JK0-018_formatted

Number: 000-000
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

http://www.gratisexam.com/

CompTIA JK0-018

CompTIA Security+ E2C (2011 Edition)

Version: 17.0
CompTIA JK0-018 Exam

Topic 1, Volume A

Exam A

QUESTION 1
Which of the following inspects traffic entering or leaving a network to look for anomalies against expected baselines?

A. IPS
B. Sniffers
C. Stateful firewall
D. Stateless firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following BEST describes a software vulnerability that is actively being used by Sara and Jane, attackers, before the vendor releases a protective patch or update?

A. Buffer overflow
B. IV attack
C. Zero day attack
D. LDAP injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following BEST allows Pete, a security administrator, to determine the type, source, and flags of the packet traversing a network for troubleshooting purposes?

A. Switches
B. Protocol analyzers
C. Routers
D. Web security gateways

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Sara, an attacker, is recording a person typing in their ID number into a keypad to gain access to the building. Sara then calls the helpdesk and informs them that their PIN no longer works and would like to change it. Which of the following attacks occurred LAST?

A. Phishing

B. Shoulder surfing
C. Impersonation
D. Tailgating

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Sara, a security administrator, is noticing a slow down in the wireless network response. Sara launches a wireless sniffer and sees a large number of ARP packets being sent to the AP. Which of the following type of attacks is underway?

A. IV attack
B. Interference
C. Blue jacking
D. Packet sniffing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following would Pete, a security administrator, change to limit how far a wireless signal will travel?

A. SSID
B. Encryption methods
C. Power levels
D. Antenna placement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Topic 4, Volume D

QUESTION 7
Which of the following ports should be open in order for Sara and Pete, users, to identify websites by domain name?

A. TCP 21

B. UDP22
C. TCP 23
D. UDP 53

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Sara, an administrator, suspects a denial of service attack on the network, but does not know where the network traffic is coming from or what type of traffic it is. Which of the following would help Sara further assess the situation?

A. Protocol analyzer
B. Penetration testing
C. HTTP interceptor
D. Port scanner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Sara, a security administrator, has configured a trusted OS implementation on her servers. Which of the following controls are enacted by the trusted OS implementation?

A. Mandatory Access Controls
B. Time-based Access Controls
C. Discretionary Access Controls
D. Role Based Access Controls

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following ports would be blocked if Pete, a security administrator, wants to deny access to websites?

A. 21
B. 25
C. 80
D. 3389

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 11
Pete, the security administrator, is implementing a web content fitter. Which of the following is the MOST important design consideration in regards to availability?

A. The number of filter categories
B. Other companies who are using the system
C. Fail state of the system
D. The algorithm of the filtering engine

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following is where an unauthorized device is found allowing access to a network?

A. Bluesnarfing
B. Rogue access point
C. Honeypot
D. IV attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
When used alone, which of the following controls mitigates the risk of Sara, an attacker, launching an online brute force password attack?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Pete, a security engineer, is trying to inventory all servers in a rack. The engineer launches RDP sessions to five different PCs and notices that the hardware properties are similar. Additionally, the MAC addresses of all five servers appear on the same switch port. Which of the following is MOST likely the cause?

A. The system is running 802.1 x
B. The system is using NAC
C. The system is in active-standby mode
D. The system is virtualized

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following security concepts establishes procedures where creation and approval are performed through distinct functions?

A. Discretionary access control
B. Job rotation
C. Separation of duties
D. Principle of least privilege

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
While traveling Matt, an employee, decides he would like to download some new movies onto his corporate laptop. While installing software designed to download movies from multiple computers across the Internet. Matt agrees to share portions of his hard drive. This scenario describes one of the threats involved in which of the following technologies?

A. Social networking
B. ALE
C. Cloud computing
D. P2P

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following is an attack where Pete spreads USB thumb drives throughout a bank's parking lot in order to have malware installed on the banking systems?

A. Tailgating
B. Replay attack
C. Virus
D. Social engineering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Pete, a security administrator, has configured and implemented an additional public intermediate CA. Which of the following must Pete submit to the major web browser vendors in order for the certificates, signed by this intermediate, to be trusted?

A. Die root CA's private key
B. The root CA's public key
C. The intermediate CA's public key
D. The intermediate CA's private key

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following is BEST described by a scenario where organizational management chooses to implement an internal Incident Response Structure for the business?

A. Deterrence
B. Separation of duties
C. Transference
D. Mitigation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A data loss prevention strategy would MOST likely incorporate which of the following to reduce the risk associated with data loss?

A. Enforced privacy policy, encryption of VPN connections, and monitoring of communications entering the organization.
B. Enforced acceptable usage policy, encryption of confidential emails, and monitoring of communications leaving the organization.
C. Enforced privacy policy, encryption of VPN connections, and monitoring of communications leaving the organization.
D. Enforced acceptable usage policy, encryption of confidential emails, and monitoring of communications entering the organization.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 21
In a wireless network, which of the following components could cause too much coverage, too little coverage, and interference?

A. MAC filter
B. AP power levels
C. Phones or microwaves
D. SSID broadcasts

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following has a default port of 22?

A. SSH
B. FTP
C. TELNET
D. SCAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
The public key is used to perform which of the following? (Select THREE).

A. Validate the CRL
B. Validate the identity of an email sender
C. Encrypt messages
D. Perform key recovery
E. Decrypt messages
F. Perform key escrow

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Pete, a network administrator, implements the spanning tree protocol on network switches. Which of the

following issues does this address?

A. Flood guard protection
B. ARP poisoning protection
C. Loop protection
D. Trunking protection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Matt, a security administrator, has noticed that the website and external systems have been subject to many attack attempts. To verify integrity of the website and critical files, Matt should:

A. Require all visitors to the public web home page to create a username and password to view the pages in the website
B. Configure the web application firewall to send a reset packet to the incoming IP from where an attack or scan signature has been detected.
C. Create file hashes for website and critical system files, and compare the current file hashes to the baseline at regular time intervals.
D. Reboot the web server and database server nightly after the backup has been completed.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Matt, the administrator, has been told to confirm what account an email was sent from. Which of the following is this an example of?

A. Surveillance
B. E-discovery
C. Chain of custody
D. Integrity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following BEST describes a denial of service attack?

A. Sara, the attacker, attempts to have the receiving server run a payload using programming commonly found on web servers.
B. Sara, the attacker, overwhelms a system or application, causing it to crash and bring the server down to cause an outage.

C. Sara, the attacker, overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload.
D. Sara, the attacker, attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
The Chief Information Officer (CIO) wants to protect laptop users from zero day attacks. Which of the following would BEST achieve the CIO's goal?

A. Host based firewall
B. Host based IDS
C. Anti-virus
D. Anti-spyware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Matt, a server administrator, sets up database forms based on security rating levels. If a user has the lowest security rating then the database automatically determines what access that user has. Which of the following access control methods does this describe?

A. Mandatory access control
B. Role based access control
C. Rule based access control
D. Discretionary access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following is a best practice when securing a switch from physical access?

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 31
Pete, a security administrator, has observed repeated attempts to break into the network. Which of the following is designed to stop an intrusion on the network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Jane, an IT security technician working at a bank, has implemented encryption between two locations. Which of the following security concepts BEST exemplifies the protection provided by this example?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
While Sara is logging into the server from her workstation, she notices Pete watching her enter the username and password. Which of the following social engineering attacks is Pete executing?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
The log management system at Company A is inadequate to meet the standards required by their corporate governance team. A new automated log management system has been put in place.

This is an example of which of the following?

A. Data integrity measurement
B. Network traffic analysis
C. Risk acceptance process
D. Continuous monitoring

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Several users' computers are no longer responding normally and sending out spam email to the users' entire contact list. This is an example of which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following should Sara, a security technician, perform as the FIRST step when creating a disaster recovery plan for a mission critical accounting system?

A. Implementing redundant systems
B. Removal of single points of failure
C. Succession planning
D. Business impact assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following is the MOST secure protocol for Pete, an administrator, to use for managing network devices?

A. FTP
B. TELNET
C. FTPS
D. SSH

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following is the BEST incident response procedure to take when a previous employee enters a facility?

A. Notify Computer Emergency Response Team (CERT) of the security breach to document it.
B. Take screenshots of the employee's workstation.
C. Take hashes of the employee's workstation.
D. Notify security to identify employee's whereabouts.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following activities should be completed in order to detect anomalies on a network?

A. Incident management
B. Change management
C. User permissions reviews
D. Log reviews

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following reduces the likelihood of a single point of failure when a server fails?

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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 41
Jane, a security administrator, wants to prevent users in sales from accessing their servers after 6:00 p.m., and prevent them from accessing accounting's network at all times. Which of the following should Jane implement to accomplish these goals? (Select TWO).

A. Separation of duties
B. Time of day restrictions
C. Access control lists
D. Mandatory access control
E. Single sign-on

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following describes the ability for a third party to verify the sender or recipient of a given electronic message during authentication?

A. Entropy
B. Principle of least privilege
C. Non-repudiation
D. Code signing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following protocols provides Pete, an administrator, with the HIGHEST level of security for device traps?

A. ICMP
B. SNMPv3
C. SSH
D. IPSec

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44

Jane has a vendors server in-house for shipping and receiving. She wants to ensure that if the server goes down that the server in-house will be operational again within 24 hours. Which of the following should Jane define with the vendor?

A. Mean time between failures
B. A warm recovery site
C. Mean time to restore
D. A hot recovery site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following procedures would be used to mitigate the risk of an internal developer embedding malicious code into a production system?

A. Audit management
B. Mobile device management
C. Incident management
D. Change management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
To mitigate the adverse effects of network modifications, which of the following should Matt, the security administrator, implement?

A. Change management
B. Routine auditing
C. Incident management
D. Log auditing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Jane, a security technician, wants to implement secure wireless with authentication. Which of the following allows for wireless to be authenticated via MSCHAPv2?

A. PEAP
B. WPA2 personal
C. TKIP

D. CCMP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Pete, a user, is having trouble dialing into the network from their house. The administrator checks the RADIUS server, the switch connected to the server, and finds that the switch lost configuration after a recent power outage. The administrator replaces the switch and is able to ping the switch, but not the RADIUS server. Which of the following is the MOST likely cause?

A. The switch needs to have QoS setup correctly.
B. Port security is not enabled on the switch.
C. VLAN mismatch is occurring.
D. The DMZ is not setup correctly

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following would MOST likely be implemented in order to prevent employees from accessing certain websites?

A. VPN gateway
B. Router
C. Proxy server
D. Packet filtering firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
When reviewing a digital certificate for accuracy, which of the following would Matt, a security administrator, focus on to determine who affirms the identity of the certificate owner?

A. Trust models
B. CRL
C. CA
D. Recovery agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Sara, a security analyst, suspects that a rogue web server is running on the network. Which of the following would MOST likely be used to identify the server's IP address?

A. Port scanner
B. Telnet
C. Traceroute
D. Honeypot

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following is an improved version of the LANMAN hash?

A. LM2
B. NTLM
C. SHA
D. MD5

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following will help Matt, an administrator; mitigate the risk of static electricity?

A. Lightening rods
B. EMI shielding
C. Humidity controls
D. Temperature controls

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
An application company sent out a software patch for one of their applications on Monday. The company has been receiving reports about intrusion attacks from their customers on Tuesday.
Which of the following attacks does this describe?

A. Zero day

B. Directory traversal
C. Logic bomb
D. Session hijacking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A company needs to remove sensitive data from hard drives in leased computers before the computers are returned to the supplier. Which of the following is the BEST solution?

A. Re-image with a default OS
B. Physical destruction of the hard drive
C. Format drive using a different file system
D. Sanitization using appropriate software

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following techniques floods an application with data in an attempt to find vulnerabilities?

A. Header manipulation
B. Steganography
C. Input validation
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Jane, a security administrator, has applied security labels to files and folders to manage and restrict access. Which of the following is Jane using?

A. Mandatory access control
B. Role based access control
C. Implicit access control
D. Discretionary access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Sara, a user, on a public Wi-Fi network logs into a webmail account and is redirected to a search engine. Which of the following attacks may be occurring?

A. Evil twin
B. Bluesnarfing
C. War chalking
D. Bluejacking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
When moving from an internally controlled environment to a fully outsourced infrastructure environment, such as cloud computing, it is MOST important to:

A. Implement mandatory access controls.
B. Ensure RAID 0 is implemented on servers.
C. Impose time of day restrictions across all services
D. Encrypt all confidential data.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following would help Pete, an administrator, prevent access to a rogue access point connected to a switch?

A. Enable spanning tree protocol
B. Enable DHCP snooping
C. Disable VLAN trunking
D. Establish a MAC limit and age

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A company wants to have a backup site that is a good balance between cost and recovery time objectives. Which of the following is the BEST solution?

A. Hot site

B. Remote site
C. Cold site
D. Warm site

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
While conducting a network audit, Sara, a security administrator, discovers that most clients are routing their network traffic through a desktop client instead of the company router. Which of the following is this attack type?

A. ARP poisoning
B. Session hijacking
C. DNS poisoning
D. Pharming attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following is a reason why Pete, a security administrator, would implement port security?

A. To inspect the TPC and UDP ports of incoming traffic
B. To port C++code into Java bit-code in a secure manner
C. To implement secure datacenter electronic access
D. To limit the number of endpoints connected through the same switch port

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which of the following is the MAIN benefit of server-side versus client-side input validation?

A. Server-side input validation results in a more secure system than client-side input validation.
B. Client-side input validation can lead to local buffer overflows while server-side input validation can lead to remote buffer overflow.
C. Client-side input validation results in a more secure system than server-side input validation.
D. Server-side input validation is prone to buffer overflows while client-side input validation is not.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following would be the BEST reason for Jane, a security administrator, to initially select individual file encryption over whole disk encryption?

A. It provides superior key redundancy for individual files.
B. The management of keys is easier to maintain for file encryption
C. It is faster to encrypt an individual file.
D. It provides protected access to all users

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following implements two factor authentication based on something you know and something you have?

A. Users shall authenticate to the system via a Kerberos enabled authentication server working with an integrated PKI only.
B. The system shall require users to authenticate to the system with a combination of a password or PIN and a smartcard
C. The system shall authenticate only authorized users by fingerprint and retina scan.
D. Users shall possess a combination of 8 digit PINs and fingerprint scanners.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following attacks is characterized by Sara attempting to send an email from a Chief Information Officer's (CIO's) non-corporate email account to an IT staff member in order to have a password changed?

A. Spamming
B. Pharming
C. Privilege escalation
D. Impersonation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which of the following should be done before resetting a user's password due to expiration?

A. Verify the user's domain membership
B. Verify the user's identity
C. Advise the user of new policies
D. Verity the proper group membership

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Sara, an attacker, calls the company's from desk and tries to gain insider information by providing specific company information to gain the attendant's trust. The front desk immediately alerts the IT department about this incident. This is an example of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following is based on X.500 standards?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following functions of a firewall allows Pete, an administrator, to map an external service to an internal host?

A. AP isolation
B. Port forwarding
C. DMZ
D. NAT

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Hashing algorithms are used to address which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
After setting up a root CA. which of the following can Pete, a security administrator, implement to allow intermediate CAs to handout keys and certificates?

A. CRL
B. Spanning tree
C. Trust model
D. Key escrow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following should be implemented to restrict wireless access to the hardware address of a NIC?

A. URL filtering
B. WPA2 and EAP
C. PEAP and WPA
D. MAC filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which of the following is the purpose of the spanning tree protocol?

A. Loop protection
B. Access control lists
C. Secure device configuration
D. Implicit deny

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Sara, the security engineer, has discovered that a breach is in progress on a non-production system of moderate importance. Which of the following should Sara collect FIRST?

A. Memory dump, ARP cache
B. Live system image, route table
C. Temp files, hosts file
D. Offline system image, router logs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
While traveling, users need access to an internal company web server that contains proprietary information. Pete, the security administrator, should implement a:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following is used by Matt, a security administrator, to lower the risks associated with electrostatic discharge, corrosion, and thermal breakdown?

A. Temperature and humidity controls
B. Routine audits
C. Fire suppression and EMI shielding
D. Hot and cold aisles

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Workers of a small local organization have implemented an off-site location in which the organization can resume operations within 10 business days in the event of a disaster. This type of site is BEST known as which of the following?

A. Hot site
B. High-availability site
C. Cold site
D. Warm site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following may cause Jane, the security administrator, to seek an ACL work around?

A. Zero day exploit
B. Dumpster diving
C. Virus outbreak
D. Tailgating

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following ports would be blocked if Pete, a security administrator, wants to disable FTP?

A. 21

B. 23
C. 25
D. 110

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Sara, a security administrator, suspects that a web server may be under attack. The web logs have several entries containing variations of the following entries:

'or 1=1--

or1'=1--

'or1=1'--

Which of the following attacks is MOST likely occurring?

A. Zero day exploit
B. Buffer overflow
C. SQL injection
D. Man-in-the-middle

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following attacks would be used if Sara, a user, is receiving unwanted text messages?

A. Packet sniffing
B. Bluesnarfing
C. Smurf attack
D. Blue jacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following practices reduces the attack surface of a wireless network? (Select TWO)

A. Antenna placement
B. Using TKIP instead on AES
C. Power-level control

D. Using WPA2 instead of WPA
E. Using RADIUS

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Matt, a security administrator, is responsible for provisioning role-based user accounts in an enterprise environment. A user has a temporary business need to perform multiple roles within the organization. Which of the following is the BEST solution to allow the user to perform multiple roles?

A. Create expiring unique user IDs per role
B. Allow access to an existing user ID
C. Assign multiple roles to the existing user ID
D. Create an additional expiring generic user ID

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
An application programmer reports to Sara, the security administrator, that the antivirus software installed on a server is interfering with one of the production HR applications, and requests that antivirus be temporarily turned off. How should Sara respond to this request?

A. Ask the programmer to replicate the problem in a test environment.
B. Turn off antivirus, but install a host intrusion prevention system on the server.
C. Update the server's antivirus and anti-malware definitions from the vendor's site
D. Turn off antivirus, but turn on the host-based firewall with a deny-all rule set.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
A packet filtering firewall can protect from which of the following?

A. SOL injection
B. Brute force attack
C. Port scan
D. DNS poisoning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following can Matt, an administrator, use to ensure the confidentiality of a file when it is being sent over FTP?

A. WPA2
B. PGP
C. MD5
D. NTLMv2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Pete, a user, submitted a form on the Internet but received an unexpected response shown below

Server Error in "/" Application

Runtime error in script on asp.net version 2.0

Which of the following controls should be put in place to prevent Pete from learning this information about the web server in the future?

A. Patch management
B. Error handling
C. Fuzzing
D. Input validation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Employees are reporting that they are receiving unusual calls from the help desk for the purpose of verifying their user credentials. Which of the following attack types is occurring?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Sara, a forensic invest gator, believes that the system image she was presented with is not the same as the original source. Which of the following should be done to verify whether or not the image has been tampered with?

A. Compare file sizes from the original with the system image.
B. Reimage the original source with a read-only tool set to ignore errors.
C. Compare hashes of the original source and system image.
D. Compare time stamps from the original with the system image.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following is a feature of Kerberos?

A. One-way encryption
B. Vendor patch management
C. Only available for Linux systems
D. Single sign-on

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
An SQL injection vulnerability can be caused by which of the following?

A. Password complexity
B. Improper input validation
C. Discretionary access controls
D. Cross-site request forgery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which of the following is BEST used to break a group of IP addresses into smaller network segments or blocks?

A. NAT
B. Visualization

C. NAC
D. Subnetting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following would Sara, a security administrator, utilize to identity a weakness within various applications without exploiting that weakness?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Matt, a security administrator, wants to allow content owners to determine who has access to tiles. Which of the following access control types does this describe?

A. Rule based access control
B. Discretionary access control
C. Role based access control
D. Mandatory access control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following commands can Matt, an administrator, use to create a forensically sound hard drive image?

A. grep
B. dump
C. dcfldd
D. hex

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following technologies would allow the removal of a single point of failure?

A. Dual-homing a server
B. Clustering a SQL server
C. Adding a second VLAN to a switch
D. Assigning a second IP address to a NIC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Jane, the administrator, is tasked with deploying a strong encryption cipher. Which of the following ciphers would she be the LEAST likely to choose?

A. DES
B. Two fish
C. 3DES
D. AES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Exam B

QUESTION 1
Pete, a network administrator, is capturing packets on the network and notices that a large amount of the traffic on the LAN is SIP and RTP protocols. Which of the following should he do to segment that traffic from the other traffic?

A. Connect the WAP to a different switch
B. Create a voice VLAN
C. Create a DMZ
D. Set the switch ports to 802.1q mode

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following security tools can Jane, a security administrator, use to deter theft?

A. Visualization
B. Cable locks
C. GPS tracking
D. Device encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following can be implemented on a laptop hard drive to help prevent unauthorized access to data?

A. Full disk encryption
B. Key escrow
C. Screen lock
D. Data loss prevention

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following network devices allows Jane, a security technician, to perform malware inspection?

A. Load balancer
B. VPN concentrator
C. Firewall

D. NIPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following is a valid server-role in a Kerberos authentication system?

A. Token issuing system
B. Security assertion server
C. Authentication agent
D. Ticket granting server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
The accounting department needs access to network share A to maintain a number of financial reporting documents. The department also needs access to network share B in HR to view payroll documentation for cross-referencing items. Jane, an administrative assistant, needs access to view one document in network share A to gather data for management reports. Which of the following gives accounting and Jane the correct rights to these areas?

A. Accounting should be given read/write access to network share A and read access to network share B. Jane should be given read access for the specific document on network share A.
B. Accounting should be given read/write access to network share A and read access to network share B. Jane should be given read access to network share A.
C. Accounting should be given full access to network share A and read access to network share B. Jane should be given read/write access for the specific document on network share A.
D. Accounting should be given full access to network share A and read access to network share B. Jane should be given read/write access to network share A.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following creates ciphertext by changing the placement of characters?

A. Transposition cryptography
B. Hashing
C. Elliptical cryptography
D. Digital signatures

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following malware types uses stealth techniques to conceal itself, cannot install itself without user interaction, and cannot automatically propagate?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
When Pete, an employee, leaves a company, which of the following should be updated to ensure Pete's security access is reduced or eliminated?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following should Matt, an administrator, change FIRST when installing a new access point?

A. SSID broadcast
B. Encryption
C. DHCP addresses
D. Default password

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A datacenter has two rows of racks which are facing the same direction. Sara, a consultant, recommends the racks be faced away from each other. This is an example of which of the following environmental concepts?

A. Fire suppression
B. Raised floor implementation
C. Hot and cool aisles
D. Humidity controls implementation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following password policies is the MOST effective against a brute force network attack?

A. Password complexity
B. Password recovery
C. 30 day password expiration
D. Account lockout

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following would BEST be used by Sara, the security administrator, to calculate the likelihood of an event occurring?

A. SLE
B. ALE
C. ROI
D. ARO

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following should Matt, an administrator, implement in a server room to help prevent static electricity?

A. GFI electrical outlets
B. Humidity controls
C. ESD straps
D. EMI shielding

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 15
Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building Sara should immediately implement which of the following?

A. Acceptable Use Policy
B. Physical security controls
C. Technical controls
D. Security awareness training

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Pete, an IT security technician, has been tasked with implementing physical security controls for his company's workstations. Which of the following BEST meets this need?

A. Host-based firewalls
B. Safe
C. Cable locks
D. Remote wipe

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following creates ciphertext by replacing one set of characters for another?

A. Substitution cryptography
B. Elliptical cryptography
C. Digital signatures
D. Transposition cryptography

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Sara, the IT Manager, would like to ensure that the router and switches are only available from the network administrator's workstation. Which of the following would be the MOST cost effective solution to ensure that only the network administrator can access these devices?

A. Restrict console ports
B. Time of day restrictions
C. Implement ACLs
D. Implement an out-of-band administrative network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
A company is performing internal security audits after a recent exploitation on one of their proprietary applications. Sara, the security auditor, is given the workstation with limited documentation regarding the application installed for the audit. Which of the following types of testing methods is this?

A. Sandbox
B. White box
C. Black box
D. Gray box

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A web server sitting in a secure DMZ has antivirus and anti-malware software which updates daily. The latest security patches are applied and the server does not run any database software. A day later, the web server is compromised and defaced. Which of the following is the MOST likely type of attack?

A. Header manipulation
B. Zero day exploit
C. Session hijacking
D. SQL injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following protocols is MOST likely associated with network audit logging?

A. ICMP
B. FTPS
C. DNS
D. SNMP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Pete, a security administrator, is asked to install and configure centralized software to securely manage and collect statistics from all of the company's network devices. Which of the following should the software support?

A. 802.1x
B. ICMP
C. SNMPv3
D. SNMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
A network consists of various remote sites that connect back to two main locations. Pete, the security administrator, needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Pete, a security administrator, is informed that people from the HR department should not have access to the accounting department's server, and the accounting department should not have access to the HR department's server. The network is separated by switches. Which of the following is designed to keep the HR department users from accessing the accounting department's server and vice-versa?

A. ACLs
B. VLANs
C. DMZs
D. NATS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following is BEST utilized to actively test security controls on a particular system?

A. Port scanning
B. Penetration test
C. Vulnerability scanning
D. Grey/Gray box

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site?

A. Internet content filter
B. Firewall
C. Proxy server
D. Protocol analyzer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following has serious security implications for large organizations and can potentially allow an attacker to capture conversations?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Upper management decides which risk to mitigate based on cost. This is an example of:

A. Qualitative risk assessment
B. Business impact analysis

C. Risk management framework
D. Quantitative risk assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Isolation mode on an AP provides which of the following functionality types?

A. Segmentation of each wireless user from other wireless users
B. Disallows all users from communicating directly with the AP
C. Hides the service set identifier
D. Makes the router invisible to other routers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Employees are reporting that unauthorized personnel are in secure areas of the building. This is MOST likely due to lack of security awareness in which of the following areas?

A. Impersonation
B. Logical controls
C. Physical security controls
D. Access control policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A forensic image of a hard drive has been created. Which of the following can be used to demonstrate the image has not been tampered with?

A. Chain of custody
B. Document the image file's size and time stamps
C. Encrypt the image file
D. Hash of the image file

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following secure protocols is MOST commonly used to remotely administer Unix/Linux systems?

A. SSH
B. SCP
C. SFTP
D. SNMP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following security concepts can Matt, a security administrator, implement to support integrity?

A. Digital signatures
B. Trust models
C. Key escrow
D. Recovery agents

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following combinations represents multifactor authentication?

A. Smart card and hard token
B. Voice print analysis and facial recognition
C. Username and PIN
D. Cipher lock combination and proximity badge

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Matt, a developer, recently attended a workshop on a new application. The developer installs the new application on a production system to test the functionality. Which of the following is MOST likely affected?

A. Application design
B. Application security
C. Initial baseline configuration
D. Management of interfaces

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following is Jane, a security administrator, MOST likely implementing when deleting all the unneeded files and modules of a newly installed application?

A. Exception handling
B. Patch management
C. System file clean up
D. Application hardening

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following should be used when a business needs a block cipher with minimal key size for internal encryption?

A. AES
B. Blowfish
C. RC5
D. 3DES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following best practices makes a wireless network more difficult to find?

A. Implement MAC filtering
B. UseWPA2-PSK
C. Disable SSD broadcast
D. Power down unused WAPs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
The use of social networking sites introduces the risk of:

A. Disclosure of proprietary information
B. Data classification issues
C. Data availability issues
D. Broken chain of custody

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which the following flags are used to establish a TCP connection? (Select TWO).

A. PSH
B. ACK
C. SYN
D. URG
E. FIN

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following is MOST likely to result in data loss?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Sara, a security administrator, sends an email to the user to verify their password has been reset. Which of the following threats is BEST mitigated by this action?

A. Spear phishing
B. Impersonation
C. Hoaxes
D. Evil twin

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following describes an LDAP injection attack?

A. Creating a copy of user credentials during the LDAP authentication session
B. Manipulating an application's LDAP query to gain or alter access rights
C. Sending buffer overflow to the LDAP query service
D. Using XSS to direct the user to a rogue LDAP server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following concepts defines the requirement for data availability?

A. Authentication to RADIUS
B. Non-repudiation of email messages
C. Disaster recovery planning
D. Encryption of email messages

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following is an example of multifactor authentication?

A. Credit card and PIN
B. Username and password
C. Password and PIN
D. Fingerprint and retina scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following is an attack designed to steal cell phone data and contacts?

A. Bluesnarfing
B. Smurfing
C. Fuzzing
D. Bluejacking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following best practices is commonly found at the end of router ACLs?

A. Time of day restrictions
B. Implicit deny
C. Implicit allow
D. Role-based access controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following uses TCP / UDP port 53 by default?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
An organization is recovering data following a datacenter outage and determines that backup copies of files containing personal information were stored in an unsecure location, because the sensitivity was unknown. Which of the following activities should occur to prevent this in the future?

A. Business continuity planning
B. Quantitative assessment
C. Data classification
D. Qualitative assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Sara, the network administrator, was alerted to an unauthorized email that was sent to specific VIPs in the company with a malicious attachment. Which of the following types of attacks is MOST likely being described?

A. Vishing
B. Whaling
C. DDoS
D. Pharming

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
In the event of a mobile device being lost or stolen, which of the following BEST protects against sensitive information leakage?

A. Cable locks

B. Remote wipe
C. Screen lock
D. Voice encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following should Sara, a security administrator, perform periodically to reduce an organization's risk exposure by verifying employee access?

A. Account revalidation
B. Incident management
C. Qualitative analysis
D. Quantitative analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following is the MAIN benefit of server-side versus client-side input validation?

A. Server-side input validation results in a more secure system than client-side input validation.
B. Client-side input validation can lead to local buffer overflows while server-side input validation can lead to remote buffer overflow.
C. Client-side input validation results in a more secure system than server-side input validation.
D. Server-side input validation is prone to buffer overflows while client-side input validation is not.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following is MOST appropriate when storing backup tapes in a physically non-secure room?

A. Use an in-tape GPS tracking device.
B. Store the tapes in a locked safe.
C. Encrypt the tapes with AES.
D. Securely wipe the tapes.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Grandfather-Father-Son and Tower of Hanoi are common:

A. Trojans that collect banking information.
B. Backup tape rotation strategies.
C. Penetration testing best practices.
D. Failover practices in clustering.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following is the below pseudo-code an example of?

IF VARIABLE (CONTAINS NUMBERS = TRUE) THEN EXIT

A. Buffer overflow prevention
B. Input validation
C. CSRF prevention
D. Cross-site scripting prevention

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following can BEST be implemented on a mobile phone to help prevent any sensitive data from being recovered if the phone is lost?

A. Voice encryption
B. Screen locks
C. Device encryption
D. GPS tracking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following security concepts would Sara, the security administrator, use to mitigate the risk of data loss?

A. Record time offset

B. Clean desk policy
C. Cloud computing
D. Routine log review

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
If Organization A trusts Organization B and Organization B trusts Organization C, then Organization A trusts Organization C. Which of the following PKI concepts is this describing?

A. Transitive trust
B. Public key trust
C. Certificate authority trust
D. Domain level trust

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following is BEST associated with PKI?

A. Private key
B. Block ciphers
C. Stream ciphers
D. NTLMv2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following malware types is BEST described as protecting itself by hooking system processes and hiding its presence?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Sara, a security administrator, manually hashes all network device configuration files daily and compares them to the previous days' hashes. Which of the following security concepts is Sara using?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Following a security failure incident, the chain of custody must be followed in order to:

A. Determine who accessed the compromised equipment pre-incident.
B. Securely lock down any compromised equipment.
C. Preserve and maintain evidence integrity.
D. Provide an accurate timeline detailing how the incident occurred.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Jane, an IT administrator, is implementing security controls on a Microsoft Windows based kiosk used at a bank branch. This kiosk is used by the public for Internet banking. Which of the following controls will BEST protect the kiosk from general public users making system changes?

A. Group policy implementation
B. Warning banners
C. Command shell restrictions
D. Host based firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
After Matt, a user, enters his username and password at the login screen of a web enabled portal, the following appears on his screen:

'Please only use letters and numbers on these fields'

Which of the following is this an example of?

A. Proper error handling
B. Proper input validation
C. Improper input validation
D. Improper error handling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
The corporate NIPS requires a daily download from its vendor with updated definitions in order to block the latest attacks. Which of the following describes how the NIPS is functioning?

A. Heuristics
B. Anomaly based
C. Signature based
D. Behavior based

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Pete, a security administrator, needs to update the community strings on the router since they have been compromised. Which of the following needs to be changed?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following symmetric key algorithms are examples of block ciphers? (Select THREE)

A. RC4
B. 3DES
C. AES
D. MD5
E. PGP

F. Blowfish

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Matt, an account manager, arrives at work early in the morning and cannot log into his workstation. He calls the help desk an hour later to open a trouble ticket, but they tell him there is nothing wrong with his account. Matt tries his login once more and is granted access. Which of the following control types BEST explains this anomaly?

A. Discretionary access control
B. Time of day restrictions
C. Separation of duties
D. Single sign-on

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A targeted email attack sent to Sara, the company's Chief Executive Officer (CEO), is known as which of the following?

A. Whaling
B. Bluesnarfing
C. Vishing
D. Dumpster diving

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following network devices allows web traffic to be distributed amongst servers?

A. Web security gateway
B. Load balancers
C. NIDS
D. Routers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following provides the LEAST availability?

A. RAID 0
B. RAID 1
C. RAID 3
D. RAID 5

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Sara, a security guard, reports that the side of the company building has been marked with spray paint. Which of the following could this be an example of?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Matt, a security administrator, has the VPN tunnel application set up so that after multiple incorrect attempts, the VPN service is disabled. Which of the following deterrent techniques does this describe?

A. Intrusions detection system
B. Baseline reporting
C. Failopen
D. Failsafe

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Sara, a user, receives a call and the caller asks if Sara would be willing to answer a few marketing questions, and in return be placed in the drawing to win a trip to Hawaii. After Sara agrees, she is transferred to an automated service which states that some personal information needs to be collected to verify her full name, birthday, address, and email to be eligible for the Hawaii trip. After providing the details Sara is then solicited for banking preferences, general purchasing preferences, and debit card details. Which of the following BEST describes this type of attack?

A. A hoax
B. Pharming
C. Smurfing
D. Vishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following devices is BEST suited for servers that need to store private keys?

A. Hardware security module
B. Hardened network firewall
C. Solid state disk drive
D. Hardened host firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Sara, the Chief Information Officer (CIO), has requested an audit take place to determine what services and operating systems are running on the corporate network. Which of the following should be used to complete this task?

A. Fingerprinting and password crackers
B. Fuzzing and a port scan
C. Vulnerability scan and fuzzing
D. Port scan and fingerprinting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following types of data encryption would Matt, a security administrator, use to encrypt a specific table?

A. Full disk
B. Individual files
C. Database
D. Removable media

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following security controls enforces user permissions based on a job role?

A. Single sign-on access
B. Group based privileges
C. Account policy enforcement
D. User assigned privileges

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
A business has paper forms on hand in the event of a credit processing system failure. This is an example of which of the following?

A. Business process re-engineering
B. Disaster recovery
C. Continuity of operations
D. Enterprise resource planning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
By default, which of the following ports would Pete, an administrator, block to prevent incoming RDP connections to a Windows Server?

A. 22
B. 161
C. 3389
D. 5631

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following encrypts the body of a packet, rather than just the password, while sending information?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following should Matt, a security administrator, include when encrypting smartphones? (Select TWO).

A. Steganography images
B. Internal memory
C. Master boot records
D. Removable memory cards
E. Public keys

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following risk related concepts BEST supports the identification of fraud?

A. Risk avoidance
B. Job rotation
C. ALE calculation
D. Clean desk policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following would Pete, a security administrator, do to limit a wireless signal from penetrating the exterior walls?

A. Implement TKIP encryption
B. Consider antenna placement
C. Disable the SSID broadcast
D. Disable WPA

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 88
Which of the following are restricted to 64-bit block sizes? (Select TWO).

A. PGP
B. DES
C. AES256
D. RSA
E. 3DES
F. AES

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following would be implemented to create a network inside a network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following is a system designed to lure attackers away from production systems?

A. Proxy server
B. Spam filter
C. Honeypot
D. Flood guard

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Sara, a security analyst, discovers which operating systems the client devices on the network are running by only monitoring a mirror port on the router. Which of the following techniques did Sara use?

A. Active fingerprinting
B. Passive fingerprinting
C. Protocol analyzing
D. Network enumerating

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following authentication services uses a ticket granting system to provide access?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Matt, the Chief Information Officer (CIO), wants to protect laptop users from zero day attacks. Which of the following would BEST achieve Matt's goal?

A. Host based firewall
B. Host based IDS
C. Anti-virus
D. Anti-spyware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Which of the following is often rated based on its ability to increase the time it takes to perform an attack?

A. Safe
B. Screen lock
C. Patch management
D. Visualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
The human resources department of a company has requested full access to all network resources, including those of the financial department. Jane, the administrator, denies this, citing:

A. Conflict of interest
B. Separation of duties
C. Role authentication
D. Implicit deny

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following is a way to gain access to a protected system while another user is entering credentials?

A. Spim
B. Shoulder surfing
C. DDoS
D. Backdoor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which of the following would Pete, a security administrator, MOST likely implement in order to allow employees to have secure remote access to certain internal network services such as file servers?

A. Packet filtering firewall
B. VPN gateway
C. Switch
D. Router

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Jane, a security administrator, needs to deploy a wireless network where the wireless encryption key is negotiated automatically. Which of the following MUST be implemented?

A. WPA2-PSK

B. 802.1n
C. MAC filtering
D. WPA enterprise

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following can be implemented on the company gateway router to prevent IP packets with a source IP of the internal company network from being routed by the external interface of the router into the company's network?

A. 802.1x
B. Flood guards
C. Access control lists
D. Loop protection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following BEST explains the security benefit of a standardized server image?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Topic 2, Volume B

Exam C

QUESTION 1
Jane, a security administrator, has completed the imaging process for 20 computers that were deployed. The image contains the operating system and all required software. Which of the following is this an example of?

A. Implementing configuration hardening
B. Implementing configuration baseline
C. Implementing due diligence
D. Deploying and using a trusted OS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following open standards should Pete, a security administrator, select for remote authentication of users?

A. TACACS
B. RADIUS
C. WPA2
D. RIPEMD

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Matt, a system administrator, wants to establish a nightly available SQL database. Which of the following would be implemented to eliminate a single point of failure in storage and servers?

A. RAID 5 and a storage area network
B. Two striped drives and clustering
C. Two mirrored drives and clustering
D. RAID 0 and load balancing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following malware types is MOST commonly associated with command and control?

A. Rootkits
B. Logic bombs

C. Botnets
D. Backdoors

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following security chips does BitLocker utilize?

A. BIOS
B. CPU
C. CMOS
D. TPM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
While performing basic forensic analysis of a hard drive in Sara's, the security administrator, possession, which of the following should be verified during the analysis?

A. Witness statements
B. Image hashes
C. Chain of custody
D. Order of volatility

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Topic 5, Volume E

QUESTION 7
Which of the following policies is implemented in order to minimize data loss or theft?

A. PII handling
B. Password policy
C. Chain of custody
D. Zero day exploits

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following allows Pete, a security technician, to prevent email traffic from entering the company servers?

A. IDS
B. URL filtering
C. VPN concentrators
D. Spam filter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following should be implemented to secure Pete's, a network administrator, day-to- day maintenance activities? (Select TWO).

A. TFTP
B. Telnet
C. TACACS+
D. FTP
E. SSH

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
When integrating source material from an open source project into a highly secure environment, which of the following precautions should prevent hidden threats?

A. Design review
B. Code review
C. Risk assessment
D. Vulnerability scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following can Sara, a security administrator, implement to ensure that encrypted files and devices can be recovered if the passphrase is lost?

A. Private key rings

B. Trust models
C. Registration
D. Key escrow

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
An administrator responsible for building and validating security configurations is a violation of which of the following security principles?

A. Least privilege
B. Job rotation
C. Separation of duties
D. Best business practices

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Sara, a network security administrator, has been tasked with setting up a guest wireless network for her corporation. The requirements for this connection state that it must have password authentication, with passwords being changed every week. Which of the following security protocols would meet this goal in the MOST secure manner?

A. WPA CCMP
B. WPA PSK
C. WPA2-CCMP
D. WPA2-PSK

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following are security relevant policies? (Select THREE)

A. Information classification policy
B. Network access policy
C. Data security standard
D. Procurement policy
E. Domain name policy
F. Auditing and monitoring policy
G. Secure login process

Correct Answer: ABF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following attacks is manifested as an embedded HTML image object or JavaScript image tag in an email?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following network solutions would BEST allow Jane, a security technician, to host an extranet application for her company?

A. Platform as a Service
B. Infrastructure as a Service
C. Storage as a Service
D. Software as a Service

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Jane, a VPN administrator, was asked to implement an encryption cipher with a MINIMUM effective security of 128-bits. Which of the following should Jane select for the tunnel encryption?

A. Blowfish
B. DES
C. SHA256
D. HMAC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which of the following could Sara, an administrator, use in a workplace to remove sensitive data at rest from the premises?

A. Network sniffer
B. Personally owned devices
C. Vulnerability scanner
D. Hardware locks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following administrative controls BEST mitigates the risk of ongoing inappropriate employee activities in sensitive areas?

A. Mandatory vacations
B. Collusion
C. Time of day restrictions
D. Least privilege

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Traffic has stopped flowing to and from the company network after the inline IPS hardware failed.
Which of the following has occurred?

A. Failsafe
B. Congestion
C. Fuzzing
D. Disaster recovery

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
A company is installing a wireless network in a building that houses several tenants. Which of the following should be considered to make sure none of the other tenants can detect the company's wireless network? (Select TOO).

A. Static IP addresses
B. Wireless encryption

C. MAC filtering
D. Antenna placement
E. Power levels

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Pete is reporting an excessive amount of junk mail on the network email server. Which of the following would ONLY reduce the amount of unauthorized mail?

A. Network firewall
B. Port 25 restriction
C. Spam fitters
D. URL filters

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following network devices will prevent port scans?

A. Firewall
B. Load balancers
C. NIDS
D. Sniffer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following multifactor authentication methods uses biometrics?

A. Somewhere you are
B. Something you have
C. Something you know
D. Something you are

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Marketing creates a new folder and requests the following access be assigned:

Sales Department - Read

Marketing Department - Full Control

Inside Sales - Read Write

This is an example of which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Sara, the software security engineer, is trying to detect issues that could lead to buffer overflows or memory leaks in the company software. Which of the following would help Sara automate this detection?

A. Input validation
B. Exception handling
C. Fuzzing
D. Code review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following control types is video monitoring?

A. Detective
B. Management
C. Preventative
D. Access

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Pete, the Chief Executive Officer (CEO) of a company, has increased his travel plans for the next two years to improve business relations. Which of the following would need to be in place in case something happens to Pete?

A. Succession planning
B. Disaster recovery
C. Separation of duty
D. Removing single loss expectancy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following allows a server to request a website on behalf of Jane, a user?

A. Sniffers
B. Proxies
C. Load balancers
D. Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Matt, a systems security engineer, is determining which credential-type authentication to use within a planned 802.1x deployment. He is looking for a method that does not require a client certificate, has a server side certificate, and uses TLS tunnels for encryption. Which credential- type authentication method BEST fits these requirements?

A. EAP-TLS
B. EAP-FAST
C. PEAP-CHAP
D. PEAP-MSCHAPv2

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Sara, a security administrator, has generated a key pair for the company web server. Which of the following should she do next to ensure all web traffic to the company web server is encrypted?

A. Install both the private and the public key on the client machine.
B. Install both the private and the public key on the web server.

C. Install the public key on the web server and the private key on the client machine.
D. Install the public key on the client machine and the private key on the web server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Pete, a security administrator, would like to implement laptop encryption to protect data. The Chief Executive Officer (CEO) believes this will be too costly to implement and decides the company will purchase an insurance policy instead. Which of the following is this an example of?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Matt, a security administrator, needs to Telnet into a router to change some configurations. Which of the following ports would need to be open to allow Matt to change the configurations?

A. 23
B. 125
C. 143
D. 3389

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
The IT Security Department has completed an internal risk assessment and discovered the use of an outdated antivirus definition file. Which of the following is the NEXT step that management should take?

A. Analyze the vulnerability results from the scan.
B. Mitigate risk and develop a maintenance plan.
C. Ignore risk and document appropriately to address at a later time.
D. Transfer risk to web application developers.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following elements makes up the standard equation used to define risk? (Select TWO).

A. Confidence
B. Reproducibility
C. Impact
D. Likelihood
E. Exploitability

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Matt's CRL is over six months old. Which of the following could Matt do in order to ensure he has the current information? (Select TWO).

A. Update the CRL
B. Change the trust model
C. Deploy a key escrow
D. Query the intermediate CA
E. Deploy a recovery agent
F. Deploy OCSP

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Matt, the security administrator, notices a spike in the number of SQL injection attacks against a web server connected to a backend SQL database. Which of the following practices should be used to prevent an application from passing these attacks on to the database?

A. OS hardening
B. Application patch management
C. Error and exception handling
D. Input validation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Jane's guest, Pete, comes to her office to meet her for lunch. She uses her encoded badge to enter, and he follows in behind her. This is an example of which of the following?

A. Tailgating
B. Least privilege
C. Whaling
D. Vishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A vulnerability has been found in a service that is unnecessary for the corporate environment. Which of the following is the BEST way to mitigate this vulnerability?

A. Issue a hotfix to lower the vulnerability risk on the network
B. Issue a group policy to disable the service on the network.
C. Issue a service pack to ensure the service is current with all available patches
D. Issue a patch to ensure the service has a lower level of risk if compromised.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Broadcast traffic is having a negative impact on network performance. Which of the following might help minimize this issue?

A. Use NAT to hide the IPs of each of the workstations.
B. Separate the network onto a number of different switches.
C. Separate the network into a number of different VLANs.
D. Route all the Unicast traffic through the proxy server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
One of the concerns regarding portable digital music devices in a corporate environment is they:

A. can distract users during various security training exercises.
B. can also be used as a USB removable drive.
C. can be used as recorders during meetings.
D. may cause interference with wireless access points

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following describes separating encryption keys into multiple parts to store with trusted third parties?

A. Ticket granting ticket
B. Key recovery
C. Key escrow
D. Key registration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following authentication services relies on a shared secret?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following is characterized by an attack against a mobile device?

A. Evil twin
B. Header manipulation
C. Blue jacking
D. Rogue AP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following should Pete, a security technician, apply to a server to BEST prevent SYN attacks?

A. Loop protection
B. Flood guards
C. Port security
D. ACL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
When implementing a wireless network, which of the following will decrease the visibility of the network?

A. Decreasing the encryption strength
B. Disabling the SSID broadcast
C. Enabling WPA2 encryption
D. Enabling MAC filtering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following describes the process of removing unnecessary accounts and services from an application to reduce risk exposure?

A. Error and exception handling
B. Application hardening
C. Application patch management
D. Cross-site script prevention

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Mandatory vacation, job rotation, and separation of duties policies all enhance the overall security posture by doing which of the following?

A. Making it more convenient to review logs for malicious activity
B. Making it more difficult to hide malicious activity by insiders
C. Reducing risks associated with viruses and malware
D. Reducing risks associated with Internet attackers

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 49
A recent policy change requires Pete, a security administrator, to implement TLS wherever possible. Which of the following can TLS secure? (Select THREE).

A. SNMP
B. HTTP
C. LDAP
D. ICMP
E. SMTP
F. IPSec
G. SSH

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following allows a company to correct security issues within their software?

A. Application fuzzing
B. Cross-site scripting
C. Configuration baseline
D. Patch management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Matt, a security analyst, discovered that a commonly used website is serving up a script that redirects users to a questionable website. Which of the following solutions MOST likely prevents this from occurring?

A. Anti-malware
B. NIDS
C. Pop-up blocker
D. Anti-spam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Matt, a network engineer, is setting up an IPSec VPN. Which network-layer key management standard and its protocol can be used to negotiate the connection?

A. AH
B. Kerberos
C. EAP
D. IKE

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following devices can Sara, an administrator, implement to detect and stop known attacks?

A. Signature-based NIDS
B. Anomaly-based NIDS
C. Signature-based NIPS
D. Anomaly-based NIPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following represents the WEAKEST password?

A. PaSsWoRd
B. P@sSWOr&
C. P@sSW1r&
D. PassW1rD

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following is mainly used for remote access into the network?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
In order to prevent users from surfing the web at work, Jane, the administrator, should block which of the following ports? (Select TWO).

A. TCP 25
B. TCP 80
C. TCP 110
D. TCP 443
E. UDP 80
F. UDP 8080

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Matt, the IT administrator, wants to ensure that if any mobile device gets lost no data can be retrieved. Which of the following can he implement on the mobile devices to help accomplish this?

A. Cable locks
B. Strong passwords
C. Voice encryption
D. Remote sanitization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Matt, a security administrator, wants to configure all the switches and routers in the network in order to security monitor their status. Which of the following protocols would he need to configure on each device?

A. SMTP
B. SNMPv3
C. IPSec
D. SNMP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Jane, a security administrator, recently configured the firewall for the corporate office. Some users report that they are unable to access any resources outside of the company. Which of the following is the MOST likely reason for the lack of access?

A. Jane forgot to save the configuration on the firewall
B. Jane forgot to account for the implicit deny statement
C. Jane forgot to connect the internal firewall port back to the switch
D. Jane specifically denied access for all users

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following describes common concerns when implementing IPS?

A. Legitimate traffic will be incorrectly blocked
B. False negatives will disrupt network throughput
C. Incompatibilities with existing routers will result in a DoS
D. Security alerts will be minimal until adequate traffic is collected

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following network design elements will allow Jane, a security technician, to access internal company resources without the use of a DS3, Satellite, or T1 connection?

A. CSU/DSU
B. Firewall
C. Router
D. DSL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following utilizes the ECHO function of Internet Control Message Protocol (ICMP) to overwhelm a victim's system?

A. Logic bomb
B. Whaling

C. Man-in-the-middle
D. Smurf attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Matt, an administrator, is concerned about the wireless network being discovered by war driving. Which of the following can be done to mitigate this?

A. Enforce a policy for all users to authentic through a biometric device.
B. Disable all SSID broadcasting
C. Ensure all access points are running the latest firmware.
D. Move all access points into public access areas.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Jane, the administrator of a small company, wishes to track people who access the secured server room, which is secured only by a simple hardware key lock. Jane does not have much of a budget or the approval to make significant construction changes. Given the limitations, which of the following can she do in the meantime?

A. Implement a sign in/out sheet with on-site security personnel
B. Install a 24/7 closed-circuit camera system
C. Install a separate hardware lock with limited keys
D. Implement a cipher key lock

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following enterprise security controls is BEST implemented by the use of a RADIUS server?

A. ACL
B. NAT
C. VLAN
D. 802.1X

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Pete, the security administrator at a financial institution, has finished downloading a new system patch and needs to verify its authenticity. Which of the following is the correct MD5 string for the file he downloaded?

A. 1a03b7fe4c67d9012gb42b4de49d9f3b
B. b42b4de49d9f3b1a03b7fe4c67d9012
C. 303b7fe4c67d9012b42b4de49d9f3b134
D. ab42b4de49d9f3b1a03b7f34c67d9012

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
One of the advantages of Trusted Platform Modules (TPM) is:

A. it cannot be modified by a silent background process.
B. it is tied to the system's MAC address for secured tracking.
C. it cannot be used as the basis for securing other encryption methods.
D. it can be tied to the user's logon account for additional authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which of the following protocols is MOST closely linked with SSL?

A. SNMP
B. TLS
C. FTP
D. ICMP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which of the following would Jane, an administrator, use to detect an unknown security vulnerability?

A. Patch management
B. Application fuzzing
C. ID badge

D. Application configuration baseline

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following data center environmental controls must be property configured to prevent equipment failure from water?

A. Lighting
B. Temperature
C. Humidity
D. Halon fire suppression

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Matt, a corporate user, has volunteered to participate in a test group for full disk encryption on employees' laptops. After his laptop's hard drive has been fully encrypted, the network administrator is still able to access Matt's files across a SMB share. Which of the following is the MAIN reason why the files are still accessible to the administrator?

A. Matt must reboot his laptop before the encryption is activated.
B. Files moved by the network administrator off Matt's laptop are automatically decrypted
C. Full disk encryption only secures files when the laptop is powered off
D. The network administrator can decrypt anyone's files.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Hashing and encryption provide for which of the following? (Select TWO)

A. Authentication
B. Availability
C. Identification
D. Confidentiality
E. Authorization
F. Integrity

Correct Answer: DF
Section: (none)

Explanation

Explanation/Reference:

QUESTION 73
Which of the following will require exceptions when considering the use of 802.1x port security?

A. Switches
B. Printers
C. Laptops
D. Desktops

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following data encryption types will BEST protect data in motion and at rest to a cloud provider?

A. File encryption
B. Transport
C. PKI
D. SHA-256

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following will mitigate the effects of devices in close proximity?

A. EMI shielding
B. Load balancing
C. Grounding
D. Video monitoring

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A major CA has been compromised and a new patch has been released to make necessary changes on user machines. Which of the following is likely to be updated as a part of this patch?

A. Recovery agent

B. CRL
C. Key escrow
D. PKI

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following uses both a public and private key?

A. RSA
B. AES
C. MD5
D. SHA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Visitors entering a building are required to close the back door before the front door of the same entry room is open. Which of the following is being described?

A. Tailgating
B. Fencing
C. Screening
D. Mantrap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Symmetric encryption utilizes_____. While asymmetric encryption utilizes_____.

A. Public keys, one time
B. Shared keys, private keys
C. Private keys, session keys
D. Private keys, public keys

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Jane, an administrator, notices that after 2.000 attempts a malicious user was able to compromise an employee's password. Which of the following security controls BEST mitigates this type of external attack? (Select TWO).

A. Account expiration
B. IDS
C. Password complexity
D. Server logging
E. Account lockout
F. Proxy server

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Matt, the network engineer, has been tasked with separating network traffic between virtual machines on a single hypervisor. Which of the following would he implement to BEST address this requirement? (Select TWO).

A. Virtual switch
B. NAT
C. System partitioning
D. Access-list
E. Disable spanning tree
F. VLAN

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Sara, an IT manager, wants to change the firewall rules to allow RemoteOfficeB to connect to the corporate network using SSH. Which of the following rules would only allow necessary access?

A. Permit RemoteOfficeB any port 69
B. Permit RemoteOfficeB any all
C. Permit RemoteOfficeB any port 22
D. Permit any corporate port 443

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following attacks is characterized by someone following a staff member who is entering a corporate facility?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Speaking a passphrase into a voice print analyzer is an example of which of the following security concepts?

A. Two factor authentication
B. Identification and authorization
C. Single sign-on
D. Single factor authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Jane, a corporate user, is trying to secure her laptop from drive-by download before she leaves for a computer conference. Which of the following should be installed to keep Jane's laptop secure from these attacks?

A. Full disk encryption
B. Host based firewall
C. Antivirus system
D. Network based firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following detection methods may generate an alert when Matt, an employee, accesses a server during non-business hours?

A. Signature
B. Time of Day restrictions
C. Heuristic

D. Behavioral

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following data is typically left unencrypted in software based full disk encryption?

A. OS registry
B. Extended partition
C. BIOS
D. MBR

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following is an authentication service that uses symmetrical keys and tickets?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following application attacks is identified by use of the <SCRIPT> tag?

A. XSS
B. Buffer overflow
C. Directory traversal
D. Zero day

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Jane, a security architect, is working on setting up a secure email solution between internal employees and

external customers. Which of the following would BEST meet her goal?

A. Public key infrastructure
B. Key escrow
C. Internal certificate authority
D. Certificate revocation list

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following allows multiple internal IP addresses to be mapped to one specific external IP address?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following would Jane, a security administrator, use to encrypt transmissions from streaming video transmissions, keeping in mind that each bit must be encrypted as it comes across the network?

A. IDEA
B. AES
C. RC4
D. 3DES

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Matt, a user, finds a flash drive in the parking lot and decides to see what is on it by using his company laptop. A few days later Matt reports his laptop is running slow and is unable to perform simple tasks. The security administrator notices several unauthorized applications have been installed. CPU usage is unusually high, and a collection of screenshots of Matt's recent activity has been transmitted over the network .This is an example of which of the following?

A. Backdoor
B. Logic bomb
C. Rootkit

D. Spyware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Pete, the security administrator, found that several of the company's workstations are infected with a program aimed at stealing users' cookies and reporting them back to the malicious user. Which of the following attack types is the malicious user MOST likely to carry out with this information?

A. Man-in-the-middle
B. Session hijacking
C. Command injection
D. Trojan infection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Sara, a security administrator, is implementing remote management for network infrastructure using SNMP. Which of the following statements is true about SNMP?

A. Read communities allow write permissions
B. Relays mail based on domain keys and access headers
C. SNMP communities are encrypted using PKI
D. Write communities allow both read and write permissions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following mitigation techniques is Pete, a security administrator, MOST likely to implement after the software has been released to the public?

A. Error and exception handling
B. Fuzzing
C. Secure coding
D. Patch management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which of the following BEST defines risk?

A. A threat will have a larger impact than anticipated
B. Remediation of a known vulnerability is cost prohibitive
C. A degree of probability of loss
D. A user leaves a system unsecure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Companies allowing remote access to internal systems or systems containing sensitive data should provide access using:

A. dial-up or broadband networks using passwords.
B. wireless networks using WPA encryption.
C. VPN with two factor authentication.
D. carrier based encrypted data networks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following is the proper order for incident response?

A. Detection, preparation, containment, eradication, recovery
B. Preparation, detection, containment, eradication, recovery
C. Preparation, detection, recovery, eradication, containment
D. Detection, containment, eradication, recovery, preparation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following is considered the MOST secure wireless encryption measure to implement?

A. TKIP
B. CCMP
C. WPA2
D. WEP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Exam D

QUESTION 1
Sara, a security engineer, is testing encryption ciphers for performance. Which of the following ciphers offers strong encryption with the FASTEST speed?

A. 3DES
B. Blowfish
C. Serpent
D. AES256

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A team is developing a new application with many different screens that users can access. The team decides to simplify access by creating just two internal application roles. One role is granted read-only access to the summary screen. The other role is granted update access to all screens. This simplified access model may have a negative security impact on which of the following?

A. Remote access
B. Identity management
C. Least privilege
D. Authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following would be the BEST choice for attacking a complex password hash?

A. Man in the middle
B. Dictionary files
C. Rainbow tables
D. Brute-force intrusion

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
In order for Pete, a user, to logon to his desktop computer, he must provide his username, password, and use a common access card with a PIN. Which of the following authentication methods is Pete using?

A. Single factor

B. Two factor
C. Three factor
D. Four factor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following is a reason why a company might deploy data encryption?

A. To maintain the integrity of the information
B. To keep information confidential
C. To prevent data corruption
D. To prevent backup tape theft

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following would Sara, a security administrator, implement to divert and analyze attacks?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Topic 6, Volume F

QUESTION 7
In PKI, the public key is used to:

A. Decrypt the signature CRC
B. Decrypt an email message
C. Encrypt an email message
D. Encrypt the signature hash

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Jane, a security technician, needs to open ports on a firewall to allow for domain name resolution. Which of the following ports should Jane open? (Select TWO).

A. TCP 21
B. TCP 23
C. TCP 53
D. UDP 23
E. UDP 53

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
After a new firewall has been installed, devices cannot obtain a new IP address. Which of the following ports should Matt, the security administrator, open on the firewall?

A. 25
B. 68
C. 80
D. 443

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
The health care department is storing files with names, addresses, and social security numbers on a corporate file server. Matt, the security analyst, comes across this data in an audit. Which of the following has Matt discovered?

A. Personal identifiable information
B. Data classification rules
C. Data disposal procedures
D. Data handling rules

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Matt, a forensic analyst, wants to obtain the digital fingerprint for a given message. The message is 160-bits long. Which of the following hashing methods would Matt have to use to obtain this digital fingerprint?

A. SHA1

B. MD2
C. MD4
D. MD5

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following would Jane, a security administrator, use to authenticate remote users into the network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A company wants to implement a policy that helps reduce employee stress and decrease the likelihood of security incidents caused by job dissatisfaction. Which of the following will MOST likely have a positive impact on the employee stress and job satisfaction?

A. Change management
B. Mandatory vacations
C. Due care
D. Service Level Agreements

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Pete would like to implement a new tape backup plan for HR to speed up the process of nightly backups on their file systems HR does not make many file alterations on Tuesday through Thursday. Pete does a full backup on Monday and again on Friday. Which of the following should Pete do to speed up the backups Tuesday through Thursday?

A. Incremental backups Tuesday through Thursday
B. Full backups Tuesday through Thursday
C. Differential backups Tuesday through Thursday
D. Differential backups Tuesday and Wednesday

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Sara, a user, needs to copy a file from a Linux workstation to a Linux server using the MOST secure file transfer method available. Which of the following protocols would she use?

A. SCP
B. FTP
C. SNMP
D. TFTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following would Matt, a security administrator, use to encrypt transmissions from an internal database to an internal server, keeping in mind that the encryption process must add as little latency to the process as possible?

A. ECC
B. RSA
C. SHA
D. 3DES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Matt, a system administrator, notices that there have been many failed login attempts to the virtual server's management interface. Which of the following would be the BEST way for him to secure the virtual server's OS?

A. Implement QoS
B. Create an access control list
C. Isolate the management network
D. Enable SSH

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which of the following wireless attacks MOST likely targets a smart phone?

A. War driving
B. Whaling
C. IV attack
D. Bluesnarfing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following host security procedures will facilitate in the identification of Advanced Persistent Threats (APT)?

A. Remote wipe
B. Group policy implementation
C. Host software baselining
D. Antivirus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Jane, a security technician, has been called into a meeting with the management team who has a requirement for comprehensive vetting of specialized employees as part of the hiring process. Funding and resources are not an issue since staff members are in high risk positions and have access to sensitive data. Which of the following access control types BEST meets the requirement?

A. Rule based access control
B. Discretionary access control
C. Mandatory access control
D. Role based access control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
A company wants to ensure that its hot site is prepared and functioning. Which of the following would be the BEST process to verily the backup datacenter is prepared for such a scenario?

A. Site visit to the backup data center
B. Disaster recovery plan review

C. Disaster recovery exercise
D. Restore from backup

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Pete, the security administrator, would like all users connecting to the corporate SSL VPN router to have up-to-date patches and antivirus signatures verified prior to accessing the internal network. Which of the following would MOST likely be employed as the verification process?

A. The router ACL matches VPN traffic. The NAC server verifies antivirus signatures are supported and up-to-date.
B. The NAC server processes the authentication, and then it matches patches and antivirus signatures with its local database.
C. The access control server connects to the agent on the users' client to set minimal accepted levels of patching and signatures allowed. The agent creates a token which the router can match for access.
D. The router sends queries to the access control server; the access control server handles proxy requests to third party patching and antivirus servers.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
In which of the following access control types does the operating system data classification determine who has access to certain resources?

A. Discretionary Access Control
B. Role based Access Control
C. Mandatory Access Control
D. Rule based Access Control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Sara, a security administrator, needs to simplify the management of access to remote files and folders. Which of the following can she implement to BEST accomplish this?

A. Group based ACLs
B. Creating multiple copies of the files and folders
C. Discretionary access control
D. User based ACLs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Matt, a security administrator, wants to implement a secure wireless network. Which of the following is the MOST secure wireless protocol?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following protocols allows for the LARGEST address space?

A. IPX
B. IPv4
C. IPv6
D. Appletalk

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
In order to justify the cost of a new security appliance, the administrator should do which of the following?

A. RIO analysis
B. Benchmarking
C. Market analysis
D. Usability testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following is responsible for masking the activity of an on-going attack from the administrator's operating system monitoring tools?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following forms of FTP uses TLS to securely send information?

A. SCP
B. FTPS
C. SFTP
D. HTTPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following BEST allows Jane, a security administrator, to perform ongoing assessments of existing weaknesses within an enterprise?

A. Vulnerability scanning
B. NIPS
C. HIDS
D. Protocol analyzer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Jane, an attacker, compromises a payroll system and replaces a commonly executed application with a modified version which appears to run as normal but also executes additional functions. Which of the following would BEST describe the slightly modified application?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
To protect corporate data on removable media, a security policy should mandate that all removable devices use which of the following?

A. Full disk encryption
B. Application isolation
C. Digital rights management
D. Data execution prevention

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following would allow Pete, a security analyst, to assess his company's proficiency with a particular security process?

A. Risk Assessment
B. Capability Maturity Model
C. Risk Calculation
D. Trusted Platform Module

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
The Chief Security Officer (CSO) informs Jane, the technician, that there is a new requirement for all data repositories where data must be encrypted when not in use. The CSO wants Jane to apply this requirement to all corporate servers. Which of the following data encryption types will BEST fill this requirement?

A. Mobile device encryption
B. Full disk encryption
C. Transport encryption
D. Database encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35

Jane, a security technician, needs to develop access controls for the network. In which of the following access control types does a user determine who has access to certain network resources?

A. Mandatory Access Control
B. Rule based Access Control
C. Role based Access Control
D. Discretionary Access Control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following should Pete, the security technician, use to secure DNS zone transfers?

A. VLAN
B. DIMSSEC
C. ACL
D. 802.1X

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Matt, a network engineer, is implementing a VPN solution. Which of the following can Matt use to secure the user authentication session?

A. GPG
B. PGP
C. CHAP
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Sara, a user in the human resources department, requests a privacy screen for her monitor at work. Which of the following social engineering attack is Sara attempting to prevent?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
New Question

QUESTION 39
A password history value of three means which of the following?

A. Three different passwords are used before one can be reused.
B. A password cannot be reused once changed for three years.
C. After three hours a password must be re-entered to continue.
D. The server stores passwords in the database for three days.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
In order to provide flexible working conditions, a company has decided to allow some employees remote access into corporate headquarters. Which of the following security technologies could be used to provide remote access? (Select TWO).

A. Subnetting
B. NAT
C. Firewall
D. NAC
E. VPN

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following is the BEST approach to perform risk mitigation of user access control rights?

A. Conduct surveys and rank the results.
B. Perform routine user permission reviews.
C. Implement periodic vulnerability scanning.
D. Disable user accounts that have not been used within the last two weeks.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42

All of the following are valid cryptographic hash functions EXCEPT:

A. RIPEMD
B. RC4
C. SHA-512
D. MD4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following can prevent an unauthorized person from accessing the network by plugging into an open network jack?

A. 802.1x
B. DHCP
C. 802.1q
D. NIPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A targeted email attack sent to Sara, the company's Chief Executive Officer (CEO), is known as which of the following?

A. Whaling
B. Bluesnarfing
C. Vishing
D. Dumpster diving

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
After verifying that the server and database are running, Jane, the administrator, is still unable to make a TCP connection to the database. Which of the following is the MOST likely cause for this?

A. The server has data execution prevention enabled
B. The server has TPM based protection enabled
C. The server has HIDS installed
D. The server is running a host-based firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
In regards to secure coding practices, why is input validation important?

A. It mitigates buffer overflow attacks.
B. It makes the code more readable.
C. It provides an application configuration baseline.
D. It meets gray box testing standards.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following is a best practice before deploying a new desktop operating system image?

A. Install network monitoring software
B. Perform white box testing
C. Remove single points of failure
D. Verify operating system security settings

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following steps should follow the deployment of a patch?

A. Antivirus and anti-malware deployment
B. Audit and verification
C. Fuzzing and exploitation
D. Error and exception handling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following would be used when a higher level of security is desired for encryption key storage?

A. TACACS+

B. L2TP
C. LDAP
D. TPM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check?

A. Firewall
B. Application
C. IDS
D. Security

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
If Pete, a security administrator, wants to ensure that certain users can only gain access to the system during their respective shifts, which of the following best practices would he implement?

A. Separation of duties
B. Time of day restrictions
C. Implicit deny rule
D. Least privilege

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following MUST be updated immediately when an employee is terminated to prevent unauthorized access?

A. Registration
B. CA
C. CRL
D. Recovery agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
A small business owner has asked the security consultant to suggest an inexpensive means to deter physical intrusions at their place of business. Which of the following would BEST meet their request?

A. Fake cameras
B. Proximity readers
C. Infrared cameras
D. Security guards

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Employee badges are encoded with a private encryption key and specific personal information. The encoding is then used to provide access to the network. Which of the following describes this access control type?

A. Smartcard
B. Token
C. Discretionary access control
D. Mandatory access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following devices would MOST likely have a DMZ interface?

A. Firewall
B. Switch
C. Load balancer
D. Proxy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A security administrator is observing congestion on the firewall interfaces and a high number of half open incoming connections from different external IP addresses. Which of the following attack types is underway?

A. Cross-site scripting

B. SPIM
C. Client-side
D. DDoS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following tools would Matt, a security administrator, MOST likely use to analyze a malicious payload?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following application security testing techniques is implemented when an automated system generates random input data?

A. Fuzzing
B. XSRF
C. Hardening
D. Input validation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file?

A. Cognitive password
B. Password sniffing
C. Brute force
D. Social engineering

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A security administrator wants to check user password complexity. Which of the following is the BEST tool to use?

A. Password history
B. Password logging
C. Password cracker
D. Password hashing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Certificates are used for: (Select TWO).

A. client authentication
B. WEP encryption
C. access control lists
D. code signing
E. password hashing

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following is a hardware based encryption device?

A. EFS
B. TrueCrypt
C. TPM
D. SLE

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following BEST describes a protective countermeasure for SQL injection?

A. Eliminating cross-site scripting vulnerabilities

B. Installing an IDS to monitor network traffic
C. Validating user input in web applications
D. Placing a firewall between the Internet and database servers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which of the following MOST interferes with network-based detection techniques?

A. Mime-encoding
B. SSL
C. FTP
D. Anonymous email accounts

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A certificate authority takes which of the following actions in PKI?

A. Signs and verifies all infrastructure messages
B. Issues and signs all private keys
C. Publishes key escrow lists to CRLs
D. Issues and signs all root certificates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Use of a smart card to authenticate remote servers remains MOST susceptible to which of the following attacks?

A. Malicious code on the local system
B. Shoulder surfing
C. Brute force certificate cracking
D. Distributed dictionary attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Separation of duties is often implemented between developers and administrators in order to separate which of the following?

A. More experienced employees from less experienced employees
B. Changes to program code and the ability to deploy to production
C. Upper level management users from standard development employees
D. The network access layer from the application access layer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A security administrator needs to update the OS on all the switches in the company. Which of the following MUST be done before any actual switch configuration is performed?

A. The request needs to be sent to the incident management team.
B. The request needs to be approved through the incident management process.
C. The request needs to be approved through the change management process.
D. The request needs to be sent to the change management team.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Jane, an individual, has recently been calling various financial offices pretending to be another person to gain financial information. Which of the following attacks is being described?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
The security administrator wants each user to individually decrypt a message but allow anybody to encrypt it. Which of the following MUST be implemented to allow this type of authorization?

A. Use of CA certificate
B. Use of public keys only

C. Use of private keys only
D. Use of public and private keys

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A user in the company is in charge of various financial roles but needs to prepare for an upcoming audit. They use the same account to access each financial system. Which of the following security controls will MOST likely be implemented within the company?

A. Account lockout policy
B. Account password enforcement
C. Password complexity enabled
D. Separation of duties

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
An employee is granted access to only areas of a network folder needed to perform their job. Which of the following describes this form of access control?

A. Separation of duties
B. Time of day restrictions
C. Implicit deny
D. Least privilege

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
A CRL is comprised of:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following may significantly reduce data loss if multiple drives fail at the same time?

A. Visualization
B. RAID
C. Load balancing
D. Server clustering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following should be considered to mitigate data theft when using CAT5 wiring?

A. CCTV
B. Environmental monitoring
C. Multimode fiber
D. EMI shielding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

A. Management
B. Administrative
C. Technical
D. Operational

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO).

A. 10.4.4.125
B. 10.4.4.158

C. 10.4.4.165
D. 10.4.4.189
E. 10.4.4.199

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following algorithms has well documented collisions? (Select TWO).

A. AES
B. MD5
C. SHA
D. SHA-256
E. RSA

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Jane, the security administrator, needs to be able to test malicious code in an environment where it will not harm the rest of the network. Which of the following would allow Jane to perform this kind of testing?

A. Local isolated environment
B. Networked development environment
C. Infrastructure as a Service
D. Software as a Service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A company is sending out a message to all users informing them that all internal messages need to be digitally signed. This is a form of which of the following concepts?

A. Availability
B. Non-repudiation
C. Authorization
D. Cryptography

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following transportation encryption protocols should be used to ensure maximum security between a web browser and a web server?

A. SSLv2
B. SSHv1
C. RSA
D. TLS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Developers currently have access to update production servers without going through an approval process. Which of the following strategies would BEST mitigate this risk?

A. Incident management
B. Clean desk policy
C. Routine audits
D. Change management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
A server containing critical data will cost the company $200/hour if it were to be unavailable due to DoS attacks. The security administrator expects the server to become unavailable for a total of two days next year. Which of the following is true about the ALE?

A. The ALE is $48.
B. The ALE is $400.
C. The ALE is $4,800.
D. The ALE is $9,600.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
To reduce an organization's risk exposure by verifying compliance with company policy, which of the following should be performed periodically?

A. Qualitative analysis
B. Quantitative analysis
C. Routine audits
D. Incident management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following is a difference between TFTP and FTP?

A. TFTP is slower than FTP.
B. TFTP is more secure than FTP.
C. TFTP utilizes TCP and FTP uses UDP.
D. TFTP utilizes UDP and FTP uses TCP.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A system administrator decides to use SNMPv3 on the network router in AuthPriv mode. Which of the following algorithm combinations would be valid?

A. AES-RC4
B. 3DES-MD5
C. RSA-DSA
D. SHA1-HMAC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following are encryption algorithms that can use a 128-bit key size? (Select TWO).

A. AES
B. RC4
C. Twofish
D. DES
E. SHA2

Correct Answer: AC
Section: (none)

Explanation

Explanation/Reference:

QUESTION 88
Matt, an administrator, notices a flood fragmented packet and retransmits from an email server. After disabling the TCP offload setting on the NIC, Matt sees normal traffic with packets flowing in sequence again. Which of the following utilities was he MOST likely using to view this issue?

A. Spam filter
B. Protocol analyzer
C. Web application firewall
D. Load balancer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following specifications would Sara, an administrator, implement as a network access control?

A. 802.1q
B. 802.3
C. 802.11n
D. 802.1x

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following is characterized by an attacker attempting to map out an organization's staff hierarchy in order to send targeted emails?

A. Whaling
B. Impersonation
C. Privilege escalation
D. Spear phishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following defines when Pete, an attacker, attempts to monitor wireless traffic in order to perform malicious activities?

A. XSS
B. SQL injection
C. Directory traversal
D. Packet sniffing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following provides the MOST protection against zero day attacks via email attachments?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following access controls enforces permissions based on data labeling at specific levels?

A. Mandatory access control
B. Separation of duties access control
C. Discretionary access control
D. Role based access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A username provides which of the following?

A. Biometrics
B. Identification
C. Authorization
D. Authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Use of group accounts should be minimized to ensure which of the following?

A. Password security
B. Regular auditing
C. Baseline management
D. Individual accountability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Privilege creep among long-term employees can be mitigated by which of the following procedures?

A. User permission reviews
B. Mandatory vacations
C. Separation of duties
D. Job function rotation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
In which of the following scenarios is PKI LEAST hardened?

A. The CRL is posted to a publicly accessible location.
B. The recorded time offsets are developed with symmetric keys.
C. A malicious CA certificate is loaded on all the clients.
D. All public keys are accessed by an unauthorized user.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Configuring the mode, encryption methods, and security associations are part of which of the following?

A. IPSec
B. Full disk encryption
C. 802.1x
D. PKI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following assessments would Pete, the security administrator, use to actively test that an application's security controls are in place?

A. Code review
B. Penetration test
C. Protocol analyzer
D. Vulnerability scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following would be used to identify the security posture of a network without actually exploiting any weaknesses?

A. Penetration test
B. Code review
C. Vulnerability scan
D. Brute Force scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Exam E

QUESTION 1
Which of the following is used to certify intermediate authorities in a large PKI deployment?

A. Root CA
B. Recovery agent
C. Root user
D. Key escrow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following components MUST be trusted by all parties in PKI?

A. Key escrow
B. CA
C. Private key
D. Recovery key

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
When checking his webmail, Matt, a user, changes the URL's string of characters and is able to get into another user's inbox. This is an example of which of the following?

A. Header manipulation
B. SQL injection
C. XML injection
D. Session hijacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Elliptic curve cryptography: (Select TWO)

A. is used in both symmetric and asymmetric encryption.
B. is used mostly in symmetric encryption.
C. is mostly used in embedded devices.
D. produces higher strength encryption with shorter keys.

E. is mostly used in hashing algorithms.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Topic 7, Volume G

QUESTION 5
Which of the following would an antivirus company use to efficiently capture and analyze new and unknown malicious attacks?

A. Fuzzer
B. IDS
C. Proxy
D. Honeynet

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Why is it important for a penetration tester to have established an agreement with management as to which systems and processes are allowed to be tested?

A. Penetration test results are posted publicly, and some systems tested may contain corporate secrets.
B. Penetration testers always need to have a comprehensive list of servers, operating systems, IP subnets, and department personnel prior to ensure a complete test.
C. Having an agreement allows the penetration tester to look for other systems out of scope and test them for threats against the in-scope systems.
D. Some exploits when tested can crash or corrupt a system causing downtime or data loss.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
A system administrator is using a packet sniffer to troubleshoot remote authentication. The administrator detects a device trying to communicate to TCP port 49. Which of the following authentication methods is MOST likely being attempted?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
An administrator wants to minimize the amount of time needed to perform backups during the week. It is also acceptable to the administrator for restoration to take an extended time frame. Which of the following strategies would the administrator MOST likely implement?

A. Full backups on the weekend and incremental during the week
B. Full backups on the weekend and full backups every day
C. Incremental backups on the weekend and differential backups every day
D. Differential backups on the weekend and full backups every day

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following can be used in code signing?

A. AES
B. RC4
C. GPG
D. CHAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following can use RC4 for encryption? (Select TWO).

A. CHAP
B. SSL
C. WEP
D. AES
E. 3DES

Correct Answer: BC
Section: (none)

Explanation

Explanation/Reference:

QUESTION 11
Which of the following defines a business goal for system restoration and acceptable data loss?

A. MTTR
B. MTBF
C. RPO
D. Warm site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following defines an organization goal for acceptable downtime during a disaster or other contingency?

A. MTBF
B. MTTR
C. RTO
D. RPO

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

A. CCTV system access
B. Dial-up access
C. Changing environmental controls
D. Ping of death

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
An ACL placed on which of the following ports would block IMAP traffic?

A. 110

B. 143
C. 389
D. 465

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following provides the HIGHEST level of confidentiality on a wireless network?

A. Disabling SSID broadcast
B. MAC filtering
C. WPA2
D. Packet switching

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following controls should be used to verify a person in charge of payment processing is not colluding with anyone to pay fraudulent invoices?

A. Least privilege
B. Security policy
C. Mandatory vacations
D. Separation of duties

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Please be aware that if you do not accept these terms you will not be allowed to take this CompTIA exam and you will forfeit the fee paid.

A. RETURN TO EXAM
B. EXIT EXAM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following should be implemented to stop an attacker from mapping out addresses and/or devices on a network?

A. Single sign on
B. IPv6
C. Secure zone transfers
D. VoIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following anti-malware solutions can be implemented to mitigate the risk of phishing?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following can be used to mitigate risk if a mobile device is lost?

A. Cable lock
B. Transport encryption
C. Voice encryption
D. Strong passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following should the security administrator do when taking a forensic image of a hard drive?

A. Image the original hard drive, hash the image, and analyze the original hard drive.
B. Copy all the files from the original into a separate hard drive, and hash all the files.
C. Hash the original hard drive, image the original hard drive, and hash the image.
D. Image the original hard drive, hash the original hard drive, and analyze the hash.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
A marketing employee requests read and write permissions to the finance department's folders. The security administrator partially denies this request and only gives the marketing employee read-only permissions. This is an example of which of the following?

A. Job rotation
B. Separation of duties
C. Least privilege
D. Change management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Mike, a network administrator, has been asked to passively monitor network traffic to the company's sales websites. Which of the following would be BEST suited for this task?

A. HIDS
B. Firewall
C. NIPS
D. Spam filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
An administrator notices an unusual spike in network traffic from many sources. The administrator suspects that:

A. it is being caused by the presence of a rogue access point.
B. it is the beginning of a DDoS attack.
C. the IDS has been compromised.
D. the internal DNS tables have been poisoned.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Mike, a security professional, is tasked with actively verifying the strength of the security controls on a company's live modem pool. Which of the following activities is MOST appropriate?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Users at a company report that a popular news website keeps taking them to a web page with derogatory content. This is an example of which of the following?

A. Evil twin
B. DNS poisoning
C. Vishing
D. Session hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
An encrypted message is sent using PKI from Sara, a client, to a customer. Sara claims she never sent the message. Which of the following aspects of PKI BEST ensures the identity of the sender?

A. CRL
B. Non-repudiation
C. Trust models

D. Recovery agents

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following protocols would be used to verify connectivity between two remote devices at the LOWEST level of the OSI model?

A. DNS
B. SCP
C. SSH
D. ICMP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

A. Common access card
B. Role based access control
C. Discretionary access control
D. Mandatory access control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Jane, a security administrator, has observed repeated attempts to break into a server. Which of the following is designed to stop an intrusion on a specific server?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Matt, the security administrator, notices a large number of alerts on the NIDS. Upon further inspection, it is determined that no attack has really taken place. This is an example of a:

A. false negative
B. true negative
C. false positive
D. true positive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

A. Create a VLAN without a default gateway.
B. Remove the network from the routing table.
C. Create a virtual switch.
D. Commission a stand-alone switch.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

A. 20
B. 21
C. 22
D. 23

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

A. Availability
B. Integrity

C. Confidentiality
D. Fire suppression

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following pseudocodes can be used to handle program exceptions?

A. If program detects another instance of itself, then kill program instance.
B. If user enters invalid input, then restart program.
C. If program module crashes, then restart program module.
D. If user's input exceeds buffer length, then truncate the input.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following devices can Sara, an administrator, implement to detect and stop known attacks?

A. Signature-based NIDS
B. Anomaly-based NIDS
C. Signature-based NIPS
D. Anomaly-based NIPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following protocols would be implemented to secure file transfers using SSL?

A. TFTP
B. SCP
C. SFTP
D. FTPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following security concepts are used for data classification and labeling to protect data? (Select TWO).

A. Need to know
B. Role based access control
C. Authentication
D. Identification
E. Authorization

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?

A. EAP-TLS
B. PEAP
C. WEP
D. WPA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Jane, an administrator, hears reports of circles being drawn in the parking lot. Because the symbols fall within range of the company's wireless AP, the MOST likely concern is:

A. that someone has used war chalking to help others access the company'snetwork
B. that the symbols indicate the presence ofan evil twin of a legitimate AP
C. that someone is planning to install an AP where the symbols are, to cause interference
D. that a rogue access point has been installed within range of the symbols

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following are used to implement VPNs? (Select TWO).

A. SFTP
B. IPSec
C. HTTPS

D. SNMP
E. SSL

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device?

A. Man-in-the-middle
B. Bluejacking
C. Bluesnarfing
D. Packet sniffing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Matt, a security administrator, is receiving reports about several SQL injections and buffer overflows through his company's website. Which of the following would reduce the amount of these attack types?

A. Antivirus
B. Anti-spam
C. Input validation
D. Host based firewalls

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Enforcing data encryption of removable media ensures that the:

A. lost media cannot easily be compromised.
B. media can be identified.
C. location of the media is known at all times.
D. identification of the user is non-repudiated.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Pete, an employee, is terminated from the company and the legal department needs documents from his encrypted hard drive. Which of the following should be used to accomplish this task? (Select TWO).

A. Private hash
B. Recovery agent
C. Public key
D. Key escrow
E. CRL

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A company had decided to assign employees laptops instead of desktops to mitigate the risk of company closures due to disasters. Which of the following is the company trying to ensure?

A. Succession planning
B. Fault tolerance
C. Continuity of operations
D. Removing single points of failure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems?

A. Incident management
B. Server clustering
C. Change management
D. Forensic analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following can Pete, a security administrator, use to distribute the processing effort when generating hashes for a password cracking program?

A. RAID

B. Clustering
C. Redundancy
D. Visualization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?

A. Identify user habits
B. Disconnect system from network
C. Capture system image
D. Interview witnesses

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Pete, the security administrator, wants to ensure that traffic to the corporate intranet is secure using HTTPS. He configures the firewall to deny traffic to port 80. Now users cannot connect to the intranet even through HTTPS. Which of the following is MOST likely causing the issue?

A. The web server is configured on the firewall's DMZ interface.
B. The VLAN is improperly configured.
C. The firewall's MAC address has not been entered into the filtering list.
D. The firewall executes an implicit deny.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Mike, a user, receives an email from his grandmother stating that she is in another country and needs money. The email address belongs to his grandmother. Which of the following attacks is this?

A. Man-in-the-middle
B. Spoofing
C. Relaying
D. Pharming

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 53
Which of the following protocols can be used to secure traffic for telecommuters?

A. WPA
B. IPSec
C. ICMP
D. SMTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

A. Implement WPA
B. Disable SSID
C. Adjust antenna placement
D. Implement WEP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following is a management control?

A. Logon banners
B. Written security policy
C. SYN attack prevention
D. Access Control List (ACL)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following risk concepts BEST supports the identification of fraud?

A. Risk transference
B. Management controls

C. Mandatory vacations
D. Risk calculation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following security strategies allows a company to limit damage to internal systems and provides loss control?

A. Restoration and recovery strategies
B. Deterrent strategies
C. Containment strategies
D. Detection strategies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
In order for Sara, a client, to logon to her desktop computer, she must provide her username, password, and a four digit PIN. Which of the following authentication methods is Sara using?

A. Three factor
B. Single factor
C. Two factor
D. Four factor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following must Jane, a security administrator, implement to ensure all wired ports are authenticated before a user is allowed onto the network?

A. Intrusion prevention system
B. Web security gateway
C. Network access control
D. IP access control lists

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Mike, a server engineer, has received four new servers and must place them in a rack in the datacenter. Which of the following is considered best practice?

A. All servers' air exhaust toward the cold aisle.
B. All servers' air intake toward the cold aisle.
C. Alternate servers' air intake toward the cold and hot aisle.
D. Servers' air intake must be parallel to the cold/hot aisles.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Mike, a security analyst, has captured a packet with the following payload.

GET ../../../../system32\/cmd.exe

Which of the following is this an example of?

A. SQL injection
B. Directory traversal
C. XML injection
D. Buffer overflow

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
A security administrator needs to open ports on the firewall to allow for secure data transfer. Which of the following TCP ports would allow for secure transfer of files by default?

A. 21
B. 22
C. 23
D. 25

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following technologies would allow for a secure tunneled connection from one site to another?

(Select TWO).

A. SFTP
B. IPSec
C. SSH
D. HTTPS
E. ICMP

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which of the following sets numerous flag fields in a TCP packet?

A. XMAS
B. DNS poisoning
C. SYN flood
D. ARP poisoning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following network design elements provides for a one-to-one relationship between an internal network address and an external network address?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Using proximity card readers instead of the traditional key punch doors would help to mitigate:

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
In planning for a firewall implementation, Pete, a security administrator, needs a tool to help him understand what traffic patterns are normal on his network. Which of the following tools would help Pete determine traffic patterns?

A. Syslog
B. Protocol analyzer
C. Proxy server
D. Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
TKIP uses which of the following encryption ciphers?

A. RC5
B. AES
C. RC4
D. 3DES

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Jane, an administrator, needs to transfer DNS zone files from outside of the corporate network. Which of the following protocols must be used?

A. TCP
B. ICMP
C. UDP
D. IP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Common access cards use which of the following authentication models?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following application attacks is used to gain access to SEH?

A. Cookie stealing
B. Buffer overflow
C. Directory traversal
D. XML injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following does a second authentication requirement mitigate when accessing privileged areas of a website, such as password changes or user profile changes?

A. Cross-site scripting
B. Cookie stealing
C. Packet sniffing
D. Transitive access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Jane, a security technician, has been tasked with preventing contractor staff from logging into the company network after business hours. Which of the following BEST allows her to accomplish this?

A. Time of day restrictions
B. Access control list
C. Personal identity verification
D. Mandatory vacations

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 74
Which of the following ports does DNS operate on, by default?

A. 23
B. 53
C. 137
D. 443

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Sara from IT Governance wants to provide a mathematical probability of an earthquake using facts and figures. Which of the following concepts would achieve this?

A. Qualitative Analysis
B. Impact Analysis
C. Quantitative Analysis
D. SLE divided by the ARO

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A buffer overflow can result in which of the following attack types?

A. DNS poisoning
B. Zero-day
C. Privilege escalation
D. ARP poisoning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following is true concerning WEP security?

A. WEP keys are transmitted in plain text.

B. The WEP key initialization process is flawed.
C. The pre-shared WEP keys can be cracked with rainbow tables.
D. WEP uses the weak RC4 cipher.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following can be used on a smartphone to BEST protect against sensitive data loss if the device is stolen? (Select TWO).

A. Tethering
B. Screen lock PIN
C. Remote wipe
D. Email password
E. GPS tracking
F. Device encryption

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following can be implemented on a lost mobile device to help recover it?

A. Remote sanitization
B. GPS tracking
C. Voice encryption
D. Patch management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Sara, a security administrator, needs to implement the equivalent of a DMZ at the datacenter entrance. Which of the following must she implement?

A. Video surveillance
B. Mantrap
C. Access list
D. Alarm

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 81
Jane, a security analyst, is reviewing logs from hosts across the Internet which her company uses to gather data on new malware. Which of the following is being implemented by Jane's company?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Sara, a senior programmer for an application at a software development company, has also assumed an auditing role within the same company. She will be assessing the security of the application. Which of the following will she be performing?

A. Blue box testing
B. Gray box testing
C. Black box testing
D. White box testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Jane, a security analyst, wants to ensure that data is being stored encrypted, in the event that a corporate laptop is stolen. Which of the following encryption types will accomplish her goal?

A. IPSec
B. Secure socket layer
C. Whole disk
D. Transport layer security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following BEST describes a directory traversal attack?

A. A malicious user can insert a known pattern of symbols in a URL to access a file in another section of the directory.
B. A malicious user can change permissions or lock out user access from a webroot directory or subdirectories.
C. A malicious user can delete a file or directory in the webroot directory or subdirectories.
D. A malicious user can redirect a user to another website across the Internet.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Sara, the Chief Executive Officer (CEO) of a corporation, wishes to receive her corporate email and file attachments on her corporate mobile computing device. If the device is lost or stolen, the BEST security measure to ensure that sensitive information is not comprised would be:

A. to immediately file a police report and insurance report
B. the ability to remotely wipe the device to remove the data
C. to immediately issue a replacement device and restore data from the last backup
D. to turn on remote GPS tracking to find thedevice and track its movements

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
In her morning review of new vendor patches, a security administrator has identified an exploit that is marked as critical. Which of the following is the BEST course of action?

A. The security administrator should wait seven days before testing the patch to ensure that the vendor does not issue an updated version, which would require reapplying the patch.
B. The security administrator should download the patch and install it to her workstation to test whether it will be able to be applied to all workstations in the environment.
C. The security administrator should alert the risk management department to document the patch and add it to the next monthly patch deployment cycle.
D. The security administrator should download the patch to the test network, apply it to affected systems, and evaluate the results on the test systems.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following protocols allows for secure transfer of files? (Select TWO).

A. ICMP

B. SNMP
C. SFTP
D. SCP
E. TFTP

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Sara, a security administrator, is configuring a new firewall. She has entered statements into the firewall configuration as follows:

- Allow all Web traffic
- Deny all Telnet traffic
- Allow all SSH traffic

Mike, a user on the network, tries unsuccessfully to use RDP to connect to his work computer at home. Which of the following principles BEST explains why Mike's attempt to connect is not successful?

A. Explicit deny
B. Loop protection
C. Implicit deny
D. Implicit permit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Jane, a security administrator, notices that a program has crashed. Which of the following logs should Jane check?

A. Access log
B. Firewall log
C. Audit log
D. Application log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Users at a corporation are unable to login using the directory access server at certain times of the day. Which of the following concepts BEST describes this lack of access?

A. Mandatory access control

B. Least privilege
C. Time of day restrictions
D. Discretionary access control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following passwords is the LEAST complex?

A. MyTrain!45
B. Mytr@in!!
C. MyTr@in12
D. MyTr@in#8

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
During a penetration test from the Internet, Jane, the system administrator, was able to establish a connection to an internal router, but not successfully log in to it. Which ports and protocols are MOST likely to be open on the firewall? (Select FOUR).

A. 21
B. 22
C. 23
D. 69
E. 3389
F. SSH
G. Terminal services
H. Rlogin
I. Rsync
J. Telnet

Correct Answer: BCFJ
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
During an anonymous penetration test, Jane, a system administrator, was able to identify a shared print spool directory, and was able to download a document from the spool. Which statement BEST describes her privileges?

A. All users have write access to the directory.

B. Jane has read access to the file.
C. All users have read access to the file.
D. Jane has read access to the directory.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Sara, an IT security technician, has identified security weaknesses within her company's code. Which of the following is a common security coding issue?

A. Input validation
B. Application fuzzing
C. Black box testing
D. Vulnerability scanning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which of the following is an application security coding problem?

A. Error and exception handling
B. Patch management
C. Application hardening
D. Application fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Matt, an IT security technician, needs to create a way to recover lost or stolen company devices. Which of the following BEST meets this need?

A. Locking cabinets
B. GPS tracking
C. Safe
D. Firewalls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
An IT security technician needs to establish host based security for company workstations. Which of the following will BEST meet this requirement?

A. Implement IIS hardening by restricting service accounts.
B. Implement database hardening by applying vendor guidelines.
C. Implement perimeter firewall rules to restrict access.
D. Implement OS hardening by applying GPOs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Jane, an IT security technician, receives a call from the vulnerability assessment team informing her that port 1337 is open on a user's workstation. Which of the following BEST describes this type of malware?

A. Logic bomb
B. Spyware
C. Backdoor
D. Adware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following is the MOST specific plan for various problems that can arise within a system?

A. Business Continuity Plan
B. Continuity of Operation Plan
C. Disaster Recovery Plan
D. IT Contingency Plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?

A. Certification authority
B. Key escrow

C. Certificate revocation list
D. Registration authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Exam F

QUESTION 1
Which of the following is an authentication service that uses UDP as a transport medium?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following is a hardware-based security technology included in a computer?

A. Symmetric key
B. Asymmetric key
C. Whole disk encryption
D. Trusted platform module

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
An administrator might choose to implement a honeypot in order to:

A. Provide load balancing for network switches.
B. Distract potential intruders away from critical systems.
C. Establish a redundant server in case of a disaster.
D. Monitor any incoming connections from the Internet.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
In an enterprise environment, which of the following would be the BEST way to prevent users from accessing inappropriate websites when AUP requirements are constantly changing?

A. Deploy a network proxy server
B. Configure Internet content filters on each workstation
C. Deploy a NIDS
D. Deploy a HIPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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. Implement a password expiration policy.
B. Implement an account expiration date for permanent employees.
C. Implement time of day restrictions for all temporary employees.
D. Run a last logon script to look for inactive accounts.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:

A. logic bomb
B. backdoor
C. adware application
D. rootkit

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following protocols uses TCP instead of UDP and is incompatible with all previous versions?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

A. EAP-MD5
B. WEP
C. PEAP-MSCHAPv2
D. EAP-TLS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A security analyst needs to ensure all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended?

A. DMZ
B. Cloud computing
C. VLAN
D. Visualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Layer 7 devices used to prevent specific types of html tags are called:

A. firewalls.
B. content filters.
C. routers.
D. NIDS.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following allows a network administrator to implement an access control policy based on individual user characteristics and NOT on job function?

A. Attributes based
B. Implicit deny
C. Role based
D. Rule based

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following network architecture concepts is used to securely isolate at the boundary between networks?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified?

A. Security control frameworks
B. Best practice
C. Access control methodologies
D. Compliance activity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following devices is typically used to provide protection at the edge of the network attack surface?

A. Firewall
B. Router
C. Switch
D. VPN concentrator

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

A. ICMP
B. BGP
C. NetBIOS
D. DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks. Which of the following is MOST likely the reason for the sub-interfaces?

A. The network uses the subnet of 255.255.255.128.
B. The switch has several VLANs configured on it.
C. The sub-interfaces are configured for VoIP traffic.
D. The sub-interfaces each implement quality of service.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Digital Signatures provide which of the following?

A. Confidentiality
B. Authorization
C. Integrity
D. Authentication
E. Availability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
-- Exhibit --

-- Exhibit --

Use the exhibit button to show a video of an attack.

Which of the following BEST describes the type of attack that is occurring?

A. Smurf Attack
B. Man in the middle
C. Backdoor
D. Replay
E. Spear Phishing
F. Xmas Attack
G. Blue Jacking
H. Ping of Death

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following BEST describes a SQL Injection attack?

A. The attacker attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information.
B. The attacker attempts to have the receiving server run a payload using programming commonly found on web servers.
C. The attacker overwhelms a system or application, causing it to crash and bring the server down to cause an outage.
D. The attacker overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
An encryption method where the plain text and cipher text are always the same size is an example of which of the following types of encryption?

A. RC4
B. MD5
C. Steam Cipher
D. Block Cipher

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
The information security team does a presentation on social media and advises the participants not to provide too much personal information on social media web sites. This advice would BEST protect people from which

of the following?

A. Rainbow tables attacks
B. Brute force attacks
C. Birthday attacks
D. Cognitive passwords attacks

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
The compliance team comes out with a new policy that all data stored on tapes over 3 years must be degaussed. This BEST describes which of the following types of policies?

A. Data handling
B. Data classification
C. Data labeling
D. Data disposal

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Pete's corporation has outsourced help desk services to a large provider. Management has published a procedure that requires all users, when receiving support, to call a special number. Users then need to enter the code provided to them by the help desk technician prior to allowing the technician to work on their PC. Which of the following does this procedure prevent?

A. Collusion
B. Impersonation
C. Pharming
D. Transitive Access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Pete, the security engineer, would like to prevent wireless attacks on his network. Pete has implemented a security control to limit the connecting MAC addresses to a single port. Which of the following wireless attacks would this address?

A. Interference
B. Man-in-the-middle

C. ARP poisoning
D. Rogue access point

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following can be implemented with multiple bit strength?

A. AES
B. DES
C. SHA-1
D. MD5
E. MD4

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Jane, the security administrator, is having issues with unauthorized users connecting to the wireless network. For administrative reasons, she cannot implement any wireless encryption methods. Which of the following can she implement to prevent unauthorized users from connecting to the network?

A. NIPS
B. Disable unused ports
C. MAC filtering
D. WEP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Matt, the security administrator, wants to secure the wireless network. Which of the following encryption methods offers the MOST security?

A. WPA2 ENT AES
B. WPA2 PSK AES
C. WPA2 ENT TKIP
D. WPA2 PSK TKIP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Sara, the IT administrator, wants to control which devices can connect to the wireless network. Which of the following can she implement to accomplish this task?

A. WPA2 Enterprise with AES encryption
B. Decrease the WAP's power levels
C. Static IP addressing
D. MAC address filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Pete, the system administrator, has instituted a policy banning personal digital music and video players from the company premises. Which of the following would be the BEST reason for such a policy?

A. The company would be legally liable for any personal device that is lost on its premises.
B. It is difficult to verify ownership of offline device's digital rights management and ownership.
C. The media players may act as distractions during work hours and adversely affect user productivity.
D. If connected to a computer, unknown malware may be introduced into the environment.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide?

A. No competition with the company's official social presence
B. Protection against malware introduced by banner ads
C. Increased user productivity based upon fewer distractions
D. Elimination of risks caused by unauthorized P2P file sharing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Pete, the system administrator, is concerned about unauthorized access at all entrances into the building. PIN pad readers have been installed, but users have developed the habit of holding the door for others behind

them. Which of the following would BEST prevent this?

A. Install mantraps at every unmanned entrance.
B. Replace the PIN pad readers with card readers.
C. Implement video and audio surveillance equipment.
D. Require users to sign conduct policies forbidding these actions.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Pete, the system administrator, is reviewing his disaster recovery plans. He wishes to limit the downtime in the event of a disaster, but does not have the budget approval to implement or maintain an offsite location that ensures 99.99% availability. Which of the following would be Pete's BEST option?

A. Use hardware already at an offsite location and configure it to be quickly utilized.
B. Move the servers and data to another part of the company's main campus from the server room.
C. Retain data back-ups on the main campus and establish redundant servers in a virtual environment.
D. Move the data back-ups to the offsite location, but retain the hardware on the main campus for redundancy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Jane, a network administrator, has configured a 48-port switch to isolate four different departments. Which of the following has Jane MOST likely configured on the switch?

A. NAC
B. 802.1x
C. VLAN
D. DMZ

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A network stream needs to be encrypted. Sara, the network administrator, has selected a cipher which will encrypt 8 bits at a time before sending the data across the network. Which of the following has Sara selected?

A. Block cipher
B. Stream cipher
C. CRC
D. Hashing algorithm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Pete, a security auditor, has detected clear text passwords between the RADIUS server and the authenticator. Which of the following is configured in the RADIUS server and what technologies should the authentication protocol be changed to?

A. PAP, MSCHAPv2
B. CHAP, PAP
C. MSCHAPv2, NTLMv2
D. NTLM, NTLMv2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password?

A. Authentication server
B. Server certificate
C. Key length
D. EAP method

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?

A. Warm site
B. Load balancing
C. Clustering
D. RAID

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
How would a technician secure a router configuration if placed in an unsecured closet?

A. Mount the router into an immovable rack.
B. Enable SSH for maintenance of the router.
C. Disable the console port on the router.
D. Label the router with contact information.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following firewall rules would only block tftp traffic and record it?

A. deny udp any server log
B. deny udp any server eq 69
C. deny tcp any server log
D. deny udp any server eq 69 log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following services should be disabled to stop attackers from using a web server as a mail relay?

A. IMAP
B. SMTP
C. SNMP
D. POP3

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
A security administrator has a requirement to encrypt several directories that are non-hierarchical. Which of the following encryption models would BEST meet this requirement?

A. AES512
B. Database encryption
C. File encryption
D. Full disk encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are backdoors and logic bombs. Which of the following differentiates these two types of malware?

A. A backdoor is a coding issue that can be discovered by proper configuration management processes.
B. A logic bomb is typically hidden within the boot sector of the hard drive and is used to cause DDoS.
C. A backdoor is a third generation attack which is typically low risk because only highly trained staff can achieve it.
D. A logic bomb is undetectable by current antivirus signatures because a patch has not been issued.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are botnets and viruses. Which of the following explains the difference between these two types of malware?

A. Viruses are a subset of botnets which are used as part of SYN attacks.
B. Botnets are a subset of malware which are used as part of DDoS attacks.
C. Viruses are a class of malware which create hidden openings within an OS.
D. Botnets are used within DR to ensure network uptime and viruses are not.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following BEST explains the use of an HSM within the company servers?

A. Thumb drives present a significant threat which is mitigated by HSM.
B. Software encryption can perform multiple functions required by HSM.
C. Data loss by removable media can be prevented with DLP.
D. Hardware encryption is faster than software encryption.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following technologies can store multi-tenant data with different security requirements?

A. Data loss prevention
B. Trusted platform module
C. Hard drive encryption
D. Cloud computing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following technologies prevents USB drives from being recognized by company systems?

A. Registry keys
B. Full disk encryption
C. USB encryption
D. Data loss prevention

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Matt, a security analyst, needs to implement encryption for company data and also prevent theft of company data. Where and how should Matt meet this requirement?

A. Matt should implement access control lists and turn on EFS.
B. Matt should implement DLP and encrypt the company database.
C. Matt should install Truecrypt and encrypt the company server.
D. Matt should install TPMs and encrypt the company database.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following types of encryption will help in protecting files on a PED?

A. Mobile device encryption
B. Transport layer encryption
C. Encrypted hidden container
D. Database encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following is MOST closely associated with BitLocker?

A. ACL
B. DOS
C. DLP
D. TPM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following does full disk encryption prevent?

A. Client side attacks
B. Clear text access
C. Database theft
D. Network-based attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT?

A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.
B. Tell the application development manager to code the application to adhere to the company's password policy.
C. Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.
D. Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Sara, a security manager, has decided to force expiration of all company passwords by the close of business day. Which of the following BEST supports this reasoning?

A. A recent security breach in which passwords were cracked.
B. Implementation of configuration management processes.
C. Enforcement of password complexity requirements.
D. Implementation of account lockout procedures.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following presents the STRONGEST access control?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following encompasses application patch management?

A. Configuration management
B. Policy management
C. Cross-site request forgery
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Sara, an application developer, implemented error and exception handling alongside input validation. Which of the following does this help prevent?

A. Buffer overflow
B. Pop-up blockers
C. Cross-site scripting
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following is the LEAST volatile when performing incident response procedures?

A. Registers
B. RAID cache
C. RAM
D. Hard drive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following can allow Sara, a security analyst, to encrypt individual files on a system?

A. EFS
B. Single sign-on
C. TLS
D. Journaled file system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following BEST describes the weakness in WEP encryption?

A. The initialization vector of WEP uses a crack-able RC4 encryption algorithm. Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived.
B. The WEP key is stored in plain text and split in portions across 224 packets of random data. Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key.
C. The WEP key has a weak MD4 hashing algorithm used. A simple rainbow table can be used to generate key possibilities due to MD4 collisions.
D. The WEP key is stored with a very small pool of random numbers to make the cipher text. As the random numbers are often reused it becomes easy to derive the remaining WEP key.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following is used to ensure message integrity during a TLS transmission?

A. RIPEMD
B. RSA
C. AES
D. HMAC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years. Which of the following should Sara do to address the risk?

A. Accept the risk saving $10,000.
B. Ignore the risk saving $5,000.
C. Mitigate the risk saving $10,000.
D. Transfer the risk saving $5,000.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A company has asked Pete, a penetration tester, to test their corporate network. Pete was provided with all of the server names, configurations, and corporate IP addresses. Pete was then instructed to stay off of the Accounting subnet as well as the company web server in the DMZ.

Pete was told that social engineering was not in the test scope as well. Which of the following BEST describes this penetration test?

A. Gray box
B. Black box
C. White box
D. Blue box

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Topic 8, Volume H

QUESTION 62
Which of the following is an authentication and accounting service that uses TCP for connecting to routers and

switches?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

A. Input validation
B. Network intrusion detection system
C. Anomaly-based HIDS
D. Peer review

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection?

A. Sign in and sign out logs
B. Mantrap
C. Video surveillance
D. HVAC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

A. Water base sprinkler system
B. Electrical
C. HVAC
D. Video surveillance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Matt, a security consultant, has been tasked with increasing server fault tolerance and has been given no budget to accomplish his task. Which of the following can Matt implement to ensure servers will withstand hardware failure?

A. Hardware load balancing
B. RAID
C. A cold site
D. A host standby

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Pete has obtained a highly sensitive document and has placed it on a network drive which has been formatted with NTFS and is shared via CIFS. Which of the following access controls apply to the sensitive file on the server?

A. Discretionary
B. Rule based
C. Role based
D. Mandatory

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which of the following fire suppression systems is MOST likely used in a datacenter?

A. FM-200
B. Dry-pipe
C. Wet-pipe
D. Vacuum

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A security administrator has installed a new KDC for the corporate environment. Which of the following authentication protocols is the security administrator planning to implement across the organization?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following uses only a private key?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks?

A. Cross-site scripting
B. Buffer overflow
C. Header manipulation
D. Directory traversal

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Jane has recently implemented a new network design at her organization and wishes to passively identify security issues with the new network. Which of the following should Jane perform?

A. Vulnerability assessment
B. Black box testing
C. White box testing
D. Penetration testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
A database server containing personal information and a file server containing non-critical information must be secured. Which of the following would be a BEST practice to secure the servers? (Select TWO).

A. Place the file server behind a door requiring biometric authorization.
B. Place both servers under the system administrator's desk.
C. Place the database server behind a door with a cipher lock.
D. Place the file server in an unlocked rack cabinet.
E. Place the database server behind a door requiring biometric authorization.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A company is experiencing an extraordinary amount of web traffic that is crippling the server. The web traffic suddenly stops. The mail server experiences the same amount of traffic as before then crashes. Which of the following attacks would this BEST describe?

A. DoS
B. Spam
C. Man-in-the-middle
D. Replay

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following would ensure confidentiality and authorization to the management interface of a router?

A. Enable an access list and RADIUS
B. Enable SSH and TACACS
C. Enable an access list and PKI
D. Enable LDAP and strong passwords

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which of the following BEST describes a demilitarized zone?

A. A buffer zone between protected and unprotected networks.
B. A network where all servers exist and are monitored.
C. A sterile, isolated network segment with access lists.
D. A private network that is protected by a firewall and a VLAN.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
A security technician is attempting to explain why some of the company policies should be changed for high risk IT positions. Which of the following concepts BEST explains the support for fraud detection?

A. Time of day restrictions is more likely to discover fraud than the other fraud detection methods.
B. Least privilege principles allow internal audit teams to discover fraud while a staff member is out of the office.
C. Separation of duties is a better fraud detection method than mandatory vacations; therefore, it should be used.
D. Mandatory vacations support the company discovering fraud while staff members are out of the office.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
A security technician is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks the security technician to explain the access control type found in a firewall. With which of the following should the security technician respond?

A. Rule based access control
B. Role based access control
C. Discretionary access control
D. Mandatory access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Sara, a security administrator, has been tasked with explaining smart cards to the company's management team. Which of the following are smart cards? (Select TWO).

A. DAC
B. Tokens
C. CAC
D. ACL
E. PIV

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Jane, a security architect, is implementing security controls throughout her organization. Which of the following BEST explains the vulnerability in the formula that a Risk = Threat x Vulnerability x Impact?

A. Vulnerability is related to the risk that an event will take place.
B. Vulnerability is related to value of potential loss.
C. Vulnerability is related to the probability that a control will fail.
D. Vulnerability is related to the probability of the event.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
The information security department regularly walks the campus and around the buildings looking for unauthorized open wireless networks. This is an example of which of the following?

A. A site survey
B. Antenna placement
C. War dialing
D. War driving

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
The lobby of the hotel allows users to plug in their laptops to access the Internet. This network is also used for the IP based phones in the hotel lobby. Mike, the security engineer, wants to secure the phones so that guests cannot electronically eavesdrop on other guests. Which of the following would Mike MOST likely implement?

A. VLAN
B. Port security
C. MPLS
D. Separate voice gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Jane, the security engineer, is tasked with hardening routers. She would like to ensure that network access to the corporate router is allowed only to the IT group and from authorized machines. Which of the following would MOST likely be implemented to meet this security goal? (Select TWO).

A. SNMP
B. HTTPS
C. ACL
D. Disable console
E. SSH
F. TACACS+

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following can be used to discover if a security attack is occurring on a web server?

A. Creating a new baseline
B. Disable unused accounts
C. Implementing full disk encryption
D. Monitoring access logs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Jane, the CEO, receives an email wanting her to clink on a link to change her username and password. Which of the following attacks has she just received?

A. Hoaxes
B. Whaling
C. Bluejacking
D. Vishing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Pete, the system administrator, wishes to monitor and limit users' access to external websites.
Which of the following would BEST address this?

A. Block all traffic on port 80.
B. Implement NIDS.
C. Use server load balancers.
D. Install a proxy server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Sara, the security administrator, must configure the corporate firewall to allow all public IP addresses on the internal interface of the firewall to be translated to one public IP address on the external interface of the same firewall. Which of the following should Sara configure?

A. PAT
B. NAP
C. DNAT
D. NAC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following settings can Jane, the network administrator, implement in the computer lab to ensure that user credentials cannot be captured by the next computer user?

A. Implement full drive encryption on all lab computers.
B. Reverse the computer to its original state upon reboot.
C. Do not display last username in logon screen.
D. Deploy privacy screens on all lab computers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Jane, a security administrator, is reviewing the company's official documentation to mitigate the risk of data loss due to personally owned devices being connected to perform company related work. Which of the following documentation should Jane MOST likely review and update?

A. Acceptable risk
B. Data retention policy
C. Acceptable use policy
D. End user license agreement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service?

A. Succession planning
B. Disaster recovery plan
C. Information security plan
D. Business impact analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Pete, a security administrator, has implemented SSH across all network infrastructure devices in the enterprise. Which of the following protocols will be used to exchange keying material within SSH?

A. Transport layer protocol
B. IPSec
C. Diffie-Hellman
D. Secure socket layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability?

A. Twofish
B. Diffie-Hellman
C. ECC
D. RSA

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Sara, a security analyst, is trying to prove to management what costs they could incur if their customer database was breached. This database contains 250 records with PII. Studies show that the cost per record for a breach is $300. The likelihood that their database would be breached in the next year is only 5%. Which of the following is the ALE that Sara should report to management for a security breach?

A. $1,500
B. $3,750
C. $15,000
D. $75,000

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Matt must come up with a design solution which will enable remote users to securely access network resources. Which of the following design elements will enable Matt to meet this objective?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Sara, a security technician, has been asked to design a solution which will enable external users to have access to a Web server, while keeping the internal network unaffected by this access. Which of the following would BEST meet this objective?

A. Place the Web server on a VLAN
B. Place the Web server inside of the internal firewall
C. Place the Web server in a DMZ
D. Place the Web server on a VPN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?

A. TCP 23
B. UDP 69
C. TCP 22
D. TCP 21

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Matt, a security technician, notices a high number of ARP spoofing attacks on his network. Which of the following design elements would mitigate ARP spoofing attacks?

A. Flood guards
B. Implicit deny
C. VLANs
D. Loop protection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Matt works for an organization that requires data to be recovered in the shortest amount of time possible. Which of the following backup types would BEST meet the organization's needs?

A. Full backups daily
B. Differential backups monthly
C. Full backups weekly
D. Incremental backups monthly

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

A. Confidentiality
B. Availability

C. Succession planning
D. Integrity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
In the initial stages of an incident response, Matt, the security administrator, was provided the hard drives in question from the incident manager. Which of the following incident response procedures would he need to perform in order to begin the analysis? (Select TWO).

A. Take hashes
B. Begin the chain of custody paperwork
C. Take screen shots
D. Capture the system image
E. Decompile suspicious files

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

Exam G

QUESTION 1
Pete, the security administrator, wants to implement password controls to mitigate attacks based on password reuse. Which of the following password controls used together BEST accomplishes this? (Select TWO).

A. Minimum password age and password history
B. Password complexity and password history
C. Password history and password expiration
D. Password complexity and password expiration
E. Maximum password age and password expiration

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A company that trains their users to lock the doors behind them is MOST likely trying to prevent:

A. Vishing attacks
B. Dumpster diving
C. Shoulder surfing
D. Tailgating

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following security controls would be applied on individual hosts to monitor suspicious activities, by actively analyzing events occurring within that host, and blocking any suspicious or abnormal activity?

A. HIPS
B. Spam filter
C. HIDS
D. Firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Jane, a security administrator, forgets his card to access the server room. Jane asks Matt if she could use his card for the day. Which of the following is Jane using to gain access to the server room?

A. Man-in-the-middle

B. Tailgating
C. Impersonation
D. Spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
During a forensic investigation, which of the following information is compared to verify the contents of a hard drive image match the original drive and have not been changed by the imaging process?

A. Hash values
B. Chain of custody
C. Order of volatility
D. Time offset

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Jane brought a laptop in from home and connected the Ethernet interface on the laptop to a wall jack with a patch cable. Jane was unable to access any network resources. Which of the following is the MOST likely cause?

A. Flood guards were enabled on the switch.
B. Loop protection prevented the laptop from accessing the network.
C. Port security was enabled on the switch.
D. Router access control lists prevented the laptop from accessing the network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Topic 3, Volume C

QUESTION 7
Matt, a new employee, installed an application on his workstation that allowed Internet users to have access to his workstation. Which of the following security related training could have mitigated this action?

A. Use of proper password procedures
B. Use of personally owned devices
C. Use of social networking and P2P networks
D. Use of clean desk policies

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 8
Which of the following threats can result from a lack of controls for personal webmail?

A. Bandwidth exhaustion
B. Cross-site request forgery
C. Data leakage
D. Least privilege

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following is identified by the command: INSERT INTO users ("admin", "admin");'?

A. SQL Injection
B. Directory traversal
C. LDAP injection
D. Session hijacking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following attacks is MOST likely to be performed against an FTP server?

A. DLL injection
B. SQL injection
C. LDAP injection
D. Command injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
After performing a port scan, Sara, a network administrator, observes that port 443 is open. Which of the following services is MOST likely running?

A. SSL

B. FTP
C. TELNET
D. SSH

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Establishing a published chart of roles, responsibilities, and chain of command to be used during a disaster is an example of which of the following?

A. Fault tolerance
B. Succession planning
C. Business continuity testing
D. Recovery point objectives

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Matt, a security administrator, conducted a scan and generated a vulnerability report for the Chief Executive Officer (CEO). The vulnerability report indicated several vulnerabilities but the CEO has decided that cost and operational impact outweigh the risk. This is an example of which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A good password policy should contain which of the following rules? (Select THREE)

A. Length
B. Expiration
C. Tokens
D. Smart card
E. Enrollment
F. Complexity
G. Biometrics

Correct Answer: ABF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Jane, a security administrator, identifies a WEP-encrypted WAP on the network that is located at the end of the building. Jane has noticed that it is the most utilized WAP on the network. When trying to manage the WAP, she is unable to gain access. Which of the following has MOST likely happened to the WAP?

A. The WAP is under an IV attack
B. The WAP's MAC address has been spoofed
C. The WAP is a rogue access point
D. The WAP was victim to a bluejacking attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Jane, a human resources employee, receives an email from a family member stating there is a new virus going around. In order to remove the virus, a user must delete the Boot.ini file from the system immediately. This is an example of which of the following?

A. Hoax
B. Spam
C. Whaling
D. Phishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
A network IPS is used for which of the following?

A. To identify and document network based intrusions and network traffic
B. To document and analyze network visualization threats and performance
C. To identify and prevent network based intrusions or unwanted network traffic
D. To document and analyze malware and viruses on the Internet

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A risk is identified that an attacker, given the right credentials, could potentially connect to the corporate network from a nearby business's parking lot. Which of the following controls can be put in place to reduce the likelihood of this occurring? (Select TWO).

A. TKIP
B. Antenna placement
C. Power level controls
D. WPA
E. WPA2
F. Disable SSID broadcasting

Correct Answer: EF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following could cause a browser to display the message below? "The security certificate presented by this website was issued for a different website's address."

A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAs.
B. The website is using a wildcard certificate issued for the company's domain,
C. HTTPS://127.0.01 was used instead of HTTPS://localhost.
D. The website is using an expired self signed certificate.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Sara, an administrator, is hardening email application communication to improve security. Which of the following could be performed?

A. Remove gateway settings from the route table
B. Password protect the server BIOS
C. Disabling high I/O services
D. Require TLS when using SMTP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following increases proper airflow in a datacenter?

A. Humidity controls

B. Video monitoring
C. Temperature controls
D. Hot and cold aisles

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Jane, an IT security technician, needs to create a way to secure company mobile devices. Which of the following BEST meets this need?

A. Implement voice encryption, pop-up blockers, and host-based firewalls.
B. Implement firewalls, network access control, and strong passwords.
C. Implement screen locks, device encryption, and remote wipe capabilities.
D. Implement application patch management, antivirus, and locking cabinets.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
In which of the following orders should Jane, an administrator, capture a system's data for forensics investigation?

A. Hard disk, swap file, system memory, CPU cache
B. CPU cache, system memory, swap file, hard disk
C. System clock, flash BIOS, memory, hard disk
D. Flash BIOS, system memory, swap file, hard disk

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
In PKI, a key pair consists of:

A. A key ring
B. A public key
C. A private key
D. Key escrow
E. A passphrase

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following would MOST likely ensure that swap space on a hard disk is encrypted?

A. Database encryption
B. Full disk encryption
C. Folder and file encryption
D. Removable media encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following can be utilized in order to provide temporary IT support during a disaster, where the organization sets aside funds for contingencies, but does not necessarily have a dedicated site to restore those services?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following, when used on a file, creates a non-reversible numeric representation of the file's composition?

A. AES
B. SHA
C. 3DES
D. RC4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Banning of personally owned electronic devices at work BEST strengthens which of the following security principles?

A. Encourages hard drive encryption
B. Impedes shoulder surfing
C. Prevention of data leakage
D. Decreases workplace disruption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Implementation of routine file hash validation is an example of which of the following security concepts?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following is the BEST method for ensuring all files and folders are encrypted on all corporate laptops where the file structures are unknown?

A. Folder encryption
B. File encryption
C. Whole disk encryption
D. Steganography

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A company is installing a new security measure that would allow one person at a time to be authenticated to an area without human interaction. Which of the following does this describe?

A. Fencing
B. Mantrap
C. A guard
D. Video surveillance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following provides authentication, authorization, and accounting services?

A. PKI
B. WPA2
C. NTLMv2
D. RADIUS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following should be considered when implementing WPA vs. WPA2?

A. LEAP vs. PEAP
B. SSID vs. MAC
C. SHA1 vs. MD5
D. CCMP vs. TKIP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A popular software application is used on all company workstation desktop and laptop computers. Which of the following is the BEST patch management process?

A. The patch management software should be approved by the change management group to ensure adherence to corporate policies.
B. The Chief Information Officer should approve and centrally deploy the patch to all company workstations in a staggered manner.
C. Users should individually download and verify the patch with an MD5 checksum utility before applying it to their own workstation.
D. The support team should receive vendor update notifications and deploy patches in test environment before deploying to workstations.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following network protocols transmits a user's credentials in clear-text? (Select TWO).

A. SSH
B. HTTPS
C. SCP
D. Telnet
E. FTP
F. TFTP

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Data classification and labeling is an example of:

A. Preventative administrative control
B. Deterrent technical control
C. Preventative technical control
D. Deterrent administrative control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Jane, a security administrator, must be able to identify and validate every use of local administrative accounts across a large number of Windows and Linux servers. Which of the following offers the BEST solution?

A. Modify the system baseline to increase log retention and enable a host firewall
B. Monitor LDAP and Active Directory for the use of Administrative accounts
C. Add or enable a NIDS signature for administrative activity
D. Implement centralized log collection for each server and define a log review process

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following is MOST likely used to establish a secure connection between email gateways?

A. TLS
B. PGP
C. HTTPS
D. SCP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following describes how Pete, an employee, gains access to a location by entering with a fellow co-worker and not using his own credentials?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Sara, a security administrator, examines a network session to a compromised database server with a packet analyzer. Within the session there is a repeated series of the hex character 90 (x90).
Which of the following attack types has occurred?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
When employees that use certificates leave the company they should be added to which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42

Which of the following should Matt, a security technician, implement to identify untrusted certificates?

A. CA
B. PKI
C. CRL
D. Recovery agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Jane, a security analyst, noticed an increase in malware infections on a user's system. She identified an email that requests the user change her password. This attack would BEST be described as which of the following?

A. Phishing
B. Spoofing
C. Privilege escalation
D. Shoulder surfing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A corporate datacenter operates in a humid area near an ocean and often has hardware failures. Which of the following controls would help prevent these issues?

A. Fire suppression
B. HVAC
C. RAID
D. Cold aisles

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
When Pete, a security administrator, cannot verify who provided a hard drive image, then:

A. Chain of custody is preserved
B. The image must be rehashed
C. The hash must be verified
D. Chain of custody is destroyed

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
If Sara, an attacker, is attempting to determine the operating system using banner information, which of the following techniques could she be using?

A. Whois lookup
B. nslookup
C. Port scanning
D. Fingerprinting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Pete, an administrator, is creating a new security policy and must consider many stakeholders as well as current regulations, and the company direction. For the BEST success in policy roll out, which stakeholder is the MOST important for Pete to consider?

A. End users
B. Information security team
C. Senior leadership team
D. Customers and vendors

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following is an encapsulated authentication protocol?

A. CCMP
B. LEAP
C. TKIP
D. WEP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following is a layer three protocol used for VPN connections?

A. SSH
B. ICMP
C. IPSec
D. SSL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following can Matt, a security administrator, implement on a mobile device to help prevent a conversation from being picked up on another device?

A. Bluetooth
B. Screen locks
C. Strong passwords
D. Voice encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
When a username is checked against an access list, which of the following does it provide?

A. Identification and authentication
B. Identification and authorization
C. Authentication and authorization
D. Authentication and integrity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
A network device that protects an enterprise based only on source and destination addresses is BEST described as:

A. IDS
B. ACL
C. Stateful packet filtering
D. Simple packet filtering

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 53
Which of the following terms is used to describe predictable failure points for equipment or services?

A. RTO
B. MTTR
C. RPO
D. MTBF

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following account policies would Sara, a security administrator, implement to disable a user's account after a certain period of time?

A. Lockout
B. Expiration
C. Complexity
D. Recovery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Highly sensitive data is stored in a database and is accessed by an application on a DMZ server. The disk drives on all servers are fully encrypted. Communication between the application server and end-users is also encrypted. Network ACLs prevent any connections to the database server except from the application server. Which of the following can still result in exposure of the sensitive data in the database server?

A. SQL Injection
B. Theft of the physical database server
C. Cookies
D. Cross-site scripting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Matt, the security administrator, is implementing a new design to minimize the footprint in the datacenter and

reduce the amount of wasted resources without losing physical control of the equipment. Which of the following would Matt need to implement?

A. Visualization
B. Cloud computing
C. New ACLs
D. VLAN management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
A third party application has the ability to maintain its own user accounts or it may use single sign- on. To use single sign-on, the application is requesting the following information: OU=Users, DC=Domain, DC=COM. This application is requesting which of the following authentication services?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following can grant access based solely on TCP/IP information?

A. Time of day restrictions
B. Implicit deny
C. ACLs
D. Least privilege

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following should Sara, a technician, apply to prevent guests from plugging in their laptops and accessing the company network?

A. Secure router configuration
B. Port security
C. Sniffers
D. Implicit deny

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Pete, the Chief Security Officer (CSO), is concerned about misuse of company assets and wishes to determine who may be responsible. Which of the following would be the BEST course of action?

A. Create a single, shared user account for every system that is audited and logged based upon time of use.
B. Implement a single sign-on application on equipment with sensitive data and high-profile shares.
C. Enact a policy that employees must use their vacation time in a staggered schedule.
D. Separate employees into teams led by a person who acts as a single point of contact for observation purposes.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Jane, a user, has attempted to enter her username and password three times unsuccessfully. Jane receives a message to try again in one hour. This is an example of which of the following?

A. Account expiration
B. Account recovery
C. Account lockout
D. Account disablement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Sara, an attacker, tricks a user into authenticating to a fake wireless network and then inserts malicious code into strings as the user passes by. Which of the following describes this attack?

A. SQL injection
B. Malicious insider
C. Evil twin
D. User impersonation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following is a vulnerability associated with disabling pop-up blockers?

A. An alert message from the administrator may not be visible
B. A form submitted by the user may not open
C. The help window may not be displayed
D. Another browser instance may execute malicious code

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Due to limited resources, a company must reduce their hardware budget while still maintaining availability. Which of the following would MOST likely help them achieve their objectives?

A. Visualization
B. Remote access
C. Network access control
D. Blade servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Jane, a security administrator, has been tasked with explaining authentication services to the company's management team. The company runs an active directory infrastructure. Which of the following solutions BEST relates to the host authentication protocol within the company's environment?

A. Kerberos
B. Least privilege
C. TACACS+
D. LDAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following could be applied on a router in order to permit or deny certain ports?

A. Port security
B. Subnetting
C. Access control lists

D. Network address translation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following incident response procedures BEST allows Sara, the security technician, to identify who had possession of a hard drive prior to forensics analysis?

A. Chain of custody
B. Tracking man hours
C. Witnesses
D. Capturing system images

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Ticket-Granting-Tickets (TGTs) are common in which of the following authentication schemes?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Sara, a security administrator, implemented design changes which allowed for greater availability of IP addresses. Which of the following did Sara implement?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Jane, an IT security administrator, is attempting to implement PKI within her organization. Which of the following BEST explains why the company needs PKI?

A. The company needs PKI because the organization is based on trust models with many external organizations.
B. The company needs PKI because they need the ability to encrypt messages with centralized verification.
C. The company needs PKI because there is insufficient key escrow for outsourced SSL certificates.
D. The company needs PKI because it only has one recovery agent within the company.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following BEST prevents collusion?

A. Separation of duties
B. Signal sign-on
C. Mandatory vacations
D. Job rotation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following allows Pete, a security technician, to recover from a loss of staff after an earthquake?

A. Business continuity plan
B. Continuity of operations
C. Disaster recovery
D. Succession planning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Jane, an administrator, values transport security strength above network speed when implementing an SSL VPN. Which of the following encryption ciphers would BEST meet her needs?

A. SHA256
B. RC4
C. 3DES
D. AES128

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following is an authentication method that can be secured by using SSL?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following is a symmetrical key block cipher that encrypts MOST quickly?

A. 3DES
B. RSA
C. Blowfish
D. SHA256
E. Diffie-Hellman

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which of the following would BEST meet a server authentication requirement for a wireless network, but the network has no PKI in place?

A. PEAP
B. PAP
C. EAP-TLS
D. LEAP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77

Which of the following can be used to determine which services may be running on a host, but not if they are exploitable?

A. Baseline analyzer
B. Port scanner
C. Virus scanner
D. Vulnerability scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following, when incorporated into a disk encryption solution, adds the MOST security?

A. SHA256 hashing
B. Password complexity requirement
C. HMAC
D. Trusted platform module

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Upon inspecting sniffer traffic, Jane, a technician, observes an entry that originates from port TCP 53422 with a destination of TCP 22. Which of the following protocols is MOST likely in use?

A. HTTP
B. HTTPS
C. SSH
D. DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Role-based access control is BEST defined as an authorization system by which:

A. Privileges are granted to persons based on membership in one or more functional groups.
B. A separate user account is created for each functional role a person has.
C. Access is limited to the time of day a person is expected to work.
D. Privileges are assigned to each person based upon authorized requests.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following fire suppression systems should be used in a datacenter that will put out the fire and not cause physical harm to equipment and data?

A. Water
B. Halon
C. Oxygen
D. Foam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
In order to enter a corporate office, employees must enter a PIN. Which of the following are common risks when using this type of entry system? (Select TWO)

A. Shoulder surfing
B. Key logging
C. Tailgating
D. Man-in-the-middle attacks
E. Dumpster diving

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following is often used to verify connectivity on a network?

A. DNS
B. DHCP
C. ICMP
D. NAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following is BEST identified as an attack where a large number of users are fooled into entering

user credentials into a fake website?

A. Pharming
B. Whaling
C. Phishing
D. Privilege escalation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Sara, a student, is interested in learning about distributed denial of service attacks. Which of the following types of malware is MOST likely the primary focus of her study?

A. Botnets
B. Logic bombs
C. Spyware
D. Trojans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following BEST describes a DMZ?

A. A subnet that allows all outbound activity
B. A network that allows all inbound traffic
C. A transitional subnet that screens all traffic
D. A subnet that denies all inbound connectivity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Following the order of volatility, taking hashes, and maintaining a chain of custody describes which of the following?

A. Forensics
B. Incident response
C. Business continuity
D. Disaster recovery

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following is an example of a false negative?

A. The IDS does not identify a buffer overflow
B. Anti-virus identifies a benign application as malware.
C. Anti-virus protection interferes with the normal operation of an application.
D. A user account is locked out after the user mistypes the password too many times.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Sara and Jane, users, are reporting an increase in the amount of unwanted email that they are receiving each day. Which of the following would be the BEST way to respond to this issue without creating a lot of administrative overhead?

A. Deploy an anti-spam device to protect the network.
B. Update the anti-virus definitions and make sure that it is set to scan all received email
C. Set up spam filtering rules in each user's mail client.
D. Change the firewall settings to block SMTP relays so that the spam cannot get in.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following is similar to a smurf attack, but uses UDP instead to ICMP?

A. X-Mas attack
B. Fraggle attack
C. Vishing
D. Man-in-the-middle attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Pete, a security administrator, wants to secure remote telnet services and decides to use the services over SSH. Which of the following ports should Pete allow on the firewall by default?

A. 21
B. 22
C. 23
D. 25

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following accurately describes the STRONGEST multifactor authentication?

A. Something you are, something you have
B. Something you have, something you know
C. Something you are near to, something you have
D. Something you have, someone you know

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following is the BEST solution to securely administer remote servers?

A. SCP
B. SSH
C. Telnet
D. SFTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A company has sent all of its private keys to a third party. The third party company has created a secure list of these keys. Which of the following has just been implemented?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which of the following authentication protocols forces centralized wireless authentication?

A. WPA2-Personal
B. WPA2-Enterprise
C. WPA2-CCMP
D. WPA2-TKIP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
The fundamental information security principals include confidentiality, availability and which of the following?

A. The ability to secure data against unauthorized disclosure to external sources
B. The capacity of a system to resist unauthorized changes to stored information
C. The confidence with which a system can attest to the identity of a user
D. The characteristic of a system to provide uninterrupted service to authorized users

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which of the following risks could IT management be mitigating by removing an all-in-one device?

A. Continuity of operations
B. Input validation
C. Single point of failure
D. Single sign on

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Social networking sites are used daily by the marketing team for promotional purposes. However, confidential company information, including product pictures and potential partnerships, have been inadvertently exposed to the public by dozens of employees using social networking sites. Which of following is the BEST response to mitigate this threat with minimal company disruption?

A. Mandate additional security awareness training for all employees.

B. Report each employee to Human Resources for termination for violation of security policies
C. Implement a data loss prevention program to filter email.
D. Block access to social networking sites from the corporate network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A computer is put into a restricted VLAN until the computer's virus definitions are up-to-date. Which of the following BEST describes this system type?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Sara, an IT administrator, wants to protect a cluster of servers in a DMZ from zero day attacks. Which of the following would provide the BEST level of protection?

A. NIPS
B. NIDS
C. ACL
D. Antivirus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Exam H

QUESTION 1
Jane, the security administrator for a company, needs to assign permissions for users on her network. Which of the following would allow Jane to give ONLY the appropriate permissions necessary?

A. Separation of duties
B. Job rotation
C. Privilege escalation
D. Least privilege

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Users in the marketing department are given a different level of access to files than users in the accounting department. Which of the following types of access control does this BEST describe?

A. Standard access control
B. Role based access control
C. Mandatory access control
D. Discretionary access control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following types of data encryption would Jane, a security administrator, use if MBR and the file systems needed to be included?

A. Full disk
B. Individual files
C. Database
D. Partial disk

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Sara, an employee, enters the datacenter but does not ensure the door was fully closed afterwards. Which of the following could directly result from this situation?

A. Clean desk policy

B. Social engineering
C. Tailgating
D. Chain of custody

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following should Pete, the security administrator, change to help mitigate the risk associated with war drivers discovering the wireless network?

A. WPA encryption
B. WEP encryption
C. MAC filtering
D. AP power levels

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following is used to verify the identity of the sender of a signed email?

A. Public key
B. Sender's IP
C. From field
D. Private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following is the MOST important security requirement for mobile devices storing PII?

A. Remote data wipe
B. GPS location service
C. VPN pass-through
D. WPA2 wireless

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following is a way to confirm that all staff members know their roles and responsibilities during an IT disaster or other IT contingency event?

A. Table-top exercise
B. Hot site
C. Disaster recovery plan
D. MTTR

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
The main corporate website has a service level agreement that requires availability 100% of the time, even in the case of a disaster. Which of the following would be required to meet this demand?

A. Warm site implementation for the datacenter
B. Geographically disparate site redundant datacenter
C. Localized clustering of the datacenter
D. Cold site implementation for the datacenter

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency?

A. Business continuity planning
B. Continuity of operations
C. Business impact analysis
D. Succession planning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following will allow proper ventilation for servers in a data center?

A. Hot/cold aisles
B. Humidity controls
C. EMI shielding
D. Load balancing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following combinations represents multifactor authentication?

A. Key and proximity badge
B. Fingerprint and proximity badge
C. Retina scan and voice analysis
D. Password and PIN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Jane, an administrator, is primarily concerned with blocking external attackers from gaining information on remote employees by scanning their laptops. Which of the following security applications is BEST suited for this task?

A. Host IDS
B. Personal firewall
C. Anti-spam software
D. Anti-virus software

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following can Pete, the security administrator, implement to filter Internet traffic?

A. Warning banners
B. Spam filters
C. Host-based firewalls
D. Command shell restrictions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following should Jane, the security administrator, do FIRST when an employee reports the loss of a corporate mobile device?

A. Remotely lock the device with a PIN
B. Enable GPS location and record from the camera
C. Remotely uninstall all company software
D. Remotely initiate a device wipe

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following protocols is used to authenticate the client and server's digital certificate?

A. PEAP
B. DNS
C. TLS
D. ICMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following authentication services uses the AAA architecture and runs on TCP?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Users have notified Sara, a technician, that the performance of a specific set of servers has degraded. All of the

servers are in the same facility and accessible, but are very slow to respond.
Which of the following is MOST likely the cause?

A. The servers are not configured in a hot aisle and cool aisle containment.
B. Redundancy and data de-duplication has failed.
C. The UPS is overloaded and has begun the shutdown process.
D. HVAC has failed causing server CPUs to overheat and throttle.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Matt, an administrator, captures malicious DNS traffic on the network. Which of the following tools would be used to analyze the nature of this traffic?

A. Sniffer
B. Zone transfer
C. Network tap
D. Application firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following should Pete, an administrator, use to verify the integrity of a downloaded file?

A. CRL
B. CSR
C. AES
D. MD5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Pete, a security analyst, must authenticate himself and his company when obtaining a certificate. Which of the following would validate this information for Pete?

A. Certification authority
B. Key escrow
C. Registration authority
D. Trust model

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
How often, at a MINIMUM, should Sara, an administrator, review the accesses and right of the users on her system?

A. Annually
B. Immediately after an employee is terminated
C. Every five years
D. Every time they patch the server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Jane, a user, has reported an increase in email phishing attempts. Which of the following can be implemented to mitigate the attacks?

A. Anti-spyware
B. Anti-adware
C. Anti-virus
D. Anti-spam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following is a policy that would force all users to organize their areas as well as help in reducing the risk of possible data theft?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25

Which of the following is the BEST reason to have a formal and exercised incident management plan?

A. All vulnerabilities are mitigated
B. Users do not maintain excessive permissions
C. Patches are not made without testing
D. All parties understand their role in the process

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following identifies certificates that have been compromised or suspected of being compromised?

A. Certificate revocation list
B. Access control list
C. Key escrow registry
D. Certificate authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following time periods is a best practice for requiring user awareness training?

A. Every 5 years
B. Every 3 years
C. Every 2 years
D. Annually

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
In which of the following locations would Sara, a forensic analyst, look to find a hooked process?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A company notices that there is a flaw in one of their proprietary programs that the company runs in-house. The flaw could cause damage to the HVAC system. Which of the following would the company transfer to an insurance company?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following features would allow Pete, a network administrator, to allow or deny access to a specific list of network clients?

A. Content filtering
B. Flood guard
C. URL filtering
D. MAC filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Pete, a system administrator, is using a packet sniffer to troubleshoot remote authentication. Pete detects a device trying to communicate to UDP ports 1812 and 1813. Which of the following authentication methods is MOST likely being attempted?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following is an example of authentication using something Jane, a user, has and something she

knows?

A. GSM phone card and PIN
B. Username and password
C. Username and PIN
D. Fingerprint scan and signature

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following controls mitigates the risk of Matt, an attacker, gaining access to a company network by using a former employee's credential?

A. Account expiration
B. Password complexity
C. Account lockout
D. Dual factor authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following MUST Matt, a security administrator, implement to verify both the integrity and authenticity of a message while requiring a shared secret?

A. RIPEMD
B. MD5
C. SHA
D. HMAC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following does Jane, a software developer, need to do after compiling the source code of a program to attest the authorship of the binary?

A. Place Jane's name in the binary metadata
B. Use Jane's private key to sign the binary
C. Use Jane's public key to sign the binary
D. Append the source code to the binary

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
During the analysis of malicious code, Matt, a security analyst, discovers JavaScript being used to send random data to another service on the same system. This is MOST likely an example of which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Account lockout is a mitigation strategy used by Jane, the administrator, to combat which of the following attacks? (Select TWO).

A. Spoofing
B. Man-in-the-middle
C. Dictionary
D. Brute force
E. Privilege escalation

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A company's backup solution performs full backups weekly and is running into capacity issues. Without changing the frequency of backups, which of the following solutions would reduce the storage requirement?

A. Differential backups
B. Magnetic media backups
C. Load balancing
D. Incremental backups

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
3DES is created when which of the following scenarios occurs?

A. The DES algorithm is run three consecutive times against the item being encrypted.
B. The DES algorithm has been used by three parties: the receiving party, sending party, and server.
C. The DES algorithm has its key length increased to 256.
D. The DES algorithm is combined with AES and SHA1.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following mitigates the risk of proprietary information being compromised?

A. Cloud computing
B. Digital signatures
C. File encryption
D. Visualization

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following security tools can Jane, an administrator, implement to mitigate the risks of theft?

A. Visualization
B. Host based firewalls
C. HIPS
D. Device encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Matt, an attacker, drops a USB flash drive labeled "CEO's music collection" in the reception area of a bank hoping an employee will find it. The drive actually contains malicious code. Which of the following attacks is this?

A. Vishing
B. Social engineering
C. Spim
D. Impersonation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Sara, an employee, visits a website and downloads the PDF application to officially become a member. The network administrator notices large amounts of bandwidth at night from Sara's workstation. Which of the following attacks does this describe?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Matt, the Chief Information Security Officer (CISO), tells the network administrator that a security company has been hired to perform a penetration test against his network. The security company asks Matt which type of testing would be most beneficial for him. Which of the following BEST describes what the security company might do during a black box test?

A. The security company is provided with all network ranges, security devices in place, and logical maps of the network.
B. The security company is provided with no information about the corporate network or physical locations.
C. The security company is provided with limited information on the network, including all network diagrams.
D. The security company is provided with limited information on the network, including some subnet ranges and logical network diagrams.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
If Pete, an administrator, is blocking port 22, which of the following protocols will this affect? (Select TWO)

A. SNMP
B. SSH
C. SMTP
D. FTP
E. Telnet
F. SCP

Correct Answer: BF
Section: (none)

Explanation

Explanation/Reference:

QUESTION 46
Which of the following allows active exploitation of security vulnerabilities on a system or network for the purpose of determining true impact?

A. Port scanning
B. Penetration testing
C. Vulnerability scanning
D. Performing risk analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following web application security weaknesses can be mitigated by preventing the use of HTML tags?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A recent virus outbreak has finally been contained and now several users are reporting latency issues. A vulnerability scan was performed and no backdoors were found. Upon further investigation, Matt, the security administrator, notices that websites are being redirected to unauthorized sites. This is an example of which of the following?

A. Botnet
B. Rootkits
C. Trojan
D. Spyware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49

Which of the following is BEST used to control access to the LAN?

A. DMZ
B. NAC
C. NAT
D. Remote access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following is a technical preventive control?

A. IDS
B. Data backup
C. Audit logs
D. ACLs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
When deploying virtualized servers, which of the following should a company be the MOST concerned with?

A. Integrity
B. Non-repudiation
C. Power consumption
D. Availability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
The main difference between symmetric and asymmetric encryption is that:

A. Symmetric encryption uses the same key for encryption and decryption, while asymmetric encryption uses one key to encrypt and one to decrypt.
B. In symmetric encryption the encryption key must be of even number length so that it can be split in two, where one part is used for encryption and the other is used for decryption.
C. Asymmetric encryption uses the same key for encryption and decryption, while symmetric encryption uses one key to encrypt and one to decrypt.
D. In asymmetric encryption the same key is given to one user in a hashed format and used for encryption, and to another used in plain text and used for decryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Jane, an information security manager, often receives reports about the sharing of cipher lock codes to gain access to secure areas. Jane would like to implement a new control that would prevent the sharing of codes and limit access points to only key employees. Which of the following security controls would BEST mitigate this issue?

A. Use ACLs
B. Separation of duties
C. Install proximity readers
D. Time of day restrictions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Jane, a security administrator, has been tasked with explaining access control aspects to a peer. Which of the following is a directory service supporting both Windows and Linux authentication?

A. LDAP
B. Trusted OS
C. TACACS+
D. PAM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Pete, a system administrator, has concerns regarding his users accessing systems and secured areas using others' credentials. Which of the following can BEST address this concern?

A. Create conduct policies prohibiting sharing credentials.
B. Enforce a policy shortening the credential expiration timeframe.
C. Implement biometric readers on laptops and restricted areas.
D. Install security cameras in areas containing sensitive systems.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following is the MOST secure solution for connecting remote sites to the corporate headquarters?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following is the BEST method to use when preventing a cross-site scripting attack on a Human Resource system?

A. Require all data be filtered through a web application firewall.
B. Restrict permitted HTML encoding to a limited subset of tags and attributes.
C. Provide user education on the threat of cross-site scripting.
D. Input validation upon arrival at the server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Jane's, a user, word processing software is exhibiting strange behavior, opening and closing itself at random intervals. There is no other strange behavior on the system. Which of the following would mitigate this problem in the future?

A. Install application updates
B. Encrypt the file system
C. Install HIDS
D. Install anti-spam software

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Jane, a user, has an IP address of 172.16.24.43 and visits a website which states that she has an IP address of 204.211.38.89. Which of the following is being used on the network? (Select TWO).

A. NAT
B. NAC

C. Spoofing
D. DMZ
E. VLANs
F. PAT

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following data loss prevention strategies mitigates the risk of replacing hard drives that cannot be sanitized?

A. Visualization
B. Patch management
C. Full disk encryption
D. Database encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following is characterized by Matt, an attacker, attempting to leave identification markings for open wireless access points?

A. Initialization vector
B. War chalking
C. Packet sniffing
D. War driving

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following can Matt, a security administrator, implement to support confidentiality and integrity?

A. PKI
B. Non-repudiation
C. Digital signatures
D. Recovery agents

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following can Pete, an administrator, use to verify that a downloaded file was not corrupted during the transfer?

A. NTLM tag
B. LANMAN hash
C. MD5 checksum
D. SHA summary

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Planning what traffic will be separated, assigning tags, and configuring routing are part of configuring which of the following?

A. IPSec
B. ACL
C. NAT
D. VLAN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Jane, an employee, receives an error on an encrypted laptop, making the laptop un-bootable. Jane now cannot access any files on the laptop. The desktop technician is unable to recover the key from the computer and will have to inform Jane that the files are now unrecoverable. Which of the following would have prevented Jane from losing access to the files?

A. Certificate Authority
B. Private keys
C. Public keys
D. Key escrow

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following combines authentication and authorization, and does not use the TCP protocol?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following occurs when two access points share the same SSID broadcast where one access point is used to capture data?

A. Rogue access point
B. Bluesnarfing
C. Evil twin
D. Packet sniffing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Pete and Jane, users in a financial office are reporting that they are not being asked for credentials anymore when successfully connecting to the company wireless. All other offices are still being authenticated on the wireless. Which of the following is this an example of?

A. Evil twin
B. Interference
C. IV attack
D. War driving

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which of the following is BEST described by a scenario where management chooses to implement security controls to lessen the impact of a given risk?

A. Avoidance
B. Transference
C. Deterrence
D. Mitigation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
A recent network attack caused several random computers to malfunction, even though those computers had the latest updates and patches applied. Which of the following describes this type of attack?

A. Targeted
B. DDoS
C. Zero day
D. Buffer overflow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Sara, an employee, tethers her smartphone to her work PC to bypass the corporate web security gateway while connected to the LAN. While Sara is out at lunch her PC is compromised via the tethered connection and corporate data is stolen. Which of the following would BEST prevent this from occurring again?

A. Disable the wireless access and implement strict router ACLs
B. Reduce restrictions on the corporate web security gateway
C. Security policy and threat awareness training
D. Perform user rights and permissions reviews

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Sara makes a phone call to the help desk pretending to be Jane. Sara states that she has forgotten her password and asks that it be reset to 12345. Which of the following is Sara performing?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following default network ports is used by FTP?

A. 20
B. 22
C. 23
D. 25

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A company recently installed a load balancer for their servers. The company is MOST concerned with:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following pseudocodes MOST likely prevents buffer overflows?

A. If input contains < or > then escape the character and execute the program with user input
B. If input is less than 100 characters, then prompt for input again
C. If input contains \ then remove \ and execute program with user input
D. If input is greater than 1000 characters then truncate input

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which of the following is usually encrypted when stored or transmitted?

A. CRL
B. Private key
C. Root certificate
D. Public key

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 77
Which of the following could Jane, a security administrator, implement to mitigate the risk of tailgating for a large organization?

A. Train employees on correct data disposal techniques and enforce policies.
B. Only allow employees to enter or leave through one door at specified times of the day.
C. Only allow employees to go on break one at a time and post security guards 24/7 at each entrance.
D. Train employees on risks associated with social engineering attacks and enforce policies.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Pete, a security administrator, implemented design changes and moved certain servers into a dedicated area that is accessible from the outside network, yet separated from the internal network. Which of the following did Pete implement?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
While placing an order at an online bookstore, Sara, a user, enters her correct credentials and is immediately presented with a pop-up window requesting her username and password again.
Which of the following has MOST likely occurred?

A. LDAP injection attack
B. Evil twin attack
C. Phishing attack
D. SQL injection attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80

Identifying a list of all approved software on a system is a step in which of the following practices?

A. Passively testing security controls
B. Application hardening
C. Host software baselining
D. Client-side targeting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Pete, an administrator, captures traffic sent between a router and a monitoring server on port 161. The packet payload contains the strings 'PUBLIC and 'PRIVATE1. Which of the following was MOST likely used to capture this traffic?

A. Vulnerability scanner
B. Protocol analyzer
C. SNMPv3
D. SNMPv2c

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following is BEST utilized to identify common misconfigurations throughout the enterprise?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following malware types typically allows Pete, an attacker, to monitor a user's computer, is characterized by a drive-by download, and requires no user interaction?

A. Virus
B. Logic bomb
C. Spyware
D. Adware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following BEST describes a common security concern for cloud computing?

A. Data may be accessed by third parties who have compromised the cloud platform
B. Antivirus signatures are not compatible with virtualized environments
C. Network connections are too slow
D. CPU and memory resources may be consumed by other servers in the same cloud

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following is the MOST secure authentication protocol?

A. CHAP
B. PEAP
C. EAP
D. LEAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following policies could be implemented to help prevent users from displaying their login credentials in open view for everyone to see?

A. Privacy
B. Clean desk
C. Job rotation
D. Password complexity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following should Sara, a security technician, create to articulate the requirements for what is and what is not condoned on company systems?

A. Acceptable usage policy
B. Retention policy
C. Privacy policy
D. Access control policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Users have reported that when they go to the company website they are sent to a competitor's site instead. Which of the following is the MOST likely explanation?

A. Someone has employed ARP poisoning against the company.
B. Someone has employed DNS poisoning against the company.
C. Someone has accidentally unplugged the company's web server.
D. The competitor has a more powerful web server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Sara, an IT Administrator, wants to make sure that only certain devices can connect to the wireless network. Which of the following can she implement to accomplish this task?

A. MAC filtering
B. Increase the power levels of the WAP
C. Dynamic DHCP
D. Disable SSID broadcast

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following is BEST used to determine the source of a network bottleneck?

A. Sniffer
B. Router
C. Firewall
D. Switch

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 91
Sara, a system administrator, installed new database software and notices that after running port scan on the server port 21 is now open. The database does not use any type of file transfer program. Which of the following would reduce the amount of unnecessary services being used?

A. NIPS
B. Application hardening
C. NIDS
D. Application base lining

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Matt, the administrator, spots a sustained spike in disk activity and CPU utilization; network activity looks normal. Which of the following might this indicate?

A. This server is now a member of a botnet.
B. There is a virus infecting the server.
C. There is a smurf attack occurring on the server.
D. Users are copying more files from the server than normal.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Matt, the security administrator, has changed the default settings on a Web server, removing certain files and directories. This is an example of which of the following?

A. Application configuration baseline
B. Application hardening
C. Cross-site scripting prevention
D. Application patch management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Biometrics includes the use of which of the following authentication methods?

A. Single sign-on
B. Retinal scan
C. Common access card
D. ACLs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: