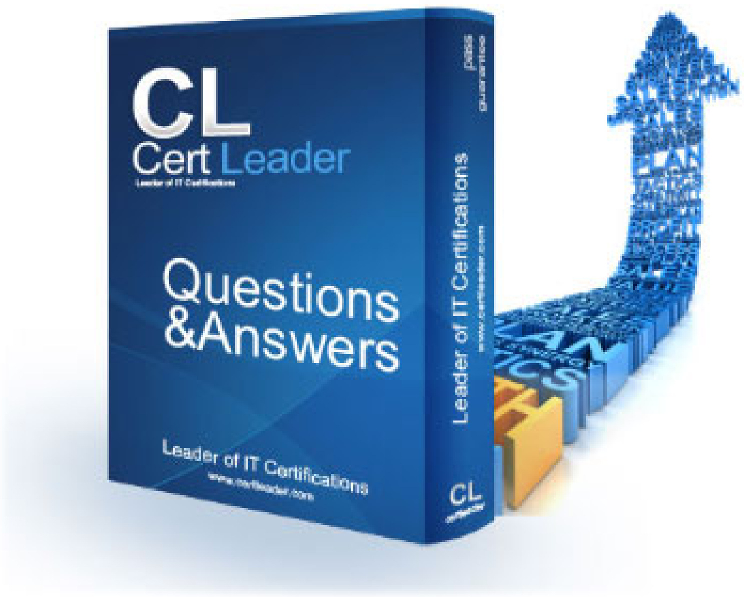
SY0-501 Dumps

CompTIA Security+ Certification Exam

https://www.certleader.com/SY0-501-dumps.html



NEW QUESTION 1
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

NEW QUESTION 2
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

NEW QUESTION 3
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

NEW QUESTION 4
Which of the following types of keys is found in a key escrow?

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

Answer: B

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

NEW QUESTION 5
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: A

NEW QUESTION 6
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

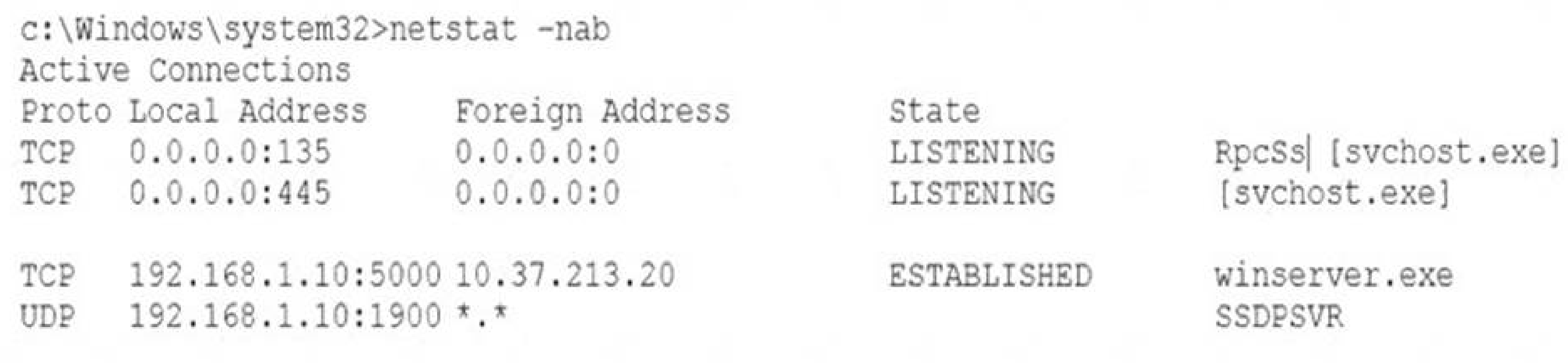
NEW QUESTION 7
Which of the following would a security specialist be able to determine upon examination of a server’s certificate?

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

D. OID

Answer: D

NEW QUESTION 8
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: D

NEW QUESTION 9
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: D

NEW QUESTION 10
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

NEW QUESTION 10
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: E

NEW QUESTION 13
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

NEW QUESTION 14
Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Select 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.

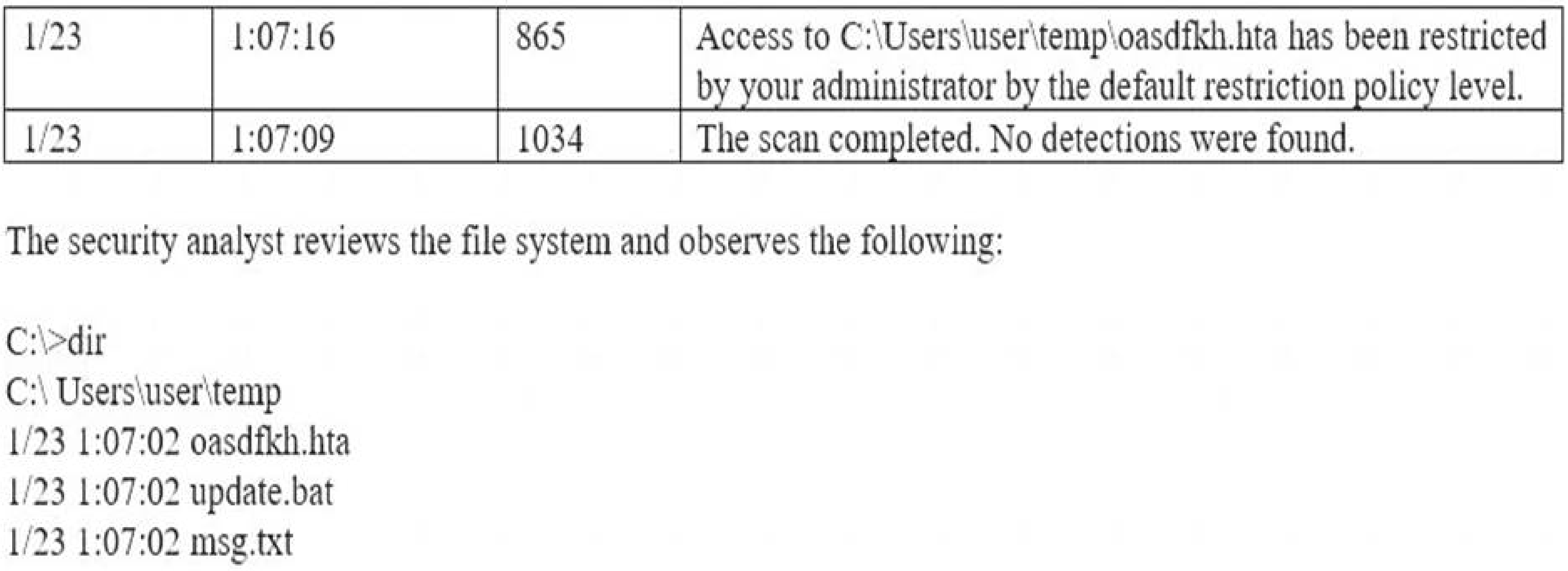
Answer: BE

NEW QUESTION 19
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

NEW QUESTION 22
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

NEW QUESTION 25
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

NEW QUESTION 26
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

NEW QUESTION 27
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? (Select two.)

A. Password expiration
B. Password length
C. Password complexity
D. Password history
E. Password lockout

Answer: CD

NEW QUESTION 28
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.

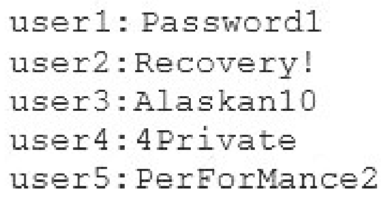
Answer: B

NEW QUESTION 29
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

NEW QUESTION 32
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

NEW QUESTION 37
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

NEW QUESTION 38
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

NEW QUESTION 41
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

NEW QUESTION 43
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

NEW QUESTION 45
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

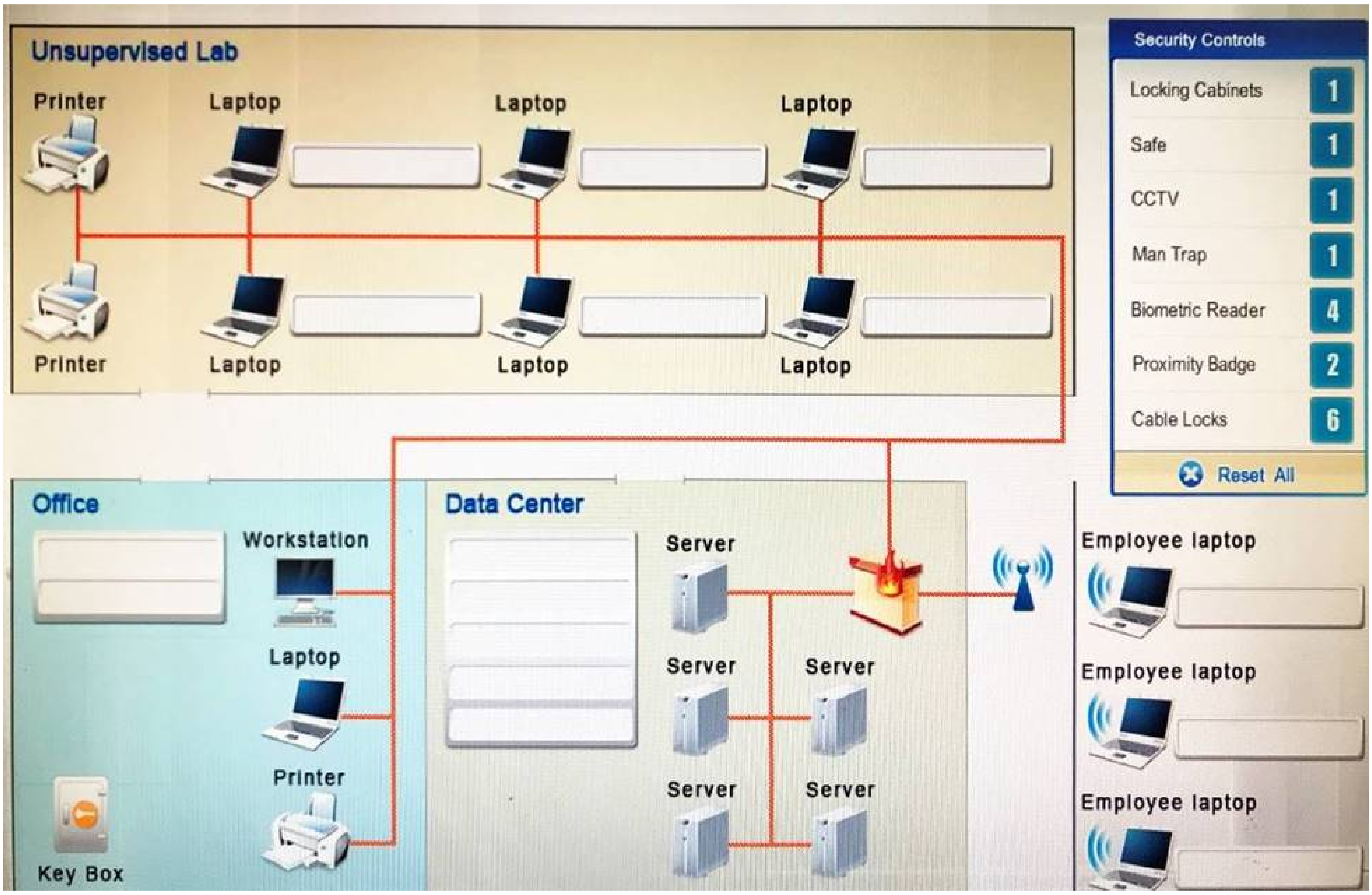
Explanation: http://archive.oreilly.com/pub/a/wireless/2005/01/01/authentication.html

NEW QUESTION 46
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

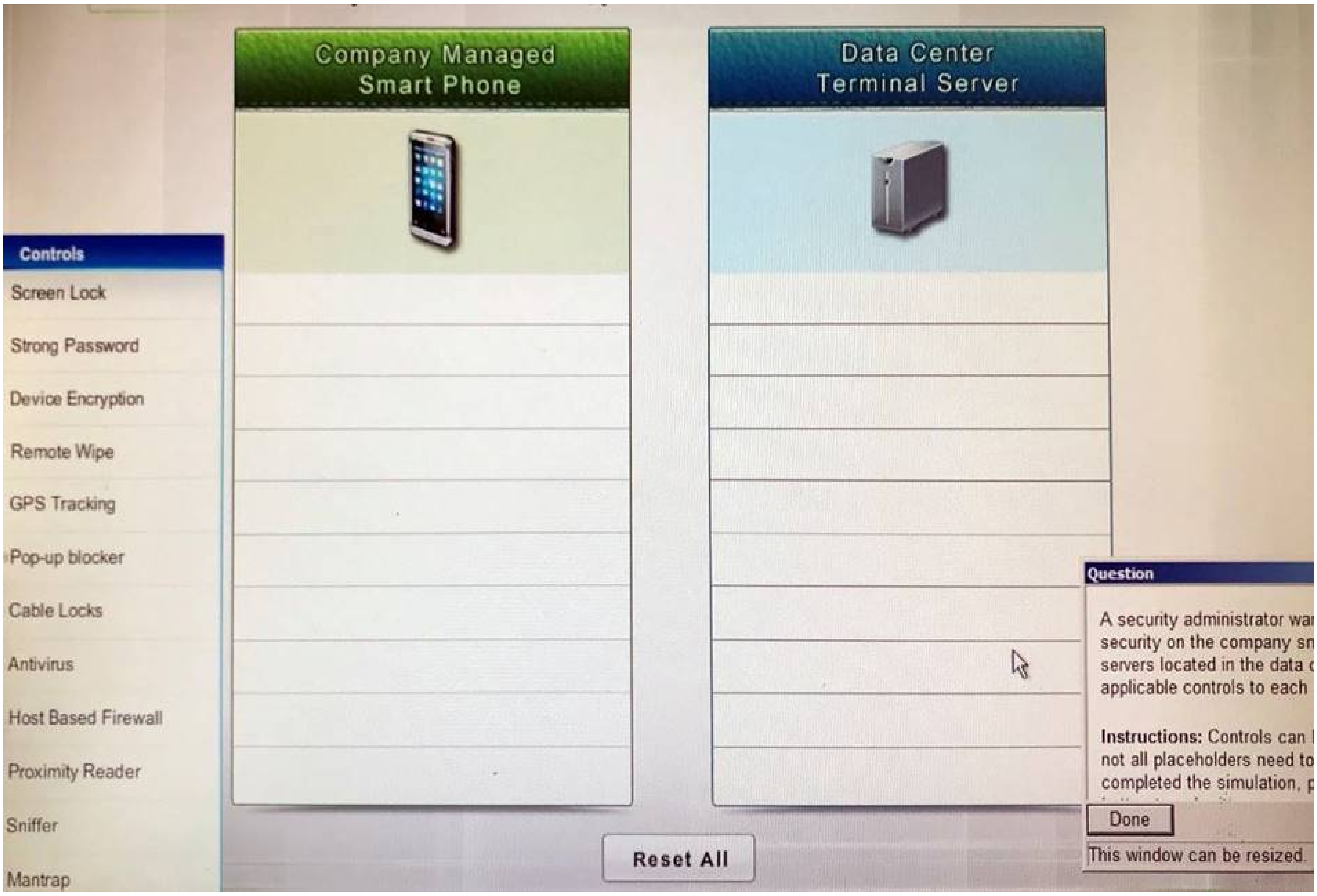
NEW QUESTION 48
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.
Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.



Answer:

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.

NEW QUESTION 53
A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset types?
Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.



A security administrator wa
security on the company sn
servers located in the data c
applicable controls to each

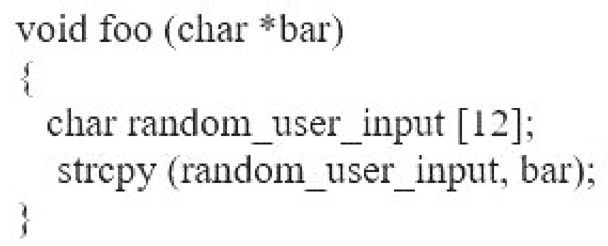
Instructions: Controls can l
not all placeholders need to
completed the simulation, p

This window can be resized.

Answer:

Explanation: Company Manages Smart Phone Screen Lock
Strong Password Device Encryption Remote Wipe GPS Tracking
Pop-up blocker
Data Center Terminal Server Cable Locks
Antivirus
Host Based Firewall Proximity Reader Sniffer
Mantrap

NEW QUESTION 58
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

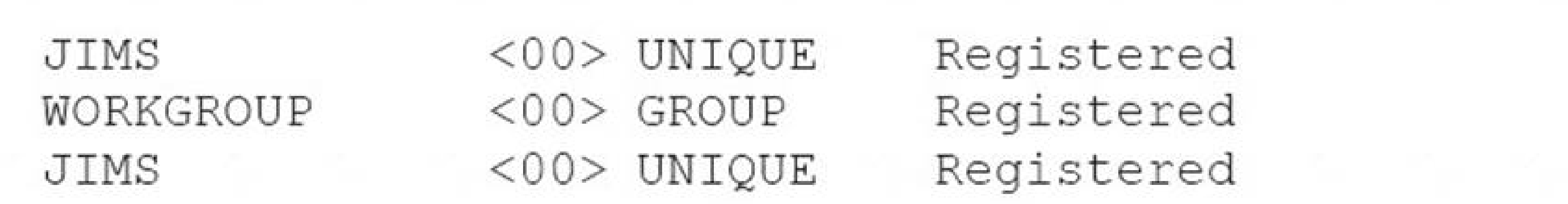
NEW QUESTION 60
When trying to log onto a company’s new ticketing system, some employees receive the following message: Access denied: too many concurrent sessions. The ticketing system was recently installed on a small VM with only the recommended hardware specifications. Which of the following is the 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

NEW QUESTION 65
An auditor wants to test the security posture of an organization by running a tool that will display the following:



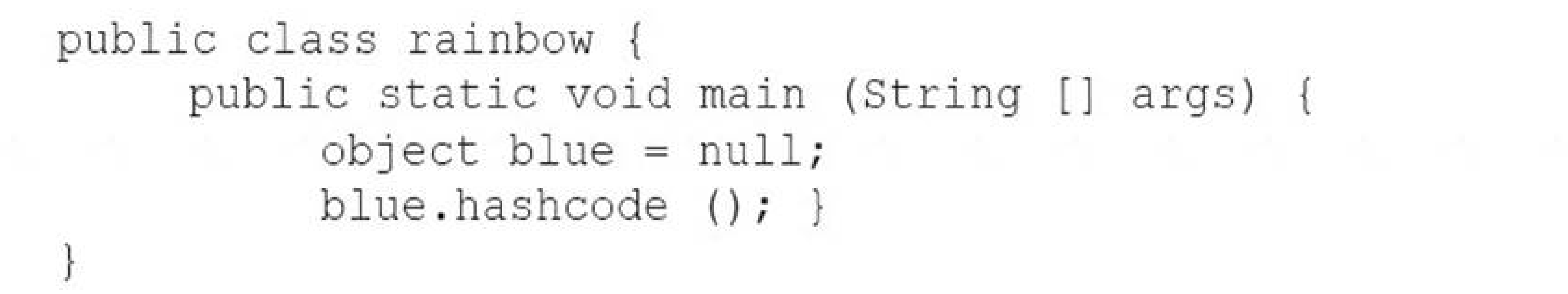
```
JIMS              <00> UNIQUE    Registered
WORKGROUP         <00> GROUP     Registered
JIMS              <00> UNIQUE    Registered
```

Which of the following commands should be used?

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

Answer: A

NEW QUESTION 68
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

NEW QUESTION 70
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

NEW QUESTION 71
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

NEW QUESTION 72
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

NEW QUESTION 76
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

NEW QUESTION 81
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

NEW QUESTION 85
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

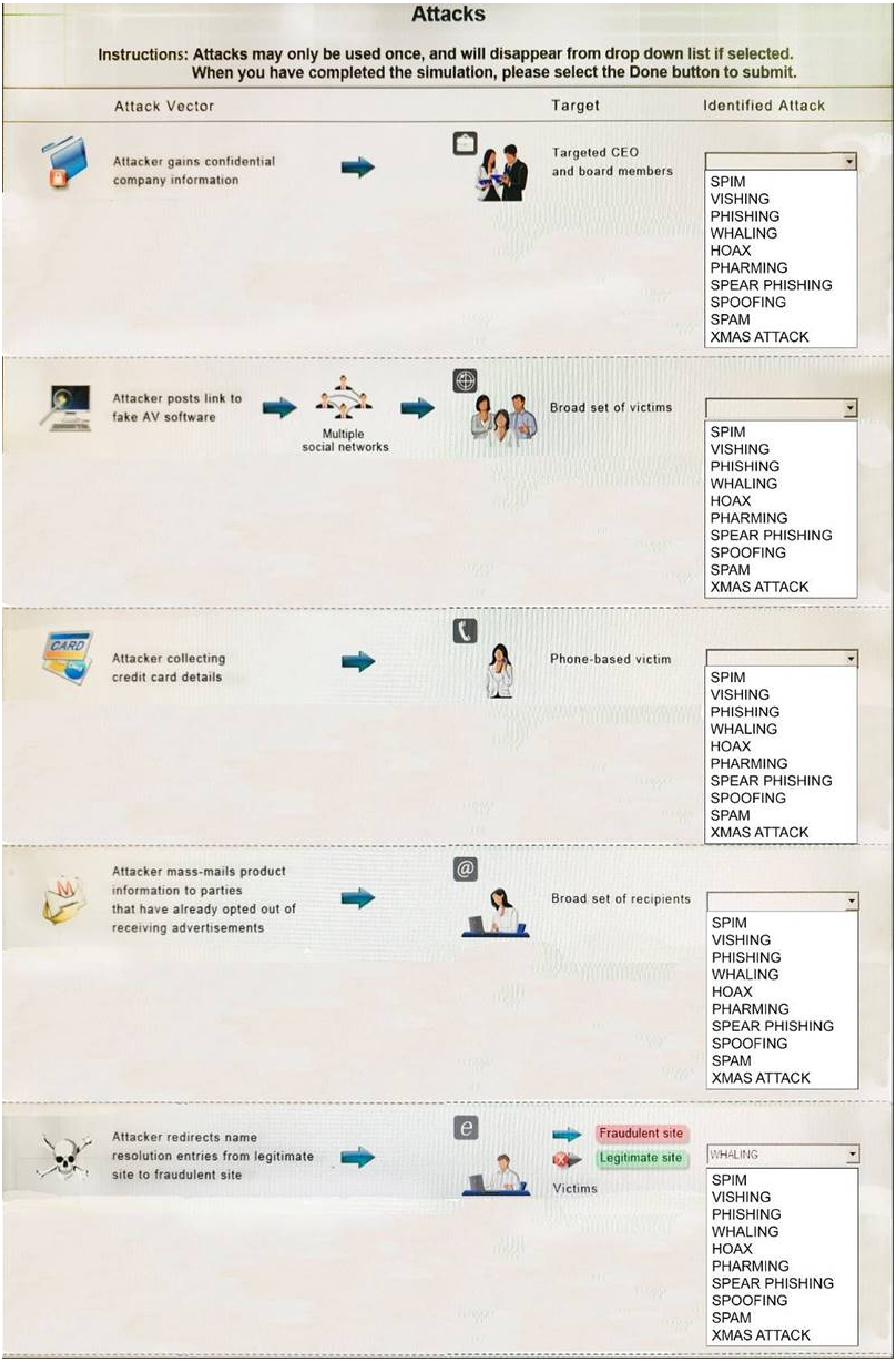
Answer: C

NEW QUESTION 88
Which of the following technologies employ the use of SAML? (Select two.)

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

Answer: AB

NEW QUESTION 92
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.



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: 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: 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.
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

NEW QUESTION 96
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

NEW QUESTION 98
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: D

NEW QUESTION 100
When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Select two.)

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

Answer: BE

NEW QUESTION 105
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

NEW QUESTION 110
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

NEW QUESTION 115
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

NEW QUESTION 117
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

NEW QUESTION 119
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? (Select 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.

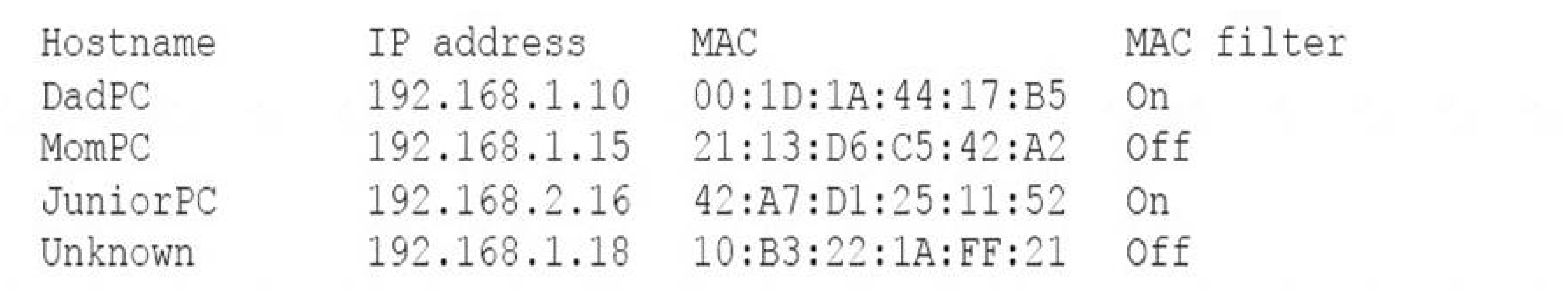
Answer: AD

NEW QUESTION 121
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

NEW QUESTION 124
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: C

NEW QUESTION 126
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? (Select three.)

A. S/MIME
B. SSH
C. SNMPv3
D. FTPS

E. SRTP
F. HTTPS
G. LDAPS

Answer: BDF

NEW QUESTION 127
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

NEW QUESTION 131
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

NEW QUESTION 134
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

NEW QUESTION 136
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

NEW QUESTION 138
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: D

NEW QUESTION 140
Which of the following AES modes of operation provide authentication? (Select two.)

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

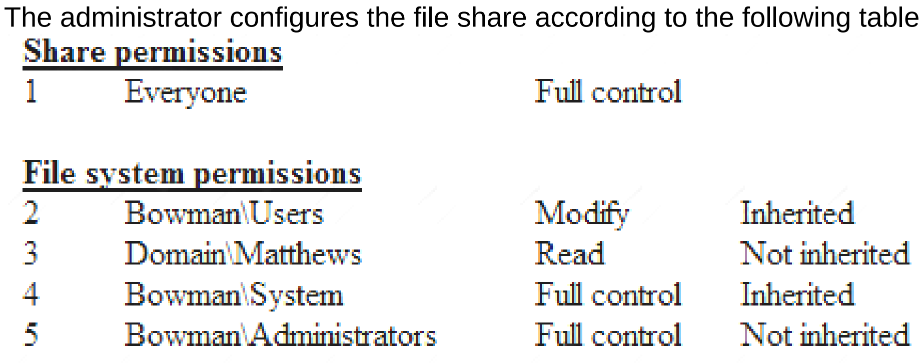
Answer: AC

NEW QUESTION 143
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

NEW QUESTION 144
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

NEW QUESTION 146
Which of the following differentiates a collision attack from a rainbow table attack?

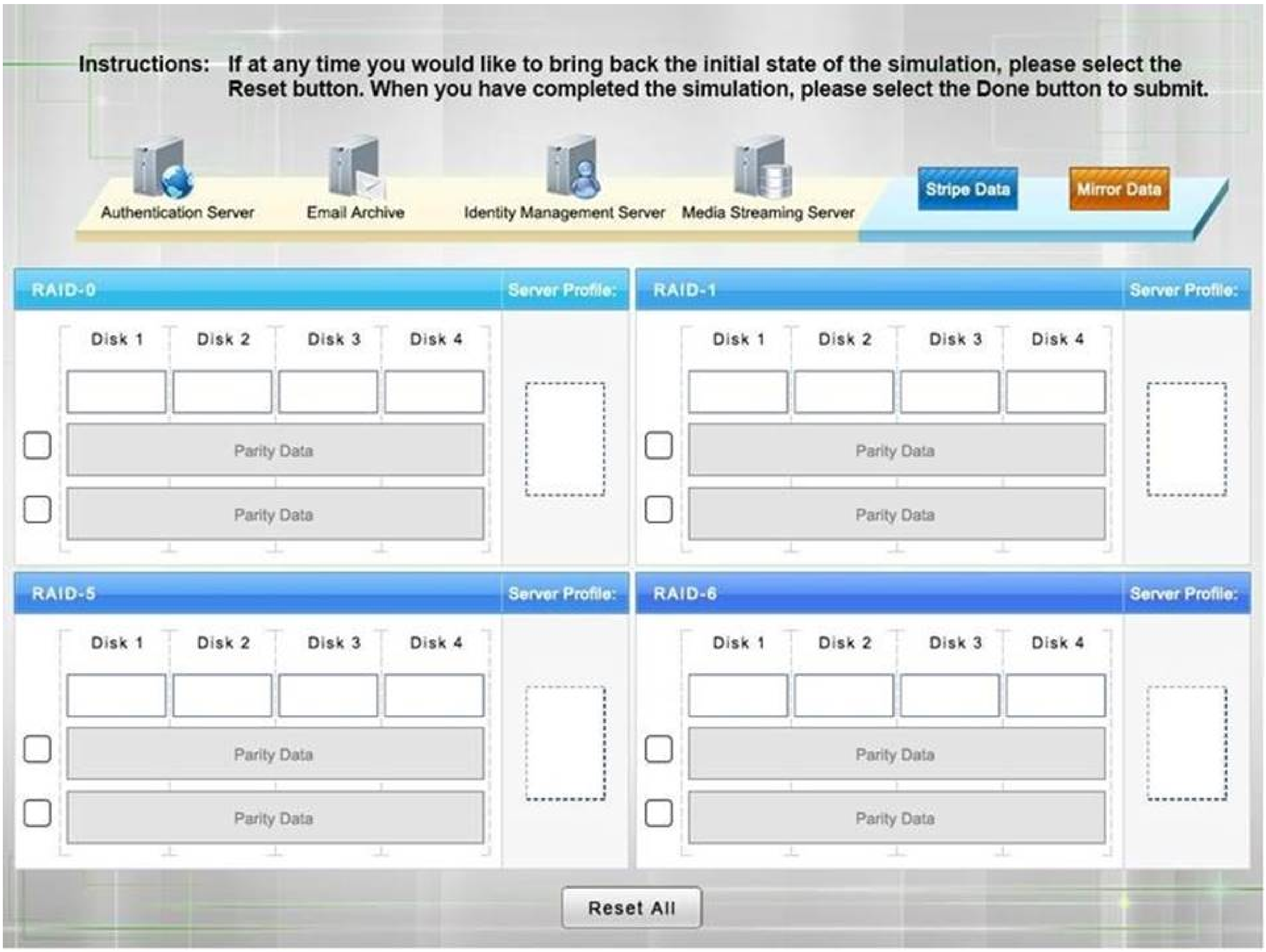
A. A rainbow table attack performs a hash lookup
B. A rainbow table attack uses the hash as a password
C. In a collision attack, the hash and the input data are equivalent
D. In a collision attack, the same input results in different hashes

Answer: A

NEW QUESTION 151
A security administrator is given the security and availability profiles for servers that are being deployed.

- Match each RAID type with the correct configuration and MINIMUM number of drives.
- 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.



Instructions: 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.

Answer:

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

NEW QUESTION 152
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

NEW QUESTION 157
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

NEW QUESTION 158
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

NEW QUESTION 159
After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition.
Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO)

A. Monitor VPN client access
B. Reduce failed login 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

NEW QUESTION 160
Which of the following are methods to implement HA in a web application server environment? (Select two.)

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

Answer: AB

NEW QUESTION 164
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: A

NEW QUESTION 168
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

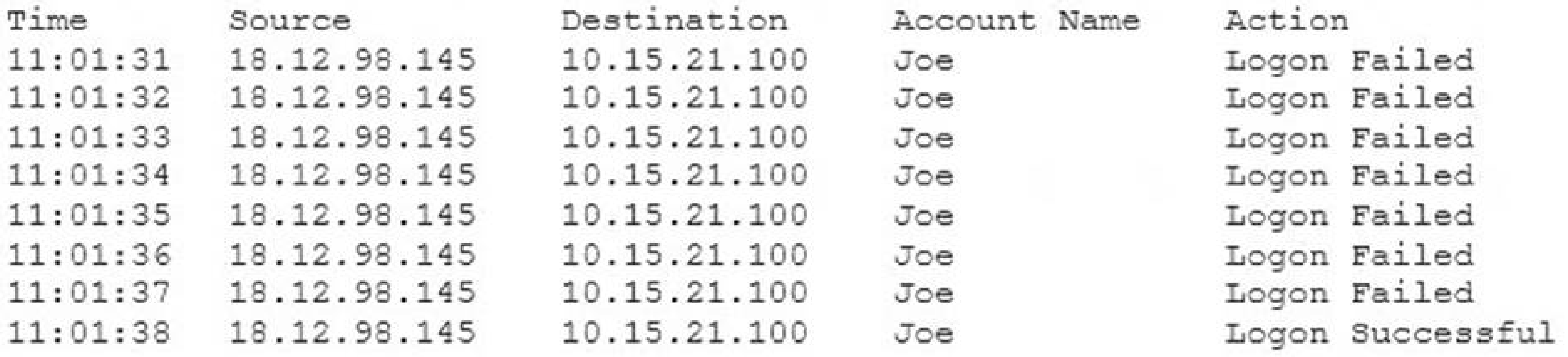
Answer: B

NEW QUESTION 172
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

NEW QUESTION 174
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

NEW QUESTION 177
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

NEW QUESTION 179
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? (Select two.)

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

Answer: BD

NEW QUESTION 184
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

NEW QUESTION 189
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

NEW QUESTION 193
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

NEW QUESTION 196
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

NEW QUESTION 201
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 cach
C. Remote logging data, paging/swap files
D. Paging/swap files, CPU cache, RAM, remote logging data
E. CPU cache, RAM, paging/swap files, remote logging data

Answer: D

NEW QUESTION 205
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

NEW QUESTION 207
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

NEW QUESTION 210
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

NEW QUESTION 211
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

NEW QUESTION 213

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

NEW QUESTION 217
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

NEW QUESTION 218
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

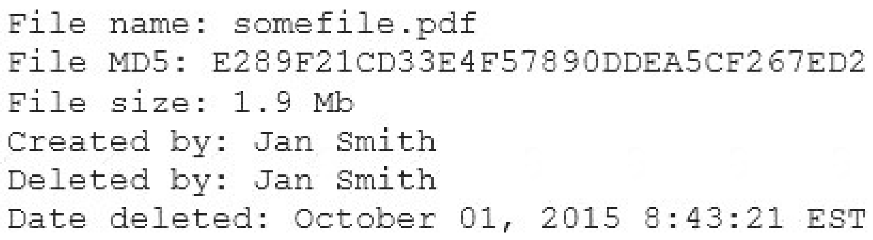
Answer: A

NEW QUESTION 219
An information security analyst needs to work with an employee who can answer QUESTION NO:s 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

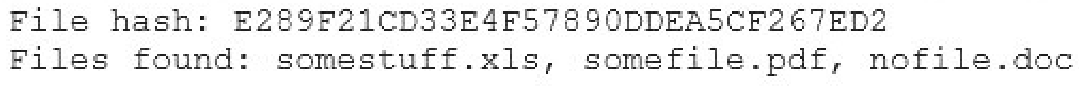
Answer: B

NEW QUESTION 223
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

NEW QUESTION 228
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: A

NEW QUESTION 230
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

NEW QUESTION 231
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

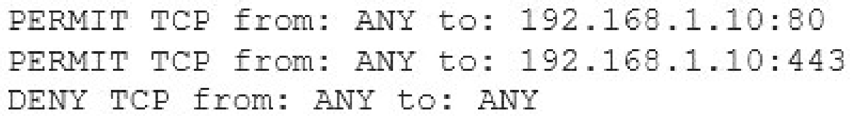
Answer: C

NEW QUESTION 234
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

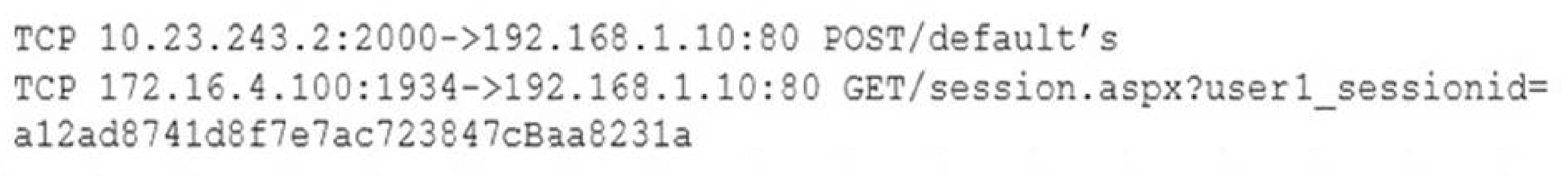
Answer: B

NEW QUESTION 239
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

NEW QUESTION 244
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

NEW QUESTION 246
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

NEW QUESTION 248
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

NEW QUESTION 251
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

NEW QUESTION 254
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: A

NEW QUESTION 256
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

NEW QUESTION 257
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

NEW QUESTION 262
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

NEW QUESTION 264
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? (Select two.)

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

Answer: AE

NEW QUESTION 269
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: C

NEW QUESTION 270
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

NEW QUESTION 271
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

NEW QUESTION 275
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: D

NEW QUESTION 278
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

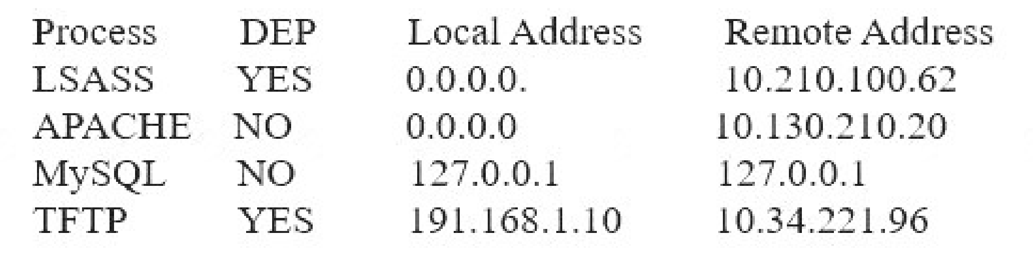
Answer: C

NEW QUESTION 279
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

NEW QUESTION 281
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

NEW QUESTION 283
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

NEW QUESTION 285
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: A

NEW QUESTION 287
The Chief Executive Officer (CEO) of a major defense contracting company a traveling overseas for a conference. The CEO will be taking a laptop. Which of the following should the security administrator implement to ensure confidentiality of the data if the
laptop were to be stolen or lost during the trip?

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

Answer: B

NEW QUESTION 291
A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

A. RSA
B. TwoFish

C. Diffie-Helman
D. NTLMv2
E. RIPEMD

Answer: B

NEW QUESTION 293
A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently, the organization uses FTP and HTTP to transfer files. Which of the following should the organization implement in order to be compliant with the new policy?

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

Answer: A

NEW QUESTION 294
A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources. Which of the following should be implemented?

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

Answer: B

NEW QUESTION 295
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

NEW QUESTION 300
A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non- repudiation. Which of the following implements all these requirements?

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

Answer: C

NEW QUESTION 301
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: D

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.

NEW QUESTION 305
A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list. Which of the following BEST describes this type of IDS?

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

Answer: A

NEW QUESTION 306
After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internetbased control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence. Which of the following is the MOST likely reason the thermostat is not connecting to the internet?

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

Answer: C

NEW QUESTION 307
Which of the following should be used to implement voice encryption?

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

Answer: C

NEW QUESTION 309
Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive. Which of the following procedures did Joe follow?

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

Answer: A

NEW QUESTION 311
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

NEW QUESTION 315
Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain. Which of the following tools would aid her to decipher the network traffic?

A. Vulnerability Scanner
B. NMAP
C. NETSTAT
D. Packet Analyzer

Answer: C

NEW QUESTION 316
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

NEW QUESTION 321
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

NEW QUESTION 326
Malware that changes its binary pattern on specific dates at specific times to avoid detection is known as a (n):

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

Answer: C

NEW QUESTION 327
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: 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.

NEW QUESTION 331
Which of the following is the LEAST secure hashing algorithm?

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

Answer: C

NEW QUESTION 334
A security administrator has been asked to implement a VPN that will support remote access over IPSEC. Which of the following is an encryption algorithm that would meet this requirement?

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

Answer: B

NEW QUESTION 337
An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times. Which of the following describes this type of attack?

A. Integer overflow attack
B. Smurf attack
C. Replay attack
D. Buffer overflow attack
E. Cross-site scripting attack

Answer: C

NEW QUESTION 342
A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes.
Which of the following risk management strategies BEST describes management's response?

A. Deterrence
B. Mitigation

C. Avoidance
D. Acceptance

Answer: C

NEW QUESTION 347
During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?

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

Answer: D

NEW QUESTION 352
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? (Select TWO.)

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

Answer: CE

NEW QUESTION 356
A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations. Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)

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

Answer: AF

NEW QUESTION 360
Which of the following is the summary of loss for a given year?

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

Answer: B

NEW QUESTION 363
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: 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.

NEW QUESTION 368
Which of the following can affect electrostatic discharge in a network operations center?

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

Answer: D

NEW QUESTION 372
Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

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

Answer: D

NEW QUESTION 377
While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security?

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

Answer: A

NEW QUESTION 381
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: C

NEW QUESTION 382
Which of the following best describes the initial processing phase used in mobile device forensics?

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

Answer: D

NEW QUESTION 386
A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results. Which of the following is the best method for collecting this information?

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

Answer: A

NEW QUESTION 391
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: 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).

NEW QUESTION 396

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

NEW QUESTION 399
Which of the following is commonly used for federated identity management across multiple organizations?

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

Answer: A

NEW QUESTION 400
An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?

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

Answer: A

NEW QUESTION 402
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

NEW QUESTION 404
Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data. Which of the following controls can be implemented to mitigate this type of inside threat?

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

Answer: B

NEW QUESTION 409
Which of the following use the SSH protocol?

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

Answer: BF

NEW QUESTION 410
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: D

NEW QUESTION 415
A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected. Which of the following MUST the technician implement?

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

Answer: B

NEW QUESTION 418
During an application design, the development team specifics a LDAP module for single sign-on communication with the company's access control database. This is an example of which of the following?

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

Answer: D

NEW QUESTION 420
An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient.
Which of the following capabilities would be MOST appropriate to consider implementing is response to the new requirement?

A. Transitive trust
B. Symmetric encryption
C. Two-factor authentication
D. Digital signatures
E. One-time passwords

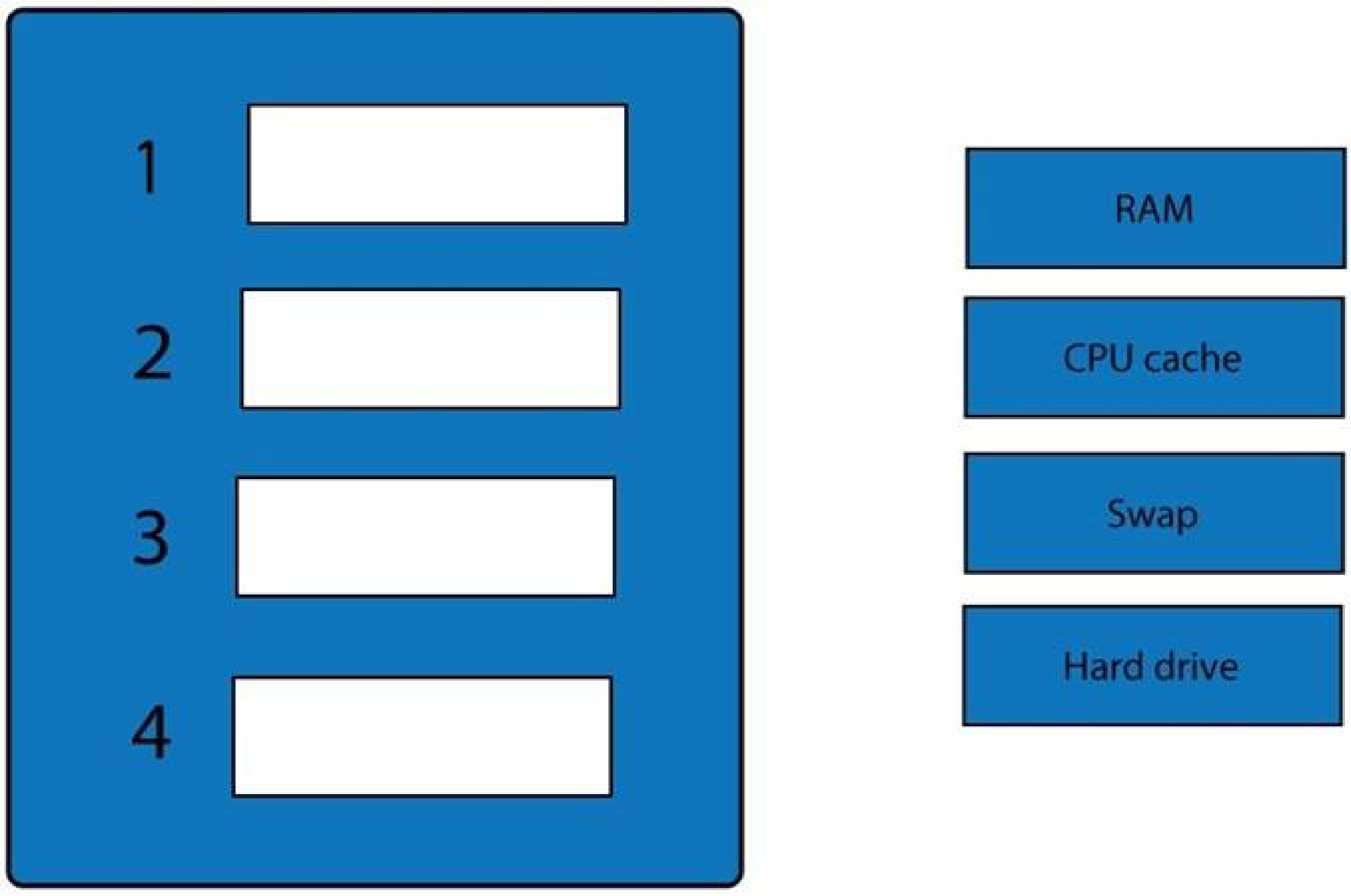
Answer: D

NEW QUESTION 425
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

NEW QUESTION 430
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.



Answer:

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.

NEW QUESTION 433
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

NEW QUESTION 437
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

NEW QUESTION 438
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

NEW QUESTION 439
The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate severs at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?

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

Answer: B

NEW QUESTION 444
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

NEW QUESTION 448
The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administer has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled. Which of the following would further obscure the presence of the wireless network?

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

Answer: D

NEW QUESTION 449
The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected. Which of the following is required to complete the certificate chain?

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

Answer: B

NEW QUESTION 454
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: 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.

NEW QUESTION 457
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

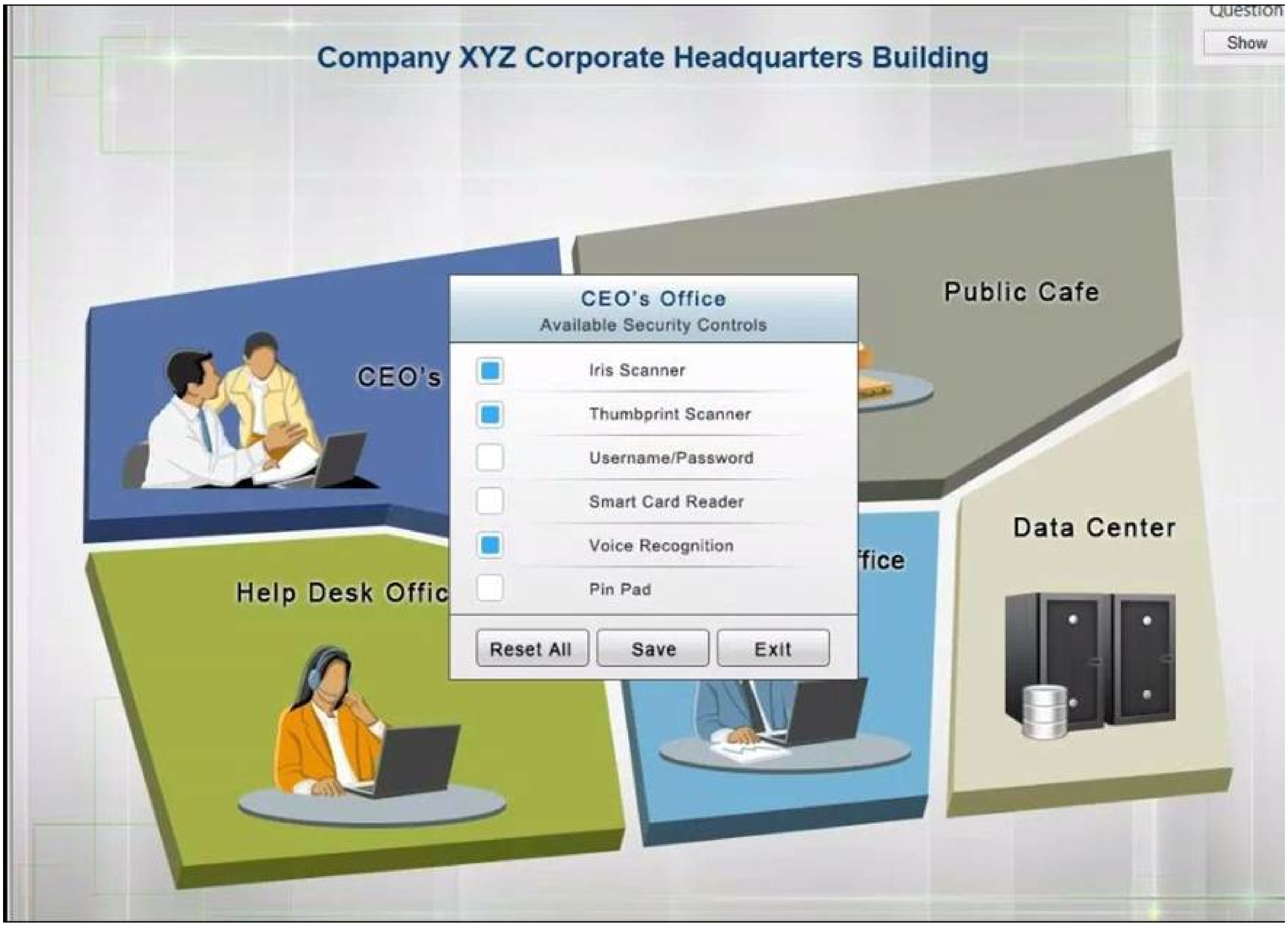
Answer: B

NEW QUESTION 458
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

NEW QUESTION 462
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.

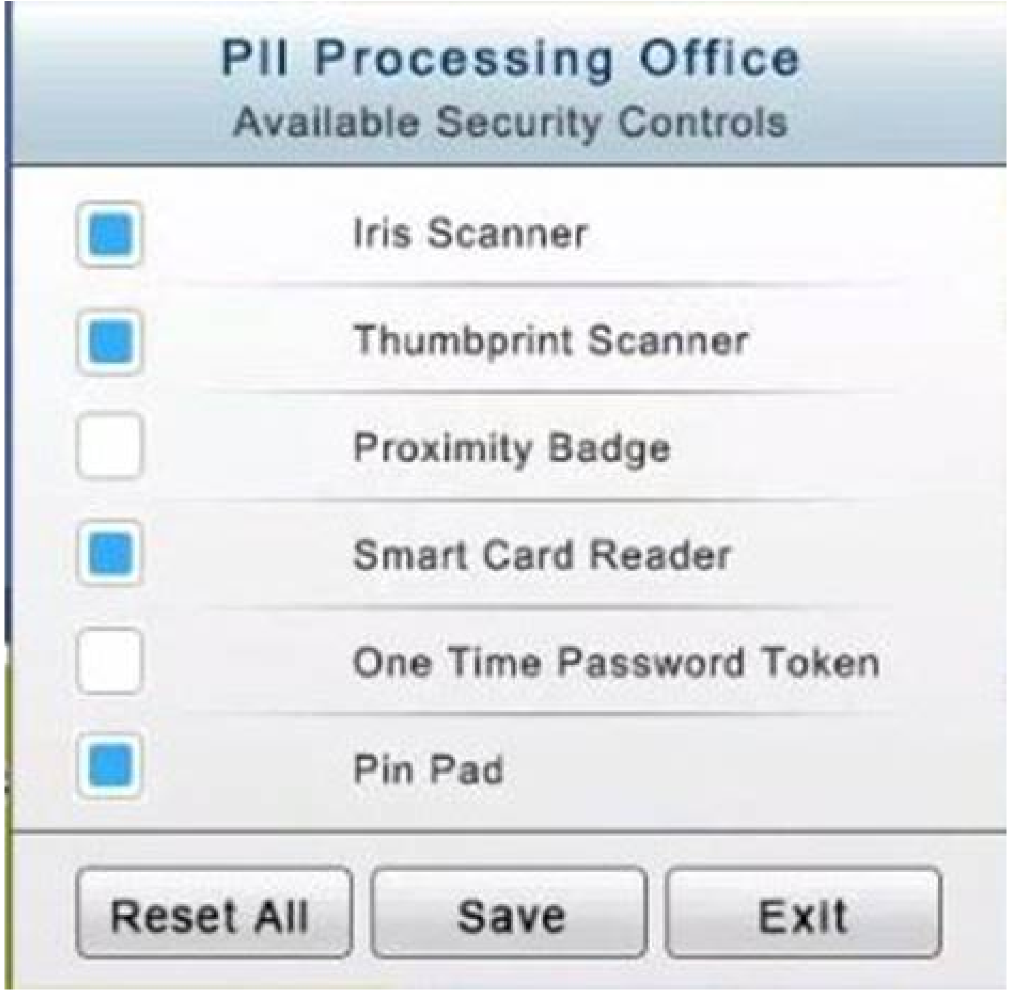


Company XYZ Corporate Headquarters Building

CEO's Office
Available Security Controls

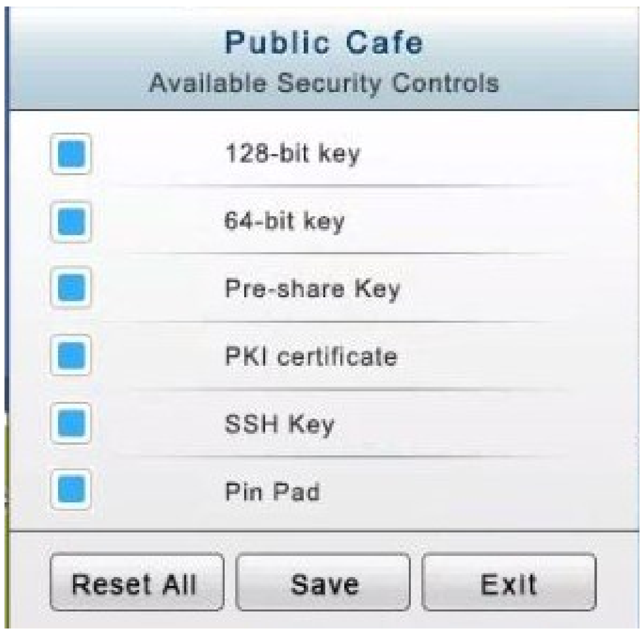
- ☑ Iris Scanner
- ☑ Thumbprint Scanner
- ☐ Username/Password
- ☐ Smart Card Reader
- ☑ Voice Recognition
- ☐ Pin Pad

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.



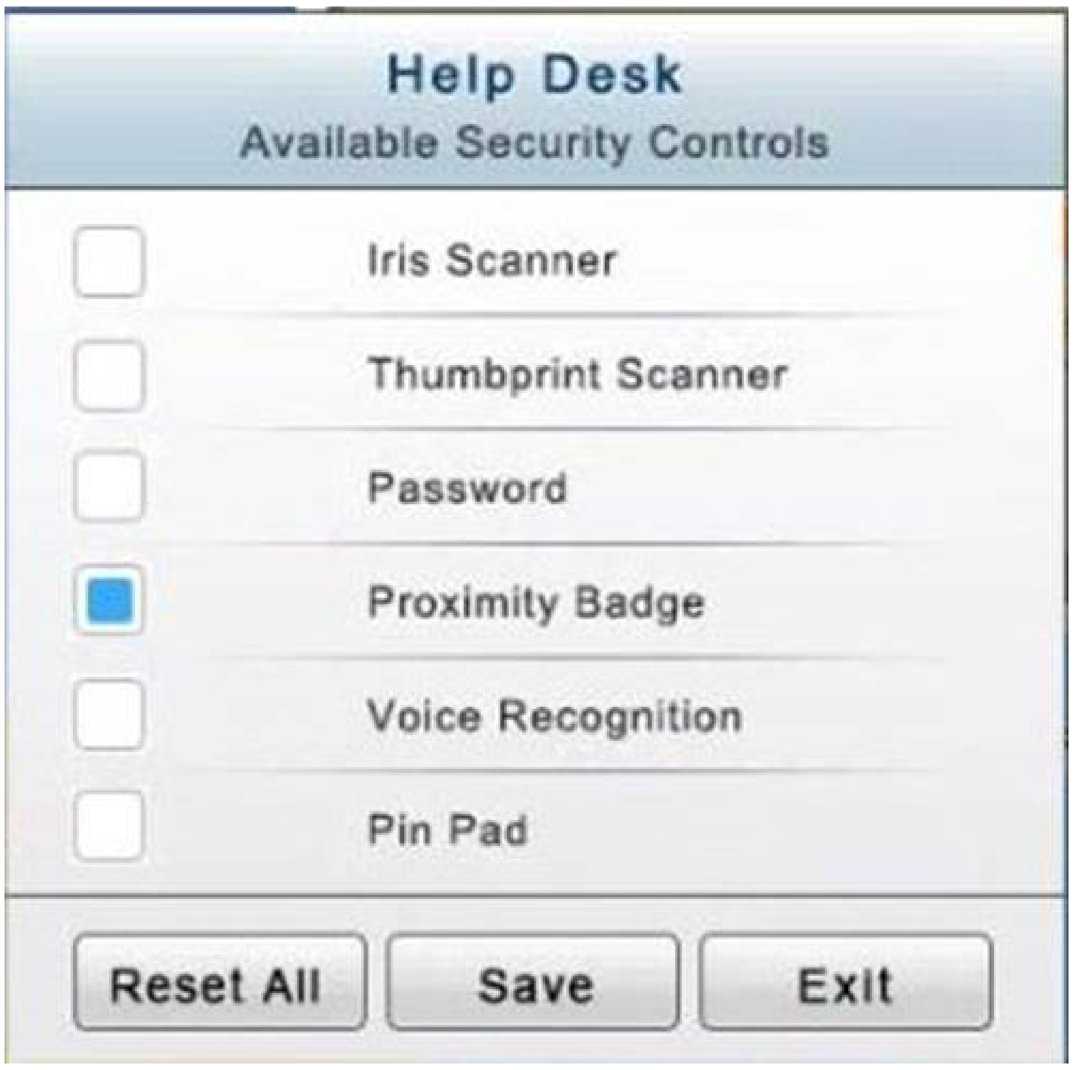
PII Processing Office
Available Security Controls

- ☑ Iris Scanner
- ☑ Thumbprint Scanner
- ☐ Proximity Badge
- ☑ Smart Card Reader
- ☐ One Time Password Token
- ☑ Pin Pad



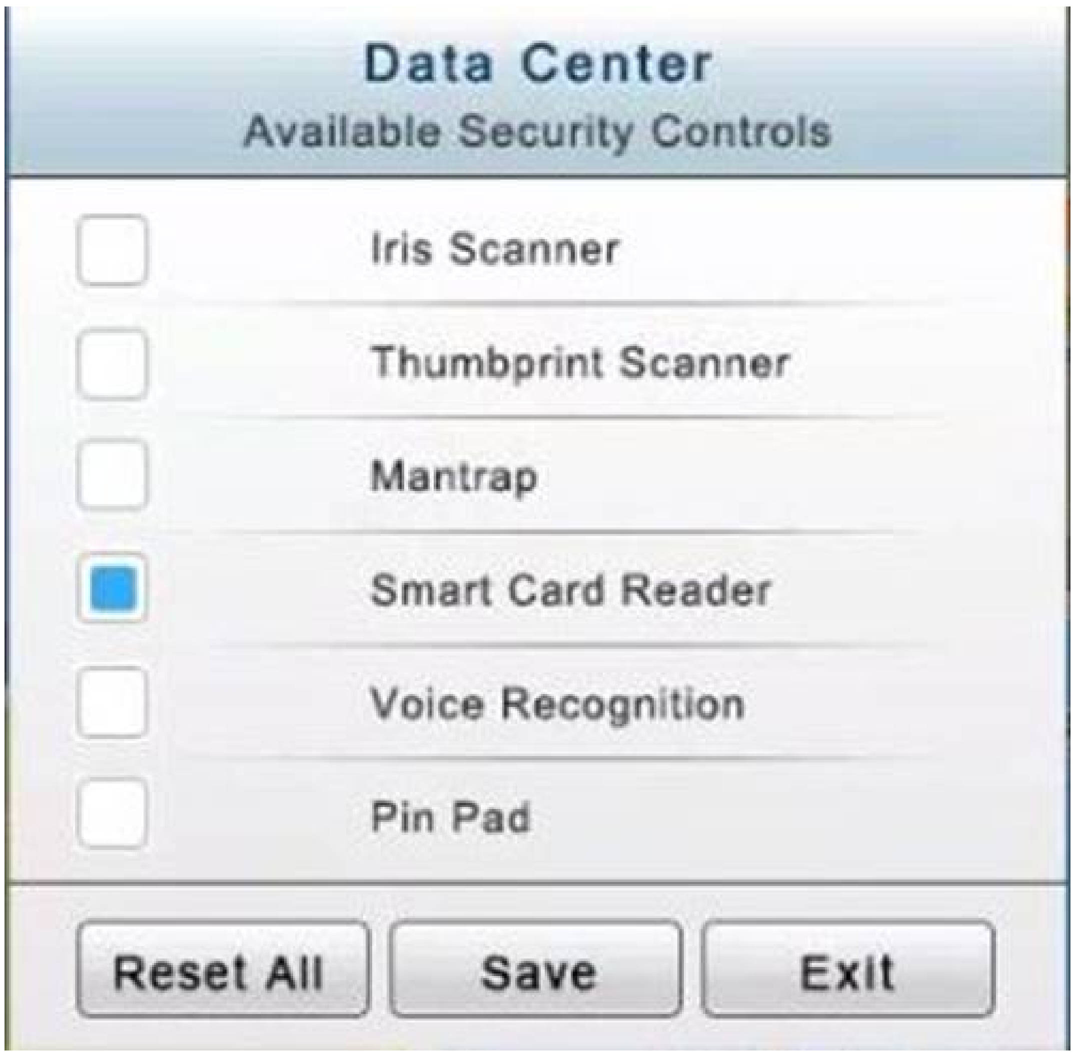
Public Cafe
Available Security Controls

- ☑ 128-bit key
- ☑ 64-bit key
- ☑ Pre-share Key
- ☑ PKI certificate
- ☑ SSH Key
- ☑ Pin Pad



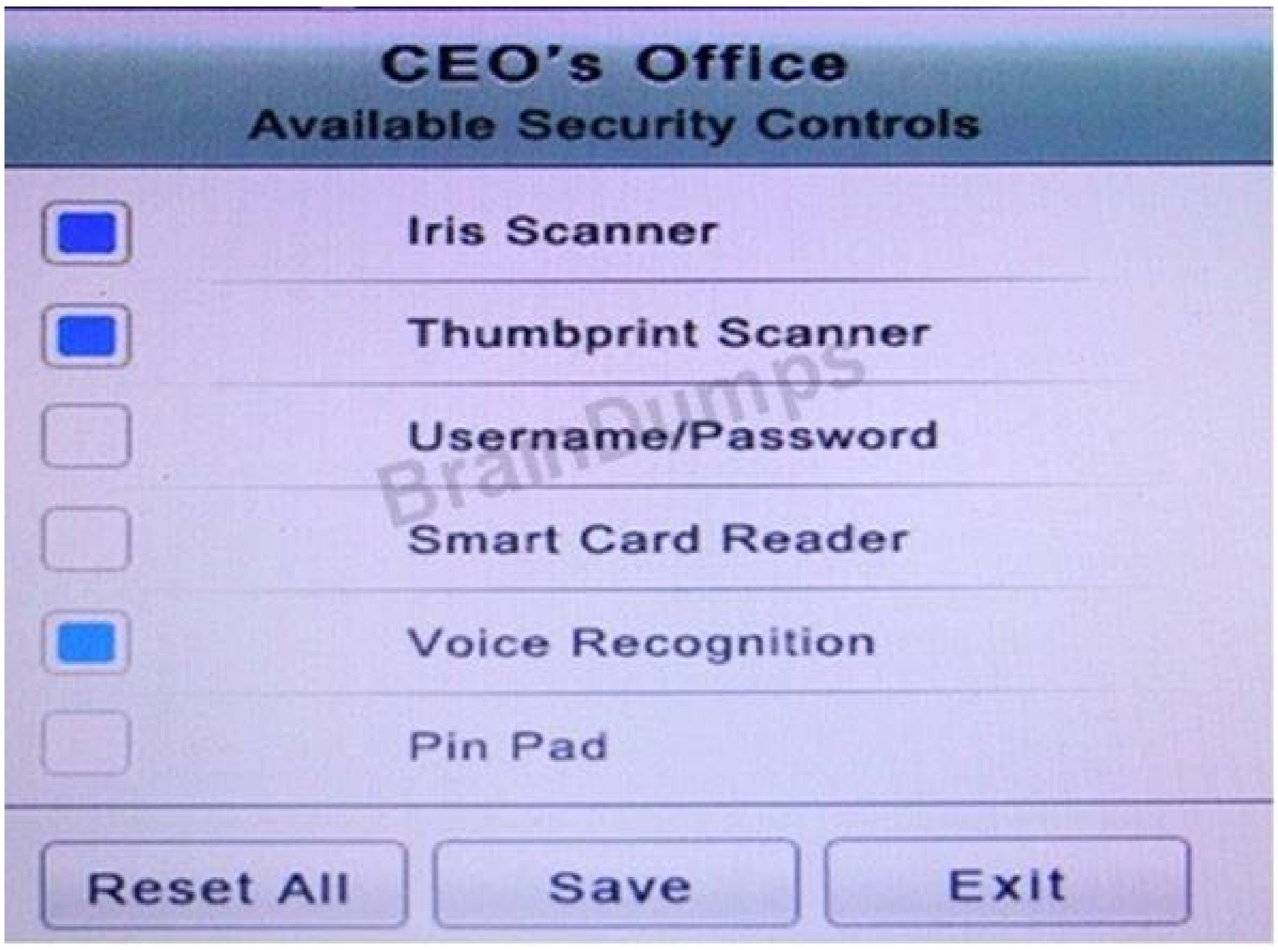
Help Desk
Available Security Controls

- ☐ Iris Scanner
- ☐ Thumbprint Scanner
- ☐ Password
- ☑ Proximity Badge
- ☐ Voice Recognition
- ☐ Pin Pad



Data Center
Available Security Controls

- ☐ Iris Scanner
- ☐ Thumbprint Scanner
- ☐ Mantrap
- ☑ Smart Card Reader
- ☐ Voice Recognition
- ☐ Pin Pad

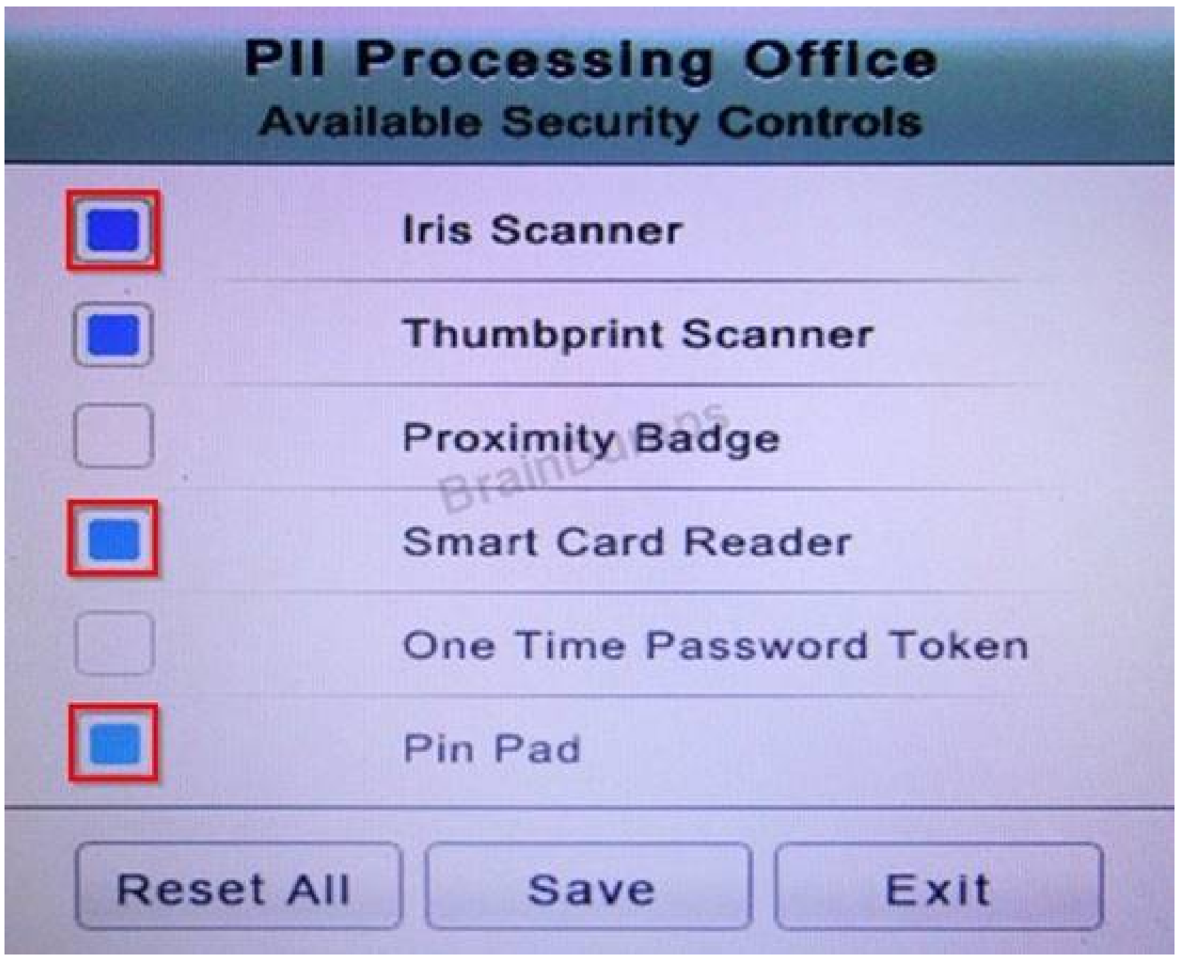


CEO's Office
Available Security Controls

☑ Iris Scanner
☑ Thumbprint Scanner
□ Username/Password
□ Smart Card Reader
☑ Voice Recognition
□ Pin Pad

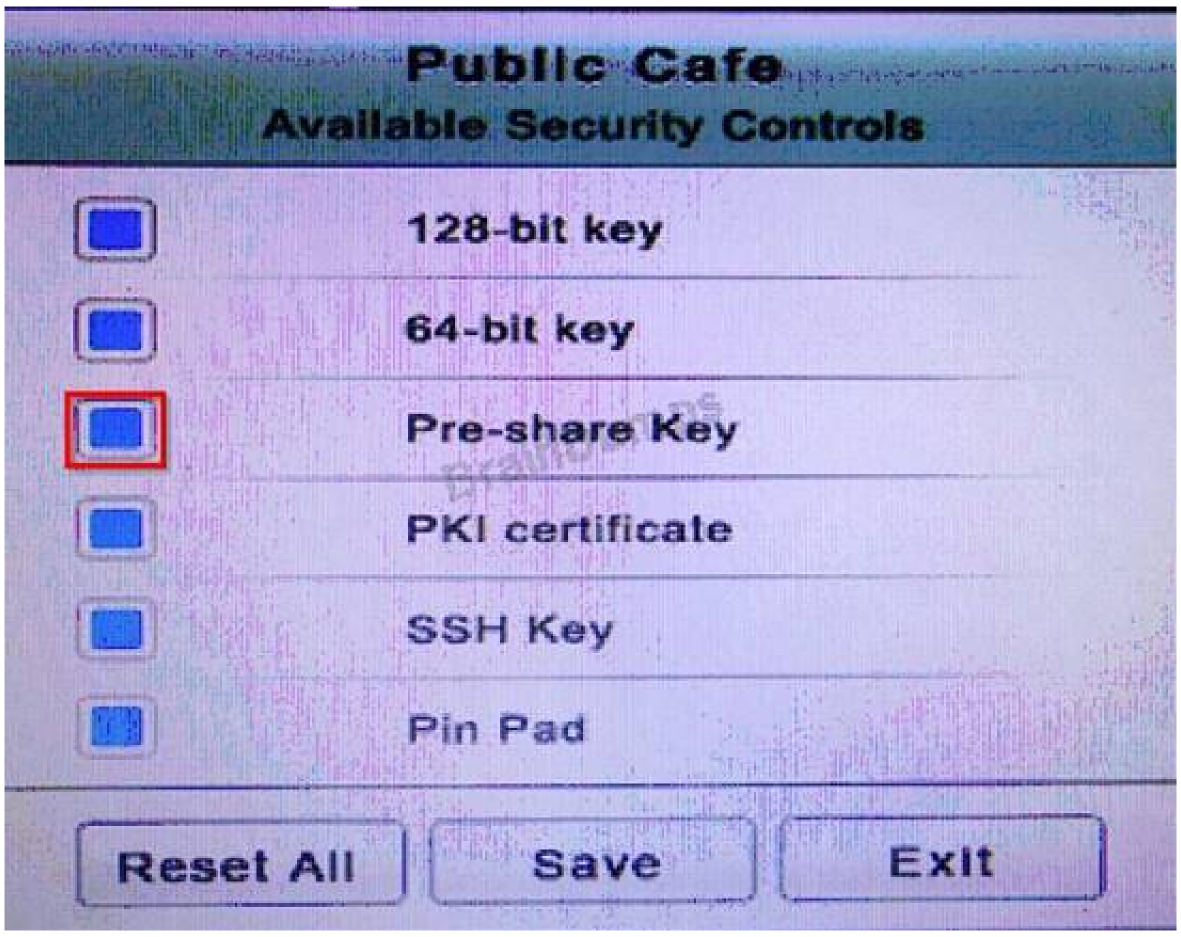
Answer:

Explanation:
Solution as



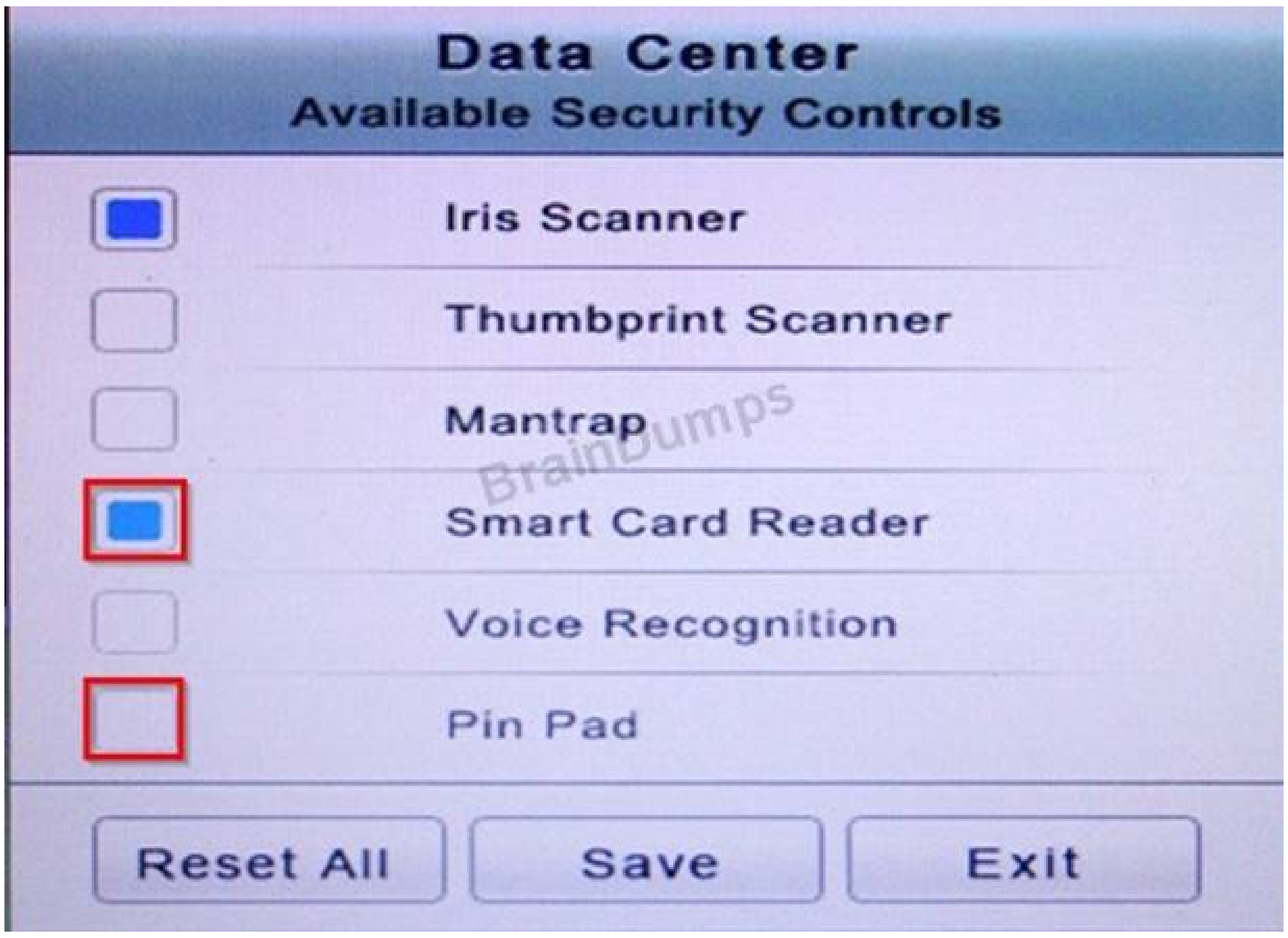
PII Processing Office
Available Security Controls

☑ Iris Scanner
☑ Thumbprint Scanner
□ Proximity Badge
☑ Smart Card Reader
□ One Time Password Token
☑ Pin Pad



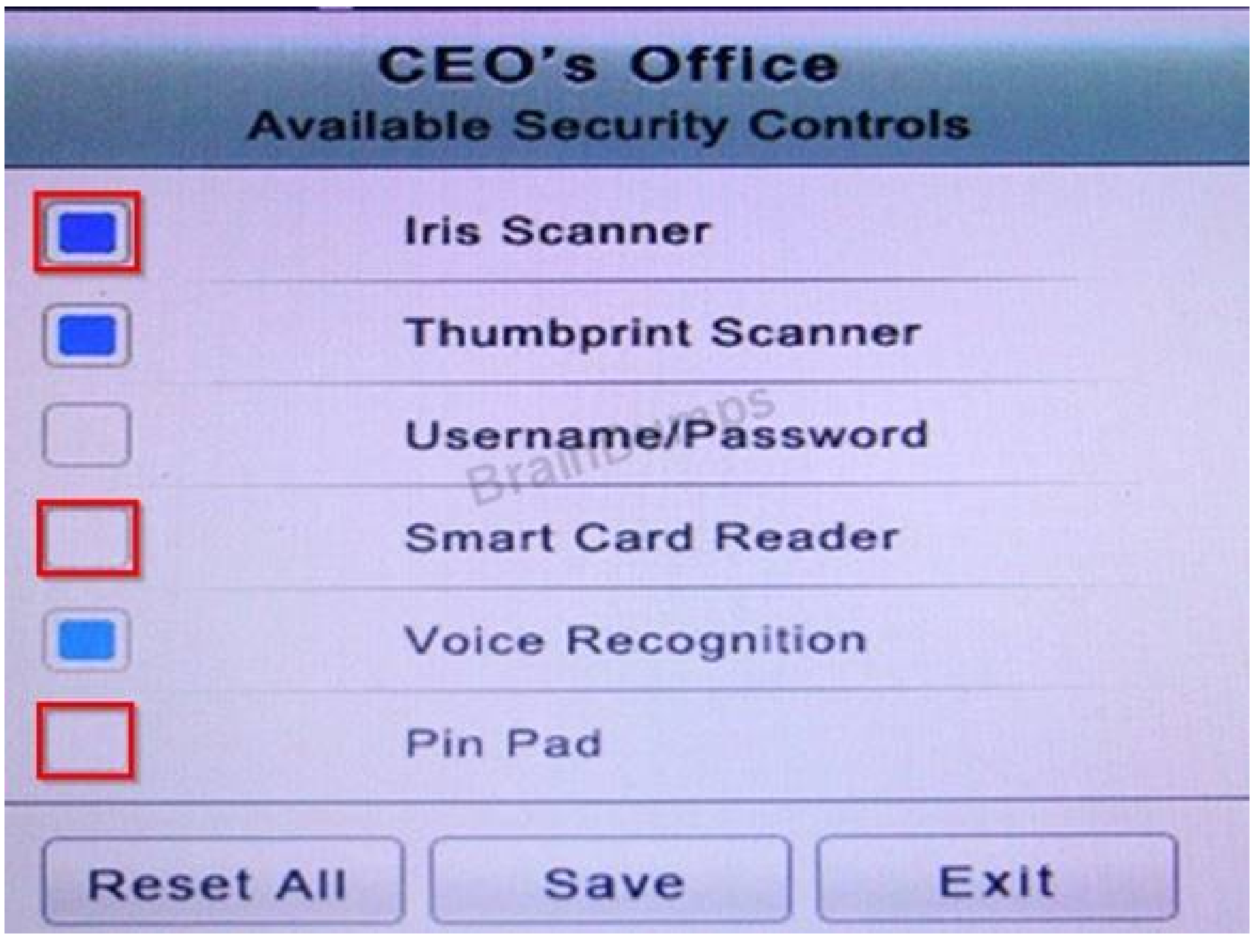
Public Cafe
Available Security Controls

☑ 128-bit key
☑ 64-bit key
☑ Pre-share Key
☑ PKI certificate
☑ SSH Key
☑ Pin Pad



Data Center
Available Security Controls

☑ Iris Scanner
□ Thumbprint Scanner
□ Mantrap
☑ Smart Card Reader
□ Voice Recognition
□ Pin Pad



CEO's Office
Available Security Controls

☑ Iris Scanner
☑ Thumbprint Scanner
□ Username/Password
□ Smart Card Reader
☑ Voice Recognition
□ Pin Pad

NEW QUESTION 466
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

NEW QUESTION 471
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

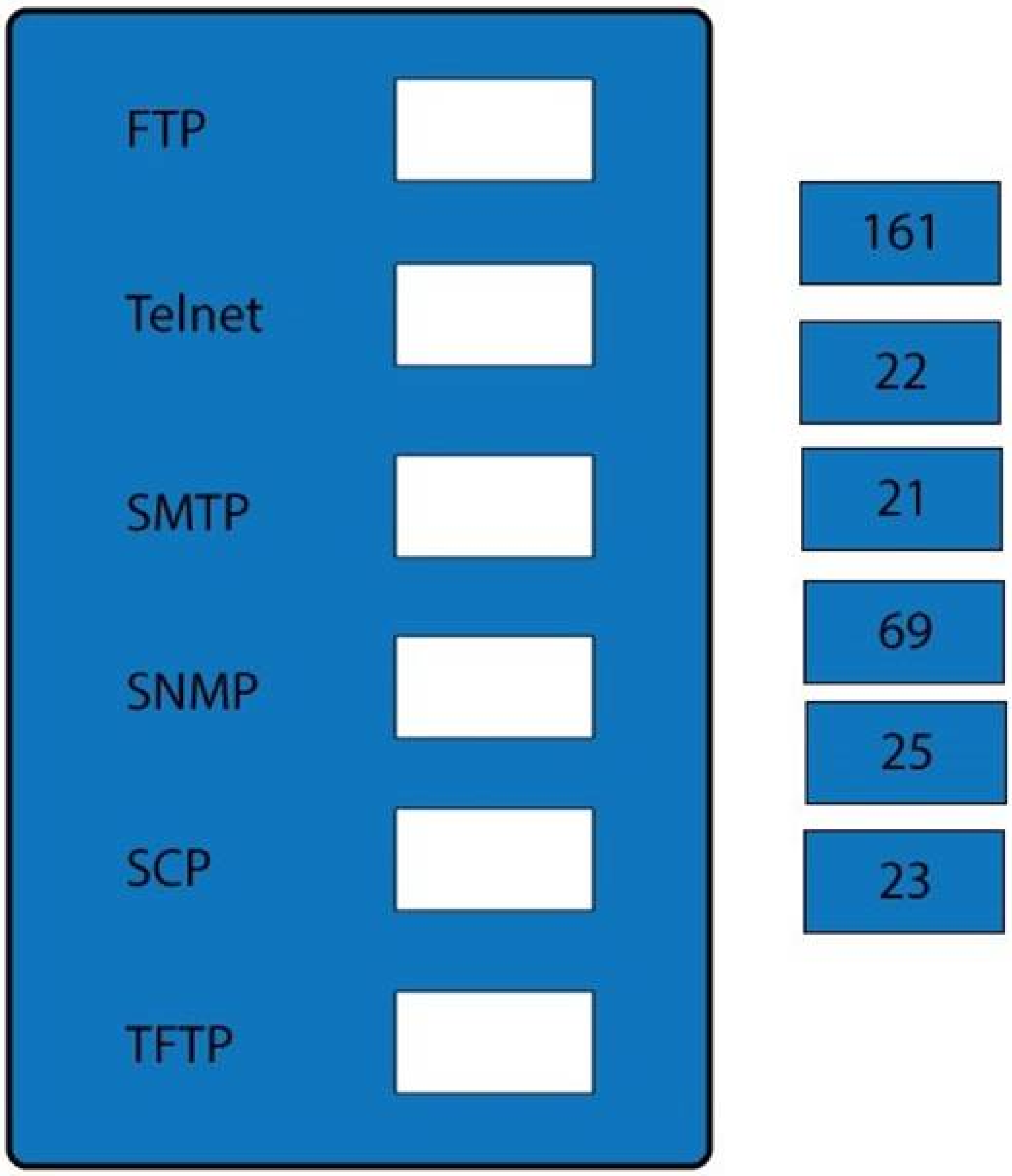
Answer: B

NEW QUESTION 475
AChief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net). Which of the following rules is preventing the CSO from accessing the site?
Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

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

Answer: C

NEW QUESTION 478
Drag and drop the correct protocol to its default port.



Answer:

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

NEW QUESTION 480
After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

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

Answer: D

NEW QUESTION 485
Which of the following are MOST susceptible to birthday attacks?

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

Answer: A

NEW QUESTION 487
Having adequate lighting on the outside of a building is an example of which of the following security controls?

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

Answer: A

NEW QUESTION 492
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: 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.

NEW QUESTION 493
A datacenter manager has been asked to prioritize critical system recovery priorities. Which of the following is the MOST critical for immediate recovery?

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

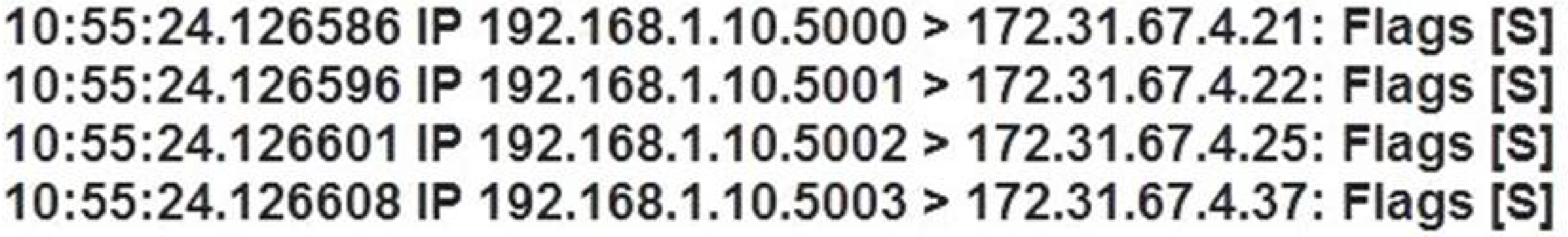
Answer: B

NEW QUESTION 495
While performing a penetration test, the technicians want their efforts to go unnoticed for as long as possible while they gather useful data about the network they are assessing. Which of the following would be the BEST choice for the technicians?

A. Vulnerability scanner
B. Offline password cracker
C. Packet sniffer
D. Banner grabbing

Answer: C

NEW QUESTION 497
A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:



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

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

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

Answer: D

NEW QUESTION 501
To determine the ALE of a particular risk, which of the following must be calculated? (Select two.)

A. ARO
B. ROI
C. RPO
D. SLE
E. RTO

Answer: AD

NEW QUESTION 505
A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

A. Non-intrusive
B. Authenticated
C. Credentialed
D. Active

Answer: C

NEW QUESTION 507
Which of the following are used to increase the computing time it takes to brute force a password using an offline attack? (Select TWO)

A. XOR
B. PBKDF2
C. bcrypt
D. HMAC
E. RIPEMD

Answer: BC

NEW QUESTION 512
Due to regulatory requirements, a security analyst must implement full drive encryption on a Windows file server. Which of the following should the analyst implement on the system to BEST meet this requirement? (Choose two.)

A. Enable and configure EFS on the file system.
B. Ensure the hardware supports TPM, and enable it in the BIOS.
C. Ensure the hardware supports VT-X, and enable it in the BIOS.
D. Enable and configure BitLocker on the drives.
E. Enable and configure DFS across the file system.

Answer: BD

NEW QUESTION 517
Ann, a security administrator, wants to ensure credentials are encrypted in transit when implementing a RADIUS server for SSO. Which of the following are needed given these requirements? (Select TWO)

A. Public key
B. Shared key
C. Elliptic curve
D. MD5
E. Private key
F. DES

Answer: AE

NEW QUESTION 521
Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.
Which of the following authentication methods should be deployed to achieve this goal?

A. PIN
B. Security QUESTION NO:
C. Smart card
D. Passphrase
E. CAPTCHA

Answer: C

NEW QUESTION 523
A datacenter recently experienced a breach. When access was gained, an RF device was used to access an air-gapped and locked server rack. Which of the following would BEST prevent this type of attack?

A. Faraday cage
B. Smart cards
C. Infrared detection
D. Alarms

Answer: A

NEW QUESTION 528
A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert. Which of the following methods has MOST likely been used?

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

Answer: E

NEW QUESTION 531
A global gaming console manufacturer is launching a new gaming platform to its customers. Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

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

Answer: AD

NEW QUESTION 535
A security analyst is working on a project that requires the implementation of a stream cipher. Which of the following should the analyst use?

A. Hash function
B. Elliptic curve
C. Symmetric algorithm
D. Public key cryptography

Answer: C

NEW QUESTION 540
The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems.
The help desk is receive reports that users are experiencing the following error when attempting to log in to their previous system:
Logon Failure: Access Denied
Which of the following can cause this issue?

A. Permission issues
B. Access violations
C. Certificate issues
D. Misconfigured devices

Answer: C

NEW QUESTION 542
A consultant has been tasked to assess a client's network. The client reports frequent network outages. Upon viewing the spanning tree configuration, the consultant notices that an old and law performing edge switch on the network has been elected to be the root bridge. Which of the following explains this scenario?

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

Answer: C

NEW QUESTION 547
A security auditor is putting together a report for the Chief Executive Officer (CEO) on personnel security and its impact on the security posture of the whole organization. Which of the following would be the MOST important factor to consider when it comes to personnel security?

A. Insider threats
B. Privilege escalation
C. Hacktivist
D. Phishing through social media
E. Corporate espionage

Answer: A

NEW QUESTION 551
A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL. Which of the following is the attacker most likely utilizing?

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

Answer: A

NEW QUESTION 556
Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select Two)

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

Answer: BC

NEW QUESTION 561
Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

A. Remote exploit
B. Amplification
C. Sniffing
D. Man-in-the-middle

Answer: A

NEW QUESTION 563
An organization recently moved its custom web applications to the cloud, and it is obtaining managed services of the back-end environment as part of its subscription. Which of the following types of services is this company now using?

A. SaaS
B. CASB
C. IaaS
D. PaaS

Answer: B

Explanation: Security Broker (CASB) gives you both visibility into your entire cloud stack and the security automation tool your IT team needs.

NEW QUESTION 568
Many employees are receiving email messages similar to the one shown below:
From IT department To employee Subject email quota exceeded Pease click on the following link http:www.website.info/email.php?quota=1Gb and provide your username and password to increase your email quotA. Upon reviewing other similar emails, the security administrator realized that all the phishing URLs have the following common elements; they all use HTTP, they all come from .info domains, and they all contain the same URI. Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?

A. BLOCKhttp://www.*.info/ "
B. DROPhttp:// "website.info/email.php?*
C. Redirecthttp://www,*.Info/email.php?quota=*TOhttp://company.com/corporate_polict.html
D. DENYhttp://*.info/email.php?quota=1Gb

Answer:

D

NEW QUESTION 572
Which of the following allows an auditor to test proprietary-software compiled code for security flaws?

A. Fuzzing
B. Static review
C. Code signing
D. Regression testing

Answer: A

NEW QUESTION 576
An audit has revealed that database administrators are also responsible for auditing database changes and backup logs. Which of the following access control methodologies would BEST mitigate this concern?

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

Answer: D

NEW QUESTION 580
While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack. Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Select two)

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

Answer: AD

NEW QUESTION 582
After a security incident, management is meeting with involved employees to document the incident and its aftermath. Which of the following BEST describes this phase of the incident response process?

A. Lessons learned
B. Recovery
C. Identification
D. Preparation

Answer: A

NEW QUESTION 587
The security administrator has noticed cars parking just outside of the building fence line. Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Select TWO)

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

Answer: DE

NEW QUESTION 589
An organization wants to utilize a common, Internet-based third-party provider for authorization and authentication. The provider uses a technology based on OAuth 2.0 to provide required services. To which of the following technologies is the provider referring?

A. Open ID Connect
B. SAML
C. XACML
D. LDAP

Answer: A

NEW QUESTION 594
A security administrator receives an alert from a third-party vendor that indicates a certificate that was installed in the browser has been hijacked at the root of a small public CA. The security administrator knows there are at least four different browsers in use on more than a thousand computers in the domain worldwide. Which of the following solutions would be BEST for the security administrator to implement to most efficiently assist with this issue?

A. SSL
B. CRL
C. PKI
D. ACL

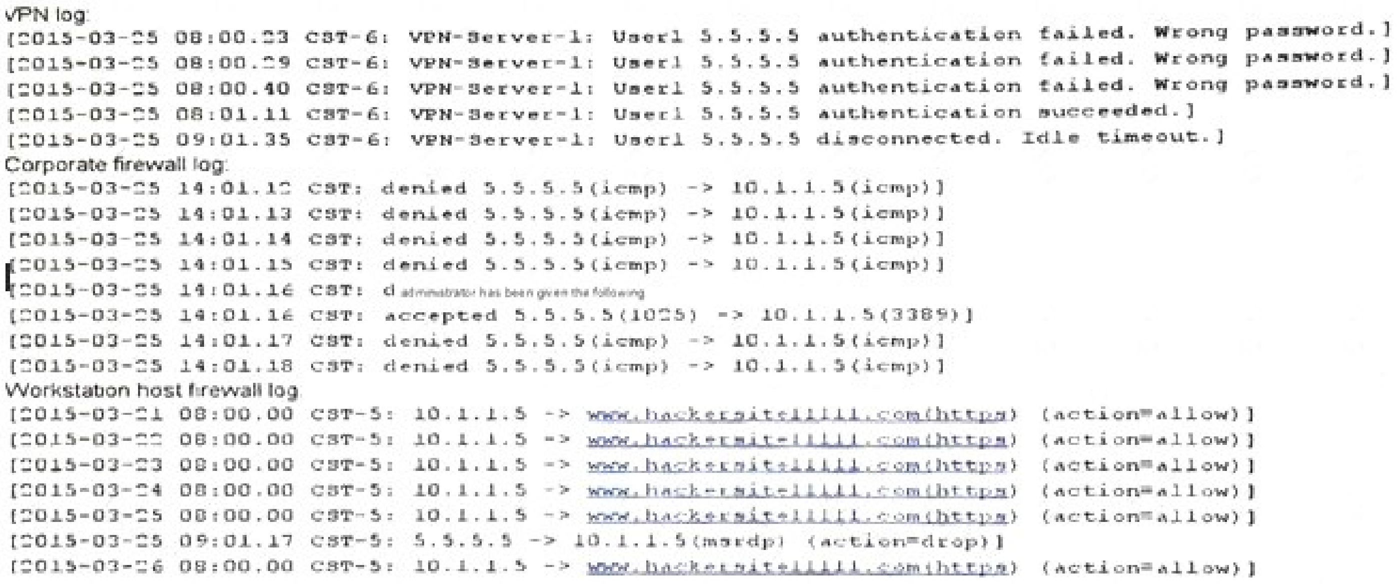
Answer: B

NEW QUESTION 599
A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility. Which of the following configuration commands should be implemented to enforce this requirement?

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

Answer: B

NEW QUESTION 600
A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.



```
VPN log:
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
Corporate firewall log:
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: d administrator has been given the following
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
Workstation host firewall log
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-23 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp) (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
```

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

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

Answer: B

NEW QUESTION 605
Ann, a user, states that her machine has been behaving erratically over the past week. She has experienced slowness and input lag and found text files that appear to contain pieces of her emails or online conversations with coworkers. The technician runs a standard virus scan but detects nothing. Which of the following types of malware has infected the machine?

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

Answer: D

NEW QUESTION 610
A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system.
Which of the following methods should the security administrator select the best balances security and efficiency?

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

Answer: C

NEW QUESTION 612
An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity. Which of the following actions will help detect attacker attempts to further alter log files?

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

Answer: C

NEW QUESTION 615
Which of the following could occur when both strong and weak ciphers are configured on a VPN concentrator? (Select TWO)

A. An attacker could potentially perform a downgrade attack.
B. The connection is vulnerable to resource exhaustion.
C. The integrity of the data could be at risk.
D. The VPN concentrator could revert to L2TP.
E. The IPSec payload reverted to 16-bit sequence numbers.

Answer: AE

NEW QUESTION 619
An actor downloads and runs a program against a corporate login page. The program imports a list of usernames and passwords, looking for a successful attempt. Which of the following terms BEST describes the actor in this situation?

A. Script kiddie
B. Hacktivist
C. Cryptologist
D. Security auditor

Answer: A

NEW QUESTION 620
The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts. Which of the following controls should be implemented to curtail this activity?

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

Answer: D

NEW QUESTION 621
A web server, which is configured to use TLS with AES-GCM-256, SHA-384, and ECDSA, recently suffered an information loss breach. Which of the following is MOST likely the cause?

A. Insufficient key bit length
B. Weak cipher suite
C. Unauthenticated encryption method
D. Poor implementation

Answer: D

NEW QUESTION 622
Which of the following is the BEST reason for salting a password hash before it is stored in a database?

A. To prevent duplicate values from being stored
B. To make the password retrieval process very slow
C. To protect passwords from being saved in readable format
D. To prevent users from using simple passwords for their access credentials

Answer: A

NEW QUESTION 627
A security analyst is investigating a security breach. Upon inspection of the audit an access logs, the analyst notices the host was accessed and the /etc/passwd file was modified with a new entry for username “gotcha” and user ID of 0. Which of the following are the MOST likely attack vector and tool the analyst should use to determine if the attack is still ongoing? (Select TWO)

A. Logic bomb
B. Backdoor
C. Keylogger
D. Netstat
E. Tracert
F. Ping

Answer: BD

NEW QUESTION 629

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

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

Answer: D

NEW QUESTION 631
A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company. Which of the following portions of the company's mobile device management configuration would allow the company data to be removed from the device without touching the new hire's data?

A. Asset control
B. Device access control
C. Storage lock out
D. Storage segmentation

Answer: B

NEW QUESTION 633
......