SY0-301

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

CompTIA SY0-301

CompTIA Security+ Certification Exam

Version: 13.2
CompTIA SY0-301 Exam

Topic 1, Volume A

Exam A

QUESTION 1

All of the following are valid approaches to providing switch port security EXCEPT:

A. firewall rules.
B. 802.1x.
C. disable unused ports.
D. ARP protection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2

Which of the following ports are used for NetBIOS by default?

A. 135
B. 139
C. 143
D. 443

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3

Which of the following services uses port TCP/23 by default?

A. FTP
B. TFTP
C. Telnet
D. SSH

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4

Which of the following is the MOST secure authentication protocol?

A. CHAP
B. PEAP

C. EAP
D. LEAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
Which of the following BEST describes fuzzing?

A. Security architecture review to detect design flaws before they get implemented
B. Injecting faults into applications in order to discover security weaknesses
C. Prevention of system vulnerabilities by applying firewall techniques
D. Vulnerability scanning of both application and infrastructure components

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
Which of the following access control systems is BEST suited to assign rights based on a single policy administrator?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
Which of the following is an example of only allowing alpha-numeric characters when submitting a website form?

A. SQL injection
B. Cross-site scripting

C. Input validation
D. Fuzzing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
Which of the following provides authentication, authorization, and accounting services?

A. PKI
B. WPA2
C. NTLMv2
D. RADIUS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
Setting the account lockout threshold too low can cause which of the following conditions?

A. Denial of service
B. Data loss
C. Unauthorized access
D. Non-secure passwords

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
Which of the following is the BEST way to prevent Cross-Site Request Forgery (XSRF) attacks?

A. Check the referrer field in the HTTP header
B. Disable Flash content
C. Use only cookies for authentication
D. Use only HTTPS URLs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
To BEST mitigate the loss of corporate data on a stolen mobile device, the IT department should have the ability to do which of the following?

A. Monitor SMS
B. GPS tracking
C. Remote wipe
D. Enable screen locks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
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:
Explanation:

QUESTION 13
Which of the following network principles will MOST effectively isolate network traffic?

A. Flood guards
B. VLAN
C. Loop protection
D. Bridged network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
Which of the following wireless security technologies continuously supplies new keys for WEP?

A. TKIP
B. Mac filtering
C. WPA2
D. WPA

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
Which of the following application security principles involves inputting random data into a program?

A. Brute force attack
B. Sniffing
C. Fuzzing
D. Buffer overflow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
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:
Explanation:

QUESTION 17
Which of the following is MOST appropriate when storing backup tapes in a physically non-secure room?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
Which of the following is an important step in the initial stages of deploying a host-based firewall?

A. Selecting identification versus authentication
B. Determining the list of exceptions
C. Choosing an encryption algorithm
D. Setting time of day restrictions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
Identifying a list of all approved software on a system is a step in which of the following practices?

A. Passively testing security controls
B. Application hardening
C. Host software baselining
D. Client-side targeting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
Which of the following threats can result from a lack of controls for personal webmail?

A. Bandwidth exhaustion
B. Cross-site request forgery
C. Data leakage
D. Least privilege

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
Which of the following can grant access based solely on TCP/IP information?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 22
Which of the following controls can prevent or detect specific information leaving a network in the form of an email?

A. Data loss prevention
B. Fuzzing
C. Antivirus
D. Network-based firewalls

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
Which of the following will terminate encrypted traffic?

A. Layer 3 switch
B. Sniffer
C. Router
D. VPN concentrator

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
Which of the following is used to perform end point posture assessment?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
A security administrator was recently terminated. Upon deleting their account, all the company data was also deleted from the servers. Which of the following malware types is being described in this situation?

A. Botnet
B. Trojan
C. Logic bomb

D. Virus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
Which of the following, when used periodically, is MOST likely to detect users with multiple accounts?

A. Account logging
B. Account deletion
C. Account locking
D. Account revalidation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
Which of the following is MOST likely to be detected during application security testing if secure coding techniques were not followed?

A. Malicious software embedded in the application web service
B. Outdated antivirus signatures and missing server patches
C. Invalid input data handling and possible cross-site scripting issues
D. Missing server patches leading to operating system exploits

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
Which of the following account policies would a security administrator implement to disable a user's account after a certain period of time?

A. Lockout
B. Expiration
C. Complexity
D. Recovery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
Which of the following attacks allows access to contact lists on cellular phones?

A. War chalking
B. Blue jacking
C. Packet sniffing
D. Bluesnarfing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Which of the following can be implemented to prevent portable devices from being stolen?

A. Whole disk encryption
B. Cable locks
C. GPS tracking
D. Screen locks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
In order for a user to visit a website without certificate warnings, the certificate MUST have been issued by a:

A. CA listed in the CRL.
B. CA the user's browser trusts.
C. CA trusted by the web server.

D. CRL trusted by the user's browser.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
An administrator values transport security strength above network speed when implementing an SSL VPN. Which of the following encryption ciphers would BEST meet their needs?

A. SHA256
B. RC4
C. 3DES
D. AES128

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 33
Which of the following identifies certificates that have been compromised or suspected of being compromised?

A. Certificate revocation list
B. Access control list
C. Key escrow registry
D. Certificate authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 34
Users in a high crime area commonly report cell phone theft. These reports are made anywhere from hours to days after the theft. A security administrator is tasked with implementing a strategy to recover cell phones if they are stolen, as well as prevent their data from being accessed. Which of the following strategies would BEST accomplish these goals? (Select TWO).

A. WPA wireless
B. Mobile firewall
C. Device encryption
D. GPS tracking
E. Mobile antivirus

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
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:
Explanation:

QUESTION 36
Which of the following network devices allows web traffic to be distributed amongst servers?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
All of the following are encryption types EXCEPT:

A. full disk.
B. SMIME.
C. file and folder.
D. RADIUS.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 38
The FIRST step when developing a contingency plan is to:

A. determine if a business impact analysis is needed.
B. identify the systems and resources impacted.
C. test the disaster recovery plan.
D. remove the single point of failure.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 39
A company has had several known incidents of employees copying sensitive data to USB drives, posting trade secrets to Internet websites, and emailing trade secrets to competitors. This company should implement which

of the following? (Select TWO).

A. Full disk encryption

B. Network IDS

C. Data loss prevention

D. Anti-spyware

E. USB device control

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
Highly sensitive data is stored in a database and is accessed by an application on a DMZ server. The disk drives on all servers are fully encrypted. Communication between the application server and end-users is also encrypted. Network ACLs prevent any connections to the database server except from the application server. Which of the following can still result in exposure of the sensitive data in the database server?

A. SQL Injection

B. Theft of the physical database server

C. Cookies

D. Cross-site scripting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 41
An application vendor recommends that an application be installed with a non-administrative account. This is an example of:

A. a discretionary access control list.

B. least privilege.

C. OS hardening.

D. separation of duties.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 42
Role-based access control is BEST defined as an authorization system by which:

A. privileges are granted to persons based on membership in one or more functional groups.
B. a separate user account is created for each functional role a person has.
C. access is limited to the time of day a person is expected to work.
D. privileges are assigned to each person based upon authorized requests.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43

Security of data at rest and in transit is important in cloud computing because unlike traditional corporate server environments:

A. applications in a cloud are load balanced across multiple hosts.
B. data in a cloud is transient and moved regularly.
C. systems in a cloud can be shared by multiple parties.
D. hardware in a cloud is located overseas and accessed by a single party.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 44
Full disk encryption is MOST effective against which of the following threats?

A. Denial of service by data destruction
B. Eavesdropping emanations
C. Malicious code
D. Theft of hardware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 45
In order to use a two-way trust model the security administrator MUST implement which of the following?

A. DAC
B. PKI
C. HTTPS
D. TPM

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 46

A user was able to access a system when they arrived to work at 5:45 a.m. Just before the user left at 6:30 p.m., they were unable to access the same system, even though they could ping the system. In a Kerberos realm, which of the following is the MOST likely reason for this?

A. The user's ticket has expired.
B. The system has lost network connectivity.
C. The CA issued a new CRL.
D. The NTP server is down.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
Which of the following would MOST likely be used to control the type of traffic going in and out of an email server?

A. Spam filter
B. Host based IDS
C. Host based firewall
D. Network based IDS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 48
Which of the following should be implemented to prevent exposure of sensitive data when a smartphone is lost or stolen? (Select TWO).

A. Camera
B. Encryption
C. Removable SD card
D. PIN
E. GPS tracking software

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
When a security administrator cannot verify who provided a hard drive image, then:

A. chain of custody is preserved.
B. the image must be rehashed.
C. the hash must be verified.
D. chain of custody is destroyed.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 50
Which of the following MUST be implemented when a company has only one available publicly addressable IP address and many users that need Internet connectivity?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 51
Which of the following ports would need to be open to allow HTTPS by default?

A. 25
B. 80
C. 443
D. 530

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52

An administrator begins the initial configuration of a replacement IPS. The device reports IRC attacks, SMTP relays, port scans, and other various malicious network activities. Which of the following is MOST likely occurring?

A. The old IPS was infected
B. False positives are being reported
C. There is a malicious insider threat
D. The new IPS is on the wrong subnet

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 53
Which of following is listed in order of highest volatility to lowest volatility?

A. Memory, Swap, Network Processes, System Processes, and File System
B. Swap files, Memory, Network Processes, System Processes, and File System
C. Network Process, Swap, System Processes, Memory, and File System
D. Memory, Swap, File System, Network and System Processes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
Which of the following is a reason 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:
Explanation:

QUESTION 55

Proper labeling of sensitive information supports which of the following security principles?

A. Enforces proper authentication of accessing users
B. Supports integrity in data backups
C. Ensures accountability for destruction of the document
D. Prevents disclosure of sensitive information

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
Which of the following is a correct formula for calculating mean time between failures (MTBF)?

A. MTBF = (Time observed) / (number of failures)
B. MTBF = (Number of failures) / (time observed)
C. MTBF = (Time observed) (number of failures)
D. MTBF = (Number of failures) x (time observed)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 57
Which of the following is often used to verify connectivity on a network?

A. DNS
B. DHCP
C. ICMP
D. NAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
Requiring technicians to report spyware infections is a step in which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 59
Routers are MOST often used as edge devices to:

A. remove viruses and scan content.
B. filter high volumes of traffic efficiently.
C. filter out spam from SMTP traffic.
D. authenticate multiple IPSec tunnels.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 60
After performing a port scan, a network administrator observes that port 443 is open. Which of the following services is MOST likely running?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 61
Secure Shell uses which of the following ports by default?

A. 21

B. 22
C. 23
D. 25

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 62
Which of the following software types should be installed if users have issues with random browser screens appearing while working on the Internet?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 63
An administrator successfully establishes an SSH tunnel between two servers for SMTP and FTP communication. However, attempts to establish a SSH tunnel for TFTP communication fails. Which of the following is MOST likely the reason for the communication failure?

A. TFTP uses the same port as SSH.

B. SSH has a tunnel limitation of two.

C. TFTP and FTP cannot coexist with a SSH tunnel.

D. SSH tunnels are limited to TCP.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 64
Which of the following would help secure a router? (Select TWO).

A. Disable Telnet

B. Enable HTTP

C. Enable IPX

D. Disable hash route updates

E. Enable encrypted passwords

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 65
Which of the following malware types typically allows an attacker to monitor a user's computer, is characterized by a drive-by download, and requires no user interaction?

A. Virus

B. Logic bomb

C. Spyware

D. Adware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 66
Which of the following is a cryptographic attack against a WEP enabled access point?

A. Interference
B. IV attack
C. Bluesnarfing
D. Packet sniffing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 67
An attacker tricks a user into authenticating to a fake wireless network and then inserts malicious code into strings as the user passes by. Which of the following describes this attack?

A. SQL injection
B. Malicious insider
C. Evil twin
D. User impersonation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 68
Which of the following application attacks is used against a corporate directory service where there are unknown servers on the network?

A. Rogue access point
B. Zero day attack
C. Packet sniffing
D. LDAP injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 69
Which of the following application attacks MOST likely requires `x90' to be placed into the malicious code?

A. MAC filtering
B. Buffer overflow
C. War driving
D. Code review

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
Which of the following is identified by the command:. `INSERT INTO users ("admin", "admin");'?

A. SQL Injection
B. Directory traversal
C. LDAP injection
D. Session hijacking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 71
Which of the following protocols provides transport security for web-enabled applications?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 72
Which of the following mitigation strategies is intended to give the BEST ROI?

A. Implement security controls before routine audits
B. Implement security controls based on risk
C. Implement security controls based on training
D. Implement all possible security controls

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 73
Which of the following data restorations has to be performed in sequence?

A. Differential
B. Off-site

C. Incremental
D. Redundant

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 74
A security administrator examines a network session to a compromised database server with a packet analyzer. Within the session there is a repeated series of the hex character 90 (x90).
Which of the following attack types has occurred?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 75
Examination of a compromised web server shows that an attacker was able to access a vulnerable sample script that was included with the default website instance as the entry point. Which of the following would prevent this type of incident in the future?

A. OS hardening
B. Application hardening
C. IDS
D. Antivirus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 76
A security administrator must be able to identify and validate every use of local administrative accounts across a large number of Windows and Linux servers. Which of the following offers the BEST solution?

A. Modify the system baseline to increase log retention and enable a host firewall.
B. Monitor LDAP and Active Directory for the use of Administrative accounts.
C. Add or enable a NIDS signature for administrative activity.
D. Implement centralized log collection for each server and define a log review process.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 77
Which of the following, when incorporated into a disk encryption solution, adds the MOST security?

A. SHA256 hashing
B. Password complexity requirement
C. HMAC
D. Trusted platform module

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 78
When a username is checked against an access list, which of the following does it provide?

A. Identification and authentication
B. Identification and authorization
C. Authentication and authorization
D. Authentication and integrity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 79
FTP/S uses which of the following TCP ports by default?

A. 20 and 21

B. 139 and 445

C. 443 and 22

D. 989 and 990

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 80
Which of the following should be considered when implementing WPA vs. WPA2?

A. LEAP vs. PEAP

B. SSID vs. MAC

C. SHA1 vs. MD5

D. CCMP vs. TKIP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 81
Which of the following is an encapsulated authentication protocol?

A. CCMP

B. LEAP

C. TKIP

D. WEP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 82
Following the order of volatility, taking hashes, and maintaining a chain of custody describes which of the following?

A. Forensics

B. Incident response

C. Business continuity

D. Disaster recovery

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 83
Which of the following attacks is MOST likely to be performed against an FTP server?

A. DLL injection
B. SQL injection
C. LDAP injection
D. Command injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 84
Which of the following should be used when deploying an e-commerce site?

A. Commercial CA certificate
B. Header manipulation
C. Self-signed certificate
D. Digital signature

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 85
Which of the following authentication services uses a ticket granting system to provide access?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 86
Various users throughout the company are reporting heavy latency and even outage issues. The security administrator believes that the issues may be due to an incorrectly configured network. Which of the following would assist the security administrator in finding the location of the faults?

A. Log analysis

B. ACLs
C. Vulnerability scan
D. Port scanner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 87
During a recent protocol analysis, the security administrator notices that port 23 is being used to access various network devices. Which of the following protocols is MOST likely being used by default?

A. TELNET
B. SSH
C. SSL
D. SNMP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 88
A security administrator wants to ensure that the message they are sending does not get intercepted or modified in transit. This concern relates to which of the following concepts?

A. Availability
B. Integrity

C. Accounting
D. Confidentiality

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 89
The security administrator is implementing a new design to minimize the footprint in the datacenter and reduce the amount of wasted resources without losing physical control of the equipment. Which of the following would they need to implement?

A. Virtualization
B. Cloud computing
C. New ACLs
D. VLAN management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 90
Which of the following would a company use as photo identification as well as authorization and access control for physical and logical reasons?

A. ACLs
B. Smart card
C. Key fobs
D. Common access card

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 91
A company replaces a number of devices with a mobile appliance, combining several functions. Which of the following descriptions fits this new implementation? (Select TWO).

A. Cloud computing
B. Virtualization
C. All-in-one device
D. Load balancing
E. Single point of failure

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 92
A security administrator with inside knowledge of a company is asked to perform a penetration test. Which of the following describes this type of testing?

A. White Hat
B. Black Hat
C. White Box
D. Black Box

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 93
A security consultant is asked to perform a penetration test with no inside knowledge of the company. Which of the following describes this type of testing?

A. White Hat
B. Black Hat
C. White Box
D. Black Box

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 94
A security administrator is asked to perform a penetration test for their company. Which of the following describes this type of penetration tester?

A. Black Box
B. White Hat
C. White Box
D. Black Hat

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 95
A security administrator decides to perform an unauthorized penetration test against a competing company. Which of the following describes this type of penetration tester?

A. White Box
B. Black Box
C. White Hat
D. Black Hat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 96
Which of the following is used to encrypt defined groups of data before they are transmitted?

A. Digital signature

B. Block cipher

C. Hashing

D. Stream cipher

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 97
Which of the following technological implementations uses PKI? (Select TWO).

A. FTP

B. HTTPS

C. WEP

D. VPN

E. VLAN

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 98
Which of the following should be used when a business needs a block cipher with minimal key size for internal encryption?

A. AES

B. Blowfish

C. RC5

D. 3DES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 99
A corporation requires that all employees have a backup for their position in case of disaster. This is known as which of the following?

A. Succession planning

B. Collusion

C. Separation of duties

D. Job rotation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 100
Which of the following could a security administrator implement to mitigate the risk of tailgating for a large organization?

A. Train employees on correct data disposal techniques and enforce policies.
B. Only allow employees to enter or leave through one door at specified times of the day.
C. Only allow employees to go on break one at a time and post security guards 24/7 at each entrance.
D. Train employees on risks associated with social engineering attacks and enforce policies.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Topic 2, Volume B

QUESTION 101
An employee receives an email message that looks like it was sent from the Chief Executive Officer (CEO) but is attempting to sell them prescription medicine. This could be an example of which of the following?

A. XML injection
B. SQL injection
C. Spoofing
D. Session hijacking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 102
The main difference between symmetric and asymmetric encryption is that:

A. symmetric encryption uses the same key for encryption and decryption, while asymmetric encryption uses one key to encrypt and one to decrypt.
B. in symmetric encryption the encryption key must be of even number length so that it can be split in two, where one part is used for encryption and the other is used for decryption.
C. asymmetric encryption uses the same key for encryption and decryption, while symmetric encryption uses one key to encrypt and one to decrypt.
D. in asymmetric encryption the same key is given to one user in a hashed format and used for encryption, and to another used in plain text and used for decryption.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 103
Which of the following is usually encrypted when stored or transmitted?

A. CRL
B. Private key
C. Root certificate
D. Public key

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 104
The private key is used to do which of the following? (Select TWO).

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 105
A security administrator must block all incoming traffic, except for HTTP from the Internet to the company's web server with the IP 10.x.x.x. Which of the following ACLs BEST achieves this administrator's task?

A. PERMIT ANY 10.x.x.x 80
DENY ANY ANY
B. DENY ANY ANY
PERMIT 10.x.x.x 80
C. PERMIT 10.x.x.x any 80
DENY ANY ANY

D. PERMIT ANY ANY 80
DENY ANY ANY

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 106
A security administrator would implement 802.1x to establish:

A. VLAN trunking.
B. a complex ACL.
C. authenticated endpoints.
D. TKIP on a wireless.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 107
Which of the following is a security administrator performing when redirecting the output of an OS random generator device into the input of an executable program?

A. Hardening the executable
B. Patching the executable
C. Fuzzing
D. Testing XSRF

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 108
Users in a financial office are reporting that they are not being asked for credentials anymore when successfully connecting to the company wireless. All other offices are still being authenticated on the wireless. Which of the following is this an example of?

A. Evil twin

B. Interference
C. IV attack
D. War driving

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 109
A security administrator has noticed a large number of ACL entries on the firewall for a specific host. Which of the following hardening practices can help reduce the complexity of the ACL?

A. Enabling the application logs

B. Enabling and configuring IPv6

C. Disabling unused accounts

D. Disabling unnecessary services

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 110
Which of the following measures can an administrator implement to prevent rootkits on a system? (Select TWO).

A. Antivirus

B. Stateful firewall

C. IDS

D. Log parser

E. Network sniffer

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 111
Which of the following is BEST used to separate and group devices based on business need or security requirements?

A. Virtualization

B. NAT

C. VLAN

D. Subnetting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 112
Products like Metasploit and Cain & Abel are often used to perform which of the following?

A. SNMP trap collection
B. Penetration testing
C. Code review
D. Application baselining

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 113
Which of the following are the Rijndael ciphers chosen to replace DES?

A. 3DES
B. Serpent
C. Twofish
D. AES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 114
Which of the following uses openly available standards to provide a hashing function? (Select TWO).

A. Twofish

B. AES
C. HMAC
D. RC4
E. GPG

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 115
Which of the following use port 22 by default? (Select TWO).

A. SSH
B. SMTP
C. SNMP
D. SCP
E. SSL

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 116
An attacker captures wireless traffic and changes their laptop's wireless card setting to 00-12-79- BD-65-7D to match an observed wireless client. Which AP security measure would this defeat?

A. WEP

B. SSID broadcast

C. WPA2

D. MAC filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 117
Which of the following can be used to determine which services may be running on a host, but not if they are exploitable?

A. Baseline analyzer

B. Port scanner

C. Virus scanner

D. Vulnerability scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 118
An administrator captures traffic sent between a router and a monitoring server on port 161. The packet payload contains the strings 'PUBLIC' and 'PRIVATE'. Which of the following was MOST likely used to capture this traffic?

A. Vulnerability scanner

B. Protocol analyzer

C. SNMPv3

D. SNMPv2c

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 119
An administrator is hardening email application communication to improve security. Which of the following could be performed?

A. Remove gateway settings from the route table
B. Password protect the server BIOS
C. Disabling high I/O services
D. Require TLS when using SMTP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 120
Which of the following can be utilized in order to provide temporary IT support during a disaster, where the organization sets aside funds for contingencies, but does not necessarily have a dedicated site to restore those services?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 121
Which of the following terms is used to describe predictable failure points for equipment or services?

A. RTO
B. MTTR
C. RPO
D. MTBF

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 122

Which of the following is BEST utilized to identify common misconfigurations throughout the enterprise?

A. Vulnerability scanning

B. Port scanning

C. Penetration testing

D. Black box

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 123

A security administrator is aware that a portion of the company's Internet-facing network tends to be non-secure due to poorly configured and patched systems. The business owner has accepted the risk of those systems being compromised, but the administrator wants to determine the degree to which those systems can be used to gain access to the company intranet. Which of the following should the administrator perform?

A. Patch management assessment

B. Business impact assessment

C. Penetration test

D. Vulnerability assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 124
Which of the following BEST describes the primary business reasons to collect security incident data for trending purposes? (Select TWO).

A. To determine if security monitoring should be outsourced

B. To determine if protective controls are adequate

C. To determine if the cost of security controls are adequate

D. To determine if IDS products are functioning correctly

E. To determine if incident response capability is sufficient

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 125
Which of the following is a technical preventive control?

A. IDS

B. Data backup
C. Audit logs
D. ACLs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 126
Data classification and labeling is an example of:

A. preventative administrative control.
B. deterrent technical control.
C. preventative technical control.
D. deterrent administrative control.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 127
Which of the following authentication methods is typical among corporate environments to authenticate a list of employees?

A. Twofish
B. ACLs
C. LDAP
D. Kerberos

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 128
Which of the following tools can be used by an attacker to assess running applications on a remote host?

A. Baseline
B. Honeypot
C. Port scanner
D. Honeynet

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 129
An administrator has noticed that the accounting department's PCs are being used after hours, and there is suspicious outbound traffic on the firewall. Which of the following is MOST likely occurring?

A. The machines have been turned into a botnet.
B. The machines have been infected with a logic bomb.
C. A rogue user has given themselves escalated privileges.
D. A rootkit has been installed on the monitoring equipment.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 130
Which of the following security controls would be applied on individual hosts to monitor suspicious activities, by actively analyzing events occurring within that host, and blocking any suspicious or abnormal activity?

A. HIPS
B. Spam filter
C. HIDS
D. Firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 131
Which of the following is the STRONGEST algorithm for password hashes?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 132
A company is looking to implement a new system of desktops to its employees based on thin client technology. Which of the following implementations would fit the company's needs and allow for quick reimaging of machines in case of a virus attack?

A. SCAP
B. VLAN
C. SAN
D. VDI

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 133
A maintenance director is requesting a new insurance quote through email from the insurance agent. The quote is for a new building complex that was bought last month by the director's company. Which of the following can be used to ensure that the quote is legitimate and from the trusted insurance agent?

A. Certificate revocation list
B. Hashing
C. Digital signature
D. Code signing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 134
A technician would like to separate network access to the accounting department because of previous attacks targeting the accounting workstations. Which of the following allows the technician to separate networks by using existing network equipment?

A. DNS

B. OCSP
C. SAN
D. VLAN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 135

An administrator is creating a new security policy and must consider many stakeholders as well as current regulations, and the company direction. For the BEST success in policy roll out, which stakeholder is the MOST important to consider?

A. End users
B. Information security team
C. Senior leadership team
D. Customers and vendors

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 136
Which of the following ports is used by FTPS by default?

A. 69
B. 443
C. 990
D. 1025

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 137
Which of the following ports is used by RDP by default?

A. 990

B. 1494
C. 3389
D. 8080

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 138
Which of the following increases proper airflow in a datacenter?

A. Humidity controls
B. Video monitoring
C. Temperature controls
D. Hot and cold aisles

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 139
Implementation of routine file hash validation is an example of which of the following security concepts?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 140
Which of the following should the security administrator implement to limit all network traffic based on country of origin?

A. URL filtering

B. Firewalls
C. Spam filtering
D. Proxies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 141
In which of the following orders should an administrator capture a system's data for forensics investigation?

A. Hard disk, swap file, system memory, CPU cache
B. CPU cache, system memory, swap file, hard disk
C. System clock, flash BIOS, memory, hard disk
D. Flash BIOS, system memory, swap file, hard disk

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 142
Employees are reporting that unauthorized personnel are in secure areas of the building. This is MOST likely due to lack of security awareness in which of the following areas?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 143
A security administrator conducted a scan and generated a vulnerability report for the Chief Executive Officer (CEO). The vulnerability report indicated several vulnerabilities but the CEO has decided that cost and operational impact outweigh the risk. This is an example of which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 144
A company suspects that one of its employees is conducting fraudulent activities by selling company information to its competitors through email. Which of the following should the company do FIRST?

A. Contain the email system
B. Conduct an analysis of the employee's system
C. Contact senior management
D. Activate the incident response team

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 145
Which of the following BEST represents the goal of a vulnerability assessment?

A. To test how a system reacts to known threats

B. To reduce the likelihood of exploitation
C. To determine the system's security posture
D. To analyze risk mitigation strategies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 146
When physically installing wireless networks, one must consider that:

A. the access point is placed near structures to avoid attenuation-based attacks.
B. the access points have matching MACs to provide secure redundant connection profiles.
C. neighboring access points must operate on the same frequency.
D. the placement of the antennae does not allow network access outside of the building.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 147
In an effort to secure data in the event of a stolen laptop with minimal user impact, which of the following strategies should the IT department use?

A. Require users to carry token identification
B. Enforce two-factor authentication using biometrics
C. Install full disk encryption on the system's hard drive
D. Disable the use of USB ports through group policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 148
Following the recovery from a major virus incident, the incident response team is assembled to perform post-mortem analysis and review lessons learned. This activity is MOST likely to occur during which of the following phases?

A. Validation
B. Identification
C. Recovery
D. Containment
E. Eradication

F. Follow-up

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 149
"Pass Any Exam. Any Time." - www.actualtests.com 51
CompTIA SY0-301 Exam
A financial services company is concerned about the risk of employees sending confidential and proprietary information outside of the network. Which of the following solutions will BEST mitigate the perceived risk?

A. Intrusion prevention system
B. Intrusion detection system
C. Vulnerability scanning
D. Data loss prevention

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 150
A user reports that their wireless mobile device containing confidential information was stolen from the hotel room over the weekend. Which of the following BEST remediates the risk of confidential data loss?

A. Data loss prevention
B. Screen lock
C. Remote wipe
D. Global positioning software

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 151
A customer service department has a business need to send high volumes of confidential information to customers electronically. All emails go through a DLP scanner. Which of the following is the BEST solution to meet the business needs and protect confidential information?

A. Automatically encrypt impacted outgoing emails
B. Automatically encrypt impacted incoming emails
C. Monitor impacted outgoing emails
D. Prevent impacted outgoing emails

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 152
A bollard is an example of which of the following security measures?

A. Network security

B. Physical security

C. Internet security

D. Cyber security

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 153
A user reports that they cannot access a website by typing in the URL, but can access a network share on the server by IP address. Which of the following should be checked FIRST?

A. Subnet mask on the workstation

B. DNS server settings on the workstation

C. Encryption on the workstation

D. Default services on the workstation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 154
Which of the following represents the strongest password?

A. P@sSW1r&

B. P@sSWor&

C. PassW1rD

D. password

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 155
A security administrator implemented design changes and moved certain servers into a dedicated area that is accessible from the outside network, yet separated from the internal network. Which of the following did they implement?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 156
Which of the following pseudo-codes will prevent XSS?

A. If input contains ` or input contains ` then reject input
B. If input contains < or input contains > then reject input
C. If input contains ! or input contains ! then reject input
D. If input contains \ or input contains \ then reject input

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 157
A security administrator wants to ensure that the MAC address of the computers in the payroll department cannot be determined by users in other departments. Which of the following should be done?

A. Connect all of the payroll department computers into a separate switch.
B. Connect all of the payroll department computers to a hub and configure the uplink port in half duplex.
C. Place a router between the payroll department and the rest of the network.
D. Use static ARP mappings to obfuscate the MAC addresses of the payroll department computers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 158
A user who locks the computer screen while playing a game during work hours is MOST likely concerned with which of the following?

A. Saving electricity

B. Confidentiality
C. Availability
D. Policy violation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 159
Which of the following pseudocodes MOST likely prevents buffer overflows?

A. If input contains < or > then escape the character and execute the program with user input.
B. If input is less than 100 characters, then prompt for input again.
C. If input contains \ then remove \ and execute program with user input.
D. If input is greater than 1000 characters then truncate input.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 160
Which of the following hardware based encryption devices is used as a part of multi-factor authentication to access a secured computing system?

A. Database encryption
B. USB encryption
C. Whole disk encryption
D. TPM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 161
Which of the following is MOST likely used to establish a secure connection between email gateways?

A. TLS
B. PGP
C. HTTPS
D. SCP

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 162
Establishing a published chart of roles, responsibilities, and chain of command to be used during a disaster is an example of which of the following?

A. Fault tolerance
B. Succession planning
C. Business continuity testing
D. Recovery point objectives

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 163
A security administrator has changed the default settings on a web server, removing certain files and directories. This is an example of which of the following?

A. Application configuration baseline
B. Application hardening
C. Cross-site scripting prevention
D. Application patch management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 164
The security administrator takes a snapshot of all current applications on a server for future comparison. This is an example of which of the following?

A. Cross-site scripting prevention
B. Application patch management
C. Application hardening
D. Application configuration baseline

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 165

Which of the following devices would be MOST useful when a large number of remote users need secure access to a system in the main office?

A. VPN concentrator
B. Web security gateway
C. Switch
D. Load balancer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 166
A security administrator has noticed a large number of requests coming into the network on an unused port number. Which of the following devices would be BEST to use to block those requests, while still allowing access to other services on the network?

A. Switch
B. Load balancer
C. Proxy

D. Firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 167
Which of the following protocols uses UDP for file transfer?

A. HTTP
B. TELNET
C. FTP
D. TFTP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 168
A local bookstore wishes to provide wireless Internet access for its customers, but wants to limit the signal strength to prevent adjacent businesses from accessing the wireless network. Which of the following would BEST achieve this objective? (Select TWO).

A. Manually set channel
B. Antenna placement

C. MAC filtering
D. SSID broadcast
E. Site survey
F. Power level controls

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 169
Which of the following is used to manage network devices?

A. SMTP

B. SNMP
C. FTPS
D. ICMP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 170
A user needs to transfer a file in the LEAST secure but FASTEST way possible. Which of the following protocols could be used?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 171
A user has an IP address of 172.16.24.43 and visits a website which states that they have an IP address of 204.211.38.89. Which of the following is being used on the network? (Select TWO).

A. NAT
B. NAC
C. Spoofing
D. DMZ
E. VLANs
F. PAT

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 172
A company recently implemented a TLS on their network. The company is MOST concerned with:

A. confidentiality.
B. availability.
C. integrity.
D. accessibility.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 173
Which of the following will prevent unapproved outgoing calls if a mobile phone is lost? (Select TWO).

A. Screen lock
B. GPS Tracking
C. Remote sanitization
D. Whole disk encryption
E. Disabled Bluetooth
F. Voice encryption

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 174
A user has several random browser windows opening on their computer. Which of the following programs can be installed on his machine to help prevent this from happening?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 175
Which of the following protocols would BEST report network response?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 176
Which of the following describes how an attacker can get someone's contacts and calendar schedule off a nearby mobile device?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 177
Which of the following will allow proper ventilation for servers in a data center?

A. Hot/cold aisles
B. Humidity controls
C. EMI shielding
D. Load balancing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 178
Which of the following is a way to gain access to a protected system while another user is entering credentials?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 179
A system administrator installed new database software and notices that after running port scan on the server port 21 is now open. The database does not use any type of file transfer program. Which of the following would reduce the amount of unnecessary services being used?

A. NIPS
B. Application hardening
C. NIDS
D. Application baselining

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 180
The security risk manager has implemented a clean desk policy for the entire organization. Which of the following would make sure users were adhering to the new policy?

A. Review user permissions
B. Perform routine audits
C. Incident management
D. Change management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 181
A server intrusion occurred and the incident team performed the necessary steps to report their findings and mitigate future attacks. The legal team decided to take action against the suspect.

With the evidence, which of the following is the MOST important to maintain? (Select TWO).

A. Chain of custody
B. Track man hours and expenses
C. Order of volatility
D. Interview the witnesses
E. Zero-day exploit prevention

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 182
A company is installing a new security measure that would allow one person at a time to be authenticated to an area without human interaction. Which of the following does this describe?

A. Fencing
B. Mantrap
C. A guard
D. Video surveillance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 183
A security administrator identifies a WEP-encrypted WAP on the network that is located at the end of the building. They have noticed that it is the most utilized WAP on the network. When trying to manage the WAP, they are unable to gain access. Which of the following has MOST likely happened to the WAP?

A. The WAP is under an IV attack.
B. The WAP's MAC address has been spoofed.
C. The WAP is a rogue access point.
D. The WAP was victim to a bluejacking attack.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 184
A network device that protects an enterprise based only on source and destination addresses is BEST described as:

A. IDS.
B. ACL.

C. stateful packet filtering.
D. simple packet filtering.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 185
An IT manager is concerned that the CRL list is not being updated in a timely manner. Which of the following technologies would BEST mitigate the problem?

A. OCSP
B. PKI
C. PGP
D. CRL centralization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 186
A DNS server has become unresponsive. The protocol analyzer shows many DNS queries from IP addresses located around the world. Which of the following attacks is occurring?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 187
A human resources employee receives an email from a family member stating there is a new virus going around. In order to remove the virus, a user must delete the Boot.ini file from the system immediately. This is an example of which of the following?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 188
A third party application has the ability to maintain its own user accounts or it may use single sign- on. To use single sign-on, the application is requesting the following information: OU=Users, DC=Domain, DC=COM. This application is requesting which of the following authentication services?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 189
Which the following flags are used to establish a TCP connection? (Select TWO).

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 190
If an attacker is attempting to determine the operating system using banner information, which of the following techniques could they be using?

A. Whois lookup
B. nslookup
C. Port scanning
D. Fingerprinting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 191
Over the years, a company has found that too many administrators are making system modifications. Management has asked its IT staff to focus on simplifying the environment. Which of the following is the MOST likely focus of remediation?

A. Business continuity planning and testing
B. Change management
C. Removing single points of failure
D. Incident management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 192
An administrator is looking to implement a security device which will be able to not only detect network intrusions at the organization level, but help defend against them as well. Which of the following is being described here?

A. NIDS
B. NIPS
C. HIPS

D. HIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 193
An attacker has compromised a server and retrieved a copy of the NTLM database. Which of the following is the FASTEST way to obtain the user passwords?

A. Brute-force
B. Dictionary
C. Rainbow tables
D. Enumeration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 194
For which of the following is Trusted Platform Module hardware MOST likely used?

A. Full disk encryption
B. Certificate authority private keys
C. Network transport security
D. Trusted OS controls

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 195
A security administrator would like to protect the confidentiality of data traffic leaving the network while still maintaining the use of all current outgoing protocols. Which of the following would BEST help to change unsecured traffic to secured traffic?

A. Eliminate TFTP
B. Switch the default FTP port to 22

C. Move SSL to TLS
D. Eliminate ICMP
E. Establish an SSL VPN

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 196
A user has random Internet browser windows opening on their screen. Which of the following types of malware is this an example of?

A. Pop-up blocker
B. Trojan
C. Adware
D. Logic bomb

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 197
Which of the following default network ports is used by FTP?

A. 20
B. 22
C. 23

D. 25

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 198
Which of the following allows a security technician to provide LAN access to multiple remote users?

A. Load balancers

B. Sniffers
C. VPN concentrators
D. Proxies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 199
Which of the following should a technician apply to prevent guests from plugging in their laptops and accessing the company network?

A. Secure router configuration
B. Port security
C. Sniffers
D. Implicit deny

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 200
Which of the following should a technician apply to the network for retroactive identification of security breaches?

A. Port security
B. NAT
C. Firewall
D. Log analysis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Topic 3, Volume C

QUESTION 201
Which of the following should a security technician apply to a firewall to prevent access to internal networks?

A. Secure configuration
B. Flood guards
C. ACL
D. Port security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 202
Which of the following should a security technician provide as the BEST reason for using a layer 2 switch instead of a hub?

A. It can help prevent network bridging.
B. It supports Network Address Translation (NAT).
C. It can provide implicit deny capabilities.
D. It offers strong log analysis.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 203
Which of the following protocols is MOST likely associated with network audit logging?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 204
Which of the following should a security technician create to articulate the requirements for what is and what is not condoned on company systems?

A. Acceptable usage policy
B. Retention policy
C. Privacy policy
D. Access control policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 205
Which of the following risk related concepts BEST supports the identification of fraud?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 206
Which of the following incident response procedures allows a non-technical staff member to document an attack?

A. Recording time offset
B. Hashing files
C. Capture system image
D. Screenshots

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 207
Which of the following BEST allows the security technician to identify how much damage was caused by a security incident?

A. Screenshots
B. Chain of custody

C. Recording man hours and expenses
D. Capturing system images

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 208
Which of the following security related awareness and training activities can help prevent zero-day exploits?

A. Password complexity
B. Clean desk policies
C. Threat awareness
D. Data handling

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 209
Which of the following BEST describes data labeling in sensitive environments?

A. Data labeling describes Personally Identifiable Information (PII)
B. Data labeling identifies how and by whom certain data might be accessed
C. Data labeling provides best practices for information sharing
D. Data labeling provides the details of applicable laws by data type

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 210
Which of the following must a system administrator implement to escrow company encryption secrets?

A. Send the CRL to a third party.
B. Send the CA certificate to a third party.
C. Send the public keys to a third party.
D. Send the private keys to a third party.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 211
Which of the following must a security administrator implement to isolate public facing servers from both the corporate network and the Internet?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 212
A newly installed server is expected to fail twice in the next year and the company is expected to lose $3000 next year due to this server's failures. Which of the following is the SLE?

A. 2 hours
B. 2 days
C. $1500
D. $6000

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 213
The disaster recovery manager must contact third party vendors to implement a warm site. Which of the following items are MOST likely to be on the list?

A. HVAC, power, network cabling, racks
B. Power and cooling
C. HVAC, power, network cabling, racks, and servers
D. Power only

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 214
The security analyst has captured a port 53 packet with the following TCP/IP flags:

URG = 1

ACK = 1

PUSH = 1

RST = 1

SYN = 1

FIN = 1

Which of the following attacks is this MOST likely an example of?

A. DDOS
B. DNS poisoning
C. XMAS
D. Spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 215
A network administrator has noticed an increase in traffic on a UDP port. Which of the following protocols operates on this port?

A. SNMP
B. SMTP

C. FTPS
D. SFTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 216
A user on the network, is unable to use traceroute to determine the path to a certain destination. Which of the following protocols should be allowed through the firewall in order for traceroute to work?

A. ICMP
B. IGMP
C. SSH
D. SSL

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 217
Which of the following network devices could help to filter web content?

A. Router
B. Proxy server
C. Switch
D. Protocol analyzer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 218
The security administrator for a company needs to assign permissions for users on the network. Which of the following would allow them to give ONLY the appropriate permissions necessary?

A. Separation of duties

B. Job rotation
C. Privilege escalation
D. Least privilege

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 219
Ticket-Granting-Tickets (TGTs) are common in which of the following authentication schemes?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 220
Which of the following is BEST used to determine the source of a network bottleneck?

A. Sniffer

B. Router

C. Firewall

D. Switch

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 221
Which of the following could filter certain behaviors, such as the HTTP POST command?

A. Web application firewall

B. Network firewall

C. Load balancer

D. Antivirus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 222
A user brought a laptop in from home and connected the Ethernet interface on the laptop to a wall jack with a patch cable. They were unable to access any network resources. Which of the following is the MOST likely cause?

A. Flood guards were enabled on the switch.

B. Loop protection prevented the laptop from accessing the network.

C. Port security was enabled on the switch.

D. Router access control lists prevented the laptop from accessing the network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 223
A network technician has been tasked with designing a network solution. They were given one Class C network address (192.168.204.0/24) and must address 10 devices in the business office, and two network connections on the router. The devices in the business office and the network connections MUST be on different networks. Which of the following is the technician's BEST option?

A. Use subnets

B. Use NAT

C. Use virtualization

D. Use VLANs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 224
Which of the following network protocols transmits a user's credentials in clear-text? (Select TWO).

A. SSH
B. HTTPS
C. SCP
D. Telnet
E. FTP
F. TFTP

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 225
Which of the following is the BEST method for ensuring all files and folders are encrypted on all corporate laptops where the file structures are unknown?

A. Folder encryption
B. File encryption
C. Whole disk encryption
D. Steganography

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 226
Which of the following is the WEAKEST encryption?

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 227
Which of the following design elements translates many IP addresses to one IP address?

A. PAT
B. NAT
C. Default gateway
D. Subnet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 228
The supervisor reports that discharged employees are still able to authenticate via PKI to corporate assets. Which of the following should an engineer deploy to ensure that newly- discharged employees cannot access these resources?

A. CA
B. OCSP
C. Intermediate CA
D. Key escrow

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 229
Encryption used by RADIUS is BEST described as:

A. quantum.
B. elliptical curve.
C. asymmetric.
D. symmetric.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 230

A security technician notices a message promoting a concert on their corporate instant messenger. Which of the following attacks would this describe?

A. Spam
B. Pharming
C. Spim
D. Vishing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 231
Malicious JavaScript code can be described as which of the following attacks?

A. Client-side attack
B. Smurfing
C. Xmas attack
D. Man-in-the-middle

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 232
An IT security technician discovers that a company laptop was moved to another office building without permission. Which of the following would prevent this in the future?

A. Cable locks
B. Data loss prevention
C. GPS tracking
D. Device encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 233
Which of the following is often rated based on its ability to increase the time it takes to perform an attack?

A. Safe

B. Screen lock
C. Patch management
D. Virtualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 234
Which of the following can prevent an attacker from accessing data on a thumb drive?

A. Smart card
B. Screen lock
C. SSO
D. Device encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 235
A security technician needs to recommend a hardware based encryption solution for their company. Which of the following BEST meets this need?

A. Full disk encryption
B. Trusted platform module
C. Public key infrastructure
D. Cable locks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 236
An IT security technician is required to implement an authentication and authorization solution which provides one-time passwords for company executives. Which of the following BEST meets this requirement?

A. Tokens
B. Multifactor authentication
C. Biometrics
D. Smart cards

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 237
Which of the following is MOST closely related to SE Linux?

A. Discretionary access control
B. Trusted OS
C. Multifactor authentication
D. Biometrics

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 238
An IT security technician has been asked by the Chief Information Security Officer (CISO) how the company can minimize the number of user IDs required to access multiple resources. Which of the following can BEST address this need?

A. Trusted OS
B. Implicit deny
C. RBAC
D. PKI

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 239
A security technician is required to implement a cryptographic messaging solution that has speed as its primary factor. Which of the following BEST meets this need?

A. Digital signatures
B. Asymmetric
C. Symmetric

D. Steganography

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 240
Which of the following digital certificate management practices will ensure that a lost certificate is not compromised?

A. Key escrow
B. Non-repudiation
C. Recovery agent
D. CRL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 241
Pete and Sara need to exchange information in a secure manner. They both have requested certificates from the information security group. Which of the following keys should Pete and Sara exchange with each other to securely exchange information with one another?

A. They should both exchange their public keys.
B. Sara should send her private key and Pete should send his public key.
C. They should both exchange their private keys.
D. Pete should send his private key and Sara should send her public key.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 242
The finance department is receiving emails from the corporation's main bank. The bank has not sent emails to the corporation. Which of the following types of security awareness training can be recommended to the finance department?

A. Vishing attacks
B. Smurf attacks
C. Phishing attacks
D. Zero Day exploits

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 243
Accounting wants to send a file securely from a Unix system to a customer's FTP site. Which of the following commands would be run at a Unix command prompt?

A. SSH
B. SFTP
C. SSL
D. TELNET

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 244
A system administrator notices markings on the outside of the office building. Which of the following is this an example of?

A. War driving
B. War chalking
C. Rogue access points
D. Social engineering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 245

A firewall administrator notices large amounts of traffic coming from multiple outside IP addresses directed at the company's e-commerce server on the Internet. Which of the following attacks is taking place?

A. DoS
B. Client-side attack
C. DDoS
D. Privilege escalation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 246
Which the following BEST prevents burn-out?

A. Time of day restrictions
B. Separation of duties
C. Least privilege
D. Job rotation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 247
The use of a smart card, user ID, and password is an example of which of the following?

A. Multifactor authentication
B. Single sign-on
C. Identification
D. Authorization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 248

Which of the following, when used on a file, creates a non-reversible numeric representation of the file's composition?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 249
Which of the following is a symmetrical key block cipher that encrypts MOST quickly?

A. 3DES
B. RSA
C. Blowfish
D. SHA256

E. Diffie-Hellman

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 250
Which of the following is a common stream cipher?

A. RC4
B. 3DES
C. HMAC
D. RIPEMD

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 251

There are two access points with the same SSID broadcast. One access point is legitimate and one is used to capture traffic as it comes in. Which of the following wireless attacks is occurring?

A. Interference
B. Bluejacking
C. IV attack
D. Evil twin

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 252
A user receives an unsolicited SMS message over their mobile device regarding the sale at a store nearby. Which of the following attacks has just occurred?

A. Session hijacking
B. SQL injection
C. Whaling
D. Bluejacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 253
A security administrator has just purchased paper shredders for all departments that deal with PII. Which of the following social engineering attacks will paper shredders help prevent?

A. Session hijacking
B. Evil twin
C. Dumpster diving
D. Shoulder surfing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 254

A security administrator forgets their card to access the server room. The administrator asks a co- worker if they could use their card for the day. Which of the following is the administrator using to gain access to the server room?

A. Man-in-the-middle
B. Tailgating
C. Impersonation
D. Spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 255
An administrator has concerns regarding sensitive company data stored on USB hard drives. Which of the following BEST addresses these concerns?

A. Provide users USB drives tracked by serial numbers.
B. Implement USB drives that utilize keypad login upon connection.
C. Allow users to use personal USB drives that are approved by a supervisor.
D. Employ a group policy that backs up the drive to a network share.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 256
A system administrator has been tasked by the Payroll department to limit user access to avoid unapproved overtime. Which of the following would be the BEST solution to implement?

A. A policy that prevents users from logging in after business hours.
B. Regular auditing and updating of user account usage.
C. Create a baseline report of user accounts and monitor deviances.
D. Maintain an up-to-date access control list.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 257
A security administrator needs to implement a solution to address known third party software vulnerabilities. Which of the following must be implemented?

A. Secure coding
B. A baseline
C. Fuzzing
D. Patch management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 258
Which of the following must a security administrator implement in order to prevent user errors during data entry?

A. Input validation
B. Record duplication
C. Error handling
D. Data sanitization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 259
A security consultant has been asked to implement a process to secure active remote sessions on mobile devices against attackers who steal a device left unattended. Which of the following must be implemented to mitigate such risk?

A. Screen lock
B. Strong passwords

C. GPS tracking
D. Device encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 260
A security administrator must implement a control against online brute force attacks. Which of the following BEST accomplishes this?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 261
A security analyst wants to ensure that all data is being transmitted confidentially when sent to a cloud provider. Which of the following will accomplish this goal? (Select TWO).

A. Single sign-on
B. NTLMv2
C. Transport layer security
D. Whole disk encryption
E. Secure socket layer

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 262
Which of the following procedures would be used to mitigate the risk of an internal developer creating a text field without input validation checks on a production system?

A. Incident management
B. Code review
C. Mobile device management
D. Change management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 263
In order to enter a corporate office, employees must enter a PIN. Which of the following are common risks when using this type of entry system? (Select TWO).

A. Shoulder surfing
B. Key logging
C. Tailgating
D. Man-in-the-middle attacks
E. Dumpster diving

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 264
A corporate datacenter operates in a humid area near an ocean and often has hardware failures. Which of the following controls would help prevent these issues?

A. Fire suppression
B. HVAC
C. RAID
D. Cold aisles

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 265
The main corporate website has a service level agreement that requires availability 100% of the time, even in the case of a disaster. Which of the following would be required to meet this demand?

A. Warm site implementation for the datacenter
B. Geographically disparate site redundant datacenter
C. Localized clustering of the datacenter

D. Cold site implementation for the datacenter

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 266
Which of the following should be put in place to prevent SQL injection attacks?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 267
A security administrator is notified daily of any new vulnerabilities that affect the major systems in the company. Which of the following strategies does this address?

A. Patch management
B. Contingency planning
C. Disaster recovery
D. Certificate management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 268
A security analyst receives a call from a customer reporting that at times when the customer visits a website a prompt appears, soliciting the customer to purchase pharmaceuticals. Which of the following would BEST prevent this from occurring?

A. Antivirus
B. Pop-up blocker

C. Anti-malware
D. Host based firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 269

A PC technician is working on a former employee's encrypted laptop. Which of the following can be used to recover the data?

A. PKI
B. Public key
C. Key escrow
D. CRL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 270
A security analyst has been tasked with securing a guest wireless network. They recommend the company use an authentication server but are told the funds are not available to set this up. Which of the following BEST allows the analyst to restrict user access to approved devices?

A. Antenna placement
B. Power level adjustment
C. Disable SSID broadcasting
D. MAC filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 271
A risk is identified that an attacker, given the right credentials, could potentially connect to the corporate network from a nearby business's parking lot. Which of the following controls can be put in place to reduce the likelihood of this occurring? (Select TWO).

A. TKIP
B. Antenna placement
C. Power level controls
D. WPA
E. WPA2
F. Disable SSID broadcasting

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 272
Which of the following protocols is unsecure due to replay attacks against the IV?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 273
Which of the following BEST mitigates cross-site scripting (XSS)?

A. Filtering special characters in form input fields to prevent executing script tags
B. Moving a database from a publicly accessible web server to a secured internal database server
C. Removing or disabling server-side includes from the web server software
D. Ensuring a website uses the HTTPS protocol to transmit encrypted authentication and data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 274
An application developer is tasked with creating on-screen messages when a user does not input information correctly. Which of the following would MOST likely be included?

A. A text box displaying the current system performance metrics and workload
B. A command prompt which traps user exception errors
C. Text informing the user that they have entered improperly formatted data
D. A lockout of the user session after multiple failed attempts to format the information

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 275
An IT project manager is in charge of a new DLP project for their research department. The project is important because it will:

A. prevent malicious executable files and spyware from running on the department's computers.
B. allow restoration of data from full and incremental backups.
C. block SQL injection attempts by malicious users and software.
D. allow detection and prevention of data being copied or removed from the department's computers.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 276
A popular software application is used on all company workstation desktop and laptop computers. Which of the following is the BEST patch management process?

A. The patch management software should be approved by the change management group to ensure adherence to corporate policies.
B. The Chief Information Officer should approve and centrally deploy the patch to all company workstations in a staggered manner.
C. Users should individually download and verify the patch with an MD5 checksum utility before applying it to their own workstation.
D. The support team should receive vendor update notifications and deploy patches in test environment before deploying to workstations.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 277
Which of the following is a vulnerability associated with disabling pop-up blockers?

A. An alert message from the administrator may not be visible
B. A form submitted by the user may not open
C. The help window may not be displayed
D. Another browser instance may execute malicious code

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 278
A company maintains an off-site facility in which they can constantly replicate their base of operations. Which of the following BEST describes such a site?

A. Warm site
B. Electronic vault
C. Cold site
D. Hot site

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 279
Which of the following principles is affected by a DDoS attack?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 280

An attacker is using a technique in which they intercept a transmission between two co-workers, impersonating one of the co-workers. Which of the following is the attacker MOST likely using?

A. Man-in-the-middle
B. Spoofing
C. Smurf attack
D. Fraggle attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 281
A company's web server is attacked by an unknown exploit. Which of the following is MOST likely the culprit?

A. Zero-day exploit
B. Directory traversal
C. LDAP injection
D. XML injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 282
A security administrator has reason to believe that outsiders have been attempting to connect to an internal

server. Which of the following logs should they check?

A. Access log
B. Application log
C. System log
D. Audit log

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 283

Users in the marketing department are given a different level of access to files than users in the accounting department. Which of the following types of access control does this BEST describe?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 284
A supervisor in the human resources department has been given additional job duties in the accounting department. Part of their new duties will be to check the daily balance sheet calculations on spreadsheets that are restricted to the accounting group. In which of the following ways should the account be handled?

A. The supervisor should be allowed to have access to the spreadsheet files, and their membership in the human resources group should be terminated.
B. The supervisor should be removed from the human resources group and added to the accounting group.
C. The supervisor should be added to the accounting group while maintaining their membership in the human resources group.
D. The supervisor should only maintain membership in the human resources group.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 285
Which of the following is the fundamental risk of a single sign-on computing environment?

A. The account has access to the internal management network.
B. The account has administrator access to all production computing resources.

C. The account can access resources without requesting authenticated again.
D. The account is escalated to administrator access without logging.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 286
Which of the following attacks does the following exemplify?

http://www.internet.com/cgi-bin/some.cgi?| /bin/ps aux

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 287
A company is having problems with ad-hoc changes to their router and firewall configurations. Which type of mitigation activity would BEST address this problem?

A. Implement security controls
B. Incident management
C. Deploy RADIUS
D. Change management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 288
An IT security technician is required to create an environment which supports quickly deploying securely configured servers. Which of the following BEST meets this need?

A. Virtualization
B. Patch management
C. Host based firewall
D. Group policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 289
Which of the following will allow an IT security technician to prevent threats against the company backup tapes while in transit?

A. USB encryption
B. Mobile device encryption
C. Trusted platform module
D. Database encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 290
Which of the following will require a security technician to carefully review the company's SLAs?

A. TPM chip
B. Database encryption
C. RADIUS
D. Cloud computing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 291
A student is interested in learning about distributed denial of service attacks. Which of the following types of malware is MOST likely the primary focus of their study?

A. Botnets
B. Logic bombs
C. Spyware
D. Trojans

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 292
Which of the following should a security technician implement to identify untrusted certificates?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 293
Which of the following allows a security technician to recover from a loss of staff after an earthquake?

A. Business continuity plan
B. Continuity of operations
C. Disaster recovery
D. Succession planning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 294
Which of the following is a preventative security control?

A. Alarms
B. Hardware locks
C. Security logs
D. CCTV

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 295
A system administrator is notified by a staff member that their laptop has been lost. The laptop contains the user's digital certificate. Which of the following will help resolve the issue? (Select TWO).

A. Revoke the digital certificate
B. Mark the key as private and import it
C. Restore the certificate using a CRL
D. Issue a new digital certificate

E. Restore the certificate using a recovery agent

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 296
The IT security team creates a document that covers specific rules and requirements on data retention. Which of the following types of data retention documentation did the team create?

A. Procedures

B. Policy

C. Standards

D. Guidelines

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 297
A security analyst is establishing a disaster recovery site and is not concerned with cost. They want the recovery site to be operational within 13 hours. Which of the following would BEST help achieve this result?

A. Hot site

B. Warm site

C. Cold site

D. Mutual aid agreement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 298
One of the main objectives of disaster recovery includes:

A. uninterrupted operations.

B. safety of human lives.

C. establish a call tree system.

D. directions to the recovery site.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 299
Internal auditors would like to decrease the effectiveness of brute force attacks. Which of the following measures would aid in deterring this type of attack?

A. Password Recovery
B. Account Removal
C. Account Lockouts
D. Password Expiration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 300
Which of the following authentication services uses a Key Distribution Center?

A. Sesame
B. Kerberos
C. LDAP

D. RADIUS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Topic 4, Volume D

QUESTION 301
Which of the following authentication services uses authentication, authorization, and accounting?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 302
A security engineer has implemented a server in the DMZ that receives HTTPS Internet requests. The web pages served are retrieved via HTTP from other backend servers. Which of the following devices is MOST likely performing these functions?

A. Reverse Proxy

B. VPN Concentrator

C. URL Filter

D. Firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 303
A user often works from the public open Wi-Fi available at their favorite coffee shop. The user has asked the security engineer to recommend safe practices to prevent other coffee shop patrons from being able to acquire the sensitive information in their laptop's network traffic. Which of the following should MOST likely be recommended to meet this goal?

A. Enable the web application firewall to only allow SSL.

B. Use a host-based intrusion prevention system.

C. Use VPN connections to the corporate network.

D. Use the host-based firewall on the laptop.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 304
A security engineer is testing encryption ciphers for performance. Which of the following ciphers offers strong encryption with the slowest speed?

A. RC4

B. 3DES

C. AES

D. Blowfish

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 305
Which of the following is an authentication method that can be secured by using SSL?

A. RADIUS

B. LDAP

C. TACACS+

D. Kerberos

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 306
A security engineer is given new application extensions each month that need to be secured prior to implementation. They do not want the new extensions to invalidate or interfere with existing application security. Additionally, the engineer wants to ensure that the new requirements are approved by the appropriate personnel. Which of the following should be in place to meet these two goals? (Select TWO).

A. Patch Audit Policy
B. Change Control Policy
C. Incident Management Policy
D. Regression Testing Policy
E. Escalation Policy
F. Application Audit Policy

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 307
If an administrator is blocking port 22, which of the following protocols will this affect? (Select TWO).

A. SNMP
B. SSH
C. SMTP
D. FTP
E. Telnet
F. SCP

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 308
A user in the accounting department receives a phone call from someone stating that they are from the IT department. The caller informs the user that their username and password have been compromised. They then request the user's username and password to verify the information. Which of the following social engineering attacks is being performed?

A. Whaling
B. Vishing

C. Spoofing
D. Pharming

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 309
A user is trying to go to their banking website. They notice it looks a little different today than it looked yesterday. They enter their username and password, but the page does not change. They try it again with the same result. Which of the following has just occurred to the user?

A. IV
B. Spoofing
C. Pharming
D. Spim

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 310
Which of the following should an administrator implement in a server room to help prevent static electricity?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 311
During an audit, the security administrator discovers that there are several users that are no longer employed with the company but still have active user accounts. Which of the following should be performed?

A. Account recovery
B. Account disablement
C. Account lockouts

D. Account expiration

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 312
An IT manager is planning an overnight hardware refresh on dozens of computers. The refresh involves running an automated script to back up sensitive data from the old computers, physically replace them, and then run a data restoration script on the new computers. The new computers must be functional by the following morning with minimal impact during business activities before or after the replacement. The lab tests were successful, but the IT manager wants to be prepared for any contingency. Which of the following would be the BEST course of action?

A. Have a schedule in place with a firm time frame to allow for the old computers to be put back in place should any part of the refresh fail.
B. Enlist the users to back up their own data and restore it, thus removing this point of concern and easing the refresh time constraints.
C. Create a baseline image and install it on the new computers after they are installed to minimize network congestion upon first boot.
D. Perform the refresh in a staggered manner where small groups of computers are backed up and replaced completely before moving to the next group.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 313
The Chief Security Officer (CSO) is concerned about misuse of company assets and wishes to determine who may be responsible. Which of the following would be the BEST course of action?

A. Create a single, shared user account for every system that is audited and logged based upon time of use.
B. Implement a single sign-on application on equipment with sensitive data and high-profile shares.
C. Enact a policy that employees must use their vacation time in a staggered schedule.
D. Separate employees into teams led by a person who acts as a single point of contact for observation purposes.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 314
A system administrator has concerns regarding their users accessing systems and secured areas using others' credentials. Which of the following can BEST address this concern?

A. Create conduct policies prohibiting sharing credentials.
B. Enforce a policy shortening the credential expiration timeframe.
C. Implement biometric readers on laptops and restricted areas.

D. Install security cameras in areas containing sensitive systems.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 315
A home user has been alerted by their antivirus software of a possible malicious attack after they visited an online chat. Which of the following attacks is the computer experiencing if the antivirus alert window shows "<script> detected in input field x=0"?

A. XSS
B. Zero-day
C. XML injection
D. Malicious add-on

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 316
A security administrator is reviewing the packet-per-second counter on the firewall external interface. Which of the following should be reviewed to determine if the firewall is under a DoS attacks?

A. SNMP community string
B. Network bandwidth baseline
C. External interface port speed settings
D. Firewall access control list logs
"Pass Any Exam. Any Time." - www.actualtests.com 109 CompTIA SY0-301 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 317
A security administrator needs to install new code into the firewall to fix a known DoS vulnerability (which exists on the firewall). Which of the following should they do before upgrading the corporate firewall?

A. Obtain approval from change management.
B. Update the incident management documents.
C. Evaluate any changes to the current procedures.
D. Review the changes with the helpdesk and the users.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 318
The security director at a pharmaceutical company is reviewing the latest incident documentation and notices they cannot account for who had possession of the compromised server's hard drive during the weekend. Which of the following is this an example of?

A. Lack of incident witnesses

B. Improper order of volatility

C. Broken chain of custody

D. Invalid image hashes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 319
A security trainer is developing training to describe the benefits of using a digital signature. Which of the following is the primary benefit of this technology?

A. Encryption

B. Hashing

C. Non-repudiation

D. Steganography

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 320
A security analyst is reviewing a new application and notices that the cookies for this application are set to store information in the clear on a customer's machine when the customer checks the remember password box. Which of the following should be implemented to remediate this issue?

A. Hashing

B. Key escrow

C. Transport encryption

D. Asymmetric encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 321
A security manager received the results of a vulnerability assessment stating that several accounts were

assigned to the domain administrator group, even though the employees did not need this level of access. Which of the following needs to be performed for mitigation of this issue?

A. Incident management audits
B. Risk calculation
C. User permissions reviews
D. Change management reviews

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 322
A customer receives a pop-up box stating that their account may have been compromised and they need to enter in their password to continue. This could be an example of which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 323
A network administrator has a separate user account with rights to the domain administrator group. However, they cannot remember the password to this account and are not able to login to the server when needed. Which of the following is MOST accurate in describing the type of issue the administrator is experiencing?

A. Single sign-on
B. Authorization
C. Access control
D. Authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 324
A network administrator has no trouble remembering their password but is not able to login to the server they need to work on. They later find out they were never added to the group with rights to work on this system. Which of the following is MOST accurate in describing this type of issue?

A. Authorization
B. Authentication
C. Mandatory access control
D. Single sign-on

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 325
A security analyst noticed an increase in malware infections on a user's system. They identified an email that requests the user change their password. This attack would BEST be described as which of the following?

A. Phishing
B. Spoofing
C. Privilege escalation
D. Shoulder surfing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 326
A database administrator receives a call on an outside telephone line from a person who states that they work for a well-known database vendor. The caller states there have been problems applying the newly released vulnerability patch for their database system, and asks what version is being used so that they can assist. Which of the following is the BEST action for the administrator to take?

A. Thank the caller, report the contact to the manager, and contact the vendor support line to verify any reported patch issues.
B. Obtain the vendor's email and phone number and call them back after identifying the number of systems affected by the patch.
C. Give the caller the database version and patch level so that they can receive help applying the patch.
D. Call the police to report the contact about the database systems, and then check system logs for attack attempts.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 327
The datacenter manager is reviewing a problem with a humidity factor that is too low. Which of the following environmental problems may occur?

A. EMI emanations

B. Static electricity

C. Condensation
D. Dry-pipe fire suppression

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 328
A user receives an email from a friend. Attached to the email is a compressed file named `vacation pictures'. The user opens the attachment and immediately loses Internet connectivity. Which of the following is the MOST likely cause of the loss of connectivity?

A. The file contained a Botnet.
B. The file contained a Logic Bomb.
C. The file contained a Trojan.
D. The file contained Adware.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 329
A caller reports that they are unable to login to the server and asks that their password be reset to `abcde'. Which of the following social engineering attacks is MOST likely being attempted?

A. Whaling
B. Tailgating
C. Vishing
D. Impersonation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 330
Which of the following attacks directly modifies a data repository maintained on a server? (Select TWO).

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 331
A UNIX administrator would like to use native commands to provide a secure way of connecting to other devices remotely and to securely transfer files. Which of the following protocols could be utilized? (Select TWO).

A. RDP
B. SNMP
C. FTP
D. SCP
E. SSH

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 332
A network administrator has purchased two devices that will act as failovers for each other. Which of the following concepts does this BEST illustrate?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 333

A security technician is placing a new router into service. They have removed HTTP and TFTP abilities from the router. Which of the following does this BEST illustrate?

A. Disabling unnecessary accounts
B. Disabling unused interfaces
C. Disabling unnecessary services
D. Protecting management interfaces

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 334
An organization recently began implementing a new policy in which users' passwords must meet requirements such as length, upper and lower-case letters, numbers, and symbols, as well as requiring that passwords be changed every 20 days. This is BEST known as: (Select TWO)

A. account complexity.
B. account expiration.
C. password recovery.
D. password expiration.
E. account recovery.
F. password complexity.

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 335
A new employee installed an application on their workstation that allowed Internet users to have access to their workstation. Which of the following security related training could have mitigated this action?

A. Use of proper password procedures
B. Use of personally owned devices
C. Use of social networking and P2P networks
D. Use of clean desk policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 336
An internal server that is on an isolated network was recently compromised, and intellectual property was copied from the server. Which of the following attacks would this BEST describe?

A. Pharming
B. Client-side attack
C. Malicious insider
D. Privilege escalation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 337
A system administrator is tasked with reverting from a trusted OS to a standard OS. Which of the following AAA controls will this negate?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 338
An employee brings in their personal laptop to work and plugs into an empty jack in the office. They have a good cable and a link light, but cannot access the network. Which of the following controls BEST describes the lack of connectivity?

A. MAC filtering
B. Disabled port
C. Loop protection
D. Filtered DHCP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 339
Which of the following statements is TRUE about sending data to the cloud using HTTP?

A. The data will arrive to the cloud faster.
B. There is no guaranteed confidentiality.
C. Non-repudiation about the recipient of the data.
D. It is the most secure method of transfer.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 340
Which of the following is a layer three protocol used for VPN connections?

A. SSH
B. ICMP
C. IPSec

D. SSL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 341
Which of the following is a hardware-based control that would restrict a computer from joining a wireless network?

A. MAC filtering
B. Power level control
C. Access list
D. Antenna placement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 342
Which of the following network devices allows a security technician to perform malware inspection?

A. Load balancer
B. VPN concentrator
C. Firewall
D. NIPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 343
Which of the following network design elements allows a security administrator to control and prevent systems that are not patched from accessing the company resources remotely?

A. NAT
B. DMZ
C. Patch management
D. NAC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 344
Which of the following components does a security administrator MOST likely need a formal documented procedure for, as new staff members enter the company?

A. Trust model development
B. Private key
C. Public key infrastructure
D. Registration

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 345
A security technician has just been called into a management meeting where the team is defining requirements for their new access control system. One of the staff members brings up the issue of timing attacks. Which of the following access control methods is susceptible to timing attacks?

A. Biometrics
B. MAC
C. CAC
D. Tokens

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 346
Which of the following access control mechanisms supports strong authentication? (Select THREE).

A. PIV
B. Discretionary access control
C. Implicit deny
D. Separation of duties
E. Common access card
F. Tokens

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 347
A security administrator has been tasked with explaining access control aspects to a peer. Which of the following is a directory service supporting both Windows and Linux authentication?

A. LDAP

B. Trusted OS

C. TACACS+

D. PAM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 348
Which of the following security account management techniques should a security analyst implement to prevent staff, who has switched company roles, from exceeding privileges?

A. Internal account audits

B. Account disablement

C. Time of day restriction

D. Password complexity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 349
A user calls the technician and states that their system is performing oddly at logon. The technician runs a program to scan the computer for infections. The program identifies the Winlogon.exe and Run Once Registry key launching winlogin.exe with additional parameters that are not present on other systems. Which the following BEST describes the type of infection?

A. Rootkit

B. Virus

C. Trojan

D. Adware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 350
A technician wants to purchase a USB encryption product. They are concerned about the amount of data on the USB sticks and the time it will take to encrypt large amounts of data. Which type of

encryption should they look to implement?

A. PGP

B. TLS
C. Symmetric
D. Asymmetric

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 351
Which of the following is a legal benefit of digitally signing emails?

A. The message uses a public key.
B. The message is encrypted.
C. The message offers non-repudiation.
D. The message uses a private key.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 352
A user receives a phone call from their ISP stating they have a problem and they require access to the corporate network. The user is not aware of any problems and asks to return the phone call in a few minutes. When the user calls the ISP back they are not aware of any calls made to the user.
This was which of the following attacks?

A. Spear phishing
B. Impersonation
C. Evil Twin
D. Hoax

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 353

A network technician notices on Thursday the daily backups failed on Monday and Wednesday. The last backup was on Friday of last week. The technician wants to only backup the changes that have been made since last Friday. Which of the following backups should be run today?

A. A full backup
B. A differential backup
C. An incremental backup
D. Rerun incremental backups for Monday and Wednesday

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 354
An IT administrator is concerned about the location where a new building is being built. They believe the building is in a flood plane. The administrator has no hard facts and asks other companies in the area for their opinions. They take this initial information and present it to the CEO. Which of the following techniques has been used?

A. Incident Management
B. Risk Assessment
C. Qualitative Analysis
D. Quantitative Analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 355
XYZ Corporation is about to purchase another company to expand its operations. The CEO is concerned about information leaking out, especially with the cleaning crew that comes in at night. The CEO would like to ensure no paper files are leaked. Which of the following is the BEST policy to implement?

A. Social media policy
B. Data retention policy
C. CCTV policy
D. Clean desk policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 356
Running the following command ` or 1 = 1 -- on a website input field is an example of which of the following types of attack?

A. Cross Site Script
B. Session Hijacking
C. XML Injection
D. SQL Injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 357
The administrator would like to implement hardware assisted full disk encryption on laptops. Which of the following would MOST likely be used to meet this goal?

A. TPM
B. USB Drive
C. Key Escrow
D. PKI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 358
The system engineer needs to be able to scale the number of virtual machines they run on demand. They have outsourced this to a secure cloud provider. Of which of the following is this an example?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 359
A security architect needs to securely encrypt all of the data from a database application in transit and at rest. Web-based front end communications to the user and SQL calls to the database backend need to be secure. Which of the following should be enabled to complete this goal?

A. IPSec
B. Web Application Firewall
C. Trusted OS Extensions
D. Transparent Data Encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 360
To ensure compatibility with their flagship product, the security engineer is tasked to recommend an encryption

cipher that will be compatible with the majority of third party software and hardware vendors. Which of the following should be recommended?

A. SHA

B. MD5

C. Blowfish

D. AES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 361
A programmer is terminated. Precisely a month later, random files and folders start disappearing. Which of the following types of malware MOST likely could have been installed before the programmer was terminated?

A. Rootkit

B. Trojan

C. Backdoor

D. Logic bomb

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 362
Which of the following would be used to determine the last person who entered into a specific area?

A. Event logs

B. Audit logs

C. Access logs

D. Security logs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 363
Which of the following can BEST be implemented on a mobile phone to help prevent any sensitive data from being recovered if the phone is lost?

A. Voice encryption

B. Screen locks

C. Device encryption

D. GPS tracking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 364
Which of the following can a security administrator implement on a mobile phone to help prevent another person from picking up the phone and making personal calls?

A. Bluetooth PIN
B. Device encryption
C. Screen locks
D. Cable lock

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 365
Which of the following policies could be implemented to help prevent users from displaying their login credentials in open view for everyone to see?

A. Privacy
B. Clean desk
C. Job rotation
D. Password complexity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 366
A security administrator wants to implement a security authorization method that will determine when employees are able to use company computers. Which of the following can be implemented to accomplish this requirement?

A. Mandatory access control
B. Role based access control
C. Time of day restrictions
D. Single sign-on

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 367
The Vice President of a corporation is receiving unsolicited emails attempting to dig up sensitive information regarding the company. Which of the following attacks BEST describes this?

A. Spam
B. Bluejacking
C. Spoofing
D. Whaling

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 368
A system administrator has noticed that users change their password many times to cycle back to the original password when their passwords expire. Which of the following would BEST prevent this behavior?

A. Assign users passwords based upon job role.
B. Enforce a minimum password age policy.
C. Prevent users from choosing their own passwords.
D. Increase the password expiration time frame.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 369
A systems administrator implements a written security policy barring employees from using their own personal USB flash drives. Which of the following BEST describes what the administrator wishes to accomplish? (Select TWO).

A. Prevent autorun infections from spreading.
B. Maintain a standard equipment baseline.
C. Ensure user data is stored on network shares.
D. Protect sensitive company data.
E. Enforce policies relating to clean desks.
F. Prevent multimedia distractions during work.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 370
To prevent data loss in the event of laptop theft, which of the following should be implemented?

A. Whole disk encryption
B. Key-based cable lock
C. Complex password rules
D. Power-on password

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 371
Users are reporting to the system administrator that advertisements in browser windows open up whenever they visit popular news sites. The administrator has not seen any evidence of malicious activity regarding this. Which of the following would be the BEST course of action to address this?

A. Install anti-spyware software.
B. Disable port 80 in the firewall ruleset.
C. Enable pop-up blockers by default.
D. Update the antivirus definitions.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 372
The systems administrator notices that many employees are using passwords that can be easily guessed or are susceptible to brute force attacks. Which of the following would BEST mitigate this risk?

A. Enforce password rules requiring complexity.
B. Shorten the maximum life of account passwords.
C. Increase the minimum password length.
D. Enforce account lockout policies.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 373
The system administrator has a large group of consultants that are brought in on a temporary basis several times a year for a particular project. They do not want to recreate their accounts every time. Which of the following would be the BEST course of action to handle these consultants with minimum overhead?

A. Enforce a policy that locks all accounts after short inactivity.
B. Rename the consultant's account upon return.
C. Disable any accounts not active or currently in use.
D. Change the passwords on the consultant accounts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 374
The systems administrator has asked users not to forward email virus warnings from the Internet to each other. Which of the following is the MAIN concern?

A. Legitimate corporate virus warnings will be ignored.
B. Users will install their own antivirus software.
C. The emails are social engineering attempts.
D. Required updates will be deferred by misinformation.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 375
The system administrator wishes to prevent broadcasting over default NetBIOS ports. Which of the following ports should be disabled?

A. 110
B. 137
C. 143
D. 443

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 376
The systems administrator wishes to prevent crosstalk in the network cabling between users in two separate security domains. Which of the following addresses this?

A. Color code all network cables
B. Use only plenum rated cables
C. Employ EMI shielding
D. Use only UTP cabling

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 377
A systems administrator wishes to avoid war driving intrusions on the company's wireless network.
Which of the following would BEST address this?

A. Use WEP encryption instead of WPA.
B. Relocate the antennas to reduce external coverage.
C. Alter the access point's default configuration.
D. Change the SSID so that it does not identify the company.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 378
A system administrator is concerned that attackers might attempt to connect to the default port used by TELNET. Which of the following ports should the administrator block?

A. 21
B. 22
C. 23
D. 25
"Pass Any Exam. Any Time." - www.actualtests.com 131 CompTIA SY0-301 Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 379
The network administrator has configured an 8-port switch with three different VLANS. Which of the following should be installed to enable all computers in the three VLANS to communicate with each other?

A. Bridge
B. Load balancer
C. Proxy
D. 802.1q

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 380
When an email message is digitally signed:

A. the sender uses the recipient's public key to sign the email.
B. the sender uses their public key to sign the email.
C. the recipient validates the sender's identity with the sender's public key.
D. the recipient validates the sender's identity with the recipient's private key.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 381
The security administrator must implement a stream cipher to transmit an encrypted video stream.
Which of the following ciphers should be used?

A. Blowfish
B. DES
C. AES
D. RC4
"Pass Any Exam. Any Time." - www.actualtests.com 132 CompTIA SY0-301 Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 382
Which of the following digital certificates can be issued for use by a company's web server? (Select TWO).

A. .company.com
B. *.company.com
C. company.com
D. sales-1.department.company.com
E. 156.78.201.43

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 383
A user encrypted document files with their company's assigned digital certificate and stored them on the corporate file server. Their computer crashed and was formatted and reimaged, causing the loss of their PKI keys. Which of the following is true about the user's files because the recovery agent had not been created by the domain administrator?

A. The files can always be recovered and decrypted by the domain administrator.

B. The files can be recovered and decrypted only after a domain administrator creates a recovery agent.
C. The files cannot be recovered and decrypted because the public key is lost.
D. The files cannot be recovered and decrypted because the private key is lost.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 384
Which of the following authentication factors describes something someone knows?

A. Which finger to scan

B. A credit card PIN number
C. A smart card
D. The location of a token

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 385
A security administrator wants to implement the appropriate security control to ensure that terminated employees are disabled from the system even if the human resource department has failed to provide a termination notice to the IT department. Which of the following can be implemented to accomplish this?

A. Account lockout
B. Account expiration
C. Time of day restriction
D. Password expiration

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 386
A security administrator wants to deploy security controls to mitigate the threat of company employees' personal information being captured online. Which of the following would BEST serve this purpose?

A. Anti-spyware
B. Antivirus
C. Host-based firewall
D. Web content filter

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 387
Which of the following statements is MOST likely to be included in the security awareness training about P2P?

A. P2P is always used to download copyrighted material.
B. P2P can be used to improve computer system response.
C. P2P may prevent viruses from entering the network.
D. P2P may cause excessive network bandwidth.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 388
Which of the following mitigates the risks of an attack aimed at the continuous availability of a system?

A. Journaled File System
B. Anycast
C. Dual core
D. Multicast

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 389
A security administrator wants to ensure that the data contained within the company database cannot be modified by unauthorized employees. Which of the following should be enforced to allow for this?

A. Database encryption
B. Server clustering
C. Input validation
D. Separation of duties

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 390

A network administrator has recently deployed a layer three switch. Which of the following can they implement to prevent computers on the same broadcast domain to communicate between each other?

A. MAC filtering

B. Anti-spoofing

C. VLAN

D. IP access control lists

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 391
A forensic investigator has imaged a hard drive on August 1. Just before the case goes to court on August 10, they discover that the hard drive they had imaged has been installed on a different computer, changed by someone, and then placed back on their desk. Which of the following did the investigator MOST likely use to make such a discovery?

A. The computer's screenshot

B. The drive's image hash

C. The chain of custody

D. The order of volatility

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 392
A company's chief information officer (CIO) has analyzed the financial loss associated with the company's database breach. They calculated that one single breach could cost the company $1,000,000 at a minimum. Which of the following documents is the CIO MOST likely updating?

A. Succession plan

B. Continuity of operation plan

C. Disaster recovery plan

D. Business impact analysis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 393
An employee is undergoing training on the company information classification, as they have been tasked with assigning values to various database fields. Which of the following MOST likely describes the employee's role within the company?

A. Information security officer
B. System owner
C. Privacy officer
D. Data owner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 394
Which of the following must a technician implement in order to ensure that company policies on account management are being implemented by the IT department?

A. Perform regular interviews of the IT staff.
B. Perform routine system audits.
C. Review the IT policies.
D. Review the IT procedures.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 395
Which of the following encryption methods should be used by devices, such as cell phones, that may have limited computing power, keeping in mind that the algorithm MUST use public and private keys in the encryption process?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 396
Which of the following encryption methods is thought to be unbreakable as long as the below conditions are met?

-It must be securely distributed and stored.

-It must be used for a singular instance only.

-It must contain random values to engage the algorithm.

-It must be as long as the bits it is encrypting.

A. Whole Disk Encryption
B. Quantum Cryptography
C. Elliptical Curve Cryptography
D. One-Time-Pad

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 397
Which of the following wireless protocols could be vulnerable to a brute-force password attack? (Select TWO).

A. WPA2-PSK
B. WPA EAP - TLS
C. WPA2-CCMP
D. WPA CCMP
E. WPA - LEAP
F. WEP

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 138 CompTIA SY0-301 Exam

QUESTION 398
Which of the following wireless protocols does not offer mutual authentication? (Select TWO).

A. WPA - EAP
B. WPA2-PEAP
C. WPA2-TKIP
D. 802.11i
E. WEP

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 399
When reviewing the logs for an FTP server on the DMZ, a security analyst notices the following pattern in the logs:

Access denied user adminpassword aaaaaaaa

```
Access denieduser adminpassword aaaaaaab

Access denied user adminpassword aaaaaabb

Access granted user rmleepassword passw0rd1

Access denieduser adminpassword aaaaabbb
```

Which of the following types of attacks is MOST likely occurring?

A. Brute-force
B. DDOS
C. Zero day
D. Phishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 400
An auditor is given access to a conference room to conduct an analysis. When they connect their laptop's Ethernet cable into the wall jack, they are not able to get a connection to the Internet but have a link light. Which of the following is MOST likely causing this issue?

A. Ethernet cable is damaged
B. The host firewall is set to disallow outbound connections
C. Network Access Control
D. The switch port is administratively shutdown

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Topic 5, Volume E

QUESTION 401
Which of the following is a way to implement a management control to mitigate data loss in case of a mobile device theft?

A. Mobile device policy
B. Disk encryption
C. Parity bit requirement
D. Solid state drive

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 402
A new security administrator just enabled alerting on a replacement NIPS system and is getting a flood of emails telling them about issues on the network. Which of the following is the MOST likely cause of these alerts?

A. Separation of Duties
B. Job Rotation
C. False Positives
D. False Negatives

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 403
An intruder has gained entry into a corporate office via tailgating. Which of the following could be used as a second physical layer of defense to identify them as an intruder to the rest of the employees?

A. Video surveillance
B. Complex passwords
C. Mantrap
D. ID badges

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 404
Which of the following has the HIGHEST level of password entropy?

A. Hdkowei123%%
B. aspoonfullofsugar
C. dhoksh12$
D. Password2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 405
A security architect is working to implement an all-in-one device that acts as a firewall, URL filter, and IPS.

Which of the following is the MOST likely concern to take into consideration with this type of device?

A. Succession planning
B. Single point of failure
C. Overheating
D. Load balancing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 406
Shortly after a web administrator installed a new web server and application for the company to be used by the public, they noticed specific, targeted attacks for the type and version of web server and application code used on the site. Which of the following methods are MOST likely being used? (Select TWO).

A. The attacker used a web proxy and scanner to crawl the website to identify the servers command interpreter.
B. The attacker used DLP software to identify sensitive information in the website.
C. The attacker used SQL injection to obtain the code of the application.
D. The attacker mirrored the site with RAID software to ensure fault tolerance and redundancy.
E. The attacker searched for common default strings to identify the software and known vulnerabilities.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 407
The help desk agent enjoys surfing the Internet for information on new networking equipment and signs up for user forums that discuss new technology. Recently, advertisements for local events and businesses appear on web pages that they view. The MOST likely reason for this occurrence is that:

A. GPS tracking on their cell phone and laptop identified their location to a vendor website.
B. a polymorphic virus or rootkit has infected the kernel of their laptop operating system, and was not detected by the antivirus software.
C. their laptop has been compromised by a botnet and is performing a reconnaissance attack on the sites whose ads are displayed.
D. at least one website added adware and tracking cookies that identified the probable location of their external gateway IP address.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 408

A security engineer has been asked to come up with a design solution which will separate

departments in their organization. The departments must maintain strict security controls, only allowing access to servers by users within the same department. Which of the following design components would help meet this objective?

A. VLANs
B. NAT
C. DMZs
D. VTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 409
A technician has placed new network devices into service, and requires monitoring of these devices. Which of the following ports should be open on the firewall to allow for monitoring of network devices?

A. TCP 143
B. TCP 161
C. UDP 110
D. UDP 161

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 410
Which of the following is a non-proprietary protocol that provides secure data transmission?

A. ICMP
B. TELNET
C. TLS
D. SSL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 411
A security technician has been asked to place a device into service that will log intrusion attempts on multiple devices; no action should be taken during the intrusion attempts. Which of the following devices should be placed into service?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 412
Which of the following allows telecommuters to establish a secure remote connection to the corporate network from home?

A. IPSec
B. SNMP
C. SFTP
D. WPA2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 413
There have been several data security breaches at XYZ Company. Which of the following would BEST improve compliance with internal rules and regulations?

A. Data labeling
B. Security policy training
C. Clean desk policy
D. Information classification

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 414
A security administrator has been warned of upcoming attacks on the network. Which of the following should be implemented to isolate and log hacking attempts on a network?

A. Honeypot
B. Sniffer
C. Port scanner
D. Vulnerability scanner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 415
An administrator has recently rolled out redundant servers in their organization. Which of the following concepts does redundancy provide for?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 416
Which of the following wireless encryption technologies is based on a block cipher and provides for both authentication and confidentiality?

A. CCMP
B. TKIP
C. LEAP
D. PEAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 417
Which of the following types of trust models is used by a PKI?

A. Transitive
B. Open source
C. Decentralized
D. Centralized

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 418
Which of the following would be the MOST cost-effective security solution for a user in a small home office?

A. Network-based firewall

B. Host-based intrusion detection system

C. Network intrusion prevention system

D. Host-based firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 419
A company has developed a hot site to resume operations in the event of a catastrophe. Which of the following does this describe?

A. Removing single points of failure

B. Continuity of operations

C. Succession planning

D. Business impact analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 420
A security architect has developed a server framework in which several firewalls share state tables in order to provide redundancy. Which of the following does this describe?

A. Clustering

B. RAID

C. Cold site

D. Hot spare

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 421
Which of the following can be mitigated by not storing usernames and passwords in a web browser?

A. Cross-site scripting attacks

B. Input validation errors

C. Error and exception handling
D. Cross-site request forgery attacks

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 422
A security technician notices that certain users have been accessing newly created files on the server that are originating from other departments. Which of the following risk mitigation strategies could have prevented these actions?

A. Incident management
B. Change management
C. User rights and permission reviews
D. Routine auditing
"Pass Any Exam. Any Time." - www.actualtests.com 147 CompTIA SY0-301 Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 423
A security technician at a company that uses port security documents workstation moves due to new hires in the marketing department. Which of the following risk mitigation strategies does this BEST illustrate?

A. Incident management
B. Change management
C. Routine auditing
D. Security controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 424
A technician has implemented a system in which all workstations on the network will receive security updates on the same schedule. Which of the following concepts does this illustrate?

A. Patch management
B. Application hardening
C. White box testing
D. Black box testing

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 425
Which of the following firewall rules blocks smtp and web traffic to a server?

A. deny tcp any server lt 25
B. deny tcp any server eq 0-1024
C. deny udp any server eq 0-1024
D. deny tcp any server eq 80-1024
"Pass Any Exam. Any Time." - www.actualtests.com 148 CompTIA SY0-301 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 426
Which firewall rule would block all traffic to a server?

A. deny tcp any server 0-65535
B. deny udp any server 0-65535
C. deny ip any server
D. deny tcp any server 80

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 427
Which of the following services should be disabled to stop unsecure interactive logins? (Select TWO).

A. Rlogin
B. Terminal Services
C. Remote Desktop
D. SNMP
E. Telnet
F. SSH

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 428
The security administrator noticed a lot of input validation vulnerabilities on the corporate website. Which of the

following types of assessment tools was used?

A. Network sniffing
B. Source code review
C. Vulnerability testing

D. Baseline reporting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 429
Translating many IP addresses to one IP is an example of:

A. PAT.
B. NAC.
C. MAC.
D. DMZ.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 430
Trusted OS implementations require which of the following types of access control?

A. Mandatory
B. Role-based
C. Discretionary
D. Rule-based

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 431
Which of the following security measures assures wireless user authentication?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 432
Which of the following network elements would BEST ensure the confidentiality of transferring a virtual machine to another virtual server?

A. Crossover cable
B. DMZ
C. Dedicated VLAN
D. Server adjacency

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 433
Why would a security administrator NOT make use of an implicit deny all rule on a firewall?

A. A security administrator wants to capture specific traffic types.
B. A security administrator needs to log all denied traffic.
C. A security administrator needs to permit all certain types of traffic.
D. A security administrator needs to allow BGP traffic.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 434
The security architect needs to ensure that employees who are terminated are immediately denied access to corporate resources protected by their PKI architecture. Which of the following PKI components would BEST assure this?

A. Key escrow
B. CRL
C. Recovery agent
D. OCSP
"Pass Any Exam. Any Time." - www.actualtests.com 151 CompTIA SY0-301 Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 435

The IT director wants to allow several personal access to manage the network routers over UDP and be able to perform an audit of those changes. Which of the following should be enabled on the routers? (Select TWO).

A. VTY
B. Local console
C. RADIUS
D. SSH
E. Logging
F. TACACS

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 436
A security analyst has been tasked with explaining the different types of malware to colleagues. The two malware types that the group seems to be most interested in are trojans and rootkits. Which of the following differentiates these two types of malware?

A. Trojans are hidden within another program while rootkits are hidden from the OS.
B. Trojans are easily detectable because of replay attacks and rootkits are not.
C. Rootkits are susceptible to backdoors while trojans are usually part of adware.
D. Rootkits are easily detectable with modern day antivirus and anti-malware software.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 437
Which of the following technologies requires a special SLA to ensure that company data ownership is retained by the company?

A. Key escrow
B. Hard drive encryption
C. Cloud computing
D. Encrypting file system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 438
Which of the following BEST explains the use of encryption on PEDs?

A. Disk encryption helps prevent direct access to files.
B. Mobile phones have FDE built into the Operating System.
C. Mobile phones need device encryption to prevent theft.
D. Laptops can be GEO located via the encryption software.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 439
Which of the following offers the LEAST amount of protection against data theft by USB drives?

A. DLP
B. Database encryption
C. TPM
D. Cloud computing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 440
A security analyst implemented group-based privileges within the company active directory. Which of the following account management techniques should be undertaken regularly to ensure least privilege principles?

A. Leverage role-based access controls.
B. Perform user group clean-up.
C. Verify smart card access controls.
D. Verify SHA-256 for password hashes.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 441
A security analyst needs to implement fraud detection techniques within the company. Which of the following will allow them to accomplish this task? (Select THREE).

A. Job rotation
B. Mandatory vacations
C. RADIUS
D. Smart cards
E. Implicit deny
F. Trusted platform modules

G. Time of day restrictions

Correct Answer: ABG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 442
Which of the following can be applied to the company firewall to force the allowance of HTTP, SMTP, and DNS services?

A. Separation of duties
B. Access control list
C. Mandatory access control
D. Single sign-on

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 443

Which of the following techniques will allow an attacker to identify unknown vulnerabilities within an application?

A. Fuzzing
B. Cross-site scripting
C. Input validation
D. Error handling

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 444
Which of the following risk mitigation strategies will allow a company to cope with advanced persistent threats?

A. Incident management
B. Technical controls
C. Routine audits
D. User permissions reviews

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 445
Which of the following activities should be performed as part of the incident response imaging process?

A. Take system hashes
B. Decrypt USB drive
C. Determine ALE
D. Implement MAC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 446
"Pass Any Exam. Any Time." - www.actualtests.com 155 CompTIA SY0-301 Exam
A security analyst is reviewing a new software product that was created in house. They receive the design and specifications of the application in advance. The analyst is asked to conduct a thorough review using the information they have received. Which of the following types of reviews are they performing?

A. Grey Box Testing
B. Code review
C. White Box Testing
D. Black Box Testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 447
A systems administrator recently installed a NIDS. After 2 weeks of base lining the application, they set the NIDS for certain traffic pattern alerts. Two days later, the administrator must push software updates to the entire company. The NIDS signals alerts to the administrator. This is an example of which of the following?

A. False Negative
B. Network Firewall
C. False Positive
D. URL Filtering

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 448
A security administrator develops a web page and limits input into their fields on the web page as well as filters special characters in output. The administrator is trying to prevent which of the following attacks?

A. Spoofing
B. XSS

C. Fuzzing

D. Pharming

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 449
A penetration tester has begun flooding a switch to replace entries in the MAC address tables with an unsolicited entry. They hope to capture packets and modify packets destined for the victim machine. Which of the following are they planning to use? (Select TWO).

A. DDoS

B. Cross-site scripting

C. ARP poisoning

D. Smurf attack

E. DNS poisoning

F. Man-in-the-middle

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 450
The company CEO has received unsolicited emails all week warning of a major virus outbreak for anyone who uses social media. When the CEO notifies the help desk, they inform the CEO that the emails can be deleted and ignored. Which of the following BEST describes the content of the email?

A. Pharming

B. Whaling

C. SPAM

D. Hoax

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 451
A user often uses the open wireless network at their favorite coffee shop. A hacker knows that the user frequents the shop and was able to acquire several of their secure website passwords. Which of the following methods did the hacker use to acquire the passwords?

A. Man-in-the-middle

B. Impersonation
C. Session hijacking
D. Packet sniffing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 452
The software architect has developed a stand-alone application that runs off of a USB key. They are testing for vulnerabilities using a fuzzer. Which of the following vulnerabilities is MOST likely to be uncovered?

A. Header manipulation
B. SQL injections
C. XML injections
D. Buffer overflows

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 453
The penetration tester is providing recommendations after testing a company's public facing web application. Which of the following configuration recommendations should be suggested?

A. Disable the default web site and port
B. Enable full client side error reporting
C. Disable the sample web application
D. Disable client side scripting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 454
Which of this following is characterized by encrypting data one byte at a time?

A. Elliptical Curve
B. Block Cipher
C. Stream Cipher
D. Steganography

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 455
Which of the following functions performs with the speed of MD4 but without the inherent flaws?

A. RIPEMD
B. RC4
C. SHA
D. 3DES

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 456
Which of the following performs multiple encryption process operations to attain the ciphertext?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 457
The administrator purchases an SSL certificate from a well-known certificate authority to use on their website. They discover that the site works without warning in all browsers except one that was tested. Which of the following is MOST likely the reason the one browser issues a warning?

A. The intermediate CA issued the CSR
B. The certificate has been revoked
C. The certificate authority is not trusted
D. The OCSP has an entry for this certificate

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 458
A security engineer needs to provide SSL access to their website. The SSL certificate provider asks the

engineer to provide them with a file generated by their web server containing their organization name, location, and contact information. Which of the following was the engineer asked to provide?

A. OCSP
B. CSR
C. CA
D. CRL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 459
Which of the following should be done to harden the application server?

A. Close outgoing IP ports
B. Remove administrative accounts
C. Run a port scanner on the application
D. Enforce password complexity

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 460
The security engineer has implemented input validation and secure memory management in their application. Which of the following are they trying to protect against? (Select TWO).

A. Buffer overflow
B. Single sign-on
C. Session hijacking
D. Cross-site scripting
E. Fuzzing

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 461
Several users report to the administrator that they are having issues downloading files from the file server. Which of the following assessment tools can be used to determine if there is an issue with the file server?

A. MAC filter list
B. Recovery agent

C. Baselines

D. Access list

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 462
Which of the following will help reduce the insider threat that is caused by an employee performing the same task for several years?

A. Continuity planning

B. Acceptable use policy

C. Job rotation

D. Change management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 463
A technician has just installed a new firewall onto the network. Users are reporting that they cannot reach any website. Upon further investigation, the technician determines that websites can be reached by entering their IP addresses. Which of the following ports may have been closed to cause this issue?

A. HTTP

B. DHCP

C. DNS

D. NetBIOS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 464
The IT administrator needs to eliminate users from interactively logging on to their desktop computers while offsite. Which of the following ports should be closed?

A. 21

B. 143

C. 3389

D. 8080

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 465
The security administrator has determined that employees are bringing in their personal devices and using them to surf the Internet. Which of the following can be performed to prevent the personal devices from connecting to the network?

A. Disable unused ports on the switch
B. Disable unnecessary accounts
C. Implement stronger passwords
D. Install a NIDS onto the network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 466
A security administrator is installing new WAPs in the office. The building has several other businesses that have their own WAPs. Which of the following should be taken into consideration when trying to prevent causing interference to the other businesses?

A. SSID broadcasting
B. Antenna placements
C. Encryption methods
D. SSID naming rights

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 467
A user does several different jobs for the company and has several different usernames and passwords for the various systems they use. On occasion the user forgets which username goes with which password and which systems they belong to. Which of the following could the IT staff implement to help with this issue?

A. Smart card
B. Administrative rights
C. Biometrics
D. Single sign-on

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 468
The system administrator has been notified that many users are having difficulty connecting to the company's wireless network. They take a new laptop and physically go to the access point and connect with no problems. Which of the following would be the MOST likely cause?

A. The certificate used to authenticate users has been compromised and revoked.
B. Multiple war drivers in the parking lot have exhausted all available IPs from the pool to deny access.
C. An attacker has gained access to the access point and has changed the encryption keys.
D. An unauthorized access point has been configured to operate on the same channel.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 469
A system administrator needs to ensure proper patch installation for their users' applications. They are concerned because they are critical patches for applications used in a heavily hardened environment. Which of the following should be performed?

A. Configure the applications to update immediately and directly from the vendor.
B. Task the users to patch applications as they are used to avoid network congestion.
C. Push the patches overnight and monitor performance the following day.
D. Deploy the patches in a test environment to ensure no issues are created.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 470
The systems administrator is concerned about users accessing unattended computers in other departments. Which of the following should be done?

A. Modify all user accounts so that they only have read-only privileges.
B. Employ short inactivity periods before protected screensavers engage.
C. Create a policy that blocks users from logging onto multiple systems.
D. Distribute security screens for every monitor to prevent shoulder surfing.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 471
The systems administrator wishes to implement a hardware-based encryption method that could also be used

to sign code. They can achieve this by:

A. utilizing the already present TPM.
B. configuring secure application sandboxes.
C. enforcing whole disk encryption.
"Pass Any Exam. Any Time." - www.actualtests.com 164 CompTIA SY0-301 Exam
D. moving data and applications into the cloud.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 472
The project manager has a small team that uses a dedicated wireless network to protect sensitive client data that is not on the company network. Which of the following BEST prevents other employees from accessing this network?

A. Set up a secondary access point with the same SSID to act as a honeypot to other employees.
B. Configure the access point so that only laptops with approved MAC addresses can connect.
C. Lower the access point's power levels so that the signal does not extend outside of the building.
D. Authenticate connection access based upon user domain account validation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 473
A company has outsourced email to a third party. Of which of the following is this an example?

A. SaaS
B. PaaS
C. IMAP
D. SMTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 474
A network administrator is using simu-lation software on their desktop to design the company DMZ. The software allows them to place network devices in a map and perform real case testing of network traffic. Which of the following technologies is the administrator using?

"Pass Any Exam. Any Time." - www.actualtests.com 165 CompTIA SY0-301 Exam

A. Virtualization
B. Multitasking

C. Software as a service

D. Hyperthreading

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 475
A firewall administrator has noticed that the company's gateway firewall is starting to run with degraded performance due to the number of ACLs it is processing. Which of the following should be considered to improve firewall performance?

A. Place the ACL with the most hit at the bottom while considering ACL dependencies.

B. Place the ACL with the most hit at the top while considering ACL dependencies.

C. Place the ACL with the most hit at the top and enable logging on that ACL.

D. Place the ACL with the most hit at the bottom and enable logging on that ACL.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 476
A network administrator wants to implement a system that allows them to dynamically place company wired laptops and desktops on different VLANs based on the group of the user who authenticates to the network. Which of the following should the administrator implement on the switches?

A. VLAN management

B. Port security

C. DHCP

D. 802.1X

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 477
"Pass Any Exam. Any Time." - www.actualtests.com 166 CompTIA SY0-301 Exam
A security administrator is tasked with implementing a wireless system which will allow for both guest access as well as access into the corporate network through a single SSID. Which of the following solutions should be implemented to provide the GREATEST security for the corporate network?

A. A WPA2 enterprise wireless inside the corporate network firewall and allow employees to sponsor guests accounts.

B. A WPA2 protected wireless inside the corporate network firewall and provide a different shared key for guests and employees.

C. An open wireless with no encryption outside of the corporate network firewall and deploy a VPN client to the company laptops.

D. A WPA protected wireless in the DMZ and provide one encryption key to both employees and guests.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 478
Which of the following is used between an SSH client and an SSH server to negotiate the transport encryption key?

A. Keyed hash
B. Symmetric encryption
C. Asymmetric encryption
D. Stream cipher

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 479
A security administrator needs to send a highly classified document in an encrypted fashion. Which of the following is the MOST secure method to encrypt the document?

A. PKI
B. Steganography
C. One-time-pads
D. SHA256
"Pass Any Exam. Any Time." - www.actualtests.com 167 CompTIA SY0-301 Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 480
On Monday, a security administrator installed a new CA and issued two-year certificates which have been installed on the company web servers. On Tuesday, they notice that the CA's time is set one year forward. Which of the following is true?

A. An error will be displayed on the browser about the encryption cipher being invalid.
B. No error will be displayed on the browser because the certificate has not expired.
C. The browser of users going to the company's websites will display a certificate error.
D. As long as the web servers' time is also set one year forward no error will occur.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 481
A security administrator wants to implement an internal CRL. Which of the following should be placed in the CRL?

A. Public keys
B. Private keys
C. Escrow keys
D. Recovery keys

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 482
Which of the following can occur when the security awareness training lacks information on the importance of credential sharing?

A. Non-repudiation is affected
B. Employee productivity decreases
C. Users of open kiosks cannot be tracked

D. Accountability can be established

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 483
A security consultant has been hired to perform black box testing on the company's internally developed software application. Which of the following is MOST likely performed to test the security of the application?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 484
Which of the following can a security administrator use to store information about company employees which may be accessed by unauthenticated users?

A. ACL
B. LDAP
C. NTLM
D. HSM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 485
Which of the following is MOST often used to provide access attributes to authenticated users?

A. ACLs
B. Biometric reader

C. RADIUS
D. Kerberos

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 486
Which of the following is a commonly known security issue with users implementing password protection on their own computer systems?

A. Users do not share their passwords
B. Users tend to implement password complexity
C. Users change their password frequently
D. Users write down their passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 487
A user in the network reports a virus warning that keeps popping up on their PC. A scan is completed on the PC and determines the user does not have a virus. Which of the following is the BEST explanation for this occurrence?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 488
Digital signatures are used for ensuring which of the following items? (Select TWO).

A. Confidentiality

B. Integrity
C. Non-Repudiation
D. Availability
E. Algorithm strength

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 489
One of the servers on the network stops responding due to lack of available memory. Server administrators did not have a clear definition of what action should have taken place based on the available memory. Which of the following would have BEST kept this incident from occurring?

A. Set up a protocol analyzer
B. Set up a performance baseline
C. Review the systems monitor on a monthly basis
D. Review the performance monitor on a monthly basis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 490
When reviewing firewall logs, an administrator notices a number of connections coming from an IP address in a country where the company does not conduct business. These connections are taking place at the rate of several per minute and are affecting a number of different services.
Which of the following is MOST likely taking place?

A. Data mining
B. Blue jacking
C. Dictionary attack
D. Port scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 491

When conducting a penetration test, an administrator would perform a port scan to search for:

A. TCP and UDP responses.
B. inactive network resources.
C. SSL implementation.
D. in-depth network footprinting.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 492
Which of the following would be done during a penetration test but not a vulnerability scan?

A. Attempting to access user accounts by brute force
B. Footprinting and identifying various network segments
C. Scanning for open Wi-Fi access points
D. Performing a port sweep across the network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 493
Which of the following would BEST reveal if a server has been compromised by a rootkit?

A. Take an MD5 hash of the live system and compare it to the previous MD5 hash.
B. Examine the network monitor and see if there is any abnormal activity.
C. Update the antivirus definition files and then run a scan.
D. Compare the current system's performance to the performance baseline.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 494
The administrator spots a sustained spike in disk activity and CPU utilization; network activity looks normal. Which of the following might this indicate?

A. This server is now a member of a botnet.
B. There is a virus infecting the server.

C. There is a smurf attack occurring on the server.

D. Users are copying more files from the server than normal.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 495
Users have reported that when they go to the company website they are sent to a competitor's site instead. Which of the following is the MOST likely explanation?

A. Someone has employed ARP poisoning against the company.

B. Someone has employed DNS poisoning against the company.

C. Someone has accidentally unplugged the company's web server.

D. The competitor has a more powerful web server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 496
Workstations have been deployed to users without antivirus software installed on them. Which of the following security postures should be used to prevent this from happening in the future?

A. Use of configuration baselines

B. Acceptable Use Policy

C. Patch management control

D. Use of security templates

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 497
Which of the following is the MOST secure solution for connecting remote sites to the corporate headquarters?

A. PPTP

B. L2TP

C. HTTP

D. IPSec

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 498
A security administrator suspects that an employee has attached unauthorized in a wireless access point to the network. Which of the following would MOST likely assist the administrator in locating the rogue access point?

A. Site survey
B. Vulnerability scanner
C. Protocol analyzer
D. Port scanner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 499
As part of the company's compliance to regulations the security administrator needs to determine how difficult it would be for an outside entity to gain access to the company's e-commerce solution. Which of the following would be the BEST assessment for the security administrator to perform?

A. Vulnerability scan
B. White box testing
C. Penetration test
D. Code review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 500
"Pass Any Exam. Any Time." - www.actualtests.com 174 CompTIA SY0-301 Exam
The baseline for a company's server shows that the server can handle 1,000 users before reaching 100% memory utilization. The server is at 100% memory utilization with only 500 users connected. Which of the following tools will MOST likely notify the administrator of the problem?

A. Performance monitoring
B. System monitoring
C. Protocol analysis
D. Performance baseline

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 501

An employee received an email from a friend that contained the latest version of a popular game. The employee has noticed that since opening the file the hard disk lights on the workstation have been in constant use. Which of the following is the MOST likely cause?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 502
A hosting company protects a client's virtual machines by limiting server connectivity on the host server in which of the following ways? (Select TWO).

A. Restrict direct access between client VLANs except open public ports.
B. Deny direct file access between guest and host.
C. Configure another guest to be a gateway between client VLANs.
D. Configure default/allow between client VLANs.
E. Remove default deny settings between client VLANs.
F. Rate limit connectivity between client VLANs.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation: