PrepKing

Number: SY0-201
Passing Score: 800
Time Limit: 120 min
File Version: 8.0

PrepKing SY0-201

Exam A

QUESTION 1
All of the following provide confidentiality protection as part of the underlying protocol EXCEPT:

A. SSL.
B. SSH.
C. L2TP.
D. IPSeC.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following allows an attacker to manipulate files by using the least significant bit(s) to secretly embed data?

A. Steganography
B. Worm
C. Trojan horse
D. Virus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following type of attacks would allow an attacker to capture HTTP requests and send back a spoofed page?

A. Teardrop
B. TCP/IP hijacking
C. Phishing
D. Replay

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
How should a company test the integrity of its backup data?

A. By conducting another backup
B. By using software to recover deleted files
C. By restoring part of the backup

D. By reviewing the written procedures

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of following can BEST be used to determine the topology of a network and discover unknown devices?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
When should a technician perform penetration testing?

A. When the technician suspects that weak passwords exist on the network
B. When the technician is trying to guess passwords on a network
C. When the technician has permission from the owner of the network
D. When the technician is war driving and trying to gain access

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
An administrator has implemented a new SMTP service on a server. A public IP address translates to the internal SMTP server. The administrator notices many sessions to the server, and gets notification that the servers public IP address is now reported in a spam real-time block list.Which of the following is wrong with the server?

A. SMTP open relaying is enableD.
B. It does not have a spam filter.
C. The amount of sessions needs to be limiteD.

D. The public IP address is incorrect.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following is MOST efficient for encrypting large amounts of data?

A. Hashing algorithms
B. Symmetric key algorithms
C. Asymmetric key algorithms
D. ECC algorithms

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following is a reason why a company should disable the SSID broadcast of the wireless access points?

A. Rogue access points
B. War driving
C. Weak encryption
D. Session hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following BEST describes ARP?

A. Discovering the IP address of a device from the MAC address
B. Discovering the IP address of a device from the DNS name
C. Discovering the MAC address of a device from the IP address
D. Discovering the DNS name of a device from the IP address

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11

Which of the following would be BEST to use to apply corporate security settings to a device?

A. A security patch
B. A security hotfix
C. An OS service pack
D. A security template

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
A small call center business decided to install an email system to facilitate communications in the office.
As part of the upgrade the vendor offered to supply anti-malware software for a cost of $5,000 per year. The IT manager read there was a 90% chance each year that workstations would be compromised if not adequately protecteD. If workstations are compromised it will take three hours to restore services for the 30 staff. Staff members in the call center are paid $90 per hour. If the anti-malware software is purchased,
which of the following is the expected net savings?

A. $900
B. $2,290
C. $2,700
D. $5,000b

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is the main objective of steganography?

A. Message digest
B. Encrypt information
C. Hide information
D. Data integrity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following would allow for secure key exchange over an unsecured network without a pre-shared key?

A. 3DES
B. AES

C. DH-ECC
D. MD5

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following improves security in a wireless system?

A. IP spoofing
B. MAC filtering
C. SSID spoofing
D. Closed network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A user wants to implement secure LDAP on the network. Which of the following port numbers secure LDAP use by default?

A. 53
B. 389
C. 443
D. 636

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
On which of the following is a security technician MOST likely to find usernames?

A. DNS logs
B. Application logs
C. Firewall logs
D. DHCP logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
How many keys are utilized with asymmetric cryptography?

A. One
B. Two
C. Five
D. Seven

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
During a risk assessment it is discovered that only one system administrator is assigned several tasks critical to continuity of operations. It is recommended to cross train other system administrators to perform these tasks and mitigate which of the following risks?

A. DDoS
B. Privilege escalation
C. Disclosure of PII
D. Single point of failure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following network filtering devices will rely on signature updates to be effective?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following is a single server that is setup in the DMZ or outer perimeter in order to distract attackers?

A. Honeynet
B. DMZ
C. Honeypot

D. VLAN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following encryption algorithms is decrypted in the LEAST amount of time?

A. RSA
B. AES
C. 3DES
D. L2TP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
An administrator is trying to secure a network from threats originating outside the network. Which of the following devices provides protection for the DMZ from attacks launched from the Internet?

A. Antivirus
B. Content filter
C. Firewall
D. Proxy server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following is a way to manage operating system updates?

A. Service pack management
B. Patch application
C. Hotfix management
D. Change management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25

Which of the following is a list of discrete entries that are known to be benign?

A. Whitelist
B. Signature
C. Blacklist
D. ACL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following increases the collision resistance of a hash?

A. Salt
B. Increase the input length
C. Rainbow Table
D. Larger key space

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A programmer has decided to alter the server variable in the coding of an authentication function for a proprietary sales application. Before implementing the new routine on the production application server, which of the following processes should be followed?

A. Change management
B. Secure disposal
C. Password complexity
D. Chain of custody

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
When deploying 50 new workstations on the network, which of following should be completed FIRST?

A. Install a word processor.
B. Run the latest spywarE.
C. Apply the baseline configuration.
D. Run OS updates.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following should be implemented to have all workstations and servers isolated in their own broadcast domains?

A. VLANs
B. NAT
C. Access lists
D. Intranet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
End users are complaining about receiving a lot of email from online vendors and pharmacies.Which of the following is this an example of?

A. Trojan
B. Spam
C. Phishing
D. DNS poisoning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following BEST describes a private key in regards to asymmetric encryption?

A. The key owner has exclusive access to the private key.
B. Everyone has access to the private key on the CA.
C. Only the CA has access to the private key.
D. The key owner and a recipient of an encrypted email have exclusive access to the private key.
WBerlin
Sans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32

Which of the following logs might reveal the IP address and MAC address of a rogue device within the local network?

A. Security logs
B. DHCP logs
C. DNS logs
D. Antivirus logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is commonly used in a distributed denial of service (DDOS) attack?

A. Phishing
B. Adware
C. Botnet
D. Trojan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following practices is MOST relevant to protecting against operating system security flaws?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following is a best practice for coding applications in a secure manner?

A. Input validation
B. Object oriented coding
C. Rapid Application Development (RAD)
D. Cross-site scripting

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 36
Which of the following technologies can be used as a means to isolate a host OS from some types of security threats?

A. Intrusion detection
B. Virtualization
C. Kiting
D. Cloning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following network tools would provide the information on what an attacker is doing to compromise a system?

A. Proxy server
B. Honeypot
C. Internet content filters
D. Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Assigning proper security permissions to files and folders is the primary method of mitigating which of the following?

A. Hijacking
B. Policy subversion
C. Trojan
D. DoS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following logical access controls would be MOST appropriate to use when creating an account for a temporary worker?

A. ACL
B. Account expiration
C. Time of day restrictions
D. Logical tokens

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following may be an indication of a possible system compromise?

A. A port monitor utility shows that there are many connections to port 80 on the Internet facing web server.
B. A performance monitor indicates a recent and ongoing drop in speed, disk space or memory utilization from the baselinE.
C. A protocol analyzer records a high number of UDP packets to a streaming media server on the Internet.
D. The certificate for one of the web servers has expired and transactions on that server begins to drop rapidly.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
An administrator suspects that files are being copied to a remote location during off hours. The file server does not have logging enableD. Which of the following logs would be the BEST place to look for information?

A. Intrusion detection logs
B. Firewall logs
C. Antivirus logs
D. DNS logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following access control methods gives the owner control over providing permissions?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following access control methods grants permissions based on the users position in the company?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following access control methods includes switching work assignments at preset intervals?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following authentication methods would MOST likely prevent an attacker from being able to successfully deploy a replay attack?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following would an attacker use to footprint a system?

A. RADIUS
B. Password cracker
C. Port scanner
D. Man-in-the-middle attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following ensures a user cannot deny having sent a message?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following allows an attacker to embed a rootkit into a picture?

A. Trojan horse
B. Worm
C. Steganography
D. Virus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following is a publication of inactivated user certificates?

A. Certificate revocation list
B. Certificate suspension
C. Recovery agent
D. Certificate authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following is a method of encrypting email?

A. S/MIME
B. SMTP
C. L2TP
D. VPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following risks would be reduced by implementing screen filters?

A. Replay attacks
B. Phishing
C. Man-in-the-middle attacks
D. Shoulder surfing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following allows an attacker to hide the presence of malicious code by altering the systems process and registry entries?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following will propagate itself without any user interaction?

A. Worm
B. Rootkit
C. Trojan
D. Virus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
An administrator wants to setup their network with only one public IP address. Which of the following would allow for this?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
An administrator wants to proactively collect information on attackers and their attempted methods of gaining access to the internal network. Which of the following would allow the administrator to do this?

A. NIPS
B. Honeypot
C. DMZ
D. NIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following allows a technician to correct a specific issue with a solution that has not been fully tested?

A. Patch
B. Hotfix
C. Security roll-up
D. Service pack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
A technician wants to regulate and deny traffic to websites that contain information on hacking.Which of the following would be the BEST solution to deploy?

A. Internet content filter
B. Proxy
C. Protocol analyzer
D. NIDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following is the LEAST intrusive way of checking the environment for known software flaws?

A. Protocol analyzer
B. Vulnerability scanner
C. Port scanner
D. Penetration test

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
If a certificate has been compromised, which of the following should be done?

A. Run the recovery agent.
B. Put the certificate on the CRL.
C. Put the certificate in key escrow.
D. Suspend the certificate for further investigation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following requires an update to the baseline after installing new software on a machine?

A. Signature-based NIPS
B. Signature-based NIDS
C. Honeypot
D. Behavior-based HIDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following would be the MOST secure choice to implement for authenticating remote connections?

A. LDAP
B. 8021x
C. RAS
D. RADIUS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following is the BEST way to reduce the number of accounts a user must maintain?

A. Kerberos
B. CHAP
C. SSO
D. MD5

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following can be used as a means for dual-factor authentication?

A. RAS and username/password
B. RADIUS and L2TP
C. LDAP and WPA
D. Iris scan and proximity card

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
After implementing file auditing, which of the following logs would show unauthorized usage attempts?

A. Performance
B. System
C. Security
D. Application

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following type of attacks requires an attacker to sniff the network?

A. Man-in-the-Middle
B. DDoS attack
C. MAC flooding
D. DNS poisoning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
If a user attempts to go to a website and notices the URL has changed, which of the following attacks is MOST likely the cause?

A. DLL injection
B. DDoS attack
C. DNS poisoning
D. ARP poisoning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following attacks can be caused by a user being unaware of their physical surroundings?

A. ARP poisoning
B. Phishing
C. Shoulder surfing

D. Man-in-the-middle

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which of the following actions should be performed upon discovering an unauthorized wireless access point attached to a network?

A. Unplug the Ethernet cable from the wireless access point.
B. Enable MAC filtering on the wireless access point.
C. Change the SSID on the wireless access point.
D. Run a ping against the wireless access point.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which of the following redundancy solutions contains hardware systems similar to the affected organization, but does not provide live data?

A. Hot site
B. Uninterruptible Power Supply (UPS)
C. Warm site
D. Cold site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
During the implementation of LDAP, which of the following will typically be changed within the organizations software programs?

A. IP addresses
B. Authentication credentials
C. Non-repudiation policy
D. Network protocol

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following would be MOST useful to determine why packets from a computer outside the network are being dropped on the way to a computer inside the network?

A. HIDS log
B. Security log
C. Firewall log
D. System log

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following security policies is BEST to use when trying to mitigate the risks involved with allowing a user to access company email via their cell phone?

A. The cell phone should require a password after a set period of inactivity.
B. The cell phone should only be used for company related emails.
C. The cell phone data should be encrypted according to NIST standards.
D. The cell phone should have data connection abilities disableD.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
An administrator has been asked to encrypt credit card datA. Which of the following algorithms would be the MOST secure with the least CPU utilization?

A. 3DES
B. AES
C. SHA-1
D. MD5

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following algorithms is the LEAST secure?

A. NTLM
B. MD5
C. LANMAN

D. SHA-1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following algorithms is MOST closely associated with the signing of email messages?

A. MD5
B. TKIP
C. PGP
D. SHA-1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
An executive uses PKI to encrypt sensitive emails sent to an assistant. In addition to encrypting the body of the email, the executive wishes to encrypt the signature so that the assistant can verify that the email actually came from the executive. Which of the following asymmetric keys should the executive use to encrypt the signature?

A. Public
B. Private
C. Shared
D. Hash

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
A technician needs to detect staff members that are connecting to an unauthorized website. Which of the following could be used?

A. Protocol analyzer
B. Bluesnarfing
C. Host routing table
D. HIDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
An administrator suspects that multiple PCs are infected with a zombie. Which of the following tools could be used to confirm this?

A. Antivirus
B. Recovery agent
C. Spyware
D. Port scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following is an example of security personnel that administer access control functions, but do not administer audit functions?

A. Access enforcement
B. Separation of duties
C. Least privilege
D. Account management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A malware incident has just been detected within a company. Which of the following should be the administrators FIRST response?

A. Removal
B. Containment
C. Recovery
D. Monitor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Taking into account personal safety, which of the following types of fire suppression substances would BEST prevent damage to electronic equipment?

A. Foam
B. CO2

C. Halon
D. Water

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following describes the process of securely removing information from media (E. g. hard drive) for future use?

A. Reformatting
B. Destruction
C. Sanitization
D. Deleting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following principles should be applied when assigning permissions?

A. Most privilege
B. Least privilege
C. Rule based
D. Role based

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following type of strategies can be applied to allow a user to enter their username and password once in order to authenticate to multiple systems and applications?

A. Two-factor authentication
B. Single sign-on
C. Smart card
D. Biometrics

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
User A is a member of the payroll security group. Each member of the group should have read/write permissions to a sharE. User A was trying to update a file but when the user tried to access the file the user was denieD. Which of the following would explain why User A could not access the file?

A. Privilege escalation
B. Rights are not set correctly
C. Least privilege
D. Read only access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following threats is the MOST difficult to detect and hides itself from the operating system?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following methods is used to perform denial of service (DoS) attacks?

A. Privilege escalation
B. Botnet
C. Adware
D. Spyware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following is an attack that is triggered by a specific event or by a date?

A. Logic bomb
B. Spam
C. Rootkit

D. Privilege escalation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following can an attacker use to gather information on a system without having a user ID or password?

A. NAT
B. DNS poisoning
C. Null session
D. Spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following is a way to logically separate a network through a switch?

A. Spanning port
B. Subnetting
C. VLAN
D. NAT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following is a security threat when a new network device is configured for first-time installation?

A. Attacker privilege escalation
B. Installation of a back door
C. Denial of Service (DoS)
D. Use of default passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92

Which of the following is an exploit against a device where only the hardware model and manufacturer are known?

A. Replay attack
B. Denial of service (DoS)
C. Privilege escalation
D. Default passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A technician is implementing a new wireless network for an organization. The technician should be concerned with all of the following wireless vulnerabilities EXCEPT:

A. rogue access points.
B. 80211 modE.
C. weak encryption.
D. SSID broadcasts.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Which of the following tools will allow the technician to find all open ports on the network?

A. Performance monitor
B. Protocol analyzer
C. Router ACL
D. Network scanner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
An organization is installing new servers into their infrastructurE. A technician is responsible for making sure that all new servers meet security requirements for uptimE. In which of the following is the availability requirements identified?

A. Service level agreement
B. Performance baseline
C. Device manufacturer documentation
D. Security template

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
After issuance a technician becomes aware that some keys were issued to individuals who are not authorized to use them. Which of the following should the technician use to correct this problem?

A. Recovery agent
B. Certificate revocation list
C. Key escrow
D. Public key recovery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Password crackers are generally used by malicious attackers to:

A. verify system access.
B. facilitate penetration testing.
C. gain system access.
D. sniff network passwords.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following properly describes penetration testing?

A. Penetration tests are generally used to scan the network and identify open ports.
B. Penetration tests are generally used to map the network and grab banners.
C. Penetration tests are generally used to exploit a weakness without permission and show how an attacker might compromise a system.
D. Penetration tests are generally used to demonstrate a weakness in a system and then provide documentation on the weakness.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following should a technician review when a user is moved from one department to another?

A. User access and rights
B. Data storage and retention policies
C. Users group policy
D. Acceptable usage policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following is a reason to implement security logging on a DNS server?

A. To monitor unauthorized zone transfers
B. To measure the DNS server performance
C. To perform penetration testing on the DNS server
D. To control unauthorized DNS DoS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which of the following can an attacker use to gather information on a system without having a user ID or password?

A. NAT
B. DNS poisoning
C. Null session
D. Spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
An organization is installing new servers into their infrastructurE. A technician is responsible for making sure that all new servers meet security requirements for uptimE. In which of the following is the availability requirements identified?

A. Service level agreement
B. Performance baseline
C. Device manufacturer documentation
D. Security template

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Exam B

QUESTION 1
A technician is rebuilding the infrastructure for an organization. The technician has been tasked with making sure that the virtualization technology is implemented securely. Which of the following is a concern when implementing virtualization technology?

A. The technician should verify that the virtual servers are dual homed so that traffic is securely separateD.
B. The technician should verify that the virtual servers and the host have the latest service packs and patches applieD.
C. The technician should subnet the network so each virtual server is on a different network segment.
D. The technician should perform penetration testing on all the virtual servers to monitor performancE.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A technician is reviewing the logical access control method an organization uses. One of the senior managers requests that the technician prevent staff members from logging on during non- working days.
Which of the following should the technician implement to meet managements request?

A. Enforce Kerberos
B. Deploy smart cards
C. Time of day restrictions
D. Access control lists

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
How would a technician implement a security patch in an enterprise environment?

A. Download the patch from the vendors secure website and install it on the most vulnerable workstation.
B. Download the patch from the vendors secure website, test the patch and install it on all workstations.
C. Download the patch from the vendors secure website and install it as neededD.
D. Download the patch from the Internet, test the patch and install it on all of the production servers.WBerlin Sans

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following is considered the weakest encryption?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following encryption schemes is the public key infrastructure based on?

A. Quantum
B. Elliptical curve
C. Asymmetric
D. Symmetric

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following BEST describes the term war driving?

A. Driving from point to point with a laptop and an antenna to find unsecured wireless access points.
B. Driving from point to point with a wireless scanner to read other users emails through the access point.
C. Driving from point to point with a wireless network card and hacking into unsecured wireless access points.
D. Driving from point to point with a wireless scanner to use unsecured access points.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following statements BEST describes the implicit deny concept?

A. Blocks everything and only allows privileges based on job description
B. Blocks everything and only allows explicitly granted permissions
C. Blocks everything and only allows the minimal required privileges
D. Blocks everything and allows the maximum level of permissions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
When is the BEST time to update antivirus definitions?

A. At least once a week as part of system maintenance
B. As the definitions become available from the vendor
C. When a new virus is discovered on the system
D. When an attack occurs on the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Why would a technician use a password cracker?

A. To look for weak passwords on the network
B. To changea users passwords when they leave the company
C. To enforce password complexity requirements
D. To change users passwords if they have forgotten them

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Users on a network report that they are receiving unsolicited emails from an email address that does not change. Which of the following steps should be taken to stop this from occurring?

A. Configure a rule in eachusers router and restart the router.
B. Configure rules on the users host and restart the host.
C. Install an anti-spam filter on the domain mail servers and filter the email address.
D. Install an ACL on the firewall to block traffic from the sender and filter the IP address.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following is a true statement with regards to a NIDS?

A. A NIDS monitors and analyzes network traffic for possible intrusions.
B. A NIDS is installed on the proxy server.
C. A NIDS prevents certain types of traffic from entering a network.

D. A NIDS is normally installed on the email server.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
A technician suspects that a piece of malware is consuming too many CPU cycles and slowing down a system. Which of the following will help determine the amount of CPU cycles that are being consumed?

A. Install HIDS to determine the CPU usage.
B. Run performance monitor to evaluate the CPU usage.
C. Install malware scanning software.
D. Use a protocol analyzer to find the cause of the traffic.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following are characteristics of a hash function? (Select TWO).

A. One-way
B. Encrypts a connection
C. Ensures data can be easily decrypted
D. Fixed length output
E. Requires a key

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following is the MOST secure alternative for administrative access to a router?

A. SSH
B. Telnet
C. rlogin
D. HTTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following might an attacker resort to in order to recover discarded company documents?

A. Phishing
B. Insider theft
C. Dumpster diving
D. Shoulder surfing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following creates a security buffer zone between two rooms?

A. Mantrap
B. DMZ
C. Turnstile
D. Anti-pass back

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following tools would be used to review network traffic for clear text passwords?

A. Port scanner
B. Protocol analyzer
C. Firewall
D. Password cracker

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Kerberos uses which of the following trusted entities to issue tickets?

A. Ticket Granting System
B. Certificate Authority
C. Internet Key Exchange
D. Key Distribution Center

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following specifies a set of consistent requirements for a workstation or server?

A. Vulnerability assessment
B. Imaging software
C. Patch management
D. Configuration baseline

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A companys website allows customers to search for a product and display the current price and quantity available of each product from the production databasE. Which of the following would invalidate an SQL injection attack launched from the lookup field at the web server level?

A. Security template
B. Buffer overflow protection
C. NIPS
D. Input validation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following virtual machine components monitors and manages the various virtual instances?

A. VMOS
B. VCPU
C. Hypervisor
D. Virtual supervisor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A smurf attack is an example of which of the following threats?

A. ARP Poisoning
B. DoS
C. TCP/IP Hijacking
D. Man-in-the-middle

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following is the BEST tool for allowing users to go to approved business-related websites only?

A. Internet content filter
B. Firewall
C. ACL
D. Caching server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following is a security trait of a virtual machine?

A. Provides additional resources for testing
B. Provides real-time access to all system processes
C. Provides a read-only area for executing code
D. Provides a restricted environment for executing code

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
An unauthorized user intercepted a users password and used this information to obtain the companys administrator password. The unauthorized user can use the administrators password to access sensitive information pertaining to client datA. Which of the following is this an example of?

A. Session hijacking
B. Least privilege
C. Privilege escalation
D. Network address translation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Users are utilizing thumb drives to connect to USB ports on company workstations. A technician is concerned that sensitive files can be copied to the USB drives.Which of the following mitigation techniques would address this concern? (Select TWO).

A. Disable the USB root hub within the OS.
B. Install anti-virus software on the USB drives.
C. Disable USB within the workstations BIOS.
D. Apply the concept of least privilege to USB devices.
E. Run spyware detection against all workstations.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
An administrator has developed an OS install that will implement the tightest security controls possible.
In order to quickly replicate these controls on all systems, which of the following should be established?

A. Take screen shots of the configuration options.
B. Create an image from the OS install.
C. Create a boot disk for the operating system.
D. Implement OS hardening procedures.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
After registering an email address on a website, a user starts receiving messages from unknown sources. The email account is new, and therefore the user is concerneD. This type of message traffic is referred to as:

A. instant message traffiC.
B. SPIM.
C. S/MIME.
D. spam.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A technician is testing the security of a new database application with a website front-end. The technician

notices that when certain characters are input into the application it will crash the server. Which of the following does the technician need to do?

A. Utilize SSL on the website
B. Implement an ACL
C. Lock-down the database
D. Input validation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
An administrator in a small office environment has implemented an IDS on the network perimeter to detect malicious traffic patterns. The administrator still has a concern about traffic inside the network originating between client workstations. Which of the following could be implemented?

A. HIDS
B. A VLAN
C. A network router
D. An access list

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A user is redirected to a different website when the user requests the DNS record www.xyz.comptiA. com. Which of the following is this an example of?

A. DNS poisoning
B. DoS
C. DNS caching
D. Smurf attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
A company wants to host public servers on a new network. These servers will include a website and mail server.Which of the following should be implemented on the network to isolate these public hosts from the rest of the network?

A. IPv6
B. IPSec

C. DMZ
D. VLAN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
A user has decided that they do not want an internal LAN segment to use public IP addresses. The user wants to translate them as private IP addresses to a pool of public IP addresses to identify them on the Internet. Which of the following does the user want to implement?

A. IPSec
B. NAT
C. SSH
D. SFTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
An administrator has been studying stateful packet inspection and wants to implement this security technique on the network. Which of the following devices could the administrator use to BEST utilize stateful packet inspection?

A. Hub
B. IDS
C. Switch
D. Firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following is the primary purpose of a honeypot?

A. Translate addresses at the perimeter
B. To provide a decoy target on the network
C. Provide cryptography for the network
D. Work as a network proxy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
An administrator wants to ensure that that no equipment is damaged when there is a fire or false alarm in the server room. Which of the following type of fire suppression systems should be used?

A. Carbon Dioxide
B. Hydrogen Peroxide
C. Wet pipe sprinkler
D. Deluge sprinkler

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following is a CRL composed of?

A. Public Key Infrastructure (PKI)
B. Expired or revoked certificates
C. Certificate authorities
D. Expired user accounts

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following is the primary purpose of a CA?

A. LANMAN validation
B. Encrypt data
C. Kerberos authentication
D. Issue private/public keys

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
An administrator wants to replace telnet with a more secure protocol to manage a network device. Which of the following should be implemented on the network?

A. SMTP

B. SNMP
C. SFTP
D. SSH

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A user is attempting to receive digitally signed and encrypted email messages from a remote office. Which of the following protocols does the system need to support?

A. SMTP
B. S/MIME
C. ISAKMP
D. IPSec

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
An administrator does not want anyone to VPN from inside the network to a remote office or network. Which of the following protocols should be blocked outbound on the network?

A. TPM
B. OVAL
C. SNMP
D. ISAKMP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
An administrator is implementing a public website and they want all client connections to the server to be encrypted via their web browser. Which of the following should be implemented?

A. SSL
B. SHA-1
C. Blowfish
D. 3DES

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following is MOST likely provided by asymmetric key cryptography?

A. Performance
B. A pre-shared key
C. Kiting
D. Confidentiality

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
All of the following are symmetric key algorithms EXCEPT:

A. ECC.
B. Rijndael.
C. 3DES.
D. RC4

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following is true about ECC algorithms?

A. It is the algorithm used in PGP.
B. It is implemented in portable devices.
C. It is a private key algorithm.
D. It is CPU intensivE.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following is a way to encrypt session keys using SSL?

A. Session keys are sent unencrypteD.
B. Session keys are encrypted using an asymmetric algorithm.
C. Session keys are sent in clear text because they are private keys.

D. Session keys are encrypted using a symmetric algorithm.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following can reduce the risk associated with password guessing attacks? (Select TWO).

A. Implement single sign-on.
B. Implement shared passwords.
C. Implement account-lockout thresholds.
D. Implement shadow passwords.
E. Implement stronger password complexity policies.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following is a common practice in forensic investigation?

A. Performing a Gutman sanitization of the drive
B. Performing a binary copy of the systems storage media
C. Performing a file level copy of the systems storage media
D. Performing a sanitization of the drive

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following is done to ensure appropriate personnel have access to systems and networks? (Select TWO).

A. Conduct periodic penetration testing assessments.
B. Conduct periodic personnel employment verifications.
C. Conduct rights review of users and groups.
D. Conduct virus scan.
E. Conduct vulnerability assessments.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Antivirus software products detect malware by comparing the characteristics of known instances against which of the following type of file sets?

A. Signature
B. Text
C. NIDS signature
D. Dynamic Library

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following type of fire suppression tools would cause the MOST damage to electrical equipment?

A. Water
B. Carbon Dioxide
C. Halon
D. Foam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following is the BEST process of removing PII data from a disk drive before reuse?

A. Destruction
B. Sanitization
C. Reformatting
D. Degaussing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
When assigning permissions, which of the following concepts should be applied to enable a person to perform their job task?

A. Rule based
B. Discretionary access control (DAC)
C. Least privilege

D. Role based

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
While conducting a review of the system logs, a user had attempted to log onto the network over 250 times. Which of the following type of attacks is MOST likely occurring?

A. Brute force
B. Phishing
C. Spamming
D. DNS spoofing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Users do not want to enter credentials to each server or application to conduct their normal work. Which of the following type of strategies will resolve this issue?

A. Smart card
B. Two-factor authentication
C. Biometrics
D. SSO

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A user was trying to update an open file but when they tried to access the file they were denied. Which of the following would explain why the user could not access the file?

A. Audit only access
B. Execute only access
C. Rights are not set correctly
D. Write only access

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Accessing a system or application using permissions from another users account is a form of which of the following?

A. Phishing
B. Domain kiting
C. ARP spoofing
D. Privilege escalation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following is an important reason for password protecting the BIOS?

A. To maintain password complexity requirements
B. To prevent system start-up without knowing the password
C. To keep a user from changing the boot order of the system
D. To keep a virus from overwriting the BIOS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following is a software bundle containing multiple security fixes?

A. Patch management
B. A hotfix
C. Service pack
D. A patch

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A company uses a policy of assigning passwords to users, by default the passwords are based off of the word $ervicexx, where xx is the last two numbers of the users cell phone number. The users are not required to change this password. Which of the following is this an example of?

A. Default accounts
B. Known plain text
C. Back door

D. Weak passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following is an installable package that includes several patches from the same vendor for various applications?

A. Hotfix
B. Patch template
C. Service pack
D. Patch rollup

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following is a best practice to prevent users from being vulnerable to social engineering?

A. Have a solid acceptable use policy in place with a click through banner.
B. Provide thorough and frequent user awareness training.
C. Haveuser sign both the acceptable use policy and security based HR policy.
D. Provide a service level agreement that addresses social engineering issues.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
The RAS logs on a server show 100 errors in a two minute time period from an attempt to access an account. The error log shows unknown username or passworD. Which of the following is this an example of?

A. The local firewall is blocking GRE packets.
B. An unauthorized attempt to access the server.
C. The end users ISPis having issues with packet loss.
D. One of the users forgot their password and kept trying to login.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
An administrator notices that former temporary employees accounts are still active on a domain. Which of the following can be implemented to increase security and prevent this from happening?

A. Run a last logon script to look for inactive accounts.
B. Implement an account expiration date for temporary employees.
C. Implement a password expiration policy.
D. Implement time of day restrictions for all temporary employees.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following is the primary security risk with coaxial cable?

A. Diffusion of the core light source
B. Data emanation from the core
C. Crosstalk between the wire pairs
D. Refraction of the signal

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following is a collection of patches?

A. A security template
B. A service pack
C. A security hotfix
D. A security baseline

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following would allow an administrator to find weak passwords on the network?

A. A network mapper
B. A hash function
C. A password generator
D. A rainbow table

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which of the following is the BEST place where the disaster recovery plan should be kept?

A. Printed out and kept in the desk of the CIO
B. At multiple offsite locations
C. Multiple copies printed out and kept in the server room
D. On the network file server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which of the following is established immediately upon evidence seizure?

A. Start the incident respond plan
B. Damage and loss control
C. Chain of custody
D. Forensic analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following is a required privilege that an administrator must have in order to restore a public/private key set on a certificate authority (CA)?

A. Recovery agent
B. Registration authority
C. Domain administrator
D. Group administrator

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following algorithms have the smallest key space?

A. IDEA

B. SHA-1
C. AES
D. DES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following is the MOST recent addition to cryptography?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following requires a common pre-shared key before communication can begin?

A. Public key infrastructure
B. Symmetric key cryptography
C. Secure hashing algorithm
D. Asymmetric key cryptography

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following provides the MOST comprehensive redundancy for an entire site with the least downtime?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following allows devices attached to the same switch to have separate broadcast domains?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which of the following allows for notification when a hacking attempt is discovered?

A. NAT
B. NIDS
C. Netflow
D. Protocol analyzer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
When dealing with a 10BASE5 network, which of the following is the MOST likely security risk?

A. An incorrect VLAN
B. SSID broadcasting
C. A repeater
D. A vampire tap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following allows a technician to scan for missing patches on a device without actually attempting to exploit the security problem?

A. A vulnerability scanner
B. Security baselines
C. A port scanner
D. Group policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following allows for proof that a certain person sent a particular email?

A. Steganography
B. Integrity
C. Trusted Platform Module
D. Non-repudiation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following uses a key ring?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following allows for the highest level of security at time of login?

A. Single sign-on
B. Two-factor authentication
C. One-factor authentication
D. NTLMv2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Sending a patch through a testing and approval process is an example of which of the following?

A. Disaster planning
B. Change management
C. Acceptable use policies
D. User education and awareness training

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Sending continuous TCP requests to a device and ignoring the return information until the device ceases to accept new connections is an example of which of the following?

A. TCP/IP hijacking
B. DNS poisoning
C. Kiting
D. DoS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following would use a group of bots to stop a web server from accepting new requests?

A. DoS
B. DDoS
C. MAC
D. ARP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following is the MOST likely to generate static electricity?

A. Low humidity and high temperature
B. High humidity and low temperature
C. Low humidity and low temperature
D. High humidity and high temperature

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Using an asymmetric key cryptography system, where can a technician generate the key pairs?

A. A certificate authority
B. IETF
C. A key escrow service
D. A recovery agent

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following media is the LEAST likely to be successfully tapped into?

A. Unshielded twisted pair cable
B. Coaxial cable
C. Fiber optic cable
D. Shielded twisted pair cable

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following allows a person to find public wireless access points?

A. Weak encryption
B. 8021x
C. SSID broadcast
D. Data emanation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following allows a file to have different security permissions for users that have the same roles or user groups?

A. Mandatory Access Control (MAC)
B. Role-Based Access Control (RBAC)
C. Discretionary Access Control (DAC)

D. Rule-Based Access Control (RBAC)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A DMZ has a fake network that a hacker is attacking. Which of the following is this an example of?

A. Firewall
B. Man-in-the-middle
C. Proxy server
D. Honeypot

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
A company decides that the purchasing agent and the accounts receivable agent should exchange positions in order to allow for more oversight of past transactions. Which of the following is this an example of?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A user complains that the color laser printer continuously gives an access denied message while attempting to print a text document. The administrator logs onto the PC and prints successfully. Which of the following should the administrator check FIRST?

A. That the printer has the correct size of paper in each of the trays
B. That the toner should be changed in the printer
C. That the user has sufficient rights to print to the printer
D. That the user is attempting to print to the correct printer tray

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following uses a sandbox to manage a programs ability to access system resources?

A. Java
B. ActiveX
C. JavaScript
D. Cold Fusion

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Which of the following allows a technician to view the security permissions of a file?

A. The access control list
B. The security baseline
C. The data emanation
D. The local security template

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
A user is denied access to a filE. The user had access to the file yesterday. Which of the following is the FIRST action for the technician to take?

A. Deny the users request and forward to the human resources department.
B. Reboot the system.
C. Verify that theusers permissions are correct.
D. Grant access to the filE.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
A user is convinced that someone is attempting to use their user account at night. Which of the following should an administrator check FIRST in order to prove or disprove this claim?

A. The IDS logs
B. The security application logs
C. The local security logs

D. The firewall logs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
A user reports that a web based application is not working after a browser upgradE. Before the upgrade, a login box would appear on the screen and disappear after login. The login box does not appear after the upgradE. Which of the following BEST describes what to check FIRST?

A. That the software based firewall application trusts this site
B. That the pop-up blocker application trusts this site
C. That the antivirus application trusts this site
D. That the anti-spam application trusts this site

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
An intrusion has been detected on a companys network from the Internet. Which of the following should be checked FIRST?

A. The firewall logs
B. The DNS logs
C. The access logs
D. The performance logs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A user needs to verify that a patch file downloaded from a third party has not been modified since the time that the original manufacturer released the patch. Which of the following is the BEST way to verify that the file has not been modified?

A. Compare the final MD5 hash with the original.
B. Download the patch file over an AES encrypted VPN connection.
C. Compare the final LANMAN hash with the original.
D. Download the patch file through a SSL connection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
A technician suspects that one of the network cards on the internal LAN is causing a broadcast storm.
Which of the following would BEST diagnose which NIC is causing this problem?

A. The NIDS log file
B. A protocol analyzer
C. The local security log file
D. The local firewall log file

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
A user is convinced that someone is attempting to use their user account at night. Which of the following should an administrator check FIRST in order to prove or disprove this claim?

A. The IDS logs
B. The security application logs
C. The local security logs
D. The firewall logs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A small call center business decided to install an email system to facilitate communications in the office.
As part of the upgrade the vendor offered to supply anti-malware software for a cost of $5,000 per year. The IT manager read there was a 90% chance each year that workstations would be compromised if not adequately protecteD. If workstations are compromised it will take three hours to restore services for the 30 staff. Staff members in the call center are paid $90 per hour. If determining the risk, which of the following is
the annual loss expectancy (ALE)?

A. $2,700
B. $4,500
C. $5,000
D. $7,290b

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103

Which of the following concepts, requires users and system processes to be assigned minimum levels of permission to carry out the assigned task?

A. User authentication
B. Need-to-know
C. Least privilege
D. Job role

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Which of the following describes software that is often written solely for a specific customers application?

A. Rootkit
B. Hotfix
C. Service pack
D. Patch

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Which of the following describes the process of comparing cryptographic hash functions of system executables, configuration files, and log files?

A. File integrity auditing
B. Host based intrusion detection
C. Network based intrusion detection
D. Stateful packet filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Exam C

QUESTION 1
A user does not understand why the domain password policy is so stringent. Which of the following BEST demonstrates the security basis for the password policy?

A. Explain how easy it is for a hacker to crack weak passwords.
B. Show the user a domain overview, including a list of weak passwords.
C. Refer the user to a strong password demonstrator.
D. Ask the user to review the corporate policies and procedures manual.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A company needs to have multiple servers running low CPU utilization applications. Which of the following is the MOST cost efficient method for accomplishing this?

A. Install multiple high end servers, sharing a clustered network operating system.
B. Install a single low end server, running multiple virtual servers.
C. Install a single high end server, running multiple virtual servers.
D. Install multiple low end servers, each running a network operating system.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A programmer creates an application to accept data from a websitE. A user places more information than the program expects in the input field resulting in the back end database placing the extra information into the databasE. Which of the following is this an example of?

A. Java input error
B. Cross-site scripting
C. Buffer overflow
D. SQL injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following security threats is MOST commonly associated with a targeted distributed denial of service (DDoS)?

A. Viruses

B. Worms
C. Botnets
D. Trojans

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A developer added code to a financial system designed to transfer money to a foreign bank account on a specific time and datE. The code would activate only if human resources processed the developers termination papers. The developer implemented which of the following security threats?

A. Logic bomb
B. Rootkit
C. Botnet
D. Privilege escalation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
A CEO is concerned about staff browsing inappropriate material on the Internet via HTTPS. It has been suggested that the company purchase a product which could decrypt the SSL session, scan the content and then repackage the SSL session without staff knowing.Which of the following type of attacks is similar to this product?

A. Replay
B. Spoofing
C. TCP/IP hijacking
D. Man-in-the-middle

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
After a system risk assessment was performed it was found that the cost to mitigate the risk was higher than the expected loss if the risk was actualizeD. In this instance, which of the following is the BEST course of action?

A. Accept the risk
B. Mitigate the risk
C. Reject the risk
D. Run a new risk assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
A small call center business decided to install an email system to facilitate communications in the office.
As part of the upgrade the vendor offered to supply anti-malware software for a cost of $5,000 per year. The IT manager read there was a 90% chance each year that workstations would be compromised if not adequately protecteD. If workstations are compromised it will take three hours to restore services for the 30 staff. Staff members in the call center are paid $90 per hour. If determining the risk, which of the following is the annual loss expectancy (ALE)?

A. $2,700
B. $4,500
C. $5,000
D. $7,290b

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A technician is deciding between implementing a HIDS on the database server or implementing a NIDS. Which of the following are reasons why a NIDS may be better to implement? (Select TWO).

A. Many HIDS require frequent patches and updates.
B. Many HIDS are not able to detect network attacks.
C. Many HIDS have a negative impact on system performancE.
D. Many HIDS only offer a low level of detection granularity.
E. Many HIDS are not good at detecting attacks on database servers.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following scenarios is MOST likely to benefit from using a personal software firewall on a laptop?

A. Remote access user connecting via SSL VPN
B. Office laptop connected to the enterprise LAN
C. Remote access user connecting via corporate dial-in server
D. Office laptop connected to a homeusers network

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Virtualized applications, such as virtualized browsers, are capable of protecting the underlying operating system from which of the following?

A. Malware installation from suspects Internet sites
B. Man-in-the-middle attacks
C. Phishing and spam attacks
D. DDoS attacks against the underlying OS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
A flat or simple role-based access control (RBAC) embodies which of the following principles?

A. Users assigned to roles, permissions are assigned to groups, controls applied to groups and permissions acquired by controls
B. Users assigned permissions, roles assigned to groups and users acquire additional permissions by being a member of a group
C. Roles applied to groups, users assigned to groups and users acquire permissions by being a member of the group
D. Users assigned to roles, permissions are assigned to roles and users acquire permissions by being a member of the role

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A number of unauthorized staff has been entering the data center by piggybacking authorized staff. The CIO has mandated that this behavior stops. Which of the following is the BEST technology to install at the data center to prevent piggybacking?

A. Mantrap
B. Security badges
C. Hardware locks
D. Token access

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following is a security threat that hides its processes and files from being easily detected?

A. Trojan
B. Adware
C. Worm
D. Rootkit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Security templates are used for which of the following purposes? (Select TWO).

A. To ensure that email is encrypted by users of PGP
B. To ensure that PKI will work properly within the companys trust model
C. To ensure that performance is standardized across all servers
D. To ensure that all servers start from a common security configuration
E. To ensure that servers are in compliance with the corporate security policy

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Frequent signature updates are required by which of the following security applications? (Select TWO).

A. Antivirus
B. PGP
C. Firewall
D. PKI
E. IDS

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
When choosing an antivirus product, which of the following are the MOST important security considerations? (Select TWO).

A. The frequency of signature updates
B. The ability to scan encrypted files
C. The availability of application programming interface

D. The number of emails that can be scanned
E. The number of viruses the software can detect

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Three generally accepted activities of patch management are: determining which patches are needed, applying the patches and which of the following?

A. Updating the firewall configuration to include the patches
B. Running a NIDS report to list the remaining vulnerabilities
C. Auditing for the successful application of the patches
D. Backing up the patch file executables to a network share

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
In which of the following situations would it be appropriate to install a hotfix?

A. A patch in a service pack fixes the issue, but too many extra patches are includeD.
B. A patch is not available and workarounds do not correct the problem.
C. A patch is available, but has not yet been tested in a production environment.
D. A patch is too large to be distributed via a remote deployment tool.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Social engineering, password cracking and vulnerability exploitation are examples of which of the following?

A. Vulnerability assessment
B. Fingerprinting
C. Penetration testing
D. Fuzzing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
If an administrator does not have a NIDS examining network traffic, which of the following could be used to identify an active attack?

A. Protocol analyzer
B. Penetration testing tool
C. Network mapper
D. Vulnerability scanner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Configuration baselines should be taken at which of the following stages in the deployment of a new system?

A. Before initial configuration
B. Before loading the OS
C. After a user logs in
D. After initial configuration

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following practices should be implemented to harden workstations and servers?

A. Log on only as the administrator.
B. Install only needed softwarE.
C. Check the logs regularly.
D. Report all security incidents.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following is a mechanism that prevents electromagnetic emanations from being captured?

A. Install a repeater
B. Uninterruptible power supply (UPS)
C. Faraday cage
D. Disable SSID broadcast

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following describes the difference between a secure cipher and a secure hash?

A. A hash produces a variable output for any input size, a cipher does not.
B. A cipher produces the same size output for any input size, a hash does not.
C. A cipher can be reversed, a hash cannot.
D. A hash can be reversed, a cipher cannot.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following physical threats is prevented with mantraps?

A. Piggybacking
B. Social engineering
C. Dumpster diving
D. Shoulder surfing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following BEST describes the differences between SHA-1 and MD5?

A. MD5 produces variable length message digests.
B. SHA-1 produces few collisions than MD5
C. MD5 produces few collisions than SHA-1
D. SHA-1 produces fixed length message digests.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following BEST applies in the secure disposal of computers?

A. Computers must be configured for automated patch management.

B. Computer media must be sanitizeD.
C. Default passwords must be changed oncE.
D. Computers must be tested against known TCP/IP vulnerabilities.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following BEST describes the differences between RADIUS and TACACS?

A. TACACS separates authentication, authorization and auditing capabilities.
B. TACACS is a remote access authentication servicE.
C. RADIUS is a remote access authentication servicE.
D. RADIUS separates authentication, authorization and auditing capabilities.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following BEST describes the differences between RADIUS and TACACS?

A. RADIUS encrypts client-server negotiation dialog.
B. RADIUS is a remote access authentication servicE.
C. TACACS encrypts client-server negotiation dialog.
D. TACACS is a remote access authentication servicE.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following authentication mechanisms performs better in a secure environment?

A. RADIUS because it is a remote access authentication servicE.
B. TACACS because it encrypts client-server negotiation dialogs.
C. RADIUS because it encrypts client-server passwords.
D. TACACS because it is a remote access authentication servicE.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
To evaluate the security compliance of a group of servers against best practices, which of the following BEST applies?

A. Get a patch management report.
B. Conduct a penetration test.
C. Run a vulnerability assessment tool.
D. Install a protocol analyzer.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is a problem MOST often associated with UTP cable?

A. Fuzzing
B. Vampire tap
C. Crosstalk
D. Refraction

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
An administrator notices on the monthly firewall log that many of the internal PCs are sending packets on a routine basis to a single external PC. Which of the following BEST describes what is occurring?

A. The remote PC has a spam slave application running and the local PCs have a spam master application running.
B. The remote PC has a zombie master application running and the local PCs have a zombie slave application running.
C. The remote PC has a spam master application running and the local PCs have a spam slave application running.
D. The remote PC has a zombie slave application running and the local PCs have a zombie master application running.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
An administrator notices that a PC is sending an unusual amount of email at odd times of the day. Which of the following should the administrator check for FIRST?

A. A S/MIME buffer overflow
B. A POP3 protocol exception
C. DNS poisoning
D. A SMTP open relay

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following would a password cracker help an administrator to find?

A. Weak passwords
B. Expired passwords
C. Locked passwords
D. Backdoor passwords

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following is setup within a router?

A. ARP
B. DMZ
C. OVAL
D. DDoS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following would BEST allow for fast, highly secure encryption of a USB flash drive?

A. SHA-1
B. MD5
C. 3DES
D. AES256

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
When is the correct time to discuss the appropriate use of electronic devices with a new employee?

A. At time of hire
B. At time of first correspondence
C. At time of departure
D. At time of first system login

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following could BEST assist in the recovery of a crashed hard drive?

A. Forensics software
B. Drive optimization
C. Drive sanitization
D. Damage and loss control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following facilitates the creation of an unencrypted tunnel between two devices?

A. AES
B. HTTPS
C. L2TP
D. PPTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following allows for a secure connection to be made through a web browser?

A. L2TP
B. SSH
C. SSL
D. HTTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following is the BEST order in which crucial equipment should draw power?

A. Uninterruptible Power Supply (UPS) battery, UPS line conditioner, backup generator
B. Backup generator, UPS line conditioner, UPS battery
C. Backup generator, UPS battery, UPS line conditioner
D. UPS line conditioner, UPS battery, and backup generator

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following would require a pre-sharing of information before a home user could attach to a neighbors wireless adapter?

A. Anonymous connections enabled
B. SSID broadcasting disabled
C. SSID broadcasting enabled
D. Encryption disabled

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following would BEST allow an administrator to quickly find a rogue server on the network?

A. Review security access logs
B. A network mapper
C. A protocol analyzer
D. Review DNS logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following would BEST allow an administrator to quickly find a PC with a blank database administrator password?

A. Protocol analyzer
B. Vulnerability scanner
C. Rainbow tables
D. Security access logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
An administrator is backing up all server data nightly to a local NAS devicE. Which of the following additional steps should the administrator take for protection from disaster in the case the primary site is permanently lost?

A. Backup all data at a preset interval to tape and store those tapes at a sister site across the street.
B. Backup all data at a preset interval to tape and store those tapes at a sister site in another city.
C. Backup all data at a preset interval to removable disk and store the disk in a safety deposit box at theadministrators homE.
D. Backup all data at a preset interval to removable disk and store the disk in a fireproof safe in the buildings basement.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following is the MOST intrusive on a network?

A. Penetration testing
B. Protocol analyzers
C. Port scanners
D. Vulnerability testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
A single sign-on requires which of the following?

A. Multifactor authentication
B. One-factor authentication
C. A trust model between workstations
D. A unified trust model

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
All of the following are where backup tapes should be kept EXCEPT:

A. near a fiber optic cable entrance.
B. near a shared LCD screen.
C. near a power linE.
D. near a high end server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
All of the following require periodic updates to stay accurate EXCEPT:

A. signature based HIDS.
B. pop-up blocker applications.
C. antivirus applications.
D. rootkit detection applications.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following is the quickest method to create a secure test server for a programmer?

A. Install a network operating system on new equipment.
B. Create a virtual server on existing equipment.
C. Install a network operating system on existing equipment.
D. Create a virtual server on new equipment.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following is a collection of fixes for an application or operating system that has been tested by the vendor?

A. A security template

B. A service pack
C. A patch
D. A hotfix

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following usually applies specifically to a web browser?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Pre-shared keys apply to which of the following?

A. CA
B. PGP
C. TPM
D. Digital signature

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following is a risk associated with a virtual server?

A. If the physical server crashes, all of the local virtual servers go offline immediately.
B. If the physical server crashes, all of the physical servers nearby go offline immediately.
C. If a virtual server crashes, all of the virtual servers go offline immediately.
D. If a virtual server crashes, all of the physical servers go offline immediately.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following exploits is only triggered by a specific date or time key?

A. Trojan
B. Worm
C. Botnet
D. Logic bomb

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Threats to a network could include: (Select TWO)

A. penetration testing.
B. network audits.
C. disgruntled employees.
D. dial-up access.
E. disabled user accounts.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
An antivirus server keeps flagging an approved application that the marketing department has installed on their local computers as a threat. This is an example of:

A. false negative.
B. false positivE.
C. true negativE.
D. true positivE.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A vendor releases an application update to a recent service pack that addresses problems being experienced by some end users. This update would be considered a:

A. hotfix.
B. patch.
C. service pack rollup.

D. service pack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A technician is working on an end users desktop which has been having performance issues. The technician notices there seems to be a lot of activity on the NIC. A good tool to quickly check the current network connections of the desktop would be:

A. netops.
B. lanman.
C. netstat.
D. ipconfig /all.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
A company has an issue with field users logging into VPN to connect to the mail server, and leaving their computers connected while in public places. The administrator needs to prevent both unauthorized access to the company email and data, and limit the impact on the VPN server.
Which of the following BEST achieves this goal?

A. Set VPN to disconnect after five minutes of inactivity.
B. Use registry settings to lock computers after five minutes of inactivity, and limit VPN connections to two hours.
C. Use group policy to lock computers after five minutes of inactivity, and limit VPN connections to one hour.
D. Provide web mail access to all users.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
The service provided by message authentication code (MAC) hash is:

A. fault tolerancE.
B. key recovery.
C. data recovery.
D. integrity.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
An administrator is running a network monitoring application that looks for behaviors on the network outside the standard baseline that has been establisheD. This is typical of a(n):

A. signature-based tool.
B. protocol analyzer.
C. honeynet.
D. anomaly-based tool.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Some examples of hardening techniques include all of the following EXCEPT:

A. applying security templates.
B. running weekly spyware applications.
C. network-based patch management.
D. disabling all non-required services.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
An administrator wants to block users from accessing a few inappropriate websites as soon as possiblE. The existing firewall allows blocking by IP address. To achieve this goal the administrator will need to:

A. upgrade to a DNS based filter to achieve the desired result.
B. use the company AUP to achieve the desired result.
C. upgrade to a URL based filter to achieve the desired result.
D. upgrade to a text based filter to achieve the desired result.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A CRL contains a list of which of the following type of keys?

A. Both public and private keys

B. Steganographic keys
C. Private keys
D. Public keys

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A user logs into their network with a smart carD. Which of the following keys is used?

A. Cipher key
B. Shared key
C. Public key
D. Privatekey

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
An administrator wants to ensure that when an employee leaves the company permanently, that the company will have access to their private keys. Which of the following will accomplish this?

A. Store the keys in escrow.
B. Immediately delete the account.
C. Store them in a CRL.
D. Obtain the employees hardware token.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
When a server and workstation communicate via SSL, which of the following keys are being used? (Select TWO).

A. Public key
B. Cipher key
C. Session key
D. Recovery key
E. Keylogger

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A user is going to dispose of some old hard drives. Which of the following should the user do to the drives before disposing of them?

A. Reformat the hard drives oncE.
B. Use a certified wipe program to erase datA.
C. Install antivirus on the drives.
D. Run anti-spyware on the drives.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A user wants to implement very tight security controls for technicians that seek to enter the users datacenter. Which of the following solutions offers the BEST security controls?

A. Combination locks and key locks
B. Smartcard and proximity readers
C. Magnetic lock and pin
D. Biometric reader and smartcard

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following concepts, requires users and system processes to be assigned minimum levels of permission to carry out the assigned task?

A. User authentication
B. Need-to-know
C. Least privilege
D. Job role

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
When using discretionary access control (DAC), who determines access and what privileges they have?

A. User

B. System
C. Help desk
D. Owner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following is a security benefit of mandatory vacations?

A. Least privilege
B. Separation of duties
C. Reducing stress
D. Detecting fraud

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
The data custodian in an organization is responsible for:

A. recoverability of the datA.
B. classification of the datA.
C. completeness of the datA.
D. accuracy of the datA.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following organizational documentation describes how tasks or job functions should be conducted?

A. Standards
B. Guideline
C. Policy
D. Procedures

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following organizational documentation provides high level objectives that change infrequently?

A. Standards
B. Policy
C. Procedures
D. Guideline

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following sites can be online the QUICKEST and does not require data restoration from backup media to ensure the production data is as current as possible?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following are MOST likely to be analyzed by Internet filter appliances/servers? (Select THREE).

A. Certificates
B. Keys
C. TLSs
D. URLs
E. Content
F. CRLs

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
The primary function of risk management in an organization is to reduce risk to a level:

A. where the ARO equals the SLE.

B. the organization will mitigatE.
C. where the ALE is lower than the SLE.
D. the organization will accept.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following BEST describes risk analysis?

A. Monitoring and acceptance
B. Evaluation and assessment
C. Assessment and eradication
D. Mitigation and repudiation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
A financial institution performed a risk assessment on the DLT backup system used to store customer account details. The main risk highlighted was the long-term retention of electronically stored datA.
Which
of the following is the MOST likely reason for the risk being raised?

A. Compatibility of media and application systems
B. Application systems and technical staff
C. Compatibility and retention of data on the media
D. Retention of data on the media

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following hashing techniques is commonly disabled to make password cracking more difficult?

A. NTLM
B. AES
C. OVAL
D. Kerberos

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
An organization has recently implemented a work from home program. Employees need to connect securely from home to the corporate network. Which of the following encryption technologies might BEST accomplish this?

A. PPTP
B. IPSec
C. L2TP
D. PPPoE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
The use of a physical token, PIN and a password during authentication is an example of which of the following?

A. Two-factor authentication
B. Kerberos authentication
C. EAP authentication
D. Three-factor authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Port 3535 is typically blocked for outbound traffic on a companys LAN. An end-user has recently purchased a legitimate business program that needs to make outbound calls using this port.
Which of the
following steps should a technician take to allow this? (Select TWO).

A. Open the port on the companys proxy server.
B. Open the port on the companys firewall.
C. Change theusers subnet mask.
D. Open the port on the users personal software firewall.
E. Open the port on the VLAN.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following describes software that is often written solely for a specific customers application?

A. Rootkit
B. Hotfix
C. Service pack
D. Patch

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
A security manager believes that too many services are running on a mission critical database server. Which of the following tools might a security analyst use to determine services that are running on the server, without logging into the machine?

A. OVAL
B. Port scanner
C. Protocol analyzer
D. NIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A manufacturing corporation has decided to send a highly sensitive message to one of their suppliers. The message is concealed inside a JPEG image of a beach resort. Which of the following is this an example of?

A. Cryptography
B. Digital signature
C. Hashing
D. Steganography

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following encryption methods is often used along with L2TP?

A. S/MIME
B. SSH
C. 3DES

D. IPSec

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
An administrator is assigned to monitor servers in a data center. A web server connected to the Internet suddenly experiences a large spike in CPU activity. Which of the following is the MOST likely cause?

A. Spyware
B. Trojan
C. Privilege escalation
D. DoS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following methods will help to identify when unauthorized access has occurred?

A. Implement two-factor authentication.
B. Implement previous logon notification.
C. Implement session termination mechanism.
D. Implement session lock mechanism.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Ensuring administrators have both a regular user account and a privileged user account is an example of applying which security principle?

A. Need-to-know
B. Mandatory Access Control (MAC)
C. Least privilege
D. Discretionary Access Control (DAC)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
All of the following are steps in the incident response process EXCEPT:

A. eradication.
B. repudiation.
C. recovery.
D. containment.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following is an example of two-factor authentication for an information system?

A. ATM card and PIN
B. Username and password
C. Retina and fingerprint scanner
D. Photo ID and PIN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which of the following describes a spanned switch port in the context of IDS traffic analysis?

A. An association of a set of destination ports with a single source port
B. An association of a set of source ports with a single destination port
C. An association of a set of source ports with multiple destination ports and an IDS sensor
D. An association of a set of destination ports with an IDS sensor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
A technician is performing an assessment on a router and discovers packet filtering is employeD. Which of the following describes a security concern with stateless packet filtering?

A. Packet payload is not checkeD.
B. State connections are retained by the router.
C. Router performance is reduceD.
D. Loose routing cannot determine the exact path a packet must follow.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following describes the process of comparing cryptographic hash functions of system executables, configuration files, and log files?

A. File integrity auditing
B. Host based intrusion detection
C. Network based intrusion detection
D. Stateful packet filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following is a cryptographic representation of non-repudiation?

A. Digital signature
B. Internet key exchange
C. Certificate authority
D. Symmetric key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Ensuring administrators have both a regular user account and a privileged user account is an example of applying which security principle?

A. Need-to-know
B. Mandatory Access Control (MAC)
C. Least privilege
D. Discretionary Access Control (DAC)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
An administrator wants to set up a new web server with a static NAT. Which of the following is the BEST reason for implementing NAT?

A. Publishes the organizations internal network addressing scheme
B. Publishes the organizations external network addressing scheme
C. Hides the organizations internal network addressing scheme
D. Hides the organizations external network addressing scheme

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Restricting access to files based on the identity of the user or group and security classification of the information is an example of which of the following?

A. RBAC
B. DAC
C. NTFS
D. MAC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
A HIDS is installed to monitor which of following?

A. CPU performance
B. NIC performance
C. System files
D. Temporary Internet files

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Exam D

QUESTION 1
Which of the following reduces the effectiveness of telephone social engineering?

A. Automatic callback
B. Monitoring outbound calls
C. Awareness training
D. Use of VoIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following will execute malicious code at a pre-specified time?

A. Logic Bomb
B. DoS
C. Worm
D. Rootkit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
All of the following are weaknesses of WEP EXCEPT:

A. lack of integrity checking.
B. initialization vector.
C. replay attacks.
D. lack of strong keys.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following is LEAST likely to help reduce single points of failure?

A. Mandatory vacations
B. Cross training
C. Clustered servers
D. Disaster recovery exercises

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following reduces the attack surface of an operating system?

A. Patch management
B. Installing antivirus
C. Installing HIDS
D. Disabling unused services

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following is LEAST effective when hardening an operating system?

A. Configuration baselines
B. Limiting administrative privileges
C. Installing HIDS
D. Install a software firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following provides the MOST control when deploying patches?

A. Hotfix
B. Remote desktop
C. Patch management
D. Service packs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
If a technician wants to know when a computer application is accessing the network, which of the following logs should be reviewed?

A. Antivirus log
B. RADIUS log
C. Performance log
D. Host firewall log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
All of the following are components of IPSec EXCEPT:

A. encapsulating security payloaD.
B. Internet key exchangE.
C. temporal key interchange protocol.
D. authentication header (AH).

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
IPSec connection parameters are stored in which of the following?

A. Security association database
B. Security payload index
C. Security parameter index
D. Certificate authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following will provide a 128-bit hash?

A. MD5
B. AES128
C. ROT13
D. SHA-1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following describes a hash algorithms ability to avoid the same output from two guessed inputs?

A. Collision avoidance
B. Collision resistance
C. Collision strength
D. Collision metric

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following should be included in a forensic toolkit?

A. Compressed air
B. Tape recorder
C. Fingerprint cards
D. Digital camera

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following BEST describes the form used while transferring evidence?

A. Booking slip
B. Affidavit
C. Chain of custody
D. Evidence log

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following is the primary incident response function of a first responder?

A. To evaluate the scene and repair the problem
B. To secure the scene and preserve evidence
C. To evaluate the scene and determine the cause
D. To gather evidence and write reports

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following is the GREATEST problem with low humidity in a server room?

A. Static electricity
B. Power surge
C. Electromagnetic interference
D. Brown out

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following protocols is used to ensure secure transmissions on port 443?

A. HTTPS
B. Telnet
C. SFTP
D. SHTTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
When should a technician perform disaster recovery testing?

A. Immediately following lessons learned sessions
B. Once a month, during peak business hours
C. After the network is stable and online
D. In accordance with the disaster recovery plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following is the BEST backup method to restore the entire operating system and all related software?

A. Weekly
B. Incremental
C. Disk Image
D. Differential

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
How many keys are utilized in symmetric cryptography?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following terms is BEST associated with public key infrastructure (PKI)?

A. MD5 hashing
B. Symmetric key
C. Symmetric algorithm
D. Digital signatures

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following is the LAST step to granting access to specific domain resources?

A. Validate the user
B. Authorize the user
C. Verify the user
D. Authenticate the user

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
After an attacker has successfully gained remote access to a server with minimal privileges, which of the following is their next step?

A. Elevate system privileges.
B. Monitor network traffiC.
C. Capture private keys.
D. Begin key recovery.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following should the technician recommend as a way to logically separate various internal networks from each other?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
An organization has requested the ability to monitor all network traffic as it traverses their network. Which of the following should a technician implement?

A. Content filter
B. Protocol analyzer
C. Honeypot
D. HIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
A large amount of viruses have been found on numerous domain workstations. Which of the following should the technician implement?

A. Decentralized antivirus
B. Host based intrusion detection

C. Centralized antivirus
D. Spyware detection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following is the MOST difficult security concern to detect when contractors enter a secured facility?

A. Rogue access points being installed
B. Copying sensitive information with cellular phones
C. Removing mass storage iSCSI drives
D. Removing network attached storage

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
When are port scanners generally used on systems?

A. At the middle of a vulnerability assessment
B. At the beginning of a vulnerability assessment
C. When there is a need to documentvulnerabilities
D. At the end of a penetration test assessment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
The staff must be cross-trained in different functional areas so that fraud can be detecteD. Which of the following is this an example of?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Human Resources has requested that staff members be moved to different parts of the country into new positions. Which of the following is this an example of?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
An administrator is worried about an attacker using a compromised user account to gain administrator access to a system. Which of the following is this an example of?

A. Man-in-the-middle attack
B. Protocol analysis
C. Privilege escalation
D. Cross-site scripting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following is used to deny authorized users access to services?

A. Botnets
B. Adware
C. Spyware
D. Trojans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
An administrator recommends implementing whitelisting, blacklisting, closing-open relays, and strong authentication techniques to a server administrator. Which of the following threats are being addressed?

A. Adware
B. Spyware

C. Spam
D. Viruses

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
An administrator is asked to improve the physical security of a data center located inside the office building.
The data center already maintains a physical access log and has a video surveillance system.
Which of the following additional controls could be implemented?

A. Defense-in-depth
B. Logical token
C. ACL
D. Mantrap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
In regards to physical security, which of the following BEST describes an access control system which implements a non-trusted but secure zone immediately outside of the secure zone?

A. Smart card
B. Defense-in-depth
C. Mantrap
D. DMZ

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
A technician notices delays in mail delivery on the mail server. Which of the following tools could be used to determine the cause of the service degradation?

A. Port scanner
B. Performance monitor
C. ipconfig /all
D. TFTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Penetration testing should only be used once which of the following items is in place?

A. Acceptable use policy
B. Data retention and disclosure policy
C. Service level agreement
D. Written permission

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
An administrator recommends that management establish a trusted third party central repository to maintain all employees private keys. Which of the following BEST describes the administrators recommendation?

A. Registration
B. Certificate authority
C. Recovery agent
D. Key escrow

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
To combat transaction fraud, a bank has implemented a requirement that all bank customers enter a different, unique code to confirm every transaction. Which of the following is the MOST effective method to accomplish this?

A. ATM PIN code
B. Elliptic curve
C. One-time password
D. Digital certificate

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
All of the following should be identified within the penetration testing scope of work EXCEPT:

A. a complete list of all network vulnerabilities.

B. IP addresses of machines from which penetration testing will be executeD.
C. a list of acceptable testing techniques and tools to be utilizeD.
D. handling of information collected by the penetration testing team.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following is the MOST efficient way that an administrator can restrict network access to certain ports enterprise wide?

A. HIDS
B. Personal software firewall
C. NIDS
D. ACL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
An administrator is responsible for a server which has been attacked repeatedly in the past. The only recourse has been to reload the server from scratch. Which of the following techniques could be used to decrease the recovery time following an incident?

A. Implement the server as a honeypot.
B. Implement the server as a virtual server instance.
C. Load balance between two identical servers.
D. Install the server on a separate VLAN segment.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Validating the users claimed identity is called which of the following?

A. Authentication
B. Identification
C. Verification
D. Validation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following is planted on an infected system and deployed at a predetermined time?

A. Logic bomb
B. Trojan horse
C. Worm
D. Rootkit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following allows a user to float a domain registration for a maximum of five days?

A. DNS poisoning
B. Domain hijacking
C. Spoofing
D. Kiting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
According to company policy an administrator must logically keep the Human Resources department separated from the Accounting department.Which of the following would be the simplest way to accomplish

this?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following is an attack which is launched from multiple zombie machines in attempt to bring down a service?

A. DoS
B. Man-in-the-middle
C. DDoS
D. TCP/IP hijacking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following will MOST likely allow an attacker to make a switch function like a hub?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following is commonly programmed into an application for ease of administration?

A. Back door
B. Worm
C. Zombie
D. Trojan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following is a technique used by hackers to identify unsecured wireless network locations to other hackers?

A. Bluesnarfing
B. War dialing
C. War chalking
D. War driving

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following authentication models uses a KDC?

A. CHAP
B. PKI
C. PGP
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following disaster recovery components is a location that is completely empty, but allows the infrastructure to be built if the live site goes down?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following should be done if an organization intends to prosecute an attacker once an attack has been completed?

A. Update antivirus definitions.
B. Disconnect the entire network from the Internet.
C. Apply proper forensic techniques.
D. Restore missing files on the affected system.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following documents specifies the uptime guarantee of a web server?

A. Due process
B. Due diligence

C. Scope of work

D. Service level agreement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following authentication models uses a time stamp to prevent the risks associated with a replay attack?

A. Two-factor authentication

B. RADIUS

C. LDAP

D. Kerberos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following protocols can be implemented as an alternative to the overhead of a VPN?

A. L2TP

B. PPTP

C. SSH

D. SSL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following will set an account to lockout for 30 minutes after the maximum number attempts have failed?

A. Key distribution center

B. Account lockout duration

C. Account lockout threshold

D. Password complexity requirements

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following logs would reveal activities related to an ACL?

A. Mobile device
B. Transaction
C. Firewall
D. Performance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following encryption algorithms has the largest overhead?

A. AES256
B. 3DES
C. AES
D. RSA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following hashing algorithms is the MOST secure?

A. LANMAN
B. SHA-1
C. MD5
D. CHAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following would allow a technician to compile a visual view of an infrastructure?

A. Security log
B. Network mapper
C. Port scanner
D. Protocol analyzer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following creates separate logical networks?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following is an area of the network infrastructure that allows a technician to place public facing systems into it without compromising the entire infrastructure?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which of the following attacks commonly result in a buffer overflow?

A. ARP Poisoning
B. DNS Poisoning
C. Replay
D. DoS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following type of attacks is TCP/IP hijacking?

A. Birthday
B. ARP poisoning
C. MAC flooding
D. Man-in-the-middle

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following ports does SNMP run on?

A. 25
B. 110
C. 161
D. 443

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following is a collection of servers that is setup to attract hackers?

A. DMZ
B. Honeypot
C. Honeynet
D. VLAN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which of the following could be used to determine which flags are set in a TCP/IP handshake?

A. FIN/RST
B. SYN/ACK
C. Protocol analyzer
D. Network mapper

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which of the following would be the BEST choice to ensure only ports 25, 80 and 443 were open from outside of the network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following media is LEAST susceptible to a tap being placed on the line?

A. Fiber
B. UTP
C. STP
D. Coaxial

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following is responsible for establishing trust models?

A. The firewall
B. The information security officer
C. The certificate authority
D. The key escrow agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following allows attackers to gain control over the web camera of a system?

A. ActiveX component
B. SQL injection
C. Cross-site scripting
D. XML

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following type of attacks sends out numerous MAC resolution requests to create a buffer overflow attack?

A. Smurf
B. ARP poisoning
C. DDoS
D. DNS poisoning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following would a former employee MOST likely plant on a server that is not traceable?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following would be MOST effective in stopping phishing attempts?

A. Antivirus
B. User training
C. NIDS
D. HIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which of the following consists of markings outside a building that indicate the connection speed of a nearby

unsecured wireless network?

A. War driving
B. War chalking
C. Blue jacking
D. Bluesnarfing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following would be of MOST interest to someone that is dumpster diving?

A. User education manual
B. Business card of computer contractor
C. List of expired usernames
D. Receipts from the supply store

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following could involve moving physical locations every two years to help mitigate security risks?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following could be used to capture website GET requests?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following does the process of least privilege fall under?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following hashing algorithms is the LEAST secure?

A. SHA-1
B. LANMAN
C. NTLM
D. MD5

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following is the MOST secure transmission algorithm?

A. 3DES
B. TKIP
C. AES256
D. AES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following protocols is used for encryption between email servers?

A. TLS
B. PPTP
C. L2TP

D. S/MIME

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following scenarios would a penetration test BEST be used for?

A. When providing a proof of concept demonstration for a vulnerability
B. While in the reconnaissance phase
C. When performing network mapping
D. When conducting performance monitoring

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following would be the easiest to use in detection of a DDoS attack?

A. Performance monitor
B. Application log
C. System log
D. Protocol analyzer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following implements the strongest hashing algorithm?

A. NTLMv2
B. NTLM
C. VLAN
D. LANMAN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following is BEST used to determine whether network utilization is abnormal?

A. Security log
B. Performance baseline
C. Application log
D. Systems monitor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following is the BEST solution to implement to reduce unsolicited email?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Identification is a critical component of the authentication process because it is:

A. used to confirm the privileges of a user.
B. when the user is verifieD.
C. when the user is authorizeD.
D. used to prevent authorized access.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Identity proofing occurs during which phase of identification and authentication?

A. Testing
B. Verification
C. Authentication
D. Identification

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following BEST describes the practice of dumpster diving?

A. Sorting through the garbage of an organization to obtain information used for configuration management.
B. Sorting through the garbage of an organization to obtain information used for a subsequent attack.
C. Sorting through the trash of an organization to obtain information found on their intranet.
D. Sorting through the trash of an organization to recover an old user ID badge previously used for an attack.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Implementation of proper environmental controls should be considered by administrators when recommending facility security controls because of which of the following?

A. Proper environmental controls provide redundancy to the facility.
B. Proper environmental controls helpensure availability of IT systems.
C. Proper environmental controls make authentication simpler.
D. Proper environmental controls provide integrity to IT systems.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
An administrator is asked to recommend the most secure transmission mediA. Which of the following should be recommended?

A. Unshielded twisted pair cable
B. Fiber optic cable
C. Ethernet CAT5 cable
D. Coaxial cable

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
An administrator is selecting a device to secure an internal network segment from traffic external to the segment. Which of the following devices could be selected to provide security to the network segment?

A. NIPS

B. HIDS
C. Internet content filter
D. DMZ

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which of the following devices should be deployed to protect a network against attacks launched from a business to business intranet? (Select TWO).

A. NIPS
B. Content filter
C. HIPS
D. Firewall
E. NIDS

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
To prevent the use of previously issued PKI credentials which have expired or otherwise become invalid, administrators should always design programs to check which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
To prevent the use of stolen PKI certificates on web servers, which of the following should an administrator ensure is available to their web servers?

A. Registration
B. CA
C. CRL
D. Key escrow

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 98
Which of the following describes an implementation of PKI where a copy of a users private key is stored to provide third party access and to facilitate recovery operations?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A security administrator has been asked to deploy a biometric authentication system in a corporation. Which of the following devices is the MOST reliable and has the lowest cross over error rate?

A. Iris scanner
B. Handprint scanner
C. Retina scanner
D. Fingerprint scanner

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
To increase the security of the network authentication process, an administrator decides to implement three-factor authentication. Which of the following authentication combinations is a three-factor system?

A. A PKI enabled smart card, strong password and 12-digit PIN
B. A retina scanner, PKI enabled smart card and a six-digit PIN
C. A fingerprint scanner, PKI enabled smart card and badge proximity reader
D. An Iris scanner, a user generated pass phrase and a palm reader

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which of the following protocols is used to ensure secure transmissions on port 443?

A. HTTPS
B. Telnet
C. SFTP
D. SHTTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Which of the following would allow for secure key exchange over an unsecured network without a pre-shared key?

A. 3DES
B. AES
C. DH-ECC
D. MD5

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
If a certificate has been compromised, which of the following should be done?

A. Run the recovery agent.
B. Put the certificate on the CRL.
C. Put the certificate in key escrow.
D. Suspend the certificate for further investigation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Password crackers are generally used by malicious attackers to:

A. verify system access.
B. facilitate penetration testing.
C. gain system access.
D. sniff network passwords.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Exam E

QUESTION 1
To facilitate compliance with the Internet use portion of the corporate acceptable use policy, an administrator implements a series of proxy servers and firewalls. The administrator further recommends installation of software based firewalls on each host on the network. Which of the following would have provided an alternative simpler solution?

A. Internet content filter
B. Hardware IDS
C. Software HIPS
D. DMZ

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
The marketing department wants to distribute pens with embedded USB drives to clients. In the past this client has been victimized by social engineering attacks which led to a loss of sensitive datA. The security administrator advises the marketing department not to distribute the USB pens due to which of the following?

A. The risks associated with the large capacity of USB drives and their concealable nature
B. The security costs associated with securing the USB drives over time
C. The cost associated with distributing a large volume of the USB pens
D. The security risks associated with combining USB drives and cell phones on a network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
USB drives create a potential security risk due to which of the following?

A. Operating system incompatibility
B. Large storage capacity
C. Widespread use
D. Potential for software introduction

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
As a best practice, risk assessments should be based upon which of the following?

A. A qualitative measurement of risk and impact

B. A survey of annual loss, potential threats and asset value
C. A quantitative measurement of risk, impact and asset value
D. An absolute measurement of threats

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following is a cryptographic hash function?

A. RSA
B. SHA
C. RC4
D. ECC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
From a security standpoint, which of the following is the BEST reason to implement performance monitoring applications on network systems?

A. To detect network intrusions from external attackers
B. To detect integrity degradations to network attached storage
C. To detect host intrusions from external networks
D. To detect availability degradations caused by attackers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
All of the following are methods used to conduct risk assessments EXCEPT:

A. penetration tests.
B. security audits.
C. vulnerability scans.

D. disaster exercises.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
After conducting a risk assessment, the main focus of an administrator should be which of the following?

A. To report the results of the assessment to the users
B. To ensure all threats are mitigated
C. To ensure all vulnerabilities are eliminated
D. To ensure risk mitigation activities are implemented

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following is a BEST practice when implementing a new system?

A. Disable unneeded services.
B. Use group policies.
C. Implement open source alternatives.
D. Use default installations.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
When installing and securing a new system for a home user which of the following are best practices? (Select THREE).

A. Use a strong firewall.
B. Block inbound access to port 80
C. Apply all system patches.
D. Use input validation.
E. Install remote control softwarE.
F. Apply all service packs.

Correct Answer: ACF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following describes a logic bomb?

A. A piece of malicious code that can spread on its own
B. A piece of malicious code that is concealed from all detection
C. A piece of malicious code that executes based on an event or date
D. A piece of malicious code that exploits a race condition

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following is a prerequisite for privilege escalation to occur?

A. The attacker has to create their own zero day attack for privilege escalation.
B. The attacker must already have physical access to the system.
C. The attacker must use a rootkit in conjunction with privilege escalation.
D. The attacker must have already gained entry into the system.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is an example of an attack that executes once a year on a certain date?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following is the GREATEST threat to highly secure environments?

A. Network attached storage
B. BIOS configuration
C. RSA256
D. USB devices

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Management has asked a technician to prevent data theft through the use of portable drives. Which of the following should the technician implement?

A. Install a CCTV system.
B. Use security templates.
C. Implement a biometric system.
D. Disable USB drives.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A technician has been informed that many of the workstations on the network are flooding servers. Which of the following is the MOST likely cause of this?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following BEST describes a way to prevent buffer overflows?

A. Apply all security patches to workstations.
B. Apply security templates enterprise widE.
C. Apply group policy management techniques.
D. Monitor P2P program usage through content filters.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which of the following is a security reason to implement virtualization throughout the network infrastructure?

A. To analyze the various network traffic with protocol analyzers
B. To centralize the patch management of network servers
C. To isolate the various network services and roles
D. To implement additional network services at a lower cost

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following is a reason to use a Faraday cage?

A. To allow wireless usage
B. To minimize weak encryption
C. To mitigate data emanation
D. To find rogue access points

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Weak encryption is a common problem with which of the following wireless protocols?

A. WPA2-Enterprise
B. WEP
C. WPA2-Personal
D. WPA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following describes a tool used by organizations to verify whether or not a staff member has been involved in malicious activity?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following is a cross-training technique where organizations minimize collusion amongst staff?

A. Least privilege
B. Job rotation
C. Cross-site scripting
D. Separation of duties

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following will allow a technician to restrict a users access to the GUI?

A. Access control lists
B. Group policy implementation
C. Use of logical tokens
D. Password policy enforcement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following is the MOST common logical access control method?

A. Access control lists
B. Usernames and password
C. Multifactor authentication
D. Security ID badges

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following verifies control for granting access in a PKI environment?

A. System administrator
B. Certificate authority
C. Recovery agent

D. Certificate revocation list

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following explains the difference between a public key and a private key?

A. The public key is only used by the client while the private key is available to all. Both keys are mathematically relateD.
B. The private key only decrypts the data while the public key only encrypts the datA. Both keys are mathematically relateD.
C. The private key is commonly used in symmetric key decryption while the public key is used in asymmetric key decryption.
D. The private key is only used by the client and kept secret while the public key is available to all.WBerlinSans

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following is a countermeasure when power must be delivered to critical systems no matter what?

A. Backup generator
B. Redundant power supplies
C. Uninterruptible power supplies (UPSs)
D. Warm site

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following is the MOST important step to conduct during a risk assessment of computing systems?

A. The identification of USB drives
B. The identification of missing patches
C. The identification of mantraps
D. The identification of disgruntled staff members

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following tools will allow a technician to detect security-related TCP connection anomalies?

A. Logical token
B. Performance monitor
C. Public key infrastructure
D. Trusted platform module

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following monitoring methodologies will allow a technician to determine when there is a security related problem that results in an abnormal condition?

A. Signature-based
B. NIDS
C. Anomaly-based
D. NIPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following systems is BEST to use when monitoring application activity and modification?

A. RADIUS
B. OVAL
C. HIDS
D. NIDS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following is the MOST important thing to consider when implementing an IDS solution?

A. The cost of the device
B. Distinguishing between false negatives
C. Distinguishing between false positives
D. The personnel to interpret results

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is the FIRST step in the implementation of an IDS?

A. Decide on the typE.
B. Decide on the model.
C. Purchase the equipment.
D. Document the existing network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following encryption algorithms is used for encryption and decryption of data?

A. MD5
B. SHA-1
C. NTLM
D. RC5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following are the authentication header modes?

A. Encrypt and Route
B. Transport and Tunnel
C. Tunnel and Encrypt
D. Transport and Encrypt

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following would a technician use to check data integrity?

A. Digital signature algorithm

B. Encapsulating security protocol
C. Rivest cipher 4
D. Message authentication code

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following are the functions of asymmetric keys?

A. Decrypt,decipher, encode and encrypt
B. Sign,validate, encrypt and verify
C. Decrypt,validate, encode and verify
D. Encrypt, sign, decrypt and verify

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following is the purpose of the AH?

A. Provides non-repudiation
B. Provides integrity
C. Provides authorization
D. Provides confidentiality

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following describes the insertion of additional bytes of data into a packet?

A. Header injection
B. TCP hijacking
C. Encapsulating
D. Padding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following is true regarding authentication headers (AH)?

A. The authentication information is a keyed hash based on all of the bytes in the packet.
B. The authentication information hash will increase by one if the bytes remain the same on transfer.
C. The authentication information hash will remain the same if the bytes change on transfer.
D. The authentication information may be the same on different packets if the integrity remains in placE.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following will allow wireless access to network resources based on certain ports?

A. 80211n
B. 80211g
C. 8021x
D. 80211a

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
The method of controlling how and when users can connect in from home is called which of the following?

A. Remote access policy
B. Terminal access control
C. Virtual Private Networking (VPN)
D. Remote authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following is the main limitation with biometric devices?

A. The false rejection rate
B. They are expensive and complex
C. They can be easily fooled or bypassed
D. The error human factor

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Who is ultimately responsible for the amount of residual risk?

A. The senior management
B. The security technician
C. The organizations security officer
D. The DRP coordinator

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following typically use IRC for command and control activities?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
When designing a firewall policy, which of the following should be the default action?

A. Least privilege
B. Implicit allow
C. DMZ
D. Implicit deny

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
If hashing two different files creates the same result, which of the following just occurred?

A. A duplication

B. A collision
C. A pseudo-random event
D. Amirror

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following type of protection is hashing used to provide?

A. Integrity
B. Cryptographic randomness
C. Collision
D. Confidentiality

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
All of the following are part of the disaster recovery plan EXCEPT:

A. obtaining management buy-in.
B. identifying all assets.
C. system backups.
D. patch management softwarE.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following is MOST likely to make a disaster recovery exercise valuable?

A. Revising the disaster recovery plan during the exercise
B. Conducting intricate, large-scale mock exercises
C. Learning from the mistakes of the exercise
D. Management participation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following allows directory permissions to filter down through the sub-directory hierarchy?

A. Impedance
B. Inheritance
C. Mirroring
D. Replication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following access control models BEST follows the concept of separation of duties?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following would MOST likely prevent a PC application from accessing the network?

A. Virtualization
B. Host-based firewall
C. Antivirus
D. HIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
A technician is investigating intermittent switch degradation. The issue only seems to occur when the buildings roof air conditioning system runs. Which of the following would reduce the connectivity issues?

A. Adding a heat deflector
B. Redundant HVAC systems
C. Shielding
D. Add a wireless network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A technician tracks the integrity of certain files on the server. Which of the following algorithms provide this ability?

A. SHA-1
B. 3DES
C. XOR
D. AES

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following describes the standard load for all systems?

A. Configuration baseline
B. Group policy
C. Patch management
D. Security template

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
When testing a newly released patch, a technician should do all of the following EXCEPT:

A. verify the integrity of the patch.
B. deploy immediately using Patch Management.
C. verify the patch is relevant to the system.
D. test it in a non-production environment.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
A botnet zombie is using HTTP traffic to encapsulate IRC traffiC. Which of the following would detect this encapsulated traffic?

A. Vulnerability scanner
B. Proxy server
C. Anomaly-based IDS
D. Rootkit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Documentation review, log review, rule-set review, system configuration review, network sniffing, and file integrity checking are examples of:

A. active security testing techniques.
B. invasive security testing techniques.
C. black box testing techniques.
D. passive security testing techniques.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
To determine whether a system is properly documented and to gain insight into the systems security aspects that are only available through documentation is the purpose of:

A. hybrid security testing techniques.
B. active security testing techniques.
C. passive security testing techniques.
D. invasive security testing techniques.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following BEST describes external security testing?

A. Conducted from outside the perimeter switch but inside the firewall
B. Conducted from outside the building that hosts the organizations servers
C. Conducted from outside the organizations security perimeter
D. Conducted from outside the perimeter switch but inside the border router

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 62
Port scanners can identify all of the following EXCEPT:

A. applications.
B. operating systems.
C. vulnerabilities.
D. active hosts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
All of the following are limitations of a vulnerability scanner EXCEPT:

A. it only uncovers vulnerabilities for active systems.
B. it generates a high false-positive error ratE.
C. it relies on a repository of signatures.
D. it generates less network traffic than port scanning.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which of the following can BEST aid in preventing a phishing attack?

A. Implementing two-factor authentication
B. Enabling complex password policies
C. Conducting user awareness training
D. Requiring the use of stronger encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A travel reservation company conducts the majority of its transactions through a public facing website.

Any downtime to this website results in substantial financial damage for the company. One web server is connected to several distributed database servers. Which of the following describes this scenario?

A. Warm site
B. Proxy server
C. RAID
D. Single point of failure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following is MOST commonly used to secure a web browsing session?

A. SHTTP
B. SSH
C. HTTPS
D. S/MIME

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
One of the reasons that DNS attacks are so universal is DNS services are required for a computer to access:

A. WLANs.
B. the Internet.
C. LANs.
D. WANs.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
One of the security benefits to using virtualization technology is:

A. if an instance is compromised the damage can be compartmentalizeD.
B. applying a patch to the server automatically patches all instances.
C. if one instance is compromised no other instances can be compromiseD.
D. virtual instances are not affected by conventional port scanning techniques.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A virtual server implementation attack that affects the:

A. OS kernel will affect all virtual instances.
B. disk partition will affect all virtual instances.
C. system registry will affect all virtual instances.
D. RAM will affect all virtual instances.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
An administrator wants to set up a new web server with a static NAT. Which of the following is the BEST reason for implementing NAT?

A. Publishes the organizations internal network addressing scheme
B. Publishes the organizations external network addressing scheme
C. Hides the organizations internal network addressing scheme
D. Hides the organizations external network addressing scheme

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following is the BEST reason for an administrator to use port address translation (PAT) instead of NAT on a new corporate mail gateway?

A. PAT provides the mail gateway with protection on port 24
B. PAT allows external users to access the mail gateway on random ports.
C. PAT provides the mail gateway with protection on port 25
D. PAT allows external users to access the mail gateway on pre-selected ports.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following describes a static NAT?

A. A static NAT uses a one to many mapping.
B. A static NAT uses a many to one mapping.

C. A static NAT uses a many to many mapping.
D. A static NAT uses a one to one mapping.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following if disabled will MOST likely reduce, but not eliminate the risk of VLAN jumping?

A. LAN manager
B. ARP caching
C. DTP on all ports
D. TACACS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
An administrator is concerned that PCs on the internal network may be acting as zombies participating in external DDoS attacks. Which of the following could BEST be used to confirm the administrators suspicions?

A. HIDS logs
B. Proxy logs
C. AV server logs
D. Firewall logs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Restricting access to files based on the identity of the user or group is an example of which of the following?

A. CRL
B. PKI
C. MAC
D. DAC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Restricting access to files based on the identity of the user or group and security classification of the information is an example of which of the following?

A. RBAC
B. DAC
C. NTFS
D. MAC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
A new Internet content filtering device installed in a large financial institution allows IT administrators to log in and manage the device, but not the content filtering policy. Only the IT security operation staff can modify policies on the Internet filtering devicE. Which of the following is this an example of?

A. Role-Based Access Control (RBAC)
B. Mandatory Access Control (MAC)
C. Lightweight Directory Access Protocol (LDAP)
D. Discretionary Access Control (DAC)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following would BEST describe a disaster recovery plan (DRP)?

A. Addresses the recovery of an organizations business documentation
B. Addresses the recovery of an organizations email
C. Addresses the recovery of an organizations backup site
D. Addresses the recovery of an organizations IT infrastructure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following is the primary objective of a business continuity plan (BCP)?

A. Addresses the recovery of an organizations business operations
B. Addresses the recovery of an organizations business payroll system
C. Addresses the recovery of an organizations business facilities

D. Addresses the recovery of an organizations backup site

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A software manufacturer discovered a design flaw in a new application. Rather than recall the software, management decided to continue manufacturing the product with the flaw. Which of the following risk management strategies was adopted by management?

A. Risk mitigation
B. Risk avoidance
C. Risk acceptance
D. Risk transfer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following BEST describes an application or string of code that cannot automatically spread from one system to another but is designed to spread from file to file?

A. Adware
B. Worm
C. Botnet
D. Virus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following is considered an independent program that can copy itself from one system to another and its main purpose is to damage data or affect system performance?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
All of the following are considered malware EXCEPT:

A. spam.
B. Trojan.
C. virus.
D. logical bombs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following NIDS configurations is solely based on specific network traffic?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following only looks at header information of network traffic?

A. Internet content filter
B. Packet filter
C. Application firewall
D. Hybrid firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following access control methods could the administrator implement because of constant hiring of new personnel?

A. Rule-based
B. Role-based
C. Discretionary
D. Decentralized

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
When using a single sign-on method, which of the following could adversely impact the entire network?

A. Workstation
B. Biometrics
C. Web server
D. Authentication server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
RADIUS uses all of the following authentication protocols EXCEPT:

A. PAP.
B. CHAP.
C. EAP.
D. L2TP.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
A HIDS is installed to monitor which of following?

A. CPU performance
B. NIC performance
C. System files
D. Temporary Internet files

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following intrusion detection systems uses statistical analysis to detect intrusions?

A. Signature
B. Honeynet
C. Anomaly
D. Knowledge

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following intrusion detection systems uses well defined models of how an attack occurs?

A. Protocol
B. Behavior
C. Signature
D. Anomaly

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following is a system that will automate the deployment of updates to workstations and servers?

A. Service pack
B. Remote access
C. Patch management
D. Installer package

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A user is concerned with the security of their laptops BIOS. The user does not want anyone to be able to access control functions except themselves. Which of the following will make the BIOS more secure?

A. Password
B. Encrypt the hard drive
C. Create an access-list
D. Flash the BIOS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Which of the following is a method to apply system security settings to all workstations at once?

A. Policy analyzer
B. Patch management
C. Configuration baseline
D. A security template

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which of the following would be a method of securing the web browser settings on all network workstations?

A. Internet content filter
B. Group policy
C. Control panel
D. P2P software

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following is a limitation of a HIDS?

A. It does not capture MAC addresses.
B. Someone must manually review the logs.
C. It requires an open port on the firewall.
D. They are difficult to install.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
A technician has implemented a new network attached storage solution for a client. The technician has created many shares on the storagE. Which of the following is the MOST secure way to assign permissions?

A. Separation of duties
B. Full control
C. Authentication

D. Least privilege

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following is an example of a trust model?

A. SSL/TLS
B. Internet key exchange
C. Recovery agent
D. Managing the CA relationships

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following is the common mail format for digitally signed and encrypted messages?

A. SMTP
B. SSL
C. MIME
D. S/MIME

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following is the common way of implementing cryptography on network devices for encapsulating traffic between the device and the host managing them?

A. S/MIME
B. SNMP
C. SSH
D. SMTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101

Which of the following is a security reason to implement virtualization throughout the network infrastructure?

A. To analyze the various network traffic with protocol analyzers
B. To centralize the patch management of network servers
C. To isolate the various network services and roles
D. To implement additional network services at a lower cost

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A user is receiving an error which they have not seen before when opening an application. Which of the following is MOST likely the cause of the problem?

A. A patch was pushed out.
B. A signature update was completed on the NIPS.
C. The NIDS baseline has been updateD.
D. The HIDS baseline has been updateD.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Which of the following is a system setup to distract potential attackers?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Applying a service pack could affect the baseline of which of the following?

A. Honeynet
B. Heuristic-based NIDS
C. Signature-based NIDS
D. Signature-based NIPS

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

Exam F

QUESTION 1
Which of the following describes penetration testing?

A. Simulating an actual attack on a network
B. Hacking into a network for malicious reasons
C. Detecting active intrusions
D. Establishing a security baseline

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
When an IDS is configured to match a specific traffic pattern, then which of the following is this referring to?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
An application that gets downloaded onto a system by appearing to be a useful tool for cleaning out duplicate contacts in a users emails would be considered:

A. spyware.
B. spam.
C. a worm.
D. a Trojan.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Installing an application on every desktop in a companys network that watches for possible intrusions would be an example of:

A. a HIDS.
B. a personal software firewall.
C. hardening.

D. a NIDS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
An administrator suspects an issue retrieving files on the network and accesses the file servers performance monitor to check the results against:

A. the performance baselinE.
B. yesterdays performancE.
C. the system monitor.
D. themanufacturers websitE.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
An administrator runs a tool checking SMTP, DNS, POP3, and ICMP packets on the network. This is an example of which of the following?

A. A port scanner
B. A protocol analyzer
C. A vulnerability scan
D. A penetration test

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
A company runs a backup after each shift and the main concern is how quickly the backups are completed between shifts. Recovery time should be kept to a minimum. The administrator decides that backing up all the data that has changed during the last shift is the best way to go. This would be considered a:

A. differential backup.
B. incremental backup.
C. shadow copy.
D. full backup.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Users should be able to access their email and several secure applications from any workstation on the network. Additionally, the administrator has implemented an authentication system requiring the use of a username, password, and a company issued smart card. Which of the following is this an example of?

A. Three factor authentication
B. SSO
C. ACL
D. Least privilege

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Both the client and the server authenticate before exchanging datA. This is an example of:

A. biometrics.
B. multifactor authentication.
C. mutual authentication.
D. SSO.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following could be used to institute a tunneling protocol for security?

A. IPX/SPX
B. EAP
C. IPSec
D. FTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following is an encryption program used to secure email and voice over the Internet?

A. PGP
B. S/MIME
C. ECC

D. Blowfish

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following is used for securing communication between a client and a server?

A. NTLM
B. SHA-1
C. MD5
D. SMTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following processes are used to monitor and protect the DNS server?

A. Ping the DNS server every minute to verify connectivity.
B. Use personal firewalls to block port 53
C. Check DNS records regularly.
D. Set PTR records to purge daily.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following is the MOST effective method for stopping a phishing attempt?

A. Up-to-date antivirus definitions
B. Paper shredders
C. User education
D. SPAM filters

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A corporation has a contractual obligation to provide a certain amount of system uptime to a client. Which of the

following is this contract an example of?

A. PII
B. SLA
C. Due diligence
D. Redundancy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following would allow for a network to remain operational after a T1 failure?

A. Uninterruptible Power Supply (UPS)
B. Redundant ISP
C. Redundant servers
D. RAID 5 drive array

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following asymmetric encryption algorithms was utilized FIRST?

A. AES
B. Serpent
C. Whirlpool
D. DES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A ticket granting server is an important concept in which of the following authentication models?

A. PAP
B. RADIUS
C. Kerberos
D. CHAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following is an example of two-factor authentication?

A. User ID and password
B. Smart card and PIN
C. Fingerprint reader and iris scanner
D. Smart card and ID badge

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following could physically damage a device if a long term failure occurred?

A. OVAL
B. HVAC
C. Battery backup system
D. Shielding

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following is the easiest way to disable a 10Base2 network?

A. Introduce crosstalk.
B. Install a zombiE.
C. Remove a terminator.
D. Remove a vampire tap.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following is the BEST method for securing the data on a coaxial network?

A. Weld all terminators to the cable ends.
B. Run all cables through a conduit.
C. Make sure all terminators are groundeD.

D. Run all new cables parallel to existing alternating current (AC) cabling.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following is the weakest password?

A. Indu5tr1als
B. F%r3Walke3r
C. C0mpt!a2**8
D. P^s5W0rd

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following is the GREATEST security risk regarding removable storage?

A. Integrity of data
B. Not enough space available
C. Availability of data
D. Confidentiality of data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following mimics a legitimate program in order to steal sensitive data?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following allows for a user to have only the minimum level of access required for their job duties?

A. Least privilege
B. Privilege escalation
C. Job rotation
D. Implicit deny

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
A manager needs to control employee overtimE. Which of the following would BEST allow for the manager to control when the employees are on the network?

A. Access control list
B. User account expiration
C. Time of day restriction
D. Domain password policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following BEST describes hashing?

A. Encrypting the data payload and computing a unique mathematic identifier in order to detect change during transport.
B. Computing a unique mathematic identifier in order to prevent change during transport.
C. Encrypting the data payload and computing a unique mathematic identifier in order to prevent change during transport.
D. Computing a unique mathematic identifier in order to detect change during transport.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following is MOST likely to crash a workstation?

A. Vulnerability assessment
B. Protocol analyzer
C. Penetration test
D. Network mapper

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following is the critical piece of an encrypted communication that must be kept secret?

A. The key exchange algorithm
B. The initial salt value
C. The encryption algorithm
D. The final CRC of the key packet

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A PC is rejecting push updates from the server; all other PCs on the network are accepting the updates successfully. Which of the following should the administrator check FIRST?

A. Pop-up blocker
B. Local firewall
C. Password expiration
D. Anti-spyware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following describes an encrypted connection across public communication lines?

A. TACACS
B. VPN
C. EAP
D. CHAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
After a period of high employee turnover, which of the following should be implemented?

A. A review of NTLM hashes on the domain servers

B. A review of group policies
C. A review of user access and rights
D. A review of storage and retention policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
All PCs in a network share a single administrator ID and passworD. When the administrator attempts to remotely control a users PC the attempt fails.Which of the following should the administrator check FIRST?

A. The antivirus settings on the local PC
B. The antivirus settings on the remote PC
C. The HIPS on the remote PC
D. The HIPS on the local PC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
All of the following are considered key exchange protocols EXCEPT:

A. Diffie-Hellman.
B. KEA.
C. RSA.
D. SAFER.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following keys is generally applied FIRST to a message digest to provide non- repudiation using asymmetric cryptography?

A. Privatekey of the receiver
B. Privatekey of the sender
C. Public key of the sender
D. Public key of the receiver

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following describes a weakness of the hash functions?

A. Collision
B. Birthday attack
C. Collusion
D. Man-in-the-middle

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
All of the following are organizational policies that reduce the impact of fraud EXCEPT:

A. separation of duties.
B. password complexity rules.
C. job rotation.
D. escorting procedures.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A technician is conducting a forensics analysis on a computer system. Which of the following should be done FIRST?

A. Look for hidden files.
B. Analyze temporary files.
C. Get a binary copy of the system.
D. Search for Trojans.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A technician noticed a remote attack taking place on a system. Which of the following should be done FIRST?

A. Contain the attack.
B. Respond to the attacker.
C. Disconnect the system from the network.

D. Follow the incident management procedure in placE.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following IDS generally follows a learning process?

A. Anomaly-based IDS
B. Signature-based IDS
C. Event-based IDS
D. Rule-based IDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following algorithms is faster when encrypting data?

A. Symmetric key algorithms
B. Public key algorithms
C. Whole disk encryption algorithms
D. Asymmetric key algorithms

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following is a reason why DNS logs should be archived?

A. For complying with payment card industry (PCI) requirements
B. For complying with PII requirements
C. For use in disaster recovery of the DNS server
D. For use in an investigation in the future

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following is a best practice for securing log files?

A. Copy or save the logs to a remote log server.
B. Log all failed and successful login attempts.
C. Deny administrators all access to log files to prevent write failures.
D. Change security settings to avoid corruption.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following logs shows when the workstation was last shutdown?

A. DHCP
B. Security
C. Access
D. System

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following is a best practice auditing procedure?

A. Mitigate vulnerabilities
B. Review user access and rights
C. Set strong password requirements
D. Draft an email retention policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following tools is commonly used to detect security anomalies on a host?

A. A file system integrity checker
B. A TACACS+ implementation
C. A remote protocol analyzer
D. A network mapper

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Snort, TCPDump and Wireshark are commonly used for which of the following?

A. Port scanning
B. Host monitoring
C. DDOS attacks
D. Network sniffing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following would typically require the use of a network protocol analyzer?

A. Determining who logged on to a machine last night atmidnight
B. Determining how many users are logged onto the domain controller
C. Determining why authentication between two machines failed
D. Determining what the speed is on the external interface of a firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following security related anomalies are MOST likely to be detected by a protocol analyzer?

A. Many malformed or fragmented packets
B. Decryption of encrypted network traffic
C. Disabled network interface on a server
D. Passive sniffing of local network traffic

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Users and computers are generally grouped into domains for security purposes.Which of the following is a common attribute used to determine which domain a user or computer belongs to?

A. MAC address
B. Location
C. Password

D. OS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Malware that uses virtualization techniques can be difficult to detect because of which of the following?

A. A portion of the malware may have been removed by the IDS.
B. The malware may be using a Trojan to infect the system.
C. The malware may be implementing a proxy server for command and control.
D. The malware may be running at a more privileged level than the antivirus softwarE.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following is a reason why virtualization techniques are often used to implement a honeynet?

A. To reduce the number of physical devices needed
B. To hide the encryption being used in the honeynet
C. To slow the intruders network connection speed
D. To reduce the number of connections allowed

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following is an industry standard for remote logging?

A. ipfilter
B. RDP
C. rlogin
D. syslog

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Audit trails are used for which of the following?

A. Availability
B. Accountability
C. Authorization
D. Continuity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following can be used to centrally manage security settings?

A. Cross-site scripting
B. Group policy
C. Service pack
D. NIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following is a best practice disaster recovery strategy?

A. Use a reciprocal agreement.
B. Spend at least 5% of the IT budget.
C. Hire an independent consultant.
D. Test the recovery plan.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following activities is MOST closely associated with DLL injection?

A. Penetration testing
B. Network mapping
C. Vulnerability assessment
D. SQL servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following is true about penetration testing or vulnerability assessments?

A. Vulnerability assessment verifies incidence response
B. Penetration testing removes malware if found during a scan
C. Vulnerability assessment exploits a weakness in a system
D. Penetration testing exploitsa vulnerability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following is a security risk of not password protecting the BIOS?

A. The system may be changed to boot from alternative mediA.
B. The antivirus software will not run because it needs a BIOS passworD.
C. A virus may corrupt the SCSI settings and the system will not boot.
D. The authentication system may be subverteD.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Executing proper logging procedures would be the proper course of action in which of the following scenarios? (Select TWO).

A. Need to prevent access to a file or folder
B. Need to know which files have been accessed
C. Need to know who is logging on to the system
D. Need to prevent users from logging on to the system
E. Need to capture monitor network traffic in real time

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Executing proper logging procedures would facilitate which of the following requirements?

A. Ignore suspicious queries to the DNS server.
B. Investigate suspicious queries to the DNS server.

C. Block suspicious queries to the DNS server.
D. Monitor suspicious queries to the DNS server in real timE.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following is a concern when setting logging to a debug level?

A. The log may fill up with extraneous information.
B. The device or application will only operate in test modE.
C. Some important events will not get loggeD.
D. The events may not contain enough details.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which of the following should be considered when executing proper logging procedures? (Select TWO).

A. The information that is needed to reconstruct events
B. The number of disasters that may occur in one year
C. The password requirements for user accounts
D. The virtual memory allocated on the log server
E. The amount of disk space required

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following malicious activities might leave traces in a DNS log file?

A. Hijacking
B. Poisoning
C. Caching
D. Phishing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following NAC scanning types is the LEAST intrusive to the client?

A. Open ID
B. Agent based
C. Agentless
D. ActiveX

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Common settings configured on an Internet content filtering device are database update settings, log settings and which of the following?

A. False positive threshold
B. Content rules
C. Anomaly settings
D. Performance settings

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which of the following activities commonly involves feedback from departmental managers or human resources?

A. Clearing cookies from the browser
B. Resetting an employee password
C. User access and rights review
D. Setting system performance baseline

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
While auditing a list of active user accounts, which of the following may be revealed?

A. Accounts with weak passwords
B. Passwords with dictionary words
C. Passwordsthat are blank
D. Accounts that need to be removed

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following is the BEST option for securing an email infrastructure?

A. Set up an email proxy on the Internet and an email server in the internal network.
B. Set up an email proxy on the Internet and an email server in the DMZ.
C. Set up the email server in a DMZ.
D. Set up an email proxy in the DMZ and the email server in the internal network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following provides the BEST mechanism for non-repudiation?

A. Encryption
B. Message digests
C. Digital signatures
D. Message authentication codes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following is the BEST logical access control method for controlling system access on teams working in shifts?

A. Separation of duties
B. Job rotation
C. Time of day restrictions
D. Least privilege

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following key types does Kerberos use?

A. Ticket Grating Service
B. Symmetric keys
C. Asymmetric keys
D. Key Distribution Center

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following are recommended security measures when implementing system logging procedures? (Select TWO).

A. Perform a binary copy of the system.
B. Apply retention policies on the log files.
C. Collect system temporary files.
D. Perform hashing of the log files.
E. Perform CRC checks.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following should be considered when implementing logging controls on multiple systems? (Select TWO).

A. VLAN segment of the systems
B. Systems clock synchronization
C. Systems capacity and performance
D. External network traffic
E. Network security zone of the systems

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which of the following BEST describes actions pertaining to user account reviews? (Select TWO).

A. User account reports are periodically extracted from systems and employment verification is performeD.
B. User accounts and their privileges are periodically extracted from systems and reports are kept for auditing purposes.
C. User accounts and their privileges are periodically extracted from systems and are reviewed for the appropriate level of authorization.

D. User accounts reports are periodically extracted from systems and end users are informed.
E. User accounts reports are periodically extracted from systems and user access dates are verified

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
All of the following are attributes of an x.509 certificate EXCEPT:

A. the symmetric key of the owner.
B. the public key of the owner.
C. the version of the certificatE.
D. the issuer.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
A user complains that pop-up windows continuously appear on their screen with a message stating that they have a virus and offering to see a program that will remove it. The technician is skeptical because the antivirus definitions on the machine are up-to-datE. Which of the following BEST describes what the user is seeing?

A. SQL injection
B. Spyware
C. Adware
D. SMTP open relay

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
The GREATEST security concern in regards to data leakage with USB devices is:

A. speeD.
B. physical sizE.
C. OS compatibility.
D. storage capacity.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following is the main difference between a substitution cipher and a transposition cipher when used to encode messages?

A. One rearranges and replaces blocks while the other rearranges only.
B. One replaces blocks with other blocks while the other rearranges only.
C. One replaces blocks while the other rearranges and replaces only.
D. One is a symmetric block cipher and the other is asymmetriC.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
All of the following can be found in the document retention policy EXCEPT:

A. type of storage mediA.
B. password complexity rules.
C. physical access controls.
D. retention periods.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following reduces effectiveness when deploying and managing NIPS?

A. Encrypting all network traffic
B. Continued tuning
C. Network placement
D. Reviewing the logs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following authentication methods prevents a replay attack from occurring?

A. L2TP
B. CHAP
C. Kerberos
D. RADIUS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
To prevent disk integrity errors due to small line-power fluctuations, a system administrator should install which of the following?

A. Voltage regulator
B. Line conditioner
C. Battery backup
D. Redundant power supplies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following is the BEST way to mass deploy security configurations to numerous workstations?

A. Security hotfix
B. Configuration baseline
C. Patch management
D. Security templates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Virtual machines are MOST often used by security researchers for which of the following purposes?

A. To provide a secure virtual environment to conduct online deployments
B. To provide a virtual collaboration environment to discuss security research
C. To provide an environment where new network applications can be tested
D. To provide an environment where malware can be executed with minimal risk to equipment and software

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following is a password cracker?

A. CORE Impact
B. Cain & Abel
C. WireShark
D. NMAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following characteristics of RAID increases availability?

A. Striping without parity
B. Mirroring
C. Kiting
D. Low cost

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
A document shredder will BEST prevent which of the following?

A. Dumpster diving
B. Phishing
C. Shoulder surfing
D. Viruses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following would BEST prevent the spread of a hoax?

A. Chain of custody
B. User education
C. Up-to-date antivirus definitions
D. Up-to-date anti-spyware definitions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following is a term referring to the situation when a programmer leaves an unauthorized entry point into a program or system?

A. Back door
B. Default account
C. Poisoning
D. Privilege escalation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following refers to a system that is unable to accept new TCP connections due to a SYN flood attack?

A. Airsnort
B. Smurf
C. Teardrop
D. DoS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following would refer to a key fob with a periodically changing number that is used as part of the authentication process?

A. Installation key
B. Biometric device
C. Hardware lock
D. Physical token

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Which of the following is the MOST common method of one-factor authentication?

A. Smart card and a PIN

B. Physical token and a password
C. Fingerprint reader
D. User ID and password

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
An attorney demands to know exactly who had possession of a piece of evidence at a certain time after seizurE. Which of the following documents would provide this?

A. Due diligence
B. Chain of custody
C. Due process
D. Change management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following prevents damage to evidence during forensic analysis?

A. Write-only drive connectors
B. Drive sanitization tools
C. Read-only drive connectors
D. Drive recovery tools

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which of the following is a drawback of using PAP authentication?

A. PAP only authenticates between same vendor servers.
B. PAP requires that both workstations mutually authenticatE.
C. PAP changes its initialization vector with each packet.
D. PAP sends all passwords across the network as clear text.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following BEST describes using a third party to store the public and private keys?

A. Public key infrastructure
B. Recovery agent
C. Key escrow
D. Registration authority

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following requires the server to periodically request authentication from the client?

A. EAP
B. CHAP
C. WPA2
D. RAS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
A biometric fingerprint scanner is an example of which of the following?

A. Two-factor authentication
B. SSO
C. Three-factor authentication
D. Single-factor authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
An administrator suspects an issue retrieving files on the network and accesses the file servers performance monitor to check the results against:

A. the performance baselinE.
B. yesterdays performancE.
C. the system monitor.
D. themanufacturers websitE.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Which of the following would a former employee MOST likely plant on a server that is not traceable?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Which of the following BEST describes the practice of dumpster diving?

A. Sorting through the garbage of an organization to obtain information used for configuration management.
B. Sorting through the garbage of an organization to obtain information used for a subsequent attack.
C. Sorting through the trash of an organization to obtain information found on their intranet.
D. Sorting through the trash of an organization to recover an old user ID badge previously used for an attack.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Exam G

QUESTION 1
A user ID, PIN, and a palm scan are all required to authenticate a system. Which of the following is this an example of?

A. SSO
B. Two-factor authentication
C. Single-factor authentication
D. Three-factor authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following would be disabled to prevent SPIM?

A. P2P
B. ActiveX controls
C. Instant messaging
D. Internet mail

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A user sees an MD5 hash number beside a file that they wish to downloaD. Which of the following BEST describes a hash?

A. A hash is a unique number that is generated based upon the TCP/IP transmission header and should be verified before downloaD.
B. A hash is a unique number that is generated based upon the files contents and used as the SSL key during downloaD.
C. A hash is a unique number that is generated after the file has been encrypted and used as the SSL key during downloaD.
D. A hash is a unique number that is generated based upon the files contents and should be verified after downloaD.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
According to a good disaster recovery plan, which of the following must happen during a power outage before an uninterruptible power supply (UPS) drains its battery?

A. The PKI CA is relocateD.
B. The backup generator activates.
C. The single point of failure is remedieD.
D. Full electrical service is restoreD.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following would give a technician the MOST information regarding an external attack on the network?

A. Internet content filter
B. Proxy server
C. NIDS
D. Firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following would BEST prevent night shift workers from logging in with IDs and passwords stolen from the day shift workers?

A. Account expiration
B. Time of day restriction
C. Account lockout
D. Domain password policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following would BEST ensure that users have complex passwords?

A. ACL
B. Domain password policy
C. Logical tokens
D. Time of day restrictions

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 8
A technician finds that a malicious user has introduced an unidentified virus to a single file on the network. Which of the following would BEST allow for the user to be identified?

A. Access logs
B. Performance log
C. Firewall logs
D. Antivirus logs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following would BEST allow an administrator to find the IP address of an external attacker?

A. Antivirus logs
B. DNS logs
C. Firewall logs
D. Performance logs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
After performing a vulnerability analysis and applying a security patch, which of the following non- intrusive actions should an administrator take to verify that the vulnerability was truly removed?

A. Apply a security patch from the vendor.
B. Perform a penetration test.
C. Repeat the vulnerability scan.
D. Update the antivirus definition filE.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following could be used by a technician needing to send data while ensuring that any data tampering is easily detectible?

A. NTLM
B. LANMAN
C. SHA-1
D. AES

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following BEST allows for a high level of encryption?

A. AES with ECC
B. DES with SHA-1
C. PGP with SHA-1
D. 3DES with MD5

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is the primary security risk associated with removable storage?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
After reading about the vulnerability issues with open SMTP relays, a technician runs an application to see if port 25 is open. This would be considered a:

A. network mapper.
B. protocol analyzer.
C. vulnerabilityscan.
D. port scan.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A companys accounting application requires users to be administrators for the software to function correctly. Because of the security implications of this, a network administrator builds a user profile which allows the user to still use the application but no longer requires them to have administrator permissions.
Which of the following is this an example of?

A. Configuration baseline
B. Group policy
C. Security template
D. Privilege escalation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following backup techniques resets the archive bit and allows for the fastest recovery?

A. Full backup
B. Shadow copies
C. Differential backup
D. Incremental backup

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
The company policy for availability requires full backups on Sunday and incremental backups each week night at 10 p.m. The file server crashes on Wednesday afternoon; how many tapes will the technician need to restore the data on the file server for Thursday morning?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A company is addressing backup and recovery issues. The company is looking for a compromise between speed of backup and speed of recovery. Which of the following is the BEST recommendation?

A. Full backups every day
B. Daily differential backups
C. Full backups weekly with differential backups daily
D. Weekly differential with incremental backups daily

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following would define document destruction requirements?

A. ACL
B. User access and rights review policies
C. Group policy
D. Storage and retention policies

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Part of a standard policy for hardening workstations and servers should include applying the company security template and:

A. installing the NIDS.
B. closing unnecessary network ports.
C. applying all updates, patches and hotfixes immediately.
D. disabling SSID broadcast.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Setting a baseline is required in which of the following? (Select TWO).

A. Anomaly-based monitoring
B. NIDS
C. Signature-based monitoring
D. NIPS
E. Behavior-based monitoring

Correct Answer: AE
Section: (none)

Explanation

Explanation/Reference:

QUESTION 22
Which of the following hidden programs gathers information with or without the users knowledge with the primary purpose of advertising?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following provides best practice with a wireless network?

A. WPA
B. WPA with RADIUS
C. 3DES with RADIUS
D. WEP 128-bit

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following sites has the means (E. g. equipment, software, and communications) to facilitate a full recovery within minutes?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
When conducting an environmental security assessment, which of the following items should be included in the assessment? (Select THREE).

A. HVAC
B. Card access system
C. Off-site data storage
D. Logical access
E. Utilities
F. Fire detection

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following security steps must a user complete before access is given to the network?

A. Authentication and password
B. Identification and authentication
C. Identification and authorization
D. Authentication and authorization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
When placing a NIDS onto the network, the NIC has to be placed in which of the following modes to monitor all network traffic?

A. Promiscuous
B. Full-duplex
C. Auto
D. Half-duplex

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
An administrator wants to obtain a view of the type of attacks that are being targeted against the network perimeter. The recommended placement of a NIDS would be:

A. inside the proxy.
B. inside the DMZ.
C. outside the proxy.
D. outside the firewall.
E. inside the firewall.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Once a system has been compromised, often the attacker will upload various tools that can be used at a later date. The attacker could use which of the following to hide these tools?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following is the perfect encryption scheme and is considered unbreakable when properly used?

A. Running key cipher
B. Concealment cipher
C. One-time pad
D. Steganography

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
When using a digital signature, the message digest is encrypted with which of the following keys?

A. Receivers private key
B. Receivers public key
C. Senders public key
D. Senders private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following is the MOST basic form of IDS?

A. Signature
B. Behavioral
C. Statistical
D. Anomaly

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following BEST applies to steganography?

A. Algorithms are not used to encrypt datA.
B. Algorithms are used to encrypt datA.
C. Keys are used to encrypt datA.
D. Keys are concealed in the datA.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following can steganography be used for?

A. Watermark graphics for copyright.
B. Decrypt data in graphics.
C. Encrypt a message in WAV files.
D. Encrypt data in graphics.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Steganography could be used by attackers to:

A. encrypt and conceal messages in microdots.
B. decrypt data stored in unused disk spacE.
C. encrypt and decrypt messages in graphics.
D. hide and conceal messages in WAV files.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following BEST describes how steganography can be accomplished in graphic files?

A. Replacing the most significant byte of each bit
B. Replacing the least significant byte of each bit
C. Replacing the most significant bit of each byte
D. Replacing the least significant bit of each byte

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
An application developer is looking for an encryption algorithm which is fast and hard to break if a large key size is used. Which of the following BEST meets these requirements?

A. Transposition
B. Substitution
C. Symmetric
D. Asymmetric

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following if used incorrectly would be susceptible to frequency analysis?

A. Asymmetric algorithms
B. Transposition ciphers
C. Symmetric algorithms
D. Stream ciphers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
An administrator in an organization with 33,000 users would like to store six months of Internet proxy logs on a dedicated logging server for analysis and content reporting. The reports are not time critical, but are required by upper management for legal obligations. All of the following apply when determining the requirements for the logging server EXCEPT:

A. log details and level of verbose logging.

B. time stamping and integrity of the logs.
C. performance baseline and audit trails.
D. log storage and backup requirements.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following BEST describes when a hashing algorithm generates the same hash for two different messages?

A. A hashing chain occurreD.
B. A deviation occurreD.
C. A collision occurreD.
D. A one-way hash occurreD.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following is BEST known for self-replication in networks?

A. Spyware
B. Worm
C. Spam
D. Adware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following security threats affects PCs and can have its software updated remotely by a command and control center?

A. Zombie
B. Worm
C. Virus
D. Adware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Multiple web servers are fed from a load balancer. Which of the following is this an example of?

A. RAID
B. Backup generator
C. Hot site
D. Redundant servers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
An outside auditor has been contracted to determine if weak passwords are being used on the network.

To do this, the auditor is running a password cracker against the master password filE. Which of the following is this an example of?

A. Vulnerability assessment
B. Fingerprinting
C. Malware scan
D. Baselining

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Password crackers:

A. are sometimes able to crack both passwords and physical tokens.
B. cannot exploit weaknesses in encryption algorithms.
C. cannot be run remotely.
D. are sometimes able to crack both Windows and UNIX passwords.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Logic bombs differ from worms in that:

A. logic bombs cannot be sent through email.

B. logic bombs cannot spread from computer to computer.
C. logic bombs always contain a Trojan component.
D. logic bombs always have a date or time component.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A firewall differs from a NIDS in which of the following ways?

A. A firewall attempts to detect patterns and a NIDS operates on a rule list.
B. A firewall operates on a rule list and a NIDS attempts to detect patterns.
C. A firewall prevents inside attacks and a NIDS prevents outside attacks.
D. A firewall prevents outside attacks and a NIDS prevents inside attacks.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A vulnerability has recently been identified for a servers OS. Which of the following describes the BEST course of action?

A. Shutdown all affected servers until management can be notifieD.
B. Visit a search engine and search for a possible patch.
C. Wait for an automatic update to be pushed out to the server from the manufacturer.
D. Visit the operating systemmanufacturers website for a possible patch.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Personal software firewalls can be updated automatically using:

A. group policy.
B. cookies.
C. cross-site scripting.
D. corporate hardware firewalls.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
An accountant has logged onto the companys external banking websitE. An administrator using a TCP/IP monitoring tool discovers that the accountant was actually using a spoofed banking websitE. Which of the following could have caused this attack? (Select TWO).

A. Altered hosts file
B. Network mapper
C. Packet sniffing
D. DNS poisoning
E. Bluesnarfing

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following tools would be BEST for monitoring changes to the approved system baseline?

A. Enterprise resource planning software
B. Enterprise performance monitoring software
C. Enterprise antivirus software
D. Enterprise key management software

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
All of the following security applications can proactively detect workstation anomalies EXCEPT:

A. antivirus softwarE.
B. NIDS.
C. personal software firewall.
D. HIPS.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
A periodic security audit of group policy can:

A. show that data is being correctly backed up.
B. show that PII data is being properly protecteD.

C. show that virus definitions are up to date on all workstations.
D. show that unnecessary services are blocked on workstations.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following is the primary purpose of an audit trail?

A. To detect when a user changes security permissions
B. To prevent a user from changing security permissions
C. To prevent a user from changing security settings
D. To detect the encryption algorithm used for files

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following describes a characteristic of the session key in an SSL connection?

A. It is symmetriC.
B. It is a hash valuE.
C. It is asymmetriC.
D. It is an elliptical curvE.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following describes the cryptographic algorithm employed by TLS to establish a session key?

A. RSA
B. Diffie-Hellman
C. Blowfish
D. IKE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following describes how TLS protects against man-in-the-middle attacks?

A. The client compares the actual DNS name of the server to the DNS name on the certificatE.
B. The client relies on the MD5 value sent by the server.
C. The client compares the server certificate with the certificate listed on the CRL.
D. The client relies on the MAC value sent by the server.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following is the primary purpose of removing audit logs from a server?

A. To protect against the log file being changed
B. To demonstrate least privilege to management
C. To reduce network latency
D. To improve the server performance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following describes a common problem encountered when conducting audit log reviews?

A. The timestamp for the servers are not synchronizeD.
B. The servers are not synchronized with the clients.
C. The audit logs cannot be imported into a spreadsheet.
D. The audit logs are pulled from servers on different days.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A technician is conducting a web server audit and discovers that SSLv2 is implementeD. The technician wants to recommend that the organization consider using TLS. Which of the following reasons could the technician use to support the recommendation?

A. SSLv2 reduces server performancE.
B. SSLv2 is susceptible to network sniffing.
C. SSLv2 only uses message authentication code values.
D. SSLv2 is susceptible to man-in-the-middle attacks.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A technician is conducting a password audit using a password cracking tool. Which of the following describes a BEST business practice when conducting a password audit?

A. Use password masking.
B. Use hybrid modE.
C. Reveal the passworD.
D. Single out the accounts to crack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following is a security risk when using peer-to-peer software?

A. Cookies
B. Multiple streams
C. Data leakage
D. Licensing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following overwrites the return address within a program to execute malicious code?

A. Buffer overflow
B. Rootkit
C. Logic bomb
D. Privilege escalation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Heaps and stacks are susceptible to which of the following?

A. Cross-site scripting
B. Rootkits
C. Buffer overflows
D. SQL injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
All of the following are inline devices EXCEPT:

A. NIPS.
B. firewalls.
C. HIDS.
D. routers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following would a technician use to validate whether specific network traffic is indeed an attack?

A. NIDS
B. Firewall
C. Honeypot
D. Protocol analyzer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following creates an emulated or virtual environment to detect and monitor malicious activity?

A. Firewall
B. Honeypot
C. NIDS
D. NAC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A technician wants better insight into the websites that employees are visiting.Which of the following is BEST suited to accomplish this?

A. Proxy server
B. DHCP server
C. DNS server
D. Firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Bluetooth discover mode is similar to which of the following?

A. SSID broadcast
B. Data emanation
C. RF analysis
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
All of the following are Bluetooth threats EXCEPT:

A. bluesnarfing.
B. discovery modE.
C. blue jacking.
D. a smurf attack.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following is the BEST approach when reducing firewall logs?

A. Review chronologically.
B. Discard known traffic first.
C. Search for encrypted protocol usagE.
D. Review each protocol one at a timE.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
In which of the following logs would notation of a quarantined file appear?

A. Antivirus
B. Firewall
C. Router
D. NAC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following provides the MOST mathematically secure encryption for a file?

A. 3DES
B. One-time pad
C. AES256
D. Elliptic curve

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following encryption algorithms relies on the inability to factor large prime numbers?

A. Elliptic Curve
B. AES256
C. RSA
D. SHA-1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
All of the following provide a host active protection EXCEPT:

A. host-based firewall.
B. antivirus.
C. HIPS.
D. HIDS.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which of the following simplifies user and computer security administration?

A. Encrypted file system (EFS)
B. Printing policies
C. Data retention
D. Directory services

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following is MOST likely to cause pop-ups?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following is MOST likely to open a backdoor on a system?

A. Botnet
B. Trojan
C. Logic bomb
D. Worm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
If a company has a distributed IT staff, each being responsible for separate facilities, which of the following would be the BEST way to structure a directory information tree?

A. By department
B. By location
C. By role
D. By name

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A technician wants to be able to add new users to a few key groups by default, which of the following would allow this?

A. Auto-population
B. Template
C. Default ACL
D. Inheritance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following is a reason to use digital signatures?

A. Access control list
B. Non-repudiation
C. Logical token
D. Hardware token

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
All of the following are logical access control methods EXCEPT:

A. biometrics.
B. ACL.
C. software token.

D. group policy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Using the same initial computer image for all systems is similar to which of the following?

A. Group policy
B. Virtual machine
C. Configuration baseline
D. Patch management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following has the LEAST amount of issues when inspecting encrypted traffic?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
A technician has come across content on a server that is illegal. Which of the following should the technician do?

A. Stop and immediately make a backup of the account and contact the owner of the data.
B. Stop and immediatelyfollow company approved incident response procedures.
C. Stop and immediately copy the system files and contact the ISP.
D. Stop and immediately perform a full system backup and contact the owner of the datA.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86

Which of the following is a true statement in regards to incident response?

A. The first thing a technician should perform is a file system backup.
B. The first thing a technician should do is call in law enforcement.
C. If a technician finds illegal content, they should follow company incident response procedures.
D. If a technician finds illegal content, the first thing a technician should do is unplug the machine and back it up.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
If a technician is unable to get to a website by its address but the technician can get there by the IP address, which of the following is MOST likely the issue?

A. DHCP server
B. DNS server
C. Firewall
D. Proxy server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following is placed in promiscuous mode, in line with the data flow, to allow a NIDS to monitor the traffic?

A. Console
B. Sensor
C. Filter
D. Appliance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
In a NIDS, which of the following provides a user interface?

A. Filter
B. Screen
C. Console
D. Appliance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
An instance where an IDS identifies legitimate traffic as malicious activity is called which of the following?

A. False positive
B. True negative
C. False negative
D. True positive

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
An instance where a biometric system identifies legitimate users as being unauthorized is called which of the following?

A. False positive
B. False negative
C. False rejection
D. False acceptance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
An instance where a biometric system identifies users that are authorized and allows them access is called which of the following?

A. False negative
B. True negative
C. False positive
D. True positive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
An instance where an IDS identifies malicious activity as being legitimate activity is called which of the

following?

A. False acceptance
B. False positive
C. False negative
D. False rejection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
An instance where a biometric system identifies unauthorized users and allows them access is called:

A. false rejection.
B. false negativE.
C. false acceptancE.
D. false positivE.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
When executing a disaster recovery plan the MOST important thing to consider is:

A. financial obligations to stockholders.
B. legal and financial responsibilities.
C. data backups and recovery tapes.
D. safety and welfare of personnel.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
When choosing a disaster recovery site, which of the following is the MOST important consideration?

A. The amount of data that will be stored
B. The cost to rebuild the existing facility
C. The amount of emergency rescue personnel
D. The distance and size of the facility

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Who should be notified FIRST before testing the disaster recovery plan?

A. Senior management
B. The physical security department
C. All employees and key staff
D. Human resources

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following BEST describes the disaster recovery plan?

A. A detailed process of recovering information or IT systems after a catastrophic event
B. An emergency plan that will allow the company to recover financially
C. A plan that is put in place to recover the company assets in an emergency
D. A plan that is mandated by law to ensure liability issues are addressed in a catastrophic eventWBerlin Sans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following is the MOST important consideration when developing a disaster recovery plan?

A. Management buy-in
B. The cost of the project
C. The amount of personnel
D. The planning team

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
In order to provide management with a prioritized list of time critical business processes, an administrator would assist in conducting a:

A. risk management matrix.

B. business impact assessment.
C. continuity of operations plan.
D. disaster recovery plan.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which of the following would BEST ensure that users have complex passwords?

A. ACL
B. Domain password policy
C. Logical tokens
D. Time of day restrictions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Which of the following are recommended security measures when implementing system logging procedures? (Select TWO).

A. Perform a binary copy of the system.
B. Apply retention policies on the log files.
C. Collect system temporary files.
D. Perform hashing of the log files.
E. Perform CRC checks.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
A document shredder will BEST prevent which of the following?

A. Dumpster diving
B. Phishing
C. Shoulder surfing
D. Viruses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Exam H

QUESTION 1
Which of the following BEST allows a technician to mitigate the chances of a successful attack against the wireless network?

A. Implement an identification system and WPA2
B. Implement a biometric system and WEP.
C. Implement an authentication system and WPA.
D. Implement an authentication system and WEP.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A technician is reviewing the system logs for a firewall and is told that there is an implicit deny within the ACL. Which of the following is an example of an implicit deny?

A. An ACL is a way to secure traffic from one network to another.
B. An implicitdeny statement denies all traffic from one network to another.
C. Items which are not specifically given access are denied by default.
D. Each item is denied by default because of the implicit deny.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following is the MOST likely reason that an attacker would use a DoS attack?

A. The attacker is attempting to distract the company from the real underlining attack.
B. The attacker wants to prevent authorized users from using a certain servicE.
C. The attacker is working with outside entities to test the companys coding practices.
D. The attacker is working with inside entities to test the companys firewall.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following is a way to gather reconnaissance information from a printer resource?

A. HTTP
B. SMTP
C. RADIUS

D. SNMP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A technician gets informed that there is a worm loose on the network.Which of the following should the technician review to discover the internal source of the worm?

A. Maintenance logs
B. Antivirus logs

C. Performance logs
D. Access logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following BEST allows for the encryption of an entire hard drive?

A. Hashing function
B. Symmetric algorithm
C. Asymmetric algorithm
D. Public key infrastructure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following would a Faraday cage prevent usage of?

A. Cell phone
B. USB key
C. Uninterruptible Power Supply (UPS)
D. Storage drive

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following will allow a technician to block certain HTTP traffic from company staff members?

A. VLAN
B. Content filter
C. DMZ
D. NIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following is a security threat to a workstation that requires interaction from a staff member?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following will prevent a person from booting into removal storage media if the correct boot sequence is already set?

A. BIOS password settings
B. BIOS power on settings
C. USB key settings
D. BIOS boot options

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following ports need to be open to allow a user to login remotely onto a workstation?

A. 53
B. 636
C. 3389
D. 8080

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following, if intercepted, could allow an attacker to access a users email information?

A. Browser cookies
B. Cross-site scripting
C. Cell traffic
D. SMTP traffic

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following would allow a technician to minimize the risk associated with staff running port scanners on the network?

A. Vulnerability scanners
B. Group policy
C. Network mappers
D. Password crackers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following is the MOST effective application to implement to identify malicious traffic on a server?

A. Personal software firewall
B. Enterprise software firewall
C. Antivirus software
D. HIDS software

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following is the MOST appropriate type of software to apply on a workstation that needs to be protected from other locally accessible workstations?

A. Antivirus software
B. Personal software firewall
C. Pop-up blocker software
D. HIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following is a way for a technician to identify security changes on a workstation?

A. Group policy management
B. Service pack application
C. Security templates
D. Configuration baseline

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following is a way to correct a single security issue on a workstation?

A. A patch
B. A service pack
C. Patch management
D. Configuration baseline

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which of the following protects a home user from the Internet?

A. HIDS
B. Personal firewall

C. Anti-malware software

D. Antivirus application

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Computer equipment has been stolen from a companys officE. To prevent future thefts from occurring and to safeguard the companys trade secrets which of the following should be implemented?

A. Video surveillance and access logs

B. ID badges and passwords

C. Multifactor authentication

D. Hardware locks and door access systems

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following is the primary purpose for a physical access log in a data center?

A. Maintain a list of personnel who exit the facility.

B. Allow authorized personnel access to the data center.

C. Prevent unauthorized personnel access to the data center.

D. Maintain a list of personnel who enter the facility.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following biometric authentication devices also carries significant privacy implications due to personal health information that can be discovered during the authentication process?

A. Iris scanner

B. Fingerprint scanner

C. Retina scanner

D. Facial recognition

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
An administrator has already implemented two-factor authentication and now wishes to install a third authentication factor. If the existing authentication system uses strong passwords and PKI tokens which of the following would provide a third factor?

A. Pass phrases
B. Elliptic curve
C. Fingerprint scanner
D. Six digit PINs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
A biometric authentication system consists of all of the following components EXCEPT:

A. reader.
B. credential storE.
C. hardware token.
D. supplicant.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following is an example of remote authentication?

A. A user on a campus area network (CAN) connects to a server in another building and enters a username and password pair.
B. A user in one building logs on to the network by entering a username and password into a host in the same building.
C. A user on a metropolitan area network (MAN) accesses a host by entering a username and password pair while not connected to the LAN.
D. A user in one city logs onto a network by connecting to a domain server in another city.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following is a three-factor authentication system?

A. Username, password, token and iris scanner

B. Password, passphrase, PIN and iris scanner
C. PIN, palm recognition scanner and passphrase
D. Username, PIN and fingerprint reader

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following is an acceptable group in which to place end users?

A. Administrators
B. Backup operators
C. Domain users
D. Root

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
According to industry best practices, administrators should institute a mandatory rotation of duties policy due to which of the following?

A. Continuity of operations in the event of a spam outbreak
B. Continuity of operations in the event of a virus outbreak
C. Continuity of operations in the event of future growth of the network
D. Continuity of operations in the event of absence or accident

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
According to industry best practices, administrators should institute a mandatory rotation of duties policy due to which of the following?

A. To detect outside attackers
B. To detect malware
C. To detect viruses
D. To detect an inside threat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following is considered the strongest encryption by use of mathematical evaluation techniques?

A. ROT13
B. DES
C. AES
D. 3DES

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following should be implemented when protecting personally identifiable information (PII) and sensitive information on IT equipment that can be easily stolen (E. g. USB drive, laptops)?

A. Sensitive file encryption
B. Confidentiality
C. Whole disk encryption
D. Dual-sided certificates

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following is the BEST wireless security practice that could be implemented to prevent unauthorized access?

A. WPA2 with a strong pass-phrase
B. Disabling of the SSID broadcast
C. WPA2 with TKIP
D. WPA with MAC filtering

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following can prevent malicious software applications from being introduced while browsing the Internet?

A. Pop-up blockers

B. Anti-spyware scanners
C. Input validation
D. Strong authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following are reasons to implement virtualization technology? (Select TWO).

A. To reduce recovery time in the event of application failure
B. To decrease false positives on the NIDS
C. To eliminate virtual redundancy
D. To decrease access to security resources
E. To provide a secure virtual environment for testing

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Network security administrators should implement which of the following to ensure system abuse by administrators does not go undetected in the logs?

A. Acceptable use policy
B. Separation of duties
C. Implicit deny
D. Least privilege

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
After completing a risk assessment and penetration test against a network, a security administrator recommends the network owner take actions to prevent future security incidents. Which of the following describes this type of action?

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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 36
Public key infrastructure uses which of the following combinations of cryptographic items?

A. One time keys, WEP and symmetric cryptography
B. Private keys, public keys and asymmetric cryptography
C. Private keys, public keys and ECC-based keys
D. Public keys, symmetric keys and ECC-based keys

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
An administrator wants to implement a procedure to control inbound and outbound traffic on a network segment. Which of the following would achieve this goal?

A. NIDS
B. HIDS
C. ACL
D. Proxy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
In PKI, the CA is responsible for which of the following?

A. Maintaining the CRL
B. Maintaining the cipher block chain
C. Maintaining all private keys
D. Maintaining the browsers PKI store

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
In PKI, which of the following entities is responsible for publishing the CRL?

A. CA

B. ACL
C. Recovery agent
D. User

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following is a security risk associated with USB drives?

A. Easy to conceal and detect
B. Large storage capacity and high visibility
C. Small storage capacity and low visibility
D. Easy to conceal and large storage capacity

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following is a security risk associated with introducing cellular telephones with mobile OS installed on a closed network?

A. New vector to introduce viruses and malware to the network
B. War-dialing DoS attacks against the network
C. War-driving DDoS attacks against the network
D. New vector to introduce VoIP to the network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
The availability of portable external storage such as USB hard drives has increased which of the following threats to networks?

A. Introduction of material on to the network
B. Introduction of rogue wireless access points
C. Removal of sensitive and PII data
D. Increased loss business data

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
An administrator finds a device attached between the USB port on a host and the attached USB keyboarD. The administrator has also noticed large documents being transmitted from the host to a host on an external network. The device is MOST likely which of the following?

A. External USB drive
B. In-line keystroke logger
C. In-line network analyzer
D. USB external hub

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A user is receiving an error which they have not seen before when opening an application. Which of the following is MOST likely the cause of the problem?

A. A patch was pushed out.
B. A signature update was completed on the NIPS.
C. The NIDS baseline has been updateD.
D. The HIDS baseline has been updateD.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following is used to encrypt email and create digital signatures?

A. LDAP
B. HTTPS
C. S/MIME
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following can be used to encrypt FTP or telnet credentials over the wire?

A. SSH

B. HTTPS
C. SHTTP
D. S/MIME

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following is a vulnerability assessment tool?

A. John the Ripper
B. Cain & Abel
C. AirSnort
D. Nessus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following is a vulnerability scanner?

A. John the Ripper
B. Cain & Abel
C. Microsoft Baseline Security Analyzer
D. AirSnort

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following is a password cracking tool?

A. Nessus
B. AirSnort
C. John the Ripper
D. Wireshark

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following is a protocol analyzer?

A. John the Ripper
B. WireShark
C. Cain & Abel
D. Nessus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following is a system setup to distract potential attackers?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Changing roles every couple of months as a security mitigation technique is an example of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following should be checked if an email server is forwarding emails for another domain?

A. DNS zone transfers
B. SMTP open relay
C. Cookies
D. ActiveX controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following will allow the running of a system integrity verifier on only a single host?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following has the ability to find a rootkit?

A. Adware scanner
B. Malware scanner
C. Email scanner
D. Anti-spam scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following will be prevented by setting a BIOS password?

A. Amachine becoming infected with a virus
B. Changing the system boot order
C. Replacing a video card on a machine
D. Amachine becoming infected with a botnet

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following is a security limitation of virtualization technology?

A. It increases false positives on the NIDS.

B. Patch management becomes more time consuming.
C. A compromise of one instance will immediately compromise all instances.
D. If an attack occurs, it could potentially disrupt multiple servers.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following must be used to setup a DMZ?

A. Proxy
B. NIDS
C. Honeypot
D. Router

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following would be used to push out additional security hotfixes?

A. Patch management
B. Configuration baseline
C. Cookies
D. Local security policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following would be used to allow a server to shut itself down normally upon a loss of power?

A. Backup generator
B. Redundant ISP
C. Redundant power supply
D. Uninterruptible Power Supply (UPS)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following is the BEST security measure to use when implementing access control?

A. Password complexity requirements
B. Time of day restrictions
C. Changing default passwords
D. Disabling SSID broadcast

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Applying a service pack could affect the baseline of which of the following?

A. Honeynet
B. Heuristic-based NIDS
C. Signature-based NIDS
D. Signature-based NIPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following is the strongest encryption form that can be used in all countries?

A. WPA2
B. TKIP
C. WEP
D. WPA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
When would it be appropriate to use time of day restrictions on an account?

A. In order to ensure false positives are not received during baseline testing
B. To ensure the DMZ is not overloaded during server maintenance
C. To eliminate attack attempts of the network during peak hours
D. As an added security measure if employees work set schedules

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following could be used to restore a private key in the event of a CA server crashing?

A. Trust model verification
B. Key escrow
C. CRL
D. Recovery agent

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following is a possible security risk associated with USB devices?

A. Domain kiting
B. Cross-site scripting
C. Input validation
D. Bluesnarfing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following is MOST effective in preventing adware?

A. Firewall
B. HIDS
C. Antivirus
D. Pop-up blocker

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which of the following is the MOST important when implementing heuristic-based NIPS?

A. Perform comprehensive heuristic-based analysis on the system.

B. Enable automatic updates to the heuristic databasE.

C. Ensure the network is secure when baseline is establisheD.

D. The brand of NIPS that is being useD.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which of the following attacks enabling logging for DNS aids?

A. Virus infections

B. SQL injection

C. Local hosts file corruption

D. Botnet attacks

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
A technician gets informed that there is a worm loose on the network.Which of the following should the technician review to discover the internal source of the worm?

A. Maintenance logs

B. Antivirus logs

C. Performance logs

D. Access logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following is the BEST approach when reducing firewall logs?

A. Review chronologically.

B. Discard known traffic first.

C. Search for encrypted protocol usagE.

D. Review each protocol one at a timE.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following is MOST likely to cause pop-ups?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: