SY0-401 6-19-2016 530q

Passing Score: 850
Time Limit: 300 min

Sections

Exam A

QUESTION 1
A company is rolling out a new e-commerce website. The security analyst wants to reduce the risk of the new website being comprised by confirming that system patches are up to date, application hot fixes are current, and unneeded ports and services have been disabled. To do this, the security analyst will perform a:

A. Vulnerability assessment
B. White box test
C. Penetration test
D. Peer review

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 2
Joe, a security analyst, is attempting to determine if a new server meets the security requirements of his organization. As a step in this process, he attempts to identify a lack of security controls and to identify common misconfigurations on the server. Which of the following is Joe attempting to complete?

A. Black hat testing
B. Vulnerability scanning
C. Black box testing
D. Penetration testing

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 3
A classroom utilizes workstations running virtualization software for a maximum of one virtual machine per working station. The network settings on the virtual machines are set to bridged. Which of the following describes how the switch in the classroom should be configured to allow for the virtual machines and host workstation to connect to network resources?

A. The maximum-mac settings of the ports should be set to zero
B. The maximum-mac settings of the ports should be set to one
C. The maximum-mac settings of the ports should be set to two
D. The maximum mac settings of the ports should be set to three

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 4
Which of the following attacks initiates a connection by sending specially crafted packets in which multiple TCP flags are set to 1?

A. Replay
B. Smurf
C. Xmas
D. Fraggle

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 5
A Company transfers millions of files a day between their servers. A programmer for the company has created a program that indexes and verifies the integrity of each file as it is replicated between servers. The programmer would like to use the fastest algorithm to ensure integrity. Which of the following should the programmer use?

A. SHA1
B. RIPEMD
C. DSA
D. MD5

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 6
A system administrator is conducting baseline audit and determines that a web server is missing several critical updates. Which of the following actions should the administrator perform first to correct the issue?

A. Open a service ticket according to the patch management plan
B. Disconnect the network interface and use the administrative management console to perform the updates
C. Perform a backup of the server and install the require patches
D. Disable the services for the web server but leave the server alone pending patch updates

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 7
The IT department has been tasked with reducing the risk of sensitive information being shared with unauthorized entities from computers it is saved on, without impeding the ability of the employees to access the internet. Implementing which of the following would be the best way to accomplish this objective?

A. Host-based firewalls
B. DLP
C. URL filtering
D. Pop-up blockers

Correct Answer: B

Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 8
A server crashes at 6 pm. Senior management has determined that data must be restored within two hours of a server crash. Additionally, a loss of more than one hour worth of data is detrimental to the company's financial well-being. Which of the following is the RTO?

A. 7pm
B. 8pm
C. 9pm
D. 10pm

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 9
To mitigate the risk of intrusion, an IT Manager is concerned with using secure versions of protocols and services whenever possible. In addition, the security technician is required to monitor the types of traffic being generated. Which of the following tools is the technician MOST likely to use?

A. Port scanner

B. Network analyzer
C. IPS
D. Audit Logs

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 10
An administrator is implementing a new management system for the machinery on the company's production line. One requirement is that the system only be accessible while within the production facility. Which of the following will be the MOST effective solution in limiting access based on this requirement?

A. Access control list
B. Firewall policy
C. Air Gap
D. MAC filter

Correct Answer: C
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 11
A risk assessment team is concerned about hosting data with a cloud service provider (CSP) which of the following findings would justify this concern?

A. The CPS utilizes encryption for data at rest and in motion
B. The CSP takes into account multinational privacy concerns
C. The financial review indicates the company is a startup
D. SLA state service tickets will be resolved in less than 15 minutes

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 12

A company wishes to prevent unauthorized employee access to the data center. Which of the following is the MOST secure way to meet this goal?

A. Use Motion detectors to signal security whenever anyone entered the center
B. Mount CCTV cameras inside the center to monitor people as they enter
C. Install mantraps at every entrance to the data center in conjunction with their badges
D. Place biometric readers at the entrances to verify employees' identity

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 13
A company hosts a web server that requires entropy in encryption initialization and authentication. To meet this goal, the company would like to select a block cipher mode of operation that allows an arbitrary length IV and supports authenticated encryption. Which of the following would meet these objectives?

A. CFB
B. GCM
C. ECB
D. CBC

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 14
A chief information security officer (CISO) is providing a presentation to a group of network engineers. In the presentation, the CISO presents information regarding exploit kits. Which of the following might the CISO present?

A. Exploit kits are tools capable of taking advantage of multiple CVEs
B. Exploit kits are vulnerability scanners used by penetration testers
C. Exploit kits are WIFI scanning tools that can find new honeypots
D. Exploit kits are a new type of malware that allow attackers to control their computers

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 15
During a company-wide initiative to harden network security, it is discovered that end users who have laptops cannot be removed from the local administrator group. Which of the following could be used to help mitigate the risk of these machines becoming compromised?

A. Security log auditing
B. Firewalls
C. HIPS
D. IDS

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 16
An administrator receives a security alert that appears to be from one of the company's vendors. The email contains information and instructions for patching a serious flaw that has not been publicly announced. Which of the following can an employee use to validate the authenticity if the email?

A. Hashing algorithm
B. Ephemeral Key
C. SSL certificate chain
D. Private key
E. Digital signature

Correct Answer: E
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 17
A project team is developing requirements of the new version of a web application used by internal and external users. The application already features username and password requirements for login, but the organization is required to implement multifactor authentication to meet regulatory requirements. Which of the following would be added requirements will satisfy the regulatory requirement? (Select THREE.)

A. Digital certificate
B. Personalized URL
C. Identity verification questions
D. Keystroke dynamics
E. Tokenized mobile device
F. Time-of-day restrictions
G. Increased password complexity
H. Rule-based access control

Correct Answer: ADE
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 18
A bank is planning to implement a third factor to protect customer ATM transactions. Which of the following could the bank implement?

A. SMS
B. Fingerprint
C. Chip and Pin
D. OTP

Correct Answer: B
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 19
Which of the following internal security controls is aimed at preventing two system administrators from completing the same tasks?

A. Least privilege
B. Separation of Duties
C. Mandatory Vacation
D. Security Policy

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 20
An administrator performs a risk calculation to determine if additional availability controls need to be in place. The administrator estimates that a server fails and needs to be replaced once every 2 years at a cost of $8,000. Which of the following represents the factors that the administrator would use to facilitate this calculation?

A. ARO= 0.5; SLE= $4,000; ALE= $2,000
B. ARO=0.5; SLE=$8,000; ALE=$4,000
C. ARO=0.5; SLE= $4,000; ALE=$8,000
D. ARO=2; SLE= $4,000; ALE=$8,000
E. ARO=2; SLE= $8,000; ALE= $16,000

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 21
A security administrator needs to implement a technology that creates a secure key exchange. Neither party involved in the key exchange will have pre-existing knowledge of one another. Which of the following technologies would allow for this?

A. Blowfish
B. NTLM
C. Diffie-Hellman
D. CHAP

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 22
A technician has been assigned a service request to investigate a potential vulnerability in the organization's extranet platform. Once the technician performs initial investigative measures, it is determined that the potential vulnerability was a false-alarm. Which of the following actions should the technician take in regards to the findings?

A. Write up the findings and disable the vulnerability rule in future vulnerability scans
B. Refer the issue to the server administrator for resolution
C. Mark the finding as a false-negative and close the service request
D. Document the results and report the findings according to the incident response plan

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 23
A security administrator is using a software program to test the security of a wireless access point. After running the program for a few hours, the access point sends the wireless secret key back to the software program.
Which of the following attacks is this an example of?

A. WPS

B. IV

C. Deauth

D. Replay

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:
Explanation: Deauth attack sends disassocate packets to one or more clients which are currently associated with a particular access point. Disassociating clients can be done for a number of reasons:
Recovering a hidden ESSID. This is an ESSID which is not being broadcast. Another term for this is "cloaked".
Capturing WPA/WPA2 handshakes by forcing clients to reauthenticate Generate ARP requests (Windows clients sometimes flush their ARP cache when disconnected)

QUESTION 24
A user, Ann, has been issued a smart card and is having problems opening old encrypted email. Ann published her certificates to the local windows store and to the global address list. Which of the following would still need to be performed?

A. Setup the email security with her new certificates

B. Recover her old private certificate

C. Reinstall her previous public certificate

D. Verify the correct email address is associated with her certificate

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 25
Which of the following is a best practice when setting up a client to use the LDAPS protocol with a server?

A. The client should follow LDAP referrals to other secure servers on the network

B. The client should trust the CA that signed the server's certificate

C. The client should present a self-signed certificate to the server

D. The client should have access to port 389 on the server

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 26
A network manager needs a cost-effective solution to allow for the restoration of information with a RPO of 24 hours. The disaster recovery plan also requires that backups occur within a restricted timeframe during the week and be take offsite weekly. Which of the following should the manager choose to BEST address these requirements?

A. Daily incremental backup to tape
B. Disk-to-disk hourly server snapshots
C. Replication of the environment at a hot site
D. Daily differential backup to tape
E. Daily full backup to tape

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 27
Given the following set of firewall rules:
From the inside to outside allow source any destination any port any From inside to dmz allow source any destination any port tcp-80 From inside to dmz allow source any destination any port tcp-443 Which of the following would prevent FTP traffic from reaching a server in the DMZ from the inside network?

A. Implicit deny
B. Policy routing
C. Port forwarding
D. Forwarding proxy

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 28
During a routine configuration audit, a systems administrator determines that a former employee placed an executable on an application server. Once the system was isolated and diagnosed, it was determined that the executable was programmed to establish a connection to a malicious command and control server. Which of the following forms of malware is best described in the scenario?

A. Logic bomb
B. Rootkit
C. Back door
D. Ransomware

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 29
The chief information officer (CIO) of a major company intends to increase employee connectivity and productivity by issuing employees mobile devices with access to their enterprise email, calendar, and contacts. The solution the CIO intends to use requires a PKI that automates the enrollment of mobile device certificates. Which of the following, when implemented and configured securely, will meet the CIO's requirement?

A. OCSP
B. SCEP
C. SAML
D. OSI

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 30
An attacker impersonates a fire marshal and demands access to the datacenter under the threat of a fine. Which of the following reasons make this effective? (Select two.)

A. Consensus
B. Authority
C. Intimidation
D. Trust
E. Scarcity

Correct Answer: BC
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 31
In the course of troubleshooting wireless issues from users a technician discovers that users are connecting to their home SSIDs which the technician scans but detects none of these SSIDs. The technician eventually discovers a rouge access point that spoofs any SSID request. Which of the following allows wireless use while mitigating this type of attack?

A. Configure the device to verify access point MAC addresses
B. Disable automatic connection to known SSIDs
C. Only connect to trusted wireless networks
D. Enable MAC filtering on the wireless access point

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 32
Which of the following describes the implementation of PAT?

A. Translating the source and destination IPS, but not the source and destination ports
B. A one to one persistent mapping between on private IP and one Public IP
C. Changing the priority of a TCP stream based on the source address
D. Associating multiple private IP addresses with one public address

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 33
Which of the following forms of software testing can best be performed with no knowledge of how a system is internally structured or functions? (Select Two.)

A. Boundary testing
B. White box
C. Fuzzing
D. Black box
E. Grey Box

Correct Answer: CD
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 34
A load balancer has the ability to remember which server a particular client is using and always directs that client to the same server. This feature is called:

A. Cookie tracking
B. URL filtering
C. Session affinity
D. Behavior monitoring

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 35
A company has recently begun to provide internal security awareness for employees. Which of the following would be used to demonstrate the effectiveness of the training?

A. Metrics
B. Business impact analysis
C. Certificate of completion
D. Policies

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 36
Users in an organization are experiencing when attempting to access certain websites. The users report that when they type in a legitimate URL, different boxes appear on the screen, making it difficult to access the legitimate sites. Which of the following would best mitigate this issue?

A. Pop-up blockers
B. URL filtering
C. Antivirus
D. Anti-spam

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 37
A company hires a penetration testing team to test its overall security posture. The organization has not disclosed any information to the penetration testing team and has allocated five days for testing. Which of the following types of testing will the penetration testing team have to conduct?

A. Static analysis
B. Gray Box
C. White box

D. Black box

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 38
A web administrator has just implemented a new web server to be placed in production. As part of the company's security plan, any new system must go through a security test before it is placed in production. The security team runs a port scan resulting in the following data:
21 tcp open FTP
23 tcp open Telnet
22 tcp open SSH
25 UDP open smtp
110 tcp open pop3
443 tcp open https
Which of the following is the BEST recommendation for the web administrator?

A. Implement an IPS
B. Disable unnecessary services
C. Disable unused accounts
D. Implement an IDS
E. Wrap TELNET in SSL

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 39
Which of the following best describes the reason for using hot and cold aisles?

A. To ensure air exhaust from one aisle doesn't blow into the air intake of the next aisle
B. To ensure the dewpoint stays low enough that water doesn't condensate on equipment
C. To decrease amount of power wiring that is run to each aisle

D. Too maintain proper humidity in the datacenter across all aisles

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 40
An organization has an internal PKI that utilizes client certificates on each workstation. When deploying a new wireless network, the security engineer has asked that the new network authenticate clients by utilizes the existing client certificates. Which of the following authentication mechanisms should be utilized to meet this goal?

A. EAP-FAST
B. LEAP
C. PEAP
D. EAP-TLS

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 41
An attacker is attempting to insert malicious code into an installer file that is available on the internet. The attacker is able to gain control of the web server that houses both the installer and the web page which features information about the downloadable file. To implement the attack and delay detection, the attacker should modify both the installer file and the:

A. SSL certificate on the web server
B. The HMAC of the downloadable file available on the website
C. Digital signature on the downloadable file
D. MD5 hash of the file listed on the website

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 42
After receiving the hard drive from detectives, the forensic analyst for a court case used a log to capture corresponding events prior to sending the evidence to lawyers. Which of the following do these actions demonstrate?

A. Chain of custody
B. Order if volatility
C. Data analysis
D. Tracking man hours and expenses

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 43
A group of users from multiple departments are working together on a project and will maintain their digital output in a single location. Which of the following is the BEST method to ensure access is restricted to use by only these users?

A. Mandatory access control
B. Rule-based access
C. Group based privileges
D. User assigned privileges

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 44
Which of the following technologies when applied to android and iOS environments, can an organization use to add security restrictions and encryption to existing mobile applications? (Select Two)

A. Mobile device management
B. Containerization
C. Application whitelisting
D. Application wrapping
E. Mobile application store

Correct Answer: BD
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 45
A server administrator discovers the web farm is using weak ciphers and wants to ensure that only stronger ciphers are accepted. Which of the following ciphers should the administrator implement in the load balancer? (Select Two)

A. SHA-192
B. DES
C. MD5
D. RC4
E. CRC-32

Correct Answer: AD
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 46
An application developer has coded a new application with a module to examine all user entries for the graphical user interface. The module verifies that user entries match the allowed types for each field and that OS and database commands are rejected before entries are sent for further processing within the application.
These are example of:

A. Input validation
B. SQL injection
C. Application whitelisting
D. Error handling

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 47
Ann, a security administrator is hardening the user password policies. She currently has the following in place.
Passwords expire every 60 days
Password length is at least eight characters
Passwords must contain at least one capital letter and one numeric character Passwords cannot be reused until the password has been changed eight times She learns that several employees are still using their original password after the 60-day forced change. Which of the following can she implement to BEST mitigate this?

A. Lower the password expiry time to every 30 days instead of every 60 days
B. Require that the password contains at least one capital, one numeric, and one special character
C. Change the re-usage time from eight to 16 changes before a password can be repeated
D. Create a rule that users can only change their passwords once every two weeks

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 48
Which of the following BEST describes disk striping with parity?

A. RAID O
B. RAID 1
C. RAID 2
D. RAID 5

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 49
Which of the following will allow the live state of the virtual machine to be easily reverted after a failed upgrade?

A. Replication
B. Backups
C. Fault tolerance
D. Snapshots

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 50
An organization currently uses FTP for the transfer of large files, due to recent security enhancements, is now required to use a secure method of file transfer and is testing both SFTP and FTPS as alternatives. Which of the following ports should be opened on the firewall in order to test the two alternatives? (Select Two)

A. TCP 22
B. TCP 25
C. TCP 69
D. UDP 161
E. TCP 990
F. TCP 3380

Correct Answer: AE
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 51
Which of the following types of malware, attempts to circumvent malware detection by trying to hide its true location on the infected system?

A. Armored virus
B. Ransomware
C. Trojan
D. Keylogger

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 52
An attacker went to a local bank and collected disposed paper for the purpose of collecting data that could be used to steal funds and information from the bank's customers. This is an example of:

A. Impersonation
B. Whaling
C. Dumpster diving
D. Hoaxes

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 53
An employee reports work was being completed on a company owned laptop using a public wireless hot-spot. A pop-up screen appeared and the user closed the pop-up. Seconds later the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?

A. Ransomware
B. Rootkit
C. Scareware
D. Spyware

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 54
A small IT security form has an internal network composed of laptops, servers, and printers. The network has both wired and wireless segments and supports VPN access from remote sites. To protect the network from internal and external threats, including social engineering attacks, the company decides to implement stringent security controls. Which of the following lists is the BEST combination of security controls to implement?

A. Disable SSID broadcast, require full disk encryption on servers, laptop, and personally owned electronic devices, enable MAC filtering on WAPs, require photographic ID to enter the building.
B. Enable port security; divide the network into segments for servers, laptops, public and remote users; apply ACLs to all network equipment; enable MAC filtering on WAPs; and require two-factor authentication for network access.
C. Divide the network into segments for servers, laptops, public and remote users; require the use of one time pads for network key exchange and access; enable MAC filtering ACLs on all servers.
D. Enable SSID broadcast on a honeynet; install monitoring software on all corporate equipment' install CCTVs to deter social engineering; enable SE Linux in permissive mode.

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 55
A security analyst is working on a project team responsible for the integration of an enterprise SSO solution. The SSO solution requires the use of an open

standard for the exchange of authentication and authorization across numerous web based applications. Which of the following solutions is most appropriate for the analyst to recommend in this scenario?

A. SAML
B. XTACACS
C. RADIUS
D. TACACS+
E. Secure LDAP

Correct Answer: A
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 56
A thief has stolen mobile device and removed its battery to circumvent GPS location tracking. The device user is a four digit PIN. Which of the following is a mobile device security control that ensures the confidentiality of company data?

A. Remote wiping
B. Mobile Access control
C. Full device encryption
D. Inventory control

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 57
A user has called the help desk to report an enterprise mobile device was stolen. The technician receiving the call accesses the MDM administration portal to identify the device's last known geographic location. The technician determines the device is still communicating with the MDM. After taking note of the last known location, the administrator continues to follow the rest of the checklist. Which of the following identifies a possible next step for the administrator?

A. Remotely encrypt the device
B. Identify the mobile carrier's IP address

C. Reset the device password
D. Issue a remote wipe command

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 58
A risk management team indicated an elevated level of risk due to the location of a corporate datacenter in a region with an unstable political climate. The chief information officer (CIO) accepts the recommendation to transition the workload to an alternate datacenter in a more stable region. Which of the following forms of risk mitigation has the CIO elected to pursue?

A. Deterrence
B. Transference
C. Avoidance
D. Acceptance
E. sharing

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 59
During a recent audit, the auditors cited the company's current virtual machine infrastructure as a concern. The auditors cited the fact that servers containing sensitive customer information reside on the same physical host as numerous virtual machines that follow less stringent security guild lines. Which of the following would be the best choice to implement to address this audit concern while maintain the current infrastructure?

A. Migrate the individual virtual machines that do not contain sensitive data to separate physical machines
B. Implement full disk encryption on all servers that do not contain sensitive customer data
C. Move the virtual machines that contain the sensitive information to a separate host
D. Create new VLANs and segment the network according to the level of data sensitivity

Correct Answer: D

Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 60
A switch is set up to allow only 2 simultaneous MAC addresses per switch port. An administrator is reviewing a log and determines that a switch port has been deactivated in a conference room after it detected 3 or more MAC addresses on the same port. Which of the following reasons could have caused this port to be disabled?

A. A pc had a NIC replaced and reconnected to the switch
B. An ip telephone has been plugged in
C. A rouge access point was plugged in
D. An arp attack was launched from a pc on this port

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 61
A network administrator was to implement a solution that will allow authorized traffic, deny unauthorized traffic and ensure that appropriate ports are being used for a number of TCP and UDP protocols. Which of the following network controls would meet these requirements?

A. Stateful firewall
B. Web security gateway
C. URL filter
D. proxy server
E. web application firewall

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 62
Client computers login at specified times to check and update antivirus definitions using a dedicated account configured by the administrator. One day the clients are unable to login with the account, but the server still responds to ping requests. The administrator has not made any changed. Which of the following most likely happened?

A. Group policy is blocking the connection attempts
B. The administrator account has been disabled
C. The switch port for the server has died
D. The password on the account has expired

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 63
In performing an authorized penetration test of an organization's system security, a penetration tester collects information pertaining to the application versions that reside on a server. Which of the following is the best way to collect this type of information?

A. Protocol analyzer
B. Banner grabbing
C. Port scanning
D. Code review

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 64
a company is deploying an new video conferencing system to be used by the executive team for board meetings. The security engineer has been asked to choose the strongest available asymmetric cipher to be used for encryption of board papers, and chose the strongest available stream cipher to be configured for video streaming. Which of the following ciphers should be chosen? (Select two)

A. RSA
B. RC4
C. 3DES
D. HMAC
E. SHA-256

Correct Answer: AB
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 65
Joe has hired several new security administrators and have been explaining the design of the company's network. He has described the position and descriptions of the company's firewalls, IDS sensors, antivirus server, DMZs, and HIPS. Which of the following best describes the incorporation of these elements?

A. Load balancers
B. Defense in depth
C. Network segmentation
D. UTM security appliance

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 66
A security administrator is selecting an MDM solution for an organization, which has strict security requirements for the confidentiality of its data on end user devices. The organization decides to allow BYOD, but requires that users wishing to participate agree to the following specific device configurations; camera disablement, password enforcement, and application whitelisting. The organization must be able to support a device portfolio of differing mobile operating systems. Which of the following represents the MOST relevant technical security criteria for the MDM?

A. Breadth of support for device manufacturers' security configuration APIs
B. Ability to extend the enterprise password polices to the chosen MDM
C. Features to support the backup and recovery of the stored corporate data

D. Capability to require the users to accept an AUP prior to device onboarding

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:
Explanation: Codeproof provides the following Mobile Device Management (MDM) API's to partners & mobile developers. Integration of Codeproof MDM APIs with other software or a mobile app, allows significantly more control over reporting & management of mobile devices.

QUESTION 67
Employees are reporting that they have been receiving a large number of emails advertising products and services. Links in the email direct the users' browsers to the websites for the items being offered. No reports of increased virus activity have been observed. A security administrator suspects that the users are the targets of:

A. A watering hole attack
B. Spear phishing
C. A spoofing attack
D. A spam campaign

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 68
An employee finds a usb drive in the employee lunch room and plugs the drive into a shared workstation to determine who owns the drive. When the drive is inserted, a command prompt opens and a script begins to run. The employee notifies a technician who determines that data on a server have been compromised. This is an example of:

A. Device removal
B. Data disclosure
C. Incident identification
D. Mitigation steps

Correct Answer: C
Section: 2. Compliance and Operational security

Explanation

Explanation/Reference:

QUESTION 69

A chief information officer (CIO) is concerned about PII contained in the organization's various data warehouse platforms. Since not all of the PII transferred to the organization is required for proper operation of the data warehouse application, the CIO requests the needed PII data be parsed and securely discarded. Which of the following controls would be MOST appropriate in this scenario?

A. Execution of PII data identification assessments
B. Implementation of data sanitization routines
C. Encryption of data-at-rest
D. Introduction of education programs and awareness training
E. Creation of policies and procedures

Correct Answer: E
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 70

The security administrator receives a service ticket saying a host based firewall is interfering with the operation of a new application that is being tested in development. The administrator asks for clarification on which ports need to be open. The software vendor replies that it could use up to 20 ports and many customers have disabled the host based firewall. After examining the system the administrator sees several ports that are open for database and application servers that only used locally. The vendor continues to recommend disabling the host based firewall. Which of the following is the best course of action for the administrator to take?

A. Allow ports used by the application through the network firewall
B. Allow ports used externally through the host firewall
C. Follow the vendor recommendations and disable the host firewall
D. Allow ports used locally through the host firewall

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 71

A corporate wireless guest network uses an open SSID with a captive portal to authenticate guest users. Guests can obtain their portal password at the service desk. A security consultant alerts the administrator that the captive portal is easily bypassed, as long as one other wireless guest user is on the network. Which of the following attacks did the security consultant use?

A. ARP poisoning
B. DNS cache poisoning
C. MAC spoofing
D. Rouge DHCP server

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 72

A company requires that all wireless communication be compliant with the advanced encryption standard (AES). The current wireless infrastructure implements WEP + TKIP. Which of the following wireless protocols should be implemented?

A. CCMP
B. 802.1x
C. 802.3
D. WPA2
E. AES

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 73

A security analyst, while doing a security scan using packet capture security tools, noticed large volumes of data images of company products being exfiltrated to foreign IP addresses. Which of the following is the FIRST step in responding to scan results?

A. Incident identification
B. Implement mitigation
C. Chain of custody
D. Capture system image

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 74
An administrator deploys a WPA2 Enterprise wireless network with EAP-PEAP-MSCHAPv2. The deployment is successful and company laptops are able to connect automatically with no user intervention. A year later, the company begins to deploy phones with wireless capabilities. Users report that they are receiving a warning when they attempt to connect to the wireless network from their phones. Which of the following is the MOST likely cause of the warning message?

A. Mutual authentication on the phone is not compatible with the wireless network
B. The phones do not support WPA2 Enterprise wireless networks
C. User certificates were not deployed to the phones
D. The phones' built in web browser is not compatible with the wireless network
E. Self-signed certificates were used on the RADIUS servers

Correct Answer: C
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 75
An attacker has gained access to the company's web server by using the administrator's credentials. The attacker then begins to work on compromising the sensitive data on other servers. Which off the following BEST describes this type of attack?

A. Privilege escalation
B. Client-side attack
C. Man-in-the-middle

D. Transitive access

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 76
A security technician is concerned there is not enough security staff available the web servers and database server located in the DMZ around the clock. Which of the following technologies, when deployed, would provide the BEST round the clock automated protection?

A. HIPS & SIEM
B. NIPS & HIDS
C. HIDS & SIEM
D. NIPS & HIPS

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 77
Which of the following best describes the objectives of succession planning?

A. To identify and document the successive order in which critical systems should be reinstated following a disaster situation
B. To ensure that a personnel management plan is in place to ensure continued operation of critical processes during an incident
C. To determine the appropriate order in which contract internal resources, third party suppliers and external customers during a disaster response
D. To document the order that systems should be reinstated at the primary site following a failover operation at a backup site.

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 78
A system administrator wants to use open source software but is worried about the source code being comprised. As a part of the download and installation process, the administrator should verify the integrity of the software by:

A. Creating a digital signature of the file before installation
B. Using a secure protocol like HTTPS to download the file
C. Checking the hash against an official mirror that contains the same file
D. Encryption any connections the software makes

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 79
The chief security officer (CSO) has reported a rise in data loss but no break-ins have occurred. By doing which of the following would the CSO MOST likely to reduce the number of incidents?

A. Implement protected distribution
B. Employ additional firewalls
C. Conduct security awareness training
D. Install perimeter barricades

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:
Explanation: A protective distribution system (PDS), also called protected distribution system, is a US government term for wireline or fiber-optics telecommunication system that includes terminals and adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information. At one time these systems were called "approved circuits".

QUESTION 80
In an effort to test the effectiveness of an organization's security awareness training, a penetrator tester crafted an email and sent it to all of the employees to see how many of them clicked on the enclosed links. Which of the following is being tested?

A. How many employees are susceptible to a SPAM attack
B. How many employees are susceptible to a cross-site scripting attack
C. How many employees are susceptible to a phishing attack
D. How many employees are susceptible to a vishing attack

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 81
Devices on the SCADA network communicate exclusively at Layer 2. Which of the following should be used to prevent unauthorized systems using ARP-based attacks to compromise the SCADA network?

A. Application firewall
B. IPSec
C. Hardware encryption
D. VLANS

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 82
When information is shared between two separate organizations, which of the following documents would describe the sensitivity as well as the type and flow of the information?

A. SLA
B. ISA
C. BPA
D. MOA

Correct Answer: B
Section: 2. Compliance and Operational security

Explanation

Explanation/Reference:

QUESTION 83
Joe noticed that there is a larger than normal amount of network load on the printer VLAN of his organization, causing users to have to wait a long time for a print job. Upon investigation Joe discovers that printers were ordered and added to the network without his knowledge. Which of the following will reduce the risk of this occurring again in the future?

A. Log analysis
B. Loop protection
C. Access control list
D. Rule-based management

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:
Explanation: A rule-based management group automates the selection of conforming systems and applications and logically groups them using custom properties. Rule-based management groups work well when you have less information about the system that is being managed and you need to rely on the rules to select the correct system.

QUESTION 84
Jo an employee reports to the security manager that several files in a research and development folder that only Joe has access to have been improperly modified. The modified data on the files in recent and the modified by account is Joe's. The permissions on the folder have not been changed, and there is no evidence of malware on the server hosting the folder or on Joe's workstation. Several failed login attempts to Joe's account were discovered in the security log of the LDAP server. Given this scenario, which of the following should the security manager implement to prevent this in the future?

A. Generic account prohibition
B. Account lockout
C. Password complexity
D. User access reviews

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 85
A user contacts the help desk after being unable to log in to a corporate website. The user can log into the site from another computer in the next office, but not from the PC. The user's PC was able to connect earlier in the day. The help desk has user restart the NTP service. Afterwards the user is able to log into the website. The MOST likely reason for the initial failure was that the website was configured to use which of the following authentication mechanisms?

A. Secure LDAP
B. RADIUS
C. NTLMv2
D. Kerberos

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 86
A security analyst has been investigating an incident involving the corporate website. Upon investigation, it has been determined that users visiting the corporate website would be automatically redirected to a, malicious site. Further investigation on the corporate website has revealed that the home page on the corporate website has been altered to include an unauthorized item. Which of the following would explain why users are being redirected to the malicious site?

A. DNS poisoning
B. XSS
C. Iframe
D. Session hijacking

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 87
A news and weather toolbar was accidentally installed into a web browser. The toolbar tracks users online activities and sends them to a central logging server. Which of the following attacks took place?

A. Man-in-the-browser
B. Flash cookies
C. Session hijacking
D. Remote code execution
E. Malicious add-on

Correct Answer: E
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 88
A project manager is working with an architectural firm that focuses on physical security. The project manager would like to provide requirements that support the primary goal of safely. Based on the project manager's desires, which of the following controls would the BEST to incorporate into the facility design?

A. Biometrics
B. Escape routes
C. Reinforcements
D. Access controls

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 89
While performing surveillance activities an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security controls?

A. MAC spoofing
B. Pharming
C. Xmas attack
D. ARP poisoning

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 90
An administrator wants to configure a switch port so that it separates voice and data traffic. Which of the following MUST be configured on the switch port to enforce separation of traffic?

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

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 91
A company must send sensitive data over a non-secure network via web services. The company suspects that competitors are actively trying to intercept all transmissions. Some of the information may be valuable to competitors, even years after it has been sent. Which of the following will help mitigate the risk in the scenario?

A. Digitally sign the data before transmission
B. Choose steam ciphers over block ciphers
C. Use algorithms that allow for PFS
D. Enable TLS instead of SSL
E. Use a third party for key escrow

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 92
When implementing a mobile security strategy for an organization which of the following is the MOST influential concern that contributes to that organization's ability to extend enterprise policies to mobile devices?

A. Support for mobile OS
B. Support of mobile apps
C. Availability of mobile browsers
D. Key management for mobile devices

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 93
A recent review of accounts on various systems has found that after employees passwords are required to change they are recycling the same password as before. Which of the following policies should be enforced to prevent this from happening? (Select TWO)

A. Reverse encryption
B. Minimum password age
C. Password complexity
D. Account lockouts
E. Password history
F. Password expiration

Correct Answer: BE
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 94
A system administrator runs a network inventory scan every Friday at 10:00 am to track the progress of a large organization's operating system upgrade of all laptops. The system administrator discovers that some laptops are now only being reported as IP addresses. Which of the following options is MOST likely the

cause of this issue?

A. HIDS
B. Host-based firewalls rules
C. All the laptops are currently turned off
D. DNS outage

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 95
A security administrator working for a law enforcement organization is asked to secure a computer system at the scene of a crime for transport to the law enforcement forensic facility. In order to capture as mush evidence as possible, the computer system has been left running. The security administrator begins information by image which of the following system components FIRST?

A. NVRAM
B. RAM
C. TPM
D. SSD

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 96
A new employee has been hired to perform system administration duties across a large enterprise comprised of multiple separate security domains. Each remote location implements a separate security domain. The new employee has successfully responded to and fixed computer issues for the main office. When the new employee tries to perform work on remote computers, the following messages appears. You need permission to perform this action. Which of the following can be implemented to provide system administrators with the ability to perform administrative tasks on remote computers using their uniquely assigned account?

A. Implement transitive trust across security domains
B. Enable the trusted OS feature across all enterprise computers

C. Install and configure the appropriate CA certificate on all domain controllers

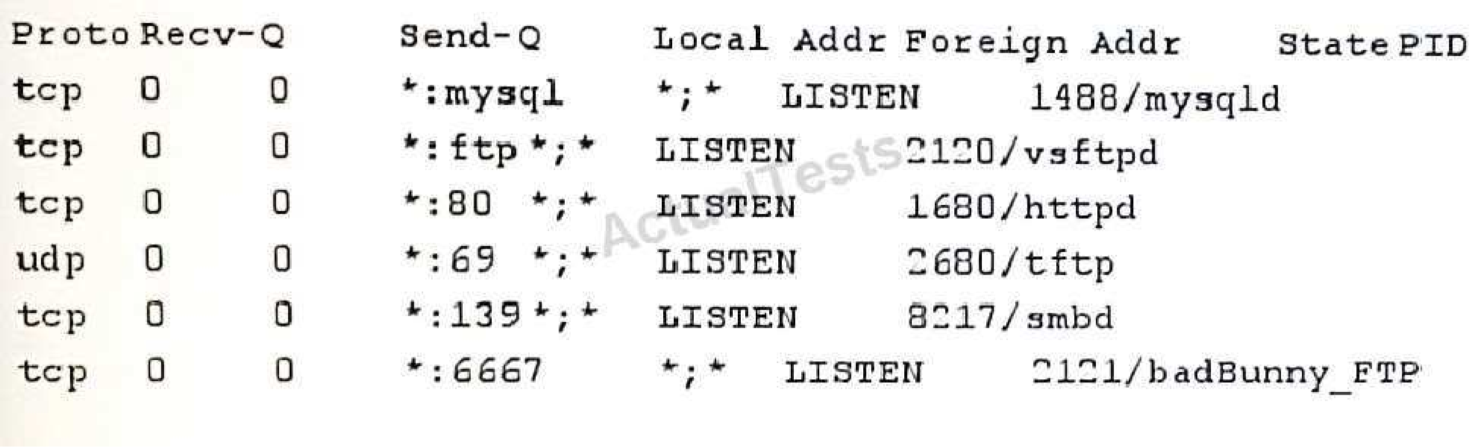
D. Verify that system administrators are in the domain administrator group in the main office

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 97

An administrator is hardening systems and wants to disable unnecessary services. One Linux server hosts files used by a Windows web server on another machine. The Linux server is only used for secure file transfer, but requires a share for the Windows web server as well. The administrator sees the following output from a netstat -1p command:



```
Proto Recv-Q     Send-Q      Local Addr Foreign Addr     State PID
tcp   0      0   *:mysql     *;*   LISTEN     1488/mysqld
tcp   0      0   *:ftp *;*   LISTEN     2120/vsftpd
tcp   0      0   *:80  *;*   LISTEN     1680/httpd
udp   0      0   *:69  *;*   LISTEN     2680/tftp
tcp   0      0   *:139 *;*   LISTEN     8217/smbd
tcp   0      0   *:6667      *;*   LISTEN     2121/badBunny_FTP
```

Which of the following processes can the administrator kill without risking impact to the purpose and function of the Linux or Windows servers? (Select Three)

A. 1488
B. 1680
C. 2120
D. 2121
E. 2680
F. 8217

Correct Answer: BDE
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:
Answer:

QUESTION 98
A project manager is evaluating proposals for a cloud computing project. The project manager is particularly concerned about logical security controls in place at the service provider's facility. Which of the following sections of the proposal would be MOST important to review, given the project manager's concerns?

A. CCTV monitoring
B. Perimeter security lighting system
C. Biometric access system
D. Environmental system configuration

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:
Explanation: Logical security consists of software safeguards for an organization's systems, including user identification and password access, authenticating, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation.

QUESTION 99
A security administrator would like to ensure that some members of the building's maintenance staff are only allowed access to the facility during weekend hours. Access to the facility is controlled by badge swipe and a man trap. Which of the following options will BEST accomplish this goal?

A. CCTV
B. Security Guard

C. Time of day restrictions

D. Job rotation

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 100
A security manager received reports of several laptops containing confidential data stolen out of a lab environment. The lab is not a high security area and is secured with physical key locks. The security manager has no information to provide investigators related to who may have stolen the laptops. Which of the following should the security manager implement to improve legal and criminal investigations in the future?

A. Motion sensors

B. Mobile device management

C. CCTV

D. Cable locks

E. Full-disk encryption

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 101
During a Linux security audit at a local college, it was noted that members of the dean's group were able to modify employee records in addition to modifying student records, resulting in an audit exception. The college security policy states that the dean's group should only have the ability to modify student records. Assuming that the correct user and group ownerships are in place, which of the following sets of permissions should have been assigned to the directories containing the employee records?

A. R-x---rwx

B. Rwxrwxrwx

C. Rwx----wx

D. Rwxrwxr--

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 102
Which of the following can be mitigated with proper secure coding techniques?

A. Input validation
B. Error handling
C. Header manipulation
D. Cross-site scripting

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 103
Recently the desktop support group has been performing a hardware refresh and has replaced numerous computers. An auditor discovered that a number of the new computers did not have the company's antivirus software installed on them, Which of the following could be utilized to notify the network support group when computers without the antivirus software are added to the network?

A. Network port protection
B. NAC
C. NIDS
D. Mac Filtering

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 104
An administrator needs to protect against downgrade attacks due to various vulnerabilities in SSL/TLS. Which of the following actions should be performed? (Select TWO)

A. Set minimum protocol supported
B. Request a new certificate from the CA
C. Configure cipher order
D. Disable flash cookie support
E. Re-key the SSL certificate
F. Add the old certificate to the CRL

Correct Answer: AC
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 105
A developer needs to utilize AES encryption in an application but requires the speed of encryption and decryption to be as fast as possible. The data that will be secured is not sensitive so speed is valued over encryption complexity. Which of the following would BEST satisfy these requirements?

A. AES with output feedback
B. AES with cipher feedback
C. AES with cipher block chaining
D. AES with counter mode

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:
Explanation: CTR is used if you want good parallelization (ie. speed), instead of CBC/OFB/CFB.

QUESTION 106
During a code review a software developer discovers a security risk that may result in hundreds of hours of rework. The security team has classified these issues as low risk. Executive management has decided that the code will not be rewritten. This is an example of:

A. Risk avoidance

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

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 107
A network was down for several hours due to a contractor entering the premises and plugging both ends of a network cable into adjacent network jacks. Which of the following would have prevented the network outage? (Select Two)

A. Port security
B. Loop Protection
C. Implicit deny
D. Log analysis
E. Mac Filtering
F. Flood Guards

Correct Answer: AB
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 108
After disabling SSID broadcast, a network administrator still sees the wireless network listed in available networks on a client laptop. Which of the following attacks may be occurring?

A. Evil Twin
B. ARP spoofing
C. Disassociation flooding
D. Rogue access point
E. TKIP compromise

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 109
A security manager is preparing the training portion of an incident plan. Which of the following job roles should receive training on forensics, chain of custody, and the order of volatility?

A. System owners
B. Data custodians
C. First responders
D. Security guards

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 110
Virtualization that allows an operating system kernel to run multiple isolated instances of the guest is called:

A. Process segregation
B. Software defined network
C. Containers
D. Sandboxing

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 111
Which of the following is a proprietary protocol commonly used for router authentication across an enterprise?

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

Correct Answer: B
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 112
While responding to an incident on a new Windows server, the administrator needs to disable unused services. Which of the following commands can be used to see processes that are listening on a TCP port?

A. IPCONFIG
B. Netstat
C. PSINFO
D. Net session

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 113
A system administrator must configure the company's authentication system to ensure that users will be unable to reuse the last ten passwords within a six months period. Which of the following settings must be configured? (Select Two)

A. Minimum password age
B. Password complexity
C. Password history
D. Minimum password length

E. Multi-factor authentication
F. Do not store passwords with reversible encryption

Correct Answer: AC
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 114
An administrator requests a new VLAN be created to support the installation of a new SAN. Which of the following data transport?

A. Fibre Channel
B. SAS
C. Sonet
D. ISCSI

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 115
Which of the following access control methodologies provides an individual with the most restrictive access rights to successfully perform their authorized duties?

A. Mandatory Access Control
B. Rule Based Access Control
C. Least Privilege
D. Implicit Deny
E. Separation of Duties

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 116
An administrator wants to provide onboard hardware based cryptographic processing and secure key storage for full-disk encryption. Which of the following should the administrator use to fulfill the requirements?

A. AES
B. TPM
C. FDE
D. PAM

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 117
When viewing IPS logs the administrator see systems all over the world scanning the network for servers with port 22 open. The administrator concludes that this traffic is a(N):

A. Risk
B. Vulnerability
C. Exploit
D. Threat

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 118
Ann a user has been promoted from a sales position to sales manager. Which of the following risk mitigation strategies would be MOST appropriate when a user changes job roles?

A. Implement data loss prevention

B. Rest the user password
C. User permissions review
D. Notify incident management

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 119
A system administrator is implementing a firewall ACL to block specific communication to and from a predefined list of IP addresses, while allowing all other communication. Which of the following rules is necessary to support this implementation?

A. Implicit allow as the last rule
B. Implicit allow as the first rule
C. Implicit deny as the first rule
D. Implicit deny as the last rule

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 120
Joe a system architect wants to implement appropriate solutions to secure the company's distributed database. Which of the following concepts should be considered to help ensure data security? (Select TWO)

A. Data at rest
B. Data in use
C. Replication
D. Wiping
E. Retention
F. Cloud Storage

Correct Answer: AC
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 121
A forensics analyst is tasked identifying identical files on a hard drive. Due to the large number of files to be compared, the analyst must use an algorithm that is known to have the lowest collision rate. Which of the following should be selected?

A. MD5
B. RC4
C. SHA1
D. AES-256

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 122
A government agency wants to ensure that the systems they use have been deployed as security as possible. Which of the following technologies will enforce protections on these systems to prevent files and services from operating outside of a strict rule set?

A. Host based Intrusion detection
B. Host-based firewall
C. Trusted OS
D. Antivirus

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 123
An organization receives an email that provides instruction on how to protect a system from being a target of new malware that is rapidly infecting systems. The incident response team investigates the notification and determines it to invalid and notifies users to disregard the email. Which of the following BEST describes this occurrence?

A. Phishing
B. Scareware
C. SPAM
D. Hoax

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 124
Joe an employee has reported to Ann a network technician an unusual device plugged into a USB port on a workstation in the call center. Ann unplugs the workstation and brings it to the IT department where an incident is opened. Which of the following should have been done first?

A. Notify the incident response team lead
B. Document chain of custody
C. Take a copy of volatile memory
D. Make an image of the hard drive

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 125
A company is implementing a system to transfer direct deposit information to a financial institution. One of the requirements is that the financial institution must be certain that the deposit amounts within the file have not been changed. Which of the following should be used to meet the requirement?

A. Key escrow
B. Perfect forward secrecy

C. Transport encryption
D. Digital signatures
E. File encryption

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 126
An organization uses a Kerberos-based LDAP service for network authentication. The service is also utilized for internal web applications. Finally access to terminal applications is achieved using the same authentication method by joining the legacy system to the Kerberos realm. This company is using Kerberos to achieve which of the following?

A. Trusted Operating System
B. Rule-based access control
C. Single sign on
D. Mandatory access control

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 127
A recent audit has revealed that all employees in the bookkeeping department have access to confidential payroll information, while only two members of the bookkeeping department have job duties that require access to the confidential information. Which of the following can be implemented to reduce the risk of this information becoming compromised in this scenario? (Select TWO)

A. Rule-based access control
B. Role-based access control
C. Data loss prevention
D. Separation of duties
E. Group-based permissions

Correct Answer: BE
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 128
A Chief Executive Officer (CEO) is steering company towards cloud computing. The CEO is requesting a federated sign-on method to have users sign into the sales application. Which of the following methods will be effective for this purpose?

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

Correct Answer: A
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 129
An administrator is configuring a new Linux web server where each user account is confined to a cheroot jail.
Which of the following describes this type of control?

A. SysV
B. Sandbox
C. Zone
D. Segmentation

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 130
Recently clients are stating they can no longer access a secure banking site's webpage. In reviewing the clients' web browser settings, the certificate chain is showing the following:
Certificate Chain:
X Digi Cert
Digi Cert High assurance C3
* banksite.com
Certificate Store:
Digi Cert Others Certificate Store
Digi Cert High assurance C3 Others Certificate Store
Based on the information provided, which of the following is the problem when connecting to the website?

A. The certificate signature request was invalid
B. Key escrow is failing for the certificate authority
C. The certificate authority has revoked the certificate
D. The clients do not trust the certificate authority

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 131
A company often processes sensitive data for the government. The company also processes a large amount of commercial work and as such is often providing tours to potential customers that take them into various workspaces. Which of the following security methods can provide protection against tour participants viewing sensitive information at minimal cost?

A. Strong passwords
B. Screen protectors
C. Clean-desk policy
D. Mantraps

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 132
Joe is a helpdesk specialist. During a routine audit, a company discovered that his credentials were used while he was on vacation. The investigation further confirmed that Joe still has his badge and it was last used to exit the facility. Which of the following access control methods is MOST appropriate for preventing such occurrences in the future?

A. Access control where the credentials cannot be used except when the associated badge is in the facility
B. Access control where system administrators may limit which users can access their systems
C. Access control where employee's access permissions is based on the job title
D. Access control system where badges are only issued to cleared personnel

Correct Answer: A
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 133
A security architect is designing an enterprise solution for the sales force of a corporation which handles sensitive customer data. The solution must allow users to work from remote offices and support traveling users. Which of the following is the MOST appropriate control for the architect to focus onto ensure confidentiality of data stored on laptops?

A. Full-disk encryption
B. Digital sign
C. Federated identity management
D. Cable locks

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 134
A security administrator needs a method to ensure that only employees can get onto the internal network when plugging into a network switch. Which of the following BEST meets that requirement?

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

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 135
Having adequate lighting on the outside of a building is an example of which of the following security controls?

A. Deterrent
B. Compensating
C. Detective
D. Preventative

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 136
During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions. Which of the following would help reduce the amount of risk the organization incurs in this situation in the future?

A. Time-of-day restrictions
B. User access reviews
C. Group-based privileges
D. Change management policies

Correct Answer: B
Section: 2. Compliance and Operational security

Explanation

Explanation/Reference:

QUESTION 137
An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data. In which of the following documents would this concern MOST likely be addressed?

A. Service level agreement
B. Interconnection security agreement
C. Non-disclosure agreement
D. Business process analysis

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 138
A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources. Which of the following should be implemented?

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

Correct Answer: B
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 139
Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

A. Spear phishing
B. Main-in-the-middle
C. URL hijacking
D. Transitive access

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 140
A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations. Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)

A. SCP
B. TFTP
C. SNMP
D. FTP
E. SMTP
F. FTPS

Correct Answer: AF
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 141
A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected.
Which of the following MUST the technician implement?

A. Dual factor authentication
B. Transitive authentication
C. Single factor authentication
D. Biometric authentication

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 142
After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internet- based control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence. Which of the following is the MOST likely reason the thermostat is not connecting to the internet?

A. The company implements a captive portal
B. The thermostat is using the incorrect encryption algorithm
C. the WPA2 shared likely is incorrect
D. The company's DHCP server scope is full

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 143
A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net). Which of the following rules is preventing the CSO from accessing the site? Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

A. Rule 1: deny from inside to outside source any destination any service smtp
B. Rule 2: deny from inside to outside source any destination any service ping
C. Rule 3: deny from inside to outside source any destination {blocked sites} service http-https
D. Rule 4: deny from any to any source any destination any service any

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 144
Malware that changes its binary pattern on specific dates at specific times to avoid detection is known as a (n):

A. armored virus
B. logic bomb
C. polymorphic virus
D. Trojan

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 145
A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key.
Which of the following could be used?

A. RSA
B. TwoFish
C. Diffie-Helman
D. NTLMv2
E. RIPEMD

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 146

Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

A. MOU
B. ISA
C. BPA
D. SLA

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 147

Which of the following are MOST susceptible to birthday attacks?

A. Hashed passwords
B. Digital certificates
C. Encryption passwords
D. One time passwords

Correct Answer: A
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 148

Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive. Which of the following procedures did Joe follow?

A. Order of volatility
B. Chain of custody
C. Recovery procedure
D. Incident isolation

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 149
A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non- repudiation. Which of the following implements all these requirements?

A. Bcrypt
B. Blowfish
C. PGP
D. SHA

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 150
Given the log output:

```
Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: msmith] [Source:
10.0.12.45]
[localport: 23] at 00:15:23:431 CET Sun Mar 15 2015
```

Which of the following should the network administrator do to protect data security?

A. Configure port security for logons

B. Disable telnet and enable SSH
C. Configure an AAA server
D. Disable password and enable RSA authentication

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 151
The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected. Which of the following is required to complete the certificate chain?

A. Certificate revocation list
B. Intermediate authority
C. Recovery agent
D. Root of trust

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 152
The Chief Executive Officer (CEO) of a major defense contracting company a traveling overseas for a conference. The CEO will be taking a laptop. Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

A. Remote wipe
B. Full device encryption
C. BIOS password
D. GPS tracking

Correct Answer: B
Section: 4. Application, Data, and Host Security

Explanation

Explanation/Reference:

QUESTION 153

In an effort to reduce data storage requirements, a company devices to hash every file and eliminate duplicates. The data processing routines are time sensitive so the hashing algorithm is fast and supported on a wide range of systems. Which of the following algorithms is BEST suited for this purpose?

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

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 154

A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently, the organization uses FTP and HTTP to transfer files. Which of the following should the organization implement in order to be compliant with the new policy?

A. Replace FTP with SFTP and replace HTTP with TLS
B. Replace FTP with FTPS and replaces HTTP with TFTP
C. Replace FTP with SFTP and replace HTTP with Telnet
D. Replace FTP with FTPS and replaces HTTP with IPSec

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 155

Joe notices there are several user accounts on the local network generating spam with embedded malicious code. Which of the following technical control should Joe put in place to BEST reduce these incidents?

A. Account lockout
B. Group Based Privileges
C. Least privilege
D. Password complexity

Correct Answer: A
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 156
Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys. Which of the following can be implemented to enable users to share encrypted data while abiding by company policies?

A. Key escrow
B. Digital signatures
C. PKI
D. Hashing

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 157
An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient. Which of the following capabilities would be MOST appropriate to consider implementing is response to the new requirement?

A. Transitive trust
B. Symmetric encryption
C. Two-factor authentication
D. Digital signatures

E. One-time passwords

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 158
Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data. Which of the following controls can be implemented to mitigate this type of inside threat?

A. Digital signatures
B. File integrity monitoring
C. Access controls
D. Change management
E. Stateful inspection firewall

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 159
The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?

A. Collision resistance
B. Rainbow table
C. Key stretching
D. Brute force attack

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 160
Which of the following is commonly used for federated identity management across multiple organizations?

A. SAML
B. Active Directory
C. Kerberos
D. LDAP

Correct Answer: A
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 161
A security administrator has been asked to implement a VPN that will support remote access over IPsec Which of the following is an encryption algorithm that would meet this requirement?

A. MD5
B. AES
C. UDP
D. PKI

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:
Explanation: Cryptographic algorithms defined for use with IPsec include:
- HMAC-SHA1/SHA2 for integrity protection and authenticity.
- TripleDES-CBC for confidentiality
- AES-CBC for confidentiality.
- AES-GCM providing confidentiality and authentication together efficiently Galois/Counter Mode (GCM) is a mode of operation for symmetric key cryptographic block ciphers that has been widely adopted because of its efficiency and performance. GCM throughput rates for state of the art, high speed communication channels can be achieved with reasonable hardware resources. The operation is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality.
GCM is defined for block ciphers with a block size of 128 bits. Galois Message Authentication Code (GMAC) is an authentication-only variant of the GCM which can

be used as an incremental message authentication code.
Both GCM and GMAC can accept initialization vectors of arbitrary length.
Different block cipher modes of operation can have significantly different performance and efficiency characteristics, even when used with the same block cipher. GCM can take full advantage of parallel processing and implementing GCM can make efficient use of an instruction pipeline or a hardware pipeline. In contrast, the cipher block chaining (CBC) mode of operation incurs significant pipeline stalls that hamper its efficiency and performance

QUESTION 162
A security administrator is evaluating three different services: Radius, Diameter, and Kerberos. Which of the following is a feature that is UNIQUE to Kerberos?

A. It provides authentication services
B. It uses tickets to identify authenticated users
C. It provides single sign-on capability
D. It uses XML for cross-platform interoperability

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 163
Which of the following can affect electrostatic discharge in a network operations center?

A. Fire suppression
B. Environmental monitoring
C. Proximity card access
D. Humidity controls

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 164
a malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL. Which of the following is the attacker most likely utilizing?

A. Header manipulation
B. Cookie hijacking
C. Cross-site scripting
D. XML injection

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:
Explanation: HTTP header injection is a general class of web application security vulnerability which occurs when Hypertext Transfer Protocol (HTTP) headers are dynamically generated based on user input. Header injection in HTTP responses can allow for HTTP response splitting, Session fixation via the Set-Cookie header, cross-site scripting (XSS), and malicious redirect attacks via the location header. HTTP header injection is a relatively new area for web-based attacks, and has primarily been pioneered by Amit Klein in his work on request/response smuggling/splitting.

QUESTION 165
A company would like to prevent the use of a known set of applications from being used on company computers. Which of the following should the security administrator implement?

A. Whitelisting
B. Anti-malware
C. Application hardening
D. Blacklisting
E. Disable removable media

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 166
A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company. Which of the following portions of the company's mobile device management configuration would allow the company data to be removed from the device without touching the new hire's data?

A. Asset control
B. Device access control

C. Storage lock out
D. Storage segmentation

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:
Explanation: Storage segmentation separates personal and business content on the device

QUESTION 167
A consultant has been tasked to assess a client's network. The client reports frequent network outages. Upon viewing the spanning tree configuration, the consultant notices that an old and slow performing edge switch on the network has been elected to be the root bridge. Which of the following explains this scenario?

A. The switch also serves as the DHCP server
B. The switch has the lowest MAC address
C. The switch has spanning tree loop protection enabled
D. The switch has the fastest uplink port

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:
Explanation: In STP all switches send BPDUs (Bridge Protocol Data Unit) which contain a priority and the BID (Bridge ID).
The BID is 8 bytes long. 6 bytes is used for the MAC address of the bridge. 12 bits is used to indicate the VLAN, this is called extended system ID. 4 bits are used to set the priority. Lower priority means it is preferred compared to a higher. The priority is set in multiples of 4096.
If there is a tie in priority then the lowest MAC address will determine which bridge becomes the root.

QUESTION 168
An organization is trying to decide which type of access control is most appropriate for the network. The current access control approach is too complex and requires significant overhead. Management would like to simplify the access control and provide user with the ability to determine what permissions should be applied to files, document, and directories. The access control method that BEST satisfies these objectives is:

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

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 169
While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack. Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Select two)

A. Minimum complexity
B. Maximum age limit
C. Maximum length
D. Minimum length
E. Minimum age limit
F. Minimum re-use limit

Correct Answer: AD
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 170
A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computers without exception. Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?

A. Deploy antivirus software and configure it to detect and remove pirated software
B. Configure the firewall to prevent the downloading of executable files
C. Create an application whitelist and use OS controls to enforce it
D. Prevent users from running as administrator so they cannot install software.

Correct Answer: C
Section: 4. Application, Data, and Host Security

Explanation

Explanation/Reference:

QUESTION 171
A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility. Which of the following configuration commands should be implemented to enforce this requirement?

A. LDAP server 10.55.199.3
B. CN=company, CN=com, OU=netadmin, DC=192.32.10.233
C. SYSLOG SERVER 172.16.23.50
D. TACACS+ server 192.168.1.100

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 172
A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert. Which of the following methods has MOST likely been used?

A. Cryptography
B. Time of check/time of use
C. Man in the middle
D. Covert timing
E. Steganography

Correct Answer: E
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 173
An attacker captures the encrypted communication between two parties for a week, but is unable to decrypt the messages. The attacker then compromises the session key during one exchange and successfully compromises a single message. The attacker plans to use this key to decrypt previously captured and future communications, but is unable to. This is because the encryption scheme in use adheres to:

A. Asymmetric encryption
B. Out-of-band key exchange
C. Perfect forward secrecy
D. Secure key escrow

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

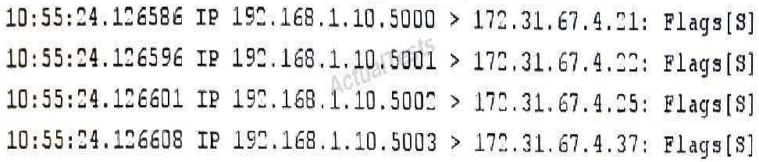
QUESTION 174
Many employees are receiving email messages similar to the one shown below:
From IT department
To employee
Subject email quota exceeded
Pease click on the following link http:www.website.info/email.php?quota=1Gb and provide your username and password to increase your email quota. Upon reviewing other similar emails, the security administrator realized that all the phishing URLs have the following common elements; they all use HTTP, they all come from .info domains, and they all contain the same URI.
Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?

A. BLOCK http://www.*.info/"
B. DROP http://"website.info/email.php?*
C. Redirect http://www,*. Info/email.php?quota=*TOhttp://company.com/corporate_polict.html
D. DENY http://*.info/email.php?quota=1Gb

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 175
A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:



```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags[S]
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags[S]
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags[S]
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags[S]
```

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

A. DENY TCO From ANY to 172.31.64.4
B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0
D. Deny TCP from 192.168.1.10 to 172.31.67.4

Correct Answer: C
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 176
The IT department needs to prevent users from installing untested applications. Which of the following would provide the BEST solution?

A. Job rotation
B. Least privilege
C. Account lockout
D. Antivirus

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 177

An attack that is using interference as its main attack to impede network traffic is which of the following?

A. Introducing too much data to a targets memory allocation
B. Utilizing a previously unknown security flaw against the target
C. Using a similar wireless configuration of a nearby network
D. Inundating a target system with SYN requests

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 178
An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys. Which of the following algorithms is appropriate for securing the key exchange?

A. DES
B. Blowfish
C. DSA
D. Diffie-Hellman
E. 3DES

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 179
Ann, a college professor, was recently reprimanded for posting disparaging remarks regarding her coworkers on a web site. Ann stated that she was not aware that the public was able to view her remakes. Which of the following security-related training could have made Ann aware of the repercussions of her actions?

A. Data Labeling and disposal
B. Use of social networking
C. Use of P2P networking

D. Role-based training

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 180
During a recent audit, it was discovered that many services and desktops were missing security patches. Which of the following BEST describes the assessment that was performed to discover this issue?

A. Network mapping
B. Vulnerability scan
C. Port Scan
D. Protocol analysis

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 181
When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

A. RC4
B. MD5
C. HMAC
D. SHA

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 182
The administrator installs database software to encrypt each field as it is written to disk. Which of the following describes the encrypted data?

A. In-transit
B. In-use
C. Embedded
D. At-rest

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 183
Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

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

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 184
A network technician is trying to determine the source of an ongoing network based attack. Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?

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

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 185
The security administrator has noticed cars parking just outside of the building fence line. Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Select TWO)

A. Create a honeynet
B. Reduce beacon rate
C. Add false SSIDs
D. Change antenna placement
E. Adjust power level controls
F. Implement a warning banner

Correct Answer: DE
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 186
A security administrator suspects that data on a server has been exfiltrated as a result of unauthorized remote access. Which of the following would assist the administrator in confirming the suspicions? (Select TWO)

A. Networking access control
B. DLP alerts
C. Log analysis
D. File integrity monitoring
E. Host firewall rules

Correct Answer: BC
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 187
A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated. Which of the following options will provide the best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

A. Put the VoIP network into a different VLAN than the existing data network.
B. Upgrade the edge switches from 10/100/1000 to improve network speed
C. Physically separate the VoIP phones from the data network
D. Implement flood guards on the data network

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 188
A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network. How could he access the server using RDP on a port other than the typical registered port for the RDP protocol?

A. TLS
B. MPLS
C. SCP
D. SSH

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 189
Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

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

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 190
Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate- based authentication with its users. The company uses SSL-inspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication. Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?

A. Use of OATH between the user and the service and attestation from the company domain
B. Use of active directory federation between the company and the cloud-based service
C. Use of smartcards that store x.509 keys, signed by a global CA
D. Use of a third-party, SAML-based authentication service for attestation

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 191

Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stakeholders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it. Which of the following BEST describes the current software development phase?

A. The system integration phase of the SDLC
B. The system analysis phase of SSDSLC
C. The system design phase of the SDLC
D. The system development phase of the SDLC

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 192
A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided from the role-based authentication system in use by the company. The situation can be identified for future mitigation as which of the following?

A. Job rotation
B. Logging failure
C. Lack of training
D. Insider threat

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 193
A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system. Which of the following methods should the security administrator select the best balances security and efficiency?

A. Temporarily permit outbound internet access for the pacs so desktop sharing can be set up
B. Have the external vendor come onsite and provide access to the PACS directly
C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing
D. Set up a web conference on the administrator's pc; then remotely connect to the pacs

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 194
A datacenter manager has been asked to prioritize critical system recovery priorities. Which of the following is the MOST critical for immediate recovery?

A. Communications software
B. Operating system software
C. Weekly summary reports to management
D. Financial and production software

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:
Answer:

QUESTION 195
Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select Two)

A. SQL injection
B. Session hijacking
C. Cross-site scripting
D. Locally shared objects
E. LDAP injection

Correct Answer: BD
Section: 4. Application, Data, and Host Security

Explanation

Explanation/Reference:
Explanation: Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session--sometimes also called a session key -- to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server.
Local shared objects (LSOs), commonly called Flash cookies (due to their similarities with HTTP cookies), are pieces of data that websites which use Adobe Flash may store on a user's computer. Flash cookies, which can be stored or retrieved whenever a user accesses a page containing a Flash application, are a form of local storage. Similar to that of cookies, they can be used to store user preferences, save data from Flash games, or to track users' Internet activity. LSOs have been criticised as a breach of browser security, but there are browser settings and addons to limit the duration of their storage.

QUESTION 196
When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

A. On the client
B. Using database stored procedures
C. On the application server
D. Using HTTPS

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 197
Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?

A. Egress traffic is more important than ingress traffic for malware prevention
B. To rebalance the amount of outbound traffic and inbound traffic
C. Outbound traffic could be communicating to known botnet sources
D. To prevent DDoS attacks originating from external network

Correct Answer: C
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 198
The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts. Which of the following controls should be implemented to curtail this activity?

A. Password Reuse
B. Password complexity
C. Password History
D. Password Minimum age

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

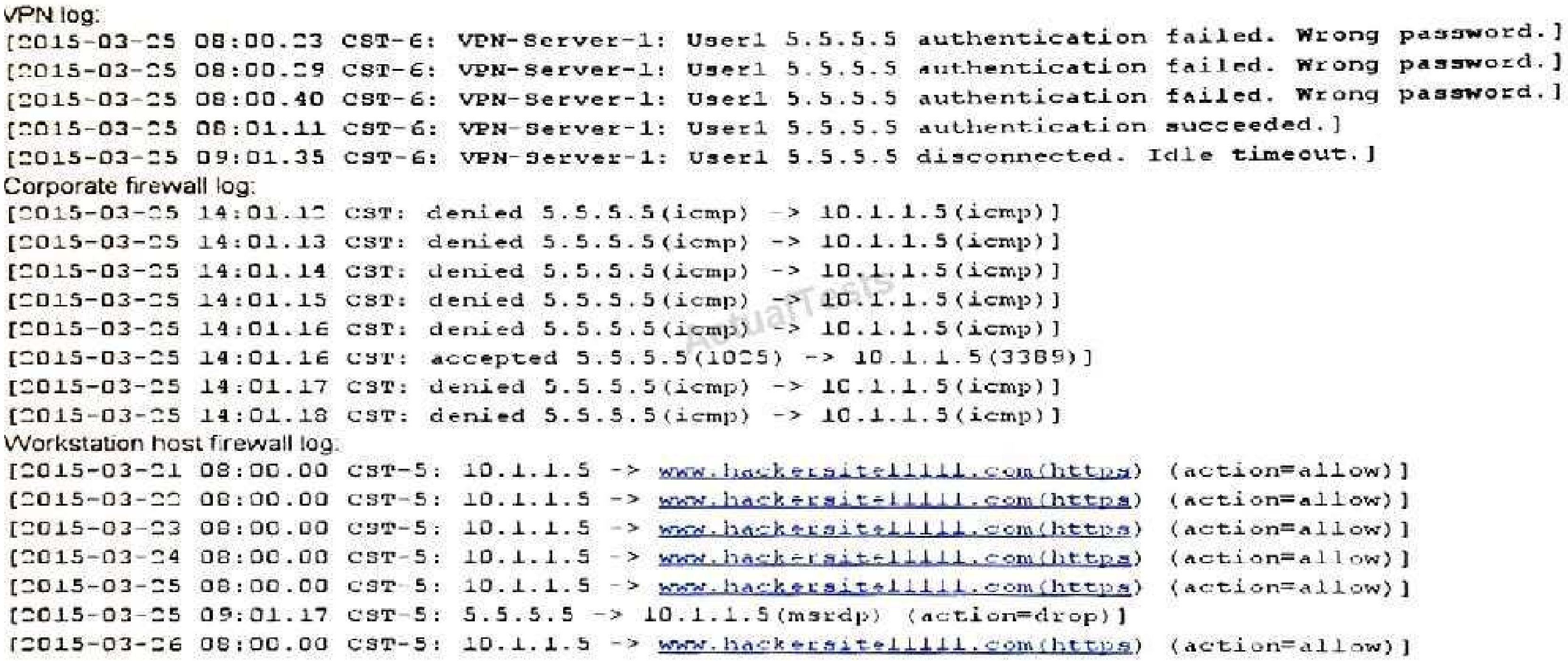
QUESTION 199
Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

A. Block level encryption
B. SAML authentication
C. Transport encryption
D. Multifactor authentication
E. Predefined challenge questions
F. Hashing

Correct Answer: BD
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 200
A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.



VPN log:

```
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
```

Corporate firewall log:

```
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
```

Workstation host firewall log:

```
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
[2015-03-23 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp)  (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https)  (action=allow)]
```

Which of the following is preventing the remote user from being able to access the workstation?

A. Network latency is causing remote desktop service request to time out
B. User1 has been locked out due to too many failed passwords
C. Lack of network time synchronization is causing authentication mismatches
D. The workstation has been compromised and is accessing known malware sites
E. The workstation host firewall is not allowing remote desktop connections

Correct Answer: E
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 201
During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem best be revisited?

A. Reporting
B. Preparation
C. Mitigation
D. Lessons learned

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 202
During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall. Which of the following will the audit team most l likely recommend during the audit out brief?

A. Discretionary access control for the firewall team
B. Separation of duties policy for the firewall team
C. Least privilege for the firewall team
D. Mandatory access control for the firewall team

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 203
Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

A. NAC
B. VLAN
C. DMZ

D. Subnet

Correct Answer: C
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 204
An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server. Which of the following will most likely fix the uploading issue for the users?

A. Create an ACL to allow the FTP service write access to user directories
B. Set the Boolean selinux value to allow FTP home directory uploads
C. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
D. Configure the FTP daemon to utilize PAM authentication pass through user permissions

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:
Explanation: SELinux doesn't allow your httpd daemon to talk to the LDAP server on the same machine. You need to be able to authenticate against LDAP. You know that the booleans which can be of interest to you contain the word httpd: setsebool -P httpd_can_network_connect on

QUESTION 205
An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity. Which of the following actions will help detect attacker attempts to further alter log files?

A. Enable verbose system logging
B. Change the permissions on the user's home directory
C. Implement remote syslog
D. Set the bash_history log file to "read only"

Correct Answer: C
Section: 4. Application, Data, and Host Security

Explanation

Explanation/Reference:

QUESTION 206
A global gaming console manufacturer is launching a new gaming platform to its customers. Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

A. Firmware version control
B. Manual software upgrades
C. Vulnerability scanning
D. Automatic updates
E. Network segmentation
F. Application firewalls

Correct Answer: AD
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 207
An audit has revealed that database administrators are also responsible for auditing database changes and backup logs. Which of the following access control methodologies would BEST mitigate this concern?

A. Time of day restrictions
B. Principle of least privilege
C. Role-based access control
D. Separation of duties

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 208
Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications.
Which of the following best describes what she will do?

A. Enter random or invalid data into the application in an attempt to cause it to fault
B. Work with the developers to eliminate horizontal privilege escalation opportunities
C. Test the applications for the existence of built-in- back doors left by the developers
D. Hash the application to verify it won't cause a false positive on the HIPS.

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 209
Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop. Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's laptop directly?

A. full-disk encryption
B. Host-based firewall
C. Current antivirus definitions
D. Latest OS updates

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 210
An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times. Which of the following describes this type of attack?

A. Integer overflow attack
B. Smurf attack
C. Replay attack

D. Buffer overflow attack
E. Cross-site scripting attack

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 211
An organization is moving its human resources system to a cloud services provider. The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords. Which of the following options meets all of these requirements?

A. Two-factor authentication
B. Account and password synchronization
C. Smartcards with PINs
D. Federated authentication

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 212
The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate servers at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?

A. Implement deduplication at the network level between the two locations
B. Implement deduplication on the storage array to reduce the amount of drive space needed
C. Implement deduplication on the server storage to reduce the data backed up
D. Implement deduplication on both the local and remote servers

Correct Answer: D
Section: 4. Application, Data, and Host Security

Explanation

Explanation/Reference:

QUESTION 213
A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results. Which of the following is the best method for collecting this information?

A. Set up the scanning system's firewall to permit and log all outbound connections
B. Use a protocol analyzer to log all pertinent network traffic
C. Configure network flow data logging on all scanning system
D. Enable debug level logging on the scanning system and all scanning tools used.

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 214
Which of the following best describes the initial processing phase used in mobile device forensics?

A. The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device
B. The removable data storage cards should be processed first to prevent data alteration when examining the mobile device
C. The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again
D. The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 215
Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain \. Which of the following tools would aid her to decipher the network traffic?

A. Vulnerability Scanner
B. Nmap
C. netstat
D. Packet Analyzer

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 216
An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?

A. Find two identical messages with different hashes
B. Find two identical messages with the same hash
C. Find a common hash between two specific messages
D. Find a common hash between a specific message and a random message

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 217
The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administrator has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled. Which of the following would further obscure the presence of the wireless network?

A. Upgrade the encryption to WPA or WPA2
B. Create a non-zero length SSID for the wireless router
C. Reroute wireless users to a honeypot
D. Disable responses to a broadcast probe request

Correct Answer: D

Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:
Explanation: When "SSID broadcast" is disabled you can:
1) Completely disable the sending of beacons
2) Disable probe responses except in cases where the probe request was explicitly addressed to the correct SSID (ignore broadcast probe requests to the wildcard SSID) and was from an authorized client (apply MAC Address filtering), and even send a null SSID in the probe responses to those.

QUESTION 218
Which of the following should be used to implement voice encryption?

A. SSLv3
B. VDSL
C. SRTP
D. VoIP

Correct Answer: C
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 219
During an application design, the development team specifics a LDAP module for single sign-on communication with the company's access control database. This is an example of which of the following?

A. Application control
B. Data in-transit
C. Identification
D. Authentication

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 220
After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

A. Time-of-day restrictions
B. Change management
C. Periodic auditing of user credentials
D. User rights and permission review

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 221
A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

A. Performance and service delivery metrics
B. Backups are being performed and tested
C. Data ownership is being maintained and audited
D. Risk awareness is being adhered to and enforced

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 222
Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

A. Calculate the ALE
B. Calculate the ARO
C. Calculate the MTBF
D. Calculate the TCO

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 223
A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list. Which of the following BEST describes this type of IDS?

A. Signature based
B. Heuristic
C. Anomaly-based
D. Behavior-based

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 224
New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority. In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?

A. Fail safe
B. Fault tolerance
C. Fail secure
D. Redundancy

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 225
A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Names (SAN) attribute of a certificate?

A. It can protect multiple domains
B. It provides extended site validation
C. It does not require a trusted certificate authority
D. It protects unlimited subdomains

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 226
After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition. Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO)

A. Monitor VPN client access
B. Reduce failed login settings
C. Develop and implement updated access control policies
D. Review and address invalid login attempts
E. Increase password complexity requirements
F. Assess and eliminate inactive accounts

Correct Answer: CF
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 227
A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle. Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle?

A. Architecture review
B. Risk assessment
C. Protocol analysis
D. Code review

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 228
A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts. Which of the following subnets would BEST meet the requirements?

A. 192.168.0.16 255.25.255.248
B. 192.168.0.16/28
C. 192.168.1.50 255.255.25.240
D. 192.168.2.32/27

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 229
A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have cause many executives in the company to travel with mini tablet devices instead of laptops. These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network. Which of the following should be implemented in order to meet the security policy requirements?

A. Virtual desktop infrastructure (VDI)
B. WS-security and geo-fencing
C. A hardware security module (HSM)
D. RFID tagging system

E. MDM software
F. Security Requirements Traceability Matrix (SRTM)

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 230
The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN. Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance
C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 231
A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network. Which of the following security measures did the technician MOST likely implement to cause this Scenario?

A. Deactivation of SSID broadcast
B. Reduction of WAP signal output power
C. Activation of 802.1X with RADIUS
D. Implementation of MAC filtering
E. Beacon interval was decreased

Correct Answer: A

Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 232
A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production. Which of the following would correct the deficiencies?

A. Mandatory access controls
B. Disable remote login
C. Host hardening
D. Disabling services

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 233
Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field. Which of the following has the application programmer failed to implement?

A. Revision control system
B. Client side exception handling
C. Server side validation
D. Server hardening

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 234
An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware the attacker is provided with access to the infected machine. Which of the following is being described?

A. Zero-day exploit
B. Remote code execution
C. Session hijacking
D. Command injection

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 235
A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine. Which of the following can be implemented to reduce the likelihood of this attack going undetected?

A. Password complexity rules
B. Continuous monitoring
C. User access reviews
D. Account lockout policies

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 236
A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening. In order to implement a true separation of duties approach the bank could:

A. Require the use of two different passwords held by two different individuals to open an account
B. Administer account creation on a role based access control approach
C. Require all new accounts to be handled by someone else other than a teller since they have different duties
D. Administer account creation on a rule based access control approach

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 237
A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day. Which of the following could the security administrator implement to reduce the risk associated with the finding?

A. Implement a clean desk policy
B. Security training to prevent shoulder surfing
C. Enable group policy based screensaver timeouts
D. Install privacy screens on monitors

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 238
Company policy requires the use if passphrases instead if passwords. Which of the following technical controls MUST be in place in order to promote the use of passphrases?

A. Reuse
B. Length
C. History
D. Complexity

Correct Answer: B

Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 239
During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could best prevent this from occurring again?

A. Credential management
B. Group policy management
C. Acceptable use policy
D. Account expiration policy

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 240
Which of the following should identify critical systems and components?

A. MOU
B. BPA
C. ITCP
D. BCP

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 241
Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

A. Logic bomb
B. Trojan
C. Scareware
D. Ransomware

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 242
A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account. This is an example of which of the following attacks?

A. SQL injection
B. Header manipulation
C. Cross-site scripting
D. Flash cookie exploitation

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:
Explanation: Say you set your browser to fully trust your bank's site and allow it to run scripts in your browser.
On the other hand, you deny that privilege from the rest of the sites you visit.
If the bank's site is vulnerable to XSS, when you click on a malformed URL that was presented to you at hacker.com, you will be redirected to your banks site (which you previously granted scripting rights) and the malicious script written by someone at hacker.com will run. XSS in that manner is an easy way to run scripts on cautious clients that allow only very specific sites to send them scripts.

QUESTION 243
Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures. Which of the following should be implemented to correct this issue?

A. Decrease the room temperature
B. Increase humidity in the room

C. Utilize better hot/cold aisle configurations
D. Implement EMI shielding

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 244
A portable data storage device has been determined to have malicious firmware. Which of the following is the BEST course of action to ensure data confidentiality?

A. Format the device
B. Re-image the device
C. Perform virus scan in the device
D. Physically destroy the device

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 245
A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable. Which of the following MUST be implemented to support this requirement?

A. CSR
B. OCSP
C. CRL
D. SSH

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 246
A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients. Which of the following is being used?

A. Gray box vulnerability testing
B. Passive scan
C. Credentialed scan
D. Bypassing security controls

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:
Explanation: Credentialed scan: Here's an analogy: traditional vulnerability scanning is like a mechanic evaluating a car just by looking at the outside and listening to the motor run. It's useful but there is so much more information available by looking under the hood and plugging into the on-board diagnostics. That level of insight and internal perspective is what credentialed scanning lends to a security assessment.

QUESTION 247
The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws. Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers
B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location
C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations
D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 248
While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy. Which of the following tool or technology would work BEST for obtaining more information on this traffic?

A. Firewall logs
B. IDS logs
C. Increased spam filtering
D. Protocol analyzer

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 249
A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer. Which of the following is the BEST way to accomplish this?

A. Enforce authentication for network devices
B. Configure the phones on one VLAN, and computers on another
C. Enable and configure port channels
D. Make users sign an Acceptable use Agreement

Correct Answer: A
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 250
An administrator has concerns regarding the traveling sales team who works primarily from smart phones. Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

A. Enable screensaver locks when the phones are not in use to prevent unauthorized access
B. Configure the smart phones so that the stored data can be destroyed from a centralized location
C. Configure the smart phones so that all data is saved to removable media and kept separate from the device
D. Enable GPS tracking on all smart phones so that they can be quickly located and recovered

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 251
A user of the wireless network is unable to gain access to the network. The symptoms are:
1.) Unable to connect to both internal and Internet resources 2.) The wireless icon shows connectivity but has no network access The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate. Which of the following is the MOST likely cause of the connectivity issues?

A. The wireless signal is not strong enough
B. A remote DDoS attack against the RADIUS server is taking place
C. The user's laptop only supports WPA and WEP
D. The DHCP scope is full
E. The dynamic encryption key did not update while the user was offline

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 252
A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls. Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

A. Password complexity policies
B. Hardware tokens
C. Biometric systems

D. Role-based permissions
E. One time passwords
F. Separation of duties
G. Multifactor authentication
H. Single sign-on
I. Least privilege

Correct Answer: DFI
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 253
A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting without the knowledge of the user. Which of the following mobile device capabilities should the user disable to achieve the stated goal?

A. Device access control
B. Location based services
C. Application control
D. Geo-Tagging

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 254
A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile date first. Which of the following is the correct order in which Joe should collect the data?

A. CPU cache, paging/swap files, RAM, remote logging data
B. RAM, CPU cache. Remote logging data, paging/swap files
C. Paging/swap files, CPU cache, RAM, remote logging data

D. CPU cache, RAM, paging/swap files, remote logging data

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 255
An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP. Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

A. Use a honeypot
B. Disable unnecessary services
C. Implement transport layer security
D. Increase application event logging

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:
:

QUESTION 256
A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another. Which of the following should the security administrator do to rectify this issue?

A. Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
B. Recommend classifying each application into like security groups and segmenting the groups from one another
C. Recommend segmenting each application, as it is the most secure approach
D. Recommend that only applications with minimal security features should be segmented to protect them

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 257
A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code. Which of the following assessment techniques is BEST described in the analyst's report?

A. Architecture evaluation
B. Baseline reporting
C. Whitebox testing
D. Peer review

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 258
An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are. The controls used by the receptionist are in place to prevent which of the following types of attacks?

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

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 259
A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The

assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test. Which of the following has the administrator been tasked to perform?

A. Risk transference
B. Penetration test
C. Threat assessment
D. Vulnerability assessment

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 260
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

A. Transitive access
B. Spoofing
C. Man-in-the-middle
D. Replay

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 261
Which of the following use the SSH protocol? (Choose two).

A. Stelnet
B. SCP
C. SNMP

D. FTPS
E. SSL
F. SFTP

Correct Answer: BF
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 262
A security administrator is developing training for corporate users on basic security principles for personal email accounts. Which of the following should be mentioned as the MOST secure way for password recovery?

A. Utilizing a single question for password recovery
B. Sending a PIN to a smartphone through text message
C. Utilizing CAPTCHA to avoid brute force attacks
D. Use a different e-mail address to recover password

Correct Answer: B
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 263
A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability. In order to prevent similar situations in the future, the company should improve which of the following?

A. Change management procedures
B. Job rotation policies
C. Incident response management
D. Least privilege access controls

Correct Answer: A
Section: 2. Compliance and Operational security

Explanation

Explanation/Reference:

QUESTION 264
A computer on a company network was infected with a zero-day exploit after an employee accidentally opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidentally opened it. Which of the following should be done to prevent this scenario from occurring again in the future?

A. Install host-based firewalls on all computers that have an email client installed
B. Set the email program default to open messages in plain text
C. Install end-point protection on all computers that access web email
D. Create new email spam filters to delete all messages from that sender

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 265
A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage. Which of the following should be implemented?

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

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 266
An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection. Which of the following AES

modes of operation would meet this integrity-only requirement?

A. GMAC
B. PCBC
C. CBC
D. GCM
E. CFB

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:
Explanation: Galois/Counter Mode (GCM) is a mode of operation for symmetric key cryptographic block ciphers that has been widely adopted because of its efficiency and performance. GCM throughput rates for state of the art, high speed communication channels can be achieved with reasonable hardware resources. The operation is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality.
GCM is defined for block ciphers with a block size of 128 bits.
Galois Message Authentication Code (GMAC) is an authentication-only variant of the GCM which can be used as an incremental message authentication code. Both GCM and GMAC can accept initialization vectors of arbitrary length.

QUESTION 267
The chief security officer (CS0) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs. Which of the following is the best solution for the network administrator to secure each internal website?

A. Use certificates signed by the company CA
B. Use a signing certificate as a wild card certificate
C. Use certificates signed by a public ca
D. Use a self-signed certificate on each internal server

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 268
A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active

user base. Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

A. Peer review
B. Component testing
C. Penetration testing
D. Vulnerability testing

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 269
An organization uses a Kerberos-based LDAP service for network authentication. The service is also utilized by internal web applications. Finally, access to terminal applications is achieved using the same authentication method by joining the legacy system to the Kerberos realm. The company is using Kerberos to achieve which of the following?

A. Trusted operating system
B. Rule-based access control
C. Single sign-on
D. Mandatory access control

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 270
A new help desk employee at a cloud services provider receives a call from a customer. The customer is unable to log into the provider's web application database. The help desk employee is unable to find the customer's user account in the directory services console, but see the customer information in the application database. The application does nit appear to have any fields for a password. The customer then remembers the password and is able to log in. The help desk employee still does not see the user account in directory services. Which of the following is the MOST likely ?

A. A bug has been discovered in the application
B. An application uses a weak encryption cipher
C. A federated authentication model is being used.
D. The application uses single sign on.

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 271
A company wants to ensure that all software executing on a corporate server have been authorized to do so by a central control point. Which of the following can be implemented to enable such a control?

A. Digital signatures
B. Mandatory access control
C. Session keys
D. Non repudiation

Correct Answer: A
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 272
A security engineer wants to communicate securely with a third party via email using PGP. Which of the following should the engineer send to the third party to securely encrypt email replies?

A. Public key

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

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 273
A network administrator recently implemented two caching proxy servers on the network. How can the administrator BEST aggregate the log files from the proxy servers?

A.
B. Configure each proxy server to write to log files stored locally
C. Configure both proxy servers to log to a network share
D. Configure both proxy servers to log to a centralized switch

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 274
Which of the following attacks takes advantage of user provided input to inject executable binary code into a running program?

A. SQL injection
B. Session hijacking
C. Heder manipulation
D. Buffer overflow

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 275
A user contacts the help desk after being unable to log in to the corporate website. The user can log into the site from another computer in the next office, but not from the PC. The user's PC was able to connect earlier in the day. The help desk has the user restart the NTP service. Afterwards, the user is able to log into the website. The MOST likely reason for the initial failure was that the website was configured to use which of the following authentication mechanisms?

A. Secure LDAP
B. RADIUS
C. NTLMv2
D. Kerberos

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 276
A security engineer notices that unknown devices are connecting to the company's wireless network and trying to access the database server. The wireless access point is configured with WPA for encryption and the network administrator setup a 8 digit pin for easy setup to the wireless access point. Which of the following is the MOST likely type of attack?

A. IV attack
B. WPS attack
C. Bluesnarfing attack
D. Replay attack

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 277
An employee connects a wireless access point to the only jack in the conference room to provide Internet access during a movie. The access point is configured to secure its users with WPA2-TKIP. A malicious user is able to intercept clear text HTTP communication between the meeting attendees and the Internet. Which of

the following is the reason the malicious user is able to intercept and see clear text communications?

A. The malicious user is running a wireless sniffer
B. The wireless access point is broadcasting the SSID
C. The malicious user is able to capture the wired communication
D. The meeting attendees are using unencrypted hard drives

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 278
In the course of troubleshooting wireless issues from users, a technician discovers that users are connecting to their home SSIDs while at work. The technician scans detects none of those SSIDs. The technician eventually discovers a rogue access point that spoofs any SSID that a client requests. Which of the following allows wireless use while mitigating this type of attack?

A. Configure the device to verify access point MAC addresses
B. Disable automatic connection to unknown SSIDs
C. Only connect to trusted wireless networks
D. Enable MAC filtering on the wireless access point

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 279
Several users require administrative access for software compatibility reasons. Over time, these users have made several changes to important system settings. Which of the following is the BEST course of action to ensure the system settings are properly enforced?

A. Require users to run under a standard user account
B. Use centralized group policy to configure the settings
C. Conduct user access reviews to determine appropriate privileges
D. Implement an application whitelist throughout the company

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 280
A media company would like to securely stream live video feeds over the Internet to clients. The security administrator suggests that the video feed is encrypted in transport and configures the web server to prefer ciphers suited to the live video feeds. Which of the following cipher suites should the administrator implement on the web server to minimize the computational and performance overhead of delivering live feeds?

A. ECDHE-RSA-RC4-SHA
B. DHE-DSA-DES-CBC-SHA
C. ECDHE-RSA-AES-CBC-SHA
D. ECDHE-RSA-AES256-CBC-SHA

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 281
A security administrator is having continued issues with malware variants infecting systems infecting systems and encrypting several types of files. The malware uses a document macro to create a randomly named executable that downloads the encrypted payload of the malware. Once downloaded, the malware searches all drives, creates and HTML file with the decryption instructions in the directory, and then proceeds to encrypt the target files. Which of the following actions would BEST interrupt the malware before it encrypts other files while minimizing the adverse impacts to the users?

A. Block execution of documents with macros
B. Block addition of documents with macros
C. Block the creation of the HTML of the HTML document on the local system
D. Block running external files from within documents.

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 282
Am organization decides to implement a BYOD policy but wants to ensure they address requirements associated with any legal investigations and controls needed to comply with the analysis and recreation of an incident. This concern is also known as which of the following?

A. Data ownership
B. Forensics
C. Chain of custody
D. Acceptable use

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 283
A security administrator is called to troubleshoot a computer infection. The computer's software correctly identified the malware and flagged it to the central management console; however the malicious payload was still executed. Which of the following can cause this scenario?

A. The payload hash did not match known malware
B. The antivirus is running an older virus definition
C. The computer is running an IDS
D. The payload is a zero-day attack

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 284
The CEO for company A has asked the security engineer to design a PKI for company A. The CEO has asked that it allow company A users to send signed and encrypted emails to company B. The users from company B must have an inherent trust in certificates from company A, because the security policy of company B disallows adding of new CAs to their trusted root container. Which of the following is the BEST solution?

A. Request email certificates for the users of company A from the PKI of company B.
B. Build a new CA within the boundary of company A and issue email certificates to the users
C. Establish a sub CA of company B's root CA to issue email certificates to the users.
D. Procure the services of a common Internet root CA to issue email certificates to the users.

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 285
A university police department is housed on the first floor of a student dormitory. Which of the following would prevent students from using ARP spoofing attacks against computers at the police department?

A. Enable proxy ARP on router
B. Private network addresses
C. Separate Layer 2 VLANs
D. Disable SSID broadcast

Correct Answer: C
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 286
Ann is preparing a presentation for management to highlight some of the issues the security department is facing trying to integrate the organizations BYOD policy. Highest of her list is the transparency of network resources. The DAC environment includes several departments including payroll, HR, IT, and Management. However, the small company's structure has never been updated to incorporate these departments. The organization continued to add users based on the same original general user profile. Which of the following security methods should Ann suggest to management to BEST fix this issue?

A. Two-factor authentication
B. Mandatory access control
C. Application firewall
D. Network segmentation

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 287
Which of the following allows an application to securely authenticate a user by receiving credentials from a remote web domain?

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

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 288
A security analyst has been asked to perform penetration testing against a web application being deployed for the first time. When performing the test the application stops responding and returns an error referring to failed database connections. Upon further investigation, the analyst finds the database server was inundated with commits which exhausted available space on the volume. Which of the following has been performed against the database server?

A. DoS
B. SQL injection
C. SYN flood
D. DDoS
E. Cross-site scripting

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 289
An application developer has coded a new application and needs to test all input fields. Which of the following should be used to fulfill this requirement?

A. Application hardening
B. Server-side validation
C. Input validation
D. Fuzzing

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 290
A company is implementing a system to transfer direct deposit to a financial institution. One of the requirements is that the institution must be certain that the deposit amounts within the file have not been charged. Which of the following should be used to meet requirement?

A. Key escrow
B. Perfect forward secrecy
C. Transport encryption
D. Digital signatures
E. File encryption

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 291
A company uses PKI certificates stored on a smart chip enabled badge. The badge is used for a small number of devices that connect to a wireless network. A user reported that their badge was stolen. Which of the following could the security administrator implement to prevent the stolen badge from being used to compromise the wireless network?

A. Asset tracking
B. Honeynet
C. Strong PSK
D. MAC filtering

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 292
A security engineer is monitoring suspicious traffic from an internal endpoint to a malicious landing page of an external entity. The internal endpoint is configured using a limited account, is fully patched to current standards, and has current antivirus signatures. No alerts have been received involving this endpoint. The security engineer finds malicious code on the endpoint during a forensic analysis. Which of the following MOST likely explains this occurrence?

A. The external entity breached the IDS
B. The antivirus engine was evaded
C. The DLP did not detect the malicious code
D. The endpoint was running on a hypervisor

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 293
The security administrator for a growing company is concerned about the increasing prevalence of personal devices connected to the corporate WLAN. Which of the following actions should the administrator take FIRST to address this concern?

A. Implement RADIUS to centrally manage access to the corporate network over WiFi.
B. Request that senior management support the development of a policy that addresses personal devices.
C. Establish a guest-access wireless network and request that employees use the guest network.
D. Distribute a memo addressing the security risks associated with the use of personally-owned devices on the corporate WLAN.

Correct Answer: B

Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 294
Upper management wishes to implement a policy forbidding the use of personal devices on the corporate network. Which of the following is the primary reason why such a policy would be put in place?

A. Devices connected to the corporate network become legally bound to company SLAs.
B. Personally owned devices might not be subjected to the same security controls as corporate devices.
C. Personal devices might contain personally owned media that could leave company open to licensing issues.
D. Employees might not be properly trained to utilize the device on the corporate network.

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 295
A company's security analyst is investigating the suspected compromise of the company's intranet web server. The compromise occurred at a time when no users were logged into the domain. Which of the following is MOST likely to have prevented the attack from a new machine introduced to the corporate network?

A. Domain log review
B. 802.1x
C. NIDS
D. Rogue detection

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 296

Following a site survey for an upcoming 5GHz wireless network implementation, the project manager determines that several areas of the facility receive inadequate coverage due to the use of vertical antennas on all access points. Which of the following activities would be MOST likely to remediate the issue without changing the current access point layout in the facility?

A. Convert all access points to models operating at 2.4GHz.
B. Install antennas with lower front-to-back ratios to narrow the focus of coverage as needed.
C. Reorient the existing antennas in horizontal configuration.
D. Install unidirectional antennas to focus coverage where needed.

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:
:

QUESTION 297
A company has implemented a public facing authentication system which uses PKI and extended attributes to allow third party web based application integration. Which of the following is this an example of? (Select THREE)

A. Federation
B. Two-factor authentication
C. Transitive trust
D. Trusted OS
E. Single sign-on
F. TOTP
G. Mandatory Access Control

Correct Answer: ACE
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 298
A building engineer just installed a new environmental control system (ECS) for a room that is critical to the company's operation and needs the ability to manage and monitor the system from any part of the network. Which of the following should the security administrator utilize to minimize the attack surface and still allow the needed access?

A. Configure the ECS host-based firewall to block non-ECS application traffic
B. Create an encrypted connection between the ECS and the engineer's computer
C. Install a firewall that only allows traffic to the ECS from a single management and monitoring network
D. Implement an ACL that permits the necessary management and monitoring traffic

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 299
A single server hosts a sensitive SQL-based database and a web service containing static content. A few of the database fields need to be encrypted due to regulatory requirements. Which of the following would provide the BEST encryption solution for this particular server?

A. Individual file
B. Database
C. Full-disk
D. Record based

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 300
An increase in the number of wireless users on the 192.168.6.0/24 subnet has caused the DHCP pool to run out of addresses, which prevents users from accessing important network resources. Which of the following should the administrator do to correct this problem?

A. Decrease the subnet mask network bits.
B. Increase the dynamic ARP timeout.
C. Switch to static IP address assignment.
D. Increase the DHCP lease time.

Correct Answer: A

Section: 1. Network Security
Explanation

Explanation/Reference:
Answer:

QUESTION 301
A forensics analyst is tasked with identifying identical files on a hard drive. Due to the large number of files to be compared, the analyst must use an algorithm that is known to have the lowest collision rate. Which of the following should be selected?

A. MD5
B. RC4
C. SHA-128
D. AES-256

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:
Answer:

QUESTION 302
Ann, a network security engineer, is trying to harden her wireless network. Currently, users are able to connect any device to the wireless network as long as they authenticate with their network username and password. She is concerned that devices that are not company-issued may gain unauthorized access. Which of the following techniques would be BEST suited to remediate this vulnerability? (Select TWO).

A. Utilize a single service account, only known by IT, to authenticate all devices
B. Install separate access points for personal devices
C. Install an IPS to protect the network from rogue devices
D. Filter the MAC addresses of all unknown devices on the wireless controller
E. Configure the RADIUS server to authenticate via compute and user

Correct Answer: DE
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:
Answer:

QUESTION 303
A company wants to ensure that all software executing on a corporate server has been authorized to do so by a central control point. Which of the following can be implemented to enable such control.

A. Digital signatures
B. Mandatory access control
C. Session keys
D. Non-repudiation

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 304
A major breach occurred at an organization. The incident response team contained the breach and recovered from the incident. A number of things were wrong during the incident response process and now the team must discuss and correct these items. Which of the following parts of the incident response process is the team conducting?

A. Lessons learned
B. Damage and loss control
C. Tabletop exercise
D. Security awareness training

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 305
A network administrator recently implemented two caching proxy servers on the network. How can the network administrator BEST aggregate the log files for the proxy servers?

A. Configure both proxy servers to log to a syslog server.

B. Configure each proxy server to write to log files stored locally.
C. Configure both proxy servers to log to a network share.
D. Configure both proxy servers to log to a centralized switch.

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 306
A company utilizes a copier on the finance subnet. The security administrator is worried that the copier could have undisclosed vulnerabilities, as it has an embedded operating system that can not be maintained. Which of the following should the administrator do to reduce the attack surface of the copier?

A. Add an ACL to the switch that restricts network traffic to LPR packets
B. Install antivirus software on the copier and enable its host-based firewall
C. Update the copier drivers on the finance PCs and enable HIPS on the PCs
D. Create a new VLAN and separate the copier and finance department onto the new VLAN

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 307
A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resources. There cannot be a possibility of any equipment being damaged in the test. Which of the following has the administrator been tasked to perform?

A. Risk transference
B. Penetration test
C. Threat assessment
D. Vulnerability assessment

Correct Answer: D

Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 308
A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computer without exception. Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?

A. Deploy antivirus software and configure it to detect and remove pirated software.
B. Configure the firewall to prevent the downloading of executable files.
C. Create an application whitelist and use OS controls to enforce it.
D. Prevent users from running as administrator so they cannot install software.

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 309
Recently, the desktop support group has been performing a hardware refresh and has replaced numerous computers. An auditor discovered that a number of the new computers did not have the company's antivirus software installed on them. Which of the following could be utilized to notify the network support group when computers without the antivirus software are added to the network?

A. Network port protection
B. NAC
C. NIDS
D. MAC filtering

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 310
A database server has been compromised. A local user logged into the console and exploited a vulnerability caused by a missing operating system patch to get a system level command shell. Which of the following does this represent?

A. Zero-day exploit
B. Buffer overflow
C. SQL injection attack
D. Privilege escalation

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 311
Which of the following is important to reduce risk?

A. Separation of duties
B. Risk acceptance
C. Risk transference
D. Threat modeling

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 312
Two visitors connected their laptops to the wired internal network and immediately began consuming excessive amounts of bandwidth. Which of the following can the administrator implement to mitigate these type of issues in the future?

A. Port security
B. Flood guards
C. VLAN configuration
D. Loop protection

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 313
A UNIX server recently had restricted directories deleted as the result of an insider threat. The root account was used to delete the directories while logged on at the server console. There are five administrators that know the root password. Which of the following could BEST identify the administrator that removed the restricted directories?

A. DHCP logs
B. CCTV review
C. DNS logs
D. Network traffic

Correct Answer: B
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 314
A plant security officer is continually losing connection to two IP cameras that monitor several critical high voltage motors. Which of the following should the network administrator do to BEST ensure the availability of the IP camera connections?

A. Use a wireless bridge instead of the network cables
B. Replace patch cables with shielded cables
C. Change existing cables with optical cables
D. Add new conduit runs for the network cables

Correct Answer: C
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 315
A security administrator is implementing a new feature on the company extranet server to provide client access to track the status of products the company makes. Which of the following will use a configuration baseline to reduce cross-site scripting and cross-site request forgery on the new feature?

A. Web application firewall
B. Reverse proxy
C. Database activity monitor
D. Application hardening guidelines

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 316
An administrator learns that port 389 will soon be blocked by the internal firewall for security reasons. Which of the following should the administrator now use to maintain compatibility with most applications?

A. SMTPS
B. LDAPS
C. SAML
D. Kerberos

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 317
A security administrator suspects that an employee has altered some fields within a noSQL database. Which of the following should the security administrator do to confirm the suspicion and identify the employee?

A. Review the video of the employee's workstation.

B. Review the database access log files.no

C. Capture a system image of the entire server.

D. Generate file hashes of the database to compare to the last version.

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 318
A vulnerability in the underlying SSL/TLS library used by a web server has been announced. The vulnerability allows an attacker to access the web server's memory. Which of the following actions should be taken after the vulnerability is patched? (Select TWO).

A. Implement a web application firewall

B. Instruct users of the website to change their passwords

C. Replace the server's private key

D. Reissue the SSL certificate

E. Create a new recovery agent

F. Change the cipher order on the server

Correct Answer: CD
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 319
Which of the following is the MAIN purpose for incorporating a DMZ into the design of a network?

A. Incorporate a secure place to house print servers and other networking equipment.

B. Isolate a network segment where attackers can be fooled into exploiting fake resources.

C. Facilitate the creation of resources accessed by internal users in a secure manner.

D. Provide an isolate location for servers accessed from the intra and inter networks.

Correct Answer: D

Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 320
A security manager has noticed several unrecognized devices connecting to the company's internal wireless network. Only company-issued devices should be connected to the network. Which of the following controls should be implemented to prevent the unauthorized devices from connecting to the wireless network? (Select TWO).

A. MAC filtering
B. Create a separate wireless VLAN
C. Implement 802.11n
D. Enable WPA2
E. Configure DHCP reservations

Correct Answer: AD
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 321
A security administrator receives reports from various organizations that a system on the company network is port scanning hosts on various networks across the Internet. The administrator determines that the compromised system is a Linux host and notifies the owner that the system will be quarantined and isolated from the network. The system does not contain confidential data, and the root user was not compromised. The administrator would like to know how the system was compromised, what the attackers did, and what remnants the attackers may have left behind. Which of the following are the administrator's NEXT steps in the investigation? (Select TWO).

A. Reinstall the procps package in case system utilities were modified.
B. Look for recently modified files in user and tmp directories.
C. Switch SELinux to enforcing mode and reboot.
D. Monitor perimeter firewall for suspicious traffic from the system.
E. Check running processes and kernel modules.
F. Remove unnecessary accounts and services.

Correct Answer: BE

Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 322
A third party has been contracted to perform a remote penetration test of the DMZ network. The company has only provided the third party with the billing department contact information for final payment and a technical point of contact who will receive the penetration test results. Which of the following tests will be performed?

A. Gray Box
B. White Box
C. Black Box
D. False Positive

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 323
A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer. Which of the following is the BEST way to accomplish this?

A. Enforce authentication for network devices
B. Configure the phones on one VLAN, and computers on another
C. Enable and configure port channels
D. Make users sign an Acceptable Use Agreement

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 324
Which of the following is an active penetration testing method?

A. Searching the WHOIS database for administrator contact information
B. Running a port scanner against the target's network
C. War driving from a target's parking lot to footprint the wireless network
D. Calling the target's helpdesk, requesting a password reset

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 325
The Chief Security Officer (CSO) has issued a new policy that requires that all internal website be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs. Which of the following is the BEST solution for the network administrator to secure each internal website?

A. Use certificates signed by the company CA.
B. Use a signing certificate as a wild card certificate.
C. Use certificates signed by a public CA.
D. Use a self-signed certificate on each internal server

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 326
Which of the following BEST represents a security challenge faced primarily by organizations employing a mobility BYOD strategy?

A. Balancing between the security of personal information and the company's information sharing requirements.
B. Balancing between the assurance of individual privacy rights and the security of corporate data.
C. Balancing between device configuration enforcement and the management of cryptographic keys.
D. Balancing between the financial security of the company and the financial security of the user.

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 327
A business has set up a Customer Service kiosk within a shopping mall. The location will be staffed by an employee using a laptop during the mall business hours, but there are still concerns regarding the physical safety of the equipment after business hours. Which of the following controls would BEST address this security concern?

A. Host-based firewall
B. Cable locks
C. Locking cabinets
D. Surveillance video

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 328
Which of the following should be implemented to enforce the corporate policy requiring up-to-date antivirus and OS patches on all computers connecting to the network via VPN?

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

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 329
As their data set rapidly grows and changes, a company is experiencing availability problems with their database. The security manager recommends switching to a more scalable system with dynamic schemas. Which of the following would meet the security manager's requirements?

A. SSDs
B. NoSQL
C. MariaDB
D. RDBMS

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 330
A security administrator wishes to implement a secure method of file transfer when communicating with outside organizations. Which of the following protocols would BEST facilitate secure file transfers? (Select TWO).

A. SCP
B. TFTP
C. SNMP
D. FTP
E. SMTP
F. FTPS

Correct Answer: AF
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 331
During a trial for possession of illegal content, a defence attorney argues that several of the files on the forensic image may have been tampered with. How can a technician BEST disprove this argument?

A. Trace the chain-of-custody from the time of arrest until the time of trial
B. Have the forensic investigator undergo a polygraph examination
C. Take hashes from the suspect source drive, and compare them to hashes on the forensic image
D. Access the system logs on the forensic image, and see if any logins occurred after the suspect's arrest

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 332
A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify.

A. performance and service delivery metrics.
B. backups are being performed and tested.
C. data ownership is being maintained and audited.
D. risk awareness is being adhered to and enforced.

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 333
Joe, a user, wants to configure his work station to make certain that the certificate he receives when connecting to websites is still valid. Which of the following should Joe enable on his workstation to achieve this?

A. Certificate revocation
B. Key escrow
C. Registration authority
D. Digital signatures

Correct Answer: A

Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 334
A company hosts sites for multiple vendors and provides information to users globally. Which of the following is a critical security consideration in this environment?

A. Proxy servers to enforce a single access mechanism to the data warehouse
B. Firewalls to ensure that the data warehouse is not accessible to the Internet
C. Access controls to prevent users from accessing the entire data warehouse
D. Query protocols should use non-standard ports to protect user result-sets

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 335
A technician wants to verify the authenticity of the system files of a potentially compromised system. Which of the following can the technician use to verify if a system file was compromised? (Select TWO).

A. AES
B. PGP
C. SHA
D. MD5
E. ECDHE

Correct Answer: CD
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 336
A firewall administrator has been instructed to block common Microsoft file sharing ports due to a recent malware outbreak. Which of the following ports should be blocked by the firewall? (Select TWO).

A. TCP/137
B. UDP/137
C. TCP/139
D. UDP/139
E. TCP/443
F. UDP/443
G. TCP/445
H. UDP/445

Correct Answer: CG
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 337
An attacker is able to successfully execute a social engineering attack by entering a building while dressed as a building security guard. Which of the following principles of effectiveness did the attacker utilize to execute the attack?

A. Urgency
B. Intimidation
C. Consensus
D. Authority

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 338

A network has been impacted by downtime resulting from unauthorized devices connecting directly to the wired network. The network administrator has been tasked to research and evaluate technical controls that would effectively mitigate risks associated with such devices. Which of the following capabilities would be MOST suitable for implementation in this scenario?

A. Host hardening
B. NIDS
C. VLAN trunking
D. Loop protection
E. Port security

Correct Answer: E
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 339

A company provides wireless access for employees and a guest wireless network for visitors. The employee wireless network is encrypted and requires a password. The guest wireless network does not use an encrypted connection and does not require a password. An administrator walks by a visitor's laptop and notices the following command line output:

```
reaver - I mon - b 7a : E5 : 9A : 42 : 2C : C1 - vv
Starting.....
[+] Trying pin 12345678
[+] 93.41% complete @ 2015-01-10 10:30:21 (15 seconds)
[!] WARNING: 10 failed connections in a row
[+] Trying pin 12345688
...
```

Which of the following should the administrator implement and why?

A. Initiate employee password changes because the visitor has captured passwords and is attempting offline cracking of those passwords.
B. Implement two-factor wireless authentication because the visitor will eventually brute force the network key.
C. Apply WPA or WPA2 encryption because the visitor is trying to crack the employee network that is encrypted with WEP.
D. Disable WPS because the visitor is trying to crack the employee network.

E. Apply MAC filtering because the visitor already has the network password.

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 340
An enterprise needs to be able to receive files that contain PII from many customers at different times. The data must remain encrypted during transport and while at rest. Which of the following encryption solutions would meet both of these requirements?

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

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 341
Which of the following is MOST effective at cracking hashed passwords?

A. Rainbow tables
B. Dictionary attack
C. Birthday attack
D. Brute force attack

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 342
The Chief Security Officer (CSO) is concerned with unauthorized access at the company's off-site datacenter. The CSO would like to enhance the security posture of the datacenter. Which of the following would BEST prevent unauthorized individuals from gaining access to the datacenter?

A. Security guard
B. Video monitoring
C. Magnetic entry cards
D. Fencing

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 343
Joe has been in the same IT position for the last 27 years and has developed a lot of homegrown applications that the company utilizes. The company is concerned that Joe is the only one who can administer these applications. The company should enforce which of the following best security practices and avoid Joe being a single point of failure?

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

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 344
A company has completed a continuity of operations plan and needs to validate that everyone knows what actions to perform. Which of the following can be performed instead of completing a full fail over to validate the requirement?

A. Tabletop exercise

B. Sandboxing

C. Business impact analysis

D. Risk assessment

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 345
A server administrator is investigating a breach and determines that an attacker modified the application log to obfuscate the attack vector. During the lessons learned activity the facilitator asks for a mitigation response to protect the integrity of the logs should a similar attack occur. Which of the following mitigations would be MOST appropriate to fulfill the requirement?

A. Host-based IDS

B. Automated log analysis

C. Enterprise SIEM

D. Real-time event correlation

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 346
A network administrator for a small business is configuring a wireless network for 20 users. Which of the following explains why the administrator would choose WPA2 Personal over WPA Enterprise?

A. It does not require a RADIUS server

B. It uses 3DES encryption

C. It has 14 channels available

D. It allows a separate password for each device

Correct Answer: A
Section: 5. Access Control and Identity Management

Explanation

Explanation/Reference:

QUESTION 347

An employee has been terminated due to inappropriate Internet use. A computer forensics technician at the organization acquired an image of the hard drive and hashed it using MD5. The former employee has filed a lawsuit. The former employee's attorney requests a copy of the image so it can be independently reviewed by the legal team. Upon receiving the image, the attorney's technician also generates a MD5 hash of the image and comes up with a different output than what was provided. Which of the following MOST likely occurred?

A. The wrong preshared key was used

B. The hashes were produced using different algorithms

C. The hashes were produced on two different operating systems

D. Files on the image have been altered

Correct Answer: D

Section: 6. Cryptography

Explanation

Explanation/Reference:

QUESTION 348

A security analyst at a nuclear power plant needs to secure network traffic from the legacy SCADA systems. Which of the following methods can the analyst use to secure network in this static environment?

A. Implement a firewall

B. Implement a HIDS

C. Implement a NIDS

D. Implement a rootjail

Correct Answer: A

Section: 1. Network Security

Explanation

Explanation/Reference:

QUESTION 349

The border firewall rules were recently modified by a network administrator to allow access to a new service on Server 1 using the default https port. When testing the new rules internal to the company network there are no issues and when testing from an external connection it does not work. The host running the service does not receive external packets. Other services hosted on Server 1 are responding fine to to both internal and external connection attempts. Which of the following is MOST likely configured improperly?

A. Network access control lists
B. 802.1x
C. Port security
D. Implicit deny

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 350
When responding to an incident on a new Windows server, the administrator needs to disable unused services. Which of the following commands can be used to see processes that are listening on a TCP port?

A. ipconfig
B. netstat
C. psinfo
D. net session

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 351
A security administrator is responsible for deployment of a new two factor authentication solution. The administrator has been informed that the solution will use soft tokens. Which of the following are valid token password schemes for the two factor solution being deployed? (Select TWO)

A. CHAP
B. PAP

C. NTLMv2
D. HMAC
E. Smart card
F. Time-based

Correct Answer: AD
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 352
A high traffic website is experiencing numerous brute force attacks against its user base. The attackers are using a very large botnet to carry out the attack. As a result, many users passwords are being compromised Which of the following actions is appropriate for the website administrator to take in order to reduce the threat from this type of attack in the future. .

A. Temporarily ban each IP address after five failed login attempts
B. Prevent users from using dictionary words that they have used before.
C. Prevent users from using passwords they have used before.
D. Require user passwords to be at least ten characters in length

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 353
A security auditor has full knowledge of company configuration and equipment. The auditor performs a test on the network, resulting in an exploitation of a zero-day vulnerability.

A. Grey box test
B. Vulnerability scan
C. Black box test
D. Penetration test

Correct Answer: D

Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 354
During a recent vulnerability assessment the penetration testers were able to successfully crack a large number of employee passwords. The company technology use agreement clearly states that passwords used on the company network must be at least eight characters long and contain at least one uppercase letter and special character. Which of the following can be used to standardize and enforce the password complexity rules across the entire organization to resolve the issue?

A. LDAP
B. Group policy
C. Discretionary access control
D. Kerberos

Correct Answer: B
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 355
A company has hired a an ex-employee to perform a penetration test of the company's proprietary application. Although the ex-employee used to be part of the development team, the application has gone through some changes since the employee left. Which of the following can the employee perform if the company is not willing to release any information to the ex-employee?

A. Black box testing
B. Regression testing
C. White box testing
D. Grey box testing

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 356
A company wants to be made aware of anyone who enters onto their property. Which of the following would be the BEST control to implement?

A. Roving guards
B. High fencing
C. Surveillance cameras
D. Motion sensors

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 357
A systems administrator is working with a third party to establish the automated transfer of large amounts of proprietary data. The interface will need to use secured credentials and the transmission will consist of data that has been encrypted prior to transit and needs no additional protection. Which of the following would be the MOST efficient method of data transmission given the established requirements?

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

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 358
A company was recently the victim of a major attack which resulted in significant reputational loss. Joe a member of the company incident response team is currently reviewing Standard Operating Procedures for the team in the wake of the attack. Which of the following BEST identifies the stage of incident response that Joe is in?

A. Reporting
B. Lessons learned

C. Mitigation steps

D. Preparation

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 359
Several customers received an email from an employee that advertised better rates at a different company. Shortly after the email was sent, Ann, the employee who sent the email, resigned and joined the other company. When confronted, Ann claimed that she did not send the email, it was another person spoofing her email address. Which of the following would eliminate Ann's excuse in the future?

A. Sender policy framework

B. Non repudiation

C. Encrypted email

D. Outgoing email filters

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 360
A security administrator is reviewing the event logs of the company server. There are numerous entries for attempts to log into the telnet service with an account named "root." After further review of the access to the server the security administrator determines that there is a business need for another server in the company via telnet to the server under review. Which of the following tasks should the security administrator perform to improve the security posture of the server? (Select TWO).

A. Change the timeout values of the telnet service

B. Allow the telnet access to the server through the firewall

C. Configure the telnet service to only accept traffic from the other server

D. Configure the telnet service to log at the debug level

E. Disable root access within the telnet service

F. Set the telnet service to enforce password changes every 90 days

Correct Answer: CE
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 361
A security engineer wants to communicate securely with a third party using PGP. Which of the following should the engineer send to the third party to enable the third party to securely encrypt email replies?

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

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 362
A security administrator has been asked to assist with the identification of a BYOD design that will ensure corporate data can be managed and monitored separately from personal data. Which of the following would the security administrator recommend?

A. Full device encryption
B. Application control
C. Key management
D. Containerization

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 363
A PKI architect is implementing a corporate enterprise solution. The solution must incorporate key escrow and recovery agents, as well as a tiered architecture. Which of the following is required to implement the architecture correctly?

A. Certificate revocation list
B. Strong ciphers
C. Intermediate authorities
D. IPSec between CAs

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

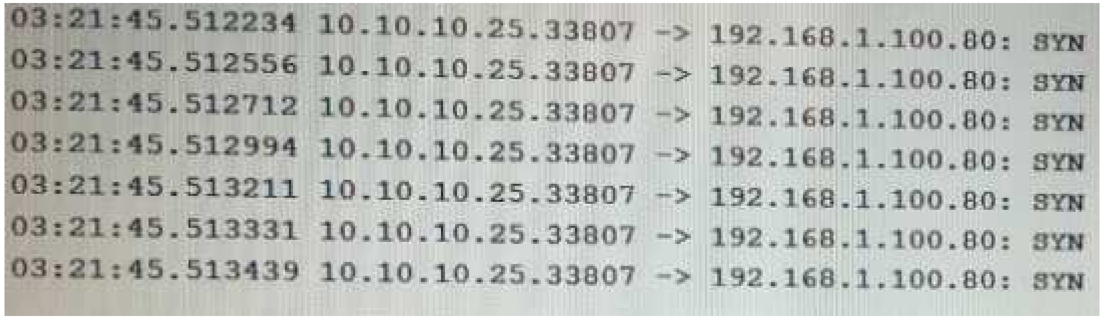
QUESTION 364
A system administrator is troubleshooting an issue affecting some FTP connections. Some employees are unable to upload or download files, although the firewall is allowing the default FTP port. Which of the following can the administrator do to fix this case?

A. Disable the use PASV in the FTP client
B. Configure all FTP clients to use BIN transfer
C. Enable inbound TCP port 20 on the firewall
D. Enable both port 21 and 22 on the firewall

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 365
Numerous users within an organization are unable to log into the web-based financial application. The network team places a sniffer on the segment where the application resides and sees the following log entries:



```
03:21:45.512234 10.10.10.25.33807 -> 192.168.1.100.80: SYN
03:21:45.512556 10.10.10.25.33807 -> 192.168.1.100.80: SYN
03:21:45.512712 10.10.10.25.33807 -> 192.168.1.100.80: SYN
03:21:45.512994 10.10.10.25.33807 -> 192.168.1.100.80: SYN
03:21:45.513211 10.10.10.25.33807 -> 192.168.1.100.80: SYN
03:21:45.513331 10.10.10.25.33807 -> 192.168.1.100.80: SYN
03:21:45.513439 10.10.10.25.33807 -> 192.168.1.100.80: SYN
```

Which of the following is most likely occurring?

A. DoS attack
B. Ping flood attack
C. Smurf attack
D. Replay attack
E. Xmas attack

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 366
A company experienced an intrusion into their network due to a perimeter firewall being compromised. A review of the firewall logs indicate that the service was accessed using the administrative account. Which of the following should be undertaken to prevent future intrusions? (Select TWO).

A. Upgrade the firewall firmware
B. Disable unnecessary accounts
C. Install an IDS
D. Setup a DMZ
E. Change default passwords

Correct Answer: BE
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 367
A security engineer notices that unknown devices are connecting to the company's wireless network and trying to access the database server. The wireless access point is configured with WPA for encryption and the network administrator setup an digit pin for easy setup to the wireless access point. Which of the following is the MOST likely type of attack?

A. IV attack
B. WPS attack
C. Bluesnarfing attack
D. Replay attack

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 368
Which of the following should mobile devices use in order to protect against data theft in an offline attack?

A. Application controls
B. Full device encryption
C. Storage segmentation
D. Whitelisting
E. Remote wiping

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 369
Which of the following can be used by PPP for authentication?

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

Correct Answer: A
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 370
Which of the following is an administrative control used to reduce tailgating?

A. Delivering security training
B. Erecting a fence
C. Implementing magnetic locks on doors
D. Installing a mantrap

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 371
Usage of which of the following technologies is MOST effective for any removable storage device, such as hard drives and flash drives?

A. Restrictive file system permissions
B. Full disk encryption
C. Password protected device access
D. Password protected file access

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 372
A network has been impacted by downtime resulting from unauthorized devices connecting directly to the wired network. The network administrator has been tasked to research and evaluate technical controls that would effectively mitigate risks associated with such devices. Which of the following capabilities would be MOST suitable for implementation in this scenario?

A. Host hardening
B. NIDS
C. VLAN trunking
D. Loop protection
E. Port security

Correct Answer: E
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 373
A virtualized server was updated with the latest operating system security patch. Upon completion of the patch installation, the file server automatically restarted and would not present a login screen. Which of the following would have prevented this issue?

A. The patch should have been tested for security benchmarks before installation on the server
B. The patch should have been deployed to a test system before installation on the server
C. The patch should have been implemented on a networked workstation before installation on the server
D. The patch should have been added to the whitelist of applications on the server

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 374

The security director has a man trap installed in the company's data center. This control is installed to mitigate:

A. transitive access
B. tailgating
C. shoulder surfing
D. impersonation

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 375
After a wireless security breach, the network administrator discovers the tool used to break into the network. Using a brute force attack, the tool is able to obtain the wireless password in less that 11,000 attempts. Which of the following should be disabled to prevent this type of attack in the future?

A. WPS
B. WEP
C. WIPS
D. WPA2-PSK

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 376
A web server at an organization has been the target of distributed denial of service attacks. Which of the following, if correctly configured, would BEST mitigate these and future attacks?

A. SYN cookies
B. Implicit deny
C. Blacklisting
D. URL filter

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 377
Virtualization would provide an ROI when implemented under which of the following situations?

A. Numerous servers with no fail-over requirement
B. Multiple existing 100% utilized physical servers
C. Numerous clients with a requirement for fast processors
D. Multiple existing but underutilized physical servers

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 378
During an audit of a software development organization, an auditor found that the organization did not properly follow industry best practices including peer review and board approval prior to moving applications into the production environment. The auditor recommended adapting a formal process incorporating these steps. To remediate the finding, the organization implemented:

A. incident management.
B. a configuration management board.
C. asset management.
D. change management.

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 379
An auditor is reviewing the following logs from the company's proxy server used to store both sensitive and public documents. The documents are edited via a client web interface and all processing is performed on the server side.

```
http://www.documents-portal.com/editdoc.php?document1=this%20is%20the%20content%20of%20document1
http://www.documents-portal.com/editdoc.php?document2=this%20is%20the%20content%20of%20document2
http://www.documents-portal.com/editdoc.php?document3=this%20is%20the%20content%20of%20document3
```

A. Two-factor authentication should be implemented for sensitive documents.
B. Sensitive documents should be signed using enterprise PKI.
C. Encryption should be implemented at the transport level.
D. Document hashing should be done to preserve document integrity.

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 380
A security engineer wants to communicate securely with a third party via email using PGP. Which of the following should the engineer send to the third party to enable the third party to securely encrypt email replies?

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

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 381
Which of the following are BEST used in the process of hardening a public facing web server? (Select TWO)

A. Vulnerability scanner

B. Protocol analyzer
C. Honeynet
D. Port scanner
E. Honeypot

Correct Answer: AD
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 382
An auditor is conducting a security audit and contacts the service desk at the target organization pretending to be a peer of the service desk employee. After engaging the employee in small talk, the auditor reports getting locked out of the organization's webmail system and requests that the employee reset the webmail password. Which of the following principles of social engineering is the auditor attempting to leverage in this attempted attack?

A. Urgency
B. Consensus
C. Authority
D. Familiarity

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 383
Which of the following types of malware can avoid detection by an antivirus system with up-to-date signatures?

A. Trojan
B. Backdoor
C. Polymorphic
D. Armored

Correct Answer: C
Section: 3. Threats and Vulnerabilities

Explanation

Explanation/Reference:

QUESTION 384
A programmer sets up a hidden account within a program to track users' personal information and habits. The programmer then uses this information to send targeted email messages to users. Which of the following best describes this hidden account?

A. Spam
B. Spyware
C. Backdoor
D. Rootkit

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 385
A security administrator has implemented a series of computers to research possible intrusions into the organizational network, and to determine the motives as well as the tool used by malicious entities. Which of the following has the security administrator implemented?

A. Honeypot
B. DMZ
C. Honeynet
D. VLANs

Correct Answer: C
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 386
The network administrator sees a "%CAM-TABLE-FULL" message on a network switch. Upon investigation, the administrator notices thousands of MAC addresses associated with a single untagged port. Which of the following should be implemented to prevent this type of attack?

A. Port security
B. BPDU guard
C. 802.1X
D. TACACS+

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 387
The operations manager for a sales group wants to ensure that sales personnel are able to use their laptops and other portable devices throughout a building using both wireless and wired connectivity. Which of the following technologies would be MOST effective at increasing security of the network while still maintaining the level of accessibility the operations manager requested?

A. 802.1X
B. 802.11n
C. WPA2 authentication
D. VLAN isolation
E. Authenticated web proxy

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 388
A security administrator wishes to monitor incoming traffic to the mail server with minimal risk of disruption of services and functions. Which of the following would BEST meet this goal?

A. Implement a host-based firewall on client computers.
B. Install a NIDS on the mail server network.
C. Implement a proxy server in the DMZ.

D. Install the mail relay server outside the DMZ.

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 389
An attacker is attempting to exploit the username field of an application. The exploitation involves writing more data than the field variable is initialized for. Which of the following attacks is being leveraged?

A. Buffer overflow
B. Integer overflow
C. XML injection
D. Session hijacking

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 390
Two companies are partnering to bid on a contract. Normally these companies are fierce competitors but for this procurement they have determined that a partnership is the only way they can win the job. Each company is concerned about unauthorized data sharing and wants to ensure other divisions within each company will not have access to proprietary data. To best protect against unauthorized data sharing they should each sign a(n):

A. NDA.
B. SLA.
C. MOU.
D. BPA

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 391
A Chief Information Office (CIO) is working with his staff to develop a contingency plan for the organization. Which of the following steps should the CIO and his staff to take FIRST?

A. Review the company's risk assessment
B. Perform a business impact analysis
C. Create contingency strategies
D. Develop the contingency plan policy statement

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 392
A security administrator runs a port scan against a server and determines that the following ports are open:
TCP 22
TCP 25
TCP 80
TCP 631
TCP 995
Which of the following MOST likely describes the server?

A. The server is an email server that requires secure email transmittal.
B. The server is a web server that requires secure communication.
C. The server is a print server that requires secure authentication.
D. The server is an email server that requires secure email retrieval.

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:
- TCP 995 - POP3 port,over TLS or POP3S
- TCP 631 - Common Unix Printing System (CUPS) administration console (extension to IPP)

QUESTION 393
A major banking institution has been the victim of recurring, widespread fraud. The fraud has all occurred on the bank's web portal. Recently, the bank implemented a requirement for all users to obtain credentials in person at a physical office. However, this has not reduced the amount of fraud against legitimate customers. Based on a review of the logs, most fraudulent transactions appear to be conducted with authentic credentials. Which of the following controls should be strengthened to reduce the fraud through the website?

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

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 394
A Chief Information Office (CIO) has recently expressed an interest in ensuring that critical business systems are protected from isolated outages. Which of the following would provide the CIO a measure of the frequency at which these critical business systems experience breakdowns?

A. MTTR
B. MTBF
C. MTTF
D. MTU

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 395
During a recent audit, it was discovered that several database services were running with local user accounts named "admin" and "dbadmin". The following controls will prevent network administrators from using these types of usernames for services in the future? (Select TWO)

A. Use shared account policies
B. Prohibit generic or default accounts
C. Perform continuous access monitoring
D. Perform user account access reviews
E. Require dedicated service accounts

Correct Answer: BE
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 396
An attacker is attempting to exploit a zero-day vulnerability in a popular enterprise application. The attacker is using personalized information to target high-value individuals in an attempt to obtain proprietary information from the organization. Which of the following attack methodologies is the attacker using?

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

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 397
A system administrator is configuring a site-to-site IPSec VPN tunnel. Which of the following should be configured on the VPN concentrator for payload encryption?

A. ECDHE
B. SHA256
C. HTTPS
D. 3DES

Correct Answer: D

Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 398
An IDS analyst while reviewing a TCPDUMP file concluded the traffic was a benign email correspondence. The presence and use of which of the following ports confirms this assumption?

A. 22
B. 25
C. 53
D. 80

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 399
A security administrator is testing an older server that is still in production. The administrator makes a copy of the registry where passwords are stored using NTLM. Which of the following should the administrator use to try and disclose the usernames and passwords of this server the FASTEST?

A. Brute Force
B. IV Attack
C. Dictionary Attack
D. Watering Hole
E. Rainbow Tables

Correct Answer: E
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 400
A recent counter threat intelligence notification states that companies should review indicators of compromise on all systems. The notification stated that the presence of a win32.dll was an identifier of a compromised system. A scan of the network reveals that all systems have this file. Which of the following should the security analyst perform FIRST to determine if the files collected are part of the threat intelligence?

A. Quarantine the file on each machine.
B. Take a full system image of each machine.
C. Take hashes of the files found for verification.
D. Verify the time and date of the files found.

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 401
Which of the following is an example of hardening a UNIX/Linux host based application?

A. Symbolic links
B. Shadow files
C. Antivirus
D. Wrapper

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 402
During a recent network audit, several devices on the internal network were found not running antivirus or HIPS. Upon further investigation, it was found that these devices were new laptops that were deployed without having the end-point protection suite used by the company installed. Which of the following could be used to mitigate the risk of authorized devices that are unprotected residing on the network?

A. Host-based firewall
B. Network-based IPS

C. Centralized end-point management

D. MAC filtering

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 403
A security analyst at a nuclear power plant needs to secure network traffic from the legacy SCADA systems. Which of the following methods could the analyst use to secure network traffic in this static environment?

A. Implement a firewall

B. Implement a HIDS

C. Implement a NIDS

D. Implement a rootjail

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 404
An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware, the attacker is provided with access to the infected machine. Which of the following is being described?

A. Zero-day exploit

B. Remote code execution
C. Session hijacking
D. Command injection

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 405
It was recently discovered that after a meeting in the datacenter, a malicious insider deleted several gigabytes of critical data and physically destroyed the accompanying tape backups. However, an investigation revealed that the insider's badge was never used to enter the server room. How could the insider BEST have accomplished this?

A. Remote access
B. Time bomb attack
C. Setting a fire
D. Tailgating

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 406
An administrator installs a system that sends an SMS message containing a password recovery token to a user's mobile device. Which of the following should also be deployed to prevent accounts from being compromised?

A. Password reuse limits
B. Secure SMS gateway
C. One-time token authentication
D. Mobile device management

Correct Answer: B
Section: 4. Application, Data, and Host Security

Explanation

Explanation/Reference:

QUESTION 407
An employee connects to a public wireless hotspot during a business trip. The employee attempts to go to a secure website, but instead connects to an attacker who is performing a man-in-the-middle attack. Which of the following should employees do to mitigate the vulnerability described in the scenario?

A. Connect to a VPN when using public wireless networks
B. Only connect to WPA2 networks regardless of whether the network is public or private
C. Ensure a host-based firewall is installed and running when using public wireless networks
D. Check the address in the web browser before entering credentials

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 408
An old 802.11b wireless bridge must be configured to provide confidentiality of data in transit to include the MAC addresses of communicating end users. Which of the following can be implemented to meet this requirement?

A. MSCHAPv2
B. WPA2
C. WEP
D. IPSec

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 409
Company policy states that when a virus or malware alert is received, the suspected host is immediately removed from the company network. Which of the following BEST describes this component of incident response?

A. Mitigation
B. Isolation
C. Recovery
D. Reporting
E. Remediation

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 410
After responding to a virus detection notification, a security technician has been tasked with discovering how the virus was downloaded to the client computer. Which of the following would BEST provide the technician with information related to the attack vector?

A. Vulnerability scanning logs
B. NIPS alerts
C. Surveillance videos
D. Proxy logs

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 411
A recent regulatory audit discovers a large number of former employees with active accounts. Terminated users are removed from the HR system but not from Active Directory. Which of the following processes would close the gap identified?

A. Send a recurring email to managers with a link to IT Security policies.
B. Perform routine audits against the HR system and Active Directory.
C. Set an account expiration date for all Active Directory accounts to expire annually.
D. Conduct permissions reviews in Active Directory for group membership.

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 412
An attacker has breached multiple lines of information security defense. Which of the following BEST describes why delayed containment would be dangerous?

A. The attacker could be blocked by the NIPS before enough forensic data can be collected.
B. The attacker could erase all evidence of how they compromised the network.
C. The attacker could cease all attack activities making forensics more difficult.
D. The attacker could escalate unauthorized access or compromise other systems.

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 413
A forensics expert needs to be able to prove that digital evidence, originally taken into custody, has not been tampered with. Which of the following is useful in this scenario?

A. Encryption
B. Non-repudiation
C. Hashing
D. Perfect forward secrecy
E. Steganography

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 414
A manager is reviewing bids for Internet service in support of a new corporate office location. The location will provide 24-hour service to the organization's global user population. In which of the following documents would the manager MOST likely find quantitative data regarding latency levels and MTTR?

A. ISA
B. SLA
C. MOU
D. BPA

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 415
A retired employee did not return a company issued mobile device and may have company data on the device. Which of the following portions of the company's mobile device management solution could be used together to remove the company data from the employee's device? (Select TWO)

A. Full device encryption
B. Application whitelisting
C. Asset tracking
D. Remote wiping
E. Storage segmentation
F. Inventory control

Correct Answer: DE
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 416
An administrator must select an algorithm for creating hashes of critical system files in order to later detect any unauthorized changes. Which of the following could the administrator use? (Select TWO).

A. 3DES
B. Diffie-Hellman
C. CHAP
D. RIPEMD
E. RSA
F. AES-256
G. SHA-512

Correct Answer: DG
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 417
A user is able to access shares that store confidential information that is not related to the user's current job duties. Which of the following should be implemented to prevent this from occurring?

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

Correct Answer: A
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 418
An attacker is attempting to determine the patch level version that a web server is running on its open ports. Which of the following is an active technique that will MOST efficiently determine the information the attacker is seeking?

A. Banner grabbing
B. Vulnerability scanning
C. Port scanning

D. Protocol analysis

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 419
Several computers in an organization are running below the normal performance baseline. A security administrator inspects the computers and finds the following pieces of information:

- Several users have uninstalled the antivirus software
- Some users have installed unauthorized software
- Several users have installed pirated software
- Some computers have had automatic updating disabled after being deployed
- Users have experienced slow responsiveness when using the Internet browser
- Users have complete control over critical system properties

Which of the following solutions would have prevented these issues from occurring? (Select TWO).

A. Using snapshots to revert unwanted user changes
B. Using an IPS instead of an antivirus
C. Placing users in appropriate security groups
D. Disabling unnecessary services
E. Utilizing an application whitelist
F. Utilizing an application blacklist

Correct Answer: CE
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 420
A company uses digital signatures to sign contracts. The company requires external entities to create an account with a third-party digital signature provider and to sign an agreement stating that they will protect the account from unauthorized access. Which of the following security goals is the company trying to address in the given scenario?

A. Availability
B. Non-repudiation
C. Authentication
D. Confidentiality
E. Due diligence

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 421
One of the driving factors towards moving an application to a cloud infrastructure is increased application availability. In the case where a company creates a private cloud, the risk of application downtime is being:

A. transferred.
B. avoided.
C. mitigated.
D. accepted.

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 422
Which of the following is a contract with a service provider that typically includes performance parameters like MTBF and MTTR?

A. SLA
B. NDA
C. ISA
D. MOU
E. ALE

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 423
A research user needs to transfer multiple terabytes of data across a network. The data is not confidential, so for performance reasons, does not need to be encrypted. However, the authentication process must be confidential. Which of the following is the BEST solution to satisfy these requirements?

A. Secured LDAP
B. Kerberized FTP
C. SCP
D. SAML 2.0

Correct Answer: B
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 424
A recent security audit revealed the company is lacking deterrent security controls. Which of the following could be implemented to address this finding?

A. Rogue machine detection
B. Continuous security monitoring
C. Security cameras
D. Intrusion detection system

Correct Answer: C
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 425
When performing a risk analysis, which of the following is considered a threat?

A. The potential exploitation of vulnerability
B. The transference of risk to another party
C. The presence of a risk in the environment
D. The lack of mitigation for vulnerabilities

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 426
An attacker would like to target a company and redirect their legitimate traffic to other sites. Which of the following attacks would be used to cause this malicious URL redirection?

A. Botnet
B. Backdoor
C. DNS Poisoning
D. Phishing

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 427
Which of the following social engineering attacks would describe a situation where an attacker calls an employee while impersonating a corporate executive?

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

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 428
An analyst is documenting the user interaction process associated with the login prompts in an application structure, the user enters a username and a one-time password, which was previously emailed to the user. Next, the user enters a PIN and is then allowed into the dashboard of the application to modify account details. In this scenario, which of the following steps immediately precedes the authorization process?

A. Accessing the account
B. Entering the username
C. Receiving the one-time password
D. Submitting the PIN

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 429
An administrator needs to deploy a new SSL wildcard certificate to three different web servers. Which of the following MUST be taken into consideration? (Select TWO).

A. The fingerprint on the certificate
B. The CRL URL of the certificate
C. Intermediate CA(s) that may need to be added
D. File format needed by the target platform
E. The CSR that was used to request the certificate
F. The OU field on the certificate

Correct Answer: CF
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 430
A security specialist has implemented antivirus software and whitelisting controls to prevent malware and unauthorized application installation on the company systems. The combination of these two technologies is an example of which of the following?

A. Defense in depth
B. Vulnerability scanning
C. Application hardening
D. Anti-malware

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 431
A healthcare organization is in the process of building and deploying a new web server in the DMZ that will enable public Internet users the ability to securely send and receive messages from their primary care physicians. Which of the following should the security administrator consider?

A. An in-band method for key exchange and an out-of-band method for the session
B. An out-of-band method for key exchange and an in-band method for the session
C. A symmetric algorithm for key exchange and an asymmetric algorithm for the session
D. An asymmetric algorithm for key exchange and a symmetric algorithm for the session

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 432
An application service provider has notified customers of a breach resulting from improper configuration changes. In the incident, a server intended for internal access only was made accessible to external parties. Which of the following configurations were likely to have been improperly modified, resulting in the breach?

A. NAT
B. IDS
C. CRL
D. VPN

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 433
A security administrator, believing it to be a security risk, disables IGMP snooping on a switch. This breaks a video application. The application is MOST likely using:

A. RTP.
B. multicast.
C. anycast.
D. VoIP.

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 434
A systems administrator is part of the organization's contingency and business continuity planning process. The systems administrator and relevant team participant in the analysis of a contingency situation intended to elicit constructive discussion. Which of the following types of activity is MOST accurately described in this scenario?

A. Business impact analysis
B. Full-Interruption exercise
C. Tabletop exercise
D. Lessons learned
E. Parallel simulation

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 435
Which of the following authentication services utilizes UDP for communication between client and server?

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

Correct Answer: D
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 436
Which of the following actions would help prevent SQL injection on a web application?

A. Blocking direct access to the SQL server's management port
B. Using exception handling to detect buffer overflows
C. Validating client input inside the application's source code
D. Regularly applying patches to the database management system

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 437

Ann, a network security engineer, is trying to harden her wireless network. Currently, users are able to connect any device to the wireless network as long as they authenticate with their network username and password. She is concerned that devices that are not company-issued may gain unauthorized access. Which of the following techniques would be BEST suited to remediate this vulnerability? (Select TWO).

A. Utilize a single service account, only known by IT, to authenticate all devices
B. Install separate access points for personal devices
C. Install an IPS to protect the network from rogue devices
D. Filter the MAC addresses of all unknown devices on the wireless controller
E. server to authenticate via computer end user

Correct Answer: DE
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 438
A server technician is about to perform a major upgrade to the operating system of a critical system. This system is currently in a virtualization environment. Which of the following actions would result in the LEAST amount of downtime if the upgrade were to fail?

A. Enabling live migration in the VM settings on the virtual server.
B. Clustering the storage for the server to add redundancy.
C. Performing a full backup of the virtual machine.
D. Taking an initial snapshot of the system.

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 439
A large retail vendor provides access to a heating, ventilation, and air conditioning vendor for the purpose of issuing billing statements and receiving payments. A security administrator wants to prevent attackers from using compromised credentials to access the billing system, moving laterally to the point-of-sale (POS) system, and installing malware to skim credit card data. Which of the following is the MOST important security architecture consideration the retail vendor should impose?

A. Data encryption
B. Network segregation
C. Virtual private networking
D. Application firewalls

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 440
A company must implement management controls to deter system administrators from making unauthorized changes to sensitive systems. Which of the following should the company implement?

A. System and data file hashing.
B. Periodic reviews of system activity.
C. Host based intrusion detection system.
D. Remote syslog server inaccessible by system administrators.

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 441
An assessment team is conducting a vulnerability scan of an organization's database servers. During the configuration of the vulnerability scanner, the lead assessor only configures the parameter of the database servers' IP range, and then runs the vulnerability scanner. Which of the following scan types is being run on the database servers?

A. Intrusive
B. Ping sweep
C. Non-credentialed
D. Offline

Correct Answer: C

Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 442
A security administrator has deployed five additional copies of the same virtualized Linux server to distribute the load of web traffic on the original server. Which of the following should the administrator do to help security harden these new systems? (Select TWO).

A. Configure for dual factor authentication
B. Team/Bond network adapters
C. Add virtual machine software extensions
D. Deploy unique public keys to each virtual server
E. Disable HTTP protocols
F. Generate new SSH keys

Correct Answer: DF
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 443
A company is planning to encrypt the files in several sensitive directories of a file server with an asymmetric key. Which of the following could be used?

A. AES
B. RSA
C. ECC
D. 3DES
E. MD5

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 444
A security administrator determined that the time required to brute force 90% of the company's password hashes is below the acceptable threshold. Which of the following, if implemented, has the GREATEST impact in bringing this time above the acceptable threshold?

A. Use a shadow password file.
B. Increase the number of PBKDF2 iterations.
C. Change the algorithm used to salt all passwords.
D. Use a stronger hashing algorithm for password storage.

Correct Answer: B
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 445
Following a site survey for an upcoming 5GHz wireless network implementation, the project manager determines that several areas of the facility receive inadequate coverage due to the use of vertical antennas on all access points. Which of the following activities would be MOST likely to remediate the issue without changing the current access point layout in the facility?

A. Convert all access points to models operating at 2.4GHz.
B. Install antennas with lower front-to-back ratios to narrow the focus of coverage as needed.
C. Reorient the existing antennas in horizontal configuration.
D. Install unidirectional antennas to focus coverage where needed.

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 446
A company has recently won a classified government contract involving both confidential and restricted information. To ensure proper authorization for authenticated users and restrict unauthorized users from accessing information above their clearance, the company should establish:

A. discretionary access control.

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

Correct Answer: B
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 447
An administrator sees the following entry in a system log:
02:23:41 AM Mar 09 2015 www: WARNING: MD5 checksum on file /etc/sudoers has changed. Please update db if this change is expected.
Which of the following describes the type of application that generated this log entry?

A. Change management
B. Security patch management
C. SELinux audit utility
D. File integrity management

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 448
A malicious insider is using an ARP spoofing tool to impersonate the gateway router. Which of the following attack types is the malicious insider implementing?

A. Man-in-the-middle attack.
B. IP spoofing attack.
C. DNS poisoning and redirect attack.
D. Replay attack.

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 449

A finance manager is responsible for approving wire transfers and processing the transfers using the software provided by the company's bank. A number of discrepancies have been found related to the wires in a recent financial audit and the wires appeared to be fraudulent. Which of the following controls should be implemented to reduce the likelihood of fraud related to the use of wire transfers?

A. Separation of duties
B. Least privilege
C. Qualitative auditing
D. Acceptable use policy

Correct Answer: A
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 450

A network technician needs to pass traffic from the company's external IP address to a front-end mail server in the DMZ without exposing the IP address of the mail server to the external network. Which of the following should the network technician use?

A. NAT
B. SMTP
C. NAC
D. SSH
E. TLS

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 451

On a campus network, users frequently remove the network cable from desktop NICs and plug personal laptops into the school network. Which of the following could be used to reduce the likelihood of unauthorized laptops on the campus network?

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

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 452
A system administrator decided to perform maintenance on a production server servicing retail store operations. The system rebooted in the middle of the day due to the installation of monthly operating system patches. The downtime results in lost revenue due to the system being unavailable. Which of the following would reduce the likelihood of this issue occurring again?

A. Routine system auditing
B. Change management controls
C. Business continuity planning
D. Data loss prevention implementation

Correct Answer: B
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 453
A data breach is suspected on a currently unidentified server in a datacenter. Which of the following is the BEST method of determining which server was breached?

A. Network traffic logs
B. System image capture
C. Asset inventory review

D. RAM analysis

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 454
An organization received a subpoena requesting access to data that resides on an employee's computer. The organization uses PKI. Which of the following is the BEST way to comply with the request?

A. Certificate authority
B. Public key
C. Key escrow
D. Registration authority
E. Key recovery agent

Correct Answer: E
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 455
Due to the commonality of Content Management System (CMS) platforms, a website administrator is concerned about security for the organization's new CMS application. Which of the following practices should the administrator implement FIRST to mitigate risks associated with CMS platform implementations?

A. Deploy CAPTCHA features
B. Modify default accounts' password
C. Implement two-factor authentication
D. Configure DNS blacklisting
E. Configure password complexity requirements

Correct Answer: B
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 456
A forensics expert needs to be able to prove that digital evidence, originally taken into custody, has not been tampered with. Which of the following are useful in this scenario?

A. Encryption
B. Non-repudiation
C. Hashing
D. Perfect forward secrecy
E. Steganography

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 457
A security administrator recently implemented IPSec for remote users. Which of the following ports must be allowed through the firewall in order for remote access to be successful if the tunneling protocol is PPTP?

A. UDP 500
B. UDP 1723
C. TCP 1723
D. TCP 4500

Correct Answer: C
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 458
The firewall administrator is installing a VPN application and must allow GRE through the firewall. Which of the following MUST the administrator allow through the

firewall?

A. IPSec
B. IP protocol 47
C. IP protocol 50
D. IP protocol 51

Correct Answer: B
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 459
A company is providing mobile devices to all employees. The system administrator has been tasked with providing input for the company's new mobile device policy. Which of the following are valid security concepts that the system administrator should include when offering feedback to management? (Select TWO)

A. Transitive trust
B. Asset tracking
C. Remote wiping
D. HSM
E. Key management

Correct Answer: CE
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 460
Ann, a recently terminated programmer, can access the program she wrote without using any login credentials. Which of the following attack types is this?

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

Correct Answer: B
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 461
When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

A. RC4
B. MD5
C. RIPEMD
D. SHA

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 462
A security administrator creates separate VLANs for employee devices and HVAC equipment that is network attached. Which of the following are security reasons for this design? (Select THREE).

A. IDS often requires network segmentation of HVAC endpoints for better reporting.
B. Broadcasts from HVAC equipment will be confined to their own network segment.
C. HVAC equipment can be isolated from compromised employee workstations.
D. VLANs are providing loop protection for the HVAC devices.
E. Access to and from the HVAC equipment can be more easily controlled.
F. Employee devices often interfere with proper functioning of HVAC devices.

Correct Answer: BCE
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 463
A company needs to ensure that employees that are on vacation or leave cannot access network resources, while still retaining the ability to receive emails in their inboxes. Which of the following will allow the company to achieve this goal?

A. Set up an email alias
B. Remove user privileges
C. Install an SMTP proxy server
D. Reset user passwords

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 464
Which of the following types of attacks are MOST likely to be successful when using fuzzing against an executable program? (Select TWO).

A. SQL injection
B. Session hijacking
C. Integer overflow
D. Buffer overflow
E. Header manipulation

Correct Answer: AD
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 465
An organization's security policy requires that data be available in case of a natural disaster. Which of the following would BEST meet this goal?

A. RAID array
B. Encrypted storage

C. Cloud backups
D. Load balancing

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 466
Usage of which of the following technologies is MOST effective for any removable storage device, such as hard drives and flash drives, in an organization to help prevent data loss or theft?

A. Restrictive file system permissions
B. Full disk encryption
C. Password protection device access
D. Password protected file access

Correct Answer: B
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 467
A security manager is required to protect the disclosure of sensitive data stored on laptops and mobile devices while users are traveling. Users are required to connect via VPN to the company's network and are also issued cable locks. Which of the following should the security manager implement to further secure the data? (Select TWO).

A. Screen locks
B. Remote wipe
C. One-time tokens
D. BIOS password
E. Full-disk encryption

Correct Answer: BE
Section: 4. Application, Data, and Host Security

Explanation

Explanation/Reference:

QUESTION 468
An outside testing company performing black box testing against a new application determines that it is possible to enter any characters into the application's web-based form. Which of the following controls should the application developers use to prevent this from occurring?

A. CSRF prevention
B. Sandboxing
C. Fuzzing
D. Input validation

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 469
A network administrator would like to implement a wireless solution that uses a very high performance stream cipher encryption protocol. Which of the following solutions should the administrator implement to meet this goal?

A. EAP-TLS
B. WPA2 Enterprise
C. WEP
D. CCMP

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 470
An administrator is tasked with reducing the malware infection rate of PC applications. To accomplish this, the administrator restricts the locations from which programs can be launched. After this is complete, the administrator notices that malware continues to run from locations on the disk and infect the hosts. Which of

the following did the administrator forget to do?

A. Restrict write access to the allowed executable paths
B. Install the host-based intrusion detection system
C. Configure browser sandboxing
D. Disable unnecessary services

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 471
Which of the following network configurations provides security analysts with the MOST information regarding threats, while minimizing the risk to internal corporate assets?

A. Configuring the wireless access point to be unencrypted
B. Increasing the logging level of internal corporate devices
C. Allowing inbound traffic to a honeypot on the corporate LAN
D. Placing a NIDS between the corporate firewall and ISP

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 472
Joe, a user, wants to configure his workstation to make certain that the certificate he receives when connecting to websites is still valid. Which of the following should Joe enable on his workstation to achieve this?

A. Certificate revocation
B. Key escrow
C. Registration authority
D. Digital signatures

Correct Answer: A
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 473
A security administrator wishes to ensure that one file in a confidential location is not altered. With very limited technology or restrictions to the file or folder, which of the following controls could the security administrator use to determine if the file has been altered?

A. Role-based access
B. File-based encryption
C. Rule-based access
D. MD5 checksum

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 474
The first responder to an incident has been asked to provide an after action report. This supports which of the following Incident Response procedures?

A. Incident identification
B. Mitigation
C. Lessons learned
D. Escalation/Notification

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 475

An attacker is attempting to determine the patch level version that a web server is running on its open ports. Which of the following is an active technique that will MOST efficiently determine the information the attacker is seeking?

A. Banner grabbing
B. Vulnerability scanning
C. Port scanning
D. Protocol analysis

Correct Answer: A
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 476
An employee is conducting a presentation at an out-of-town conference center using a laptop. The wireless access point at the employee's office has an SSID of *OFFICE.* The laptop was set to remember wireless access points. Upon arriving at the conference, the employee powered on the laptop and noticed that it was connected to the *OFFICE* access point. Which of the following MOST likely occurred?

A. The laptop connected to a legitimate WAP.
B. The laptop connected as a result of an IV attack.
C. The laptop connected to an evil twin WAP.
D. The laptop connected as a result of near field communication.

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 477
An administrator is reviewing the logs for a content management system that supports the organization's public-facing website. The administrator is concerned about the number of attempted login failures from other countries for administrator accounts. Which of the following capabilities is BEST to implement if the administrator wants the system to dynamically react to such attacks?

A. Netflow-based rate limiting
B. Disable generic administrative accounts

C. Automated log analysis
D. Intrusion prevention system

Correct Answer: A
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 478
A company has a proprietary device that requires access to the network be disabled. Only authorized users should have access to the device. To further protect the device from unauthorized access, which of the following would also need to be implemented?

A. Install NIPS within the company to protect all assets.
B. Block port 80 and 443 on the firewall.
C. Install a cable lock to prevent theft of the device.
D. Install software to encrypt access to the hard drive.

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 479
Which of the following attack types is MOST likely to cause damage or data loss for an organization and be difficult to investigate?

A. Man-in-the-middle
B. Spoofing
C. DDoS
D. Malicious insider

Correct Answer: D
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 480
After Ann arrives at the company's co-location facility, she determines that she is unable to access the cage that holds the company's equipment after a co-worker updated the key card server the night before. This is an example of failure of which of the following?

A. Testing controls
B. Access signatures
C. Fault tolerance
D. Non-repudiation

Correct Answer: A
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 481
A security administrator wants to implement a system that will allow the organization to quickly and securely recover from a computer breach. The security administrator notices that the majority of malware infections are caused by zero-day armored viruses and rootkits. Which of the following solutions should the system administrator implement?

A. Install an antivirus solution that provides HIPS capabilities.

B. Implement a thick-client model with local snapshots.
C. Deploy an enterprise patch management system.
D. Enable the host-based firewall and remove users' administrative rights.

Correct Answer: A
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 482
A server administrator is investigating a breach and determines that an attacker modified the application log to obfuscate the attack vector. During the lessons learned activity, the facilitator asks for a mitigation response to protect the integrity of the logs should a similar attack occur. Which of the following mitigations would be MOST appropriate to fulfill the requirement?

A. Host-based IDS
B. Automated log analysis
C. Enterprise SIEM
D. Real-time event correlation

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 483
Which of the following network design components would assist in separating network traffic based on the logical location of users?

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

Correct Answer: D
Section: 1. Network Security
Explanation

Explanation/Reference:

QUESTION 484
The network engineer for an organization intends to use certificate-based 802.1X authentication on a network. The engineer's organization has an existing PKI that is used to issue server and user certificates. The PKI is currently not configured to support the issuance of 802.1X certificates. Which of the following represents an item the engineer MUST configure?

A. OCSP responder
B. Web enrollment portal
C. Symmetric cryptography
D. Certificate extension

Correct Answer: D
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 485
A company has begun construction on a new building. The construction crews have noticed that valuable materials have been stolen from the site. Which of the following preventative controls should be used by the Chief Security Officer (CSO) to prevent future theft?

A. Motion sensors
B. CCTV
C. Fencing
D. Lighting

Correct Answer: C
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 486
A security administrator has detected the following pattern in a TCP packer: URG=1, ACK=1, PSH=1, RST=1, SYN=1, FIN=1. Which of the following attacks is this an example of?

A. Replay
B. Spoofing
C. Xmas
D. DDoS

Correct Answer: C

Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 487
Which of the following types of attacks are MOST likely to be successful when using fuzzing against an executable program? (Select TWO).

A. SQL injection
B. Session hijacking
C. Integer overflow
D. Buffer overflow
E. Header manipulation

Correct Answer: AD
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 488
Which of the following should be used to implement voice encryption?

A. SSLv3
B. VDSL
C. SRTP
D. VoIP

Correct Answer: C
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 489
Multi-function devices are being deployed in various departments. All departments will be able to copy, print and scan to file. Some departments will be authorized

to use their devices to fax and email, while other departments will not be authorized to use those functions on their devices. Which of the following is the MOST important mitigation technique to avoid an incident?

A. Disable unnecessary accounts.
B. Password protection.
C. Monitor access logs.
D. Disable unnecessary services.

Correct Answer: D
Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 490
An attacker is able to successfully execute a social engineering attack by entering a building while dressed as a building security guard. Which of the following principles of effectiveness did the attacker utilize to execute the attack?

A. Urgency
B. Intimidation
C. Consensus
D. Authority

Correct Answer: D
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 491
During a recent audit, it was discovered that the employee who deploys patches also approves the patches. The audit found there is no documentation supporting the patch management process, and there is no formal vetting of installed patches. Which of the following controls should be implemented to mitigate this risk? (Select TWO).

A. IT contingency planning
B. Change management policy
C. Least privilege

D. Separation of duties
E. Dual control
F. Mandatory job rotation

Correct Answer: BD
Section: 2. Compliance and Operational security
Explanation

Explanation/Reference:

QUESTION 492
During a trial for possession of illegal content, a defence attorney argues that several of the files on the forensic image may have been tampered with. How can a technician BEST disprove this argument?

A. Trace the chain-of-custody from the time of arrest until the time of trial
B. Have the investigator undergo a polygraph examination
C. Take hashes from the suspect source drive, and compare them to hashes on the forensic image
D. Access the system logs on the forensic image, and see if any logins occurred after the suspect's arrest

Correct Answer: C
Section: 6. Cryptography
Explanation

Explanation/Reference:

QUESTION 493
Which of the following remote authentication methods uses a reliable transport layer protocol for communication?

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

Correct Answer: C
Section: 5. Access Control and Identity Management
Explanation

Explanation/Reference:

QUESTION 494

A company has classified the following database records:

OBJECT	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
First Name	LOW	MEDIUM	LOW
Last Name	LOW	MEDIUM	LOW
Address	MEDIUM	HIGH	LOW
Bank Account Number	HIGH	HIGH	MEDIUM
Credit Card Number	HIGH	HIGH	MEDIUM

Which of the following is a management control the company can implement to increase the security of the above information with respect to confidentiality?

A. Implement a client based software filter to prevent some employees from viewing confidential information.

B. Use privacy screen on all computers handling and displaying sensitive information.

C. Encrypt the records which have a classification of HIGH in the confidentiality column.

D. Disseminate the data classification table to all employees and provide training on data disclosure.

Correct Answer: D

Section: 2. Compliance and Operational security

Explanation

Explanation/Reference:

QUESTION 495

Analysis of a recent security breach at an organization revealed that the attack leveraged a telnet server that had not been used in some time. Below are partial results of an audit that occurred a week before the breach was detected.

OPEN PORTS---TCP 23, TCP 80, TCP 443
OS PATCH LEVEL---CURRENT
PASSWORD AUDIT---PASS, STRONG
FILE INTEGRITY---PASS

Which of the following could have mitigated or deterred this breach?

A. Routine patch management on the server

B. Greater frequency of auditing the server logs

C. Password protection on the telnet server

D. Disabling unnecessary services

Correct Answer: D

Section: 4. Application, Data, and Host Security
Explanation

Explanation/Reference:

QUESTION 496
A security administrator receives an IDS alert that a single internal IP address is connecting to several known malicious command and control domains. The administrator connects to the switch and adds a MAC filter to Port 18 to block the system from the network.

BEFORE			**AFTER**		
MAC Address	VLAN	Port	MAC Address	VLAN	Port
67A7.353B.5064	101	4	67A7.353B.5064	101	4
7055.4961.1F33	100	9	7055.4961.1F33	100	9
0046.6416.5809	101	21	0046.6416.5809	101	21
7027.0108.31B5	100	16	7027.0108.31B5	100	16
5243.6353.7720	101	6	5243.6353.7720	101	6
1484.A471.6542	100	2	1484.A471.6542	100	2
80C7.8669.5845	101	7	80C7.8669.5845	101	7
7513.77B9.4130	101	18	0046.6419.5809	101	18
5A77.1816.3859	101	19	5A77.1816.3859	101	19
8294.7E31.3270	100	8	8294.7E31.3270	100	8

A few minutes later, the same malicious traffic starts again from a different IP. Which of the following is the MOST likely reason that the system was able to bypass the administrator's MAC filter?

A. The system is now ARP spoofing a device on the switch.
B. The system is now VLAN hopping to bypass the switch port MAC filter.
C. The system is now spoofing a MAC address.
D. The system is now connecting to the switch.

Correct Answer: C
Section: 3. Threats and Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 497
In order to establish a connection to a server using secure LDAP, which of the following must be installed on the client?

A. Server public key
B. Subject alternative names certificate
C. CA anchor of trust
D. Certificate signing request

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 498
A security administrator conducts a vulnerability scan on multiple web servers. Some of findings are not found on the web server. Which of the following BEST explains this situation?

A. False positive results
B. Host-based IPS dropped packets
C. Improper network segmentation
D. Web application firewall interference

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 499
A recent policy change at an organization requires that all remote access connections to and from file servers at remote locations must be encrypted. Which of the following protocols would accomplish this new objective? (Select TWO).

A. TFTP
B. SSH
C. FTP
D. RDP
E. HTTP

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 500
A security administrator has been tasked hardening operating system security on tablets that will be deployed for use by floor salespeople at retail outlets. Which of the following could the administrator implement to reduce the likelihood that unauthorized users will be able to access information on the tablets?

A. GPS device tracking
B. Remote wiping
C. Cable locks
D. Password protection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 501
A network administrator is in the process of developing a new network security infrastructure. One of the requirements for the new system is the ability to perform advanced authentication, authorization, and accounting. Which of the following technologies BEST meets the stated requirement?

A. Kerberos
B. SAML
C. TACACS+
D. LDAPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 502
An organization that uses a cloud infrastructure to present a payment portal is using:

A. software as a service
B. platform as a service
C. monitoring as a service
D. infrastructure as a service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 503
A company is providing mobile devices to all its employees. The system administrator has been tasked with providing input for the company's new mobile device policy. Which of the following are valid security concepts that the system administrator should include when offering feedback to management? (Select TWO)

A. Transitive trust
B. Asset tracking
C. Remote wiping
D. HSM
E. Key management

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 504
Attackers use techniques when sending tailored emails to engage their targets and make them feel personally involved. Which of the following social engineering techniques BEST describes this type of attack?

A. Spear phishing
B. Whaling
C. SMiShing

D. Pharming

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 505
A forensics investigator needs to be able to prove that digital evidence was not tampered with after being taken into custody. Which of teh following is useful in this scenario?

A. Encryption
B. Non-repudiation
C. Hashing
D. Perfect forward secrecy
E. Steganography

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 506
A penetration tester is attempting to determine the operating system of a remote host. Which of the following will provide this information?

A. Protocol analyzer
B. Honeypot
C. Fuzzer
D. Banner grabbing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 507
Members of the accounting group save all of their work in a directory on a Linux server. The directory has the default permissions of rwxrwxr-x. The accounting users suspect that a user in the Human Resources group is aware of the existence of a confidential file. What is the reason for the accounting users suspicions?

A. The default permissions, other users can add files to the directory
B. The default permissions, other users have no access to the directory
C. The default permissions, other users can view contents of the directory
D. The default permissions, other users can remove files from the directory

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 508
A company is hosting both sensitive and public information at a cloud provider. Prior to the company going out of business, the administrator will decommission all virtual servers hosted in the cloud. When wiping the virtual hard drive, which of the following should be removed?

A. Hardware specifications
B. Encrypted files
C. Data remnants
D. Encrypted keys

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 509
A software development manager needs to create several different environments for application development, testing, and quality control. Controls are being put in place to manage how software is moved into the production environment. Which of the following should the software development manager request be put in place to implement the three new environments?

A. Application firewalls
B. Network segmentation
C. Trusted computing
D. Network address translation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 510
When implementing a new system, a systems administrator works with the information system owner to identify and document the responsibilities of various positions within teh organization. Once responsibilities are identified, groups are created within the system to accommodate the various responsibilities of each position type, with users being placed in these groups. Which of the following principles of authorization is being developed?

A. Rule-based access control
B. Least privilege
C. Separation of duties
D. Access control lists
E. Role-based access control

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 511
An organization experienced a fire at its datacenter and was unable to operate at that location. The company moved to a location where HVAC and power are available, but must supply and configure its own computing resources in order to provide services. The company has relocated to a:

A. hot site
B. co-location site
C. warm site
D. cold site

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 512
Based on a review of the existing access policies the network administrator determines that that changes are needed to meet current regulatory requirements of the organization's access control process. To initiate changes in teh process, the network administrator should FIRST:

A. update the affected policies and inform the user community of the changes
B. distribute a memo stating that all new accounts must follow current regulatory requirements
C. inform senior management that changes are needed to existing policies
D. notify the user community that non-compliant account will be required to use the new process

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 513
A company has noticed a recent increase in machines that have been exploited using vulnerabilities via third party software. Which of the following would BEST help the company reduce the likelihood of vulnerabilities within the software creating future problems?

A. Patch management
B. Host-based firewalls
C. Antivirus software
D. White-listing applications

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 514
The content of a document that is routinely used by several employees and contains confidential information has been changed. While investigating the issue, it is discovered that payment information for all teh company's clients has been removed from the document. Which of the following could be used to determine who changed the information?

A. Audit logs
B. Server baseline
C. Document hashing
D. Change management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 515
A datacenter has suffered repeated burglaries that lead to equipment theft and arson. In the past, the thieves have demonstrated a determination to bypass any installed safeguards. After mantraps had been installed to prevent tailgating, the thieves crashed through the wall of the datacenter with a vehicle after normal business hours. Which of teh following options could further improve the physical safety and security of the datacenter? (select TWO).

A. Cipher locks
B. CCTV
C. Escape routes
D. K-rated fencing
E. FM200 fire suppression

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 516
A company uses digital signatures to sign contracts. The company requires external entities to create an account with a third-party digital signature provider and sign an agreement stating they will protect the account from unauthorized access. Which of the following security goals is the company trying to address in the

given scenario?

A. Availability
B. Non-repudiation
C. Authentication
D. Confidentiality
E. Due diligence

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 517
A CA is attempting to publicize the acceptable parameters for certificate signing requests. Which of the following should a server administrator use to fulfill the requirements of the CA?

A. Interconnection security agreement
B. Certificate templates
C. Client-side certificates
D. Software token

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 518
A security administrator is troubleshooting a network connectivity issue. The administrator believes that a router's ACL may be blocking network traffic to a remote network. Which of the following, if enabled, would confirm the administrator's theory by providing helpful feedback?

A. DNS
B. NAT
C. NetBIOS

D. ICMP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 519
A network administrator discovers that telnet was enabled on the company's Human Resources (HR) payroll server and that someone outside the HR subnet has been attempting to log into the server. The network administrator has disabled telnet on the payroll server. Which of the following is a method of tracking attempts to log onto telnet without exposing important telnet data.

A. Banner grabbing
B. Active port monitors
C. Honeypot
D. Passive IPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Active Ports is a tool that monitors all open TCP and UDP ports on a local computer. You can watch which process has opened which port, because the program maps ports to its owning application. Active Ports 1.4 also displays a local and remote IP address for each connection and allows you to terminate the owning process. In this way, this program can help you to detect and stop trojans and other malicious programs. When you run Active Ports 1.4, it scans all your open ports, and displays the following information about them: Process Name, PID, Local IP, Local Port, Remote IP, Remote Port, State, Protocol and Path. If you want to know more about certain process, you can click on it and press the "Query Names" button. You will then see the name of the server trying to reach your IP. If you don´t trust that process, you can terminate it through this program, pressing the "Terminate Process" button. You can also export the list of processes to a .csv file, in order to keep or give someone a detailed report about your port usage.

QUESTION 520
After a private key has been compromised, an administrator realized that downloading a CRL once per day was not effective. The administrator wants to immediately revoke certificates. Which of the following should the administrator investigate?

A. CSR
B. PKI
C. IdP

D. OCSP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 521
An organization's security policy requires secure file transfers to and from internal hosts. An employee is attempting to upload a file using an unsecure method to a Linux-based dedicated file server and fails. Which of the following should the employee use to transfer the file?

A. FTP
B. HTTPS
C. SSL
D. SCP
E. TLS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 522
A security administrator wants to implement a multi-factor, location-based authentication system. The authentication system must incorporate something unique about each user. Which of the following are user authentication factors that can be used by the system? (Select THREE).

A. IP address
B. Employee ID
C. Username
D. Unique identification number
E. Keyboard timing
F. Password

Correct Answer: AEF
Section: (none)

Explanation

Explanation/Reference:

QUESTION 523
Ann, a security administrator, needs to implement a transport encryption solution that will enable her to detect attempts to sniff packets. Which of the following could be implemented?

A. Eliptical curve algorithms
B. Ephemeral keys
C. Quantum cryptography
D. Steganography

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 524
An administrator must change the IP address of the corporate web server. Since this is a critical web server, downtime must be kept to a minimum. To minimize downtime as much as possible, which of the following DNS properties should be changed well before the actual IP change?

A. PTR
B. TTL
C. SRV
D. A

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 525
A security administrator is seeking a secure way to send emails to a subcontractor without requiring user action. Which of the following would BEST provide security between email gateways?

A. SSL
B. PGP
C. HTTPS
D. S/MIME
E. TLS
F. SSH

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 526
A company has implemented a public-facing authentication system that uses PKI and extended attributes to allow third-party, web-based application integration. Which of the following is this an example of? (Select THREE).

A. Federation
B. Two-factor authentication
C. Transitive trust
D. Trusted OS
E. Single sign-on
F. TOTP
G. MAC

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 527
An administrator wants to configure the security setting in the AD domain to force users to use a unique new password at least ten times before a password can be reused. Which of the following security controls is the administrator enforcing?

A. Password age
B. Password expiration
C. Password history
D. Password complexity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 528
A security manager needs to implement a backup solution as part of the disaster recovery plan. The system owners have indicated that the business cannot afford to lose more than a day of transactions following an event where data would have been restored. The security manager should set a value of 24 hours for the:

A. recovery time objective
B. service level agreement
C. recovery point objective
D. system backup window
E. disaster recovery plan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 529
A security administrator has been tasked to only allow traffic from HTTPS and SSH on a segregated network that contains sensitive information. Which of the following MUST be completed on the firewall?

A. Allow 22, 143
B. Allow 80, 21 and Deny All
C. Allow 443, 22 and Deny All
D. Allow 443, 80

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 530

A system administrator wants to ensure that only authorized devices can connect to the wired and wireless corporate system. Unauthorized devices should be automatically be placed on a guest network. Which of the following MUST be implemented to support these requirements? (Select TWO).

A. Port security
B. 802.1X
C. Proxy
D. VLAN
E. NAT

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference: