Exam A

QUESTION 1
DRAG DROP

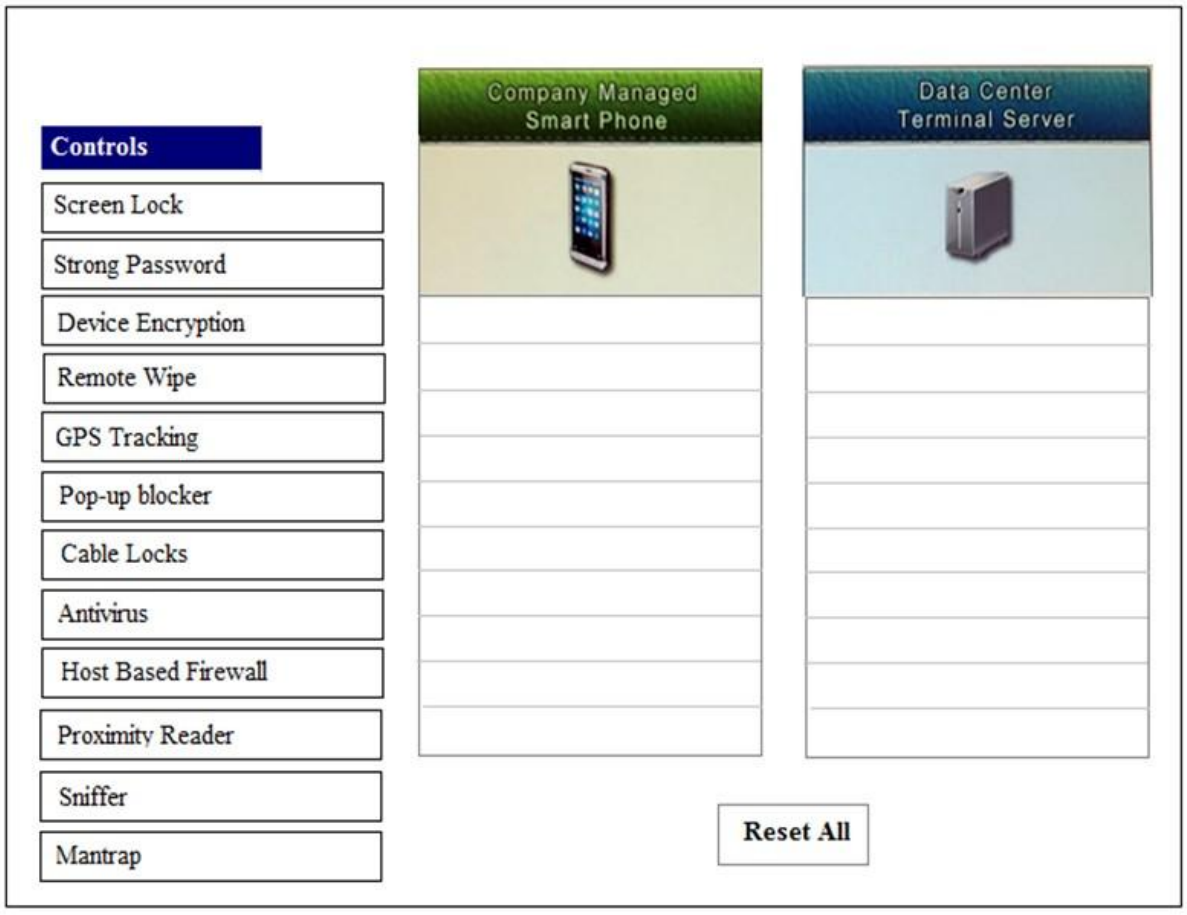
A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center.

INSTRUCTIONS
Drag and drop the applicable controls to each asset type.

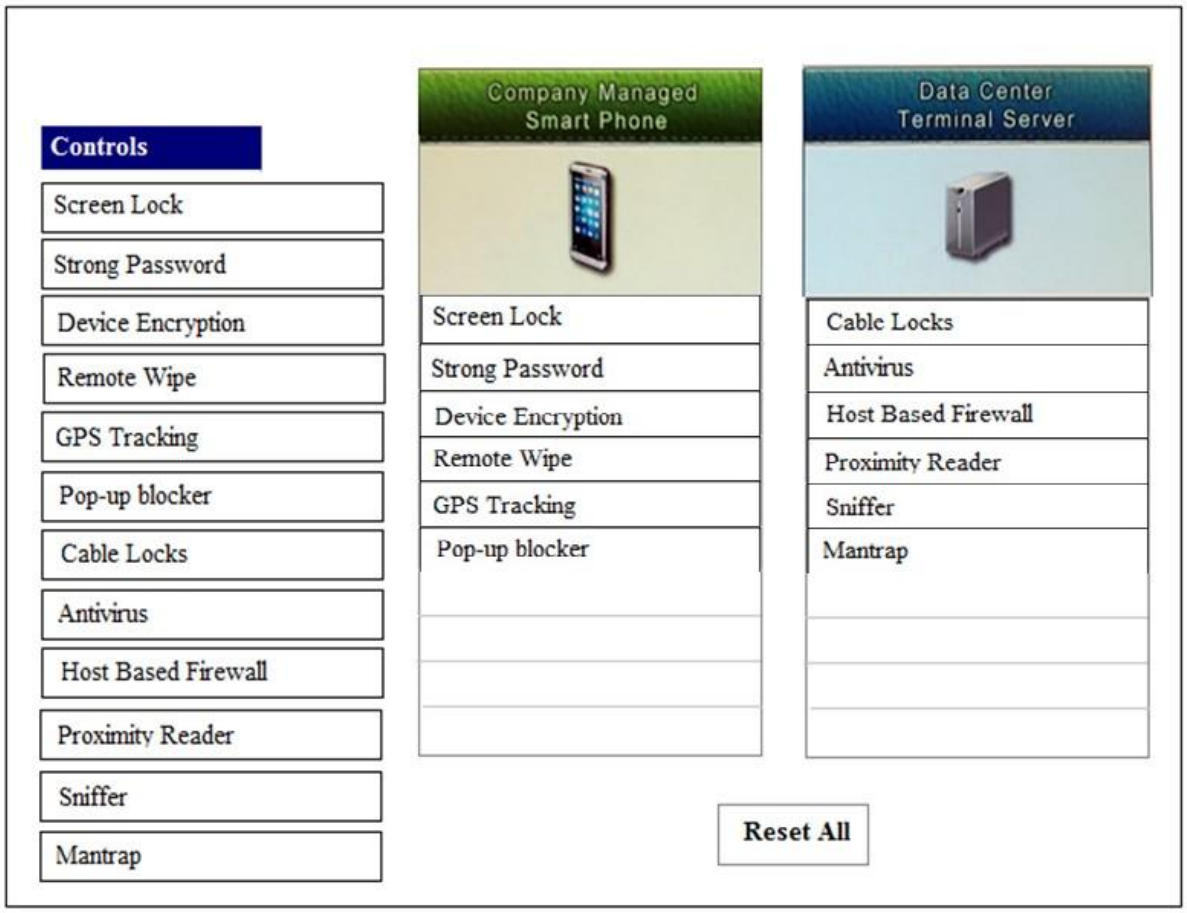
Controls can be used multiple times and not all placeholders need to be filled.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:



Answer:



Explanation

Explanation/Reference:

QUESTION 2
HOTSPOT

Select the appropriate attack from each drop down list to label the corresponding illustrated attack.

Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

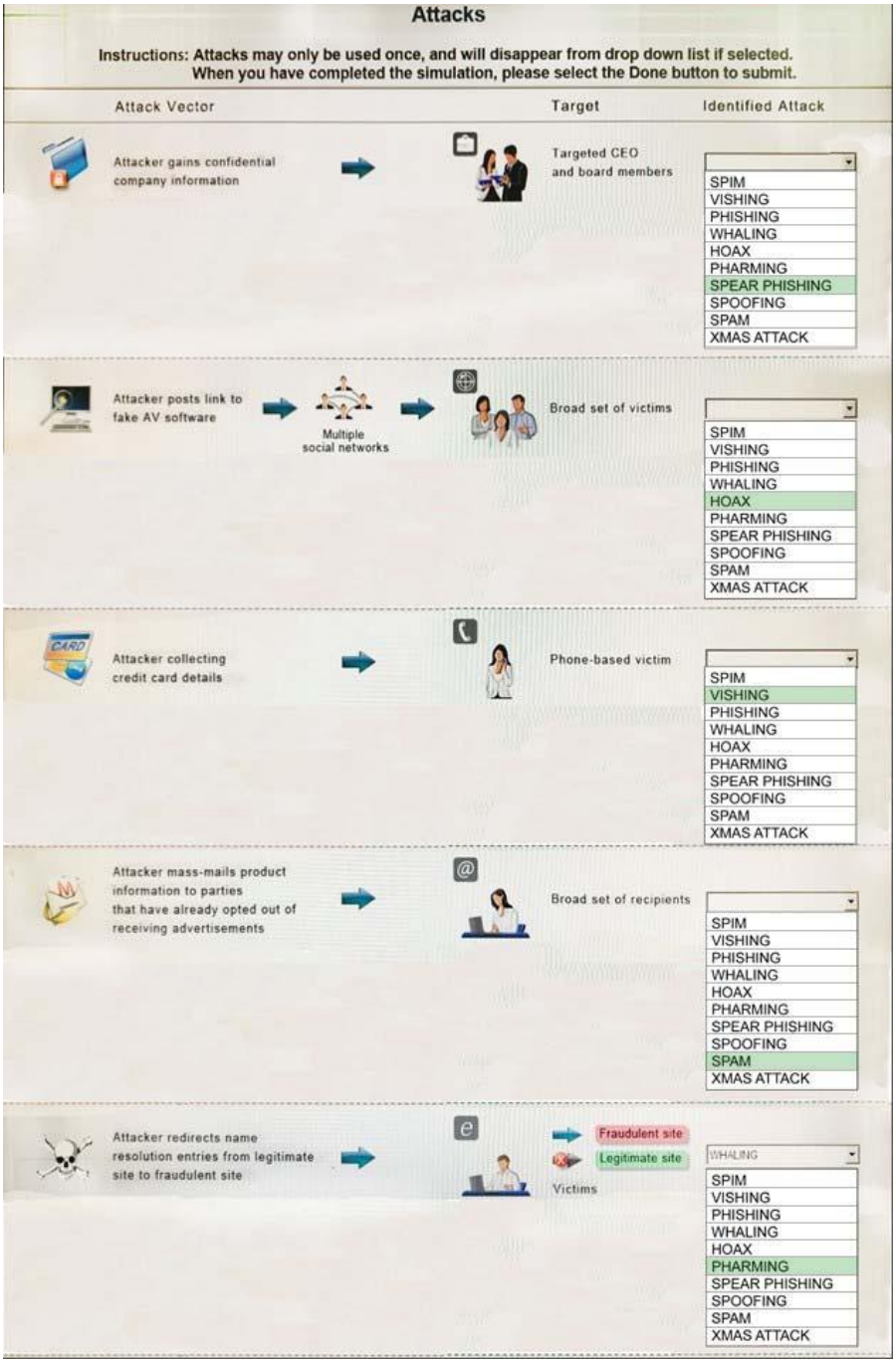
Hot Area:

Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Attack Vector	Target	Identified Attack
Attacker gains confidential company information	Targeted CEO and board members	SPIM, VISHING, PHISHING, WHALING, HOAX, PHARMING, SPEAR PHISHING, SPOOFING, SPAM, XMAS ATTACK
Attacker posts link to fake AV software → Multiple social networks	Broad set of victims	SPIM, VISHING, PHISHING, WHALING, HOAX, PHARMING, SPEAR PHISHING, SPOOFING, SPAM, XMAS ATTACK
Attacker collecting credit card details	Phone-based victim	SPIM, VISHING, PHISHING, WHALING, HOAX, PHARMING, SPEAR PHISHING, SPOOFING, SPAM, XMAS ATTACK
Attacker mass-mails product information to parties that have already opted out of receiving advertisements	Broad set of recipients	SPIM, VISHING, PHISHING, WHALING, HOAX, PHARMING, SPEAR PHISHING, SPOOFING, SPAM, XMAS ATTACK
Attacker redirects name resolution entries from legitimate site to fraudulent site	Fraudulent site / Legitimate site / Victims	WHALING; SPIM, VISHING, PHISHING, WHALING, HOAX, PHARMING, SPEAR PHISHING, SPOOFING, SPAM, XMAS ATTACK

Answer:



Explanation

Explanation/Reference:

Explanation:

1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

2: The Hoax in this question is designed to make people believe that the fake AV (anti- virus) software is genuine.

3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

4: Email spam, also referred to as junk email, is unsolicited messages sent in bulk by email (spamming).

5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

References:
http://searchsecurity.techtarget.com/definition/spear-phishing
http://www.webopedia.com/TERM/V/vishing.html
http://www.webopedia.com/TERM/P/phishing.html
http://www.webopedia.com/TERM/P/pharming.html

QUESTION 3
DRAG DROP

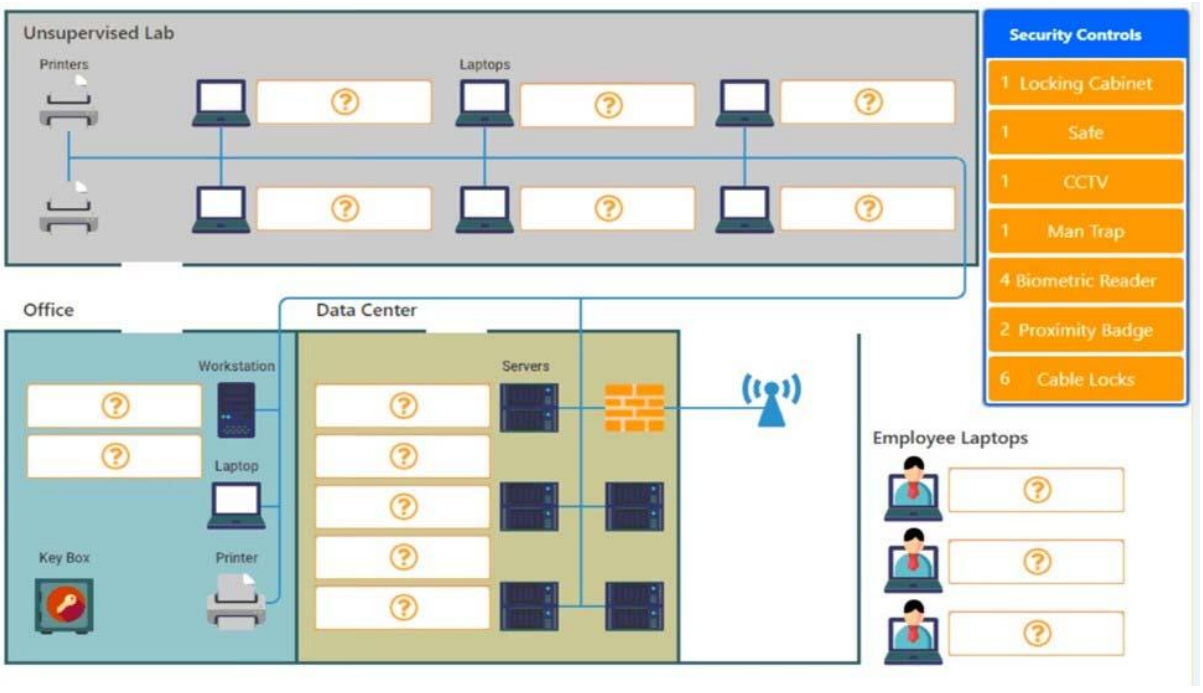
You have been tasked with designing a security plan for your company.

INSTRUCTIONS
Drag and drop the appropriate security controls on the floor plan.

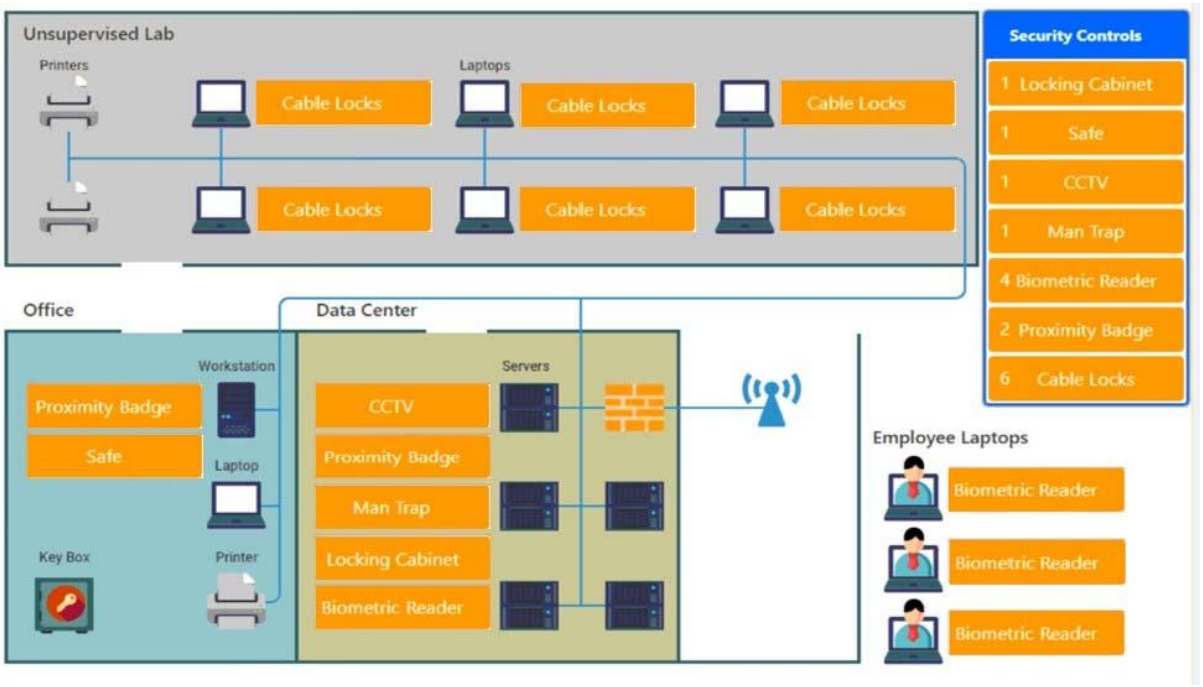
All objects must be used and all place holders must be filled. Order does not matter.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:



Answer:



Explanation

Explanation/Reference:
Explanation:
Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away
Proximity badge + reader
Safe is a hardware/physical security measure
Mantrap can be used to control access to sensitive areas.
CCTV can be used as video surveillance.
Biometric reader can be used to control and prevent unauthorized access.
Locking cabinets can be used to protect backup media, documentation and other physical artefacts.

QUESTION 4
Which of the following would a security specialist be able to determine upon examination of a server's certificate?

A. CA public key
B. Server private key
C. CSR
D. OID

Answer: D

Explanation

Explanation/Reference:

QUESTION 5
A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.0:6666. Which of the following should the security analyst do to determine if the compromised system still has an active connection?

A. tracert
B. netstat
C. ping
D. nslookup

Answer: B

Explanation

Explanation/Reference:

QUESTION 6
Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?

A. Shibboleth
B. RADIUS federation
C. SAML
D. OAuth
E. OpenID connect

Answer: B

Explanation

Explanation/Reference:
Explanation: http://archive.oreilly.com/pub/a/wireless/2005/01/01/authentication.html

QUESTION 7
Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?

A. Sustainability
B. Homogeneity
C. Resiliency
D. Configurability

Answer: C

Explanation

Explanation/Reference:

QUESTION 8
In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?

A. Elasticity
B. Scalability
C. High availability

D. Redundancy

Answer: A

Explanation

Explanation/Reference:
Explanation:
Elasticity is defined as “the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible”.

QUESTION 9
A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

A. PFX
B. PEM
C. DER
D. CER

Answer: B

Explanation

Explanation/Reference:

QUESTION 10
Which of the following attacks specifically impact data availability?

A. DDoS
B. Trojan
C. MITM
D. Rootkit

Answer: A

Explanation

Explanation/Reference:
Reference: https://www.netscout.com/what-is-ddos

QUESTION 11
A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Choose two.)

A. Generate an X.509-compliant certificate that is signed by a trusted CA.
B. Install and configure an SSH tunnel on the LDAP server.
C. Ensure port 389 is open between the clients and the servers using the communication.
D. Ensure port 636 is open between the clients and the servers using the communication.
E. Remote the LDAP directory service role from the server.

Answer: AD

Explanation

Explanation/Reference:

QUESTION 12
Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market?

A. Competitor
B. Hacktivist
C. Insider
D. Organized crime.

Answer: A

Explanation

Explanation/Reference:

QUESTION 13
A penetration tester is crawling a target website that is available to the public. Which of the following represents the actions the penetration tester is performing?

A. URL hijacking
B. Reconnaissance
C. White box testing
D. Escalation of privilege

Answer: B

Explanation

Explanation/Reference:

QUESTION 14
Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Choose two.)

A. Rainbow table attacks greatly reduce compute cycles at attack time.
B. Rainbow tables must include precomputed hashes.
C. Rainbow table attacks do not require access to hashed passwords.
D. Rainbow table attacks must be performed on the network.
E. Rainbow table attacks bypass maximum failed login restrictions.

Answer: BE

Explanation

Explanation/Reference:

QUESTION 15
Which of the following best describes routine in which semicolons, dashes, quotes, and commas are removed from a string?

A. Error handling to protect against program exploitation
B. Exception handling to protect against XSRF attacks.
C. Input validation to protect against SQL injection.
D. Padding to protect against string buffer overflows.

Answer: C

Explanation

Explanation/Reference:

QUESTION 16
A security analyst wishes to increase the security of an FTP server. Currently, all traffic to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modern FTP client software.
The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections. Which of the following would BEST accomplish these goals?

A. Require the SFTP protocol to connect to the file server.
B. Use implicit TLS on the FTP server.
C. Use explicit FTPS for connections.
D. Use SSH tunneling to encrypt the FTP traffic.

Answer: C

Explanation

Explanation/Reference:

QUESTION 17
Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

A. The recipient can verify integrity of the software patch.
B. The recipient can verify the authenticity of the site used to download the patch.
C. The recipient can request future updates to the software using the published MD5 value.
D. The recipient can successfully activate the new software patch.

Answer: A

Explanation

Explanation/Reference:

QUESTION 18
Refer to the following code:

```
public class rainbow {
     public static void main (String [] args) {
          object blue = null;
          blue.hashcode (); }
}
```

Which of the following vulnerabilities would occur if this is executed?

A. Page exception
B. Pointer deference
C. NullPointerException
D. Missing null check

Answer: D

Explanation

Explanation/Reference:

QUESTION 19
Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened. The network and security teams perform the following actions:

- Shut down all network shares.
- Run an email search identifying all employees who received the malicious message.
- Reimage all devices belonging to users who opened the attachment.

Next, the teams want to re-enable the network shares. Which of the following BEST describes this phase of the incident response process?

A. Eradication
B. Containment
C. Recovery
D. Lessons learned

Answer: C

Explanation

Explanation/Reference:

QUESTION 20
An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

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

Answer: A

Explanation

Explanation/Reference:

QUESTION 21
Which of the following types of keys is found in a key escrow?

A. Public
B. Private
C. Shared
D. Session

Answer: B

Explanation

Explanation/Reference:
Explanation:
https://www.professormesser.com/security-plus/sy0-401/key-escrow-3/

QUESTION 22
A security analyst is reviewing the following output from an IPS:

```
[**] [1:2467:7] EXPLOIT IGMP IGAP message overflow attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
07/30-19:45:02.238185 250.19.18.71 -> 250.19.18.22
IGMP TTL:255 TOS: 0x0 ID: 9742 IpLen:20 DgmLen: 502 MF
Frag offset: 0x1FFF Frag Size: 0x01E2
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0367]
```

Given this output, which of the following can be concluded? (Choose two.)

A. The source IP of the attack is coming from 250.19.18.22.
B. The source IP of the attack is coming from 250.19.18.71.
C. The attacker sent a malformed IGAP packet, triggering the alert.
D. The attacker sent a malformed TCP packet, triggering the alert.
E. The TTL value is outside of the expected range, triggering the alert.

Answer: BC

Explanation

Explanation/Reference:

QUESTION 23
Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords. Which of the following technical controls would help prevent these policy violations? (Choose two.)

A. Password expiration
B. Password length

C. Password complexity
D. Password history
E. Password lockout

Answer: CD

Explanation

Explanation/Reference:

QUESTION 24
Which of the following types of cloud infrastructures would allow several organizations with similar structures and interests to realize the benefits of shared storage and resources?

A. Private
B. Hybrid
C. Public
D. Community

Answer: D

Explanation

Explanation/Reference:

QUESTION 25
A company is currently using the following configuration:

- IAS server with certificate-based EAP-PEAP and MSCHAP
- Unencrypted authentication via PAP

A security administrator needs to configure a new wireless setup with the following configurations:

- PAP authentication method
- PEAP and EAP provide two-factor authentication

Which of the following forms of authentication are being used? (Choose two.)

A. PAP
B. PEAP
C. MSCHAP
D. PEAP- MSCHAP
E. EAP
F. EAP-PEAP

Answer: AC

Explanation

Explanation/Reference:

QUESTION 26

An auditor wants to test the security posture of an organization by running a tool that will display the following:

```
JIMS            <00> UNIQUE    Registered
WORKGROUP       <00> GROUP     Registered
JIMS            <00> UNIQUE    Registered
```

Which of the following commands should be used?

A. nbtstat
B. nc
C. arp
D. ipconfig

Answer: A

Explanation

Explanation/Reference:

QUESTION 27
A company determines that it is prohibitively expensive to become compliant with new credit card regulations. Instead, the company decides to purchase insurance to cover the cost of any potential loss. Which of the following is the company doing?

A. Transferring the risk
B. Accepting the risk
C. Avoiding the risk
D. Migrating the risk

Answer: A

Explanation

Explanation/Reference:

QUESTION 28
A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:

- There is no standardization.
- Employees ask for reimbursement for their devices.
- Employees do not replace their devices often enough to keep them running efficiently.
- The company does not have enough control over the devices.

Which of the following is a deployment model that would help the company overcome these problems?

A. BYOD
B. VDI
C. COPE
D. CYOD

Answer: D

Explanation

Explanation/Reference:

QUESTION 29
A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack. News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong?

A. SoC
B. ICS
C. IoT
D. MFD

Answer: C

Explanation

Explanation/Reference:

QUESTION 30
Users report the following message appears when browsing to the company's secure site: This website cannot be trusted. Which of the following actions should a security analyst take to resolve these messages? (Choose two.)

A. Verify the certificate has not expired on the server.
B. Ensure the certificate has a .pfx extension on the server.
C. Update the root certificate into the client computer certificate store.
D. Install the updated private key on the web server.
E. Have users clear their browsing history and relaunch the session.

Answer: AC

Explanation

Explanation/Reference:

QUESTION 31
When trying to log onto a company's new ticketing system, some employees receive the following message: Access denied: too many concurrent sessions. The ticketing system was recently installed on a small VM with only the recommended hardware specifications. Which of the following is the MOST likely cause for this error message?

A. Network resources have been exceeded.
B. The software is out of licenses.
C. The VM does not have enough processing power.
D. The firewall is misconfigured.

Answer: C

Explanation

Explanation/Reference:

QUESTION 32
Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone. Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Choose two.)

A. Near-field communication.
B. Rooting/jailbreaking
C. Ad-hoc connections
D. Tethering
E. Sideloading

Answer: BE

Explanation

Explanation/Reference:

QUESTION 33
Which of the following can be provided to an AAA system for the identification phase?

A. Username
B. Permissions
C. One-time token
D. Private certificate

Answer: A

Explanation

Explanation/Reference:

QUESTION 34
Which of the following implements two-factor authentication?

A. A phone system requiring a PIN to make a call
B. At ATM requiring a credit card and PIN
C. A computer requiring username and password
D. A datacenter mantrap requiring fingerprint and iris scan

Answer: B

Explanation

Explanation/Reference:

QUESTION 35
Malicious traffic from an internal network has been detected on an unauthorized port on an application server.

Which of the following network-based security controls should the engineer consider implementing?

A. ACLs
B. HIPS
C. NAT
D. MAC filtering

Answer: A

Explanation

Explanation/Reference:

QUESTION 36
A network administrator wants to implement a method of securing internal routing. Which of the following should the administrator implement?

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

Answer: C

Explanation

Explanation/Reference:

QUESTION 37
A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

- All access must be correlated to a user account.
- All user accounts must be assigned to a single individual.
- User access to the PHI data must be recorded.
- Anomalies in PHI data access must be reported.
- Logs and records cannot be deleted or modified.

Which of the following should the administrator implement to meet the above requirements? (Choose three.)

A. Eliminate shared accounts.
B. Create a standard naming convention for accounts.
C. Implement usage auditing and review.
D. Enable account lockout thresholds.
E. Copy logs in real time to a secured WORM drive.
F. Implement time-of-day restrictions.
G. Perform regular permission audits and reviews.

Answer: ACE

Explanation

Explanation/Reference:

QUESTION 38
Which of the following encryption methods does PKI typically use to securely protect keys?

A. Elliptic curve
B. Digital signatures
C. Asymmetric
D. Obfuscation

Answer: C

Explanation

Explanation/Reference:

QUESTION 39
An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

A. False negative
B. True negative
C. False positive
D. True positive

Answer: C

Explanation

Explanation/Reference:

QUESTION 40
An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.
The IT security department finds the following security configuration for the accounts payable module:

- New Vendor Entry – Required Role: Accounts Payable Clerk
- New Vendor Approval – Required Role: Accounts Payable Clerk
- Vendor Payment Entry – Required Role: Accounts Payable Clerk
- Vendor Payment Approval – Required Role: Accounts Payable Manager

Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?

A.
```
New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable
Manager
```

B. New Vendor Entry – Required Role: Accounts Payable Manager
New Vendor Approval – Required Role: Accounts Payable Clerk
Vendor Payment Entry – Required Role: Accounts Payable Clerk
Vendor Payment Approval – Required Role: Accounts Payable Manager

C. New Vendor Entry – Required Role: Accounts Payable Clerk
New Vendor Approval – Required Role: Accounts Payable Clerk
Vendor Payment Entry – Required Role: Accounts Payable Manager
Vendor Payment Approval – Required Role: Accounts Payable Manager

D. New Vendor Entry – Required Role: Accounts Payable Clerk
New Vendor Approval – Required Role: Accounts Payable Manager
Vendor Payment Entry – Required Role: Accounts Payable Manager
Vendor Payment Approval – Required Role: Accounts Payable Manager

Answer: A

Explanation

Explanation/Reference:

QUESTION 41
A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?

A. Time-of-day restrictions
B. Permission auditing and review
C. Offboarding
D. Account expiration

Answer: C

Explanation

Explanation/Reference:

QUESTION 42
A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

A. 1
B. 2
C. 3

D. 4

Answer: B

Explanation

Explanation/Reference:

QUESTION 43
Which of the following security controls does an iris scanner provide?

A. Logical
B. Administrative
C. Corrective
D. Physical
E. Detective
F. Deterrent

Answer: D

Explanation

Explanation/Reference:

QUESTION 44
As part of a new industry regulation, companies are required to utilize secure, standardized OS settings. A technical must ensure the OS settings are hardened. Which of the following is the BEST way to do this?

A. Use a vulnerability scanner.
B. Use a configuration compliance scanner.
C. Use a passive, in-line scanner.
D. Use a protocol analyzer.

Answer: B

Explanation

Explanation/Reference:

QUESTION 45
A user has attempted to access data at a higher classification level than the user's account is currently authorized to access. Which of the following access control models has been applied to this user's account?

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

Answer: A

Explanation

Explanation/Reference:

QUESTION 46
A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

A. An attacker can access and change the printer configuration.
B. SNMP data leaving the printer will not be properly encrypted.
C. An MITM attack can reveal sensitive information.
D. An attacker can easily inject malicious code into the printer firmware.
E. Attackers can use the PCL protocol to bypass the firewall of client computers.

Answer: B

Explanation

Explanation/Reference:

QUESTION 47
An organization finds that most help desk calls are regarding account lockout due to a variety of applications running on different systems. Management is looking for a solution to reduce the number of account lockouts while improving security. Which of the following is the BEST solution for this organization?

A. Create multiple application accounts for each user.
B. Provide secure tokens.
C. Implement SSO.
D. Utilize role-based access control.

Answer: C

Explanation

Explanation/Reference:

QUESTION 48
A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

Hostname	IP address	MAC	MAC filter
DadPC	192.168.1.10	00:1D:1A:44:17:B5	On
MomPC	192.168.1.15	21:13:D6:C5:42:A2	Off
JuniorPC	192.168.2.16	42:A7:D1:25:11:52	On
Unknown	192.168.1.18	10:B3:22:1A:FF:21	Off

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

A. Apply MAC filtering and see if the router drops any of the systems.
B. Physically check each of the authorized systems to determine if they are logged onto the network.

C. Deny the “unknown” host because the hostname is not known and MAC filtering is not applied to this host.
D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

Answer: B

Explanation

Explanation/Reference:

QUESTION 49
When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Choose two.)

A. USB-attached hard disk
B. Swap/pagefile
C. Mounted network storage
D. ROM
E. RAM

Answer: BE

Explanation

Explanation/Reference:

QUESTION 50
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

Answer: A

Explanation

Explanation/Reference:

QUESTION 51
An attacker compromises a public CA and issues unauthorized X.509 certificates for Company.com. In the future, Company.com wants to mitigate the impact of similar incidents. Which of the following would assist Company.com with its goal?

A. Certificate pinning
B. Certificate stapling
C. Certificate chaining
D. Certificate with extended validation

Answer: A

Explanation

Explanation/Reference:

QUESTION 52
A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials. Which of the following account types is the systems administrator using?

A. Shared account
B. Guest account
C. Service account
D. User account

Answer: C

Explanation

Explanation/Reference:

QUESTION 53
A security administrator has found a hash in the environment known to belong to malware. The administrator then finds this file to be in in the preupdate area of the OS, which indicates it was pushed from the central patch system.

File: winx86_adobe_flash_upgrade.exe
Hash: 99ac28bede43ab869b853ba62c4ea243

The administrator pulls a report from the patch management system with the following output:

Install Date	Package Name	Target Devices	Hash
10/10/2017	java_11.2_x64.exe	HQ PC's	01ab28bbde63aa879b35bba62cdes283
10/10/2017	winx86_adobe_flash_upgrade.exe	HQ PC's	99ac28bede43ab869b853ba62c4ea243

Given the above outputs, which of the following MOST likely happened?

A. The file was corrupted after it left the patch system.
B. The file was infected when the patch manager downloaded it.
C. The file was not approved in the application whitelist system.
D. The file was embedded with a logic bomb to evade detection.

Answer: B

Explanation

Explanation/Reference:

QUESTION 54
A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network. Which of the following should be implemented in the administrator does not want to provide the wireless password or he certificate to the employees?

A. WPS
B. 802.1x
C. WPA2-PSK
D. TKIP

Answer: A

Explanation

Explanation/Reference:

QUESTION 55
When connected to a secure WAP, which of the following encryption technologies is MOST likely to be configured when connecting to WPA2-PSK?

A. DES
B. AES
C. MD5
D. WEP

Answer: B

Explanation

Explanation/Reference:

QUESTION 56
A company has a data classification system with definitions for "Private" and "Public". The company's security policy outlines how data should be protected based on type. The company recently added the data type "Proprietary".

Which of the following is the MOST likely reason the company added this data type?

A. Reduced cost
B. More searchable data
C. Better data classification
D. Expanded authority of the privacy officer

Answer: C

Explanation

Explanation/Reference:

QUESTION 57
When configuring settings in a mandatory access control environment, which of the following specifies the subjects that can access specific data objects?

A. Owner
B. System
C. Administrator

D. User

Answer: C

Explanation

Explanation/Reference:

QUESTION 58
A high-security defense installation recently begun utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation. Which of the following types of controls does this BEST describe?

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

Answer: A

Explanation

Explanation/Reference:

QUESTION 59
A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are MOST likely occurring? (Select two.)

A. Replay
B. Rainbow tables
C. Brute force
D. Pass the hash
E. Dictionary

Answer: CE

Explanation

Explanation/Reference:

QUESTION 60
Ann. An employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:

- Slow performance
- Word documents, PDFs, and images no longer opening
- A pop-up

Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?

A. Spyware
B. Crypto-malware
C. Rootkit
D. Backdoor

Answer: D

Explanation

Explanation/Reference:

QUESTION 61
A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

A. Obtain a list of passwords used by the employee.
B. Generate a report on outstanding projects the employee handled.
C. Have the employee surrender company identification.
D. Have the employee sign an NDA before departing.

Answer: C

Explanation

Explanation/Reference:

QUESTION 62
A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment?

A. A perimeter firewall and IDS
B. An air gapped computer network
C. A honeypot residing in a DMZ
D. An ad hoc network with NAT
E. A bastion host

Answer: B

Explanation

Explanation/Reference:

QUESTION 63
Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production?

A. Roll back changes in the test environment
B. Verify the hashes of files
C. Archive and compress the files
D. Update the secure baseline

Answer: B

Explanation

Explanation/Reference:

QUESTION 64
A user clicked an email link that led to a website than infected the workstation with a virus. The virus encrypted all the network shares to which the user had access. The virus was not deleted or blocked by the company's email filter, website filter, or antivirus. Which of the following describes what occurred?

A. The user's account was over-privileged.
B. Improper error handling triggered a false negative in all three controls.
C. The email originated from a private email server with no malware protection.
D. The virus was a zero-day attack.

Answer: D

Explanation

Explanation/Reference:

QUESTION 65
An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment of DNSSEC at the organization?

A. LDAP
B. TPM
C. TLS
D. SSL
E. PKI

Answer: C

Explanation

Explanation/Reference:

QUESTION 66
A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm?

A. Vulnerability scanning
B. Penetration testing
C. Application fuzzing
D. User permission auditing

Answer: A

Explanation

Explanation/Reference:

QUESTION 67
An administrator is replacing a wireless router. The configuration of the old wireless router was not documented before it stopped functioning. The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard. Which of the following configuration options should the administrator select for the new wireless router?

A. WPA+CCMP
B. WPA2+CCMP
C. WPA+TKIP
D. WPA2+TKIP

Answer: C

Explanation

Explanation/Reference:

QUESTION 68
An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call. The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

A. Give the application team administrator access during off-hours.
B. Disable other critical applications before granting the team access.
C. Give the application team read-only access.
D. Share the account with the application team.

Answer: C

Explanation

Explanation/Reference:

QUESTION 69
Which of the following cryptographic attacks would salting of passwords render ineffective?

A. Brute force
B. Dictionary
C. Rainbow tables
D. Birthday

Answer: C

Explanation

Explanation/Reference:

QUESTION 70
A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is

mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

A. LDAP services
B. Kerberos services
C. NTLM services
D. CHAP services

Answer: B

Explanation

Explanation/Reference:
Explanation:
Only Kerberos that can do Mutual Auth and Delegation.

QUESTION 71
Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Which of the following should be used to sign the user's certificates?

A. RA
B. CA
C. CRL
D. CSR

Answer: B

Explanation

Explanation/Reference:

QUESTION 72
Which of the following attack types BEST describes a client-side attack that is used to manipulate an HTML iframe with JavaScript code via a web browser?

A. Buffer overflow
B. MITM
C. XSS
D. SQLi

Answer: C

Explanation

Explanation/Reference:

QUESTION 73
An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT?

A. Capture and document necessary information to assist in the response.
B. Request the user capture and provide a screenshot or recording of the symptoms.
C. Use a remote desktop client to collect and analyze the malware in real time.

D. Ask the user to back up files for later recovery.

Answer: A

Explanation

Explanation/Reference:

QUESTION 74
A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours. Which of the following types of malware is MOST likely causing this issue?

A. Botnet
B. Ransomware
C. Polymorphic malware
D. Armored virus

Answer: A

Explanation

Explanation/Reference:

QUESTION 75
Which of the following technologies employ the use of SAML? (Choose two.)

A. Single sign-on
B. Federation
C. LDAP
D. Secure token
E. RADIUS

Answer: AB

Explanation

Explanation/Reference:

QUESTION 76
Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?

A. Privilege escalation
B. Pivoting
C. Process affinity
D. Buffer overflow

Answer: A

Explanation

Explanation/Reference:

QUESTION 77
After a user reports stow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.

The systems administrator reviews the output below:

```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address     Foreign Address        State
TCP   0.0.0.0:135       0.0.0.0:0              LISTENING        RpcSs [svchost.exe]
TCP   0.0.0.0:445       0.0.0.0:0              LISTENING        [svchost.exe]

TCP   192.168.1.10:5000 10.37.213.20           ESTABLISHED      winserver.exe
UDP   192.168.1.10:1900 *.*                                     SSDPSVR
```

Based on the above information, which of the following types of malware was installed on the user's computer?

A. RAT
B. Keylogger
C. Spyware
D. Worm
E. Bot

Answer: A

Explanation

Explanation/Reference:

QUESTION 78
Which of the following network vulnerability scan indicators BEST validates a successful, active scan?

A. The scan job is scheduled to run during off-peak hours.
B. The scan output lists SQL injection attack vectors.
C. The scan data identifies the use of privileged-user credentials.
D. The scan results identify the hostname and IP address.

Answer: B

Explanation

Explanation/Reference:

QUESTION 79
An analyst wants to implement a more secure wireless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?

A. PEAP
B. EAP
C. WPA2
D. RADIUS

Answer: A

Explanation

Explanation/Reference:
Explanation:
EAP by itself is only an authentication framework.
PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated. The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel is protected. As a result, when EAP messages are able to be discovered in the "clear" they do not provide the protection that was assumed when the protocol was originally authored.
PEAP, EAP-TTLS, and EAP-TLS "protect" inner EAP authentication within SSL/TLS sessions.

QUESTION 80
When systems, hardware, or software are not supported by the original vendor, it is a vulnerability known as:

A. system sprawl
B. end-of-life systems
C. resource exhaustion
D. a default configuration

Answer: B

Explanation

Explanation/Reference:

QUESTION 81
A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords. The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Choose two.)

A. The portal will function as a service provider and request an authentication assertion.
B. The portal will function as an identity provider and issue an authentication assertion.
C. The portal will request an authentication ticket from each network that is transitively trusted.
D. The back-end networks will function as an identity provider and issue an authentication assertion.
E. The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store.
F. The back-end networks will verify the assertion token issued by the portal functioning as the identity provider.

Answer: CD

Explanation

Explanation/Reference:

QUESTION 82
Which of the following is the BEST explanation of why control diversity is important in a defense-in-depth architecture?

A. Social engineering is used to bypass technical controls, so having diversity in controls minimizes the risk of demographic exploitation
B. Hackers often impact the effectiveness of more than one control, so having multiple copies of individual controls provides redundancy
C. Technical exploits to defeat controls are released almost every day; control diversity provides overlapping protection.
D. Defense-in-depth relies on control diversity to provide multiple levels of network hierarchy that allow user domain segmentation

Answer: D

Explanation

Explanation/Reference:

QUESTION 83
A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees. Which of the following would provide strong security and backward compatibility when accessing the wireless network?

A. Open wireless network and SSL VPN
B. WPA using a preshared key
C. WPA2 using a RADIUS back-end for 802.1x authentication
D. WEP with a 40-bit key

Answer: B

Explanation

Explanation/Reference:

QUESTION 84
An information security specialist is reviewing the following output from a Linux server.

```
user@server:~$ crontab -1
5 * * * *  /usr/local/bin/backup.sh
user@server: ~$ cat /usr/local/bin/backup.sh
#!/bin/bash
if ! grep - - quiet joeuser/etc/passwd
then rm –rf /
fi
```

Based on the above information, which of the following types of malware was installed on the server?

A. Logic bomb
B. Trojan
C. Backdoor
D. Ransomware
E. Rootkit

Answer: A

Explanation

Explanation/Reference:

QUESTION 85
In terms of encrypting data, which of the following is BEST described as a way to safeguard password data by adding random data to it in storage?

A. Using salt
B. Using hash algorithms
C. Implementing elliptical curve
D. Implementing PKI

Answer: A

Explanation

Explanation/Reference:

QUESTION 86
A system administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees. Which of the following should the administrator implement?

A. Shared accounts
B. Preshared passwords
C. Least privilege
D. Sponsored guest

Answer: D

Explanation

Explanation/Reference:

QUESTION 87
Which of the following would MOST likely appear in an uncredentialed vulnerability scan?

A. Self-signed certificates
B. Missing patches
C. Auditing parameters
D. Inactive local accounts

Answer: D

Explanation

Explanation/Reference:

QUESTION 88

A security analyst observes the following events in the logs of an employee workstation:

1/23	1:07:16	865	Access to C:\Users\user\temp\oasdfkh.hta has been restricted by your administrator by the default restriction policy level.
1/23	1:07:09	1034	The scan completed. No detections were found.

The security analyst reviews the file system and observes the following:

```
C:\>dir
C:\ Users\user\temp
1/23 1:07:02 oasdfkh.hta
1/23 1:07:02 update.bat
1/23 1:07:02 msg.txt
```

Given the information provided, which of the following MOST likely occurred on the workstation?

A. Application whitelisting controls blocked an exploit payload from executing.
B. Antivirus software found and quarantined three malware files.
C. Automatic updates were initiated but failed because they had not been approved.
D. The SIEM log agent was not tuned properly and reported a false positive.

Answer: A

Explanation

Explanation/Reference:

QUESTION 89
When identifying a company's most valuable assets as part of a BIA, which of the following should be the FIRST priority?

A. Life
B. Intellectual property
C. Sensitive data
D. Public reputation

Answer: A

Explanation

Explanation/Reference:

QUESTION 90
An organization needs to implement a large PKI. Network engineers are concerned that repeated transmission of the OCSP will impact network performance. Which of the following should the security analyst recommend is lieu of an OCSP?

A. CSR
B. CRL
C. CA
D. OID

Answer: B

Explanation

Explanation/Reference:

QUESTION 91
When considering a third-party cloud service provider, which of the following criteria would be the BEST to include in the security assessment process? (Choose two.)

A. Use of performance analytics
B. Adherence to regulatory compliance
C. Data retention policies
D. Size of the corporation
E. Breadth of applications support

Answer: BC

Explanation

Explanation/Reference:

QUESTION 92
Which of the following occurs when the security of a web application relies on JavaScript for input validation?

A. The integrity of the data is at risk.
B. The security of the application relies on antivirus.
C. A host-based firewall is required.
D. The application is vulnerable to race conditions.

Answer: A

Explanation

Explanation/Reference:

QUESTION 93
An analyst is reviewing a simple program for potential security vulnerabilities before being deployed to a Windows server. Given the following code:

```
void foo (char *bar)
{
  char random_user_input [12];
   strcpy (random_user_input, bar);
}
```

Which of the following vulnerabilities is present?

A. Bad memory pointer
B. Buffer overflow
C. Integer overflow

D. Backdoor

Answer: B

Explanation

Explanation/Reference:

QUESTION 94
An organization's file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

A. Snapshot
B. Full
C. Incremental
D. Differential

Answer: C

Explanation

Explanation/Reference:

QUESTION 95
A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant. Which of the following represents the authentication architecture in use?

A. Open systems authentication
B. Captive portal
C. RADIUS federation
D. 802.1x

Answer: D

Explanation

Explanation/Reference:

QUESTION 96
An employer requires that employees use a key-generating app on their smartphones to log into corporate applications. In terms of authentication of an individual, this type of access policy is BEST defined as:

A. Something you have.
B. Something you know.
C. Something you do.
D. Something you are.

Answer: A

Explanation

Explanation/Reference:

QUESTION 97
Adhering to a layered security approach, a controlled access facility employs security guards who verify the authorization of all personnel entering the facility. Which of the following terms BEST describes the security control being employed?

A. Administrative
B. Corrective
C. Deterrent
D. Compensating

Answer: A

Explanation

Explanation/Reference:

QUESTION 98
A security analyst is hardening a web server, which should allow a secure certificate-based session using the organization's PKI infrastructure. The web server should also utilize the latest security techniques and standards. Given this set of requirements, which of the following techniques should the analyst implement to BEST meet these requirements? (Choose two.)

A. Install an X- 509-compliant certificate.
B. Implement a CRL using an authorized CA.
C. Enable and configure TLS on the server.
D. Install a certificate signed by a public CA.
E. Configure the web server to use a host header.

Answer: AC

Explanation

Explanation/Reference:

QUESTION 99
A manager wants to distribute a report to several other managers within the company. Some of them reside in remote locations that are not connected to the domain but have a local server. Because there is sensitive data within the report and the size of the report is beyond the limit of the email attachment size, emailing the report is not an option. Which of the following protocols should be implemented to distribute the report securely? (Choose three.)

A. S/MIME
B. SSH
C. SNMPv3
D. FTPS
E. SRTP
F. HTTPS
G. LDAPS

Answer: BDF

Explanation

Explanation/Reference:

QUESTION 100
An auditor is reviewing the following output from a password-cracking tool:

```
user1: Password1
user2:Recovery!
user3:Alaskan10
user4:4Private
user5:PerForMance2
```

Which of the following methods did the auditor MOST likely use?

A. Hybrid
B. Dictionary
C. Brute force
D. Rainbow table

Answer: A

Explanation

Explanation/Reference:

QUESTION 101
Which of the following must be intact for evidence to be admissible in court?

A. Chain of custody
B. Order of volatility
C. Legal hold
D. Preservation

Answer: A

Explanation

Explanation/Reference:

QUESTION 102
A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a:

A. Credentialed scan.
B. Non-intrusive scan.
C. Privilege escalation test.
D. Passive scan.

Answer: A

Explanation

Explanation/Reference:

QUESTION 103
Which of the following cryptography algorithms will produce a fixed-length, irreversible output?

A. AES
B. 3DES
C. RSA
D. MD5

Answer: D

Explanation

Explanation/Reference:

QUESTION 104
A technician suspects that a system has been compromised. The technician reviews the following log entry:

WARNING- hash mismatch: C:\Window\SysWOW64\user32.dll
WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll

Based solely ono the above information, which of the following types of malware is MOST likely installed on the system?

A. Rootkit
B. Ransomware
C. Trojan
D. Backdoor

Answer: A

Explanation

Explanation/Reference:

QUESTION 105
A new firewall has been places into service at an organization. However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network. Which of the following steps should be completed to BEST resolve the issue?

A. The firewall should be configured to prevent user traffic form matching the implicit deny rule.
B. The firewall should be configured with access lists to allow inbound and outbound traffic.
C. The firewall should be configured with port security to allow traffic.
D. The firewall should be configured to include an explicit deny rule.

Answer: A

Explanation

Explanation/Reference:

QUESTION 106
A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org. Which of the following commands should the security analyst use? (Choose two.)

A.
```
nslookup
comptia.org
set type=ANY
ls-d example.org
```

B.
```
nslookup
comptia.org
set type=MX
example.org
```

C. dig –axfr comptia.org @example.org

D. ipconfig /flushDNS

E.
```
ifconfig eth0 down
ifconfig eth0 up
dhclient renew
```

F. dig @example.org comptia.org

Answer: AC

Explanation

Explanation/Reference:

QUESTION 107
Which of the following are the MAIN reasons why a systems administrator would install security patches in a staging environment before the patches are applied to the production server? (Choose two.)

A. To prevent server availability issues

B. To verify the appropriate patch is being installed

C. To generate a new baseline hash after patching

D. To allow users to test functionality

E. To ensure users are trained on new functionality

Answer: AD

Explanation

Explanation/Reference:

QUESTION 108
A Chief Information Officer (CIO) drafts an agreement between the organization and its employees. The agreement outlines ramifications for releasing information without consent and/or approvals. Which of the following BEST describes this type of agreement?

A. ISA

B. NDA
C. MOU
D. SLA

Answer: B

Explanation

Explanation/Reference:

QUESTION 109
Which of the following would meet the requirements for multifactor authentication?

A. Username, PIN, and employee ID number
B. Fingerprint and password
C. Smart card and hardware token
D. Voice recognition and retina scan

Answer: B

Explanation

Explanation/Reference:

QUESTION 110
A manager suspects that an IT employee with elevated database access may be knowingly modifying financial transactions for the benefit of a competitor. Which of the following practices should the manager implement to validate the concern?

A. Separation of duties
B. Mandatory vacations
C. Background checks
D. Security awareness training

Answer: A

Explanation

Explanation/Reference:

QUESTION 111
A penetration tester finds that a company's login credentials for the email client were being sent in clear text. Which of the following should be done to provide encrypted logins to the email server?

A. Enable IPSec and configure SMTP.
B. Enable SSH and LDAP credentials.
C. Enable MIME services and POP3.
D. Enable an SSL certificate for IMAP services.

Answer: D

Explanation

Explanation/Reference:

QUESTION 112
Before an infection was detected, several of the infected devices attempted to access a URL that was similar to the company name but with two letters transposed. Which of the following BEST describes the attack vector used to infect the devices?

A. Cross-site scripting
B. DNS poisoning
C. Typo squatting
D. URL hijacking

Answer: C

Explanation

Explanation/Reference:

QUESTION 113
A systems administrator is reviewing the following information from a compromised server:

Process	DEP	Local Address	Remote Address
LSASS	YES	0.0.0.0.	10.210.100.62
APACHE	NO	0.0.0.0	10.130.210.20
MySQL	NO	127.0.0.1	127.0.0.1
TFTP	YES	191.168.1.10	10.34.221.96

Given the above information, which of the following processes was MOST likely exploited via a remote buffer overflow attack?

A. Apache
B. LSASS
C. MySQL
D. TFTP

Answer: A

Explanation

Explanation/Reference:

QUESTION 114
Joe, a security administrator, needs to extend the organization's remote access functionality to be used by staff while travelling. Joe needs to maintain separate access control functionalities for internal, external, and VOIP services. Which of the following represents the BEST access technology for Joe to use?

A. RADIUS
B. TACACS+

C. Diameter

D. Kerberos

Answer: B

Explanation

Explanation/Reference:

QUESTION 115
The availability of a system has been labeled as the highest priority. Which of the following should be focused on the MOST to ensure the objective?

A. Authentication

B. HVAC

C. Full-disk encryption

D. File integrity checking

Answer: B

Explanation

Explanation/Reference:

QUESTION 116
As part of the SDLC, a third party is hired to perform a penetration test. The third party will have access to the source code, integration tests, and network diagrams. Which of the following BEST describes the assessment being performed?

A. Black box

B. Regression

C. White box

D. Fuzzing

Answer: C

Explanation

Explanation/Reference:

QUESTION 117
A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online. Which of the following methods would have MOST likely prevented the data from being exposed?

A. Removing the hard drive from its enclosure

B. Using software to repeatedly rewrite over the disk space

C. Using Blowfish encryption on the hard drives

D. Using magnetic fields to erase the data

Answer: D

Explanation

Explanation/Reference:

QUESTION 118
Which of the following are methods to implement HA in a web application server environment? (Choose two.)

A. Load balancers
B. Application layer firewalls
C. Reverse proxies
D. VPN concentrators
E. Routers

Answer: AB

Explanation

Explanation/Reference:

QUESTION 119
An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request.

Which of the following secure protocols is the developer MOST likely to use?

A. FTPS
B. SFTP
C. SSL
D. LDAPS
E. SSH

Answer: C

Explanation

Explanation/Reference:

QUESTION 120
Which of the following precautions MINIMIZES the risk from network attacks directed at multifunction printers, as well as the impact on functionality at the same time?

A. Isolating the systems using VLANs
B. Installing a software-based IPS on all devices
C. Enabling full disk encryption
D. Implementing a unique user PIN access functions

Answer: A

Explanation

Explanation/Reference:

QUESTION 121
After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

A. Recovery
B. Identification
C. Preparation
D. Documentation
E. Escalation

Answer: B

Explanation

Explanation/Reference:

QUESTION 122
A company was recently audited by a third party. The audit revealed the company's network devices were transferring files in the clear. Which of the following protocols should the company use to transfer files?

A. HTTPS
B. LDAPS
C. SCP
D. SNMPv3

Answer: C

Explanation

Explanation/Reference:

QUESTION 123
During a monthly vulnerability scan, a server was flagged for being vulnerable to an Apache Struts exploit. Upon further investigation, the developer responsible for the server informs the security team that Apache Struts is not installed on the server. Which of the following BEST describes how the security team should reach to this incident?

A. The finding is a false positive and can be disregarded
B. The Struts module needs to be hardened on the server
C. The Apache software on the server needs to be patched and updated
D. The server has been compromised by malware and needs to be quarantined.

Answer: A

Explanation

Explanation/Reference:

QUESTION 124
A systems administrator wants to protect data stored on mobile devices that are used to scan and record assets in a warehouse. The control must automatically destroy the secure container of mobile devices if they

leave the warehouse. Which of the following should the administrator implement? (Choose two.)

A. Geofencing
B. Remote wipe
C. Near-field communication
D. Push notification services
E. Containerization

Answer: AE

Explanation

Explanation/Reference:

QUESTION 125
A security analyst is performing a quantitative risk analysis. The risk analysis should show the potential monetary loss each time a threat or event occurs. Given this requirement, which of the following concepts would assist the analyst in determining this value? (Choose two.)

A. ALE
B. AV
C. ARO
D. EF
E. ROI

Answer: BD

Explanation

Explanation/Reference:

QUESTION 126
Which of the following AES modes of operation provide authentication? (Choose two.)

A. CCM
B. CBC
C. GCM
D. DSA
E. CFB

Answer: AC

Explanation

Explanation/Reference:

QUESTION 127
An audit takes place after company-wide restricting, in which several employees changed roles. The following deficiencies are found during the audit regarding access to confidential data:

Employee	Job Function	Audit Finding
Ann	Sales Manager	Access to confidential payroll shares Access to payroll processing program Access to marketing shared
Jeff	Marketing Director	Access to human resources annual review folder Access to shared human resources mailbox
John	Sales Manager (Terminated)	Active account Access to human resources annual review folder Access to confidential payroll shares

Which of the following would be the BEST method to prevent similar audit findings in the future?

A. Implement separation of duties for the payroll department.
B. Implement a DLP solution on the payroll and human resources servers.
C. Implement rule-based access controls on the human resources server.
D. Implement regular permission auditing and reviews.

Answer: D

Explanation

Explanation/Reference:

QUESTION 128
A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols MUST the security engineer select?

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

Answer: C

Explanation

Explanation/Reference:

QUESTION 129
A system's administrator has finished configuring firewall ACL to allow access to a new web server.

```
PERMIT TCP from: ANY to: 192.168.1.10:80
PERMIT TCP from: ANY to: 192.168.1.10:443
DENY TCP from: ANY to: ANY
```

The security administrator confirms form the following packet capture that there is network traffic from the internet to the web server:

```
TCP 10.23.243.2:2000->192.168.1.10:80 POST/default's
TCP 172.16.4.100:1934->192.168.1.10:80 GET/session.aspx?user1_sessionid=
a12ad8741d8f7e7ac723847cBaa8231a
```

The company's internal auditor issues a security finding and requests that immediate action be taken. With which of the following is the auditor MOST concerned?

A. Misconfigured firewall
B. Clear text credentials
C. Implicit deny
D. Default configuration

Answer: B

Explanation

Explanation/Reference:

QUESTION 130
Which of the following vulnerability types would the type of hacker known as a script kiddie be MOST dangerous against?

A. Passwords written on the bottom of a keyboard
B. Unpatched exploitable Internet-facing services
C. Unencrypted backup tapes
D. Misplaced hardware token

Answer: B

Explanation

Explanation/Reference:

QUESTION 131
An in-house penetration tester is using a packet capture device to listen in on network communications. This is an example of:

A. Passive reconnaissance
B. Persistence
C. Escalation of privileges
D. Exploiting the switch

Answer: A

Explanation

Explanation/Reference:

QUESTION 132
A black hat hacker is enumerating a network and wants to remain covert during the process. The hacker initiates a vulnerability scan. Given the task at hand the requirement of being covert, which of the following

statements BEST indicates that the vulnerability scan meets these requirements?

A. The vulnerability scanner is performing an authenticated scan.
B. The vulnerability scanner is performing local file integrity checks.
C. The vulnerability scanner is performing in network sniffer mode.
D. The vulnerability scanner is performing banner grabbing.

Answer: C

Explanation

Explanation/Reference:

QUESTION 133
A development team has adopted a new approach to projects in which feedback is iterative and multiple iterations of deployments are provided within an application's full life cycle. Which of the following software development methodologies is the development team using?

A. Waterfall
B. Agile
C. Rapid
D. Extreme

Answer: B

Explanation

Explanation/Reference:

QUESTION 134
A Chief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

A. Implement time-of-day restrictions.
B. Audit file access times.
C. Secretly install a hidden surveillance camera.
D. Require swipe-card access to enter the lab.

Answer: D

Explanation

Explanation/Reference:

QUESTION 135
A company hires a third-party firm to conduct an assessment of vulnerabilities exposed to the Internet. The firm informs the company that an exploit exists for an FTP server that had a version installed from eight years ago. The company has decided to keep the system online anyway, as no upgrade exists form the vendor. Which of the following BEST describes the reason why the vulnerability exists?

A. Default configuration

B. End-of-life system
C. Weak cipher suite
D. Zero-day threats

Answer: B

Explanation

Explanation/Reference:

QUESTION 136
An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization's security policy, the employee's access to all network resources is terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server. Which of the following represents the BEST course of action?

A. Approve the former employee's request, as a password reset would give the former employee access to only the human resources server.
B. Deny the former employee's request, since the password reset request came from an external email address.
C. Deny the former employee's request, as a password reset would give the employee access to all network resources.
D. Approve the former employee's request, as there would not be a security issue with the former employee gaining access to network resources.

Answer: C

Explanation

Explanation/Reference:

QUESTION 137
Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

A. Encrypt it with Joe's private key
B. Encrypt it with Joe's public key
C. Encrypt it with Ann's private key
D. Encrypt it with Ann's public key

Answer: D

Explanation

Explanation/Reference:

QUESTION 138
A director of IR is reviewing a report regarding several recent breaches. The director compiles the following statistic's

-Initial IR engagement time frame
-Length of time before an executive management notice went out

-Average IR phase completion

The director wants to use the data to shorten the response time. Which of the following would accomplish this?

A. CSIRT
B. Containment phase
C. Escalation notifications
D. Tabletop exercise

Answer: D

Explanation

Explanation/Reference:

QUESTION 139
To reduce disk consumption, an organization's legal department has recently approved a new policy setting the data retention period for sent email at six months. Which of the following is the BEST way to ensure this goal is met?

A. Create a daily encrypted backup of the relevant emails.
B. Configure the email server to delete the relevant emails.
C. Migrate the relevant emails into an "Archived" folder.
D. Implement automatic disk compression on email servers.

Answer: B

Explanation

Explanation/Reference:

QUESTION 140
A security administrator is configuring a new network segment, which contains devices that will be accessed by external users, such as web and FTP server. Which of the following represents the MOST secure way to configure the new network segment?

A. The segment should be placed on a separate VLAN, and the firewall rules should be configured to allow external traffic.
B. The segment should be placed in the existing internal VLAN to allow internal traffic only.
C. The segment should be placed on an intranet, and the firewall rules should be configured to allow external traffic.
D. The segment should be placed on an extranet, and the firewall rules should be configured to allow both internal and external traffic.

Answer: D

Explanation

Explanation/Reference:

QUESTION 141
Which of the following types of attacks precedes the installation of a rootkit on a server?

A. Pharming
B. DDoS
C. Privilege escalation
D. DoS

Answer: C

Explanation

Explanation/Reference:

QUESTION 142
Which of the following cryptographic algorithms is irreversible?

A. RC4
B. SHA-256
C. DES
D. AES

Answer: B

Explanation

Explanation/Reference:

QUESTION 143
A security analyst receives an alert from a WAF with the following payload:
var data= "<test test test>" ++ <../../../../../../etc/passwd>"

Which of the following types of attacks is this?

A. Cross-site request forgery
B. Buffer overflow
C. SQL injection
D. JavaScript data insertion
E. Firewall evasion script

Answer: D

Explanation

Explanation/Reference:

QUESTION 144
A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him. Which of the following BEST describes what occurred?

A. The hacker used a race condition.
B. The hacker used a pass-the-hash attack.
C. The hacker-exploited improper key management.

D. The hacker exploited weak switch configuration.

Answer: D

Explanation

Explanation/Reference:

QUESTION 145
Audit logs from a small company's vulnerability scanning software show the following findings:
Destinations scanned:
-Server001- Internal human resources payroll server
-Server101-Internet-facing web server
-Server201- SQL server for Server101
-Server301-Jumpbox used by systems administrators accessible from the internal network

Validated vulnerabilities found:
-Server001- Vulnerable to buffer overflow exploit that may allow attackers to install software
-Server101- Vulnerable to buffer overflow exploit that may allow attackers to install software
-Server201-OS updates not fully current
-Server301- Accessible from internal network without the use of jumpbox
-Server301-Vulnerable to highly publicized exploit that can elevate user privileges

Assuming external attackers who are gaining unauthorized information are of the highest concern, which of the following servers should be addressed FIRST?

A. Server001
B. Server101
C. Server201
D. Server301

Answer: B

Explanation

Explanation/Reference:

QUESTION 146
A security analyst wants to harden the company's VoIP PBX. The analyst is worried that credentials may be intercepted and compromised when IP phones authenticate with the BPX. Which of the following would best prevent this from occurring?

A. Implement SRTP between the phones and the PBX.
B. Place the phones and PBX in their own VLAN.
C. Restrict the phone connections to the PBX.
D. Require SIPS on connections to the PBX.

Answer: A

Explanation

Explanation/Reference:

QUESTION 147

An organization is comparing and contrasting migration from its standard desktop configuration to the newest version of the platform. Before this can happen, the Chief Information Security Officer (CISO) voices the need to evaluate the functionality of the newer desktop platform to ensure interoperability with existing software in use by the organization. In which of the following principles of architecture and design is the CISO engaging?

A. Dynamic analysis
B. Change management
C. Baselining
D. Waterfalling

Answer: B

Explanation

Explanation/Reference:

QUESTION 148
A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Choose two.)

A. Ping
B. Ipconfig
C. Tracert
D. Netstat
E. Dig
F. Nslookup

Answer: BC

Explanation

Explanation/Reference:

QUESTION 149
A user is presented with the following items during the new-hire onboarding process:
-Laptop
-Secure USB drive
-Hardware OTP token
-External high-capacity HDD
-Password complexity policy
-Acceptable use policy
-HASP key
-Cable lock

Which of the following is one component of multifactor authentication?

A. Secure USB drive
B. Cable lock
C. Hardware OTP token
D. HASP key

Answer: C

Explanation

Explanation/Reference:

QUESTION 150
An organization requires users to provide their fingerprints to access an application. To improve security, the application developers intend to implement multifactor authentication. Which of the following should be implemented?

A. Use a camera for facial recognition
B. Have users sign their name naturally
C. Require a palm geometry scan
D. Implement iris recognition

Answer: B

Explanation

Explanation/Reference:

QUESTION 151
A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

A. Pre-shared key
B. Enterprise
C. Wi-Fi Protected setup
D. Captive portal

Answer: D

Explanation

Explanation/Reference:

QUESTION 152
After a routine audit, a company discovers that engineering documents have been leaving the network on a particular port. The company must allow outbound traffic on this port, as it has a legitimate business use. Blocking the port would cause an outage. Which of the following technology controls should the company implement?

A. NAC
B. Web proxy
C. DLP
D. ACL

Answer: C

Explanation

Explanation/Reference:

QUESTION 153
A security analyst has received the following alert snippet from the HIDS appliance:

PROTOCOL	SIG	SRC.PORT	DST.PORT
TCP	XMAS SCAN	192.168.1.1:1091	192.168.1.2:8891
TCP	XMAS SCAN	192.168.1.1:649	192.168.1.2:9001
TCP	XMAS SCAN	192.168.1.1:2264	192.168.1.2:6455
TCP	XMAS SCAN	192.168.1.1:3464	192.168.1.2:8744

Given the above logs, which of the following is the cause of the attack?

A. The TCP ports on destination are all open
B. FIN, URG, and PSH flags are set in the packet header
C. TCP MSS is configured improperly
D. There is improper Layer 2 segmentation

Answer: B

Explanation

Explanation/Reference:

QUESTION 154
A security analyst reviews the following output:

```
File name: somefile.pdf
File MD5: E289F21CD33E4F57890DDEA5CF267ED2
File size: 1.9 Mb
Created by: Jan Smith
Deleted by: Jan Smith
Date deleted: October 01, 2015 8:43:21 EST
```

The analyst loads the hash into the SIEM to discover if this hash is seen in other parts of the network. After inspecting a large number of files, the security analyst reports the following:

```
File hash: E289F21CD33E4F57890DDEA5CF267ED2
Files found: somestuff.xls, somefile.pdf, nofile.doc
```

Which of the following is the MOST likely cause of the hash being found in other areas?

A. Jan Smith is an insider threat
B. There are MD5 hash collisions
C. The file is encrypted
D. Shadow copies are present

Answer: B

Explanation

Explanation/Reference:

QUESTION 155
A company's AUP requires:
- Passwords must meet complexity requirements.
- Passwords are changed at least once every six months.
- Passwords must be at least eight characters long.

An auditor is reviewing the following report:

Username	Last login	Last changed
Carol	2 hours	90 days
David	2 hours	30 days
Ann	1 hour	247 days
Joe	0.5 hours	7 days

Which of the following controls should the auditor recommend to enforce the AUP?

A. Account lockout thresholds
B. Account recovery
C. Password expiration
D. Prohibit password reuse

Answer: C

Explanation

Explanation/Reference:

QUESTION 156
An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts BEST represents the risk described in this scenario?

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

Answer: A

Explanation

Explanation/Reference:

QUESTION 157
A security analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the following should the security analyst do NEXT?

A. Document and lock the workstations in a secure area to establish chain of custody
B. Notify the IT department that the workstations are to be reimaged and the data restored for reuse

C. Notify the IT department that the workstations may be reconnected to the network for the users to continue working
D. Document findings and processes in the after-action and lessons learned report

Answer: D

Explanation

Explanation/Reference:

QUESTION 158
An employee receives an email, which appears to be from the Chief Executive Officer (CEO), asking for a report of security credentials for all users.
Which of the following types of attack is MOST likely occurring?

A. Policy violation
B. Social engineering
C. Whaling
D. Spear phishing

Answer: D

Explanation

Explanation/Reference:

QUESTION 159
An information security analyst needs to work with an employee who can answer questions about how data for a specific system is used in the business. The analyst should seek out an employee who has the role of:

A. steward
B. owner
C. privacy officer
D. systems administrator

Answer: B

Explanation

Explanation/Reference:

QUESTION 160
A group of non-profit agencies wants to implement a cloud service to share resources with each other and minimize costs. Which of the following cloud deployment models BEST describes this type of effort?

A. Public
B. Hybrid
C. Community
D. Private

Answer: C

Explanation

Explanation/Reference:

QUESTION 161
An administrator is configuring access to information located on a network file server named “Bowman”. The files are located in a folder named “BalkFiles”. The files are only for use by the “Matthews” division and should be read-only. The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model. Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files.

The administrator configures the file share according to the following table:

Share permissions			
1	Everyone	Full control	
File system permissions			
2	Bowman\Users	Modify	Inherited
3	Domain\Matthews	Read	Not inherited
4	Bowman\System	Full control	Inherited
5	Bowman\Administrators	Full control	Not inherited

Which of the following rows has been misconfigured?

A. Row 1
B. Row 2
C. Row 3
D. Row 4
E. Row 5

Answer: D

Explanation

Explanation/Reference:

QUESTION 162
A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization. Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?

A. Implement a DLP solution and classify the report as confidential, restricting access only to human resources staff
B. Restrict access to the share where the report resides to only human resources employees and enable auditing
C. Have all members of the IT department review and sign the AUP and disciplinary policies
D. Place the human resources computers on a restricted VLAN and configure the ACL to prevent access from the IT department

Answer: B

Explanation

Explanation/Reference:

QUESTION 163
A company is developing a new system that will unlock a computer automatically when an authorized user sits in front of it, and then lock the computer when the user leaves. The user does not have to perform any action for this process to occur. Which of the following technologies provides this capability?

A. Facial recognition
B. Fingerprint scanner
C. Motion detector
D. Smart cards

Answer: A

Explanation

Explanation/Reference:

QUESTION 164
A security analyst accesses corporate web pages and inputs random data in the forms. The response received includes the type of database used and SQL commands that the database accepts. Which of the following should the security analyst use to prevent this vulnerability?

A. Application fuzzing
B. Error handling
C. Input validation
D. Pointer dereference

Answer: C

Explanation

Explanation/Reference:

QUESTION 165
Which of the following differentiates a collision attack from a rainbow table attack?

A. A rainbow table attack performs a hash lookup
B. A rainbow table attack uses the hash as a password
C. In a collision attack, the hash and the input data are equivalent
D. In a collision attack, the same input results in different hashes

Answer: A

Explanation

Explanation/Reference:

QUESTION 166

A help desk is troubleshooting user reports that the corporate website is presenting untrusted certificate errors to employees and customers when they visit the website. Which of the following is the MOST likely cause of this error, provided the certificate has not expired?

A. The certificate was self signed, and the CA was not imported by employees or customers
B. The root CA has revoked the certificate of the intermediate CA
C. The valid period for the certificate has passed, and a new certificate has not been issued
D. The key escrow server has blocked the certificate from being validated

Answer: B

Explanation

Explanation/Reference:

QUESTION 167

A security analyst is investigating a suspected security breach and discovers the following in the logs of the potentially compromised server:

Time	Source	Destination	Account Name	Action
11:01:31	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:32	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:33	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:34	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:35	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:36	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:37	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:38	18.12.98.145	10.15.21.100	Joe	Logon Successful

Which of the following would be the BEST method for preventing this type of suspected attack in the future?

A. Implement password expirations
B. Implement restrictions on shared credentials
C. Implement account lockout settings
D. Implement time-of-day restrictions on this server

Answer: C

Explanation

Explanation/Reference:

QUESTION 168

DRAG DROP

A security administrator is given the security and availability profiles for servers that are being deployed.

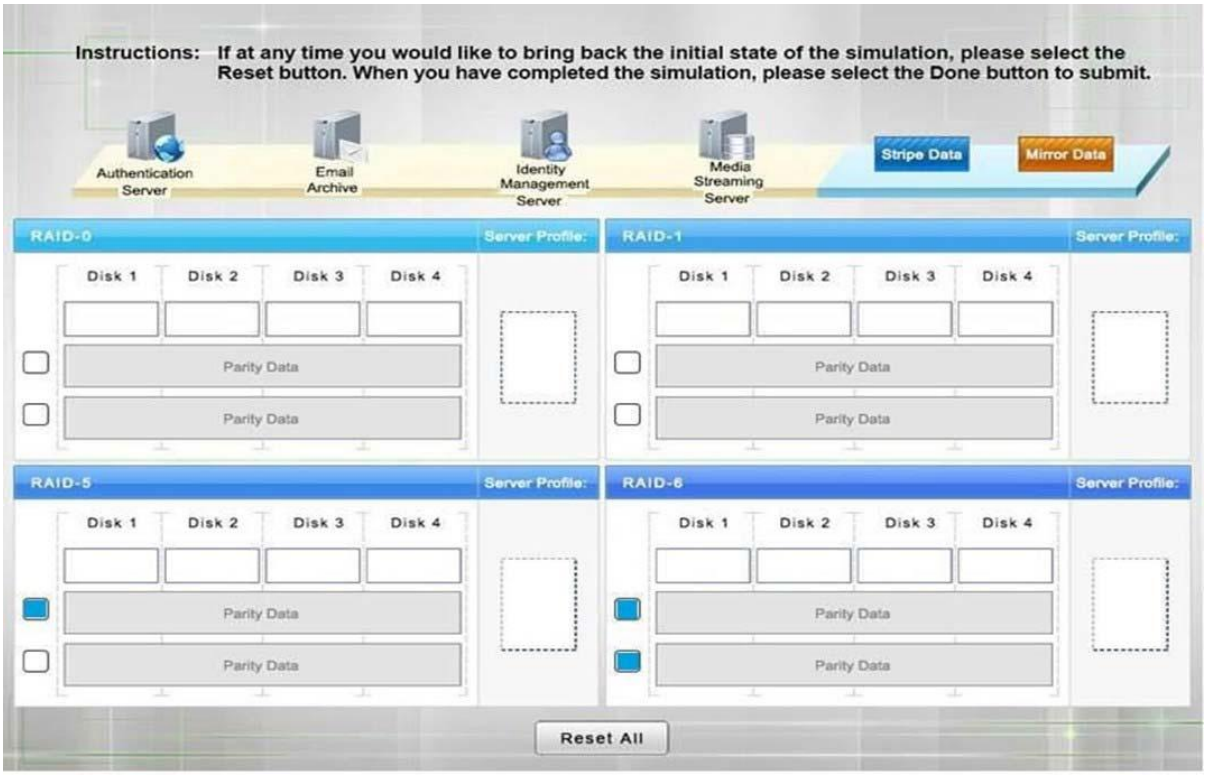
1. Match each RAID type with the correct configuration and MINIMUM number of drives.
2. Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements. Instructions:

- All drive definitions can be dragged as many times as necessary
- Not all placeholders may be filled in the RAID configuration boxes

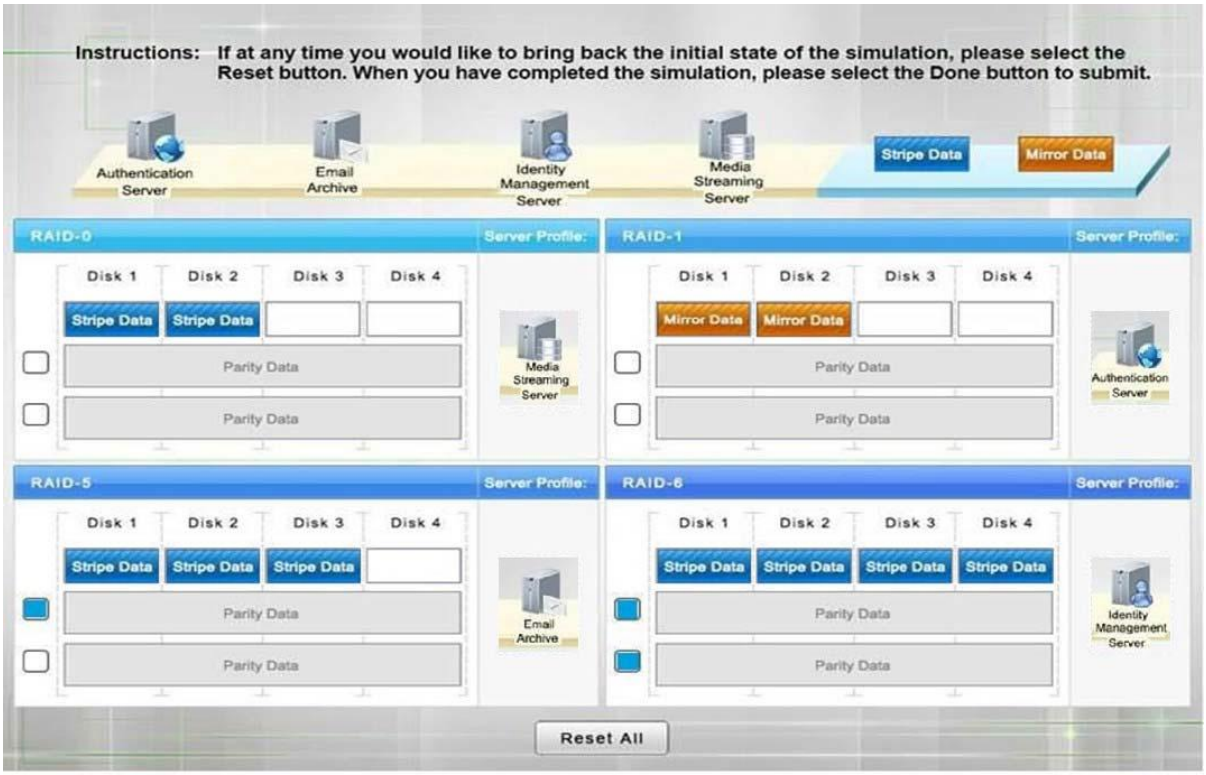
- If parity is required, please select the appropriate number of parity checkboxes
- Server profiles may be dragged only once

If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Select and Place:



Answer:



Explanation

Explanation/Reference:
Explanation:
RAID-0 is known as striping. It is not a fault tolerant solution but does improve disk performance for read/write operations. Striping requires a minimum of two disks and does not use parity.
RAID-0 can be used where performance is required over fault tolerance, such as a media streaming server.
RAID-1 is known as mirroring because the same data is written to two disks so that the two disks have identical data. This is a fault tolerant solution that halves the storage space. A minimum of two disks are used in mirroring and does not use parity. RAID-1 can be used where fault tolerance is required over performance, such as on an authentication server. RAID-5 is a fault tolerant solution that uses parity and striping. A minimum of three disks are required for RAID-5 with one disk's worth of space being used for parity information. However, the parity information is distributed across all the disks. RAID-5 can recover from a sing disk failure.
RAID-6 is a fault tolerant solution that uses dual parity and striping. A minimum of four disks are required for RAID-6. Dual parity allows RAID-6 to recover from the simultaneous failure of up to two disks. Critical data should be stored on a RAID-6 system.

http://www.adaptec.com/en-us/solutions/raid_levels.html

QUESTION 169
A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) 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

Answer: B

Explanation

Explanation/Reference:

QUESTION 170
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? (Choose two.)

A. Monitor VPN client access
B. Reduce failed login out 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

Answer: CF

Explanation

Explanation/Reference:

QUESTION 171
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

Answer: D

Explanation

Explanation/Reference:

QUESTION 172
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

Answer: B

Explanation

Explanation/Reference:

QUESTION 173
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 (IDI)
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)

Answer: E

Explanation

Explanation/Reference:

QUESTION 174
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 175
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

Answer: A

Explanation

Explanation/Reference:

QUESTION 176
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 177
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 178
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

Answer: A

Explanation

Explanation/Reference:

QUESTION 179
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

Answer: B

Explanation

Explanation/Reference:

QUESTION 180
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 181
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 182
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

Answer: B

Explanation

Explanation/Reference:

QUESTION 183
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

Answer: D

Explanation

Explanation/Reference:

QUESTION 184
Which of the following should identify critical systems and components?

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

Answer: D

Explanation

Explanation/Reference:

QUESTION 185
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

Answer: A

Explanation

Explanation/Reference:

QUESTION 186
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 187
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

Answer: B

Explanation

Explanation/Reference:

QUESTION 188
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 189
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 190
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 191
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.

Answer: C

Explanation

Explanation/Reference:

QUESTION 192
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

Answer: B

Explanation

Explanation/Reference:

QUESTION 193
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

Answer: A

Explanation

Explanation/Reference:

QUESTION 194
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

Answer: B

Explanation

Explanation/Reference:

QUESTION 195
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 196
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? (Choose 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. Lease privilege

Answer: DFI

Explanation

Explanation/Reference:

QUESTION 197
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

Answer: D

Explanation

Explanation/Reference:

QUESTION 198
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

Answer: D

Explanation

Explanation/Reference:

QUESTION 199
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

Answer: B

Explanation

Explanation/Reference:

QUESTION 200
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

Answer: B

Explanation

Explanation/Reference:

QUESTION 201
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

Answer: D

Explanation

Explanation/Reference:

QUESTION 202
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 203
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

Answer: D

Explanation

Explanation/Reference:

QUESTION 204
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 205
Which of the following use the SSH protocol?

A. Stelnet
B. SCP
C. SNMP
D. FTPS
E. SSL
F. SFTP

Answer: BF

Explanation

Explanation/Reference:

QUESTION 206
Which of the following is the GREATEST risk to a company by allowing employees to physically bring their personal smartphones to work?

A. Taking pictures of proprietary information and equipment in restricted areas.
B. Installing soft token software to connect to the company's wireless network.
C. Company cannot automate patch management on personally-owned devices.
D. Increases the attack surface by having more target devices on the company's campus

Answer: A

Explanation

Explanation/Reference:

QUESTION 207
Which of the following is the summary of loss for a given year?

A. MTBF
B. ALE
C. SLA
D. ARO

Answer: B

Explanation

Explanation/Reference:

QUESTION 208
A Security Officer on a military base needs to encrypt several smart phones that will be going into the field.

Which of the following encryption solutions should be deployed in this situation?

A. Elliptic curve
B. One-time pad
C. 3DES
D. AES-256

Answer: D

Explanation

Explanation/Reference:

QUESTION 209
An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week.

Which of the following would be the BEST method of updating this application?

A. Configure testing and automate patch management for the application.
B. Configure security control testing for the application.
C. Manually apply updates for the application when they are released.
D. Configure a sandbox for testing patches before the scheduled monthly update.

Answer: A

Explanation

Explanation/Reference:

QUESTION 210
A technician must configure a firewall to block external DNS traffic from entering a network.

Which of the following ports should they block on the firewall?

A. 53
B. 110
C. 143
D. 443

Answer: A

Explanation

Explanation/Reference:

QUESTION 211
A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols.

Which of the following summarizes the BEST response to the programmer's proposal?

A. The newly developed protocol will only be as secure as the underlying cryptographic algorithms used.
B. New protocols often introduce unexpected vulnerabilities, even when developed with otherwise secure and tested algorithm libraries.
C. A programmer should have specialized training in protocol development before attempting to design a new encryption protocol.
D. The obscurity value of unproven protocols against attacks often outweighs the potential for introducing new vulnerabilities.

Answer: B

Explanation

Explanation/Reference:

QUESTION 212
A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion.

Which of the following technologies would BEST be suited to accomplish this?

A. Transport Encryption
B. Stream Encryption
C. Digital Signature
D. Steganography

Answer: D

Explanation

Explanation/Reference:
Explanation:
Steganography is the process of hiding a message in another message so as to obfuscate its importance. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

QUESTION 213
A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database.

Which of the following risk mitigation strategies should have been implemented when the supervisor was demoted?

A. Incident management
B. Routine auditing
C. IT governance
D. Monthly user rights reviews

Answer: B

Explanation

Explanation/Reference:

QUESTION 214
Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

A. War chalking
B. Bluejacking
C. Bluesnarfing
D. Rogue tethering

Answer: B

Explanation

Explanation/Reference:
Explanation:
Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

QUESTION 215
Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially.

Which of the following would explain the situation?

A. An ephemeral key was used for one of the messages
B. A stream cipher was used for the initial email; a block cipher was used for the reply
C. Out-of-band key exchange has taken place
D. Asymmetric encryption is being used

Answer: D

Explanation

Explanation/Reference:

Explanation:
Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

QUESTION 216
Recently several employees were victims of a phishing email that appeared to originate from the company president. The email claimed the employees would be disciplined if they did not click on a malicious link in the message.

Which of the following principles of social engineering made this attack successful?

A. Authority
B. Spamming
C. Social proof
D. Scarcity

Answer: A

Explanation

Explanation/Reference:

QUESTION 217
Which of the following is the LEAST secure hashing algorithm?

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

Answer: C

Explanation

Explanation/Reference:

QUESTION 218
An employee uses RDP to connect back to the office network.

If RDP is misconfigured, which of the following security exposures would this lead to?

A. A virus on the administrator's desktop would be able to sniff the administrator's username and password.
B. Result in an attacker being able to phish the employee's username and password.
C. A social engineering attack could occur, resulting in the employee's password being extracted.
D. A man in the middle attack could occur, resulting the employee's username and password being captured.

Answer: D

Explanation

Explanation/Reference:

QUESTION 219
Joe, the security administrator, sees this in a vulnerability scan report:

"The server 10.1.2.232 is running Apache 2.2.20 which may be vulnerable to a mod_cgi exploit."

Joe verifies that the mod_cgi module is not enabled on 10.1.2.232. This message is an example of:

A. a threat.
B. a risk.
C. a false negative.
D. a false positive.

Answer: D

Explanation

Explanation/Reference:

QUESTION 220
An auditor has identified an access control system that can incorrectly accept an access attempt from an unauthorized user. Which of the following authentication systems has the auditor reviewed?

A. Password-based
B. Biometric-based
C. Location-based
D. Certificate-based

Answer: B

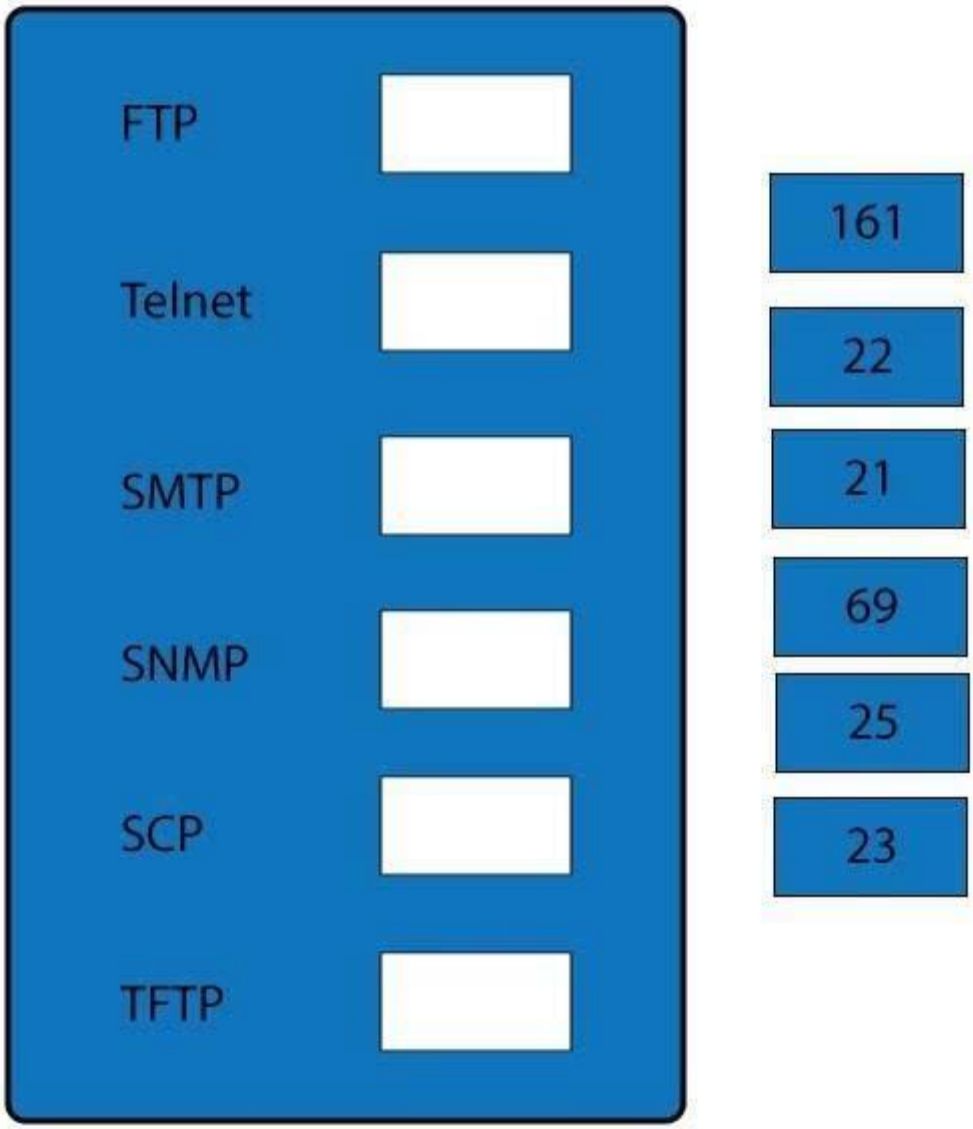
Explanation

Explanation/Reference:

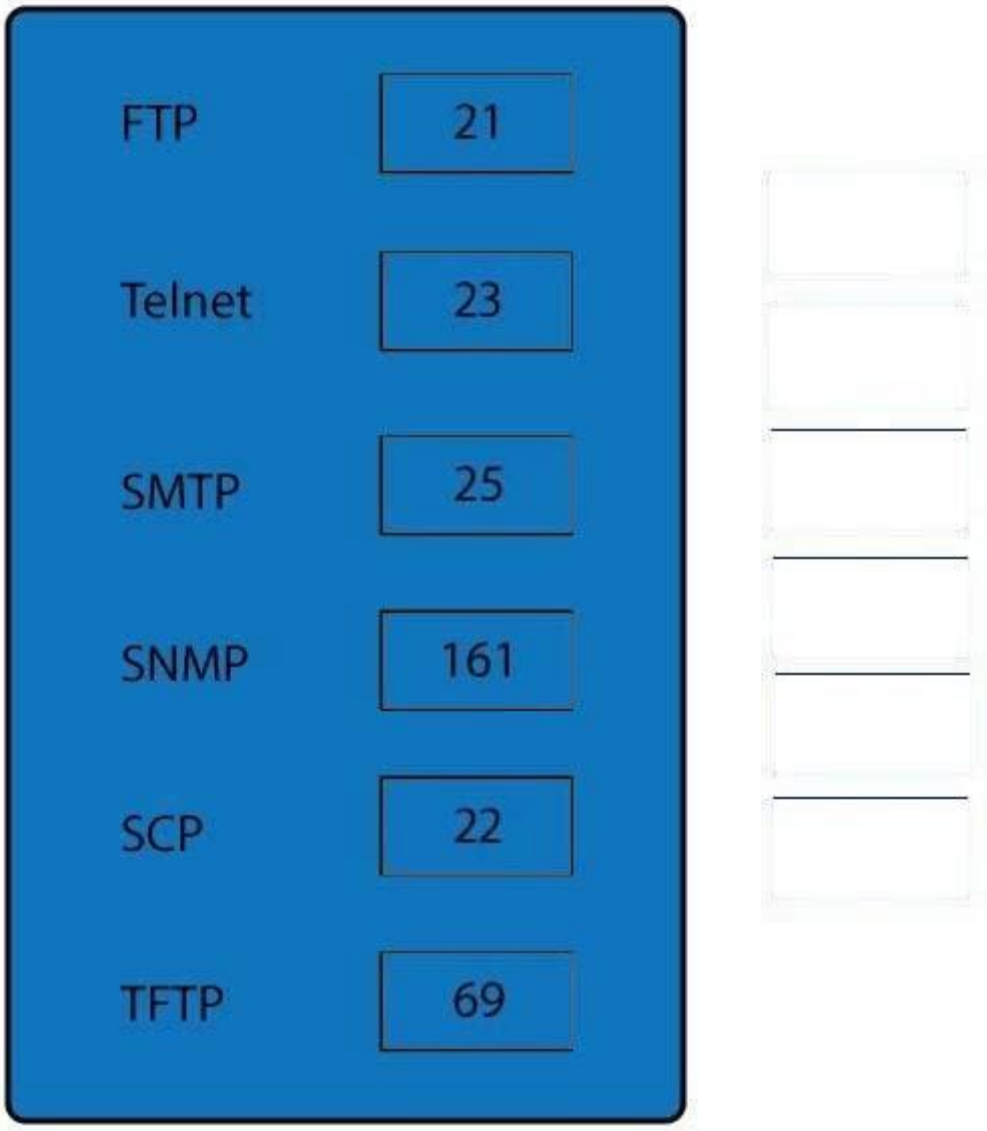
QUESTION 221
DRAG DROP

Drag and drop the correct protocol to its default port.

Select and Place:



Answer:



Explanation

Explanation/Reference:
Explanation:

FTP uses TCP port 21. Telnet uses port 23.
SSH uses TCP port 22.
All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.
Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).
Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). SMTP uses TCP port 25.
Port 69 is used by TFTP.
SNMP makes use of UDP ports 161 and 162.
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 222
The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.

Which of the following categories BEST describes what she is looking for?

A. ALE
B. MTTR
C. MTBF
D. MTTF

Answer: D

Explanation

Explanation/Reference:

QUESTION 223
A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet.

Which of the following should be used in the code? (Choose two.)

A. Escrowed keys
B. SSL symmetric encryption key
C. Software code private key
D. Remote server public key
E. OCSP

Answer: CE

Explanation

Explanation/Reference:

QUESTION 224
A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange white markings in different areas of the parking lot.

The person is attempting which of the following types of attacks?

A. Jamming
B. War chalking
C. Packet sniffing
D. Near field communication

Answer: B

Explanation

Explanation/Reference:

QUESTION 225
A system administrator is configuring a site-to-site VPN tunnel.

Which of the following should be configured on the VPN concentrator during the IKE phase?

A. RIPEMD
B. ECDHE
C. Diffie-Hellman
D. HTTPS

Answer: C

Explanation

Explanation/Reference:

QUESTION 226
A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks.

Which of the following is the reason the manager installed the racks this way?

A. To lower energy consumption by sharing power outlets
B. To create environmental hot and cold isles
C. To eliminate the potential for electromagnetic interference
D. To maximize fire suppression capabilities

Answer: B

Explanation

Explanation/Reference:

QUESTION 227
Phishing emails frequently take advantage of high-profile catastrophes reported in the news.

Which of the following principles BEST describes the weakness being exploited?

A. Intimidation
B. Scarcity
C. Authority
D. Social proof

Answer: D

Explanation

Explanation/Reference:

QUESTION 228
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

Answer: A

Explanation

Explanation/Reference:

QUESTION 229
Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network.

This is MOST likely which of the following types of attacks?

A. Vishing
B. Impersonation
C. Spim
D. Scareware

Answer: A

Explanation

Explanation/Reference:

QUESTION 230
An administrator discovers the following log entry on a server:

Nov 12 2013 00:23:45 httpd[2342]: GET /app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadow

Which of the following attacks is being attempted?

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

Answer: A

Explanation

Explanation/Reference:

QUESTION 231
A security team wants to establish an Incident Response plan. The team has never experienced an incident.

Which of the following would BEST help them establish plans and procedures?

A. Table top exercises
B. Lessons learned
C. Escalation procedures
D. Recovery procedures

Answer: A

Explanation

Explanation/Reference:

QUESTION 232
Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

A. Protocol analyzer
B. Vulnerability scan
C. Penetration test
D. Port scanner

Answer: B

Explanation

Explanation/Reference:
Explanation:
A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.
Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.
Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

QUESTION 233
Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

A. Cloud computing
B. Virtualization
C. Redundancy
D. Application control

Answer: B

Explanation

Explanation/Reference:
Explanation:
Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs. Virtualization

offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

QUESTION 234

A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN.

Which of the following protocols should be used?

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

Answer: A

Explanation

Explanation/Reference:

QUESTION 235

A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued.

Which of the following should the administrator submit to receive a new certificate?

A. CRL
B. OSCP
C. PFX
D. CSR
E. CA

Answer: D

Explanation

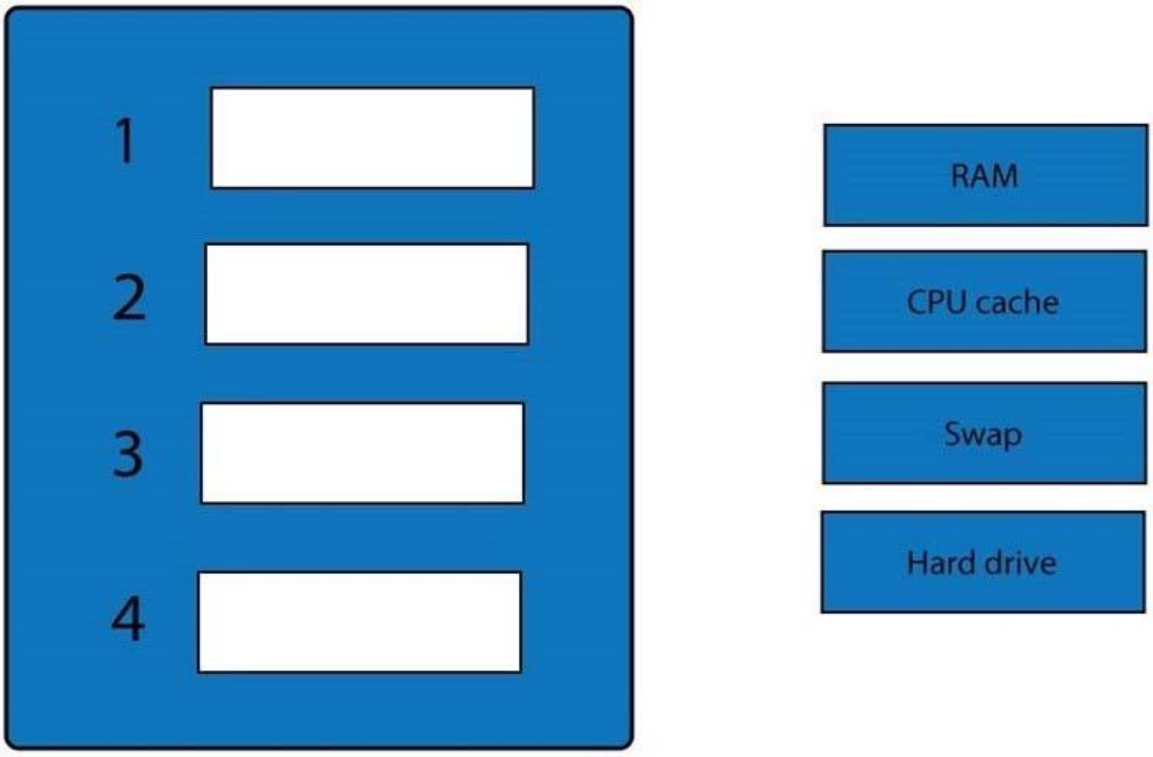
Explanation/Reference:

QUESTION 236

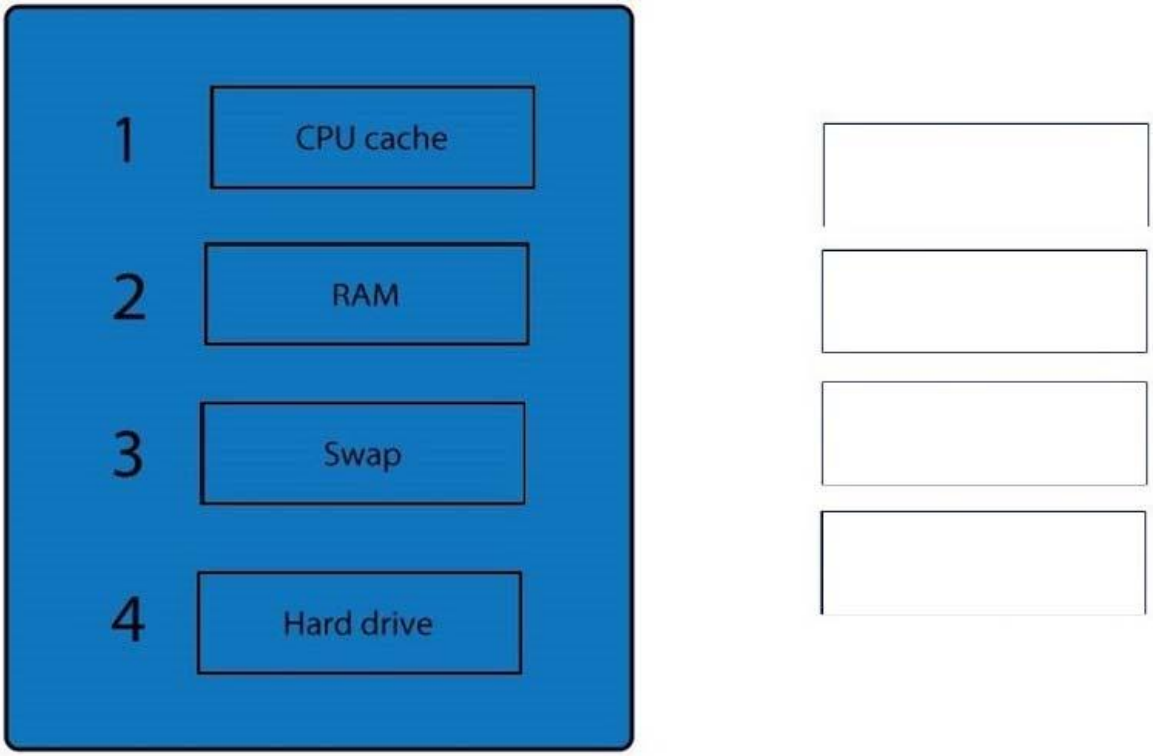
DRAG DROP

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

Select and Place:



Answer:



Explanation

Explanation/Reference:
Explanation:

When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.
Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

QUESTION 237

A company wants to host a publicly available server that performs the following functions:

- Evaluates MX record lookup
- Can perform authenticated requests for A and AAA records
- Uses RRSIG

Which of the following should the company use to fulfill the above requirements?

A. DNSSEC
B. SFTP
C. nslookup
D. dig
E. LDAPS

Answer: A

Explanation

Explanation/Reference:
Explanation:
DNS Security Extensions (DNSSEC) provides, among other things, cryptographic authenticity of responses using Resource Record Signatures (RRSIG) and authenticated denial of existence using Next-Secure (NSEC) and Hashed-NSEC records (NSEC3).

QUESTION 238

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 Qfor 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

Answer: B

Explanation

Explanation/Reference:

QUESTION 239

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

Answer: A

Explanation

Explanation/Reference:

QUESTION 240
A computer on a company network was infected with a zero-day exploit after an employee accidently opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidently 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

Answer: B

Explanation

Explanation/Reference:

QUESTION 241
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

Answer: C

Explanation

Explanation/Reference:

QUESTION 242
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. HMAC
B. PCBC
C. CBC
D. GCM
E. CFB

Answer: A

Explanation

Explanation/Reference:

QUESTION 243
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

Answer: A

Explanation

Explanation/Reference:
Explanation:
This is a way to update all internal sites without incurring additional costs?
To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

QUESTION 244
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

Answer: C

Explanation

Explanation/Reference:
Explanation:

A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

QUESTION 245

A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access.

Which of the following would be the BEST course of action?

A. Modify all the shared files with read only permissions for the intern.
B. Create a new group that has only read permissions for the files.
C. Remove all permissions for the shared files.
D. Add the intern to the "Purchasing" group.

Answer: B

Explanation

Explanation/Reference:

QUESTION 246

A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected.

To protect the laptops while connected to untrusted wireless networks, which of the following would be the BEST method for reducing the risk of having the laptops compromised?

A. MAC filtering
B. Virtualization
C. OS hardening
D. Application white-listing

Answer: C

Explanation

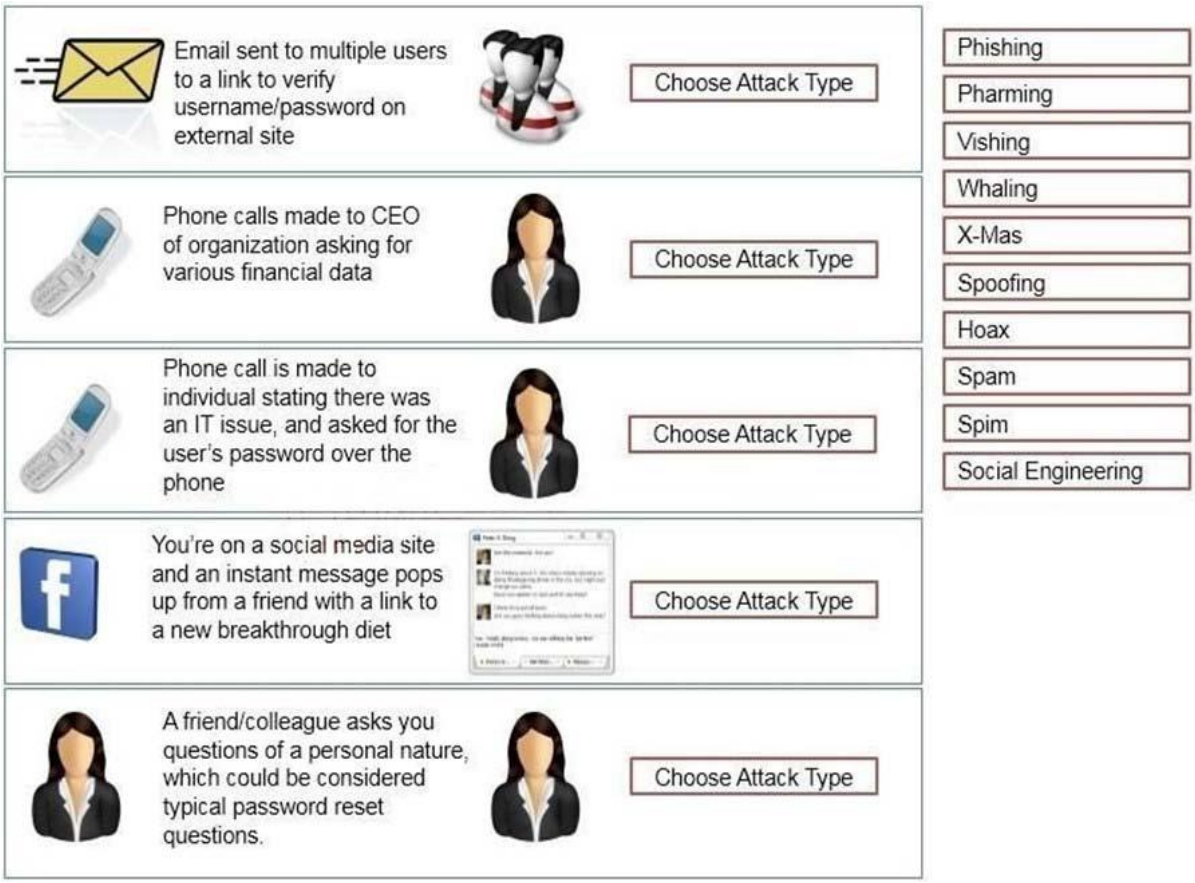
Explanation/Reference:

QUESTION 247

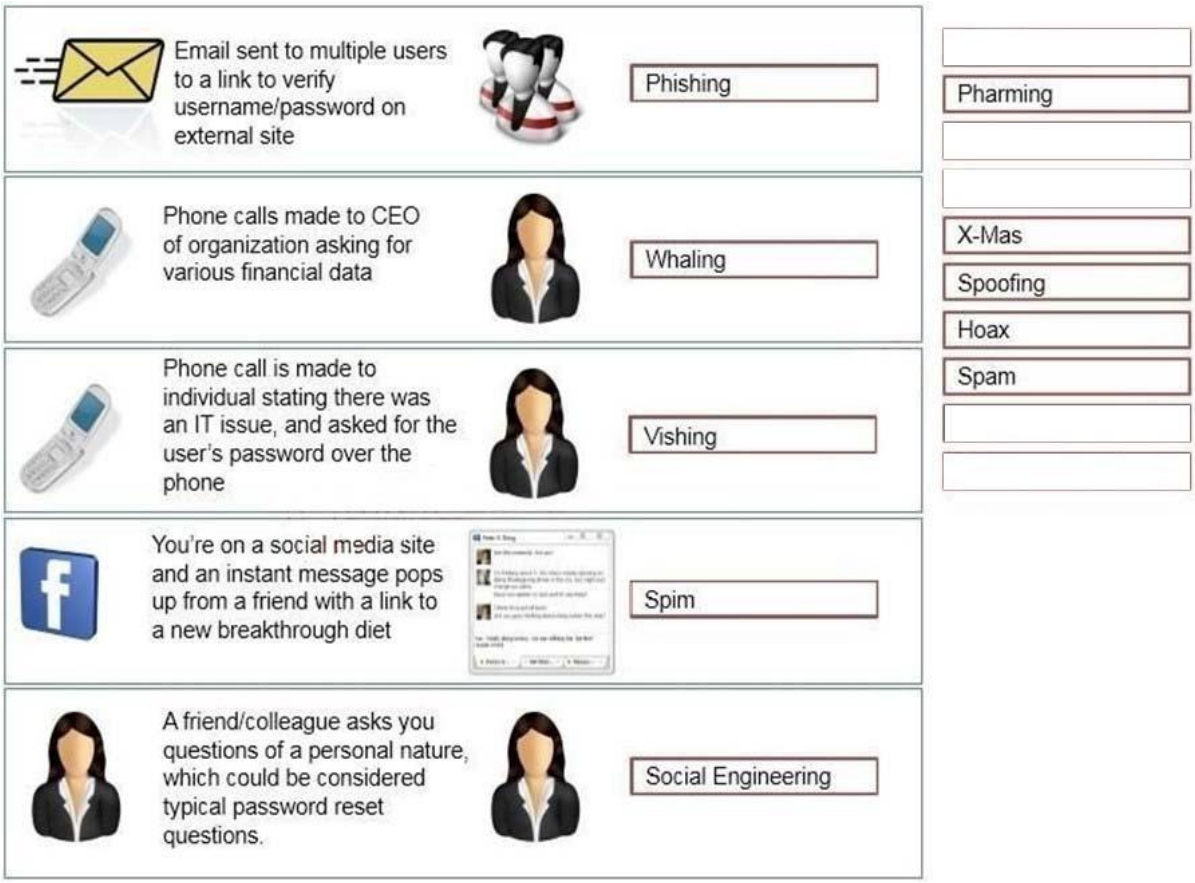
DRAG DROP

Task: Determine the types of attacks below by selecting an option from the dropdown list.

Select and Place:


Email sent to multiple users to a link to verify username/password on external site
Choose Attack Type
Phone calls made to CEO of organization asking for various financial data
Choose Attack Type
Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone
Choose Attack Type
You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet
Choose Attack Type
A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.
Choose Attack Type
Phishing
Pharming
Vishing
Whaling
X-Mas
Spoofing
Hoax
Spam
Spim
Social Engineering

Answer:



Explanation

Explanation/Reference:
Explanation:

A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.

C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS)

E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.

http://www.webopedia.com/TERM/P/phishing.html
http://www.techopedia.com/definition/28643/whaling
http://www.webopedia.com/TERM/V/vishing.html
http://searchsecurity.techtarget.com/definition/social-engineering

QUESTION 248

SIMULATION

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.

The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.

In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.

In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.

The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.

Instructions: The original security controls for each office can be reset at any time by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.


Public Cafe
Available Security Controls
128-bit key
64-bit key
Pre-share Key
PKI certificate
SSH Key
Pin Pad
Reset All
Save
Exit


Help Desk
Available Security Controls
Iris Scanner
Thumbprint Scanner
Password
Proximity Badge
Voice Recognition
Pin Pad
Reset All
Save
Exit

Answer: See the solution below.

Explanation

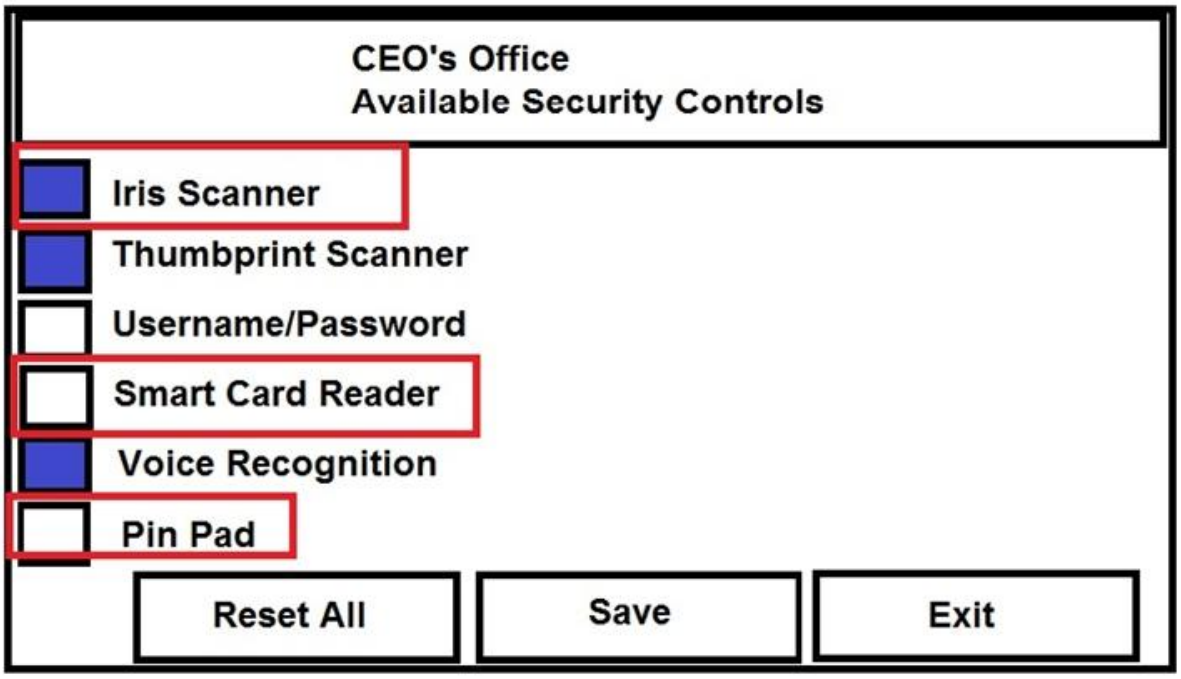
Explanation/Reference:
Explanation:


PII Processing Office
Available Security Controls
Iris Scanner
Thumbprint Scanner
Proximity Badge
Smart Card Reader
One Time Password Token
Pin Pad
Reset All
Save
Exit


Public Cafe
Available Security Controls
128-bit key
64-bit key
Pre-share Key
PKI certificate
SSH Key
Pin Pad
Reset All
Save
Exit


Help Desk
Available Security Controls
Iris Scanner
Thumbprint Scanner
Password
Proximity Badge
Voice Recognition
Pin Pad
Reset All
Save
Exit

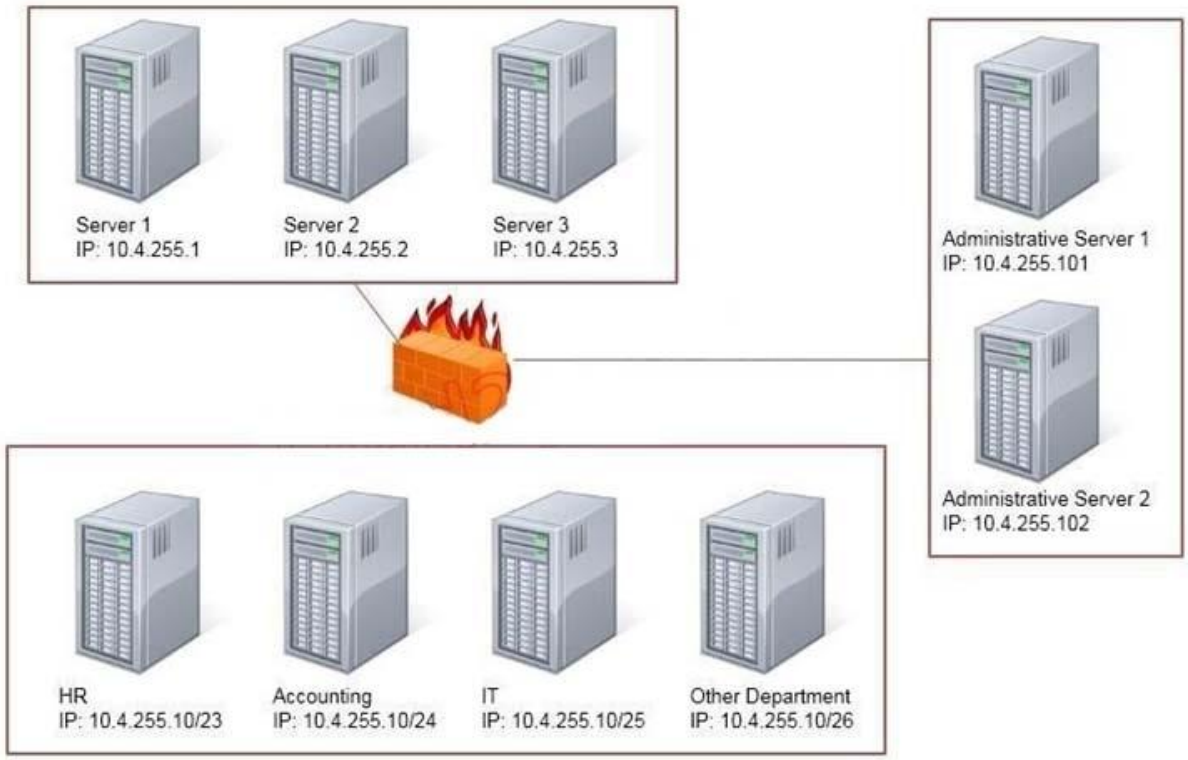

Data Center
Available Security Controls
Iris Scanner
Thumbprint Scanner
Mantrap
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit



QUESTION 249
SIMULATION

Task: Configure the firewall (fill out the table) to allow these four rules:

- Only allow the Accounting computer to have HTTPS access to the Administrative server.
- Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
- Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

Answer: See the solution below.

Explanation

Explanation/Reference:
Explanation:

Use the following answer for this simulation task.
Below table has all the answers required for this question.

Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny
10.4.255.10/24	10.4.255.101	443	TCP	Allow
10.4.255.10/23	10.4.255.2	22	TCP	Allow
10.4.255.10/25	10.4.255.101	Any	Any	Allow
10.4.255.10/25	10.4.255.102	Any	Any	Allow

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the

internal network. Three possible actions can be taken based on the rule's criteria:

Block the connection Allow the connection
Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent.
Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session.
When the session ends, the connection is torn down.
UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP.
The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications.
The primary purpose of UDP is to send small packets of information.
The application is responsible for acknowledging the correct reception of the data. Port 22 is used by both SSH and SCP with UDP.
Port 443 is used for secure web connections? HTTPS and is a TCP port.
Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)
Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between: 10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)
10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

QUESTION 250

HOTSPOT

For each of the given items, select the appropriate authentication category from the dropdown choices.
Instructions: When you have completed the simulation, please select the Done button to submit.

Hot Area:

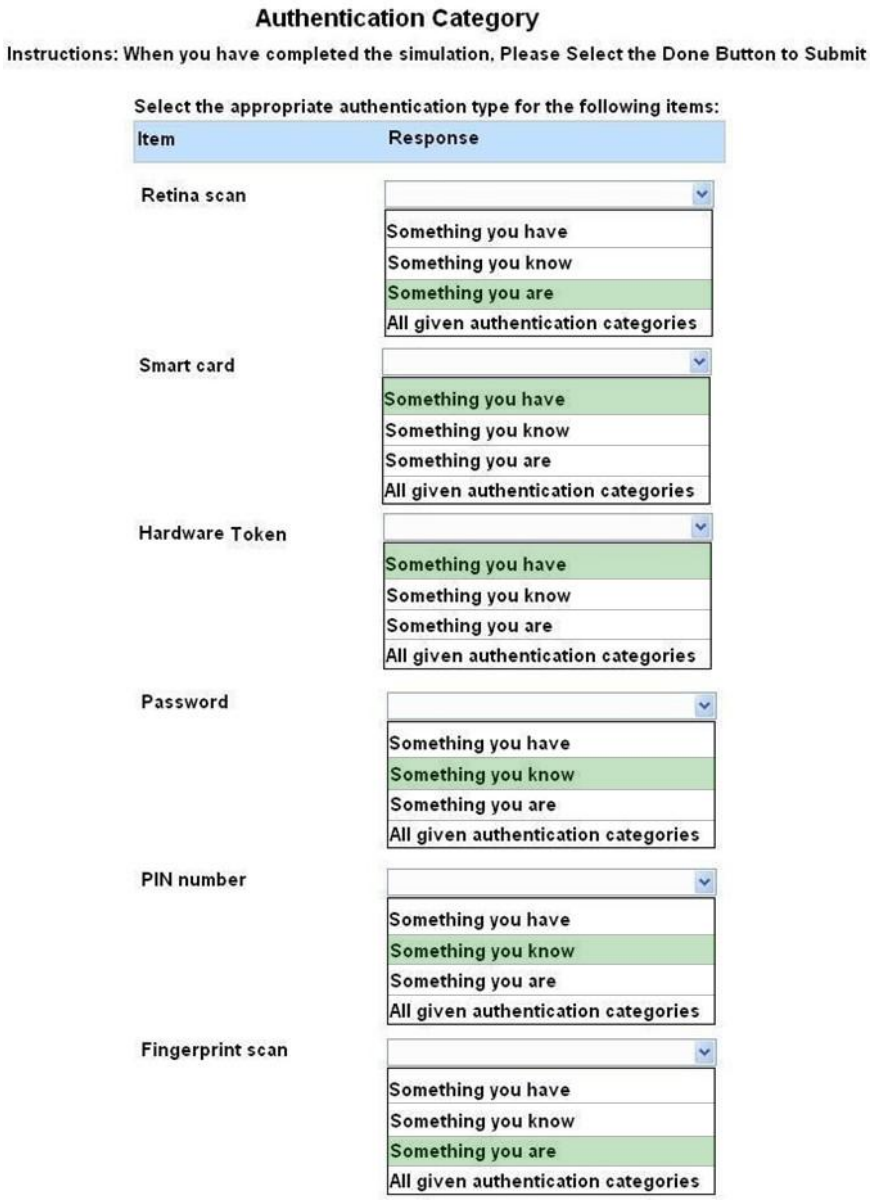
Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	Something you have Something you know Something you are All given authentication categories
Smart card	Something you have Something you know Something you are All given authentication categories
Hardware Token	Something you have Something you know Something you are All given authentication categories
Password	Something you have Something you know Something you are All given authentication categories
PIN number	Something you have Something you know Something you are All given authentication categories
Fingerprint scan	Something you have Something you know Something you are All given authentication categories

Answer:



Explanation

Explanation/Reference:
Answer:

Something you are includes fingerprints, retina scans, or voice recognition.
Something you have includes smart cards, token devices, or keys.
Something you know includes a password, codes, PINs, combinations, or secret phrases. Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.
Something you do includes your typing rhythm, a secret handshake, or a private knock http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle http://en.wikipedia.org/wiki/Smart_card#Security

QUESTION 251
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?