SY0-301_01-10-13_Anontester Brad

Number: SY0-301
Passing Score: 750
Time Limit: 90 min
File Version: 20.1

http://www.gratisexam.com/

Sections

1. Group 1
2. Group 2
3. Group 3
4. Group 4
5. Group 5
6. Group 6
7. Group 7
8. Group 8
9. Group 9
10. Group 10
11. Brad

ExamA

QUESTION 1
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: Group 1
Explanation

Explanation/Reference:
Explanation: Password history forces a user to not reuse a password for a specified duration.

QUESTION 2
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: Group 1
Explanation

Explanation/Reference:
Explanation: VPNs are specifically designed for remote access. Some firewalls have the ability to support remote access either by VPN or SSL.

QUESTION 3
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: Group 1
Explanation

Explanation/Reference:
Explanation: User permission reviews should be done periodically to ensure the concept of least privilege is being enforced.

QUESTION 4
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: Group 1
Explanation

Explanation/Reference:
Explanation: A hardware security module (HSM) is a device that manages digital keys and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card. Each module contains one or more secure cryptoprocessor chips to prevent tampering.

QUESTION 5
All of the following are valid cryptographic hash functions EXCEPT:

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

Correct Answer: B
Section: Group 1
Explanation

Explanation/Reference:
Explanation: RC4 is a symmetric stream cipher.

QUESTION 6
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: Group 1
Explanation

Explanation/Reference:
Explanation: IEEE's 802.1x is a standard for providing port-based network access control (NAC).

QUESTION 7
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: Group 1
Explanation

Explanation/Reference:
Explanation: Whaling is a social engineering attack targeted at upper management and executives.

QUESTION 8
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: Group 1
Explanation

Explanation/Reference:
Explanation: Host-based firewalls prevent externals devices from creating connections to the host unless explicitly allowed.

QUESTION 9
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: Group 1
Explanation

Explanation/Reference:
Explanation: When programs run each variable are allocated a fixed amount of memory. If the coder doesn't check to make sure the user isn't inputting more data than can be stored in the allocated memory a buffer overflow can occur.

QUESTION 10
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: Group 1
Explanation

Explanation/Reference:
Explanation: The operating system security settings should meet all your companies requirements as stated in the various security policies.

QUESTION 11
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: Group 1
Explanation

Explanation/Reference:
Explanation: It's important to audit a patch installation to ensure proper functioning of all the software.

QUESTION 12
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: Group 1
Explanation

Explanation/Reference:
Explanation: Trusted platform module (TPM) is a piece of hardware installed on most current PCs and allows for secure cryptographic key generation and storage.

QUESTION 13
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: Group 1
Explanation

Explanation/Reference:
Explanation: The three logs in the Windows OS are the Application, System, and Security. Login auditing is done in the Security log.

QUESTION 14
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: Group 1
Explanation

Explanation/Reference:
Explanation: Time of day restrictions allow you to specify days/times when individual users can access systems.

QUESTION 15
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: Group 1
Explanation

Explanation/Reference:
Explanation: The certificate revocation list (CRL) must be updated to show that the terminated employee's certificate is no longer valid.

QUESTION 16
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: Group 1
Explanation

Explanation/Reference:
Explanation: Of all the choices, fake cameras is the least expensive.

QUESTION 17
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. Smart card
B. Token

C. Discretionary access control
D. Mandatory access control

Correct Answer: A
Section: Group 1
Explanation

Explanation/Reference:
Explanation: Smart cards are a type of token but with added functionality.

QUESTION 18
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: Group 1
Explanation

Explanation/Reference:
Explanation: Firewalls separate the trusted and untrusted (or semi-trusted) zones so one of the interfaces would be in the DMZ.

QUESTION 19
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: Group 1
Explanation

Explanation/Reference:
Explanation: Because the connections are half open it would indicate it's a SYN flood.

QUESTION 20
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: Group 1
Explanation

Explanation/Reference:
Explanation: Protocol analyzer would allow Matt to see the actual bits in the payload.

QUESTION 21
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: Group 1
Explanation

Explanation/Reference:
Explanation: Fuzzing is a form of black-box testing where you send a lot of various inputs to a program to see if it crashes.

QUESTION 22
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: Group 1
Explanation

Explanation/Reference:
Explanation: Of the choices, brute force is the only valid one.

QUESTION 23
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: Group 1
Explanation

Explanation/Reference:
Explanation: A password cracker can be used to make sure users are choosing strong passwords.

QUESTION 24
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: Group 1
Explanation

Explanation/Reference:
Explanation: Certificates can be used in the form of digital signatures for both client authentication and code signing.

QUESTION 25
Which of the following is a hardware based encryption device?

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

Correct Answer: C
Section: Group 1
Explanation

Explanation/Reference:
Explanation: Trusted platform module (TPM) is a piece of hardware installed on most current PCs and allows for secure cryptographic key generation and storage.

QUESTION 26
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: Group 1
Explanation

Explanation/Reference:
Explanation: Web front-ends must validate user supplied data before passing it to the SQL server.

QUESTION 27
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: Group 1
Explanation

Explanation/Reference:
Explanation: Using cloud technologies inherently means you lose control over your data because it is stored on hardware you don't control.

QUESTION 28
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: Group 1
Explanation

Explanation/Reference:
Explanation: SSL encrypts the communication between the browser and web server which makes it unreadable as it transits the network.

QUESTION 29
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: Group 1
Explanation

Explanation/Reference:
Explanation: A certificate authority (CA) issues certificates after having them validated by the registration authority (RA).

QUESTION 30
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: Group 1
Explanation

Explanation/Reference:
Explanation: If the local system is compromised it will be able to read all the data on the smart card.

QUESTION 31
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: Group 2
Explanation

Explanation/Reference:
Explanation: Meant to prevent programmers from creating programs and then putting them on the network without an approval process.

QUESTION 32
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: Group 2
Explanation

Explanation/Reference:
Explanation: To prevent ad-hoc changes to the network which can create security issues all changes must be properly approved through the change management process.

QUESTION 33
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: Group 2
Explanation

Explanation/Reference:
Explanation: She's using the telephone which makes it vishing.

QUESTION 34
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: Group 2
Explanation

Explanation/Reference:
Explanation: Asymmetric encryption used public and private keys.

QUESTION 35
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: Group 2
Explanation

Explanation/Reference:
Explanation: Separation of duties is designed to prevent fraud and misuse of resources.

QUESTION 36
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: Group 2
Explanation

Explanation/Reference:
Explanation: Least privilege is the idea that each user should only be given the minimal amount of access to perform his/her task and no more.

QUESTION 37
A CRL is comprised of:

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

Correct Answer: D
Section: Group 2
Explanation

Explanation/Reference:
Explanation: A CRL is a list of public keys that became invalid before they expired.

QUESTION 38
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: Group 2
Explanation

Explanation/Reference:
Explanation: A trojan is a program that does one thing but also does something else unknown to the person running the program.

QUESTION 39
Which of the following may significantly reduce data loss if multiple drives fail at the same time?

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

Correct Answer: B
Section: Group 2
Explanation

Explanation/Reference:
Explanation: Redundant array of independent disks (RAID) is meant to provide redundancy for hard drives.

QUESTION 40
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: Group 2
Explanation

Explanation/Reference:
Explanation: Copper cabling radiates an electromagnetic field. Electromagnetic interference (EMI) shielding can prevent data leakage by reducing these emissions.

QUESTION 41
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: Group 2
Explanation

Explanation/Reference:
Explanation: Technical controls use technology to reduce vulnerabilities. An administrator installs/configures a technical control and the control provides protection automatically. Examples include: A/V software, firewalls, and intrusion detection systems

QUESTION 42
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: Group 2
Explanation

Explanation/Reference:
Explanation: SIP and RTP are both used as voice over IP (VOIP) protocols. Voice traffic is very delay sensitive both overall and between each packet. VOIP traffic should be segregated to its own VLAN so as to provide the proper quality of service and to prevent someone from eavesdropping on conversations.

QUESTION 43
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: Group 2
Explanation

Explanation/Reference:
Explanation: With the subnet mask 255.255.255.224, the IP address 10.4.4.125 is on the 10.4.4.96 network. The IP address 10.4.4.158 is on the 10.4.4.128 network. The IP address 10.4.4.199 is on the 10.4.4.192 network. The IP addresses 10.4.4.165 and 10.4.4.189 are both on the 10.4.4.160 network.

QUESTION 44
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: Group 2
Explanation

Explanation/Reference:
Explanation: Neither MD5 nor SHA were designed to be collision resistant.

QUESTION 45
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: Group 2
Explanation

Explanation/Reference:
Explanation: An isolated environment is need to limit the damage if the the malicious code escapes.

QUESTION 46
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: Group 2
Explanation

Explanation/Reference:
Explanation: Digital signatures provide authentication, non-repudiation, and integrity.

QUESTION 47
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: Group 2
Explanation

Explanation/Reference:
Explanation: Transport layer security (TLS) is the improved replacement for SSL. SSH is an application layer protocol.

QUESTION 48
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: Group 2
Explanation

Explanation/Reference:
Explanation: To prevent ad-hoc changes to the network which can create security issues all changes must be properly approved through the change management process.

QUESTION 49
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: Group 2
Explanation

Explanation/Reference:
Explanation: The annual loss expectancy (ALE): $200/hour x 48 hours = $9,600

QUESTION 50
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: Group 2
Explanation

Explanation/Reference:
Explanation: Audits should be conducted periodically to ensure all systems and personnel are complying with the company's security policies.

QUESTION 51
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: Group 2
Explanation

Explanation/Reference:
Explanation: TFTP utilizes UDP port 69 and FTP uses TCP port 21.

QUESTION 52
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: Group 2
Explanation

Explanation/Reference:
Explanation: AuthPriv allows MD5 or SHA authentication and also allows you to encrypt SNMP packets by using DES, 3DES, AES, or AES192.

QUESTION 53
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: Group 2
Explanation

Explanation/Reference:
Explanation: DES uses a 56-bit key. RC4 uses a 40-bit key. SHA2 doesn't use keys because it's a hashing algorithm.

QUESTION 54
Matt, an administrator, notices a flood of fragmented packets 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: Group 2
Explanation

Explanation/Reference:
Explanation: Protocol analyzer allows you to see the traffic as it exists on the network.

QUESTION 55
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: Group 2
Explanation

Explanation/Reference:
Explanation: IEEE's 802.1x is a standard for providing port-based network access control (NAC). 802.1q is IEEE's VLAN trunking protocol. 802.3 is IEEE's version of ethernet. 802.11n is IEEE's latest wireless LAN protocol.

QUESTION 56
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: Group 2
Explanation

Explanation/Reference:
Explanation: Whaling is a social engineering attack targeted at upper management and executives.

QUESTION 57
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: Group 2
Explanation

Explanation/Reference:
Explanation: Packet sniffing is collecting all the network traffic even though it may not be addressed to you.

QUESTION 58
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: Group 2
Explanation

Explanation/Reference:
Explanation: Antivirus software will not detect it if it's a zero-day. Host-based firewalls don't look at email attachments. It's a zero-day so the vendor hasn't developed a patch for it yet.

QUESTION 59
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: Group 2
Explanation

Explanation/Reference:
Explanation: Full disk encryption ensures the entire hard drive is encrypted.

QUESTION 60
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: Group 2
Explanation

Explanation/Reference:
Explanation: Mandatory access control has data labeled and users are given access to only a certain type of

label.

QUESTION 61
A username provides which of the following?

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

Correct Answer: B
Section: Group 3
Explanation

Explanation/Reference:
Explanation: A username uniquely identifies an individual. The password provides authentication.

QUESTION 62
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: Group 3
Explanation

Explanation/Reference:
Explanation: Each user should be given an individual username/password. Users should not be allowed to share a share a username/password because then you really don't know who is logging in.

QUESTION 63
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: Group 3
Explanation

Explanation/Reference:
Explanation: User permission reviews should be done periodically to ensure the concept of least privilege is being enforced.

QUESTION 64
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: Group 3
Explanation

Explanation/Reference:
Explanation: A false CA certificate undermines the the trustworthiness of PKI.

QUESTION 65
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: Group 3
Explanation

Explanation/Reference:
Explanation: IPSec modes: tunnel and transport; IPSec methods: certificates, shared secret, and encrypted nonces; IPSec security associations: A set of security information that describes a particular kind of secure connection between one device and another. You can consider it a "contract", if you will, that specifies the particular security mechanisms that are used for secure communications between the two.

QUESTION 66
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: Group 3
Explanation

Explanation/Reference:
Explanation: Penetration testing is considered an active approach to security testing.

QUESTION 67
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: Group 3
Explanation

Explanation/Reference:
Explanation: Vulnerability scanning is considered a passive approach to security testing. You are checking to see if machines are vulnerable not using an exploit to compromise them.

QUESTION 68
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: Group 3
Explanation

Explanation/Reference:
Explanation: Hot sites are part of an organization's business continuity plan and are meant to get them up and running again after some sort of disaster.

QUESTION 69
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: Group 3
Explanation

Explanation/Reference:
Explanation: Taking a hash of the original hard drive is a means of proving the authenticity of the evidence. Capturing the system image (bit for bit copy) allows you to forensically investigate the evidence using the copy without contaminating the original hard drive.

QUESTION 70
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: Group 3
Explanation

Explanation/Reference:
Explanation: Intermediate certificate authorities (CA) are trusted because their certificates are digitally signed by the root CA thereby creating a chain or path of trust.

QUESTION 71
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: Group 3
Explanation

Explanation/Reference:
Explanation: The root certificate authority (CA) is the foundation on which the chain or path of trust is based.

QUESTION 72
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: Group 3
Explanation

Explanation/Reference:
Explanation: If the internal memory and removable memory cards are not encrypted the attacker could use that plaintext to possibly acquire sensitive information perhaps even the decryption key which quite possibly could be stored in RAM.

QUESTION 73
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: Group 3
Explanation

Explanation/Reference:
Explanation: This is an example of parameter tampering in order to hijack an existing email session.

QUESTION 74
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: Group 3
Explanation

Explanation/Reference:
Explanation: A, B, and C are wrong because ECC is used only in asymmetric encryption.

QUESTION 75
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: Group 3
Explanation

Explanation/Reference:
Explanation: This is an example of using an if statement to test to see if a variable has numbers in it and if it does to exit the program.

QUESTION 76
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: Group 3
Explanation

Explanation/Reference:
Explanation: Honeynets are "pretend" networks set up to look like real networks in order to slow down hackers and/or learn the techniques and exploits they are using.

QUESTION 77
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: Group 3
Explanation

Explanation/Reference:
Explanation: A penetration tester must have an well-defined agreement with the customer so that if the penetration test crashes or corrupts a system causing downtime or data loss the customer has no legal standing to say that the downtime or data loss is the responsibility of the penetration tester.

QUESTION 78
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: Group 3
Explanation

Explanation/Reference:
Explanation: XTACACS, TACACS, and TACACS+ all use port 49. However, TACACS+ uses TCP while XTACACS and TACACS use UDP. RADIUS uses UDP port 1812 and 1813. Kerberos uses UDP port 88. LDAP uses TCP port 389.

QUESTION 79
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: Group 3
Explanation

Explanation/Reference:
Explanation: Since the admin wants to minimize the amount of time needed to perform backups during the week he will not do full backups during the week (full backups take the longest time) but instead do full backups on the weekend. The admin also doesn't mind the restoration process taking a long time so he will do incremental backups during the week (incremental backups typically take the most time to restore because of having to switch between several sets of tapes).

QUESTION 80
Which of the following can be used in code signing?

A. AES

B. RC4
C. GPG
D. CHAP

Correct Answer: C
Section: Group 3
Explanation

Explanation/Reference:
Explanation: Signing (digitial signature) requires the use of an asymmetric encryption. AES, RC4, and CHAP are all symmetric.

QUESTION 81
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: Group 3
Explanation

Explanation/Reference:
Explanation: SSL and WEP support the use of a stream cipher (RC4). CHAP, AES, 3DES are all based on block ciphers.

QUESTION 82
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: Group 3
Explanation

Explanation/Reference:
Explanation: Recovery point objective (RPO) defines the age of files that must be recovered from backup storage for normal operations to resume if a failure occurs. The RPO is expressed backward in time (that is, into the past) from the instant at which the failure occurs, and can be specified in seconds, minutes, hours, or days. It an important consideration in disaster recovery planning (DRP).

QUESTION 83
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: Group 3
Explanation

Explanation/Reference:
Explanation: The recovery time objective (RTO) is the maximum tolerable length of time that a system can be down after a failure occurs. The RTO is determined by the extent to which the interruption disrupts normal operations and the amount of revenue lost per unit time as a result of the failure. An RTO is measured in seconds, minutes, hours, or days and is an important consideration in disaster recovery planning (DRP).

QUESTION 84
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: Group 3
Explanation

Explanation/Reference:
Explanation: An automatic trust association between entities typically associated with MS Active Directory/ Kerberos.

QUESTION 85
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: Group 3
Explanation

Explanation/Reference:
Explanation: If an attacker can disable the datacenter's HVAC the equipment can overheat which can cause physical damage.

QUESTION 86
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: Group 3

Explanation

Explanation/Reference:
Explanation: Pre-defining who will take over if the existing responsible party is disabled or eliminated.

QUESTION 87
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: Group 3
Explanation

Explanation/Reference:
Explanation: IMAP uses TCP port 143.

QUESTION 88
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: Group 3
Explanation

Explanation/Reference:
Explanation: WPA2 uses AES with CCMP.

QUESTION 89
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: Group 3
Explanation

Explanation/Reference:
Explanation: Mandatory vacations would allow someone to possibly discover the collusion when the they began filling in for the person on vacation. Separation of duties does not apply because it's already being used. The two duties are being performed by two individuals but they are colluding. Separation of duties doesn't prevent collusion.

QUESTION 90
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: Group 3
Explanation

Explanation/Reference:
Explanation: Recovery agent is responsible for recovering an employee's private key when it is lost or no longer accessible because they don't work there anymore.

QUESTION 91
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: Group 10
Explanation

Explanation/Reference:
Explanation: Demilitarized zone (DMZ) is an area outside the company's internal network but inside the network perimeter.

QUESTION 92
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: Group 10
Explanation

Explanation/Reference:
Explanation: Creating applicable corporate security policies and managing users based on groups are both considered best practices.

QUESTION 93
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: Group 10
Explanation

Explanation/Reference:
Explanation: Firewalls sit at the perimeter of the network to control who has access to the internal network.

QUESTION 94
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: Group 10
Explanation

Explanation/Reference:
Explanation: The LMHOSTS file is used to map NetBIOS names (machine names) to IP addresses. Typically used when there is not a WINS server on the network and to provide a backup in case the WINS server is not available.

QUESTION 95
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: Group 10
Explanation

Explanation/Reference:
Explanation: A proxy server (such as squid) can be configured to allow internal machines to only connect to authorized websites.

QUESTION 96
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: Group 10
Explanation

Explanation/Reference:
Explanation: User permission reviews need to be done periodically to ensure the concept of least privilege is being enforced.

ExamB

QUESTION 1
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: Group 7
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
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: Group 7
Explanation

Explanation/Reference:
Explanation: Using group policy objects (GPO) you can set up a workstation object to have the security settings that need to be applied to all workstations and then simply add all the workstations to that GPO and they will all inherit the same security settings. Using GPOs allows you to do the configuration once.

QUESTION 3
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: Group 7
Explanation

Explanation/Reference:
Explanation: Optixpro is a backdoor which listens on port 1337.

QUESTION 4
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: Group 7
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
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: Group 7
Explanation

Explanation/Reference:
Explanation: A certificate authority (CA) issues certificates after having them validated by the registration authority (RA).

QUESTION 6
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: Group 7
Explanation

Explanation/Reference:
Explanation: WEP uses a 24-bit initialization vector (IV) which is too small. Once all the IVs are used up WEP starts reusing them, much like your odometer rolling over. This reuse is one of the things that weakens WEP.

QUESTION 7
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: Group 7
Explanation

Explanation/Reference:
Explanation: A hashed message authentication code (HMAC), sometimes called a keyed hash function, accepts as input a secret key and an arbitrary-length message to be authenticated, hashes it, and outputs a message authentication code (MAC). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

QUESTION 8
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: Group 7
Explanation

Explanation/Reference:
Explanation: The cost of doing nothing until the system was replaced would be $30,000 ($3,000/breach x 2 breaches/year x 5 years). Since the cost to repair the hole is only $25,000 Sara should have it repaired. She would be transferring the risk to the third party vendor thereby saving $5,000.

QUESTION 9
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: Group 7
Explanation

Explanation/Reference:
Explanation: Since Pete was provided all of the server names, configurations, and corporate IP addresses. This is a considerable amount of insider information so Pete is conducting a white box test.

QUESTION 10
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: Group 7
Explanation

Explanation/Reference:
Explanation: TACACS+ is a protocol for centralized authentication when connecting to routers and switches. As opposed to TACACS and XTACACS which use UDP, TACACS+ uses TCP.

QUESTION 11
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: Group 7
Explanation

Explanation/Reference:
Explanation: Checking user supplied input is the best way to prevent cross-site scripting attacks and buffer overflows.

QUESTION 12
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: Group 7
Explanation

Explanation/Reference:
Explanation: Mantraps are the effective solution of the the four choices.

QUESTION 13
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: Group 7

Explanation

Explanation/Reference:
Explanation: The HVAC should be shutdown if there's a fire so the smoke isn't spread throughout the building and the fire isn't fed oxygen.

QUESTION 14
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: Group 7
Explanation

Explanation/Reference:
Explanation: Redundant array of independent disks (RAID) is meant to provide redundancy for hard drives and if currently supported in hardware or software can be implemented with no cost.

QUESTION 15
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: Group 7
Explanation

Explanation/Reference:
Explanation: NTFS uses discretionary access control.

QUESTION 16
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: Group 7
Explanation

Explanation/Reference:
Explanation: FM-200 is a waterless fire protection system.

QUESTION 17
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: Group 7
Explanation

Explanation/Reference:
Explanation: Kerberos uses a key distribution center (KDC) as part of its infrastructure.

QUESTION 18
Which of the following uses only a private key?

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

Correct Answer: C
Section: Group 7
Explanation

Explanation/Reference:
Explanation: AES is a symmetric cipher so it uses a private key. RSA and ECC are asymmetric so they use both a private and public key. SHA is a hashing algorithm so it doesn't use a key.

QUESTION 19
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: Group 7
Explanation

Explanation/Reference:
Explanation: If a program crashes it's an indicator that a buffer overflow may have happened.

QUESTION 20
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: Group 7
Explanation

Explanation/Reference:
Explanation: Vulnerability assessments are considered a passive approach to security testing.

QUESTION 21
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: Group 7
Explanation

Explanation/Reference:
Explanation: Of the 3 factors of authentication, biometrics is considered the most secure. Placing both servers in a secure room that requires biometric authentication would be the best practice.

QUESTION 22
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: Group 7
Explanation

Explanation/Reference:
Explanation: A large amount of traffic directed at a single machine which results in it crashing is an indicator of a denial of service (DoS) attack.

QUESTION 23
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: Group 7
Explanation

Explanation/Reference:
Explanation: Time of day restrictions are used to restrict when a user can logon to the system.

QUESTION 24
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: Group 7
Explanation

Explanation/Reference:
Explanation: SSH provides confidentiality because the communication with the router is encrypted and TACACS provides centralized authentication.

QUESTION 25
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: Group 7
Explanation

Explanation/Reference:
Explanation: Demilitarized zone (DMZ) is an area outside the company's internal network but inside the network perimeter.

QUESTION 26
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: Group 7
Explanation

Explanation/Reference:
Explanation: Mandatory vacations would allow someone to possibly discover the fraud when the they began

filling in for the person on vacation. Separation of duties, time of day restrictions, least privilege are all a fraud prevention measures not fraud detection measures.

QUESTION 27
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: Group 7
Explanation

Explanation/Reference:
Explanation: Access control lists (ACLs) are an example of rule based access control.

QUESTION 28
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: Group 7
Explanation

Explanation/Reference:
Explanation: Common access cards (CAC) and personal identity verification (PIV) are examples of smart cards.

QUESTION 29
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: Group 7
Explanation

Explanation/Reference:
Explanation: Kerberos is the default authentication method used in a Windows active directory network.

QUESTION 30
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: Group 7
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
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: Group 8
Explanation

Explanation/Reference:
Explanation: War driving is walking or driving around an area looking wireless networks.

QUESTION 32
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: Group 8
Explanation

Explanation/Reference:
Explanation: Placing all the IP based phones in their own virtual LAN (VLAN) would segregate that traffic and prevent eavesdropping.

QUESTION 33
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: Group 8
Explanation

Explanation/Reference:
Explanation: TACACS+ provides centralized authentication to ensure only authorized users are allowed to login to the router. An access cotrol list (ACL) on the router can be used to only allow connections from authorized machines.

QUESTION 34
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: Group 8
Explanation

Explanation/Reference:
Explanation: Of the choices, only monitoring the access logs will tell you if an attack is occurring on a web server.

QUESTION 35
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: Group 8
Explanation

Explanation/Reference:
Explanation: Whaling is a social engineering attack targeted at upper management and executives.

QUESTION 36
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: Group 8
Explanation

Explanation/Reference:
Explanation: A proxy server (such as squid) can be configured to allow internal machines to only connect to authorized websites.

QUESTION 37
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: Group 8
Explanation

Explanation/Reference:
Explanation: Port address translation (PAT) is a specific type of network address translation (NAT) where you have more translated addresses (internal) then shared addresses (external) so port numbers are used to distinguish between the internal addresses that share a common external address.

QUESTION 38
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: Group 8
Explanation

Explanation/Reference:
Explanation: When a user goes to logon some OSes will automatically fill in the username field with the username of the last user to have logged out. This practice is not secure and so should be disabled.

QUESTION 39
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: Group 8
Explanation

Explanation/Reference:
Explanation: The acceptable use policy (AUP) should define what devices are allowed to be connected to the network.

QUESTION 40
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: Group 8
Explanation

Explanation/Reference:
Explanation: The disaster recovery plan (DRP) lists what order systems should be restored based on operational needs, most critical to least critical.

QUESTION 41
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: Group 8
Explanation

Explanation/Reference:
Explanation: Diffie-Hellman is key exchange protocol. It's a method to securely exchange a symmetric key across an insecure network.

QUESTION 42
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: Group 8
Explanation

Explanation/Reference:

Explanation: Elliptical curve cryptography allows for the same encryption strength with a smaller key than RSA. Twofish is a symmetric cipher. Diffie-Hellman is key exchange protocol.

QUESTION 43
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: Group 8
Explanation

Explanation/Reference:
Explanation: 250 records x $300/record x .05 = $3,750

QUESTION 44
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: Group 8
Explanation

Explanation/Reference:
Explanation: Virtual private networks (VPNs) are specifically designed for remote access.

QUESTION 45
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: Group 8
Explanation

Explanation/Reference:
Explanation: Demilitarized zone (DMZ) is an area outside the company's internal network but inside the network perimeter. A DMZ is where all publicly offered services should be kept.

QUESTION 46

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: Group 8
Explanation

Explanation/Reference:
Explanation: Secure shell (SSH) uses TCP port 22. Telnet uses TCP port 23 and is not secure. Trivial file transfer protocol (TFTP) uses UDP port 69 and is not secure. File transfer protocol (FTP) uses TCP port 21 (among others) and is not secure.

QUESTION 47
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: Group 8
Explanation

Explanation/Reference:
Explanation: Flood guards allow you to configure a limit on the number of packets a switch will process in a given time period.

QUESTION 48
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: Group 8
Explanation

Explanation/Reference:
Explanation: Since the admin wants to minimize the amount of time needed to restore from backups, full backups are best since typically it requires the fewest number of tapes.

QUESTION 49
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: Group 8
Explanation

Explanation/Reference:
Explanation: A set of servers that work together and in many respects appear as one server.

QUESTION 50
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: Group 8
Explanation

Explanation/Reference:
Explanation: Disabling the console port on the router could prevent unauthorized access.

QUESTION 51
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: Group 8
Explanation

Explanation/Reference:
Explanation: Trivial file transfer protocol (TFTP) uses UDP port 69 and the log option must be used to record it.

QUESTION 52
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: Group 8
Explanation

Explanation/Reference:
Explanation: The simple mail transfer protocol (SMTP) is used to send and receive email.

QUESTION 53
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: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
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: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
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: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
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: Group 8
Explanation

Explanation/Reference:
Explanation: A hardware security module (HSM) is a device that manages digital keys and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card. Each module contains one or more secure cryptoprocessor chips to prevent tampering.

QUESTION 57
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: Group 8
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
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: Group 8
Explanation

Explanation/Reference:
Explanation: Keys in the Windows registry can be set to disable the USB ports.

QUESTION 59
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: Group 8
Explanation

Explanation/Reference:
Explanation: Data loss prevention is meant to detect data breach and ex-filtration and prevent them by monitoring, detecting, and locking sensitive data while in-use, in motion, and at rest. Access control, encryption, and designated DLP systems are some of the measures used.

QUESTION 60
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: Group 8
Explanation

Explanation/Reference:
Explanation: Encryption can make a personal electronic device (PED) more secure.

QUESTION 61
Which of the following is MOST closely associated with BitLocker?

A. ACL
B. DOS
C. DLP
D. TPM

Correct Answer: D
Section: Group 9
Explanation

Explanation/Reference:
Explanation: Trusted platform module (TPM) is a piece of hardware installed on most current PCs and allows for secure cryptographic key generation and storage. Bitlocker is used for full disk encryption in Windows.

QUESTION 62
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: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 63
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: Group 9
Explanation

Explanation/Reference:
Explanation: It's important that employees comply with the company's security policies.

QUESTION 64
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: Group 9
Explanation

Explanation/Reference:
Explanation: Force expiring all company passwords is a serious step and should only be done in extreme circumstances like a security breach.

QUESTION 65
Which of the following presents the STRONGEST access control?

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

Correct Answer: A
Section: Group 9
Explanation

Explanation/Reference:
Explanation: Mandatory access control does not allow the user decide who gets access to the data. The data is labeled by strict guidelines and users are given access to only to data labeled with their access level..

QUESTION 66
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: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 67
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: Group 9
Explanation

Explanation/Reference:
Explanation: Buffer overflows are a result of not properly checking user supplied input.

QUESTION 68
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: Group 9
Explanation

Explanation/Reference:
Explanation: A hard drive is non-volatile memory while registers, RAID cache, and RAM are all volatile.

QUESTION 69
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: Group 9
Explanation

Explanation/Reference:
Explanation: Encrypting file system allows you to encrypt individual files and folders.

QUESTION 70

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: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 71
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: Group 9
Explanation

Explanation/Reference:
Explanation: An example of a cognitive password attack is when someone unwittingly reveals the answers to the identity verification questions used by many websites when you forget your password.

QUESTION 72
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: Group 9
Explanation

Explanation/Reference:
Explanation: Degaussing will remove the data.

QUESTION 73
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: Group 9
Explanation

Explanation/Reference:
Explanation: Without the code, it would be possible for an attacker to socially engineer an employee by pretending to be someone from the help desk provider.

QUESTION 74
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: Group 9
Explanation

Explanation/Reference:
Explanation: A rogue access point would not be able to be plugged into a network port until the MAC address had been authorized by Pete.

QUESTION 75
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: Group 9
Explanation

Explanation/Reference:
Explanation: AES allows for 128, 192 and 256 bit keys.

QUESTION 76
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: Group 9
Explanation

Explanation/Reference:
Explanation: MAC filtering allows the access point (AP) to only talk to authorized MAC addresses.

QUESTION 77
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: Group 9
Explanation

Explanation/Reference:
Explanation: WPA2 enterprise allows each user to get a unique key which enables truly secure communications. With pre-shared key (PSK) all the users have the same key which means anyone can decrypt any other user's traffic. AES is a stronger cipher than RC4 (TKIP uses the RC4 cipher).

QUESTION 78
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: Group 9
Explanation

Explanation/Reference:
Explanation: MAC filtering allows the access point (AP) to only talk to authorized MAC addresses.

QUESTION 79
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: Group 9
Explanation

Explanation/Reference:

Explanation:

QUESTION 80
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: Group 9
Explanation

Explanation/Reference:
Explanation: Ads received via websites may introduce malware via javasript or other technique.

QUESTION 81
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: Group 9
Explanation

Explanation/Reference:
Explanation: A small space having two interlocking doors such that the second door will not open until the first door closes.

QUESTION 82
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: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 83
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: Group 9
Explanation

Explanation/Reference:
Explanation: Virtual LANs (VLANs) allow you to separate networks (broadcast domains) on a switch.

QUESTION 84
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: Group 9
Explanation

Explanation/Reference:
Explanation: A block cipher encrypts more than 1 bit at a time, in this case 8 bits.

QUESTION 85
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: Group 9
Explanation

Explanation/Reference:
Explanation: The password authentication protocol (PAP) passes passwords unencrypted. Microsoft's challenge/handshake authentication protocol (MSCHAP) does not pass passwords unencrypted.

QUESTION 86
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: Group 9
Explanation

Explanation/Reference:
Explanation: The key length directly affects security.

QUESTION 87
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: Group 9
Explanation

Explanation/Reference:
Explanation: PEAP-MSCHAPv2 is the only one that does mutual authentication.

QUESTION 88
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. Virtualization

Correct Answer: A
Section: Group 9
Explanation

Explanation/Reference:
Explanation: Demilitarized zone (DMZ) is an area outside the company's internal network but inside the network perimeter. A DMZ is where all publicly offered services should be kept.

QUESTION 89
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: Group 9
Explanation

Explanation/Reference:

Explanation: Content filters look at the application data in the packets.

QUESTION 90
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: Group 9
Explanation

Explanation/Reference:
Explanation:

QUESTION 91
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: Group 10
Explanation

Explanation/Reference:
Explanation: Virtual LANs (VLANs) allow you to separate networks (broadcast domains) on a switch. Each network needs to have it's own default gateway because each is a different IP address block. Since the router has only one ethernet interface sub-interfaces are used to provide three virtual interfaces.

QUESTION 92
Digital Signatures provide which of the following?

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

Correct Answer: CD
Section: Group 10
Explanation

Explanation/Reference:
Explanation: Digital signatures provide authentication, non-repudiation, and integrity

QUESTION 93
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: Group 10
Explanation

Explanation/Reference:
Explanation:

QUESTION 94
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: Group 10
Explanation

Explanation/Reference:
Explanation: Inactive accounts should be investigated to determine if they are really needed anymore, if not they should be deleted.

QUESTION 95
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: Group 10
Explanation

Explanation/Reference:
Explanation: A backdoor can allow unauthorized access to data.

ExamC

QUESTION 1
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: Group 4
Explanation

Explanation/Reference:
Explanation: DNS information must be securely transferred between the primary and secondary DNS servers because it contains network information an attacker could find useful.

QUESTION 2
Matt, an IT administrator, wants to protect a newly built server from zero day attacks. Which of the following would provide the BEST level of protection?

A. HIPS
B. Antivirus
C. NIDS
D. ACL

Correct Answer: A
Section: Group 4
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
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: Group 4
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
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: Group 4
Explanation

Explanation/Reference:
Explanation: Phishing attacks use email as the attack vector.

QUESTION 5
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: Group 4
Explanation

Explanation/Reference:
Explanation: Having a strong password can prevent someone from guessing the password.

QUESTION 6
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: Group 4
Explanation

Explanation/Reference:
Explanation: Clean desk policy prevents someone from getting sensitive company information because it was left unsecured on a desk.

QUESTION 7
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: Group 4
Explanation

Explanation/Reference:

Explanation: Credit card and pin is something you have and something you know. Username and password is single factor authentication, password is something you know. Password and PIN is also single factor, both are something you know. Fingerprint and retina scan is also single factor, both are something you are.

QUESTION 8
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: Group 4
Explanation

Explanation/Reference:
Explanation: The web server is checking the user supplied input to make sure it's valid.

QUESTION 9
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: Group 4
Explanation

Explanation/Reference:
Explanation: Hashing the original hard drive will create a fingerprint of the data to be able to tell if it's been changed in the future. Imaging the drive lets you investigate the drive while preserving the original. Hashing the image will create a fingerprint of the data to be able to tell if it's the same as the original.

QUESTION 10
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: Group 4
Explanation

Explanation/Reference:
Explanation: Changing the configuration of a system, which includes installing additional software, affects the initial baseline configuration.

QUESTION 11
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: Group 4
Explanation

Explanation/Reference:
Explanation: Least privilege is the idea that each user should only be given the minimal amount of access to perform his/her task and no more.

QUESTION 12
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: Group 4
Explanation

Explanation/Reference:
Explanation: Employees are apparently giving the codes to unauthorized persons. Security awareness training should be conducted to remind the employees of the security policies and the implications for violating them.

QUESTION 13
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. Protocol analyzer
D. Spam filter

Correct Answer: C
Section: Group 4
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
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: Group 4
Explanation

Explanation/Reference:
Explanation: A spike in network traffic could indicate denial of service (DoS) attack and since the traffic is coming from many sources it means it's a distributed attack.

QUESTION 15
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: Group 4
Explanation

Explanation/Reference:
Explanation: War dialing is dialing telephone numbers to identify the ones that where a modem answers.

QUESTION 16
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: Group 4
Explanation

Explanation/Reference:
Explanation: Domain name system (DNS) poisoning is changing the mapping between a domain name and IP address to direct users from the original website to a website the attacker wants them to visit.

QUESTION 17
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: Group 4
Explanation

Explanation/Reference:
Explanation: Non-repudiation is not being able to deny you took some action.

QUESTION 18
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: Group 4
Explanation

Explanation/Reference:
Explanation: The internet control message protocol's (ICMP) echo message can be used to verify connectivity between two remote devices.

QUESTION 19
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: Group 4
Explanation

Explanation/Reference:
Explanation: Role based access control creates roles based on job function and the permissions needed to perform that job function are assigned to the role. Users are not assigned permissions directly but are assigned roles and then they assume the permissions assigned to that role.

QUESTION 20
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: Group 4
Explanation

Explanation/Reference:
Explanation: Host-based intrusion prevention systems (HIPS) run on individual systems and when they detect

an intrusion they take steps to prevent it.

QUESTION 21
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: Group 4
Explanation

Explanation/Reference:
Explanation: A false positive on a NIDS means it alerted when there was no attack. A false negative means it didn't alert when there was an attack. A true negative means it didn't alert when there was no attack. A true positive means it alerted when there was an attack.

QUESTION 22
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: Group 4
Explanation

Explanation/Reference:
Explanation: VPN gateways are specifically designed for remote access.

QUESTION 23
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: Group 4
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
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: Group 4
Explanation

Explanation/Reference:
Explanation: File transfer protocol (FTP) listens on TCP port 21.

QUESTION 25
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: Group 4
Explanation

Explanation/Reference:
Explanation:The URL typed in to the browser must match the common name in the certificate presented by the website.

QUESTION 26
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: Group 4
Explanation

Explanation/Reference:
Explanation: Keeping the servers running at the correct temperature requires a heating/ventilating/air conditioning system (HVAC).

QUESTION 27
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: Group 4
Explanation

Explanation/Reference:
Explanation: Program exceptions are when a program encounters something it doesn't expect or know how to handle.

QUESTION 28
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: Group 4
Explanation

Explanation/Reference:
Explanation: A signature-based network intrusion prevention system (NIPS) takes steps to prevent an attack when it matches a signature (it's known).

QUESTION 29
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: Group 4
Explanation

Explanation/Reference:
Explanation: FTP secure (FTPS) uses SSL. TFTP is not secure. SCP and SFTP use SSH to secure communications.

QUESTION 30
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: Group 5
Explanation

Explanation/Reference:
Explanation: You must be authorized to view data classified at a certain level and also you must justify your

need to view that data.

QUESTION 31
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: Group 5
Explanation

Explanation/Reference:
Explanation:Wired equivalent privacy (WEP) is no longer a secure protocol.

QUESTION 32
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's network
B. that the symbols indicate the presence of an 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: Group 5
Explanation

Explanation/Reference:
Explanation: War chalking is marking wireless networks so others will know they are there.

QUESTION 33
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: Group 5
Explanation

Explanation/Reference:
Explanation: VPNs are specifically designed for remote access and can be created with either by IPSec or SSL.

QUESTION 34
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: Group 5
Explanation

Explanation/Reference:
Explanation: Bluejacking is sending spam to a bluetooth device.

QUESTION 35
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: Group 5
Explanation

Explanation/Reference:
Explanation: SQL injections and buffer overflows are a result of not properly checking user supplied input.

QUESTION 36
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: Group 5
Explanation

Explanation/Reference:
Explanation: Without the key someone who steals the removable media will not be able to easily decrypt the data.

QUESTION 37
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: Group 5

Explanation

Explanation/Reference:
Explanation: Recovery agent is someone within the company who can recover private keys. Key escrow is when a third party has access to the private key.

QUESTION 38
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: Group 5
Explanation

Explanation/Reference:
Explanation: Certificates that are no longer valid but haven't expired need to be added the certificate revocation list (CRL).

QUESTION 39
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: Group 5
Explanation

Explanation/Reference:
Explanation: Continuity of operations is ensuring that if a disaster occurs the company will be able to continue to operate.

QUESTION 40
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: Group 5
Explanation

Explanation/Reference:
Explanation: An effective change management strategy ensures that updates do not bring down business critical systems or introduce vulnerabilities into the network.

QUESTION 41
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. Virtualization

Correct Answer: B
Section: Group 5
Explanation

Explanation/Reference:
Explanation: You split the task of cracking the hashes across many servers that are in a cluster.

QUESTION 42
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: Group 5
Explanation

Explanation/Reference:
Explanation: Imaging the drive lets you investigate the drive while preserving the original.

QUESTION 43
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: Group 5
Explanation

Explanation/Reference:
Explanation: The implicit deny rule denies all traffic unless it is explicitly allowed.

QUESTION 44
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: Group 5
Explanation

Explanation/Reference:
Explanation: Spoofing an address is pretending you're someone else.

QUESTION 45
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: Group 5
Explanation

Explanation/Reference:
Explanation: IPSec is a protocol used to create a virtual private network (VPN) used for remote access.

QUESTION 46
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: Group 5
Explanation

Explanation/Reference:
Explanation: Wifi protected access (WPA) is more secure than wired equivalent privacy (WEP).

QUESTION 47
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: Group 5
Explanation

Explanation/Reference:
Explanation: Management controls are typically administrative. Some of the areas they cover are policies and procedures, risk assessments, and vulnerability assessments.

QUESTION 48
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: Group 5
Explanation

Explanation/Reference:
Explanation: Mandatory vacations would allow someone to possibly discover the fraud when the they began filling in for the person on vacation.

QUESTION 49
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: Group 5
Explanation

Explanation/Reference:
Explanation: Chain of custody identifies who had control over a piece of evidence and when.

QUESTION 50
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: Group 5
Explanation

Explanation/Reference:
Explanation: Containment strategies focus on of stopping the spread of malware or damage from an infected system.

QUESTION 51
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: Group 5
Explanation

Explanation/Reference:
Explanation: The password and PIN are both something you know..

QUESTION 52
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: Group 5
Explanation

Explanation/Reference:
Explanation: Network access control allows only authorized systems to connect to the network.

QUESTION 53
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: Group 5
Explanation

Explanation/Reference:
Explanation: The hot/cold aisle approach allows for the proper cooling of equipment in the data center.

QUESTION 54
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: Group 5
Explanation

Explanation/Reference:
Explanation: Directory traversal is a form of command injection where an user is trying to execute commands outside of the web root directory.

QUESTION 55
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: Group 5
Explanation

Explanation/Reference:
Explanation: Secure shell (SSH) uses TCP port 22.

QUESTION 56
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: Group 5
Explanation

Explanation/Reference:
Explanation: Only IPSec and SSH supports tunneling.

QUESTION 57
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: Group 5
Explanation

Explanation/Reference:
Explanation: An XMAS scan will have at least the FIN, URG, and PSH bits (FUP) set in the TCP header.

QUESTION 58

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: Group 5
Explanation

Explanation/Reference:
Explanation: Network address translation (NAT) replaces an IP address with another.

QUESTION 59
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: Group 5
Explanation

Explanation/Reference:
Explanation: Proximity card readers don't use PINs so without a PIN no one can look over your shoulder and see you type in the PIN.

QUESTION 60
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: Group 6
Explanation

Explanation/Reference:
Explanation: Protocol analyzer would allow someone to see/collect all the traffic on the network.

QUESTION 61
TKIP uses which of the following encryption ciphers?

A. RC5
B. AES
C. RC4
D. 3DES

Correct Answer: C
Section: Group 6
Explanation

Explanation/Reference:
Explanation: Temporal key integrity protocol (TKIP) uses the RC4 stream cipher.

QUESTION 62
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: Group 6
Explanation

Explanation/Reference:
Explanation: DNS zone transfers between the primary and secondary DNS servers is done with TCP.

QUESTION 63
Common access cards use which of the following authentication models?

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

Correct Answer: A
Section: Group 6
Explanation

Explanation/Reference:
Explanation: CACs use certificates that are part of a public key infrastructure (PKI).

QUESTION 64
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: Group 6
Explanation

Explanation/Reference:
Explanation: Structured exception handling (SEH) is a mechanism for handling both hardware and software exceptions. A buffer overflow could create an exception.

QUESTION 65

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: Group 6
Explanation

Explanation/Reference:
Explanation: If an attacker stole a cookie he would still need the second authentication method.

QUESTION 66
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: Group 6
Explanation

Explanation/Reference:
Explanation: Time of day restrictions are used to restrict when a user can logon to the system.

QUESTION 67
Which of the following ports does DNS operate on, by default?

A. 23
B. 53
C. 137
D. 443

Correct Answer: B
Section: Group 6
Explanation

Explanation/Reference:
Explanation: DNS operates on TCP/UDP port 53. Zone transfers use TCP port 53 and lookup requests use UDP port 53.

QUESTION 68
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: Group 6
Explanation

Explanation/Reference:
Explanation: Using actual facts and figures would be quantitative analysis.

QUESTION 69
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: Group 6
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
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: Group 6
Explanation

Explanation/Reference:
Explanation: RADIUS uses UDP. TACACS+, LDAP, and Kerberos all use TCP.

QUESTION 71
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: Group 6
Explanation

Explanation/Reference:
Explanation: The wired equivalent privacy (WEP) protocol initialization process is broke because the initialization vector is too small.

QUESTION 72
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: Group 6
Explanation

Explanation/Reference:
Explanation:

QUESTION 73
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: Group 6
Explanation

Explanation/Reference:
Explanation:

QUESTION 74
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: Group 6
Explanation

Explanation/Reference:
Explanation: A small space having two interlocking doors such that the second door will not open until the first door closes.

QUESTION 75
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: Group 6
Explanation

Explanation/Reference:
Explanation: Honeynets are "pretend" networks set up to look like real networks in order to slow down hackers and/or learn the techniques and exploits they are using.

QUESTION 76
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: Group 6
Explanation

Explanation/Reference:
Explanation: Since the auditor is an insider it would be a white box test.

QUESTION 77
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: Group 6
Explanation

Explanation/Reference:
Explanation: Whole disk encryption is the best way to ensure that all the data on a hard drive is protected.

QUESTION 78
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: Group 6
Explanation

Explanation/Reference:
Explanation: Directory traversal is a form of command injection where an user is trying to execute commands outside of the web root directory.

QUESTION 79
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 the device and track its movements

Correct Answer: B
Section: Group 6
Explanation

Explanation/Reference:
Explanation: Remote wiping allows you to delete all the data on the device despite not having physical access to it.

QUESTION 80
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: Group 6
Explanation

Explanation/Reference:
Explanation: In a corporate environment patches typically need to be tested prior to deploying them to systems to make sure the patch isn't going to create additional problems. Since it's a critical patch this needs to be done asap.

QUESTION 81
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: Group 6
Explanation

Explanation/Reference:
Explanation: SSH FTP (SFTP) and secure copy (SCP) both use SSH for secure communication.

QUESTION 82
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: Group 6
Explanation

Explanation/Reference:
Explanation: Firewalls use the implicit deny approach so unless it is explicitly allowed (in this case only web and SSH traffic is allowed) it will be blocked.

QUESTION 83
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: Group 6
Explanation

Explanation/Reference:
Explanation: Program errors are logged to the Windows application log.

QUESTION 84
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: Group 6
Explanation

Explanation/Reference:
Explanation: Time of day restrictions are used to restrict when a user can logon to the system.

QUESTION 85
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: Group 6
Explanation

Explanation/Reference:
Explanation: Mytr@in!! only has uppercase letters, lowercase letters, and special characters. The others are all more complex because they have uppercase letters, lowercase letters, special characters, and numbers.

QUESTION 86
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: Group 6
Explanation

Explanation/Reference:
Explanation: The most common protocols used for remote router access are telnet and SSH. Telnet uses TCP port 23 and SSH uses TCP port 22.

QUESTION 87
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: Group 6
Explanation

Explanation/Reference:
Explanation: All users must have read access if Jane was able to download it.

QUESTION 88
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: Group 6
Explanation

Explanation/Reference:
Explanation:Not checking the user supplied input to make sure it's valid is a common security coding issue.

QUESTION 89
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: Group 6
Explanation

Explanation/Reference:
Explanation:

QUESTION 90
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: Group 10
Explanation

Explanation/Reference:
Explanation: Trusted platform module (TPM) is a piece of hardware installed on most current PCs and allows for secure cryptographic key generation and storage.

QUESTION 91

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: Group 10
Explanation

Explanation/Reference:
Explanation: A content filter is able to look at the application data in order to make decisions about whether the traffic should be allowed. In this case it's able to look into the HTTP message ans allow/deny traffic based on the URL requested.

QUESTION 92
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 an access log and a security guard
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: Group 10
Explanation

Explanation/Reference:
Explanation: A cipher lock could be used and each person can be given a unique access code. The system would be able to track the people who access the server room by the access code used to gain entry.

QUESTION 93
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: Group 10
Explanation

Explanation/Reference:
Explanation: A honeypot could be used as bait to get attackers to target it instead of the critical systems. This would give the administrators time to react to the attack.

QUESTION 94
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: Group 10
Explanation

Explanation/Reference:
Explanation:

QUESTION 95
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: Group 10
Explanation

Explanation/Reference:
Explanation: Blowfish, AES, and 3DES are block ciphers. RC4 is a stream cipher. MD5 is a hashing algorithm. PGP is asymmetric.

ExamD

QUESTION 1
Actively monitoring data streams in search of malicious code or behavior is an example of:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following network devices would MOST likely be used to detect but not react to suspicious behavior on the network?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
The security administrator is getting reports from users that they are accessing certain websites and are unable to download anything off of those sites. The security administrator is also receiving several alarms from the IDS about suspicious traffic on the network. Which of the following is the MOST likely cause?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following tools provides the ability to determine if an application is transmitting a password in clear-text?

A. Protocol analyzer

B. Port scanner
C. Vulnerability scanner
D. Honeypot

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following can a security administrator implement to help identify smurf attacks?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following wireless security controls can be easily and quickly circumvented using only a network sniffer? (Select TWO).

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following functions is MOST likely performed by a web security gateway?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

http://www.gratisexam.com/

QUESTION 8
Which of the following devices is often used to cache and filter content?

A. Proxies
B. Firewall
C. VPN
D. Load balancer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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 10
Which of the following devices is used to optimize and distribute data workloads across multiple computers or networks?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
An IT administrator wants to provide 250 staff with secure remote access to the corporate network. Which of the following BEST achieves this requirement?

A. Software based firewall
B. Mandatory Access Control (MAC)
C. VPN concentrator
D. Web security gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following should be installed to prevent employees from receiving unsolicited emails?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following should a security administrator implement to prevent users from disrupting network connectivity, if a user connects both ends of a network cable to different switch ports?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A user is no longer able to transfer files to the FTP server. The security administrator has verified the ports are open on the network firewall. Which of the following should the security administrator check?

A. Anti-virus software

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following BEST describes the proper method and reason to implement port security?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following would need to be configured correctly to allow remote access to the network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
By default, which of the following stops network traffic when the traffic is not identified in the firewall rule set?

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 18
Based on logs from file servers, remote access systems, and IDS, a malicious insider was stealing data using a personal laptop while connected by VPN. The affected company wants access to the laptop to determine loss, but the insider's lawyer insists the laptop cannot be identified. Which of the following would BEST be used to identify the specific computer used by the insider?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Applying detailed instructions to manage the flow of network traffic at the edge of the network including allowing or denying traffic based on port, protocol, address, or direction is an implementation of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following is the default rule found in a corporate firewall's access control list?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following is BEST used to prevent ARP poisoning attacks across a network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A small company needs to invest in a new expensive database. The company's budget does not include the purchase of additional servers or personnel. Which of the following solutions would allow the small company to save money on hiring additional personnel and minimize the footprint in their current data center?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following is MOST likely to be the last rule contained on any firewall?

A. IP allow any any
B. Implicit deny
C. Separation of duties
D. Time of day restrictions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following cloud computing concepts is BEST described as providing an easy-to-configure OS and on-demand computing for customers?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
MAC filtering is a form of which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Reviewing an access control list on a firewall reveals a Drop All statement at the end of the rules. Which of the following describes this form of access control?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
An administrator is taking an image of a server and converting it to a virtual instance. Which of the following BEST describes the information security requirements of a virtualized server?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Webmail is classified under which of the following cloud-based technologies?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A security engineer is troubleshooting a server in the DMZ, which cannot be reached from the Internet or the internal network. All other servers on the DMZ are able to communicate with this server. Which of the following is the MOST likely cause?

A. The server is configured to reject ICMP packets.
B. The server is on the external zone and it is configured for DNS only.
C. The server is missing the default gateway.
D. The server is on the internal zone and it is configured for DHCP only.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following may cause a user, connected to a NAC-enabled network, to not be prompted for credentials?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following would be implemented to allow access to services while segmenting access to the internal network?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
A security administrator needs to separate two departments. Which of the following would the administrator implement to perform this?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is a security control that is lost when using cloud computing?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following protocols should be blocked at the network perimeter to prevent host enumeration by sweep devices?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following uses TCP port 22 by default?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following allows a security administrator to set device traps?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A security administrator needs to implement a site-to-site VPN tunnel between the main office and a remote branch. Which of the following protocols should be used for the tunnel?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following protocols would be the MOST secure method to transfer files from a host machine?

A. SFTP
B. WEP
C. TFTP
D. FTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following port numbers is used for SCP, by default?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following is the MOST secure method of utilizing FTP?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following protocols can be implemented to monitor network devices?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following protocols would an administrator MOST likely use to monitor the parameters of network devices?

A. SNMP
B. NetBIOS
C. ICMP

D. SMTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A remote office is reporting they are unable to access any of the network resources from the main office. The security administrator realizes the error and corrects it. The administrator then tries to ping the router at the remote office and receives no reply; however, the technician is able to telnet to that router. Which of the following is the MOST likely cause of the security administrator being unable to ping the router?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A network administrator is implementing a network addressing scheme that uses a long string of both numbers and alphanumeric characters to create addressing options and avoid duplicates. Which of the following describes a protocol built for this purpose?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
In which of the following locations would a forensic analyst look to find a hooked process?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following file transfer protocols is an extension of SSH?

A. FTP
B. TFTP
C. SFTP
D. FTPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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 48
The security administrator notices a number of TCP connections from the development department to the test network segregation. Large volumes of data are being transmitted between the two networks only on port 22. Which of the following is MOST likely occurring?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
An administrator who wishes to block all database ports at the firewall should include which of the following ports in the block list?

A. 445

B. 433
C. 1501
D. 3389

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
If a security administrator wants to TELNET into a router to make configuration changes, which of the following ports would need to be open by default?

A. 23
B. 135
C. 161
D. 3389

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following ports would a security administrator block if the administrator wanted to stop users from accessing outside SMTP services?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
A network consists of various remote sites that connect back to two main locations. The security administrator needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 53
Which of the following are the default ports for HTTP and HTTPS protocols? (Select TWO).

A. 21
B. 80
C. 135
D. 443
E. 445

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
In an 802.11n network, which of the following provides the MOST secure method of both encryption and authorization?

A. WEP with 802.1x
B. WPA Enterprise
C. WPA2-PSK
D. WPA with TKIP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
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 56
Which of the following is the BEST choice for encryption on a wireless network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
A user reports that their 802.11n capable interface connects and disconnects frequently to an access point that was recently installed. The user has a Bluetooth enabled laptop. A company in the next building had their wireless network breached last month. Which of the following is MOST likely causing the disconnections?

A. An attacker inside the company is performing a bluejacking attack on the user's laptop.
B. Another user's Bluetooth device is causing interference with the Bluetooth on the laptop.
C. The new access point was mis-configured and is interfering with another nearby access point.
D. The attacker that breached the nearby company is in the parking lot implementing a war driving attack.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following should the security ad to gain more coverage?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which of the following protocols requires the use of a CA based authentication process?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
When configuring multiple computers for RDP on the same wireless router, it may be necessary to do which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A technician needs to limit the wireless signal from reaching outside of a building. Which of the following actions should the technician take?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following will provide the HIGHEST level of wireless network security?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following facilitates computing for heavily utilized systems and networks?

A. Remote access

B. Provider cloud
C. VPN concentrator
D. Telephony

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Risk can be managed in the following ways EXCEPT:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A company that purchases insurance to reduce risk is an example of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following is a best practice to identify fraud from an employee in a sensitive position?

A. Which of the following is a best practice to identify fraud from an employee in a sensitive position?
B. Separation of duties
C. False positives
D. Mandatory vacations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A security administrator with full administrative rights on the network is forced to temporarily take time off of their duties. Which of the following describes this form of access control?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Instead of giving a security administrator full administrative rights on the network, the administrator is given rights only to review logs and update security related network devices. Additional rights are handed out to network administrators for the areas that fall within their job description. Which of the following describes this form of access control?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A security administrator wants to determine what data is allowed to be collected from users of the corporate Internet-facing web application. Which of the following should be referenced?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
An administrator is updating firmware on routers throughout the company. Where should the administrator document this work?

A. Event Viewer

B. Router's System Log
C. Change Management
D. Compliance Review System

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Due to sensitive data concerns, a security administrator has enacted a policy preventing the use of flash drives. Additionally, which of the following can the administrator implement to reduce the risk of data leakage?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Performing routine security audits is a form of which of the following controls?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following is MOST commonly a part of routine system audits?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following is a method to prevent ad-hoc configuration mistakes?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following should be reviewed periodically to ensure a server maintains the correct security configuration?

A. NIDS configuration
B. Firewall logs
C. User rights
D. Incident management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A security administrator finished taking a forensic image of a computer's memory. Which of the following should the administrator do to ensure image integrity?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
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:

QUESTION 78
Which of the following describes when forensic hashing should occur on a drive

A. After the imaging process and before the forensic image is captured
B. Before the imaging process and then after the forensic image is created
C. After the imaging process and after the forensic image is captured
D. Before and after the imaging process and then hash the forensic image

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following assists in identifying if a system was properly handled during transport

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following describes the purpose of chain of custody as applied to forensic image retention?

A. To provide proof the evidence has not been tampered with or modified
B. To provide verification that the forensic examiner is qualified
C. To provide documentation as to who has handled the evidence
D. To provide a baseline reference

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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 82
Which of the following will educate employees about malicious attempts from an attacker to obtain bank account information?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following is a reason to perform user awareness and training?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Used in conjunction, which of the following are PII? (Select TWO).

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

Correct Answer: DE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
On-going annual awareness security training should be coupled with:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following risks may result from improper use of social networking and P2P software?

A. Shoulder surfing
B. Denial of service
C. Denial of service
D. Data loss prevention

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following is the MAIN reason to require data labeling?

A. To ensure that staff understands what data they are handling and processing
B. To ensure that new viruses do not transfer to removable media
C. To ensure that all media sanitization requirements are met
D. To ensure that phishing attacks are identified and labeled properly

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
DRPs should contain which of the following?

A. Hierarchical list of non-critical personnel

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Recovery Point Objectives and Recovery Time Objectives directly relate to which of the following BCP concepts?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A security firm has been engaged to assess a software application. A production-like test environment, login details, production documentation and source code have been provided. Which
of the following types of testing is being described?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following environmental controls would BEST be used to regulate cooling within a datacenter?

A. Fire suppression
B. Video monitoring
C. EMI shielding
D. Hot and cold aisles

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following environmental variables reduces the potential for static discharges?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following should be considered when trying to prevent somebody from capturing network traffic?

A. Video monitoring
B. Hot aisles
C. HVAC controls
D. EMI shielding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
With which of the following is RAID MOST concerned?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which of the following reduces the likelihood of a single point of failure when a server fails?

A. Clustering
B. Virtualization
C. RAID

D. Cold site

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following is the BEST way to secure data for the purpose of retention?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
A security administrator is tasked with ensuring that all servers are highly available and that hard drive failure will not affect an individual server. Which of the following configurations will allow for high availability? (Select TWO).

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
A security administrator is in charge of a datacenter, a hot site and a cold site. Due to a recent disaster, the administrator needs to ensure that their cold site is ready to go in case of a disaster. Which of the following does the administrator need to ensure is in place for a cold site?

A. Location with all required equipment loaded with all current patches and updates
B. Location with duplicate systems found in the datacenter
C. Location near the datacenter that meets power requirements
D. Location that meets power and connectivity requirements

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A critical system in the datacenter is not connected to a UPS. The security administrator has coordinated an authorized service interruption to resolve this issue. This is an example of which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
In order to ensure high availability of all critical servers, backups of the main datacenter are done in the middle of the night and then the backup tapes are taken to an offsite location. Which of the following would ensure the minimal amount of downtime in the case of a disaster?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which of the following concepts ensures that the data is only viewable to authorized users?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A security administrator working for a health insurance company needs to protect customer data by installing an HVAC system and a mantrap in the datacenter. Which of the following are being addressed? (Select TWO).

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
A bulk update process fails and writes incorrect data throughout the database. Which of the following concepts describes what has been compromised?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
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 105
While browsing the Internet, an administrator notices their browser behaves erratically, appears to download something, and then crashes. Upon restarting the PC, the administrator notices performance is extremely slow and there are hundreds of outbound connections to various websites. Which of the following BEST describes what has occurred?

A. The PC has become part of a botnet.
B. The PC has become infected with spyware
C. The PC has become a spam host.

D. The PC has become infected with adware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Which of the following malware types is an antivirus scanner MOST unlikely to discover? (Select TWO).

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which of the following is the primary difference between a virus and a worm?

A. A worm is undetectable
B. A virus is typically larger
C. A virus is easily removed
D. A worm is self-replicating

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
Logs from an IDS show that a computer has been compromised with a botnet and is actively communicating with a command and control server. If the computer is powered off, which of the following data types will be unavailable for later investigation?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Upon investigation, an administrator finds a suspicious system-level kernel module which modifies file system operations. This is an example of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Which of the following is the MOST likely cause of a single computer communicating with an unknown IRC server and scanning other systems on the network?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Which of the following malware types is MOST commonly installed through the use of thumb drives to compromise systems and provide unauthorized access?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
A system administrator could have a user level account and an administrator account to prevent:

A. password sharing.
B. escalation of privileges.

C. implicit deny.
D. administrative account lockout.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
When examining HTTP server logs the security administrator notices that the company's online store crashes after a particular search string is executed by a single external user. Which of the following BEST describes this type of attack?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
Which of the following would allow traffic to be redirected through a malicious machine by sending false hardware address updates to a switch?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Which of the following threats corresponds with an attacker targeting specific employees of a company?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
A user receives an automated call which appears to be from their bank. The automated recording provides details about the bank's privacy policy, security policy and requests that the user clearly state their name, birthday and enter the banking details to validate the user's identity. Which of the following BEST describes this type of attack?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
Which of the following is a technique designed to obtain information from a specific person?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following is another name for a malicious attacker?

A. Black hat
B. White hat
C. Penetration tester
D. Fuzzer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
Which of the following logical controls does a flood guard protect against?

A. Spanning tree

B. Xmas attacks
C. Botnet attack
D. SYN attacks

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Which of the following attacks is BEST described as the interruption of network traffic accompanied by the insertion of malicious code?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
A targeted email attack sent to the company's Chief Executive Officer (CEO) is known as which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
The security administrator implemented privacy screens, password protected screen savers, and hired a secure shredding and disposal service. Which of the following attacks is the security administrator trying to mitigate? (Select TWO).

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

Correct Answer: BC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which of the following security threats does shredding mitigate?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Which of the following attacks would password masking help mitigate?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Which of the following is an example of allowing another user physical access to a secured area without validation of their credentials?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Which of the following is specific to a buffer overflow attack?

A. Memory addressing

B. Directory traversal
C. Initial vector
D. Session cookies

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Which of the following wireless attacks uses a counterfeit base station with the same SSID name as a nearby intended wireless network?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
Data can potentially be stolen from a disk encrypted, screen-lock protected, smartphone by which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
Which of the following is an unauthorized wireless router that allows access to a secure network?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
A security administrator performs several war driving routes each month and recently has noticed a certain area with a large number of unauthorized devices. Which of the following attack types is MOST likely occurring?

A. Interference
B. Rogue access points
C. IV attack
D. Bluejacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Proper wireless antenna placement and radio power setting reduces the success of which of the following reconnaissance methods?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
A rogue access point with the same SSID as the production wireless network is found. Which of the following BEST describes this attack?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
A programmer allocates 16 bytes for a string variable, but does not adequately ensure that more than 16 bytes cannot be copied into the variable. This program may be vulnerable to which of the following attacks?

A. Buffer overflow

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
Which of the following MUST a programmer implement to prevent cross-site scripting?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
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 136
During the analysis of malicious code, a security analyst discovers JavaScript being used to send random data to another service on the same system. This is MOST likely an example of which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
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 138
A web application has been found to be vulnerable to a SQL injection attack. Which of the following BEST describes the required remediation action?

A. Change the server's SSL key and add the previous key to the CRL.
B. Install a host-based firewall.
C. Install missing security updates for the operating system.
D. Add input validation to forms.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
A web application has been found to be vulnerable to a SQL injection attack. Which of the following BEST describes the required remediation action?

A. Change the server's SSL key and add the previous key to the CRL.
B. Install a host-based firewall.
C. Install missing security updates for the operating system.
D. Add input validation to forms.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Which of the following is MOST relevant to a buffer overflow attack?

A. Sequence numbers

B. Set flags
C. IV length
D. NOOP instructions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
The detection of a NOOP sled is an indication of which of the following attacks?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Which of the following devices BEST allows a security administrator to identify malicious activity after it has occurred?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Which of the following should be enabled to ensure only certain wireless clients can access the network?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
Which of the following BEST describes an intrusion prevention system?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
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 146
Which of the following can prevent an unauthorized employee from entering a datacenter? (Select TWO).

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
Two systems are being designed. System A has a high availability requirement. System B has a high security requirement with less emphasis on system uptime. Which of the following configurations BEST fits the need for each system?

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
Several staff members working in a datacenter have reported instances of tailgating. Which of the following could be implemented to prevent this security concern?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
A visitor plugs their laptop into the network and receives a warning about their antivirus being outof-date along with various patches that are missing. The visitor is unable to access the Internet or any network resources. Which of the following is the MOST likely cause?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
Which of the following is a detective security control?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
Which of the following identifies some of the running services on a system?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
A security administrator is tasked with revoking the access of a terminated employee. Which of the following account policies MUST be enacted to ensure the employee no longer has access to the network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
A company needs to be able to prevent entry, at all times, to a highly sensitive area inside a public building. In order to ensure the BEST type of physical security, which of the following should be implemented?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
Which of the following would provide the MOST reliable proof that a datacenter was accessed at a certain time of day?

A. Video surveillance
B. Security log
C. Entry log
D. Proximity readers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
Which of the following should be performed on a computer to protect the operating system from malicious software? (Select TWO).

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
A new enterprise solution is currently being evaluated due to its potential to increase the company's profit margins. The security administrator has been asked to review its security implications. While evaluating the product, various vulnerability scans were performed. It was determined that the product is not a threat but has the potential to introduce additional vulnerabilities. Which of the following assessment types should the security administrator also take into consideration while evaluating this product?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
Which of the following would be the BEST action to perform when conducting a corporate vulnerability assessment?

A. Document scan results for the change control board.
B. Organize data based on severity and asset value.

C. Examine the vulnerability data using a network analyzer.
D. Update antivirus signatures and apply patches.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
Which of the following is used when performing a quantitative risk analysis?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
Which of the following describes a passive attempt to identify weaknesses?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
An existing application has never been assessed from a security perspective. Which of the following is the BEST assessment technique in order to identify the application's security posture?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
An administrator identifies a security issue on the corporate web server, but does not attempt to exploit it. Which of the following describes what the administrator has done?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
The server log shows 25 SSH login sessions per hour. However, it is a large company and the administrator does not know if this is normal behavior or if the network is under attack. Where should the administrator look to determine if this is normal behavior?

A. Change management
B. Code review
C. Baseline reporting
D. Security policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Users of specific systems are reporting that their data has been corrupted. After a recent patch update to those systems, the users are still reporting issues of data being corrupt. Which of the following assessment techniques need to be performed to identify the issue?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
Which of the following is used when performing a qualitative risk analysis?

A. Exploit probability
B. Judgment

C. Threat frequency
D. Asset value

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
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 166
A security administrator wants to know which systems are more susceptible to an attack compared to other systems on the network. Which of the following assessment tools would be MOST effective?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
Which of the following is a management control type?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
Which of the following devices would allow a technician to view IP headers on a data packet?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
Which of the following penetration testing types is performed by security professionals with limited inside knowledge of the network?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
Which of the following is a reason to perform a penetration test?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
Penetration testing should only be used during controlled conditions with express consent of the system owner because:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
Which of the following security practices should occur initially in software development?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
A penetration test shows that almost all database servers were able to be compromised through a default database user account with the default password. Which of the following is MOST likely missing from the operational procedures?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
Which of the following is an example of verifying new software changes on a test system?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
Which of the following would an administrator do to ensure that an application is secure and all unnecessary services are disabled?

A. Baselining
B. Application hardening
C. Secure application coding
D. Patch management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
A security administrator ensures that certain characters and commands entered on a web server are not interpreted as legitimate data and not passed on to backend servers. This is an example of which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

A. The firewall should be configured to allow the application to auto-update.
B. The firewall should be configured to prevent the application from auto-updating.
C. A port scan should be run against the application's server.

D. Vendor-provided hardening documentation should be reviewed and applied.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Which of the following has a programmer MOST likely failed to consider if a user entering improper input is able to crash a program?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
Which of the following is the MOST efficient way to combat operating system vulnerabilities?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
Which of the following is a hardening step of an application during the SDLC?

A. Disabling unnecessary accounts
B. Application patch management schedule
C. Secure coding concepts
D. Disabling unnecessary services

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
Which of the following should be performed if a smartphone is lost to ensure no data can be retrieved from it?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
Several classified mobile devices have been stolen. Which of the following would BEST reduce the data leakage threat?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
Which of the following should be used to help prevent device theft of unused assets?

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 186
Which of the following devices would be installed on a single computer to prevent intrusion?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
A security administrator has been receiving support tickets for unwanted windows appearing on user's workstations. Which of the following can the administrator implement to help prevent this from happening?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
Which of the following would an administrator apply to mobile devices to BEST ensure the confidentiality of data?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
Which of the following is a security vulnerability that can be disabled for mobile device users?

A. Group policy

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
Which of the following software should a security administrator implement if several users are stating that they are receiving unwanted email containing advertisements?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
An employee stores their list of passwords in a spreadsheet on their local desktop hard drive. Which of the following encryption types would protect this information from disclosure if lost or stolen?

A. Database
B. Removable media
C. File and folder level
D. Mobile device

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
A company has remote workers with laptops that house sensitive data. Which of the following can be implemented to recover the laptops if they are lost?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
When decommissioning old hard drives, which of the following is the FIRST thing a security engineer should do?

A. Perform bit level erasure or overwrite
B. Flash the hard drive firmware
C. Format the drive with NTFS
D. Use a waste disposal facility

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
Which of the following devices provides storage for RSA or asymmetric keys and may assist in user authentication? (Select TWO).

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
Which of the following is true about hardware encryption? (Select TWO).

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
Which of the following BEST describes the function of TPM?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
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 198
A security administrator is implementing a solution that can integrate with an existing server and provide encryption capabilities. Which of the following would meet this requirement?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
Which of the following are the BEST reasons to use an HSM? (Select TWO).

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

Correct Answer: CE
Section: (none)

Explanation

Explanation/Reference:

QUESTION 200
A company needs to reduce the risk of employees emailing confidential data outside of the company. Which of the following describes an applicable security control to mitigate this threat?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
Which of the following can cause hardware based drive encryption to see slower deployment?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
Which of the following is the MOST secure way of storing keys or digital certificates used for decryption/ encryption of SSL sessions?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
Which of the following is a removable device that may be used to encrypt in a high availability clustered environment?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
A security administrator is implementing a solution that encrypts an employee's newly purchased laptop but does not require the company to purchase additional hardware or software. Which of the following could be used to meet this requirement?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205
During incident response, which of the following procedures would identify evidence tampering by outside entities?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
Which of the following protocols only encrypts password packets from client to server?

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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 207
Which of the following methods of access, authentication, and authorization is the MOST secure by default?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
Which of the following uses tickets to identify users to the network?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
A purpose of LDAP authentication services is:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
When granting access, which of the following protocols uses multiple-challenge responses for authentication, authorization and audit?

A. TACACS

B. TACACS+
C. LDAP
D. RADIUS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
A security administrator is setting up a corporate wireless network using WPA2 with CCMP but does not want to use PSK for authentication. Which of the following could be used to support 802.1x authentication?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
Which of the following authentication services would be used to authenticate users trying to access a network device?

A. SSH
B. SNMPv3
C. TACACS+
D. TELNET

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
Which of the following requires special handling and explicit policies for data retention and data distribution?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
Centrally authenticating multiple systems and applications against a federated user database is an example of:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
A Human Resource manager is assigning access to users in their specific department performing the same job function. This is an example of:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216
The security administrator often observes that an employee who entered the datacenter does not match the owner of the PIN that was entered into the keypad. Which of the following would BEST prevent this situation?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217
Which of the following allows a user to have a one-time password?

A. Biometrics
B. SSO

C. PIV
D. Tokens

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
Which of the following is a technical control?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
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 the administrator 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 220
A thumbprint scanner is used to test which of the following aspects of human authentication?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
A security administrator with full administrative rights on the network is forced to change roles on a quarterly basis with another security administrator. Which of the following describes this form of access control?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 222
In order to access the network, an employee must swipe their finger on a device. Which of the following describes this form of authentication?

A. Single sign-on
B. Multifactor
C. Biometrics
D. Tokens

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
A proximity card reader is used to test which of the following aspects of human authentication?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
Which of the following would be considered multifactor authentication?

A. Pin number and a smart card
B. ACL entry and a pin number

C. Username and password
D. Common access card

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
Which of the following is a form of photo identification used to gain access into a secure location?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
Which of the following is a trusted OS implementation used to prevent malicious or suspicious code from executing on Linux and UNIX platforms?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227
Which of the following is an example of allowing a user to perform a self-service password reset?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228
Which of the following is an example of requiring users to have a password of 16 characters or more?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
A security administrator is asked to email an employee their password. Which of the following account policies MUST be set to ensure the employee changes their password promptly?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 230
Employees are required to come up with a passphrase of at least 15 characters to access the corporate network. Which of the following account policies does this exemplify?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
An administrator has implemented a policy that passwords expire after 60 days and cannot match their last six previously used passwords. Users are bypassing this policy by immediately changing their passwords six times and then back to the original password. Which of the following can the administrator MOST easily employ to prevent this unsecure practice, with the least administrative effort?

A. Create a policy that passwords must be no less than ten characters.
B. Monitor user accounts and change passwords of users found to be doing this.

C. Create a policy that passwords cannot be changed more than once a day.
D. Monitor user accounts and lock user accounts that are changing passwords excessively.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232
Which of the following MUST be implemented in conjunction with password history, to prevent a user from re-using the same password?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
Which of the following represents the complexity of a password policy which enforces lower case password using letters from 'a' through 'z' where 'n' is the password length?

A. $_{n}26$
B. $2^{n} * 26$
C. 26^{n}
D. $n^{2} * 26$

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234
Which of the following BEST describes the process of key escrow?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
Which of the following is the primary purpose of using a digital signature? (Select TWO).

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses:

A. multiple keys for non-repudiation of bulk data.
B. different keys on both ends of the transport medium.
C. bulk encryption for data transmission over fiber.
D. the same key on each end of the transmission medium.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 237
Which of the following methods BEST describes the use of hiding data within other files?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238
When a user first moves into their residence, the user receives a key that unlocks and locks their front door. This key is only given to them but may be shared with others they trust. Which of the following cryptography concepts is illustrated in the example above?

A. Asymmetric key sharing
B. Exchange of digital signatures
C. Key escrow exchange
D. Symmetric key sharing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 239
Which of the following cryptography types provides the same level of security but uses smaller key sizes and less computational resources than logarithms which are calculated against a finite field?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240
The BEST way to protect the confidentiality of sensitive data entered in a database table is to use:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
WEP is seen as an unsecure protocol based on its improper use of which of the following?

A. RC6
B. RC4
C. 3DES
D. AES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242
Which of the following is used in conjunction with PEAP to provide mutual authentication between peers?

A. LEAP
B. MSCHAPv2
C. PPP
D. MSCHAPv1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243
Which of the following is seen as non-secure based on its ability to only store seven uppercase characters of data making it susceptible to brute force attacks?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 244
Which of the following access control technologies provides a rolling password for one-time use?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
A security administrator has discovered through a password auditing software that most passwords can be discovered by cracking the first seven characters and then cracking the second part of the password. Which of the following is in use by the company?

A. LANMAN

B. MD5
C. WEP
D. 3DES

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
NTLM is an improved and substantially backwards compatible replacement for which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247
Which of the following does a TPM allow for?

A. Cloud computing
B. Full disk encryption
C. Application hardening
D. Input validation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248
The company encryption policy requires all encryption algorithms used on the corporate network to have a key length of 128-bits. Which of the following algorithms would adhere to company policy?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249
The security administrator wants to ensure messages traveling between point A and point B are encrypted and authenticated. Which of the following accomplishes this task?

A. MD5
B. RSA
C. Diffie-Hellman
D. Whole disk encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 250
Which of the following elements of PKI are found in a browser's trusted root CA?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
Where are revoked certificates stored?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
Which of the following asymmetric encryption keys is used to encrypt data to ensure only the intended recipient can decrypt the ciphertext?

A. Private
B. Escrow
C. Public

D. Preshared

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
Which of the following must a security administrator do when the private key of a web server has been compromised by an intruder?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 254
Which of the following PKI implementation element is responsible for verifying the authenticity of certificate contents?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255
If a user wishes to receive a file encrypted with PGP, the user must FIRST supply the:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256
A certificate that has been compromised should be published to which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 257
The security administrator is tasked with authenticating users to access an encrypted database. Authentication takes place using PKI and the encryption of the database uses a separate cryptographic process to decrease latency. Which of the following would describe the use of encryption in this situation?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 258
When a certificate issuer is not recognized by a web browser, which of the following is the MOST common reason?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259
Public keys are used for which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
Which of the following is a requirement when implementing PKI if data loss is unacceptable?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
Which of the following is true about PKI? (Select TWO).

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 262
The recovery agent is used to recover the:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263
Which of the following is true about the CRL?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264
A file has been encrypted with an employee's private key. When the employee leaves the company, their account is deleted. Which of the following are the MOST likely outcomes? (Select TWO).

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 265
Which of the following is the BEST filtering device capable of stateful packet inspection?

A. Switch
B. Protocol analyzer
C. Firewall
D. Router

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 266
An employee's workstation is connected to the corporate LAN. Due to content filtering restrictions, the employee attaches a 3G Internet dongle to get to websites that are blocked by the corporate gateway. Which of the following BEST describes a security implication of this practice?

A. A corporate LAN connection and a 3G Internet connection are acceptable if a host firewall is installed.
B. The security policy should be updated to state that corporate computer equipment should be dual-homed.
C. Content filtering should be disabled because it may prevent access to legitimate sites.
D. Network bridging must be avoided otherwise it may join two networks of different classifications.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 267
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 268
In a disaster recovery situation, operations are to be moved to an alternate site. Computers and network connectivity are already present; however, production backups are several days out-of-date. Which of the following site types is being described?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 269
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 270
Which of the following PKI components identifies certificates that can no longer be trusted?

A. CRL
B. CA public key
C. Escrow
D. Recovery agent

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271
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 272
A digital signature provides which of the following security functions for an email message?

A. Encryption
B. Hashing
C. Input validation
D. Non-repudiation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273
By default, CCMP will use which of the following to encrypt wireless transmissions?

A. RC4
B. Blowfish
C. AES
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274
A programmer cannot change the production system directly and must have code changes reviewed and approved by the production system manager. Which of the following describes this control type?

A. Discretionary access control
B. Separation of duties
C. Security policy
D. Job rotation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 275
ARP poison routing attacks are an example of which of the following?

A. Distributed Denial of Service
B. Smurf Attack
C. Man-in-the-middle
D. Vishing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 276
A company hires a security firm to assess the security of the company's network. The company does not provide the firm with any internal knowledge or documentation of the network. Which of the following should the security firm perform?

A. Black hat
B. Black box
C. Gray hat
D. Gray box

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277
Steganography is a form of which of the following?

A. Block ciphering

B. Quantum cryptography
C. Security through obscurity
D. Asymmetric encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 278
In a public key infrastructure, a trusted third party is also known as which of the following?

A. Public key
B. Certificate signing request
C. Common name
D. Certificate authority

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 279
Which of the following relies on creating additional traffic to congest networks? (Select TWO).

A. Logic bomb
B. Smurf attack
C. Man-in-the-middle attack
D. DDoS
E. DNS poisoning

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 280
Which of the following threats are specifically targeted at high profile individuals?

A. Whaling
B. Malicious insider
C. Privilege escalation
D. Shoulder surfing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 281
Which of the following devices is MOST commonly vulnerable to bluesnarfing?

A. Mobile devices
B. Desktops
C. Digital signage
D. Ethernet jacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 282
Which of the following application attacks typically involves entering a string of characters and bypassing input validation to display additional information?

A. Session hijacking
B. Zero day attack
C. SQL injection
D. Cross-site scripting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283
Which of the following features should be enabled on perimeter doors to ensure that unauthorized access cannot be gained in the event of a power outage?

A. Manual override
B. Fail closed
C. Mantrap
D. Fail open

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 284
Which of the following is the BEST tool to use when analyzing incoming network traffic?

A. Sniffer
B. Port scanner
C. Firewall

D. Syslog

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 285
Which of the following MOST likely has its access controlled by TACACS+? (Select TWO).

A. Mobile devices
B. Active directory
C. Router
D. Switch
E. Kerberos

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 286
Providing elastic computing resources that give a client access to more resources, allowing for distribution of large jobs across a flexible number of machines, or allowing for distributed storage of information are all hallmarks of which technology?

A. Remote access
B. Clustering
C. Cloud computing
D. IP networking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 287
Which of the following network security techniques can be easily circumvented by using a network sniffer?

A. Disabling the SSID broadcast
B. Enabling strong wireless encryption
C. Implementing MAC filtering on WAPs
D. Reducing the wireless power level

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 288
Which of the following authentication services can be used to provide router commands to enforce policies?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 289
Which of the following ports is used for telnet by default?

A. 21
B. 23
C. 25
D. 33

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 290
Which of the following BEST describes a malicious application that attaches itself to other files?

A. Rootkits
B. Adware
C. Backdoors
D. Virus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 291
When an attack using a publicly unknown vulnerability compromises a system, it is considered to be which of the following?

A. IV attack
B. Zero day attack
C. Buffer overflow
D. Malicious insider threat

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 292
A professor at a university is given two keys. One key unlocks a classroom door and the other locks it. The key used to lock the door is available to all other faculty. The key used to unlock the door is only given to the professor. Which of the following cryptography concepts is illustrated in the example above?

A. Key escrow exchange
B. Asymmetric key sharing
C. Exchange of digital signatures
D. Symmetric key sharing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 293
Which of the following are often used to encrypt HTTP traffic? (Select TWO).

A. PAP
B. SCP
C. SHA
D. TLS
E. SSL

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 294
Which of the following attacks targets high profile individuals?

A. Logic bomb
B. Smurf attack
C. Whaling
D. Fraggle attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 295
A penetration tester is collecting a large amount of wireless traffic to perform an IV attack. Which of the following can be gained by doing this?

A. WPA2 shared secret
B. WPA key
C. WEP key
D. EAP-TLS private key

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 296
Which of the following allows users in offsite locations to connect securely to a corporate office?

A. Telnet
B. FTP
C. VPN
D. SNMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 297
On a website, which of the following protocols facilitates security for data in transit?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 298
Which of the following security controls is the BEST mitigation method to address mobile device data theft? (Select TWO).

A. Inventory logs
B. Remote wipe
C. Device encryption
D. Host-based firewall
E. Check in and check out paperwork

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 299
Which of the following BEST describes the purpose of fuzzing?

A. To decrypt network sessions
B. To gain unauthorized access to a facility
C. To hide system or session activity
D. To discover buffer overflow vulnerabilities

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 300
There are several users for a particular Human Resources database that contains PII. Which of the following principles should be applied to the users in regards to privacy of information?

A. Single sign-on
B. Least privilege
C. Time of day restrictions
D. Multifactor authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 301
Which of the following would be a reason to implement DAC as an access control model?

A. Management should have access to all resources
B. An employee's security level should determine the access level
C. The owner of the data should decide who has access
D. Centrally administered roles determine who has access

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 302
A security administrator needs to install a new switch for a conference room where two different groups will be

having separate meetings. Each of the groups uses different subnets and need to have their traffic separated. Which of the following would be the SIMPLEST solution?

A. Create ACLs to deny traffic between the two networks on the switch.
B. Install a network firewall.
C. Create two VLANs on the switch.
D. Add a router to separate the two networks.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 303
Which of the following would need to be added to a network device's configuration in order to keep track of the device's various parameters and to monitor status?

A. SNMP string
B. ACLs
C. Routing information
D. VLAN information

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 304
A user reports the ability to access the Internet but the inability to access a certain secure website. The web browser reports the site needs to be viewed under a secure connection. Which of the following is the MOST likely cause? (Select TWO).

A. The site is using TLS instead of SSL.
B. The user is not using HTTP.
C. The site is not using URL redirection.
D. ICMP needs to be enabled.
E. The user is not using HTTPS.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 305
Which of the following is a control that is gained by using cloud computing?

A. Data encryption
B. High availability of the data
C. Administrative control of the data

D. Physical control of the data

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 306
Which of the following is the BEST way to implement data leakage prevention? (Select TWO).

A. Installing DLP software on all computers along with the use of policy and procedures
B. Installing DLP software on all perimeter appliances and incorporating new policies and procedures
C. Securing all appliances and computers that control data going into the network along with the use of policy and procedures
D. Ensuring the antivirus, NIDS, anti-malware software, and signatures are up-to-date
E. Implementing firewall access control lists to block all incoming attachments

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 307
A tape library containing a database with sensitive information is lost in transit to the backup location. Which of the following will prevent this media from disclosing sensitive information? (Select TWO).

A. Mobile device encryption
B. Full disk encryption
C. Database encrypt
D. Discretionary access control
E. Trusted platform module

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 308
A security administrator ensures that rights on a web server are not sufficient to allow outside users to run JavaScript commands. This is an example of which of the following?

A. Application patch management
B. Data execution prevention
C. Error and exception handling
D. Cross-site scripting prevention

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 309
Which of the following creates a publicly accessible network and isolates the internal private network from the Internet?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 310
A security administrator is encrypting all smartphones connected to the corporate network. Which of the following could be used to meet this requirement?

A. Mobile device encryption
B. Database encryption
C. Network encryption
D. HSM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 311
Using both a username and a password is an example of:

A. biometric authentication
B. something a user knows and something a user has
C. single factor authentication
D. multifactor authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 312
Which of the following password policies are designed to increase the offline password attack time? (Select TWO).

A. Password expiration

B. Password lockout time
C. Password age time
D. Password complexity
E. Password length

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 313
GPU processing power is a mitigating factor for which of the following security concerns?

A. Password complexity
B. Cloud computing
C. Biometrics
D. Virtualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 314
Which of the following can the security administrator implement to BEST prevent laptop device theft?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 315
The pharmacy has paper forms ready to use if the computer systems are unavailable. Which of the following has been addressed?

A. Continuity of operations
B. Single point of failure
C. Disaster recovery
D. Business process reengineering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 316
Which of the following causes an issue when acquiring an image that occurs when a server hard drive is forensically examined?

A. Servers often use RAID
B. Servers contain sensitive information
C. Servers cannot be powered down
D. Servers often use file systems

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 317
Which of the following provides the BEST metric for determining the effectiveness of a Continuity of Operations Plan or Disaster Recovery Plan?

A. Average downtime
B. Mean time between failures
C. Mean time to restore
D. Average uptime

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 318
Which of the following is the correct formula for calculating mean time to restore (MTTR)?

A. MTTR = (time of fail) / (time of restore)
B. MTTR = (time of fail) # (time of restore)
C. MTTR = (time of restore) # (time of fail)
D. MTTR = (time of restore) x (time of fail)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Verify formula

QUESTION 319
The corporate NIDS keeps track of how each program acts and will alert the security administrator if it starts acting in a suspicious manner. Which of the following describes how the NIDS is functioning?

A. Behavior based

B. Signature based
C. Host based
D. Network Access Control (NAC) based

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 320
Pete, a security technician, has chosen IPSec for remote access VPN connections for company telecommuters. Which of the following combinations would be BEST for Pete to use to secure this connection?

A. Transport mode, ESP
B. Transport mode, AH
C. Tunnel mode, AH
D. Tunnel mode, ESP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 321
Matt, a security administrator, is using AES. Which of the following cipher types is used by AES?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 322
Which of the following forensic artifacts is MOST volatile?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 323
Which of the following protocols can Sara, a security administrator, use to implement security at the lowest OSI layer?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 324
Which of the following protocols uses UDP port 69 by default?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 325
After completing a forensic image of a hard drive, which of the following can Jane, a security technician, use to confirm data integrity?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 326
Which of the following can Matt, a security administrator, use to provide integrity verification when storing data?

A. Encryption
B. Hashing
C. PKI

D. ACL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 327
Which of the following is an example of implementing security using the least privilege principle?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 328
The decision to build a redundant datacenter MOST likely came from which of the following?

A. Application performance monitoring
B. Utilities cost analysis
C. Business impact analysis
D. Security procedures review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 329
Sara and Pete are unauthorized system attackers that may be able to remotely destroy critical equipment in a datacenter if they gain control over which of the following systems?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 330

In high traffic areas, Jane and Pete, security guards, need to be MOST concerned about which of the following attacks?

A. War driving
B. Blue jacking
C. Shoulder surfing
D. Tailgating

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 331
Which of the following BEST describes an attack whereby unsolicited messages are sent to nearby mobile devices?

A. Smurf attack
B. Bluejacking
C. Bluesnarfing
D. War driving

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 332
Which of the following network ACL entries BEST represents the concept of implicit deny?

A. Deny UDP any
B. Deny TCP any
C. Deny ANY any
D. Deny FTP any

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 333
Which of the following protocols assists in identifying Pete, a user, by the generation of a key, to establish a secure session for command line administration of a computer?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 334
Which of the following is a major risk for Matt, a security administrator, to consider in regards to cloud computing?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 335
Matt, a security administrator, performs various audits of a specific system after an attack. Which of the following BEST describes this type of risk mitigation?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 336
Which of the following is the MOST appropriate risk mitigation strategy for Sara, a security administrator, to use in order to identify an unauthorized administrative account?

A. Change management
B. Incident management
C. Routine audits of system logs
D. User's rights and permissions review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 337

Which of the following would Jane, a security administrator, MOST likely look for during a vulnerability assessment?

A. Ability to gain administrative access to various systems
B. Identify lack of security controls
C. Exploit vulnerabilities
D. Actively test security controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 338
Which of the following will contain a list of unassigned public IP addresses?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 339
The MAIN difference between qualitative and quantitative risk assessment is:

A. quantitative is based on the number of assets while qualitative is based on the type of asset.
B. qualitative is used in small companies of 100 employees or less while quantitative is used in larger companies of 100 employees or more.
C. quantitative must be approved by senior management while qualitative is used within departments without specific approval.
D. quantitative is based on hard numbers while qualitative is based on subjective ranking.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 340
Which of the following attacks involves sending unsolicited contact information to Bluetooth devices configured in discover mode?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 341
Which of the following assessments is directed towards exploiting successive vulnerabilities to bypass security controls?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 342
Which of the following is the technical implementation of a security policy?

A. VLAN
B. Flood guards
C. Cloud computing
D. Firewall rules

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 343
Which of the following can Mike, a security technician, use to prevent numerous SYN packets from being accepted by a device?

A. VLAN management
B. Transport encryption
C. Implicit deny
D. Flood guards

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 344

Which of the following can Jane, a security technician, use to stop malicious traffic from affecting the company servers?

A. NIDS
B. Protocol analyzers
C. Sniffers
D. NIPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 345
Which of the following tools allows a security company to identify the latest unknown attacks utilized by attackers?

A. IDS
B. Honeypots
C. Port scanners
D. Code reviews

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 346
If continuity plans are not regularly exercised, which of the following aspects of business continuity planning are often overlooked until a disaster occurs?

A. Zero day exploits
B. Succession planning
C. Tracking of man hours
D. Single points of failure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 347
Large, partially self-governing, collection of hosts executing instructions for a specific purpose is an example of which type of malware?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 348
Which of the following attacks is BEST described as an attempt to convince Matt, an authorized user, to provide information that can be used to defeat technical security controls?

A. Shoulder surfing
B. Tailgating
C. Impersonation
D. Packet sniffing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 349
Randomly attempting to connect to wireless network access points and documenting the locations of accessible networks is known as which of the following?

A. Packet sniffing
B. War chalking
C. Evil twin
D. War driving

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 350
Which of the following should Sara, a security technician, check regularly to avoid using compromised certificates?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 351
Matt, a user, was able to access a system when he arrived to work at 5:45 a.m. Just before Matt left at 6:30 p.m., he was unable to access the same system, even though he could ping the system. In a Kerberos realm, which of the following is the MOST likely reason for this?

A. Matt's ticket has expired.
B. The system has lost network connectivity.
C. The CA issued a new CRL.
D. The authentication server is down.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 352
Pete, a security administrator, is considering using TACACS+. Which of the following is a reason to use TACACS+ over RADIUS?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 353
A company is looking at various solutions to manage their large datacenter. The company has a lot of sensitive data on unreliable systems. Which of the following can Matt, a security technician, use to allow the company to minimize their footprint?

A. Infrastructure as a Service
B. Implement a NAC server
C. Software as a Service
D. Create a new DMZ

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 354
A hard drive of a terminated employee has been encrypted with full disk encryption, and Sara, a technician, is not able to decrypt the data. Which of the following ensures that, in the future, Sara will be able to decrypt this information?

A. Certificate authority

B. Key escrow
C. Public key
D. Passphrase

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 355
Which of the following is true about the private key in a PKI?

A. It is used by the recovery agent to generate a lost public key
B. It is used by the CA to validate a user's identity
C. It is used to decrypt the email hash in signed emails
D. It is used to encrypt the email hash in signed emails

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 356
Which of the following is an example of authentication using something Sara, a user, has and something she is?

A. Username and PIN
B. Token and PIN
C. Password and retina scan
D. Token and fingerprint scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 357
Which of the following allows Jane, a security administrator, to divide a network into multiple zones? (Select TWO).

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 358
Which of the following attacks is MOST likely prevented when a website does not allow the '<' character as the input in a web form field?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 359
Which of the following must Pete, a security administrator, install on a flash drive to allow for portable drive data confidentiality?

A. USB encryptor
B. Hardware write lock
C. USB extension cable
D. Ext2 file system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 360
An online banking portal is not accessible by customers during a holiday season. Sara and Pete, network administrators, notice sustained, extremely high network traffic being directed towards the web interface of the banking portal from various external networks. Which of the following BEST describes what is occurring?

A. X-Mas attack
B. DDoS attack
C. DNS poisoning
D. DOS attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 361
While chatting with friends over IM, Matt, a user, receives numerous instant messages from strangers advertising products or trying to send files. Which of the following BEST describes the threat?

A. Spear phishing
B. Spam
C. Spim
D. Spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 362
Which of the following is the MOST likely implication of a corporate firewall rule that allows TCP port 22 from any internal IP to any external site?

A. Data loss can occur as an SSH tunnel may be established to home PCs.
B. NAT of external websites to the internal network will be limited to TCP port 22 only.
C. Host based firewalls may crash due to protocol compatibility issues.
D. IPSec VPN access for home users will be limited to TCP port 22 only.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 363
Jane, a network administrator, changes the default usernames and passwords on an 802.11n router. This is an example of which of the following network management controls?

A. System hardening
B. Rule-based management
C. Network separation
D. VLAN management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 364
Jane, a security technician, needs to transfer files. Which of the following is the file transfer function that utilizes the MOST secure form of data transport?

A. TFTP
B. FTP active
C. FTP passive
D. SFTP

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 365
Which of the following, when used in conjunction with software-based encryption, enhances platform authentication by storing unique RSA keys and providing crypto processing?

A. LDAP
B. TPM
C. Kerberos
D. Biometrics

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 366
Which of the following exploitation types involves injection of pseudo-random data in order to crash or provide unexpected results from an application?

A. Cross-site forgery
B. Brute force attack
C. Cross-site scripting
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 367
Which of the following ports would Sara, a security administrator, need to be open to allow TFTP by default?

A. 69
B. 110
C. 137
D. 339

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 368
Pete, a customer, has called a company to report that all of his computers are displaying a rival company's website when Pete types the correct URL into the browser. All of the other websites he visits work correctly and

other customers are not having this issue. Which of the following has MOST likely occurred?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 369
Jane, a system administrator, sees a firewall rule that applies to 10.4.4.58/27. Which of the following IP address ranges are encompassed by this rule?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 370
Which of the following would be implemented if Jane, a security administrator, wants a door to electronically unlock when certain employees need access to a location?

A. Device locks
B. Video surveillance
C. Mantraps
D. Proximity readers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 371
Which of the following is considered strong authentication?

A. Trusted OS
B. Smart card
C. Biometrics
D. Multifactor

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 372
Which of the following is an example of a smart card?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 373
Which of the following is a security best practice that allows Pete, a user, to have one ID and password for all systems?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 374
Which of the following is an example of the type of access control methodology provided on Windows systems by default?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 375
Which of the following is the MOST thorough way to discover software vulnerabilities after its release?

A. Baseline reporting
B. Design review
C. Code review
D. Fuzzing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 376
Which of the following is the way Pete, a security administrator, can actively test security controls on a system?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 377
Which of the following is another name for fizzing third party proprietary software?

A. Grey box testing
B. Black box testing
C. White box testing
D. Blue jacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
verify- fizzing

QUESTION 378
Which of the following application attacks can be used against Active Directory based systems?

A. XML injection
B. SQL injection
C. LDAP injection
D. Malicious add-ons

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 379
Which of the following is a security best practice that Jane, a security technician, would implement before placing a new server online?

A. On-demand computing
B. Host software baselining
C. Virtualization
D. Code review

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 380
Which of the following software types can Sara, a security technician, use to protect against non-malicious but irritating malware?

A. Pop-up blockers
B. Antivirus
C. Host-based firewalls
D. Anti-spyware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 381
Which of the following is the MOST common security issue on web-based applications?

A. Hardware security
B. Transport layer security
C. Input validation
D. Fizzing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 382
Which of the following can cause data loss from web based applications?

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

D. XML

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 383
Which of the following is a preventative physical security control?

A. CCTV
B. Armed guard
C. Proper lighting
D. Access list

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 384
Matt, a security administrator, is considering using cloud computing. Which of the following security concerns is MOST prominent when utilizing cloud computing service providers?

A. Video surveillance
B. Mobile device access
C. Removable storage media
D. Blended systems and data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 385
Which of the following is a security control that can utilize a command such as 'deny ip any any'?

A. ACL
B. Content inspection
C. Network bridge
D. VPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 386

Which of the following is an account management principle for simplified user administration?

A. Ensure password complexity requirements are met.
B. Disable unused system accounts.
C. Implement access based on groups.
D. Ensure minimum password length is acquired.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 387
In which of the following locations can password complexity be enforced via group policy?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 388
A Black Box assessment of an application is one where Sara, the security assessor, has:

A. access to the source code and the development documentation
B. no access to the application's source code and development documentation
C. access to the UAT documentation but not the source code
D. no access to the source code but access to the development documentation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 389
Which of the following security controls should Pete, the security administrator, implement to prevent server administrators from accessing information stored within an application on a server?

A. File encryption
B. Full disk encryption
C. Change management
D. Implicit deny

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 390
Which of the following can Pete, a security technician, deploy to provide secure tunneling services?

A. IPv6
B. DNSSEC
C. SNMPv2
D. SNMPv3

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 391
Which of the following is a reason Pete, a security administrator, would implement Kerberos over local system authentication?

A. Authentication to multiple devices
B. Centralized file integrity protection
C. Non-repudiation
D. Greater password complexity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 392
Which of the following is Pete, a security technician, MOST likely to use to secure the creation of cryptographic keys?

A. Common access card
B. Hashing algorithm
C. Trusted platform module
D. One-time pad

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 393
Which of the following is MOST likely to reduce the threat of a zero day vulnerability?

A. Patch management

B. Network-based intrusion detection system
C. Disabling unnecessary services
D. Host-based intrusion detection system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 394
Which of the following has the capability to perform onboard cryptographic functions?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 395
Matt, a security administrator, discovers that Server1 and Server2 have been compromised, and then he observes unauthorized outgoing connections from Server1 to Server2. On Server1 there is an executable named tcpdump and several files that appear to be network dump files. Finally, there are unauthorized transactions in the database on Server2. Which of the following has MOST likely occurred?

A. A logic bomb has been installed on Server1.
B. A backdoor has been installed on Server2
C. A replay attack has been used against Server2.
D. A botnet command and control has been installed on Server1.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 396
Which of the following is MOST relevant for Jane, a security administrator, to use when investigating a SQL injection attack?

A. Stored procedures
B. Header manipulation
C. Malformed frames
D. Java byte code

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 397
Pete, a system administrator, was recently laid off for compromising various accounting systems within the company. A few months later, the finance department reported their applications were not working correctly. Upon further investigation, it was determined that unauthorized accounting software was installed onto a financial system and several application exploits existed within that system. This is an example of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 398
During a company's relocation, Sara, a security administrator, notices that several hard copies of company directories are being thrown away in public dumpsters. Which of the following attacks is the company vulnerable to without the proper user training and awareness?

A. Hoaxes
B. Pharming
C. Social engineering
D. Brute force

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 399
Matt, a security administrator, notices an unauthorized vehicle roaming the area on company grounds. Matt verifies that all network connectivity is up and running and that no unauthorized wireless devices are being used to authenticate other devices; however, he does notice an unusual spike in bandwidth usage. This is an example of which of the following attacks?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 400
A new product is being evaluated by the security team. Which of the following would take financial and business impacts into consideration if this product was likely to be purchased for large scale use?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 401
Jane, a security administrator, needs to make a change in the network to accommodate a new remote location. The new location will be connected by a serial interface, off the main router, through a commercial circuit. This remote site will also have traffic completely separated from all other traffic. Which of the following design elements will Jane need to implement to accommodate the new location?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 402
Matt, a security administrator, has recently performed a detailed datacenter inventory of all hardware and software. This analysis has resulted in identifying a lot of wasted resources. Which of the following design elements would eliminate the wasted resources and improve the datacenter's footprint?

A. NAC
B. Virtualization
C. Remote access implementation
D. Hosted IP Centrex

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 403
Pete, a user, reports that after a recent business trip, his laptop started having performance issues and

unauthorized emails have been sent out from the laptop. Which of the following will resolve this issue?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 404
When WPA is implemented using PSK by Pete, a security administrator, which of the following authentication types is he using?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 405
If Jane, a security administrator, is reviewing a verified JPEG's metadata and hash against an unverified copy of the graphic, which of the following is she looking for?

A. Steganography
B. Chain of custody
C. Digital signatures
D. Whole disk encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 406
Which of the following technologies is often used by attackers to hide the origin of an attack?

A. Open proxy
B. Load balancer
C. Flood guard
D. URL filtering

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 407
Which of the following is susceptible to reverse lookup attacks if not configured properly?

A. SSL
B. IPSec
C. ICMP
D. DNS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 408
Which of the following are the two basic components upon which cryptography relies?

A. PKI and keys
B. Algorithms and key escrow
C. Key escrow and PKI
D. Algorithms and keys

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 409
Which of the following should Jane, a security administrator, check for when conducting a wireless audit? (Select TWO).

A. Open relays
B. Antenna placement
C. Encryption of wireless traffic
D. URL filtering
E. Open proxies

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 410
Which of the following passwords have the MOST similar key space? (Select TWO).

A. AnDwWe9
B. check123
C. Mypassword!2~
D. C0mPTIA
E. 5938472938193859392

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 411
Jane, the company's Chief Information Officer (CIO), contacts the security administrator about an email asking for money in order to receive the key that would decrypt the source code that the attacker encrypted. Which of the following malware types is this MOST likely to be in this situation?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 412
Matt, a security engineer, working at a public CA is implementing and installing a new CRL. Where should he logically place the server?

A. On a wireless network
B. Inside the DMZ
C. On an non-routable network
D. On a secure internal network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 413
Jane, a security engineer, is deploying a new CA. Which of the following is the BEST strategy for the root CA after deploying an intermediate trusted CA?

A. It should be placed outside of the firewall.
B. It should be placed in the DMZ.
C. It should be placed within an internal network.
D. It should be shut down and kept in a secure location.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 414
Matt, a security administrator, has installed a new server and has asked a network engineer to place the server within VLAN 100. This server can be reached from the Internet, but Matt is unable to connect from the server to internal company resources. Which of the following is the MOST likely cause?

A. The server is connected with a crossover cable.
B. VLAN 100 does not have a default route.
C. The server is in the DMZ.
D. VLAN 100 is on the internal network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 415
Sara, a security administrator, is analyzing the packet capture from an IDS triggered filter. The packet capture shows the following string:

'or 1 ==1 - -

Which of the following attacks is occurring?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 416
Pete, a security administrator, is analyzing the packet capture from an IDS triggered filter. The packet capture shows the following string:

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

Which of the following attacks is occurring?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 417
Which of the following is true when Sara, a user, browsing to an HTTPS site receives the message: 'The site's certificate is not trusted'?

A. The certificate has expired and was not renewed.
B. The CA is not in the browser's root authority list.
C. The intermediate CA was taken offline.
D. The CA is not in the default CRL.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 418
Which of the following is true when Sara, a user, browsing to an HTTPS site receives the message: 'Site name mismatch'?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 419
Pete, a security administrator, needs to implement a wireless system that will only be available within a building. Which of the following configurations can Pete modify to achieve this? (Select TWO).

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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 420
Sara, a technician, must configure a network device to allow only certain protocols to the external servers and block requests to other internal sources. This is an example of a:

A. demilitarized zone
B. load balancer
C. layer 2 switch
D. stateful firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 421
Which of the following protocols should Pete, a security administrator, use to ensure that the data remains encrypted during transport over the Internet? (Select THREE).

A. TLS
B. SSL
C. FTP
D. SSH
E. HTTP
F. TFTP

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 422
Pete, a user, wishes to encrypt only certain files and folders within a partition. Which of the following methods should Matt, a technician, recommend?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 423
Which of the following can Jane, a security administrator, use to help prevent man-in-the-middle attacks?

A. HTTP

B. HTTPS
C. SFTP
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 424
Which of the following should Sara, a security administrator, implement on a mobile phone to help prevent a conversation from being captured?

A. Device encryption
B. Voice encryption
C. GPS tracking
D. Sniffer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 425
Which of the following access control methods provides the BEST protection against attackers logging on as authorized users?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 426
Which of the following should Matt, a security technician, integrate into the fire alarm systems to help prevent a fire from spreading?

A. HVAC
B. Humidity controls
C. Video monitoring
D. Thermostats

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 427
An in-line network device examines traffic and determines that a parameter within a common protocol is well outside of expected boundaries. This is an example of which of the following?

A. Anomaly based detection
B. Behavior based detection
C. IV attack detection
D. Signature based detection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 428
Jane, a malicious insider, obtains a copy of a virtual machine image for a server containing client financial records from the in-house virtualization cluster. Which of the following would BEST prevent Jane from accessing the client records?

A. Cloud computing
B. Separation of duties
C. Portable media encryption
D. File and folder encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 429
Which of the following is the MOST effective method to provide security for an in-house created application during software development?

A. Third-party white box testing of the completed application before it goes live
B. Third-party black box testing of the completed application before it goes live
C. Explicitly include security gates during the SDLC
D. Ensure an application firewall protects the application

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 430
Matt, an attacker, incorrectly submits data on a website's form and is able to determine the type of database used by the application and the SQL statements used to query that database. Which of the following is

responsible for this information disclosure?

A. SQL injection
B. Fuzzing
C. XSS
D. Error handling

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 431
Which of the following describes why Sara, the sender of an email, may encrypt the email with a private key?

A. Confidentiality
B. Non-repudiation
C. Transmission speed
D. Transport encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 432
Matt, a security technician, needs to increase his password's key space. Which of the following increases the key space of a password the MOST?

A. Letters, numbers, and special characters
B. 25 or more alpha-numeric characters
C. Two-factor authentication
D. Sequential alpha-numeric patterns

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 433
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 434
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. Virtualization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 435
An offsite location containing the necessary hardware without data redundancy would be an example of which of the following off-site contingency plans?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 436
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 437
Which of the following is BEST described as a scenario where organizational management decides not to

provide a service offering because it presents an unacceptable risk to the organization?

A. Mitigation
B. Acceptance
C. Deterrence
D. Avoidance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 438
Which of the following is the primary security reason why Pete, a security administrator, should block social networking sites in a large corporation?

A. The proxy server needs to be specially configured for all social networking sites.
B. The data traffic can cause system strain and can overwhelm the firewall rule sets.
C. The users' work productivity decreases greatly.
D. The users can unintentionally post sensitive company information.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 439
Which of the following describes the importance of enacting and maintaining a clean desk policy?

A. To ensure that data is kept on encrypted network shares
B. To avoid passwords and sensitive data from being unsecured
C. To verify that users are utilizing data storage resources
D. To guarantee that users comply with local laws and regulations

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 440
Matt, a security technician, is using TFTP. Which of the following port numbers is used for TFTP?

A. 22
B. 69
C. 80
D. 3389

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 441
Which of the following systems implements a secure key distribution system that relies on hardcopy keys intended for individual sessions?

A. Blowfish
B. PGP/GPG
C. One-time pads
D. PKI

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 442
Which of the following devices would Jane, a security administrator, typically use at the enclave boundary to inspect, block, and re-route network traffic for security purposes?

A. Load balancers
B. Protocol analyzers
C. Firewalls
D. Spam filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 443
Which of the following devices is Pete, a security administrator, MOST likely to install to prevent malicious attacks?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 444
Which of the following devices should Jane, a security administrator, use to allow secure remote network access for mobile users?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 445
Which of the following is capable of providing the HIGHEST encryption bit strength?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 446
Which of the following technologies is used to verify that a file was not altered?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 447
Which of the following, when used in conjunction with software-based encryption, enhances platform authentication by storing unique RSA keys and providing crypto processing?

A. LDAP
B. TPM
C. Kerberos
D. Biometrics

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

http://www.gratisexam.com/