CompTIA Testinside SY0-301 EXAM BUNDLE

Number: SY0-301
Passing Score: 800
Time Limit: 120 min
File Version: 16.6

Test Inside
Easiest Way To Pass It Exams

COMPTIA SY0-301 EXAM BUNDLE

Exam Name: Comptia CompTIA Security+ Certification Exam 2011 version

QUESTION 1
Which of the following is an example of a false positive?

A. Anti-virus identifies a benign application as malware.
B. A biometric iris scanner rejects an authorized user wearing a new contact lens.
C. A user account is locked out after the user mistypes the password too many times.
D. The IDS does not identify a buffer overflow.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
Data execution prevention is a feature in most operating systems intended to protect against which type of attack?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
Pete, the security engineer, would like to prevent wireless attacks on his network. Pete has implemented a security control to limit the connecting MAC addresses to a single port. Which of the following wireless attacks would this address?

A. Interference
B. Man-in-the-middle
C. ARP poisoning
D. Rogue access point

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
Which of the following can be implemented with multiple bit strength?

A. AES
B. DES

C. SHA-1

D. MD5

E. MD4

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide?

A. No competition with the company's official social presence

B. Protection against malware introduced by banner ads

C. Increased user productivity based upon fewer distractions

D. Elimination of risks caused by unauthorized P2P file sharing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
Pete, the system administrator, is reviewing his disaster recovery plans. He wishes to limit the downtime in the event of a disaster, but does not have the budget approval to implement or maintain an offsite location that ensures 99.99% availability. Which of the following would be
Pete's BEST option?

A. Use hardware already at an offsite location and configure it to be quickly utilized.

B. Move the servers and data to another part of the company's main campus from the server room.

C. Retain data back-ups on the main campus and establish redundant servers in a virtual environment.

D. Move the data back-ups to the offsite location, but retain the hardware on the main campus for redundancy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
A network stream needs to be encrypted. Sara, the network administrator, has selected a cipher which will

encrypt 8 bits at a time before sending the data across the network. Which of the following has Sara selected?

A. Block cipher
B. Stream cipher
C. CRC
D. Hashing algorithm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
Pete, a security auditor, has detected clear text passwords between the RADIUS server and the authenticator. Which of the following is configured in the RADIUS server and what technologies should the authentication protocol be changed to?

A. PAP, MSCHAPv2
B. CHAP, PAP
C. MSCHAPv2, NTLMv2
D. NTLM, NTLMv2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 53

QUESTION 9
Which of the following is an advantage of implementing individual file encryption on a hard drive which already deploys full disk encryption?

A. Reduces processing overhead required to access the encrypted files
B. Double encryption causes the individually encrypted files to partially lose their properties
C. Individually encrypted files will remain encrypted when copied to external media
D. File level access control only apply to individually encrypted files in a fully encrypted drive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
An IT director is looking to reduce the footprint of their company's server environment. They have decided to move several internally developed software applications to an alternate environment, supported by an external company. Which of the following BEST describes this arrangement?

A. Infrastructure as a Service
B. Storage as a Service

C. Platform as a Service

D. Software as a Service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site were facing the wrong direction to capture the incident. The analyst ensures the cameras are turned to face the proper direction. Which of the following types of controls is being used?

A. Detective

B. Deterrent

C. Corrective

D. Preventive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
The network administrator is responsible for promoting code to applications on a DMZ web server. Which of the following processes is being followed to ensure application integrity?

A. Application hardening

B. Application firewall review

C. Application change management

D. Application patch management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
An IT auditor tests an application as an authenticated user. This is an example of which of the following types of testing?

A. Penetration

B. White box

C. Black box

D. Gray box

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
The manager has a need to secure physical documents every night, since the company began enforcing the clean desk policy. The BEST solution would include: (Select TWO).

A. Fire- or water-proof safe.
B. Department door locks.
C. Proximity card.
D. 24-hour security guard.
E. Locking cabinets and drawers.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password?

A. Authentication server
B. Server certificate
C. Key length
D. EAP method

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
Some customers have reported receiving an untrusted certificate warning when visiting the company's website. The administrator ensures that the certificate is not expired and that customers have trusted the original issuer of the certificate. Which of the following could be causing the problem?

A. The intermediate CA certificates were not installed on the server.
B. The certificate is not the correct type for a virtual server.
C. The encryption key used in the certificate is too short.
D. The client's browser is trying to negotiate SSL instead of TLS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
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: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
A company's business model was changed to provide more web presence and now its ERM

software is no longer able to support the security needs of the company. The current data center will continue to provide network and security services. Which of the following network elements would be used to support the new business model?

A. Software as a Service
B. DMZ
C. Remote access support
D. Infrastructure as a Service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
Which of the following network devices is used to analyze traffic between various network interfaces?

A. Proxies
B. Firewalls
C. Content inspection
D. Sniffers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20

A network administrator needs to provide daily network usage reports on all layer 3 devices without compromising any data while gathering the information. Which of the following would be configured to provide these reports?

A. SNMP

B. SNMPv3
C. ICMP
D. SSH

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
A security administrator has been tasked to ensure access to all network equipment is controlled by a central server such as TACACS+. This type of implementation supports which of the following risk mitigation strategies?

A. User rights and permissions review
B. Change management
C. Data loss prevention
D. Implement procedures to prevent data theft

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
Which of the following types of authentication solutions use tickets to provide access to various resources from a central location?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
A corporation is looking to expand their data center but has run out of physical space in which to store hardware. Which of the following would offer the ability to expand while keeping their current data center operated by internal staff?

A. Virtualization
B. Subnetting
C. IaaS
D. SaaS

Correct Answer: A

QUESTION 24
Which of the following concepts is enforced by certifying that email communications have been sent by who the message says it has been sent by?

A. Key escrow
B. Non-repudiation
C. Multifactor authentication
D. Hashing

Correct Answer: B

QUESTION 25
After a recent breach, the security administrator performs a wireless survey of the corporate network. The security administrator notices a problem with the following output:

MACSSIDENCRYPTIONPOWERBEACONS

00:10:A1:36:12:CCMYCORPWPA2 CCMP601202

00:10:A1:49:FC:37MYCORPWPA2 CCMP709102

FB:90:11:42:FA:99MYCORPWPA2 CCMP403031

00:10:A1:AA:BB:CCMYCORPWPA2 CCMP552021

00:10:A1:FA:B1:07MYCORPWPA2 CCMP306044

Given that the corporate wireless network has been standardized, which of the following attacks is underway?

A. Evil twin
B. IV attack
C. Rogue AP
D. DDoS

Correct Answer: A

QUESTION 26
Input validation is an important security defense because it:

A. rejects bad or malformed data.

B. enables verbose error reporting.

C. protects mis-configured web servers.

D. prevents denial of service attacks.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
In order to maintain oversight of a third party service provider, the company is going to implement a Governance, Risk, and Compliance (GRC) system. This system is promising to provide overall security posture coverage. Which of the following is the MOST important activity that should be considered?

A. Continuous security monitoring

B. Baseline configuration and host hardening

C. Service Level Agreement (SLA) monitoring

D. Security alerting and trending

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
A recent audit of a company's identity management system shows that 30% of active accounts belong to people no longer with the firm. Which of the following should be performed to help avoid

this scenario? (Select TWO).

A. Automatically disable accounts that have not been utilized for at least 10 days.

B. Utilize automated provisioning and de-provisioning processes where possible.

C. Request that employees provide a list of systems that they have access to prior to leaving the firm.

D. Perform regular user account review / revalidation process.

E. Implement a process where new account creations require management approval.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
The Chief Information Officer (CIO) has mandated web based Customer Relationship Management (CRM) business functions be moved offshore to reduce cost, reduce IT overheads, and improve availability. The Chief Risk Officer (CRO) has agreed with the CIO's direction but has mandated that key authentication systems be run within the organization's network. Which of the following would BEST meet the CIO and CRO's requirements?

A. Software as a Service

B. Infrastructure as a Service
C. Platform as a Service
D. Hosted virtualization service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
An administrator connects VoIP phones to the same switch as the network PCs and printers. Which of the following would provide the BEST logical separation of these three device types while still allowing traffic between them via ACL?

A. Create three VLANs on the switch connected to a router
B. Define three subnets, configure each device to use their own dedicated IP address range, and then connect the network to a router
C. Install a firewall and connect it to the switch
D. Install a firewall and connect it to a dedicated switch for each device type

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
Which of the following wireless security measures can an attacker defeat by spoofing certain properties of their network interface card?

A. WEP
B. MAC filtering
C. Disabled SSID broadcast
D. TKIP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
Which of the following provides additional encryption strength by repeating the encryption process with additional keys?

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

Correct Answer: B

QUESTION 33
Which of the following BEST describes part of the PKI process?

A. User1 decrypts data with User2's private key
B. User1 hashes data with User2's public key
C. User1 hashes data with User2's private key
D. User1 encrypts data with User2's public key

Correct Answer: D

QUESTION 34
Two members of the finance department have access to sensitive information. The company is concerned they may work together to steal information. Which of the following controls could be implemented to discover if they are working together?

A. Least privilege access
B. Separation of duties
C. Mandatory access control
D. Mandatory vacations

Correct Answer: D

QUESTION 35
A system administrator attempts to ping a hostname and the response is 2001:4860:0:2001::68. Which of the following replies has the administrator received?

A. The loopback address
B. The local MAC address
C. IPv4 address
D. IPv6 address

Correct Answer: D

QUESTION 36
Which of the following is a best practice when a mistake is made during a forensics examination?

A. The examiner should verify the tools before, during, and after an examination.
B. The examiner should attempt to hide the mistake during cross-examination.
C. The examiner should document the mistake and workaround the problem.
D. The examiner should disclose the mistake and assess another area of the disc.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
Which of the following allows lower level domains to access resources in a separate Public Key Infrastructure?

A. Trust Model
B. Recovery Agent
C. Public Key
D. Private Key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 38
Which of the following offers the LEAST secure encryption capabilities?

A. TwoFish
B. PAP
C. NTLM
D. CHAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 39
Which of the following network architecture concepts is used to securely isolate at the boundary between networks?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
Elastic cloud computing environments often reuse the same physical hardware for multiple customers over time as virtual machines are instantiated and deleted. This has important implications for which of the following data security concerns?

A. Hardware integrity
B. Data confidentiality
C. Availability of servers
D. Integrity of data

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 41
When implementing fire suppression controls in a datacenter it is important to:

A. Select a fire suppression system which protects equipment but may harm technicians.
B. Ensure proper placement of sprinkler lines to avoid accidental leakage onto servers.
C. Integrate maintenance procedures to include regularly discharging the system.
D. Use a system with audible alarms to ensure technicians have 20 minutes to evacuate.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 42
Vendors typically ship software applications with security settings disabled by default to ensure a wide range of interoperability with other applications and devices. A security administrator should perform which of the following before deploying new software?

A. Application white listing
B. Network penetration testing
C. Application hardening
D. Input fuzzing testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
Mandatory vacations are a security control which can be used to uncover which of the following?

A. Fraud committed by a system administrator
B. Poor password security among users
C. The need for additional security staff
D. Software vulnerabilities in vendor code

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 44
Each server on a subnet is configured to only allow SSH access from the administrator's workstation. Which of the following BEST describes this implementation?

A. Host-based firewalls
B. Network firewalls
C. Network proxy
D. Host intrusion prevention

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 45
In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified?

A. Security control frameworks
B. Best practice
C. Access control methodologies
D. Compliance activity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 46
Disabling unnecessary services, restricting administrative access, and enabling auditing controls on a server are forms of which of the following?

A. Application patch management
B. Cross-site scripting prevention
C. Creating a security baseline
D. System hardening

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
A system administrator has noticed vulnerability on a high impact production server. A recent update was made available by the vendor that addresses the vulnerability but requires a reboot of the system afterwards. Which of the following steps should the system administrator implement to address the vulnerability?

A. Test the update in a lab environment, schedule downtime to install the patch, install the patch and reboot the server and monitor for any changes
B. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the patch, and monitor for any changes
C. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the update, reboot the server, and monitor for any changes
D. Backup the server, schedule downtime to install the patch, installs the patch and monitor for any changes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Topic 3, Volume C

QUESTION 48
Which of the following services are used to support authentication services for several local devices from a central location without the use of tokens?

A. TACACS+
B. Smartcards
C. Biometrics
D. Kerberos

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 71

QUESTION 49
A network administrator has recently updated their network devices to ensure redundancy is in place so that:

A. switches can redistribute routes across the network.
B. environmental monitoring can be performed.
C. single points of failure are removed.
D. hot and cold aisles are functioning.

Correct Answer: C

QUESTION 50
A network administrator recently updated various network devices to ensure redundancy throughout the network. If an interface on any of the Layer 3 devices were to go down, traffic will still pass through another interface and the production environment would be unaffected. This type of configuration represents which of the following concepts?

A. High availability
B. Load balancing
C. Backout contingency plan
D. Clustering

Correct Answer: A

QUESTION 51
A system administrator needs to ensure that certain departments have more restrictive controls to their shared folders than other departments. Which of the following security controls would be implemented to restrict those departments?

A. User assigned privileges
B. Password disablement
C. Multiple account creation
D. Group based privileges

Correct Answer: D

QUESTION 52
A network analyst received a number of reports that impersonation was taking place on the network. Session tokens were deployed to mitigate this issue and defend against which of the following attacks?

A. Replay
B. DDoS
C. Smurf
D. Ping of Death

Correct Answer: A

QUESTION 53
Which of the following controls would prevent an employee from emailing unencrypted information to their personal email account over the corporate network?

A. DLP
B. CRL
C. TPM
D. HSM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
Which of the following is a measure of biometrics performance which rates the ability of a system to correctly authenticate an authorized user?

A. Failure to capture
B. Type II
C. Mean time to register
D. Template capacity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
A software development company wants to implement a digital rights management solution to protect its intellectual property. Which of the following should the company implement to enforce software digital rights?

A. Transport encryption
B. IPsec
C. Non-repudiation
D. Public key infrastructure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
Users are unable to connect to the web server at IP 192.168.0.20. Which of the following can be inferred of a firewall that is configured ONLY with the following ACL?
PERMIT TCP ANY HOST 192.168.0.10 EQ 80

PERMIT TCP ANY HOST 192.168.0.10 EQ 443

A. It implements stateful packet filtering.
B. It implements bottom-up processing.
C. It failed closed.
D. It implements an implicit deny.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 57
Which of the following security awareness training is BEST suited for data owners who are concerned with protecting the confidentiality of their data?

A. Social networking use training
B. Personally owned device policy training
C. Tailgating awareness policy training
D. Information classification training

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
A security administrator is concerned about the strength of user's passwords. The company does not want to implement a password complexity policy. Which of the following can the security administrator implement to mitigate the risk of an online password attack against users with weak passwords?

A. Increase the password length requirements
B. Increase the password history
C. Shorten the password expiration period
D. Decrease the account lockout time

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 75

QUESTION 59
Which of the following are Data Loss Prevention (DLP) strategies that address data in transit issues? (Select TWO).

A. Scanning printing of documents.
B. Scanning of outbound IM (Instance Messaging).
C. Scanning copying of documents to USB.
D. Scanning of SharePoint document library.

E. Scanning of shared drives.

F. Scanning of HTTP user traffic.

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 60
A user casually browsing the Internet is redirected to a warez site where a number of pop-ups appear. After clicking on a pop-up to complete a survey, a drive-by download occurs. Which of the following is MOST likely to be contained in the download?

A. Backdoor

B. Spyware

C. Logic bomb

D. DDoS

E. Smurf

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 61
A security administrator plans on replacing a critical business application in five years. Recently, there was a security flaw discovered in the application that will cause the IT department to manually re-enable user accounts each month at a cost of $2,000. Patching the application today would cost $140,000 and take two months to implement. Which of the following should the security administrator do in regards to the application?

A. Avoid the risk to the user base allowing them to re-enable their own accounts

B. Mitigate the risk by patching the application to increase security and saving money

C. Transfer the risk replacing the application now instead of in five years

D. Accept the risk and continue to enable the accounts each month saving money

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 62
Purchasing receives a phone call from a vendor asking for a payment over the phone. The phone number displayed on the caller ID matches the vendor's number. When the purchasing agent asks to call the vendor back, they are given a different phone number with a different area code. Which of the following attack types is this?

A. Hoax

B. Impersonation

C. Spear phishing

D. Whaling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 63
Purchasing receives an automated phone call from a bank asking to input and verify credit card information. The phone number displayed on the caller ID matches the bank. Which of the following attack types is this?

A. Hoax
B. Phishing
C. Vishing
D. Whaling

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 64
An information bank has been established to store contacts, phone numbers and other records. A UNIX application needs to connect to the index server using port 389. Which of the following authentication services should be used on this port by default?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 65
An internal auditor is concerned with privilege creep that is associated with transfers inside the company. Which mitigation measure would detect and correct this?

A. User rights reviews
B. Least privilege and job rotation
C. Change management
D. Change Control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 66
Which of the following is the default port for TFTP?

A. 20
B. 69
C. 21
D. 68

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 79

QUESTION 67
Which of the following concepts allows an organization to group large numbers of servers together in order to deliver a common service?

A. Clustering
B. RAID
C. Backup Redundancy
D. Cold site

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 68
Which of the following security concepts identifies input variables which are then used to perform boundary testing?

A. Application baseline
B. Application hardening
C. Secure coding
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 69
Which of the following cryptographic related browser settings allows an organization to communicate securely?

A. SSL 3.0/TLS 1.0
B. 3DES

C. Trusted Sites

D. HMAC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
Which of the following is the BEST reason to provide user awareness and training programs for organizational staff?

A. To ensure proper use of social media

B. To reduce organizational IT risk

C. To detail business impact analyses

D. To train staff on zero-days

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 71
A firewall technician has been instructed to disable all non-secure ports on a corporate firewall. The technician has blocked traffic on port 21, 69, 80, and 137-139. The technician has allowed traffic on ports 22 and 443. Which of the following correctly lists the protocols blocked and allowed?

A. Blocked: TFTP, HTTP, NetBIOS; Allowed: HTTPS, FTP

B. Blocked: FTP, TFTP, HTTP, NetBIOS; Allowed: SFTP, SSH, SCP, HTTPS

C. Blocked: SFTP, TFTP, HTTP, NetBIOS; Allowed: SSH, SCP, HTTPS

D. Blocked: FTP, HTTP, HTTPS; Allowed: SFTP, SSH, SCP, NetBIOS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 72
A system administrator is responding to a legal order to turn over all logs from all company servers. The system administrator records the system time of all servers to ensure that:

A. HDD hashes are accurate.

B. the NTP server works properly.

C. chain of custody is preserved.

D. time offset can be calculated.

Correct Answer: D
Section: (none)
Explanation

QUESTION 73
While rarely enforced, mandatory vacation policies are effective at uncovering:

A. Help desk technicians with oversight by multiple supervisors and detailed quality control systems.
B. Collusion between two employees who perform the same business function.
C. Acts of incompetence by a systems engineer designing complex architectures as a member of a team.
D. Acts of gross negligence on the part of system administrators with unfettered access to system and no oversight.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 74
A company hires outside security experts to evaluate the security status of the corporate network. All of the company's IT resources are outdated and prone to crashing. The company requests that all testing be performed in a way which minimizes the risk of system failures. Which of the following types of testing does the company want performed?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 83

QUESTION 75
A security administrator notices that a specific network administrator is making unauthorized changes to the firewall every Saturday morning. Which of the following would be used to mitigate this issue so that only security administrators can make changes to the firewall?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 76
A security administrator notices large amounts of traffic within the network heading out to an external website. The website seems to be a fake bank site with a phone number that when called, asks for sensitive information. After further investigation, the security administrator notices that a fake link was sent to several users. This is an example of which of the following attacks?

A. Vishing
B. Phishing
C. Whaling
D. SPAM
E. SPIM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 77
After a user performed a war driving attack, the network administrator noticed several similar markings where WiFi was available throughout the enterprise. Which of the following is the term used to describe these markings?

A. IV attack
B. War dialing
C. Rogue access points
D. War chalking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 78
The system administrator notices that their application is no longer able to keep up with the large amounts of traffic their server is receiving daily. Several packets are dropped and sometimes the server is taken offline. Which of the following would be a possible solution to look into to ensure their application remains secure and available?

A. Cloud computing
B. Full disk encryption
C. Data Loss Prevention
D. HSM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 79

After a recent internal audit, the security administrator was tasked to ensure that all credentials must be changed within 90 days, cannot be repeated, and cannot contain any dictionary words or patterns. All credentials will remain enabled regardless of the number of attempts made. Which of the following types of user account options were enforced? (Select TWO).

A. Recovery
B. User assigned privileges
C. Lockout
D. Disablement
E. Group based privileges
F. Password expiration
G. Password complexity

Correct Answer: FG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 85

QUESTION 80
A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive's laptop they notice several pictures of the employee's pets are on the hard drive and on a cloud storage network. When the analyst hashes the images on the hard drive against the hashes on the cloud network they do not match. Which of the following describes how the employee is leaking these secrets?

A. Social engineering
B. Steganography
C. Hashing
D. Digital signatures

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 81
During a routine audit a web server is flagged for allowing the use of weak ciphers. Which of the following should be disabled to mitigate this risk? (Select TWO).

A. SSL 1.0
B. RC4
C. SSL 3.0
D. AES
E. DES
F. TLS 1.0

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 82
Review the following diagram depicting communication between PC1 and PC2 on each side of a router.
Analyze the network traffic logs which show communication between the two computers as captured by the
computer with IP 10.2.2.10.

DIAGRAM

PC1 PC2

[192.168.1.30]--------[INSIDE 192.168.1.1 router OUTSIDE 10.2.2.1]---------[10.2.2.10]

LOGS

10:30:22, SRC 10.2.2.1:3030, DST 10.2.2.10:80, SYN

10:30:23, SRC 10.2.2.10:80, DST 10.2.2.1:3030, SYN/ACK

10:30:24, SRC 10.2.2.1:3030, DST 10.2.2.10:80, ACK

Given the above information, which of the following can be inferred about the above environment?

A. 192.168.1.30 is a web server.
B. The web server listens on a non-standard port.
C. The router filters port 80 traffic.
D. The router implements NAT.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 83
The Chief Information Officer (CIO) wants to implement a redundant server location to which the production
server images can be moved within 48 hours and services can be quickly restored, in case of a catastrophic
failure of the primary datacenter's HVAC. Which of the following can be implemented?

A. Cold site
B. Load balancing
C. Warm site
D. Hot site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 84
The security administrator is observing unusual network behavior from a workstation. The workstation is
communicating with a known malicious destination over an encrypted tunnel. A full antivirus scan, with an

updated antivirus definition file, does not show any signs of infection. Which of the following has happened on the workstation?

A. Zero-day attack
B. Known malware infection
C. Session hijacking
D. Cookie stealing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 85
Which of the following controls can be used to prevent the disclosure of sensitive information stored on a mobile device's removable media in the event that the device is lost or stolen?

A. Hashing
B. Screen locks
C. Device password
D. Encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 86
Which of the following should be performed to increase the availability of IP telephony by prioritizing traffic?

A. Subnetting
B. NAT
C. Quality of service
D. NAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 87
A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

A. ICMP
B. BGP
C. NetBIOS
D. DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 88
Which of the following assets is MOST likely considered for DLP?

A. Application server content
B. USB mass storage devices
C. Reverse proxy
D. Print server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 89
In order to securely communicate using PGP, the sender of an email must do which of the
following when sending an email to a recipient for the first time?

A. Import the recipient's public key
B. Import the recipient's private key
C. Export the sender's private key
D. Export the sender's public key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 90
A security specialist has been asked to evaluate a corporate network by performing a vulnerability assessment.
Which of the following will MOST likely be performed?

A. Identify vulnerabilities, check applicability of vulnerabilities by passively testing security controls.
B. Verify vulnerabilities exist, bypass security controls and exploit the vulnerabilities.
C. Exploit security controls to determine vulnerabilities and mis-configurations.
D. Bypass security controls and identify applicability of vulnerabilities by passively testing security controls.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 90

QUESTION 91
A security technician is attempting to access a wireless network protected with WEP. The technician does not know any information about the network. Which of the following should the technician do to gather information about the configuration of the wireless network?

A. Spoof the MAC address of an observed wireless network client
B. Ping the access point to discover the SSID of the network
C. Perform a dictionary attack on the access point to enumerate the WEP key
D. Capture client to access point disassociation packets to replay on the local PC's loopback

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 92
A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks. Which of the following is MOST likely the reason for the sub-interfaces?

A. The network uses the subnet of 255.255.255.128.
B. The switch has several VLANs configured on it.
C. The sub-interfaces are configured for VoIP traffic.
D. The sub-interfaces each implement quality of service.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 93
Which of the following should be enabled in a laptop's BIOS prior to full disk encryption?

A. USB
B. HSM
C. RAID
D. TPM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 94
Company employees are required to have workstation client certificates to access a bank website. These certificates were backed up as a precautionary step before the new computer upgrade. After the upgrade and restoration, users state they can access the bank's website, but not login.
Which is the following is MOST likely the issue?

A. The IP addresses of the clients have change
B. The client certificate passwords have expired on the server
C. The certificates have not been installed on the workstations
D. The certificates have been installed on the CA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 95
Digital Signatures provide which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 96
A user ID and password together provide which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 97
A recent intrusion has resulted in the need to perform incident response procedures. The incident response team has identified audit logs throughout the network and organizational systems which hold details of the security breach. Prior to this incident, a security consultant informed the company that they needed to implement an NTP server on the network. Which of the following is a problem that the incident response team will likely encounter during their assessment?

A. Chain of custody
B. Tracking man hours
C. Record time offset
D. Capture video traffic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 98
A recent computer breach has resulted in the incident response team needing to perform a forensics examination. Upon examination, the forensics examiner determines that they cannot tell which captured hard drive was from the device in question. Which of the following would have prevented the confusion experienced during this examination?

A. Perform routine audit
B. Chain of custody
C. Evidence labeling
D. Hashing the evidence

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 99
During a recent user awareness and training session, a new staff member asks the Chief Information Security Officer (CISO) why the company does not allow personally owned devices into the company facilities. Which of the following represents how the CISO should respond?

A. Company A views personally owned devices as creating an unacceptable risk to the organizational IT systems.
B. Company A has begun to see zero-day attacks against personally owned devices disconnected from the network.
C. Company A believes that staff members should be focused on their work while in the company's facilities.
D. Company A has seen social engineering attacks against personally owned devices and does not allow their use.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 100
A user has received an email from an external source which asks for details on the company's new product line set for release in one month. The user has a detailed spec sheet but it is marked "Internal Proprietary Information". Which of the following should the user do NEXT?

A. Contact their manager and request guidance on how to best move forward
B. Contact the help desk and/or incident response team to determine next steps
C. Provide the requestor with the email information since it will be released soon anyway
D. Reply back to the requestor to gain their contact information and call them

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 101
Which of the following techniques enables a highly secured organization to assess security weaknesses in real time?

A. Access control lists
B. Continuous monitoring
C. Video surveillance
D. Baseline reporting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 102
Encryption of data at rest is important for sensitive information because of which of the following?

A. Facilitates tier 2 support, by preventing users from changing the OS
B. Renders the recovery of data harder in the event of user password loss
C. Allows the remote removal of data following eDiscovery requests
D. Prevents data from being accessed following theft of physical equipment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 103
A network administrator noticed various chain messages have been received by the company. Which of the following security controls would need to be implemented to mitigate this issue?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 104
Which of the following types of application attacks would be used to specifically gain unauthorized information

from databases that did not have any input validation implemented?

A. SQL injection
B. Session hijacking and XML injection
C. Cookies and attachments
D. Buffer overflow and XSS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 105
Which of the following should be deployed to prevent the transmission of malicious traffic between virtual machines hosted on a singular physical device on a network?

A. HIPS on each virtual machine
B. NIPS on the network
C. NIDS on the network
D. HIDS on each virtual machine

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 106
A security administrator wants to get a real time look at what attackers are doing in the wild, hoping to lower the risk of zero-day attacks. Which of the following should be used to accomplish this goal?

A. Penetration testing
B. Honeynets
C. Vulnerability scanning
D. Baseline reporting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 107
Which of the following protocols is the security administrator observing in this packet capture?

12:33:43, SRC 192.168.4.3:3389, DST 10.67.33.20:8080, SYN/ACK

A. HTTPS
B. RDP
C. HTTP
D. SFTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 108
Which of the following is true about asymmetric encryption?

A. A message encrypted with the private key can be decrypted by the same key
B. A message encrypted with the public key can be decrypted with a shared key.
C. A message encrypted with a shared key, can be decrypted by the same key.
D. A message encrypted with the public key can be decrypted with the private key.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 109
Which of the following is true about an email that was signed by User A and sent to User B?

A. User A signed with User B's private key and User B verified with their own public key.
B. User A signed with their own private key and User B verified with User A's public key.
C. User A signed with User B's public key and User B verified with their own private key.
D. User A signed with their own public key and User B verified with User A's private key.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 110
The Chief Information Officer (CIO) is concerned with moving an application to a SaaS cloud provider. Which of the following can be implemented to provide for data confidentiality assurance during and after the migration to the cloud?

A. HPM technology
B. Full disk encryption
C. DLP policy
D. TPM technology

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 111
Which of the following protocols encapsulates an IP packet with an additional IP header?

A. SFTP
B. IPSec
C. HTTPS
D. SSL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 112
A program has been discovered that infects a critical Windows system executable and stays dormant in memory. When a Windows mobile phone is connected to the host, the program infects the phone's boot loader and continues to target additional Windows PCs or phones. Which of the following malware categories BEST describes this program?

A. Zero-day
B. Trojan
C. Virus
D. Rootkit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 113
A user has unknowingly gone to a fraudulent site. The security analyst notices the following system change on the user's host:

Old `hosts' file:

127.0.0.1 localhost

New `hosts' file:

127.0.0.1 localhost

5.5.5.5 www.comptia.com

Which of the following attacks has taken place?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 114
An investigator recently discovered that an attacker placed a remotely accessible CCTV camera in a public area overlooking several Automatic Teller Machines (ATMs). It is also believed that user accounts belonging to ATM operators may have been compromised. Which of the following attacks has MOST likely taken place?

A. Shoulder surfing
B. Dumpster diving
C. Whaling attack
D. Vishing attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 115
An attacker attempted to compromise a web form by inserting the following input into the username field:

admin)(|(password=*))

 Which of the following types of attacks was attempted?

A. SQL injection
B. Cross-site scripting
C. Command injection
D. LDAP injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 116
Which of the following is BEST carried out immediately after a security breach is discovered?

A. Risk transference
B. Access control revalidation
C. Change management
D. Incident management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 117
Which of the following is a hardware-based security technology included in a computer?

A. Symmetric key
B. Asymmetric key
C. Whole disk encryption
D. Trusted platform module

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 118
 How often, at a MINIMUM, should Sara, an administrator, review the accesses and right of the users on her system?

A. Annually
B. Immediately after an employee is terminated
C. Every five years
D. Every time they patch the server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 119
An administrator is concerned that a company's web server has not been patched. Which of the following would be the BEST assessment for the administrator to perform?

A. Vulnerability scan
B. Risk assessment
C. Virus scan
D. Network sniffer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 120

A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:

A. Logic bomb.
B. Backdoor.
C. Adware application.
D. Rootkit.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 121
Which of the following protocols uses TCP instead of UDP and is incompatible with all previous versions?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 122
Which of the following symmetric key algorithms are examples of block ciphers? (Select THREE).

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

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 111

QUESTION 123
Which of the following devices will help prevent a laptop from being removed from a certain location?

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

D. Remote data wipes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 124
Which of the following BEST describes a protective countermeasure for SQL injection?

A. Eliminating cross-site scripting vulnerabilities
B. Installing an IDS to monitor network traffic
C. Validating user input in web applications
D. Placing a firewall between the Internet and database servers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 125
Which of the following MOST interferes with network-based detection techniques?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 126
A certificate authority takes which of the following actions in PKI?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 127
Separation of duties is often implemented between developers and administrators in order to

separate which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 128
A security administrator needs to update the OS on all the switches in the company. Which of the following MUST be done before any actual switch configuration is performed?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 129
A user in the company is in charge of various financial roles but needs to prepare for an upcoming audit. They use the same account to access each financial system. Which of the following security controls will MOST likely be implemented within the company?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 130
A CRL is comprised of:

A. Malicious IP addresses.
B. Trusted CA's.
C. Untrusted private keys.
D. Public keys.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 131
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: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 132
Which of the following should be considered to mitigate data theft when using CAT5 wiring?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 133
To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 10

QUESTION 134

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 135
Use of group accounts should be minimized to ensure which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 136
Privilege creep among long-term employees can be mitigated by which of the following procedures?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 137
In which of the following scenarios is PKI LEAST hardened?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 138
Configuring the mode, encryption methods, and security associations are part of which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 139
Which of the following assessments would Pete, the security administrator, use to actively test that an application's security controls are in place?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 140
A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

A. Confidentiality
B. Availability
C. Succession planning
D. Integrity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 141

In the initial stages of an incident response, Matt, the security administrator, was provided the hard drives in question from the incident manager. Which of the following incident response procedures would he need to perform in order to begin the analysis? (Select TWO).

A. Take hashes
B. Begin the chain of custody paperwork
C. Take screen shots
D. Capture the system image
E. Decompile suspicious files

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 142
Which of the following is used to certify intermediate authorities in a large PKI deployment?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 143
Which of the following components MUST be trusted by all parties in PKI?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 144
Which of the following should Matt, a security administrator, include when encrypting smartphones? (Select TWO).

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

E. Public keys

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 145
Which of the following is the below pseudo-code an example of?

IF VARIABLE (CONTAINS NUMBERS = TRUE) THEN EXIT

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 146
A system administrator is using a packet sniffer to troubleshoot remote authentication. The administrator detects a device trying to communicate to TCP port 49. Which of the following authentication methods is MOST likely being attempted?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 147
Which of the following can use RC4 for encryption? (Select TWO).

A. CHAP
B. SSL
C. WEP
D. AES
E. 3DES

Correct Answer: BC
Section: (none)
Explanation

QUESTION 148
Which of the following defines a business goal for system restoration and acceptable data loss?

A. MTTR
B. MTBF
C. RPO
D. Warm site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 149
If Organization A trusts Organization B and Organization B trusts Organization C, then Organization A trusts Organization C. Which of the following PKI concepts is this describing?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 150
Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency?

A. Business continuity planning
B. Continuity of operations
C. Business impact analysis
D. Succession planning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 151
Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 152
Please be aware that if you do not accept these terms you will not be allowed to take this CompTIA exam and you will forfeit the fee paid.

A. RETURN TO EXAM
B. EXIT EXAM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 153
Which of the following is the MOST secure protocol to transfer files?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 154
A company storing data on a secure server wants to ensure it is legally able to dismiss and prosecute staff who intentionally access the server via Telnet and illegally tamper with customer data. Which of the following administrative controls should be implemented to BEST achieve this?

A. Command shell restrictions
B. Restricted interface
C. Warning banners
D. Session output pipe to /dev/null

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 155
Which of the following protocols is used to authenticate the client and server's digital certificate?

A. PEAP
B. DNS
C. TLS
D. ICMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 156
Which of the following security concepts would Sara, the security administrator, use to mitigate the risk of data loss?

A. Record time offset
B. Clean desk policy
C. Cloud computing
D. Routine log review

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 157
Which of the following is an example of multifactor authentication?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 158
After Matt, a user, enters his username and password at the login screen of a web enabled portal, the following appears on his screen:

`Please only use letters and numbers on these fields'

Which of the following is this an example of?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 159
Several bins are located throughout a building for secure disposal of sensitive information. Which of the following does this prevent?

A. Dumpster diving
B. War driving
C. Tailgating
D. War chalking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 160
Matt, a developer, recently attended a workshop on a new application. The developer installs the new application on a production system to test the functionality. Which of the following is MOST likely affected?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 161
Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 25

QUESTION 162
Mike, a security professional, is tasked with actively verifying the strength of the security controls on a company's live modem pool. Which of the following activities is MOST appropriate?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 163
Users at a company report that a popular news website keeps taking them to a web page with derogatory content. This is an example of which of the following?

A. Evil twin
B. DNS poisoning
C. Vishing
D. Session hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 164
Jane, a security administrator, has observed repeated attempts to break into a server. Which of the following is designed to stop an intrusion on a specific server?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 165
Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

A. Create a VLAN without a default gateway.
B. Remove the network from the routing table.
C. Create a virtual switch.
D. Commission a stand-alone switch.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 166
A security administrator implements access controls based on the security classification of the data and need-to-know information. Which of the following BEST describes this level of access control?

A. Implicit deny
B. Role-based Access Control
C. Mandatory Access Controls
D. Least privilege

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 167
Which of the following could cause a browser to display the message below?

"The security certificate presented by this website was issued for a different website's address."

A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAs.
B. The website is using a wildcard certificate issued for the company's domain.
C. HTTPS://127.0.01 was used instead of HTTPS://localhost.
D. The website is using an expired self signed certificate.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 168
A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

A. Availability
B. Integrity
C. Confidentiality
D. Fire suppression

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 169
Which of the following technologies uses multiple devices to share work?

A. Switching
B. Load balancing
C. RAID
D. VPN concentrator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 170
Which of the following protocols uses an asymmetric key to open a session and then establishes a symmetric key for the remainder of the session?

A. SFTP
B. HTTPS
C. TFTP
D. TLS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 171
Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device?

A. Man-in-the-middle
B. Bluejacking
C. Bluesnarfing
D. Packet sniffing

Correct Answer: B
Section: (none)
Explanation

QUESTION 172
Pete, an employee, is terminated from the company and the legal department needs documents from his encrypted hard drive. Which of the following should be used to accomplish this task? (Select TWO).

A. Private hash
B. Recovery agent
C. Public key
D. Key escrow
E. CRL

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 173
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:
Explanation:

QUESTION 174
Jane, an administrator, needs to make sure the wireless network is not accessible from the parking area of their office. Which of the following would BEST help Jane when deploying a new access point?

A. Placement of antenna
B. Disabling the SSID
C. Implementing WPA2
D. Enabling the MAC filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 175
Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

A. Implement WPA
B. Disable SSID
C. Adjust antenna placement
D. Implement WEP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 176
Which of the following is a management control?

A. Logon banners
B. Written security policy
C. SYN attack prevention
D. Access Control List (ACL)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 177
Which of the following security strategies allows a company to limit damage to internal systems and provides
loss control?

A. Restoration and recovery strategies
B. Deterrent strategies
C. Containment strategies
D. Detection strategies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 178
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

QUESTION 179
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

QUESTION 180
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

QUESTION 181
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

QUESTION 182
Which of the following can be used on a smartphone to BEST protect against sensitive data loss if the device is stolen? (Select TWO).

A. Tethering
B. Screen lock PIN
C. Remote wipe
D. Email password
E. GPS tracking
F. Device encryption

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 183
Jane, a security analyst, is reviewing logs from hosts across the Internet which her company uses to gather data on new malware. Which of the following is being implemented by Jane's company?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 184
Which of the following should Pete, a security manager, implement to reduce the risk of employees working in collusion to embezzle funds from their company?

A. Privacy Policy
B. Least Privilege
C. Acceptable Use
D. Mandatory Vacations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Topic 2, Volume B

QUESTION 185
Which of the following will allow Pete, a security analyst, to trigger a security alert because of a tracking cookie?

A. Network based firewall
B. Anti-spam software
C. Host based firewall
D. Anti-spyware software

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 186
Which of the following protocols allows for secure transfer of files? (Select TWO).

A. ICMP
B. SNMP
C. SFTP
D. SCP
E. TFTP

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 187
Which of the following passwords is the LEAST complex?

A. MyTrain!45
B. Mytr@in!!
C. MyTr@in12
D. MyTr@in#8

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 188
During a penetration test from the Internet, Jane, the system administrator, was able to establish a connection to an internal router, but not successfully log in to it. Which ports and protocols are MOST likely to be open on the firewall? (Select FOUR).

A. 21
B. 22
C. 23
D. 69
E. 3389
F. SSH
G. Terminal services
H. Rlogin
I. Rsync
J. Telnet

Correct Answer: BCFJ
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 189
Which of the following is an application security coding problem?

A. Error and exception handling
B. Patch management
C. Application hardening
D. Application fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 190
An IT security technician needs to establish host based security for company workstations. Which of the following will BEST meet this requirement?

A. Implement IIS hardening by restricting service accounts.
B. Implement database hardening by applying vendor guidelines.
C. Implement perimeter firewall rules to restrict access.
D. Implement OS hardening by applying GPOs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 191
Which of the following is the MOST specific plan for various problems that can arise within a system?

A. Business Continuity Plan
B. Continuity of Operation Plan
C. Disaster Recovery Plan
D. IT Contingency Plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 192

Which of the following BEST describes the weakness in WEP encryption?

A. The initialization vector of WEP uses a crack-able RC4 encryption algorithm. Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived.
B. The WEP key is stored in plain text and split in portions across 224 packets of random data.
Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key.
C. The WEP key has a weak MD4 hashing algorithm used. A simple rainbow table can be used to generate key possibilities due to MD4 collisions.
D. The WEP key is stored with a very small pool of random numbers to make the cipher text. As the random numbers are often reused it becomes easy to derive the remaining WEP key.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 193
Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years.
Which of the following should Sara do to address the risk?

A. Accept the risk saving $10,000.
B. Ignore the risk saving $5,000.
C. Mitigate the risk saving $10,000.
D. Transfer the risk saving $5,000.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 194
Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 195
Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

A. Input validation
B. Network intrusion detection system
C. Anomaly-based HIDS
D. Peer review

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 196
Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection?

A. Sign in and sign out logs
B. Mantrap
C. Video surveillance
D. HVAC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 197
Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

A. Water base sprinkler system
B. Electrical
C. HVAC
D. Video surveillance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 198
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

Explanation/Reference:
Explanation:

~ 40

QUESTION 199
Which of the following fire suppression systems is MOST likely used in a datacenter?

A. FM-200
B. Dry-pipe
C. Wet-pipe
D. Vacuum

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 200
A security administrator has installed a new KDC for the corporate environment. Which of the following authentication protocols is the security administrator planning to implement across the organization?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 201
While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks?

A. Cross-site scripting
B. Buffer overflow
C. Header manipulation
D. Directory traversal

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 41

QUESTION 202
A security technician is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks the security technician to explain the access control type found in a firewall. With which of the following should the security technician respond?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 203
Jane, a security administrator, has been tasked with explaining authentication services to the company's management team. The company runs an active directory infrastructure. Which of the following solutions BEST relates to the host authentication protocol within the company's environment?

A. Kerberos
B. Least privilege
C. TACACS+
D. LDAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 204
Pete, the compliance manager, wants to meet regulations. Pete would like certain ports blocked only on all computers that do credit card transactions. Which of the following should Pete implement to BEST achieve this goal?

A. A host-based intrusion prevention system
B. A host-based firewall
C. Antivirus update system
D. A network-based intrusion detection system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 205
Pete, the system administrator, wishes to monitor and limit users' access to external websites.
Which of the following would BEST address this?

A. Block all traffic on port 80.
B. Implement NIDS.
C. Use server load balancers.
D. Install a proxy server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 206
Sara, the security administrator, must configure the corporate firewall to allow all public IP addresses on the internal interface of the firewall to be translated to one public IP address on the external interface of the same firewall. Which of the following should Sara configure?

A. PAT
B. NAP
C. DNAT
D. NAC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 207
Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability?

A. Twofish
B. Diffie-Hellman
C. ECC
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 208
Methods to test the responses of software and web applications to unusual or unexpected inputs is known as:

A. Brute force.
B. HTML encoding.
C. Web crawling.
D. Fuzzing.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 209
Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?

A. TCP 23
B. UDP 69
C. TCP 22
D. TCP 21

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 45

QUESTION 210
Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?

A. Warm site
B. Load balancing
C. Clustering
D. RAID

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 211
Which of the following firewall rules only denies DNS zone transfers?

A. deny udp any any port 53
B. deny ip any any
C. deny tcp any any port 53
D. deny all dns packets

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 212
Which of the following BEST explains the use of an HSM within the company servers?

A. Thumb drives present a significant threat which is mitigated by HSM.
B. Software encryption can perform multiple functions required by HSM.
C. Data loss by removable media can be prevented with DLP.
D. Hardware encryption is faster than software encryption.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 213
Which of the following technologies can store multi-tenant data with different security requirements?

A. Data loss prevention
B. Trusted platform module
C. Hard drive encryption
D. Cloud computing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 214
Which of the following types of encryption will help in protecting files on a PED?

A. Mobile device encryption
B. Transport layer encryption
C. Encrypted hidden container
D. Database encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 215
Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT?

A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.
B. Tell the application development manager to code the application to adhere to the company's password policy.

C. Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.
D. Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 216
Which of the following presents the STRONGEST access control?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 217
Which of the following encompasses application patch management?

A. Configuration management
B. Policy management
C. Cross-site request forgery
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 49

QUESTION 218
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

QUESTION 219
Pete, a developer, writes an application. Jane, the security analyst, knows some things about the overall application but does not have all the details. Jane needs to review the software before it is released to production. Which of the following reviews should Jane conduct?

A. Gray Box Testing
B. Black Box Testing
C. Business Impact Analysis
D. White Box Testing

Correct Answer: A

QUESTION 220
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

QUESTION 221
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

QUESTION 222
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

QUESTION 223
Which of the following devices is BEST suited for servers that need to store private keys?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 224
In regards to secure coding practices, why is input validation important?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 225
Which of the following would be used when a higher level of security is desired for encryption key storage?

A. TACACS+
B. L2TP
C. LDAP
D. TPM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 226
A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 227
Which of the following MUST be updated immediately when an employee is terminated to prevent unauthorized access?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 228
Which of the following devices would MOST likely have a DMZ interface?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 229
Which of the following application security testing techniques is implemented when an automated system generates random input data?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 230
A security administrator wants to check user password complexity. Which of the following is the BEST tool to use?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 231
Certificates are used for: (Select TWO).

A. Client authentication.
B. WEP encryption.
C. Access control lists.
D. Code signing.
E. Password hashing.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 232
Which of the following algorithms has well documented collisions? (Select TWO).

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 11

QUESTION 233
Which of the following is BEST used as a secure replacement for TELNET?

A. HTTPS
B. HMAC
C. GPG
D. SSH

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 234
An email client says a digital signature is invalid and the sender cannot be verified. The recipient is concerned
with which of the following concepts?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 235
Which of the following transportation encryption protocols should be used to ensure maximum security between
a web browser and a web server?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 236
Developers currently have access to update production servers without going through an approval process. Which of the following strategies would BEST mitigate this risk?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 237
Which of the following is a difference between TFTP and FTP?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 13

QUESTION 238
Which of the following is characterized by an attacker attempting to map out an organization's staff hierarchy in order to send targeted emails?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 239
Which of the following would a security administrator implement in order to discover comprehensive security threats on a network?

A. Design reviews
B. Baseline reporting
C. Vulnerability scan
D. Code review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: