Comptia Certkiller SY0-301 Exam Bundle

Number: SY0-301
Passing Score: 800
Time Limit: 120 min
File Version: 25.5

http://www.gratisexam.com/

Comptia SY0-301 Exam Bundle

Exam Name: Comptia CompTIA Security+ Certification Exam 2011 version

For Full Set of Questions please visit: http://www.certkiller.com/exam-SY0-301.htm

Exam A

QUESTION 1
A password history value of three means which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
In order to provide flexible working conditions, a company has decided to allow some employees remote access into corporate headquarters. Which of the following security technologies could be used to provide remote access? (Select TWO).

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following devices is BEST suited for servers that need to store private keys?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
All of the following are valid cryptographic hash functions EXCEPT:

A. RIPEMD.
B. RC4.

C. SHA-512.
D. MD4.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following can prevent an unauthorized person from accessing the network by plugging into an open network jack?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
After verifying that the server and database are running, Jane, the administrator, is still unable to make a TCP connection to the database. Which of the following is the MOST likely cause for this?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following steps should follow the deployment of a patch?

A. Antivirus and anti-malware deployment
B. Audit and verification

C. Fuzzing and exploitation
D. Error and exception handling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following would be used when a higher level of security is desired for encryption key storage?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
If Pete, a security administrator, wants to ensure that certain users can only gain access to the system during their respective shifts, which of the following best practices would he implement?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
A small business owner has asked the security consultant to suggest an inexpensive means to deter physical intrusions at their place of business. Which of the following would BEST meet their request?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A security administrator is observing congestion on the firewall interfaces and a high number of half open incoming connections from different external IP addresses. Which of the following attack types is underway?

A. Cross-site scripting
B. SPIM
C. Client-side
D. DDoS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following application security testing techniques is implemented when an automated system generates random input data?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following BEST describes a protective countermeasure for SQL injection?

A. Eliminating cross-site scripting vulnerabilities
B. Installing an IDS to monitor network traffic

C. Validating user input in web applications
D. Placing a firewall between the Internet and database servers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following BEST describes a common security concern for cloud computing?

A. Data may be accessed by third parties who have compromised the cloud platform
B. Antivirus signatures are not compatible with virtualized environments
C. Network connections are too slow
D. CPU and memory resources may be consumed by other servers in the same cloud

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A certificate authority takes which of the following actions in PKI?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Separation of duties is often implemented between developers and administrators in order to separate which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Jane, an individual, has recently been calling various financial offices pretending to be another person to gain financial information. Which of the following attacks is being described?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
The security administrator wants each user to individually decrypt a message but allow anybody to encrypt it. Which of the following MUST be implemented to allow this type of authorization?

A. Use of CA certificate
B. Use of public keys only
C. Use of private keys only
D. Use of public and private keys

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
An employee is granted access to only areas of a network folder needed to perform their job. Which of the following describes this form of access control?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?

A. Logic bomb
B. Worm

C. Trojan
D. Adware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Pete, a network administrator, is capturing packets on the network and notices that a large amount of the traffic on the LAN is SIP and RTP protocols. Which of the following should he do to segment that traffic from the other traffic?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Jane, the security administrator, needs to be able to test malicious code in an environment where it will not harm the rest of the network. Which of the following would allow Jane to perform this kind of testing?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Developers currently have access to update production servers without going through an approval process. Which of the following strategies would BEST mitigate this risk?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
A system administrator decides to use SNMPv3 on the network router in AuthPriv mode. Which of the following algorithm combinations would be valid?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following are encryption algorithms that can use a 128-bit key size? (Select TWO).

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following specifications would Sara, an administrator, implement as a network access control?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following is characterized by an attacker attempting to map out an organization's staff hierarchy in order to send targeted emails?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following provides the MOST protection against zero day attacks via email attachments?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A username provides which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Use of group accounts should be minimized to ensure which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
In which of the following scenarios is PKI LEAST hardened?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following is used to certify intermediate authorities in a large PKI deployment?

A. Root CA
B. Recovery agent
C. Root user

D. Key escrow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Elliptic curve cryptography: (Select TWO)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following would an antivirus company use to efficiently capture and analyze new and unknown malicious attacks?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A system administrator is using a packet sniffer to troubleshoot remote authentication. The administrator detects a device trying to communicate to TCP port 49. Which of the following authentication methods is MOST likely being attempted?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following can use RC4 for encryption? (Select TWO).

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

A. CCTV system access
B. Dial-up access
C. Changing environmental controls
D. Ping of death

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following provides the HIGHEST level of confidentiality on a wireless network?

A. Disabling SSID broadcast

B. MAC filtering
C. WPA2
D. Packet switching

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Matt, an IT administrator, wants to protect a newly built server from zero day attacks. Which of the following would provide the BEST level of protection?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following can be used to mitigate risk if a mobile device is lost?

A. Cable lock
B. Transport encryption
C. Voice encryption
D. Strong passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following is an example of multifactor authentication?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
After Matt, a user enters his username and password at the login screen of a web enabled portal, the following appears on his screen:

`Please only use letters and numbers on these fields'

Which of the following is this an example of?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Exam B

QUESTION 1
A marketing employee requests read and write permissions to the finance department's folders. The security administrator partially denies this request and only gives the marketing employee read-only permissions. This is an example of which of the following?

A. Job rotation
B. Separation of duties
C. Least privilege
D. Change management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
An administrator notices an unusual spike in network traffic from many sources. The administrator suspects that:

A. it is being caused by the presence of a rogue access point.
B. it is the beginning of a DDoS attack.
C. the IDS has been compromised.
D. the internal DNS tables have been poisoned.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Users at a company report that a popular news website keeps taking them to a web page with derogatory content. This is an example of which of the following?

A. Evil twin

B. DNS poisoning
C. Vishing
D. Session hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following protocols would be used to verify connectivity between two remote devices at the LOWEST level of the OSI model?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Matt, the security administrator, notices a large number of alerts on the NIDS. Upon further inspection, it is determined that no attack has really taken place. This is an example of a:

A. false negative.
B. true negative.
C. false positive.
D. true positive.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following would Pete, a security administrator, MOST likely implement in order to allow employees to have secure remote access to certain internal network services such as file servers?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following could cause a browser to display the message below? "The security certificate presented by this website was issued for a different website's address."

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following protocols would be implemented to secure file transfers using SSL?

A. TFTP

B. SCP
C. SFTP
D. FTPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Jane, an administrator, hears reports of circles being drawn in the parking lot. Because the symbols fall within range of the company's wireless AP, the MOST likely concern is:

A. that someone has used war chalking to help others access the company's network.
B. that the symbols indicate the presence of an evil twin of a legitimate AP.
C. that someone is planning to install an AP where the symbols are, to cause interference.
D. that a rogue access point has been installed within range of the symbols.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of the following are used to implement VPNs? (Select TWO).

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Matt, a security administrator, is receiving reports about several SQL injections and buffer overflows through his company's website. Which of the following would reduce the amount of these attack types?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Enforcing data encryption of removable media ensures that the:

A. lost media cannot easily be compromised.
B. media can be identified.
C. location of the media is known at all times.
D. identification of the user is non-repudiated.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A company had decided to assign employees laptops instead of desktops to mitigate the risk of company closures due to disasters. Which of the following is the company trying to ensure?

A. Succession planning
B. Fault tolerance
C. Continuity of operations
D. Removing single points of failure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems?

A. Incident management
B. Server clustering
C. Change management
D. Forensic analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Pete, the security administrator, wants to ensure that traffic to the corporate intranet is secure using HTTPS. He configures the firewall to deny traffic to port 80. Now users cannot connect to the intranet even through HTTPS. Which of the following is MOST likely causing the issue?

A. The web server is configured on the firewall's DMZ interface.
B. The VLAN is improperly configured.
C. The firewall's MAC address has not been entered into the filtering list.
D. The firewall executes an implicit deny.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following is a management control?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following incident response procedures BEST allows Sara, the security technician, to identify who had possession of a hard drive prior to forensics analysis?

A. Chain of custody
B. Tracking man hours
C. Witnesses
D. Capturing system images

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following security strategies allows a company to limit damage to internal systems and provides loss control?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following must Jane, a security administrator, implement to ensure all wired ports are authenticated before a user is allowed onto the network?

A. Intrusion prevention system
B. Web security gateway
C. Network access control
D. IP access control lists

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A security administrator needs to open ports on the firewall to allow for secure data transfer. Which of the following TCP ports would allow for secure transfer of files by default?

A. 21
B. 22
C. 23
D. 25

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following technologies would allow for a secure tunneled connection from one site to another? (Select TWO).

A. SFTP

B. IPSec
C. SSH
D. HTTPS
E. ICMP

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Using proximity card readers instead of the traditional key punch doors would help to mitigate:

A. impersonation.
B. tailgating.
C. dumpster diving.
D. shoulder surfing.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
In planning for a firewall implementation, Pete, a security administrator, needs a tool to help him understand what traffic patterns are normal on his network. Which of the following tools would help Pete determine traffic patterns?

A. Syslog
B. Protocol analyzer
C. Proxy server
D. Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
TKIP uses which of the following encryption ciphers?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Common access cards use which of the following authentication models?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following application attacks is used to gain access to SEH?

A. Cookie stealing
B. Buffer overflow
C. Directory traversal
D. XML injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following does a second authentication requirement mitigate when accessing privileged areas of a website, such as password changes or user profile changes?

A. Cross-site scripting
B. Cookie stealing
C. Packet sniffing
D. Transitive access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following ports does DNS operate on, by default?

A. 23
B. 53

C. 137
D. 443

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Sara from IT Governance wants to provide a mathematical probability of an earthquake using facts and figures. Which of the following concepts would achieve this?

A. Qualitative Analysis
B. Impact Analysis
C. Quantitative Analysis
D. SLE divided by the ARO

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A buffer overflow can result in which of the following attack types?

A. DNS poisoning
B. Zero-day
C. Privilege escalation
D. ARP poisoning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following is true concerning WEP security?

A. WEP keys are transmitted in plain text.
B. The WEP key initialization process is flawed.
C. The pre-shared WEP keys can be cracked with rainbow tables.
D. WEP uses the weak RC4 cipher.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following can be used on a smartphone to BEST protect against sensitive data loss if the device is stolen? (Select TWO).

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

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following can be implemented on a lost mobile device to help recover it?

A. Remote sanitization
B. GPS tracking
C. Voice encryption
D. Patch management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Jane, a security analyst, is reviewing logs from hosts across the Internet which her company uses to gather data on new malware. Which of the following is being implemented by Jane's company?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Sara, a senior programmer for an application at a software development company, has also assumed an auditing role within the same company. She will be assessing the security of the application. Which of the following will she be performing?

A. Blue box testing
B. Gray box testing
C. Black box testing
D. White box testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following BEST describes a directory traversal attack?

A. A malicious user can insert a known pattern of symbols in a URL to access a file in another section of the directory.
B. A malicious user can change permissions or lock out user access from a webroot directory or subdirectories.
C. A malicious user can delete a file or directory in the webroot directory or subdirectories.
D. A malicious user can redirect a user to another website across the Internet.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Sara, the Chief Executive Officer (CEO) of a corporation, wishes to receive her corporate email and file attachments on her corporate mobile computing device. If the device is lost or stolen, the BEST security measure to ensure that sensitive information is not comprised would be:

A. to immediately file a police report and insurance report.
B. the ability to remotely wipe the device to remove the data.
C. to immediately issue a replacement device and restore data from the last backup.
D. to turn on remote GPS tracking to find the device and track its movements.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
In her morning review of new vendor patches, a security administrator has identified an exploit that is marked as critical. Which of the following is the BEST course of action?

A. The security administrator should wait seven days before testing the patch to ensure that the vendor does not issue an updated version, which would require reapplying the patch.
B. The security administrator should download the patch and install it to her workstation to test whether it will be able to be applied to all workstations in the environment.
C. The security administrator should alert the risk management department to document the patch and add it

to the next monthly patch deployment cycle.

D. The security administrator should download the patch to the test network, apply it to affected systems, and evaluate the results on the test systems.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following protocols allows for secure transfer of files? (Select TWO).

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Jane, a security administrator, notices that a program has crashed. Which of the following logs should Jane check?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Users at a corporation are unable to login using the directory access server at certain times of the day. Which of the following concepts BEST describes this lack of access?

A. Mandatory access control
B. Least privilege
C. Time of day restrictions
D. Discretionary access control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following passwords is the LEAST complex?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
During an anonymous penetration test, Jane, a system administrator, was able to identify a shared print spool directory, and was able to download a document from the spool. Which statement BEST describes her privileges?

A. All users have write access to the directory.
B. Jane has read access to the file.
C. All users have read access to the file.
D. Jane has read access to the directory.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Sara, an IT security technician, has identified security weaknesses within her company's code. Which of the following is a common security coding issue?

A. Input validation
B. Application fuzzing
C. Black box testing
D. Vulnerability scanning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Matt, an IT security technician, needs to create a way to recover lost or stolen company devices. Which of the following BEST meets this need?

A. Locking cabinets
B. GPS tracking
C. Safe
D. Firewalls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
An IT security technician needs to establish host based security for company workstations. Which of the following will BEST meet this requirement?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Jane, an IT security technician, receives a call from the vulnerability assessment team informing her that port 1337 is open on a user's workstation. Which of the following BEST describes this type of malware?

A. Logic bomb
B. Spyware
C. Backdoor
D. Adware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?

A. Certification authority
B. Key escrow
C. Certificate revocation list
D. Registration authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following BEST describes the weakness in WEP encryption?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years. Which of the following should Sara do to address the risk?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Matt, a security consultant, has been tasked with increasing server fault tolerance and has been given no budget to accomplish his task. Which of the following can Matt implement to ensure servers will withstand hardware failure?

A. Hardware load balancing
B. RAID

C. A cold site
D. A host standby

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Pete has obtained a highly sensitive document and has placed it on a network drive which has been formatted with NTFS and is shared via CIFS. Which of the following access controls apply to the sensitive file on the server?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A security administrator has installed a new KDC for the corporate environment. Which of the following authentication protocols is the security administrator planning to implement across the organization?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following uses only a private key?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Jane has recently implemented a new network design at her organization and wishes to passively identify security issues with the new network. Which of the following should Jane perform?

A. Vulnerability assessment
B. Black box testing
C. White box testing
D. Penetration testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
A database server containing personal information and a file server containing non-critical information must be secured. Which of the following would be a BEST practice to secure the servers? (Select TWO).

A. Place the file server behind a door requiring biometric authorization.
B. Place both servers under the system administrator's desk.
C. Place the database server behind a door with a cipher lock.
D. Place the file server in an unlocked rack cabinet.
E. Place the database server behind a door requiring biometric authorization.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

Exam C

QUESTION 1
A company is experiencing an extraordinary amount of web traffic that is crippling the server. The web traffic suddenly stops. The mail server experiences the same amount of traffic as before then crashes. Which of the following attacks would this BEST describe?

A. DoS
B. Spam
C. Man-in-the-middle
D. Replay

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following would ensure confidentiality and authorization to the management interface of a router?

A. Enable an access list and RADIUS
B. Enable SSH and TACACS
C. Enable an access list and PKI
D. Enable LDAP and strong passwords

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A security technician is attempting to explain why some of the company policies should be changed for high risk IT positions. Which of the following concepts BEST explains the support for fraud detection?

A. Time of day restrictions is more likely to discover fraud than the other fraud detection methods.
B. Least privilege principles allow internal audit teams to discover fraud while a staff member is out of the office.
C. Separation of duties is a better fraud detection method than mandatory vacations; therefore, it should be used.
D. Mandatory vacations support the company discovering fraud while staff members are out of the office.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A security technician is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks the security technician to explain the access control type found in a firewall. With which of the following should

the security technician respond?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Jane, a security administrator, has been tasked with explaining authentication services to the company's management team. The company runs an active directory infrastructure. Which of the following solutions BEST relates to the host authentication protocol within the company's environment?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
The information security department regularly walks the campus and around the buildings looking for unauthorized open wireless networks. This is an example of which of the following?

A. A site survey
B. Antenna placement
C. War dialing
D. War driving

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Jane, the CEO, receives an email wanting her to clink on a link to change her username and password. Which of the following attacks has she just received?

A. Hoaxes
B. Whaling
C. Bluejacking
D. Vishing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Sara, the security administrator, must configure the corporate firewall to allow all public IP addresses on the internal interface of the firewall to be translated to one public IP address on the external interface of the same firewall. Which of the following should Sara configure?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service?

A. Succession planning
B. Disaster recovery plan
C. Information security plan
D. Business impact analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability?

A. Twofish
B. Diffie-Hellman
C. ECC

D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Matt must come up with a design solution which will enable remote users to securely access network resources. Which of the following design elements will enable Matt to meet this objective?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Matt works for an organization that requires data to be recovered in the shortest amount of time possible. Which of the following backup types would BEST meet the organization's needs?

A. Full backups daily
B. Differential backups monthly
C. Full backups weekly
D. Incremental backups monthly

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following services should be disabled to stop attackers from using a web server as a mail relay?

A. IMAP
B. SMTP
C. SNMP
D. POP3

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are backdoors and logic bombs. Which of the following differentiates these two types of malware?

A. A backdoor is a coding issue that can be discovered by proper configuration management processes.
B. A logic bomb is typically hidden within the boot sector of the hard drive and is used to cause DDoS.
C. A backdoor is a third generation attack which is typically low risk because only highly trained staff can achieve it.
D. A logic bomb is undetectable by current antivirus signatures because a patch has not been issued.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following BEST explains the use of an HSM within the company servers?

A. Thumb drives present a significant threat which is mitigated by HSM.
B. Software encryption can perform multiple functions required by HSM.

C. Data loss by removable media can be prevented with DLP.
D. Hardware encryption is faster than software encryption.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which of the following technologies can store multi-tenant data with different security requirements?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following is MOST closely associated with BitLocker?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT?

A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.
B. Tell the application development manager to code the application to adhere to the company's password policy.
C. Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.
D. Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 21
Which of the following presents the STRONGEST access control?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following is the LEAST volatile when performing incident response procedures?

A. Registers
B. RAID cache
C. RAM
D. Hard drive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following can allow Sara, a security analyst, to encrypt individual files on a system?

A. EFS
B. Single sign-on
C. TLS
D. Journaled file system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
An encryption method where the plain text and cipher text are always the same size is an example of which of the following types of encryption?

A. RC4

B. MD5
C. Steam Cipher
D. Block Cipher

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
The compliance team comes out with a new policy that all data stored on tapes over 3 years must be degaussed. This BEST describes which of the following types of policies?

A. Data handling
B. Data classification
C. Data labeling
D. Data disposal

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Pete's corporation has outsourced help desk services to a large provider. Management has published a procedure that requires all users, when receiving support, to call a special number. Users then need to enter the code provided to them by the help desk technician prior to allowing the technician to work on their PC. Which of the following does this procedure prevent?

A. Collusion
B. Impersonation
C. Pharming
D. Transitive Access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Pete, the security engineer, would like to prevent wireless attacks on his network. Pete has implemented a security control to limit the connecting MAC addresses to a single port. Which of the following wireless attacks would this address?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Jane, the security administrator, is having issues with unauthorized users connecting to the wireless network. For administrative reasons, she cannot implement any wireless encryption methods. Which of the following can she implement to prevent unauthorized users from connecting to the network?

A. NIPS
B. Disable unused ports
C. MAC filtering
D. WEP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Sara, the IT administrator, wants to control which devices can connect to the wireless network. Which of the following can she implement to accomplish this task?

A. WPA2 Enterprise with AES encryption
B. Decrease the WAP's power levels
C. Static IP addressing
D. MAC address filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Pete, the system administrator, is concerned about unauthorized access at all entrances into the building. PIN pad readers have been installed, but users have developed the habit of holding the door for others behind them. Which of the following would BEST prevent this?

A. Install mantraps at every unmanned entrance.
B. Replace the PIN pad readers with card readers.
C. Implement video and audio surveillance equipment.
D. Require users to sign conduct policies forbidding these actions.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Jane, a network administrator, has configured a 48-port switch to isolate four different departments. Which of the following has Jane MOST likely configured on the switch?

A. NAC
B. 802.1x
C. VLAN
D. DMZ

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
A security analyst needs to ensure all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended?

A. DMZ
B. Cloud computing
C. VLAN
D. Virtualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Layer 7 devices used to prevent specific types of html tags are called:

A. firewalls.
B. content filters.

C. routers.
D. NIDS.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Digital Signatures provide which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
In an enterprise environment, which of the following would be the BEST way to prevent users from accessing inappropriate websites when AUP requirements are constantly changing?

A. Deploy a network proxy server.
B. Configure Internet content filters on each workstation.
C. Deploy a NIDS.
D. Deploy a HIPS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
An administrator notices that former temporary employees' accounts are still active on a domain. Which of the following can be implemented to increase security and prevent this from happening?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:

A. logic bomb.
B. backdoor.
C. adware application.
D. rootkit.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following protocols uses TCP instead of UDP and is incompatible with all previous versions?

A. TACACS

B. XTACACS
C. RADIUS
D. TACACS+

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following symmetric key algorithms are examples of block ciphers? (Select THREE).

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

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A new wireless network was installed in an office building where there are other wireless networks. Which of the following can the administrator disable to help limit the discovery of the new network?

A. DHCP
B. Default user account
C. MAC filtering
D. SSID broadcast

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
The lead security engineer has been brought in on a new software development project. The software development team will be deploying a base software version and will make multiple software revisions during the project life cycle. The security engineer on the project is concerned with the ability to roll back software changes that cause bugs and/or security concerns. Which of the following should the security engineer suggest to BEST address this issue?

A. Develop a change management policy incorporating network change control.
B. Develop a change management policy incorporating hardware change control.
C. Develop a change management policy incorporating software change control.
D. Develop a change management policy incorporating oversight of the project lifecycle.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
A security administrator wants to scan an infected workstation to understand how the infection occurred. Which of the following should the security administrator do FIRST before scanning the workstation?

A. Make a complete hard drive image
B. Remove the memory
C. Defragment the hard drive
D. Delete all temporary Internet files

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following security methods should be used to ensure mobile devices are not removed by unauthorized users when the owner is away from their desk?

A. Screen lock
B. Biometrics
C. Strong passwords
D. Cable lock

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following techniques describes the use of application isolation during execution to prevent system compromise if the application is compromised?

A. Least privilege
B. Sandboxing
C. Black box
D. Application hardening

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A new AP has been installed and there are problems with packets being dropped. Which of the following BEST explains the packet loss?

A. EMI
B. XML injection
C. DDoS
D. Botnet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following is being used when a message is buried within the pixels of an image?

A. Steganography
B. Block cipher
C. Encryption
D. Hashing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Remote employees login to the network using a device displaying a digital number which changes every five minutes. This is an example of which of the following?

A. Block cipher
B. One-time pad
C. Stream cipher
D. Digital signature

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Sara, a security administrator, has recently implemented a policy to ban certain attachments from being sent through the corporate email server. This is an example of trying to mitigate which of the following?

A. SQL injection
B. LDAP injection
C. Cross-site scripting
D. Malicious add-ons

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Pete, the security administrator, wants to ensure that only secure protocols are being used to transfer and copy files. Which of the following protocols should he implement?

A. SMTP
B. SCP
C. FTP
D. HTTPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
The finance department is growing and needs additional computers to support growth. The department also needs to ensure that their traffic is separated from the rest of the network. Matt, the security administrator, needs to add a new switch to accommodate this growth. Which of the following MUST Matt configure on the switch to ensure proper network separation?

A. Implicit deny
B. VLAN management
C. Access control lists
D. Flood guards

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following would Sara, a security administrator, utilize to actively test security controls within an organization?

A. Penetration test
B. Baselining
C. Code review
D. Vulnerability scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A database server has been compromised via an unpatched vulnerability. An investigation reveals that an application crashed at the time of the compromise. Unauthorized code appeared to be running, although there were no traces of the code found on the file system. Which of the following attack types has MOST likely occurred?

A. Zero day exploit
B. SQL injection
C. LDAP injection
D. Buffer overflow

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which process will determine maximum tolerable downtime?

A. Business Continuity Planning
B. Contingency Planning
C. Business Impact Analysis
D. Disaster Recovery Plan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Who should be contacted FIRST in the event of a security breach?

A. Forensics analysis team
B. Internal auditors
C. Incident response team
D. Software vendors

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: