. Job rotation
D. System accounts with minimal rights

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
An administrator is providing management with a mobile device that allows email access. The mobile device will be password protected in case of loss. Which of the following additional security measures should the administrator ensure is in place?

A. The mobile device should erase itself after a set number of invalid password attempts.
B. The password should be alpha-numeric only, due to keypad limitations.
C. The password should be common so that the mobile device can be re-assigned.
D. The mobile device should use and be equipped with removal storage for sensitive data retrieval.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
Which of the following BEST identifies the sensitivity of a document?

A. Metadata
B. Information classification
C. Risk transference
D. Access control list

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
Which of the following alternate site types is the MOST affordable after implementation?

A. Cold site
B. Off site
C. Hot site
D. Warm site

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
Which of the following can use a trust system where public keys are stored in an online directory?

A. DES
B. AES
C. PGP

D. WEP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
Which of the following elements has the ability to hide a node's internal address from the public network?

A. NAT
B. NAC
C. NDS
D. VLAN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
An administrator would like to update a network machine with a number of vendor fixes concurrently. Which of the following would accomplish this with the LEAST amount of effort?

A. Install a service pack
B. Install a patch.
C. Install a hotfix.
D. Install a new version of the program

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
A port scan of a network identified port 25 open on an internal system. Which of the following types of traffic is this typically associated with?

A. Web traffic
B. File sharing traffic
C. Mail traffic
D. Network management traffic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
If an end-user forgets the password that encrypts the content of a critical hard drive, which of the following would aid in recovery of the data?

A. Key escrow
B. Symmetric key
C. Certificate authority
D. Chain of custody

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
A technician needs to ensure that all major software revisions have been installed on a critical network machine. Which of the following must they install to complete this task?

A. HIDS
B. Hotfixes
C. Patches
D. Service packs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
A security administrator needs to determine if an assistant's workstation is sending out corporate information. Which of the following could be used to review the assistant's network traffic?

A. Systems monitoring
B. Performance monitoring
C. Performance baselining
D. Protocol analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
An administrator has discovered that regular users are logging into a stand-alone computer and editing files they should have read-only access to. Which of the following should the administrator investigate FIRST?

A. Users installing worms under their own accounts to mine data.
B. Users escalating their privileges using an administrator account.
C. Users remotely connecting from their workstation with administrator privileges.
D. Users creating new accounts with full control to the files.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
A technician notices that unauthorized users are connecting to a wireless network from outside of the building. Which of the following can BEST be implemented to mitigate this issue?

A. Change the SSID
B. The wireless router needs to be replaced
C. Install CAT6 network cables
D. The wireless output range can be reduced

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
The company's NIDS system is setup to match specifically configured traffic patterns. Which of the following BEST describes this configuration?

A. Anomaly-based
B. Behavior-based
C. OVAL-based
D. Role-based

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205
Which of the following is commonly used to secure HTTP and SMTP traffic?

A. SHA
B. SFTP
C. TLS
D. SCP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
Company A recently purchased the much smaller Company B. The security administrator for Company A reviews the servers of Company B and determines that all employees have access to all of the files on every server. Which of the following audits did the security administrator perform?

A. User access and rights
B. Group policy
C. Storage policy
D. System policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
An administrator is concerned that users are not utilizing strong passwords. Which of the following can be done to enforce user compliance?

A. Implement a strict domain level group policy.
B. Supply the users with suggested password guidelines.
C. Offer user training regarding proper policy.
D. Supply the users with a third-party application to hash their passwords.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
Hooking processes and erasing logs are traits of which of the following?

A. Spam
B. Rootkit
C. Buffer overflow
D. Cross-site scripting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
Which of the following are used by security companies to discover the latest Internet attacks?

A. Port scanner
B. Firewall
C. NIPS
D. Honeypot

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
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: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
An email server appears to be running with an increased load. Which of the following can be used to compare historical performance?

A. Performance baselines
B. Systems monitor

C. Protocol analyzer
D. Performance monitor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
Which of the following allows a security administrator to separate networks from each other?

A. Implicit deny
B. Subnetting
C. SaaS
D. laaS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
A user wants to send personally identifiable information to the security office via email, so they can perform a background check. Which of the following should be used to send the information to the security office?

A. Level of importance
B. Digital signature
C. Encryption
D. Signature line

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
Which of the following is used to prevent attacks against the OS on individual computers and servers?

A. NAT
B. HIDS
C. HIPS
D. NIPS

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 215
Which of the following is reversible when encrypting data?

A. A private key
B. A public key
C. A hashing algorithm
D. A symmetric key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216
Which of the following is an example of a smart card?

A. PIV
B. MAC
C. One-time passwords
D. Tokens

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217
Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

A. Recovery agent
B. Certificate authority
C. Trust model
D. Key escrow

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
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:

QUESTION 219
A user reports that after a recent business trip, their laptop started having performance issues and unauthorized emails have been sent out from the laptop. Which of the following will resolve this issue?

A. Updating the user's laptop with current antivirus
B. Updating the anti-spam application on the laptop
C. Installing a new pop-up blocker
D. Updating the user's digital signature

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
Which of the following describes the direction a signal will emanate from if a Yagi antenna is placed parallel to the floor?

A. In a downward direction, perpendicular to the floor
B. Up and down, perpendicular to the floor
C. Side to side, parallel with the floor
D. Directly from the point of the antenna, parallel to the floor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
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:

QUESTION 222
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:

QUESTION 223
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:

QUESTION 224
A user receives an unsolicited email to change their online banking password. After clicking on the link contained in the email the user enters their banking credentials and changes their password. Days later, when checking their account balance they notice multiple money transfers to other accounts. Which of the following BEST describes the type of attack?

A. Malicious insider
B. Phishing
C. Smurf attack
D. Replay

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
A company is testing their backup procedures and realizes that certain critical systems are unable to be restored properly with the latest tapes. Which of the following is the MOST likely cause?

A. The backups are differential
B. EMI is affecting backups
C. Backup contingency plan is out-of-date
D. The backups are incremental

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
Which of the following is a way to control system access by department function?

A. Role-Based Access Control
B. Rule-Based Access Control
C. Mandatory Access Control
D. Discretionary Access Control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227
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:

QUESTION 228
A new product is being evaluated by the security team. Which of the following would take financial and business impacts into consideration if this product was likely to be purchased for large scale use?

A. Risk assessment
B. Strength of security controls
C. Application vulnerability
D. Technical threat

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
A user reports that the spreadsheet they use for the department will not open. The spreadsheet is located on a server that was recently patched. Which of the following logs would the technician review FIRST?

A. Access
B. Firewall
C. Antivirus
D. DNS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 230
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:

QUESTION 231
Which of the following access control methods requires significant background investigations?

A. Discretionary Access Control (DAC)
B. Rule-based Access Control (RBAC)
C. Role-based Access Control (RBAC)
D. Mandatory Access Control (MAC)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232

Which of the following is capable of providing the HIGHEST encryption bit strength?

A. DES
B. 3DES
C. AES

D. WPA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
Which of the following risk mitigation strategies would ensure that the proper configurations are applied to a system?

A. Incident management
B. Application fuzzing
C. Change management
D. Tailgating

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234
Which of the following is the way of actively testing security controls on a system?

A. White box testing
B. Port scanning
C. Penetration testing
D. Vulnerability scanning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
A hard drive of a terminated employee has been encrypted with full disk encryption, and a technician is not able to decrypt the data. Which of the following ensures that, in the future, a technician will be able to decrypt this information?

A. Certificate authority
B. Key escrow
C. Public key
D. Passphrase

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
Employees are allowed access to webmail while on the company network. The employees use this ability to upload attachments and send email from their corporate accounts to their webmail. Which of the following would BEST mitigate this risk?

A. Clean Desk Policy
B. Acceptable Use Policy
C. Data Leak Prevention
D. Fuzzing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 237
When WPA is implemented using PSK, which of the following authentication types is used?

A. MD5
B. LEAP
C. SHA
D. TKIP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238
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:

QUESTION 239

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:

QUESTION 240
Which of the following allows a security administrator to divide a network into multiple zones? (Select TWO]

A. PAT
B. EIGRP
C. VLAN
D. NAT
E. Subnetting

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
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:

QUESTION 242
Which of the following assessments is directed towards exploiting successive vulnerabilities to bypass security controls?

A. Vulnerability scanning
B. Penetration testing
C. Port scanning
D. Physical lock testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243
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:

QUESTION 244
The benefit of using software whole disk encryption is:

A. the data can be retrieved easier if the disk is damaged
B. the disk's MBR is encrypted as well.
C. unauthorized disk access is logged in a separate bit.
D. the entire file system is encrypted in case of theft.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
The company Chief Information Officer (CIO) contacts the security administrator about an email asking for money in order to receive the key that would decrypt the source code that the attacker stole and encrypted. Which of the following malware types is this MOST likely to be?

A. Worm
B. Virus
C. Spyware
D. Ransomware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246

Which of the following is an advantage of an employer providing smartphones to their employees instead of regular cellular phones?

A. Smartphones can be tied to multiple PCs for data transferring.
B. Smartphone calls have a second layer of encryption.
C. Smartphones can encrypt and password protect data.
D. Smartphones can be used to access open WAPs for coverage redundancy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247
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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248
A security administrator performs various audits of a specific system after an attack. Which of the following BEST describes this type of risk mitigation?

A. Change management
B. Incident management
C. User training
D. New policy implementation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249
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:

QUESTION 250
Which of the following protocols assists in identifying a user, by the generation of a key, to establish a secure session for command line administration of a computer?

A. SFTP
B. FTP
C. SSH
D. DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
In which of the following locations can password complexity be enforced via group policy?

A. Domain controllers
B. Local SAM databases
C. ACLs
D. NAC servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
Security related training should be used to teach the importance of which of the following behaviors?

A. Routine audits
B. Data mining
C. Data handling
D. Cross-site scripting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
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:

QUESTION 254
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:

QUESTION 255
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:

QUESTION 256
Which of the following is an example of requiring users to have a password that consists of alpha-numeric and two special characters?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 257
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:

QUESTION 258
Which of the following tools can execute a ping sweep?

A. Protocol analyzer
B. Anti-virus scanner
C. Network mapper
D. Password cracker

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259
Which of the following would be used to distribute the processing effort to generate hashes for a password cracking program?

A. RAID
B. Clustering
C. Redundancy
D. Virtualization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
Which of the following will help prevent unauthorized access to a smartphone?

A. Remote wipe
B. GPS tracking
C. Screen lock
D. Voice encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
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:

QUESTION 262
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263
Which of the following would a security administrator implement if a parking lot needs to be constantly monitored?

A. Video surveillance
B. Mandatory access control
C. Mantraps
D. Proximity readers

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 264
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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 265
A CRL is comprised of:

A. malicious IP addresses
B. trusted CA's.
C. untrusted private keys.
D. public keys.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 266
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 267

Which of the following components is MOST integral to HTTPS?

A. PGP
B. Symmetric session keys
C. Diffie-Hellman key exchange
D. Mutual authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 268
Which of the following uses TCP port 22 by default?

A. SSL, SCP, andTFTP
B. SSH, SCP, and SFTP
C. HTTPS, SFTP, andTFTP
D. TLS, TELNET, and SCP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 269
A system administrator sees a firewall rule that applies to 10.4.4.58/27. Which of the following IP address ranges are encompassed by this rule?

A. 10.4.4.27 10.4.4.58
B. 10.4.4.32 10.4.4.63
C. 10.4.4.58 10.4.4.89
D. 10.4.4.58 10.4.4.127

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 270
Employees are unable to open internal company documents as they all appear to be encrypted. The company CIO has received an email asking for $10,000 in exchange for the documents decryption key. Which of the following BEST describes this type of attack?

A. Adware
B. Ransomware
C. Trojan attack
D. Rootkit attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271
Which of the following can ensure the integrity of email?

A. MD5
B. LANMAN
C. Blowfish
D. NTLM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 272
Which of the following should the network administrator use to remotely check if a workstation is running a P2P application?

A. Port scanner
B. Network mapper
C. Ping sweeper
D. ARP scanner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273
Which of the following processes describes identity proofing?

A. Authentication and authorization
B. Access control and identity verification
C. Identification and authentication
D. Identification and non-repudiation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274
Which of the following practices is MOST relevant to protecting against operating system security flaws?

A. Patch management
B. Antivirus selection
C. Network intrusion detection
D. Firewall configuration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 275
Which of the following is MOST commonly implemented to transport network device logs to a logging server?

A. SOCKS
B. SHTTP
C. SYSLOG
D. SMTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 276
Which of the following access control methods prevents a user from accessing network resources after the end of the users typical shift?

A. Group policy
B. Time of day restrictions
C. Password policy
D. Acceptable use policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277
A user reports that after searching the Internet for office supplies and visiting one of the search engine results websites, they began receiving unsolicited pop-ups on subsequent website visits. Which of the following is the MOST likely cause of the unsolicited pop-ups?

A. Virus

B. Spam
C. Trojan
D. Adware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 278
Which of the following is a required component for deploying Kerberos?

A. Extensible authentication protocol
B. Ticket granting server
C. Remote access server
D. Certificate authority

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 279
Which of the following would protect an employees network traffic on a non-company owned network?

A. 802.1x
B. VPN
C. RADIUS
D. Antivirus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 280
Assigning access on a need-to-knows basis is a best practice in which of the following controls?

A. Account management
B. Risk assessment
C. Vulnerability assessment
D. Patch management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 281
Which of the following security threats MOST frequently uses IRC to communicate with a remote host?

A. Spam
B. Phishing
C. Botnets
D. Worm

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 282
Which of the following groups should be able to view the results of the risk assessment for an organization? (Select TWO).

A. HR employees
B. All employees
C. Executive management
D. Vendors
E. Information security employees

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283
Which of the following can restrict a computer from receiving network traffic?

A. HIDS
B. NIDS
C. Antivirus
D. Software firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 284
Which of the following would allow an administrator to perform internal research on security threats and common viruses on multiple operating systems without risking contamination of the production environment?

A. A VLAN
B. A honey pot
C. A virtual workstation

D. A firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 285
PGP is a cryptosystem based on which of the following encryption method?

A. SSL
B. Certificate authority
C. Symmetric
D. Asymmetric

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 286
Which of the following is the BEST solution for an administrator to implement in order to learn more about the zeroday exploit attacks on the internal network?

A. A stateful firewall
B. An IDS
C. A Honeypot
D. A HIDS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 287
A user reports that their system is slow and reboots on its own. The technician is unable to remotely control the computer and realizes that they no longer have administrative rights to that workstation. Which of the following is MOST likely the cause?

A. Rootkit
B. DDoS
C. Adware
D. Spam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 288
Which of the following is a mitigation technique that addresses signal emanation?

A. Placing shielding on one side of a wireless router
B. Turning off the SSID broadcast on the wireless router
C. Installing a WIDS in addition to the wireless router
D. Configuring WPA instead of WEP on the wireless router

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 289
Which of the following describes bringing risk to an acceptable level?

A. Risk avoidance
B. Risk mitigation
C. Leveraging positive risk
D. Avoiding negative risk

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 290
Which of the following technologies will ensure the datacenter remains operational until backup power can be obtained?

A. Transfer switch
B. Backup generator
C. UPS
D. Circuit breaker

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 291
Patches and updates should be applied to production systems:

A. after baselines of the affected systems are recorded for future comparison.
B. after vetting in a test environment that mirrors the production environment.
C. as soon as the Configuration Control Board is alerted and begins tracking the changes.

D. as soon as the vendor tests and makes the patch available.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 292
Which of the following security tools can view the SSIDs of wireless networks even when they have SSID broadcasting disabled?

A. NMAP
B. Kismet
C. RADIUS
D. Netstumbler

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 293
A recent risk assessment has identified vulnerabilities on a production server. The technician realizes it was recently re-imaged after a component failed on it. Which of the following is the FIRST item to assess when attempting to mitigate the risk?

A. If all current service packs and hotfixes were re-applied
B. If the spam filters have been properly applied
C. If all device drivers were updated
D. If the firewall ruleset does not allow incoming traffic to the vulnerable port

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 294
Multiple machines are detected connecting to a specific web server during non-business hours and receiving instructions to execute a DNS attack. Which of the following would be responsible?

A. Adware
B. Logic Bomb
C. Virus
D. Botnet

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 295
A network administrator is alerted to an incident on a file server. The alerting application is a file integrity checker. Which of the following is a possible source of this HIDS alert?

A. ARP poisoning
B. Teardrop attack
C. Rootkit
D. DDOS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 296
A server needs to be configured to allow the sales department ability to read and write a file. Everyone else in the company only needs read access. Which of the following access control lists will do this?

A. Sales: Read=Allow; Write=Allow
   Everyone: Read=Allow; Write=None
B. Sales: Read=None; Write=Allow
   Everyone: Read=Allow; Write=Allow
C. Sales: Read=Allow; Write=Allow
   Everyone: Read=None; Write= None
D. Sales: Read=Allow; Write=Allow
   Everyone: Read=Deny; Write=Deny

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 297
Which of the following is the BEST mitigation against DoS attacks?

A. Distributed, redundant datacenters with IPS
B. Redundant ISPs, power sources, and NAT
C. Distributed power sources, NAC, and VLANs
D. Two-factor server authentication, NIDS, and VPNs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 298
When managing user access to files and system resources with groups, users should be placed into groups based on which of the following?

A. Concept of least privilege, required access, and security role
B. Job rotation, server location, and MAC
C. Concept of implicit deny, printer location, and biometrics
D. MAC, RBAC, and IP address

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 299
A user reports that they cannot print anything from the file server or off the web to the network printer. No other users are having any problems printing. The technician verifies that the user's computer has network connectivity. Which of the following is the MOST probable reason the user cannot print?

A. The user does not have Internet access.
B. The user does not have access to the printer.
C. The user does not have full access to the file server.
D. The printer is not setup up correctly on the server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 300
Which of the following security attacks would be MOST likely to occur within the office without the use of technological tools?

A. Shoulder surfing
B. Cold calling
C. Phishing
D. SPIM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
One form of social engineering is known as shoulder surfing and involves nothing more than watching someone when they enter their sensitive data. They can see you entering a password, typing in a credit card number, or entering any other pertinent information. The best defense against this type of attack is simply to survey your environment before entering personal data.

QUESTION 301
Which of the following is the MOST common way to allow a security administrator to securely administer remote *NIX based systems?

A. SSH

B. IPSec
C. PPTP
D. SSL/TLS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 302
Identification is the process of verifying which of the following?

A. The users access level
B. The uniqueness of a users token
C. The association of a user
D. The user or computer system

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 303
Which of the following is the BEST way for an attacker to conceal their identity?

A. Deleting the cookies
B. Increase the max size of the log
C. Shoulder surfing
D. Disable logging

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 304
Which of the following is the primary location where global policies are implemented in an organization?

A. Domain
B. Physical memory
C. User documentation
D. Security group

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 305
The physical location of rogue access points can be discovered by using which of the following?

A. War driving
B. Remote monitoring
C. IPS
D. Creating honeypots

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 306
Which of the following should be implemented to mitigate the security threat of adware?

A. Antivirus
B. Pop-up blockers
C. Anti-spam
D. Subnetting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 307
Which of the following security measures can be used with 802.1x?

A. Network address translation
B. Network access control
C. IPSec VPNs
D. Internet content filter

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 308
Which of the following BEST secures ingress and egress points in a data center?

A. ID badges

B. Proximity cards
C. Escorts
D. Log book

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 309
Virtualization technology can be implemented to positively affect which of the following security concepts?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 310
A secure company portal, accessible publicly but only to company employees, frequently fails to renew its certificates, resulting in expired certificate warnings for users. These failures: (Select TWO).

A. permit man-in-the-middle attacks to steal users credentials.
B. are irritating to the user but the traffic remains encrypted.
C. breed complacency among users for all certificate warnings.
D. expose traffic sent between the server and the user's computer.
E. increase resources used by the company's web-servers.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 311
In a standard PKI implementation, which of the following keys is used to sign outgoing messages?

A. Sender's private key
B. Recipient's private key
C. Recipient's public key

D. Sender's public key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 312

After disabling SSID broadcast for all wireless routers on the network, the administrator noticed that the Same unauthorized users were still accessing the network. Which of the following did the administrator fail to do?

A. Change the SSID.
B. Disallow 802.11a traffic on the network.
C. Enable ARP cache spoofing protection.
D. Re-enable the SSID.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 313
Which of the following best practices should be applied to print resources to enforce existing information assurance controls?

A. Remove unnecessary users from groups with permissions to the resources.
B. Restrict group membership to users who do not print often.
C. Set the printer to standby mode after hours.
D. Ensure that all user groups have permission to all printers.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 314
Wireless access points with SSID broadcast make it easier to do which of the following?

A. War driving
B. Implement encryption
C. Physically tap the network
D. Decrease wireless coverage

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 315
A company is having a problem with users setting up rogue access points. Which of the following solutions would be the BEST for the administrator to implement?

A. Implement least privilege access
B. Password policy hardening
C. MAC address filtering
D. Stop SSID broadcasting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 316
The BEST way to protect data-at-rest from an attacker is:

A. secure network protocols.
B. strong authentication.
C. whole disk encryption.
D. restricting read permission.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 317
A recipient's public key can be used by a data sender to ensure which of the following?

A. Sender anonymity
B. Data confidentiality
C. Sender authentication
D. Data availability

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 318
Limiting access to a file resource to only the creator by default, is an example of applying which of the following security concepts?

A. Behavior-based security
B. Logical tokens
C. Least privilege
D. Role-based access control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 319

Which of the following BEST describes a tool used to encrypt emails in transit?

A. Whole disk encryption
B. Digital signatures
C. SSL over VPN
D. S/MIME certificates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Secure Multipurpose Internet Mail Extensions (S/MIME) is a standard used for encrypting e-mail. S/MIME contains signature data. It uses the PKCS #7 standard (Cryptographic Message Syntax Standard) and is the most widely supported standard used to secure e-mail communications.

QUESTION 320
Management has requested increased visibility into how threats might affect their organization. Which of the following would be the BEST way to meet their request without attempting to exploit those risks?

A. Conduct a penetration test.
B. Conduct a risk assessment.
C. Conduct a security awareness seminar.
D. Conduct a social engineering test.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 321
A network administrator places a firewall between a file server and the public Internet and another firewall between the file server and the company's internal servers. This is an example of which of the following design elements?

A. VLAN
B. DMZ
C. Subnetting
D. NAT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 322
Which of the following SSH configurations mitigate brute-force login attacks? (Select THREE).

A. Disabling default accounts
B. Enabling SSH version 2

C. Changing the default service port
D. Limiting failed logon attempts
E. Enforcing use of cryptographic keys
F. Filtering based upon source address

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 323
During an annual risk assessment, it is discovered the network administrators have no clear timeline of when patches must be installed. Which of the following would BEST solve this issue?

A. Report the issue to management and revisit it during the next risk assessment
B. Training network administrators on the importance of patching
C. Hiring more administrators to better assist in the patching of servers
D. Creating and disseminating a patch management policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 324
The firewall administrator sees an outbound connection on IP port 50 and UDP port 500.
Which of the following is the cause?

A. Certificate revocation list look-up
B. IPSec VPN connection
C. Incorrect DNS setup
D. SSH tunneling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 325
Which of the following represents two factor authentication?

A. A password and a PKI certificate
B. A retina and fingerprint scan
C. A security badge and a physical token
D. A passphrase and PIN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 326
Which of the following is MOST likely to be used to transfer malicious code to a corporate network by introducing viruses during manufacturing?

A. Cell phones
B. USB drives
C. BIOS chips
D. P2P software

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 327
Which of the following authentication models is the MOST vulnerable to password crackers?

A. Two factor

B. Physical tokens
C. Single factor
D. Three factor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 328
Which of the following security controls targets employee accounts that have left the company without going through the proper exit process?

A. Password complexity policy
B. Account lockout policy
C. Account expiration policy
D. Access control lists

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 329
Which of the following is an email attack targeted at a specific individual to trick the individual into revealing personal information?

A. Hoax
B. Pharming
C. Phishing
D. Spear phishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 330
Integrity is BEST provided by which of the following technologies?

A. Symmetric key cryptography
B. Whole disk encryption
C. Asymmetric key cryptography
D. Digital signatures

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 331
Which of the following is the EASIEST to implement for protecting an individual system?

A. Protocol analyzer
B. Internet content filter
C. Proxy server
D. Personal software firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 332
In general, which of the following is considered the MOST resistant to physical eavesdropping methods?

A. Coaxial cable
B. CAT5 network cable
C. Wireless access points
D. Fiber optic cable

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 333
Which of the following describes an action taken after a security breach?

A. Change management
B. Disaster recovery planning
C. Forensic evaluation
D. Business continuity planning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 334
A user reports a problem with resetting a password on the company website. The help desk determined the user was redirected to a fraudulent website. Which of the following BEST describes attack type?

A. Spyware
B. Logic bomb
C. XSS
D. Worm

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 335
During a change management meeting, changes within the firewall were approved. Which of the following processes should an administrator follow?

A. Put firewall offline to perform all changes and return it online.
B. Log all changes being performed.
C. Save all current entries and perform changes.
D. Backup all current entries, perform and log all changes.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 336
Which of the following audit systems should be enabled in order to audit user access and be able to know who is trying to access critical systems?

A. Password policy
B. Failed logon attempts

C. Account expiration
D. Group policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 337
All administrators are now required to use 15 character passwords. Which of the following is the BEST method to enforce this new password policy?

A. Forcing all users to change their password on next login
B. Account expiration configuration

C. Group policy
D. Email announcements

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 338
During a data exfiltration penetration test, which of the following is the NEXT step after gaining access to a system?

A. Privilege escalation
B. Attack weak passwords
C. DoS
D. Use default accounts

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 339
Which of the following standards could be used to rate the risk exposure of vulnerabilities on a network?

A. OVAL
B. Certificate authority
C. TACACS
D. RADIUS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Open Vulnerability and Assessment Language (OVAL) is a community standard written in XML that strives to promote open and publicly available security content. It consists of a language, interpreter, and repository and is meant to standardize information between security tools.

QUESTION 340
Which of the following should be protected from disclosure?

A. Public key infrastructure
B. User's private key passphrase
C. User's public key
D. Certificate revocation list

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 341
Rule-based access control is closely aligned with which of the following?

A. Implicit deny
B. Mandatory access control
C. Access control lists
D. Role-based access control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 342
A user is recording a file on disk. Which of the following will allow a user to verify that the file is the original?

A. NTFS
B. MD5
C. RSA
D. 3DES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 343
The administrator needs to set permissions for the new print server for a company comprised of 320 people in 18 departments. Each department has its own set of printers. Which of the following options is the BEST way to

do this?

A. Place all the people into distribution groups. Assign printer access by access group.
B. Place all the people into departmental groups. Assign printer access by matching individuals to printer groups.

C. Place all the people into departmental groups. Assign access to all printers for each group.
D. Place all the people into departmental groups. Assign printer access by matching group to department.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 344
Which of the following is BEST used for providing protection against power fluctuation?

A. Volt meter
B. Generator
C. Redundant servers
D. UPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 345
Which of the following BEST describes the function of a NIDS?

A. Analyzing network traffic for suspicious traffic
B. Analyzing LAN traffic for file sharing software
C. Diverting suspicious traffic in real-time
D. Diverting spyware traffic to the DMZ

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 346
A penetration tester is required to conduct a port scan on a network. Which of the following security tools can be used to conduct this scan? (Select TWO).

A. nslookup
B. netcat
C. Nmap
D. Kismet
E. Snort

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 347
An employee with a regular user account has downloaded a software program which allowed the user to join the administrator group. Which of the following is occurring?

A. Buffer overflow
B. Privilege escalation
C. Trojan
D. Virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 348
Command-and-Control is a key element of a:

A. logic bomb.
B. trojan.
C. rootkit.
D. botnet.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 349
WPA2-Enterprise can use which of the following to authenticate a user?

A. RRAS
B. TKIP
C. RADIUS
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 350

Which of the following is achieved and ensured by digitally signing an email?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 351
The IT department has been having issues lately with vulnerabilities occurring on the network due to outdated software on new computers that are deployed. Which of the following would be the BEST way for the administrator to address this issue?

A. Establish configuration baselines for the images
B. Implement group policies
C. Build security templates for the OS
D. Ensure that all patches are installed by employees

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 352
Which of the following authentication models often requires different systems to function together and is complicated to implement in non-homogeneous environments?

A. Three factor authentication
B. Single sign-on
C. One factor authentication
D. Two factor authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 353
Which of the following attacks can be mitigated by shredding confidential documents?

A. Shoulder surfing
B. Phishing
C. Hoax

D. Dumpster diving

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 354
A penetration tester is attempting to run a brute-force attack to discover network passwords. Which of the following tools would be BEST suited to this task?

A. Milw0rm
B. John the Ripper
C. OVAL
D. Metasploit

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords.

QUESTION 355
The manager has tasked an administrator to test the security of the network. The manager wants to know if there are any issues that need to be addressed, but the manager is concerned about affecting normal operations. Which of the following should be used to test the network?

A. Use a protocol analyzer.
B. Use a vulnerability scanner.
C. Launch a DDoD attack in the network and see what occurs.
D. Read the log files on each system on the network.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 356
In order to help maintain system security, employees are only given rights to perform their current job function. Which of the following BEST describes this practice?

A. Implicit deny
B. Job rotation
C. Separation of duties
D. Least privilege

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 357
Which of the following relies on prime numbers to generate keys?

A. IPSec
B. Elliptic curve
C. RSA
D. AES

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 358
Using a digital signature during an online transaction is a form of:

A. availability.
B. key management.
C. non-repudiation.
D. confidentiality.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 359
The network administrator has been asked to turn off access to the command prompt for some users. Which of the following is the BEST choice to complete this request?

A. Deploy a hotfix.
B. Deploy patches.
C. Deploy service packs.
D. Deploy a group policy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 360

A computer is displaying an MBR error upon restart. The technician is told the user has just installed new software. Which of the following threats is the MOST likely cause of this error?

A. Distributed DoS
B. Boot sector virus
C. Trojan
D. ActiveX

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 361
Which of the following is a best practice when creating groups of user and computer accounts in a directory service?

A. Naming conventions and technical aptitude
B. Delegation of administration and policy deployment
C. Department and salary divisions
D. Seniority at the company and access level

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 362
A user reports that after opening an email from someone they knew, their computer is now displaying unwanted images. Which of the following software can the technician MOST likely install on the computer to mitigate this threat?

A. Antivirus
B. Anti-spam
C. HIDS
D. Firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 363
Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

A. Read the last 512 bytes of the tape.
B. Restore a random file.
C. Read the first 512 bytes of the tape.

D. Perform a full restore.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 364
Which of the following can be implemented to ensure an employee cannot use the system outside of normal business hours?

A. Time of day restrictions
B. Implicit deny
C. Account expiration
D. Two factor authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 365
Which of the following can be implemented to prevent malicious code from executing?

A. Personal software firewall
B. Anti-spam software
C. Antivirus software
D. Hardware firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 366
Which of the following BEST describes NAC?

A. Provides access based on predetermined characteristics
B. Translates between DHCP requests and IP addresses
C. Provides access based on ARP requests
D. Translates between private addresses and public addresses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 367

Which of the following tools is used to report a wide range of security and configuration problems on a network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 368
A remote network administrator calls the helpdesk reporting that they are able to connect via VPN but are unable to make any changes to the internal web server. Which of the following is MOST likely the cause?

A. The VPN concentrator needs to be configured.
B. The administrator needs to be added to the web servers administration group.
C. The administrator does not have the correct access rights to dial in remotely.
D. IPSec needs to be reinstalled on the administrator's workstation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 369
Which of the following will allow a security administrator to determine potentially malicious traffic traversing the network?

A. Protocol analyzer
B. Systems monitor
C. Task manager
D. Performance monitor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 370
Which of the following is MOST closely associated with email?

A. S/MIME
B. IPSec
C. TLS
D. SSH

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 371
Which of the following is performed when conducting a penetration test?

A. Documentation of security vulnerabilities and policy gaps.
B. Demonstrations of network capabilities and resiliency.
C. Demonstrations of security vulnerabilities and flaws in policy implementation.
D. Documentation of network security settings, policy gaps and user errors.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 372
On which of the following algorithms is PGP based?

A. DES
B. MD5
C. WPA
D. RSA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 373
The success of a user security education and awareness plan is largely dependent on support from:

A. contractors.
B. senior management.
C. project management.
D. human resources.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 374
Which of the following allows two people to communicate securely without having to know each other prior to communicating?

A. AES
B. 3DES
C. Symmetric keys
D. PKI

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 375
When investigating data breaches caused by possible malicious action, it is important for members of the CIRT to document the location of data at all times. Which of the following BEST describes what the CIRT is trying to document?

A. Damage mitigation
B. Disaster recovery plan
C. Proper authorization procedures
D. Chain of custody

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 376
Which of the following is a transmission encryption that is generally regarded as weak?

A. WEP
B. PGP
C. AES256
D. SSL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 377
The MOST expensive and effective alternate site that provides the HIGHEST level of availability, is called a:

A. primary site.
B. warm site.
C. cold site.
D. hot site.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 378
Which of the following is an example of a single sign-on?

A. Authentication to individual systems with a single authentication factor.
B. The use of three factor authentication on single systems.
C. Access to individual systems with a single password.
D. Access to multiple systems with a single authentication method.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 379
A security administrator has detected that the company websites source code contains suspicious numbers of white spaces and non-printable characters at the end of each line of code. Which of the following is being used in order to leak sensitive information to the competition?

A. Encryption

B. Steganography
C. Obfuscation
D. Code fuzzing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 380
A system administrator wants to verify that the corporate users are following the security policy on password complexity requirements. Which of the following could be used to verify the passwords?

A. Password hashing
B. Password hardening
C. Password enumeration
D. Password cracking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 381
The company's NIDS system is configured to pull updates from the vendor and match traffic patterns based on these updates. Which of the following BEST describes this configuration?

A. Signature-based
B. OVAL-based
C. Anomaly-based
D. Behavior-based

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 382
Which of the following desktop solutions can a user implement to detect and delete downloaded malware?

A. Desktop firewall
B. HIPS
C. HIDS

D. Antivirus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 383
After deploying a new IDS, an administrator notices a large amount of notifications coming from a filter inspecting port 445. Which of the following can BEST help the administrator in determining if the notifications are false positives?

A. The router tables
B. Firewall log
C. IDS performance monitor
D. Protocol analyzer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 384
Which of the following BEST characterizes a DMZ?

A. A trusted network that is encrypted end-to-end.
B. A connection between two trusted networks.
C. A trusted segment to a VPN concentrator.

D. A network that resides between trusted and non-trusted networks.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 385
Which of the following would be used to gain access to a data center where the administrator would have to use multiple authentication factors?

A. Fingerprint and retina scan
B. Enter two different passwords
C. Fingerprint scan and password
D. ID badge and smartcard

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 386
A security manager decides to assign the daily responsibility of firewall and NIDS administration to different technicians. This is an example of which of the following?

A. Job rotation
B. Implicit deny
C. Separation of duties
D. Least privilege

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 387
A security administrator is worried about attackers accessing a specific server within the company's network. Which of the following would allow the security staff to identify unauthorized access to the server?

A. Honeypot
B. Antivirus
C. HIDS
D. Anti-spyware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 388
Which of the following ports is susceptible to DNS poisoning?

A. 23
B. 8080
C. 80
D. 53

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 389
Which of the following is the main disadvantage of implementing a certificate revocation list?

A. It is a single point of failure and expensive to maintain.
B. Only a certain number of certificates can be revoked.
C. Revocation is not instantaneous.
D. The CRL database cannot be duplicated.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 390
Which of the following would an administrator MOST likely update after deploying a service pack?

A. Group policy
B. Hotfix
C. Configuration baseline
D. Patch

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 391
A computer or device that is setup on the network merely to monitor the habits and techniques of a suspected attack is known as a:

A. content filter.
B. proxy.
C. honeypot.

D. dummy terminal.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 392
Which of the following devices would be used to gain access to a secure network without affecting network connectivity?

A. Fiber-optic splicer
B. Firewall

C. Vampire tap
D. Router

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 393
Which operating system hardening procedure can be implemented to ensure all systems have the most up-to-date version available?

A. Patch management
B. Configuration baselines
C. Group policies
D. Security templates

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 394
Which of the following is the primary difference between role-based access control and rule-based access control?

A. Both are based on local legal regulations but role based provides greater security.
B. One is based on job function and the other on a set of approved instructions.
C. One is based on identity and the other on authentication.
D. Both are based on job title but rule based provides greater user flexibility.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 395
Which of the following will allow a security administrator to help detect a DDoS?

A. NetBIOS
B. Task manager
C. NIC bindings
D. Performance baseline

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 396
The network administrator has determined that a large number of corporate workstations on the network are connecting to an IRC server on the Internet, and these same workstations are executing DDOS attacks on remote systems. Which of the following terms BEST describes this situation?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 397
Which of the following is used to determine who transported a hard drive during an incident response investigation?

A. Damage and loss control
B. Disclosure guidelines
C. Chain of custody
D. Forensic policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 398
Which of the following is the MAIN difference between bluejacking and bluesnarfing?

A. Bluejacking involves some social engineering while bluesnarfing does not.
B. Bluejacking involves sending unsolicited messages to a phone while bluesnarfing involves accessing the phone data.

C. Bluesnarfing can be done from a greater distance than bluejacking.
D. Bluesnarfing involves sending unsolicited messages to a phone while bluejacking involves accessing the phone data.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 399
Which of the following keys is used to sign an email message?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 400
Which of the following BEST describes the purpose of risk mitigation?

A. Reducing the time from vulnerability discovery to patch deployment.
B. Reducing the work associated with patch management.
C. Reducing the chances that a threat will exploit a vulnerability.
D. Reducing the cost to recover from a security incident.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 401
Organizational policy requiring employees to login using their username and password and a random number from their key fob is an example of:

A. two factor authentication.
B. four factor authentication.
C. single factor authentication.
D. three factor authentication.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 402
A server administrator wants to do a vulnerability assessment on a server that is not on the production network to see if FTP is open. Which of the following tools could be used?

A. Intrusion detection system
B. Port scanner
C. Antivirus software
D. Anti-spyware software

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 403
A network device contains a feature that provides emergency administrator access from any port by sending a specific character sequence. This is an example of a:

A. DDoS attack.
B. default account.
C. back door.
D. DoS attack.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 404
Which of the following provides active protection to critical operating system files?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 405
Which of the following is the BEST example of a physical security policy?

A. All new employees are required to be mentored by a senior employee for their first few months on the job.
B. All doors to the server room must have signage indicating that it is a server room.

C. All server room users are required to have unique usernames and passwords.
D. New server room construction requires a single entrance that is heavily protected.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 406
Which of the following redundancy planning concepts would MOST likely be used when trying to strike a balance between cost and recovery time?

A. Warm site
B. Field site
C. Cold site
D. Hot site

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 407
Which of the following was created to standardize the security assessment process?

A. OVAL
B. Vulnerability scanner
C. TACACS
D. Network mapper

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 408
In PKI, which of the following keys should be kept secret at all times?

A. Private key
B. Public key
C. Diffie-Hellman key
D. Shared key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 409
Which of the following security threats would MOST likely use IRC?

A. Logic bombs
B. Spam
C. Adware
D. Botnets

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 410
Employee A sends employee B an encrypted message along with a digital signature. Employee B wants to make sure that the message is truly from employee A. Which of the following will employee B do to verify the source of the message?

A. Use employee B's public key to unencrypted the message.
B. Use employee A's public key to verify the digital signature.
C. Use employee B's private key to unencrypted the message.
D. Use employee A's private key to verify the digital signature.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 411
The security administrator wants to know if a new device has any known issues with its available applications. Which of the following would be BEST suited to accomplishing this task?

A. Network mapper
B. Port scanner
C. Protocol analyzer
D. Vulnerability scanner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 412
An administrator is having difficulty getting staff to adhere to group policy directives regarding streaming audio. Bandwidth utilization increases around the time that a popular radio show is broadcast. Which of the following is the BEST solution to implement?

A. Implement time of day restrictions
B. Change the password policy
C. Deploy content filters
D. Enforce group policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 413
Which of the following is the FINAL phase of disaster recovery?

A. Hold a follow-up meeting to review lessons learned.
B. Notify all personnel that a disaster has taken place.
C. Restore all network connectivity.
D. Perform a full recovery so all devices are back in working order.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 414
A small company wants to hire a security assessment team for the server and network infrastructure. Which of the following needs to be defined before penetration testing occurs?

A. Vulnerability scan
B. Bandwidth requirements
C. Protocols analysis
D. Rules of engagement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 415
A user logs onto a laptop with an encrypted hard drive. There is one password for unlocking the encryption and one password for logging onto the network. Both passwords are synchronized and used to login to the machine. Which of the following authentication types is this?

A. Two factor
B. Biometric

C. Single sign-on

D. Three factor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 416
An intruder has gained access to a server and installed an application to obtain credentials. Which of the following applications did the intruder MOST likely install?

A. Password cracker
B. Vulnerability scanner
C. Account dictionary
D. Protocol analyzer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 417
A user wants to ensure that if a computer's hard drive is removed, the files cannot be accessed without authentication. Which of the following would be used?

A. Disk encryption
B. Single sign-on
C. Digital signature
D. Biometric reader

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 418
Which of the following would a user need to decrypt a data file that has been encrypted with the user's public key?

A. PGP's public key
B. Sender's private key
C. User's public key
D. User's private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 419
Which of the following is BEST suited to determine which services are running on a remote host?

A. Protocol analyzer
B. Antivirus
C. Log analyzer
D. Port scanner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 420
A security administrator would use which of the following to control access between network segments?

A. Firewall
B. NIDS
C. Subnetting
D. RADIUS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 421
Verifying the time and date certain users access a server is an example of which of the following audit types?

A. Retention policy
B. Account lockout
C. Account login
D. User rights

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 422
A technician wants to implement a change across the production domain. Which of the following techniques should the technician perform?

A. Edit the access control list.
B. Deploy a group policy.
C. Install service packs on the domain.
D. Change the acceptable use policy.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 423
Which of the following has a primary goal of hiding its processes to avoid detection?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 424
Which of the following can be used to prevent ongoing network based attacks?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 425
When implementing a group policy restricting users from running software installations, the administrator needs to be aware of which of the following disadvantages?

A. The policy will restrict remote patching of user workstations.
B. Not all users will know which files are executable installations.
C. Some users may have a legitimate need for installing applications.
D. Such a policy requires a great deal of administrative overhead.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 426

Which of the following is the BEST example of a technical security policy?

A. Posting a sign on the door to the server room indicating that access is restricted to authorized personnel only.
B. Installing electronic locks on the door to the server room that only allow access to a person swiping an administrators smartcard.
C. Removing all the keyboards from the server room and requiring all administrators to bring keyboards from their desks.
D. Building a new server room that only has a single entrance that is heavily protected.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 427
Employee A wants to send employee B an encrypted message that will identify employee A as the source of the message. Which of the following will employee A do to accomplish this? (Select TWO).

A. Use employee A's private key to sign the message.
B. Use the message application to mark the message as urgent.
C. Use only symmetric encryption to send the message.
D. Use employee B's private key to encrypt the message.
E. Use employee B's public key to encrypt the message.
F. Use employee A's public key to sign the message.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 428
From which of the following can a virus be loaded before an OS starts?

A. TPM
B. P2P
C. USB drive
D. Hardware locks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 429
Management wants a security assessment conducted on their network. The assessment must be conducted during normal business hours without impacting users. Which of the following would BEST facilitate this?

A. A vulnerability scan
B. A penetration test
C. A honeynet
D. A risk assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 430
Which of the following activities often involves consulting with the legal department?

A. Updating domain password policies
B. Network infrastructure planning
C. User account creation and management
D. Reviewing storage and retention policies

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 431
Which of the following protocols is used to connect a remote office LAN into the central office so resources can be shared?

A. SSH
B. HTTPS
C. IPSec
D. SNMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 432
Which of the following protocols uses a three-way handshake during communication with multiple hosts?

A. UDP
B. RDP
C. SMTP
D. TCP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 433
Which of the following technologies requires encryption and authentication?

A. WEP
B. 802.1x
C. 802.11n
D. TKIP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 434
A security administrator has received an SD memory card for the purpose of forensic analysis. The memory card is left on the administrator's office desk at the end of the day. The next day the security guard returns the SD card to the administrator because it was found by the night janitor. Which of the following incident response procedures has been violated?

A. Securing the site
B. Chain of custody
C. Evidence gathering
D. Data retention

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 435
Organization policy requiring employees to display their corporate badge at all times is an example of:

A. non-repudiation.
B. identification.
C. authentication.
D. confidentiality.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 436
Which of the following cryptographic methods provides the STRONGEST security when implemented correctly?

A. Elliptic curve
B. NTLM
C. MD5
D. WEP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 437
An on-going attack on a web server has just been discovered. This server is non-critical but holds data that could be very damaging to the company if it is disclosed. Which of the following should the administrator choose as their FIRST response?

A. Launch a counter attack on the other party.
B. Disconnect the server from the network.
C. Call over a manager and document the attack.
D. Monitor the attack until the attacker can be identified.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 438
Which of the following uses both private and public key algorithms for email encryption and decryption?

A. PGP
B. CA
C. DES
D. AES256

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 439
Which of the following is a common evasion technique by attackers to avoid reverse engineering?

A. Determining if the host is already infected
B. Determining if the host if a virtual or physical
C. Determining if the host is Windows or Linux based
D. Determining if the host can connect to the Internet

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 440
When used properly, a one time pad is considered an unbreakable algorithm because:

A. it is a symmetric key.
B. it uses a stream cipher.
C. the key is not reused.
D. it is based on the generation of random numbers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 441
Which of the following uses multiple encryption keys to repeatedly encrypt its output?

A. AES256
B. AES128

C. DES
D. 3DES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Triple DES is a variation of Data Encryption Standard (DES). It uses a 64-bit key consisting of 56 effective key bits and 8 parity bits. The size of the block for Triple-DES is 8 bytes. Triple-DES encrypts the data in 8-byte chunks. The idea behind Triple DES is to improve the security of DES by applying DES encryption three times using three different keys. Triple DES algorithm is very secure (major banks use it to protect valuable transactions), but it is also very slow.

QUESTION 442
Employees in the accounting department move between accounts payable and accounts receivable roles every three months. This is an example of which of the following security concepts?

A. Separation of duties
B. Group policies
C. Least privilege
D. Job rotation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 443
Which of the following is used to provide a fixed-size bit-string regardless of the size of the input source?

A. 3DES
B. WEP
C. SHA
D. PGP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 444
Which of the following is BEST suited to detect local operating system compromises?

A. System log
B. Anti-spam
C. Personal firewall
D. HIDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 445
Which of the following standards encodes in 64-bit sections, 56 of which are the encryption key?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DES encrypts and decrypts data in 64-bit blocks, using a 64-bit key, although the effective key strength is only 56 bits. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits.

QUESTION 446
Which of the following is part of the patch management process?

A. Replacing aging network and computing equipment.
B. Reverse engineering non-vendor supplied patches.
C. Documenting the security assessment and decision.

D. Examining firewall and NIDS logs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 447
Which of the following, if implemented on a server, will ensure availability if half of the drives fail?

A. RAID 3
B. RAID 5
C. RAID 0
D. RAID 1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
RAID level 1 RAID 1 is disk mirroring. Disk mirroring provides 100 percent redundancy because everything is stored on two disks. If one disk fails, another disk continues to operate. The failed disk can be replaced, and the RAID 1 array can be regenerated

QUESTION 448
After accessing several different Internet sites a user reports their computer is running slow. The technician verifies that the antivirus definitions on that workstation are current. Which of the following security threats is the MOST probable cause?

A. Spam
B. Worm
C. Trojan
D. Spyware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 449
A network security administrator is worried about potential man-in-the-middle attacks against users when they access a corporate website from their workstations. Which of the following is the BEST mitigation against this type of attack?

A. Mandating only client-side PKI certificates for all connections
B. Implementing server-side PKI certificates for all connections
C. Requiring strong authentication for all DNS queries
D. Requiring client and server PKI certificates for all connections

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 450
A technician reports that the email server is being compromised. Files are being uploaded to change the email portal webpage. Which of the following tools can be used to determine how the files are being uploaded?

A. VPN
B. Protocol analyzer
C. DMZ
D. Performance monitor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 451
Why is an ad-hoc network a security risk?

A. An ad-hoc network allows access to another computer at the same level of the logged in user, compromising information.
B. An ad-hoc network allows access to the nearest access point which may allow a direct connection to another computer.
C. An ad-hoc network allows access to another computer but with no rights so files cannot be copied or changed.
D. An ad-hoc network allows access to the nearest access point which may give elevated rights to the connecting user.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A wireless network operates in one of two modes, ad-hoc or infrastructure. In the ad hoc mode, each station is a peer to the other stations and communicates directly with other stations within the network. No AP is involved. All stations can send Beacon and Probe frames.

QUESTION 452
The primary purpose of a hot site is to ensure which of the following?

A. Adequate HVAC to meet environmental initiatives

B. Recovery of operations within 30 days after a disaster
C. Transition of operations in a short time period in a disaster
D. Seamless operations in the event of a disaster

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Following a disruption to the original site, the hot site exists so that the organization can relocate with minimal losses to normal operations.

QUESTION 453
Which of the following security concepts is supported by HVAC systems?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 454
User A moved from Human Resources to Accounting. A year later they mistakenly print to a network printer back in HR. This indicates which of the following needs to happen?

A. Updates and patching of the users workstation
B. Installation of antivirus software on the users workstation
C. An audit of the security logs
D. An account access and rights audit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 455
Which of following protocols can operate in tunnel mode?

A. SHTTP
B. IPSec
C. SFTP
D. SSL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 456
Cloud computing uses which of the following technologies to automatically provision guests on demand?

A. Cloning
B. Spoofing
C. Imaging
D. Virtualization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 457
Which of the following is a service that provides authentication, authorization and accounting to connecting users?

A. RADIUS
B. WPA
C. CHAP
D. LANMAN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 458
An administrator needs to implement a backup strategy that provides the fastest recovery in case of data corruption. Which of the following should the administrator implement?

A. Full backup on Sunday and differential backups every other day
B. Full backup on Sunday and incremental backups every other day
C. Full backup on Sunday and alternating differential and incremental every other day
D. Full backup on Sunday and a full backup every day

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 459
Which of the following encryption methods is being used when both parties share the same secret key?

A. Kerberos
B. Asymmetric
C. Symmetric
D. Certificate based

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 460
An administrator discovers evidence that a co-worker has been violating the law with the contents of some of their emails. Which of the following should the administrator do FIRST?

A. Inform upper management or law enforcement.
B. Confront the co-worker and demand all illegal actions cease.
C. Take what was found to another peer and have the peer confront the co-worker.
D. Go through the email server and accumulate as much evidence as possible.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 461
Which of the following can be implemented to mitigate the risks associated with open ports on a server?

A. Disable unnecessary programs
B. Disable network cards
C. Implement a password policy
D. Enable MAC filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 462
Which of the following should an HVAC system do when a fire is detected in a data center?

A. It should shut down.
B. It should change to full cooling.
C. It should decrease humidity.
D. It should increase humidity.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 463
Which of the following encryption implementations would be the MOST secure?

A. 3DES
B. SHA1
C. MD4
D. WEP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 464
Which of the following allows a technician to retroactively identify a security incident?

A. NIDS
B. Internet content filter

C. DMZ
D. Proxy server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 465
A number of users on the company network have been contracting viruses from required social networking sites.
Which of the following would be MOST effective to prevent this from happening?

A. Firewall
B. Honeypot
C. NIDS
D. Proxy server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 466
Which of the following would a technician implement to mitigate SQL injection security risks?

A. Use software firewalls.
B. Use input validation.
C. Disable Java on Internet browsers.
D. Delete Internet history.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 467
Which of the following concepts is applied when a user enters a password to gain authorized access to a system?

A. Authentication
B. Non-repudiation
C. Privatization
D. Identification

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 468
Which of the following vulnerability assessment tools would be used to identify weaknesses in a Company's router ACLs or firewall?

A. Brute force attacks
B. Rainbow tables
C. Port scanner
D. Intrusion prevention systems

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 469
Which of the following is a benefit of network access control (NAC)?

A. A user is able to control connections to the network using cached credentials on a local machine.
B. A user is able to control connections to the network using a centralized list of approved devices.
C. A user is able to distribute connections to the network for load balancing using a centralized list of approved devices.
D. A user is able to distribute connections to the network using cached credentials on a local machine.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 470
Multiple users are having trouble connecting to a secure corporate website and experience a minor delay when logging onto the website. The URL for the website is also slightly different than normal once the users are connected. The network administrator suspects which of the following attacks is being carried out?

A. Phishing
B. Man-in-the-middle
C. Spam

D. Bluesnarfing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 471
Which of the following key types would a user MOST likely receive from a secure e-commerce website?

A. Private key
B. Key escrow
C. Public key
D. CRL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 472
A company is looking for the lowest cost option for their disaster recovery operations, regardless of the amount of time it will take to bring their systems back online. Which of the following would be BEST suited for their needs?

A. Live site
B. Cold site
C. Warm site
D. Hot site

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 473
Which of the following is the MOST efficient way to secure a single laptop from an external attack?

A. NIPS
B. Hardware firewall
C. HIDS
D. Software firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 474
Which of the following should be disabled to help prevent boot sector viruses from launching when a computer boots?

A. DMZ
B. SNMP
C. Hard Drive
D. USB

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 475
Which of the following tools depends MOST heavily on regular updates to remain effective?

A. Network mapper
B. Vulnerability scanner
C. Protocol analyzer
D. Port scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 476
Which of the following can be used to create a unique identifier for an executable file?

A. DES
B. Blowfish
C. NTLM
D. SHA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 477
An administrator is configuring a new system in a domain. Which of the following security events is MOST important to monitor on the system?

A. Password changes
B. Logon attempts
C. Failed data moves
D. Data file updates

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 478
Which of the following cryptography concepts requires two keys?

A. Secret
B. Symmetric
C. Asymmetric
D. TPM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 479
Which of the following would be used to observe a runaway process?

A. Protocol analyzer
B. Performance monitor
C. Performance baseline
D. Application log

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 480

Which of the following determines if traffic is blocked or allowed?

A. Logical keys
B. Network-based Intrusion Detection System (NIDS)
C. Access Control List (ACL)
D. Username and passwords

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 481
Which of the following increases availability during periods of electromagnetic interference? (Select TWO).

A. UTP cable
B. Crossover cable
C. Fiber optic cable
D. STP cable
E. Straight-through cable

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 482
Which of the following is MOST often used in a DDoS?

A. Worm
B. Virus
C. Trojan
D. Botnet

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 483
IPSec provides which of the following?

A. NAT traversal
B. Payload encryption
C. New IP headers
D. Payload compression

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 484
Which of the following does a risk assessment include?

A. Threats, vulnerabilities, and asset values
B. Management, cost, and budget
C. Policies, procedures, and enforcement
D. Exploits, attacks, and social engineering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 485
The company's administrative assistant acts as the main point of contact for outside sales vendors and provides information over the phone. Which of the following is the GREATEST threat that the administrative assistant should be educated about?

A. Providing the corporate mailing address to unidentified callers
B. Data information verification and up-to-date reporting structure
C. Providing employee personal contact information
D. Non-redundant personnel role distribution

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 486
Which of the following centralizes authentication on a wireless network?

A. RADIUS
B. CHAP
C. RDP
D. VPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 487

Which of the following is the BEST course of action to ensure an email server is not an open relay?

A. Require authentication for all inbound SMTP traffic.
B. Require authentication for all inbound and outbound SMTP traffic.

C. Block all inbound traffic on SMTP port 25.
D. Require authentication for all outbound SMTP traffic.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 488
Which of the following helps protect logs from compromise?

A. View logs regularly.
B. Turn on all logging options.
C. Centralize log management.
D. Log failed logon attempts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 489
An administrator wants to implement disk encryption and wants to have a disaster recovery plan to decrypt data if the key is unknown. Which of the following should be implemented?

A. Certificate authority
B. Public key infrastructure
C. Certificate revocation list
D. Recovery agent

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 490
Which of the following tools would BEST allow a security administrator to view the contents of unencrypted network traffic?

A. Network access control
B. Web application firewall
C. Honeypot
D. Protocol analyzer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 491
Which of the following provides an organization with the ability to hide an internal private network, while simultaneously providing additional IP addresses?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 492
Which of the following signature-based monitoring systems is used to detect and remove known worms and Trojans on a host?

A. Anti-spam
B. NIPS
C. Antivirus
D. HIDS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 493
Which of the following allows management to track whether staff members have accessed an authorized area?

A. Hardware locks
B. Physical access logs
C. Physical tokens
D. Man-traps

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 494
To follow industry best practices for disaster recovery planning, an alternate site should be geographically:

A. near to the primary site to reduce outage duration due to conveyance of primary site staff and hardware.
B. near to the primary site to ensure frequent inspection by the primary sites staff.
C. similar to the primary sites to ensure availability of resources and environmental functions.
D. distant from the primary site to decrease the likelihood of an event affecting both.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 495
Which of the following environmental controls would require a thermostat within the datacenter?

A. Fire suppression
B. Air flow control
C. Temperature control
D. Moisture control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 496
If a user lost their private key, which of the following actions would an administrator need to take?

A. Use a recovery agent
B. Obtain a public key
C. Redesign the PKI
D. Purchase a new CA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 497
A library provides an administrator with criteria and keywords to prevent children from accessing certain websites. Which of the following would BEST accomplish this goal?

A. Discretionary access control list
B. Mandatory access control list
C. Proxy server
D. Internet content filter

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 498
Which of the following ensures that an employee cannot continue carrying out fraudulent activities?

A. Biometric reader
B. Two-factor authentication
C. Job rotation
D. Role-based access control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 499
Which of the following is used to both deploy and reapply baseline security configurations?

A. Configuration baseline
B. Performance baseline
C. Security template
D. Security agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 500
Which of the following does a malicious insider install in order to attack the system at a predetermined date?

A. Spam
B. Virus
C. Worm
D. Logic bomb

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 501
Implementing a mandatory vacation policy for administrators is a security best practice because of which of the following?

A. Increases administrators skills by providing them with a vacation.
B. Detects malicious actions by users with remote access to network resources.
C. Makes it easier to implement a job rotation policy and cross train administrators.
D. Detects malicious actions by an administrator responsible for reviewing logs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 502
On network devices where strong passwords cannot be enforced, the risk of weak passwords is BEST mitigated through the use of which of the following?

A. Limited logon attempts
B. Removing default accounts
C. Reverse proxies
D. Input validation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 503
In the event of a fire, the MOST appropriate setting for electronic cipher locks would be to:

A. allow personnel to exit the building without any forms of authentication.
B. allow personnel to exit the building only after security confirms the threat and electronically releases all locks.
C. allow personnel to exit the building using only a photo ID badge.

D. allow personnel to exit the building only after using a valid swipe card and key.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 504
Which of the following is made possible by some commercial virtualization hosting applications?

A. Seamless switching between telephony and IP telephony
B. Transfer of network infrastructure components to meet demand
C. Automatic transfer of applications when hardware fails
D. Automatic redundancy for power in the event of a blackout

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 505
Logs from a company's DNS server show requests from a remote ISPs DNS server for random sequences of characters as non-existent sub-domains to the legitimate domain name (e.g. 1357acef246.company.com). These logs MOST likely suggest the possibility of which of the following attacks?

A. ARP poisoning
B. DNS poisoning
C. TCP/IP hijacking
D. Domain name kiting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 506
Which of the following logs would show that someone has been querying information about a Company's networks?

A. Application logs for service start and stop events
B. Security logs for failed logon attempts
C. DNS logs for zone transfers
D. System logs for patch and reboot events

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 507
A company's laptops use whole disk encryption to encrypt their hard drives. A user lost their key and the technicians do not have a copy of the key. This resulted in the user losing all the data on their hard drive. Which of the following could have been implemented to prevent this situation?

A. Digital signatures
B. Non-repudiation
C. Trusted Platform Module (TPM)
D. Key escrow

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 508
Which of the following algorithms provides the LOWEST level of encryption?

A. Blowfish
B. AES
C. DES
D. SHA1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 509
In which of the following would a user find a list of activities which are prohibited when connecting to a corporate network?

A. Network procedures
B. Privacy policy
C. Due diligence
D. Acceptable use policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 510
A few computers have been off the network for 70 days and a new company policy dictates that all computers that are not on the network for over 60 days need to be disabled. These computers are for a class that is conducted every three months. Which of the following is the BEST solution?

A. Add those computers to a special group and set group policy to disable all computers within that group.
B. Perform a query every 60 days to identify those computers and disable them all at once.
C. Disable each computer as it reaches 60 days, perform queries every 30 days to identify those computers.
D. Add those computers to a special group and perform a query every 45 days to identify additional computers.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 511
Which of the following would be implemented to provide a check and balance against social engineering attacks?

A. Password policy
B. Biometric scanning

C. Separation of duties
D. Single sign-on

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 512
In which of the following situations is a web application firewall MOST likely used?

A. Communication between DNS servers needs to be encrypted.
B. External requests to UDP port 445 needs to be blocked.
C. Input to an application needs to be screened for malicious content.
D. Physical access to a console needs to be secured.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 513
Which of the following offers the MOST difficult to break encryption?

A. Block cipher
B. 3DES
C. One time pad
D. Blowfish

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 514
Which of the following describes a situation where management decided the financial impact is less than the cost of fixing the security threat?

A. Risk denial
B. Rick avoidance
C. Risk acceptance
D. Risk mitigation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 515
Which of the following is required for an anomaly detection system to evaluate traffic properly?

A. Baseline
B. Vulnerability assessment
C. Protocol analyzer
D. Signature

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 516
Which of the following could be used to gather evidence against an attacker?

A. Network mapper
B. Honeypots
C. Internet content filter
D. Encryption devices

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 517
Which of the following should be done FIRST after creating a formal disaster recovery plan?

A. Distribute the plan.
B. Update the plan as needed.
C. Store the plan where all employees can see it.
D. Test the plan.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 518
A data entry technician uses an application from the Internet to gain administrative rights on a system. Gaining unauthorized domain rights is an example of:

A. a logic bomb.
B. spyware.
C. privilege escalation.

D. a rootkit.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 519
Which of the following system types would a security administrator need to implement in order to detect and mitigate behavior-based activity on the network?

A. NIPS
B. Antivirus server
C. NIDS

D. Signature-based security devices

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 520
Which of the following should a developer use to protect cookies while in transit?

A. Proprietary formatting
B. Protocol analyzer
C. Encryption
D. Digital signing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 521
Which of the following sits inline with network traffic and helps prevent malicious behavior as it occurs by either dropping packets or correcting TCP stream related issues?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 522
Which of the following threats is mitigated by ensuring operating system patches are current?

A. Known threats
B. ARP poisoning
C. Distributed DoS
D. Unknown threats

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 523
An administrator is concerned about the amount of time it would take to investigate email that may be subject to inspection during legal proceedings. Which of the following could help limit the company's exposure and the time spent on these types of proceedings?

A. Adjust user access rights assignments
B. Decentralize email servers
C. Encrypting email transmissions
D. Storage and retention policies

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 524
Which of the following BEST controls traffic between networks?

A. Firewall
B. HIPS
C. NIDS
D. Access point

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 525
Which of the following should be updated whenever software is upgraded on a production system?

A. Antivirus
B. Baseline
C. Group policy
D. LDAP entry

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 526
Which of the following BEST describes what users are required to provide in a two factor authentication system?

A. Two distinct items from one of the authentication factor groups.
B. Two distinct items they know from the same authentication factor group.
C. Two distinct items from each of the authentication factor groups.
D. Two distinct items from distinct categories of authentication factor groups.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 527
A user reports that they opened an attachment from an email received through a distribution list. At a later date, several computers started behaving abnormally. Which of the following threats has MOST likely infected the computer?

A. Logic bomb
B. Pop-ups
C. Spam
D. Spyware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 528
Which of the following describes the role of a proxy server?

A. Forwards requests for services from a client
B. Serves as a honeypot
C. Analyzes packets
D. Blocks access to the network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 529
Which of the following would a security administrator use to perform vulnerability scanning without doing any penetration testing?

A. Logic bombs
B. Protocol analyzer
C. Brute force

D. SQL injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 530
Which of the following are BEST practices in regards to backup media? (Select TWO).

A. Format tapes annually.
B. Store tapes near the servers.
C. Keep the tapes user accessible.
D. Label the media.
E. Store backup's offsite.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 531
An administrator believes a user has more access to a financial application than they should. Which of the following policies would this MOST likely violate?

A. Storage and retention
B. Group policy
C. User rights assignment
D. Server configuration policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 532
Which of the following security applications is used to mitigate malware?

A. HIDS

B. Anti-spam
C. Personal firewall
D. Anti-spyware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 533
Which of the following BEST describes the use of geographically distinct nodes to flood a site or sites with an overwhelming volume of network traffic?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 534
Which of the following cryptographic algorithms would be the MOST secure choice for encrypting email?

A. TKIP
B. AES
C. 3DES
D. PGP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 535
Which of the following security concerns stem from the use of corporate resources on cell phones? (Select TWO).

A. There is no antivirus software for cell phones.
B. Cell phones are easily lost or stolen.
C. Cell phones are used for P2P gaming.
D. MITM attacks are easy against cell phones.
E. Encryption on cell phones is not always possible.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 536
Which of the following is a best practice for managing user accounts?

A. Use the most privilege rule to grant access to senior users.
B. Assign users to all groups in order to avoid access problems.
C. Notify account administrators when a user leaves or transfers.
D. Lock out user accounts while the user is on extended leave.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 537
A new software application is designed to interact with the company's proprietary devices. Systems where the software is installed can no longer connect to the devices. Which of the following should the administrator do FIRST?

A. Consult the firewall logs for blocked process threads or port communication.
B. Verify that the devices are not rogue machines and blocked by network policy.
C. Check the antivirus definitions for false positives caused by the new software.
D. Ensure that the software is compliant to the system's host OS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 538
A cipher lock system is which of the following security method types?

A. Biometrics
B. Proximity reader
C. Man-trap design
D. Door access

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 539
Which of the following should be done if a USB device is found in a parking lot?

A. Turn it in to the appropriate security person.
B. Reformat it for personal use at home.
C. Plug it in to a computer to see who it belongs to.
D. Call the manufacturer of the USB device.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 540
Which of the following tools is MOST commonly used to assess a system's network for a security audit?

A. Vulnerability scanner
B. Password cracker
C. Protocol analyzer
D. Physical security control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 541
The company's new administrative assistant wants to use their name as a password and asks if it is appropriate. Which of the following is the BEST reason for not allowing this?

A. It will require too much time to conduct due diligence.
B. Change management approval has not been granted.
C. The password risks disclosure of Personally Identifiable Information (PII).
D. The proposed password does not meet complexity requirements.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 542
Which of the following happens to a risk when a company buys insurance to mitigate that risk?

A. Acceptance
B. Elimination
C. Transference
D. Avoidance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 543
A user is issued a new smartcard that stores both their new private and public key. Now the user is unable to open old encrypted emails. Which of the following needs to be completed to resolve the issue?

A. Restore old private key from the RA
B. Revoke the new private key
C. Restore old public key from the RA
D. Old encrypted email needs to be resent

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 544
Which of the following describes the characteristic of an anomaly-based IDS?

A. Sending an alert when suspicious activity has been prevented from entering the network.
B. Sending an alert only when a pre-specified pattern is observed.
C. Comparing traffic and sending an alert when it differs from historical patterns.
D. Detecting traffic for specific patterns of misuse and sending an alert for each incident.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 545
Which of the following can assesses threats in non-encrypted traffic?

A. Proxy server
B. Firewall
C. NIDS
D. Internet content filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 546
Which of the following would be used for authentication in Active Directory?

A. RAS

B. Kerberos
C. TACACS
D. PPTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 547
A security administrator works for a corporation located in a state with strict data breach disclosure laws. Compliance with these local legal regulations requires the security administrator to report data losses due to which of the following?

A. Hacking
B. Backup corruption
C. Power failures
D. Cryptography

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 548
Which of the following would be MOST useful for a security technician to run on a single, stand-alone machine with no network interface to verify its overall security posture?

A. Port scanner
B. Password cracker
C. Network mapper
D. Protocol analyzer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 549
A third party conducted an assessment of a company's network, which resulted in the company's website going offline. Which of the following MOST likely occurred?

A. Penetration testing took the system offline.
B. Password crackers were used and took the system offline.

C. Performance monitors were analyzing the network traffic and took the system offline.
D. Vulnerability scanners took the system offline.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 550
A user creates an archive of files that are sensitive and wants to ensure that no one else can access them. Which of the following could be used to assess the security of the archive?

A. Firewall
B. Port scanner
C. Protocol analyzer
D. Password cracker

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 551
Which of the following is the BEST way to restrict the GUI interface on a workstation?

A. Registry edits
B. Local policy
C. Group policy
D. Batch file

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 552
Proper planning for disaster recovery includes which of the following?

A. Executing the continuity plan at random
B. Testing the plan on a regular basis
C. Documenting all HDD serial numbers
D. Having system administrators electronically sign the plan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 553
Which of the following is the reason fiber optic cable is MORE secure than CAT5 cable?

A. It is harder to tap into.

B. Data is automatically encrypted.
C. It has heavier shielding.
D. It transmits signals faster.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 554
NIDS can be used to help secure a network from threats MOST effectively by watching network traffic in order to:

A. inspect and analyze data being passed through SSH tunnels.
B. verify adequate bandwidth is being provided for existing traffic.
C. observe if any systems are communicating using unauthorized protocols.
D. ensure proper password strength.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 555
A new administrative assistant starts with the company and tries to access the personnel file for the Vice President of Operations, but is denied. Which of the following BEST describes this access control method?

A. Least privilege
B. Implicit deny
C. Job rotation
D. Separation of privilege

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 556
Which of the following is considered the MOST secure replacement for telnet?

A. SSH
B. L2TP
C. SSL
D. IPSec

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 557
A technician completes a WLAN audit and notices that a number of unknown devices are connected. Which of the following can BEST be completed to mitigate the issue?

A. Replace the firewall
B. Replace the wireless access point
C. Change the SSID
D. Enable MAC filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 558
A NIPS is primarily used for which of the following purposes?

A. To take action against known threats
B. To log any known anomalies
C. To monitor network traffic in promiscuous mode
D. To alert the administrator to known anomalies

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 559
A disaster recovery exercise should include which of the following action types?

A. Enforcing change management
B. Testing server restoration
C. Creating a chain of custody
D. Testing the performance of each workstations UPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 560
Which of the following should a web application programmer implement to avoid SQL injection attacks?

A. Encryption and hashing

B. Session cookie handling
C. Proper input validation
D. Authentication and authorization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To protect against SQL injection, user input must not directly be embedded in SQL statements. Instead, parameterized statements must be used (preferred), or user input must be carefully escaped or filtered.

QUESTION 561
Which of the following would an auditor use to determine if an application is sending credentials in clear text?

A. Port scanner
B. Vulnerability scanner
C. Protocol analyzer
D. Rainbow table

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 562
After a recent viral intrusion, an administrator wishes to verify the servers functionality post-clean-up. The administrator should:

A. compare the systems performance against the configuration baseline.

B. install any hotfixes that may have been overlooked.
C. ensure that the antivirus applications definitions are up-to-date.
D. analyze the NIDS logs for any errant connections that may have been recorded.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 563
Which of the following security applications would an administrator use to help reduce the amount of bandwidth used by web browsing?

A. Personal software firewall
B. NIPS
C. HIDS
D. Proxy server

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 564
Which of the following contains a list of certificates that are compromised and invalid?

A. CA
B. TTP
C. CRL
D. RA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Certificate revocation is the process of revoking a certificate before it expires. A certificate may need to be revoked because it was stolen, an employee moved to a new company, or someone has had their access revoked. A certificate revocation is handled either through a Certificate Revocation List (CRL).

QUESTION 565
The last company administrator failed to renew the registration for the corporate web site (e.g.

https://www.comptia.org). When the new administrator tried to register the website it is discovered that the registration is being held by a series of small companies for very short periods of time. This is typical of which of the following?

A. DNS poisoning
B. Spoofing
C. TCP/IP hijacking
D. Domain name kiting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 566
Which of the following provides a security buffer, after passing through a firewall, by separating a network and still allowing access to that network?

A. NAC
B. NAT
C. DMZ
D. VLAN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 567
Which of the following should an administrator make sure is disabled or changed prior to putting a device node into a live environment?

A. Domain user accounts
B. Local user accounts
C. Remote user accounts
D. Default account

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 568
Which of the following is associated with a command and control system?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 569
Which of the following authentication methods is the MOST expensive to implement?

A. Username and password
B. Group policies
C. Biometric reader
D. Access Control List (ACL)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 570
Which of the following would be the BEST course of action to maintain network availability during an extended power outage?

A. Use multiple servers for redundancy

B. Install UPS units on each critical device
C. Implement a SONET ring
D. Install backup generators

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 571
Which of the following events are typically written to system logs?

A. Service startup
B. DNS zone transfers
C. Web GET requests
D. Database usage

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 572
Which of the following is provided at a cold site?

A. Live redundant computers, network connections and UPS
B. Active network jacks
C. New equipment ready to be installed
D. Fully operational equipment and installed network equipment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 573
Which of the following allows an attacker to join a network and view traffic on the network by physical connection?

A. Firewall
B. IPS
C. Vampire tap
D. IDS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 574
Which of the following is a goal of penetration testing?

A. Provide a passive check of the networks security
B. Passively assess web vulnerabilities
C. To check compliance of the router configuration
D. Actively assess deployed security controls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 575
A technician wants to make sure all users in the network are in compliance with company standards for login. Which of the following tools can the technician use?

A. Password crackers
B. Network mapping software
C. Digital signatures
D. Performance baselines

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 576
Which of the following would a security administrator be MOST likely to use if a computer is suspected of continually sending large amounts of sensitive data to an external host?

A. Honeypot
B. Protocol analyzer
C. Performance baseline
D. Virus scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 577
Which of the following security protocols could be configured to use EAP when connecting to a wireless access point?

A. WPA2-enterprise

B. RADIUS
C. IPSec
D. WPA-personal/TKIP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 578
A single point of failure is a security concern primarily because it affects which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 579
An employee in the Human Resources department transfers to the Accounting department. The employee is given access to the accounting systems but no longer has access to the Human Resources systems. This is an example of which of the following security concepts?

A. Default accounts
B. Privilege escalation
C. Least privilege
D. Chain of custody

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 580
Which of the following symmetric encryption algorithms provides the HIGHEST key strength?

A. RSA
B. Elliptic curve
C. 3DES
D. AES

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 581
Which of the following encryption technologies is BEST suited for small portable devices such as PDA's and cell phones?

A. Elliptic curve
B. TKIP
C. AES192
D. PGP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 582
An administrator needs to ensure that all machines deployed to the production environment follow strict company guidelines. Which of the following are they MOST likely to use?

A. Vertical scans
B. Horizontal scans
C. Mandatory Access Control (MAC)
D. Security templates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 583
An attacker uses an account that allows read-only access to the firewall for checking logs and configuration files to gain access to an account that gives full control over firewall configuration. This type of attack is BEST known as:

A. privilege escalation.
B. exploiting a weak password.
C. exploiting a back door.
D. a man-in-the-middle attack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 584
Exploitation of the 5-day grace period for domain name registration is referred to as:

A. domain name service.
B. domain name poisoning.
C. domain name lookup.
D. domain name kiting.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 585
Which of the following audit types would a security administrator perform on the network to ensure each workstation is standardized?

A. Storage and retention policy
B. Group policy
C. User access and rights
D. Domain wide password policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 586
Which of the following defines the process and accounting structure for handling system upgrades and modifications?

A. Change management
B. Service level agreement
C. Loss control
D. Key management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 587
Which of the following security applications would be MOST useful to traveling employees? (Select THREE).

A. NIDS
B. Anti-spam
C. NIPS
D. External corporate firewall
E. Personal software firewall
F. Antivirus

Correct Answer: BEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 588
Which of the following poses the GREATEST risk of data leakage?

A. 802.1x
B. BIOS
C. Thin client
D. USB drive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 589
A company wants a security technician to make sure that users cannot use common words for their passwords. Which of the following can the technician implement? (Select TWO).

A. Two factor authentication
B. Single sign-on
C. Complex passwords
D. Logical tokens
E. Group policies

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 590
An administrator wants to make sure that network machines stay up-to-date with current solutions, which of the following should be done on a regular basis to help facilitate this need?

A. Driver updates
B. Group policy updates
C. Patch management
D. Configuration baselines

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 591
A rainbow table is used for which of the following?

A. Password cracking
B. Cryptographic hashing
C. Single sign-on
D. Protocol analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 592
Which of the following does an attacker with minimal rights need to accomplish to continue attacking a compromised system?

A. Privilege escalation
B. Logic bomb
C. Cross-site scripting
D. Rootkit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 593
Which of the following would MOST likely monitor user web traffic?

A. Enable cookie monitoring
B. Enable Internet history monitoring
C. A proxy server
D. A software firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 594
Regression testing and deployment are part of the:

A. patch management process.
B. least privilege principle.
C. disaster recovery process.
D. vulnerability assessment process.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 595
When developing a new firewall policy, which of the following methods provides the MOST secure starting point?

A. Due diligence
B. Least privilege
C. Stateful inspection
D. Implicit deny

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Implicit deny means that the firewall only permits the specific needed applications to pass through the firewall, and everything else is denied.

QUESTION 596
A security administrator wants to implement a more secure way to login to a VPN in addition to a username and password. Which of the following is the MOST secure way to log in to a VPN?

A. Implementing an ACL
B. Setting up two VPNs
C. Implementing a single sign on process
D. Setting up a PKI

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 597
Which of the following is a component of a disaster recovery plan for a company that expects a site to be rendered non-usable during a disaster and needs a nearly transparent transfer of operations?

A. Alternate site
B. Hot site
C. Warm site
D. Cold site

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 598
Which of the following tools will detect protocols that are in use?

A. DMZ
B. Port scanner
C. Spoofing
D. Proxy server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 599
Which of the following does file encryption protect?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 600
Which of the following security concepts is supported by shielding?

A. Reliability
B. Portability
C. Availability
D. Confidentiality

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 601
Which of the following technologies address key management?

A. Advanced encryption standard
B. Diffie-Hellman
C. Blowfish
D. Digital signature algorithm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 602
Which of the following security applications can be implemented to mitigate port scanning attacks from the Internet?

A. Pop-up blockers
B. Antivirus software
C. Patch management software
D. Personal software firewalls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 603
Which of the following allows remote access servers to authenticate to a central server?

A. WLAN properties
B. RADIUS
C. Password authentication
D. Authentication protocols

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 604
Key escrow is the process of:

A. removing the private key.

B. backing up the key to local storage.
C. entrusting the keys to a third party.
D. removing the public key.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A key escrow system stores keys for the purpose of law enforcement access. One of the proposed methods of dealing with key escrow involves the storage of key information with a third party, referred to as a key escrow agency .

QUESTION 605
A user reports that they can no longer access the accounting share drive. That user was moved to the Finance department but still needs access to the accounting share drive. Which of the following actions should an administrator MOST likely do?

A. Add the user to the correct security group
B. Provide the user with full access rights to that shared drive
C. Add the user to the correct distribution group
D. Give that specific user rights to the shared drive

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 606
A security administrator reassembles the output of a captured TCP stream to diagnose problems with a web server. Which of the following is the administrator MOST likely using?

A. Port scanner
B. Replay attack
C. Protocol analyzer
D. Session hijacking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 607
Which of the following system security threats negatively affects confidentiality?

A. Adware
B. Spyware
C. Worm
D. Spam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 608
Which of the following is MOST likely the reason why a security administrator would run a Wire shark report on an important server?

A. To detect files that have been altered during downloads
B. To enumerate and crack weak system passwords

C. To analyze packets and frames
D. To decrypt WEP traffic and keys

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 609
A security flaw in an operating system allows backdoor access into the system. The operating system vendor releases a solution quickly outside of its normal update cycle.
Which of the following has the vendor released?

A. Patch
B. Cookies
C. Hotfix
D. Service pack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 610
Which of the following security controls would a company use to verify that their confidential and proprietary data is not being removed?

A. Chain of custody
B. Vulnerability scanners
C. Man traps
D. Video surveillance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 611
Which of the following stores information with a trusted agent to decrypt data at a later date, even if the user destroys the key?

A. Key escrow
B. Recovery agent
C. Public trust model
D. Key registration

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Recovery Agent key recovers data encrypted to a key that no longer exists.

Incorrect answer:
The key held in escrow will not recover data for if the key is destroyed (see CRL).

QUESTION 612
Rainbow tables are primarily used to expose which of the following vulnerabilities?

A. Available IP addresses
B. Available ports
C. Weak encryption keys
D. Weak passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 613
Which of the following is the BEST reason why a security administrator should periodically get a list of current employees and positions from the Human Resource department?

A. To immediately create accounts for new employees
B. To update the employee directory with new offices and phone numbers
C. To ensure all users have the appropriate access
D. To disable the accounts of employees who have move to a different department

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 614
Which of the following will MOST likely block known network attacks?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 615
Which of the following network security devices is the BEST to use when increasing the security of an entire network, or network segment, by preventing the transmission of malicious packets from known attacking sources?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 616
A company sets up wireless access points for visitors to use wireless devices. Which of the following encryption methods should they implement to provide the highest level of security?

A. WPA2
B. WPA
C. WEP

D. SHA-256

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 617
In the past several weeks, there have been an increased amount of failed remote desktop login attempts from an external IP address. Which of the following ports should the administrator change from its default to control this?

A. 25
B. 4658
C. 21
D. 3389

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 618
If an administrator wanted to be able to identify exactly which Internet sites are being accessed most frequently, which of the following tools would MOST likely be used?

A. IDS
B. Port scanner
C. Firewall
D. Proxy server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 619
The network administrator has been tasked with creating a VPN connection to a vendors site. The vendor is using older equipment that does not support AES. Which of the following would be the network administrators BEST option for configuring this link?

A. PGP
B. 3DES
C. DES
D. One time pad

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 620
Which of the following might be referenced to determine if a server is functioning abnormally?

A. Performance baseline
B. Chain of custody
C. Video surveillance
D. Protocol analyzer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 621
A SQL database MOST likely implements which of the following access security mechanisms?

A. Biometrics
B. Domain password policy
C. Discretionary access control
D. Mandatory access control

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 622
The IPSec authentication header provides which of the following?

A. Integrity protection
B. Payload encryption
C. End-point confidentiality
D. Payload compression

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 623
In evaluating risk assessments, senior level managers would MOST likely accept a risk based on which of the following reasons?

A. Physical security measures will take weeks to install
B. Cost of mitigation outweighs the risk
C. The potential impact of the risk is easily mitigated
D. Complexity of fixing the vulnerability

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 624
A web server that the employees use to fill out their time cards needs to be protected. The web server needs to be accessible to employees both inside the campus and at remote sites. Some of the employees use computers that do not belong to the company to do their work. Which of the following would BEST protect the server?

A. Place the server in a DMZ after hardening the OS.
B. Place the server in a subnet that is blocked at the firewall.
C. Place the server in a DMZ and require all users to use the company's VPN software to access it.
D. Require all users to use a PKI token stored on a physical smart card to authenticate to the server.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 625

The technical user group has read and writes access to a network share. The executive user group has full control of the same network share. A user is a member of both groups. Which of the following BEST describes the user's permissions on the share?

A. The user is able to modify, write and delete documents in network share.
B. The user is able to modify and write documents in network share.
C. The user is able to modify, write, delete and read documents in network share.
D. The user is able to write and read documents in the network share.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 626
An administrator wants to make sure that all users of a large domain are restricted from installing software. Which of the following should MOST likely be done?

A. All workstations are rebuilt
B. A security IP audit is completed
C. A security policy template is implemented
D. Administrative rights are manually removed

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 627
An important file has been deleted off the departments file server. Management would like to know who was responsible for deleting the file. Which of the following log files can be used to inform management of the answer?

A. The access logs on the server and then the system logs on the workstation.
B. The system logs on the server and then the access logs on the workstation.
C. The access logs on the server and then the access logs on the workstation.
D. The application logs on the server and then the access logs on the workstation.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 628
Which of the following is consistent with the least privilege best practice?

A. Deploying privileged users accounts to all department managers
B. Restricting user permissions so only one person can print
C. Restricting administrator permissions to the smallest amount of staff possible

D. Enforcing physical access controls so no one can enter the data center

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 629
Modern cell phones present a security risk to corporate networks because of which of the following?

A. Cell phones are vulnerable to logic bombs.
B. Cell phone signals interfere with fiber networks.
C. Cell phones can be used to spread computer viruses.
D. It is difficult to push security policies to cell phones.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 630
Which of the following is a weakness of single sign-on?

A. Multiple points of entry into the network
B. A single point of failure on the network
C. Increased overhead for server processing
D. Requirement to remember one password

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 631
A user reports random windows opening and closing after installing new software. Which of the following has MOST likely infected the computer?

A. Spam
B. Adware
C. Rootkit
D. Worm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 632
Which of the following is MOST likely the reason why a security administrator would run a NMAP report on an important server?

A. To capture network packets for analysis
B. To determine open ports and services
C. To correlate which MAC addresses are associated with a switch port
D. To identify vulnerabilities in available services

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 633
Which of the following RAID types would be implemented for disk mirroring?

A. RAID 3
B. RAID 1
C. RAID 5
D. RAID 0

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 634
Which of the following tools is BEST suited to determine if an IDS has triggered a false positive?

A. Port scanner
B. Netflow collector
C. Network mapper
D. Protocol analyzer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 635
Which of the following techniques embeds an encrypted message within the bits of an image file?

A. Proxy avoidance
B. Steganography
C. Cipher-text attack
D. Cryptographic hashing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 636
A user can no longer access the Internet from their laptop. A technician checks the computer and realizes that it is sending out spam messages throughout the company. The computer is MOST likely the victim of which of the following security threats?

A. XSS
B. Botnet
C. DOS
D. Virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 637
Which of the following will allow a technician to restrict access to one folder within a shared folder?

A. IPSec
B. NTLMv2
C. NTLM
D. NTFS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 638
Which of the following is used to verify if internal web servers are redirecting traffic to a malicious site?

A. IDS
B. Access logs
C. DNS record
D. Performance logs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 639
A user from the accounting department is in the Customer Service area and tries to connect to the file server

through their laptop, but is unable to access the network. The network administrator checks the network connection and verifies that there is connectivity. Which of the following is the MOST likely cause of this issue?

A. Wrong VLAN
B. File server is not on the DMZ
C. IPS has blocked access
D. NAT is not properly configured

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 640
Which of the following allows the administrator to verify a file is the same as the original?

A. 3DES
B. AES
C. MD5
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 641
In order to closely monitor and detect suspicious activity on a single server, which of the following should be used?

A. Group policies
B. NIDS
C. Software firewall
D. HIDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 642
Which of the following are the MOST critical resources needed during Disaster Recovery Plan development? (Select TWO).

A. Data owners
B. Commercial vendors
C. End users

D. Customers
E. System administrators

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 643
Which of the following describes what has occurred after a user has successfully gained access to a secure system?

A. Authentication
B. Authenticity
C. Identification
D. Confidentiality

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 644
A network administrator was recently promoted from their former position as a server administrator and now can no longer log on to servers they previously supported. This is an example of:

A. job rotation.
B. single sign on.
C. separation of duties.
D. implicit deny.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 645
An administrator is required to keep certain workstations free of malware at all times, but those workstations need to be able to access any Internet site. Which of the following solutions would be the BEST choice?

A. Personal firewall
B. Pop-up blockers
C. Updated anti-spam software
D. Updated antivirus software

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:
The best initial protection against malicious code is antivirus software. Reference: CompTIA Secutiy+ Deluxe Study Guide, p. 492.

QUESTION 646
The security administrator is investigating a breach of the company's web server. One of the web developers had posted valid credentials to a web forum while troubleshooting an issue with a vendor. Logging which of the following would have created the BEST way to determine when the breach FIRST occurred? (Select TWO).

A. Source IP
B. Successful login
C. Source OS
D. Destination IP
E. Unsuccessful login
F. Number of hops from source

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 647
One of the company's sales representatives had been working as the accounts payable representative while that associate was out on leave. The accounts payable representative has returned and now the sales representative is unable to access the files on the accounting server. Which of the following BEST describes the access control method used to limit access to the accounting server?

A. Job rotation
B. Separation of duties
C. Implicit deny
D. Least privilege

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 648
Which of the following BEST describes why USB storage devices present a security risk to the confidentiality of data?

A. High raw storage capacity combined with wireless transfer capability.
B. High volume and transfer speeds combined with ease of concealment.
C. Ability to remotely install keylogger software and bypass network routing.
D. Slow data transfer speeds combined with ease of concealment.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 649
Which of the following methods allows the administrator to create different user templates to comply with the principle of least privilege?

A. Role-based access control
B. Rule-based access control
C. Physical access control
D. Mandatory access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 650
Which of the following would be used to send an encrypted email?

A. SSH
B. PPTP
C. S/MIME
D. LT2P

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 651
Disabling the SSID broadcast removes the identifier from which of the following wireless packets?

A. ACK
B. Data
C. Beacon
D. Probe

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 652
After a disaster, a security administrator is helping to execute the company disaster recovery plan. Which of the following security services should be restored FIRST?

A. Authentication mechanisms for guests.

B. New user account creation services.
C. Auditing and logging of transactions.
D. Help desk phones and staffing.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 653
A new application support technician is unable to install a new approved security application on a departments workstation. The security administrator needs to do which of the following?

A. Add that user to the local power users group
B. Add that user to the domain administrators group
C. Add that user to the domain remote desktop group
D. Add that user to the security distribution group

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 654
A call center uses 50 remote representatives to handle calls for clients. The representatives run software based IP phones on their laptops, and connect back to the call center over the Internet. However, one of the representatives reports that they can no longer connect to the call center PBX. Which of the following is the reason that only this call center representative is unable to connect to the PBX?

A. The representative has a disk defragmentation program installed.
B. The call center has recently installed HIDS.
C. The call center has placed the firewall on the edge of the network.
D. The representative has a mis-configured software firewall.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 655
Which of the following is a best practice relating to non-administrative user rights on a server?

A. Deny file access
B. Deny local logon
C. Deny network logon
D. Deny printer access

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 656
A technician places a network jack in the parking garage for administrative use. Which of the following can be used to mitigate threats from entering the network via this jack?

A. Install wireless access points
B. Replace CAT5 with CAT6 plenum
C. Disable ports when not in use
D. Install a firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 657
Which of the following redundancy planning concepts is generally the LEAST expensive?

A. Cold site
B. Hot site
C. Mobile site
D. Warm site

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 658
Which of the following is true about the application of machine virtualization?

A. Machine virtualization is only possible in a 64-bit environment.
B. Virtualization hosting is only possible on one specific OS.
C. Some malware is able to detect that they are running in a virtual environment.
D. The virtualization host OS must be within two revisions of the guest OS.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 659
Which of the following is able to detect that a local system has been compromised?

A. NIDS

B. Anti-spam
C. HIDS
D. Personal firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 660
Which of the following logs contains user logons and logoffs?

A. Security
B. DNS
C. Application
D. System

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 661
Which of the following would MOST likely determine which user inadvertently shut down the Company's web server?

A. Application logs
B. Performance logs
C. Access logs
D. DNS logs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 662
Which of the following is a tactic used by malicious domain purchasing organizations?

A. Kiting
B. DNS
C. DDoS
D. ARP spoofing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 663
Which of the following logs would MOST likely indicate that there is an ongoing brute force attack against a servers local administrator account?

A. Access
B. System
C. Performance
D. Firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 664
Which of the following is the MOST secure condition a firewall should revert to when it is overloaded with network traffic?

A. Fail danger
B. Fail open
C. Fail safe
D. Fail closed

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 665
Which of the following BEST describes when code that is initiated on a virtual machine directly affects the host?

A. VM hardware abstraction
B. VM hypervisor
C. VM escape
D. VM cluster

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 666
Users report that websites are loading slowly. Which of the following web proxy logs is MOST likely to help a system administrator identify the cause for slow web traffic?

A. System

B. Access
C. Performance
D. Security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 667
Which of the following will help hide the IP address of a computer from servers outside the network?

A. ACL
B. PAT
C. NAT
D. NAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 668
The director of security for a company needs to determine how the security and network administrators would respond to a compromised system. Which of the following would be the BEST way for the director to test the teams response?

A. Vulnerability scan
B. Penetration test
C. Port scan
D. Social engineering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 669
Which of the following describes an attack where a person searches for open access points?

A. Weak SSID
B. War driving
C. Rogue access point
D. WEP

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 670
Which of the following is used to encrypt the data sent from the server to the browser in an SSL session?

A. Public key
B. Asymmetric encryption
C. Symmetric encryption

D. Private key

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 671
A user contacts technical support stating they received notification in a web browser that their computer is infected with a virus. Which of the following would help prevent this in the future?

A. Spam blocker
B. Pop-up blocker
C. Anti-Spyware
D. Antivirus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 672
A factory fresh install has just been completed on a computer. Which of the following should be done FIRST once the computer is connected to the network?

A. Modify group policies.
B. Establish a baseline.
C. Install OS updates.
D. Install application patches.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 673
A user reports that they are seeing ads appear for sites that are not safe for work while they are reading blogs. Which of the following would be the BEST way to solve this issue?

A. Provide a second web browser for reading the blogs.
B. Install and configure a pop-up blocker on the workstation.
C. Update the Acceptable Use Policy (AUP).
D. Deploy HIDS to the workstation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 674
One of the primary purposes of virtualization in a data center is to reduce which of the following?

A. Amount of application logging required for security
B. Number of logical hosts providing services for users
C. Total complexity of the overall security architecture
D. Volume of physical equipment needing to be secured

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 675
Which of the following technologies can be used as a means to isolate a host OS from some types of security threats?

A. Virtualization
B. Intrusion detection
C. Cloning
D. Kiting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 676
Which of the following combinations of items would constitute a valid three factor authentication system?

A. PIN, password, and a thumbprint
B. Password, retina scan, and a one-time token
C. Fingerprint, retina scan, and a hardware PKI token
D. PKI smartcard, password and a one-time token

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 677
Which of the following is a valid two-factor authentication model?

A. Smartcard and hardware token
B. Retina scan and palm print
C. Iris scan and user password
D. User password and user PIN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 678
Which of the following allows an attacker to use a company's email server to distribute spam?

A. Instant messaging
B. Buffer overflow
C. Cross-site scripting
D. Open relay

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 679
At midnight on January 1st, an administrator receives an alert from the system monitoring the servers in the datacenter. All servers are unreachable. Which of the following is MOST likely to have caused the DOS?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Logic bombs are programs or snippets of code that execute when a certain predefined event occurs. Logic bombs may also be set to go off on a certain date or when a specified set of circumstances occurs.

QUESTION 680

In the event of a disaster resulting in the loss of their data center, a company had determined that they will need to be able to be back online within the next day, with some systems. Which of the following would BEST meet their needs?

A. A hot backup site
B. A warm backup site
C. A spare set of servers stored in the data center
D. A cold backup site

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 681
Which of the following logs would a system administrator scan to reveal names and IP addresses of all websites visited by a company's employees?

A. DHCP logs
B. Security log
C. DNS logs
D. Firewall logs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 682
Which of the following is of the GREATEST concern when using a biometric reader?

A. True positives
B. False positives
C. True negatives
D. False negatives

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 683
Which of the following is the process by which encryption keys are distributed?

A. User access and rights review
B. Key escrow
C. Key management

D. Trusted Platform Module (TPM)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 684
Which of the following is the process of trying to locate unsecured wireless networks?

A. War driving
B. Net hacking
C. Spoofing
D. War dialing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 685
Which of the following protocols allows a user to selectively encrypt the contents of an email message at rest?

A. Secure SMTP
B. S/MIME
C. SSL/TLS
D. Digital signature

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 686
Which of the following is the purpose of key escrow in a PKI system?

A. Ensures the security of public keys by storing the keys confidentially
B. Ensures that all private keys are publicly accessible to PKI users
C. Provides a system for recovering encrypted data when public keys are corrupted
D. Provides a system for recovering encrypted data even if the users lose private keys

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 687
In order for an organization to be successful in preventing fraud from occurring by a disgruntled employee,

which of the following best practices should MOST likely be in place?

A. Least privilege
B. Job rotation
C. Separation of duties
D. Access controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 688
Which of the following is MOST likely to occur if the input of a web form is not properly sanitized? (Select TWO).

A. Backend file system crash
B. Cross-site scripting
C. SQL injection
D. Web load balancing
E. Logic bomb

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 689
A user loses a USB device containing credit card numbers. Which of the following would BEST protect the data?

A. Password protection which destroys data on the device after 12 incorrect attempts
B. Password protection which destroys data on the device after 10 incorrect attempts
C. Encryption of the device with the key stored elsewhere
D. Encryption of the laptop to which the device is connected

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 690
An auditor would use credentials harvested from a SQL injection attack during which of the following?

A. Penetration test
B. Vulnerability assessment
C. Password strength audit
D. Forensic recovery

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 691
Which of the following uses a trusted third party key distribution center to generate authentication tokens?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 692
Which of the following should be performed during a forensic evaluation?

A. Power off the system.
B. Establish chain of custody.
C. Troubleshoot system performance.
D. Update virus definitions.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 693
Which of the following actions is an employee able to take if they are given administrative access to a workstation?

A. Installing applications, creating local user accounts, and modifying any accounts on the domain.
B. Upgrading the operating system, creating local user accounts, and modifying any accounts on the system.
C. Upgrading the operating system, creating local user accounts, and modifying accounts on the network.
D. Installing applications on remote systems, creating local user accounts, and modifying accounts they created.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 694
Which of the following behavioral biometric authentication models should a technician deploy in a secure datacenter?

A. Retina scan
B. Fingerprint recognition
C. Voice recognition
D. Iris scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 695
Which of the following prevents unsolicited email messages from entering the company's network?

A. Anti-spyware
B. Pop-up blockers
C. Anti-spam
D. Antivirus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 696
Which of the following technologies is used to verily that a file was not altered?

A. RC5
B. AES
C. DES
D. MD5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 697
Which of the following is an example of a smart card?

A. PIV
B. MAC
C. One-time passwords
D. Tokens

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 698
The security administrator wants to know if a new device has any known issues with its available applications. Which of the following would be BEST suited to accomplishing this task?

A. Network mapper
B. Port scanner
C. Protocol analyzer
D. Vulnerability scanner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 699
A technician completes a WLAN audit and notices that a number of unknown devices are connected. Which of the following can BEST be completed to mitigate the issue?

A. Replace the firewall
B. Replace the wireless access point
C. Change the SSID
D. Enable MAC filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 700
An auditor would use credentials harvested from a SQL injection attack during which of the following?

A. Penetration test
B. Vulnerability assessment
C. Password strength audit
D. Forensic recovery

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: