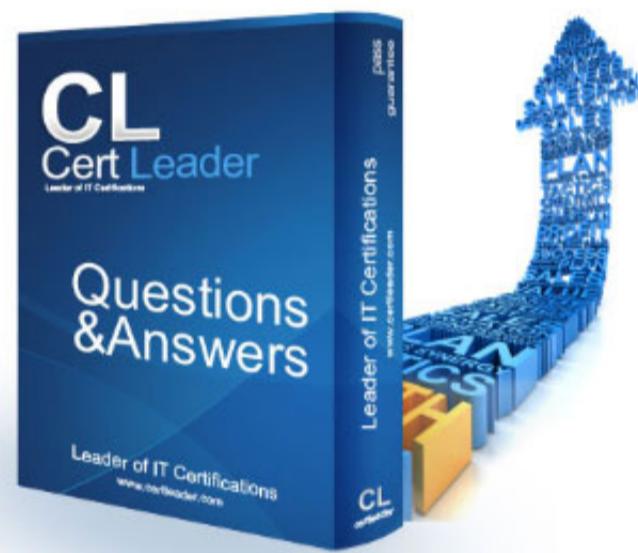


SY0-501 Dumps

CompTIA Security+ Certification Exam

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



NEW QUESTION 1

- (Exam Topic 1)

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 2**

- (Exam Topic 1)

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

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

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

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

Answer: C**NEW QUESTION 3**

- (Exam Topic 1)

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

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

Answer: A**NEW QUESTION 4**

- (Exam Topic 1)

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

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

Answer: A**NEW QUESTION 5**

- (Exam Topic 1)

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

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

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

- A. Eliminate shared accounts.
- B. Create a standard naming convention for accounts.
- C. Implement usage auditing and review.

- D. Enable account lockout thresholds.
- E. Copy logs in real time to a secured WORM drive.
- F. Implement time-of-day restrictions.
- G. Perform regular permission audits and reviews.

Answer: ACG

NEW QUESTION 6

- (Exam Topic 1)

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 7

- (Exam Topic 1)

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.htm 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.htm
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 8

- (Exam Topic 1)

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

- A. Capture and document necessary information to assist in the response.
- B. Request the user capture and provide a screenshot or recording of the symptoms.
- C. Use a remote desktop client to collect and analyze the malware in real time.
- D. Ask the user to back up files for later recovery.

Answer: A

NEW QUESTION 9

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

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 10

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 11

- (Exam Topic 1)

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 12

- (Exam Topic 1)

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

The IT security department finds the following security configuration for the accounts payable module:

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

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

- A. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager
- B. New Vendor Entry - Required Role: Accounts Payable Manager
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager
- C. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager
- D. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager

- A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 17

- (Exam Topic 1)

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 19

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 23

- (Exam Topic 1)

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 28

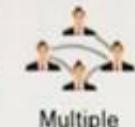
- (Exam Topic 1)

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	<input type="checkbox"/> SPIM <input type="checkbox"/> VISHING <input type="checkbox"/> PHISHING <input type="checkbox"/> WHALING <input type="checkbox"/> HOAX <input type="checkbox"/> PHARMING <input type="checkbox"/> SPEAR PHISHING <input type="checkbox"/> SPOOFING <input type="checkbox"/> SPAM <input type="checkbox"/> XMAS ATTACK	
 Attacker posts link to fake AV software	 Multiple social networks	 Broad set of victims	<input type="checkbox"/> SPIM <input type="checkbox"/> VISHING <input type="checkbox"/> PHISHING <input type="checkbox"/> WHALING <input type="checkbox"/> HOAX <input type="checkbox"/> PHARMING <input type="checkbox"/> SPEAR PHISHING <input type="checkbox"/> SPOOFING <input type="checkbox"/> SPAM <input type="checkbox"/> XMAS ATTACK
 Attacker collecting credit card details	 Phone-based victim	<input type="checkbox"/> SPIM <input type="checkbox"/> VISHING <input type="checkbox"/> PHISHING <input type="checkbox"/> WHALING <input type="checkbox"/> HOAX <input type="checkbox"/> PHARMING <input type="checkbox"/> SPEAR PHISHING <input type="checkbox"/> SPOOFING <input type="checkbox"/> SPAM <input type="checkbox"/> XMAS ATTACK	
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broad set of recipients	<input type="checkbox"/> SPIM <input type="checkbox"/> VISHING <input type="checkbox"/> PHISHING <input type="checkbox"/> WHALING <input type="checkbox"/> HOAX <input type="checkbox"/> PHARMING <input type="checkbox"/> SPEAR PHISHING <input type="checkbox"/> SPOOFING <input type="checkbox"/> SPAM <input type="checkbox"/> XMAS ATTACK	
 Attacker redirects name resolution entries from legitimate site to fraudulent site	 Victims	<input type="checkbox"/> WHALING <input type="checkbox"/> SPIM <input type="checkbox"/> VISHING <input type="checkbox"/> PHISHING <input type="checkbox"/> WHALING <input type="checkbox"/> HOAX <input type="checkbox"/> PHARMING <input type="checkbox"/> SPEAR PHISHING <input type="checkbox"/> SPOOFING <input type="checkbox"/> SPAM <input type="checkbox"/> XMAS ATTACK	

- A. Mastered
 B. Not Mastered

Answer: A

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 30

- (Exam Topic 1)

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

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

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

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

Answer: BC

NEW QUESTION 33

- (Exam Topic 1)

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 35

- (Exam Topic 1)

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

- A. Owner
- B. System
- C. Administrator
- D. User

Answer: C

NEW QUESTION 37

- (Exam Topic 2)

A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls.

Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

- A. Password complexity policies
- B. Hardware tokens

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

Answer: DFI

NEW QUESTION 40

- (Exam Topic 2)

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 41

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 43

- (Exam Topic 2)

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 PBX. 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 45

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 49

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 50

- (Exam Topic 2)

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 55

- (Exam Topic 2)

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 57

- (Exam Topic 2)

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 from 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 60

- (Exam Topic 2)

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

- A. RADIUS
- B. TACACS+
- C. Diameter
- D. Kerberos

Answer: B

NEW QUESTION 63

- (Exam Topic 2)

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

- A. To prevent server availability issues
- B. To verify the appropriate patch is being installed
- C. To generate a new baseline hash after patching
- D. To allow users to test functionality
- E. To ensure users are trained on new functionality

Answer: AD

NEW QUESTION 67

- (Exam Topic 2)

Audit logs from a small company's vulnerability scanning software show the following findings: Destinations scanned:

- Server001- Internal human resources payroll server
- Server101-Internet-facing web server

- Server201- SQL server for Server101
 - Server301-Jumpbox used by systems administrators accessible from the internal network Validated vulnerabilities found:
 - Server001- Vulnerable to buffer overflow exploit that may allow attackers to install software
 - Server101- Vulnerable to buffer overflow exploit that may allow attackers to install software
 - Server201-OS updates not fully current
 - Server301- Accessible from internal network without the use of jumpbox
 - Server301-Vulnerable to highly publicized exploit that can elevate user privileges
- Assuming external attackers who are gaining unauthorized information are of the highest concern, which of the following servers should be addressed FIRST?

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

Answer: B

NEW QUESTION 71

- (Exam Topic 2)

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 76

- (Exam Topic 2)

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 81

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 83

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 86

- (Exam Topic 2)

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 89**

- (Exam Topic 2)

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 91**

- (Exam Topic 2)

During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users.

Which of the following could best prevent this from occurring again?

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

Answer: B**NEW QUESTION 95**

- (Exam Topic 2)

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

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

Answer: B**NEW QUESTION 100**

- (Exam Topic 2)

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 105**

- (Exam Topic 2)

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

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

Answer: C**NEW QUESTION 110**

- (Exam Topic 2)

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 111

- (Exam Topic 2)

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

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

Answer: BC**NEW QUESTION 112**

- (Exam Topic 2)

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 114**

- (Exam Topic 2)

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 118**

- (Exam Topic 3)

Phishing emails frequently take advantage of high-profile catastrophes reported in the news. Which of the following principles BEST describes the weakness being exploited?

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

Answer: D**NEW QUESTION 122**

- (Exam Topic 3)

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

Authentication Category

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

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<input type="checkbox"/> Something you have <input type="checkbox"/> Something you know <input type="checkbox"/> Something you are <input type="checkbox"/> All given authentication categories
Smart card	<input type="checkbox"/> Something you have <input type="checkbox"/> Something you know <input type="checkbox"/> Something you are <input type="checkbox"/> All given authentication categories
Hardware Token	<input type="checkbox"/> Something you have <input type="checkbox"/> Something you know <input type="checkbox"/> Something you are <input type="checkbox"/> All given authentication categories
Password	<input type="checkbox"/> Something you have <input type="checkbox"/> Something you know <input type="checkbox"/> Something you are <input type="checkbox"/> All given authentication categories
PIN number	<input type="checkbox"/> Something you have <input type="checkbox"/> Something you know <input type="checkbox"/> Something you are <input type="checkbox"/> All given authentication categories
Fingerprint scan	<input type="checkbox"/> Something you have <input type="checkbox"/> Something you know <input type="checkbox"/> Something you are

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Something you are includes fingerprints, retina scans, or voice recognition. Something you have includes smart cards, token devices, or keys. Something you know includes a password, codes, PINs, combinations, or secret phrases. Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.

Something you do includes your typing rhythm, a secret handshake, or a private knock

http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle http://en.wikipedia.org/wiki/Smart_card#Security

NEW QUESTION 125

- (Exam Topic 3)

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 129

- (Exam Topic 3)

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

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

Answer: C**NEW QUESTION 133**

- (Exam Topic 3)

An employee uses RDP to connect back to the office network. If RDP is misconfigured, which of the following security exposures would this lead to?

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

Answer: D**NEW QUESTION 136**

- (Exam Topic 3)

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 137**

- (Exam Topic 3)

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

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

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

Answer: D**NEW QUESTION 141**

- (Exam Topic 3)

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 142**

- (Exam Topic 3)

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 144**

- (Exam Topic 3)

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

- A. War chalking
- B. Bluejacking
- C. Bluesnarfing

D. Rogue tethering

Answer: B

Explanation:

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

NEW QUESTION 149

- (Exam Topic 3)

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 152

- (Exam Topic 3)

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 154

- (Exam Topic 3)

Which of the following use the SSH protocol?

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

Answer: BF

NEW QUESTION 156

- (Exam Topic 3)

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 159

- (Exam Topic 3)

During an application design, the development team specifies 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 163

- (Exam Topic 3)

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

systems has the auditor reviewed?

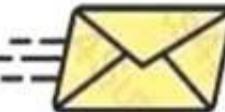
- A. Password-based
- B. Biometric-based
- C. Location-based
- D. Certificate-based

Answer: B

NEW QUESTION 166

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

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

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

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

E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal

information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.
<http://www.webopedia.com/TERM/P/phishing.html> <http://www.techopedia.com/definition/28643/whaling> <http://www.webopedia.com/TERM/V/vishing.html>
<http://searchsecurity.techtarget.com/definition/social-engineering>

NEW QUESTION 167

- (Exam Topic 3)

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 169

- (Exam Topic 3)

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

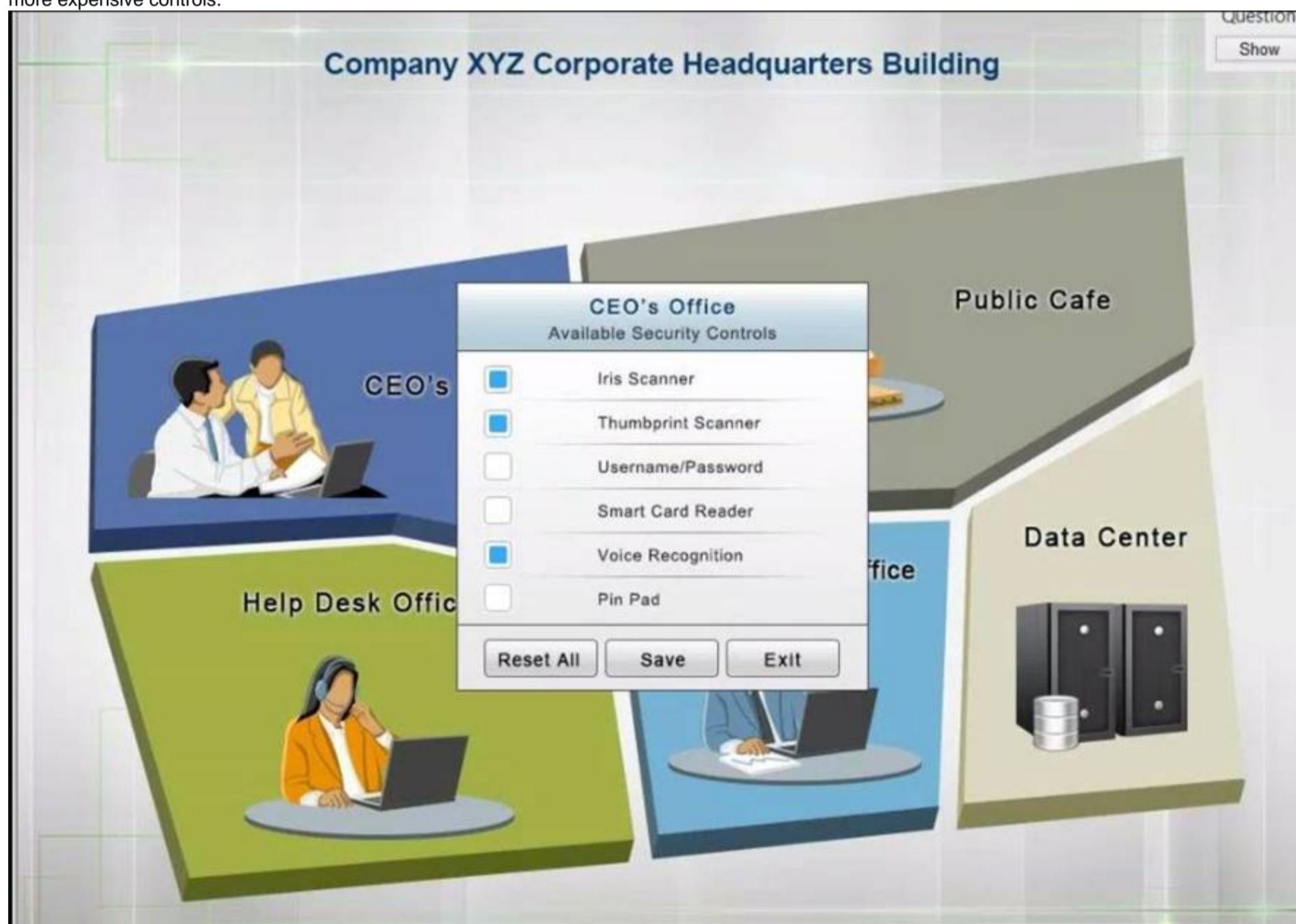
The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.

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

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

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

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



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

PII Processing Office**Available Security Controls**

Iris Scanner



Thumbprint Scanner



Proximity Badge



Smart Card Reader



One Time Password Token



Pin Pad

Reset All**Save****Exit****Public Cafe****Available Security Controls**

128-bit key



64-bit key



Pre-share Key



PKI certificate



SSH Key



Pin Pad

Reset All**Save****Exit****Help Desk****Available Security Controls**

Iris Scanner



Thumbprint Scanner



Password



Proximity Badge



Voice Recognition



Pin Pad

Reset All**Save****Exit**

Data Center

Available Security Controls

<input type="checkbox"/>	Iris Scanner
<input type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Mantrap
<input checked="" type="checkbox"/>	Smart Card Reader
<input type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

Reset All Save Exit

CEO's Office

Available Security Controls

<input checked="" type="checkbox"/>	Iris Scanner
<input checked="" type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Username/Password
<input type="checkbox"/>	Smart Card Reader
<input checked="" type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

Reset All Save Exit

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Solution as

PII Processing Office

Available Security Controls

<input checked="" type="checkbox"/>	Iris Scanner
<input type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Proximity Badge
<input checked="" type="checkbox"/>	Smart Card Reader
<input type="checkbox"/>	One Time Password Token
<input checked="" type="checkbox"/>	Pin Pad

Reset All Save Exit

Public Cafe

Available Security Controls

<input type="checkbox"/>	128-bit key
<input type="checkbox"/>	64-bit key
<input checked="" type="checkbox"/>	Pre-share Key
<input type="checkbox"/>	PKI certificate
<input type="checkbox"/>	SSH Key
<input type="checkbox"/>	Pin Pad

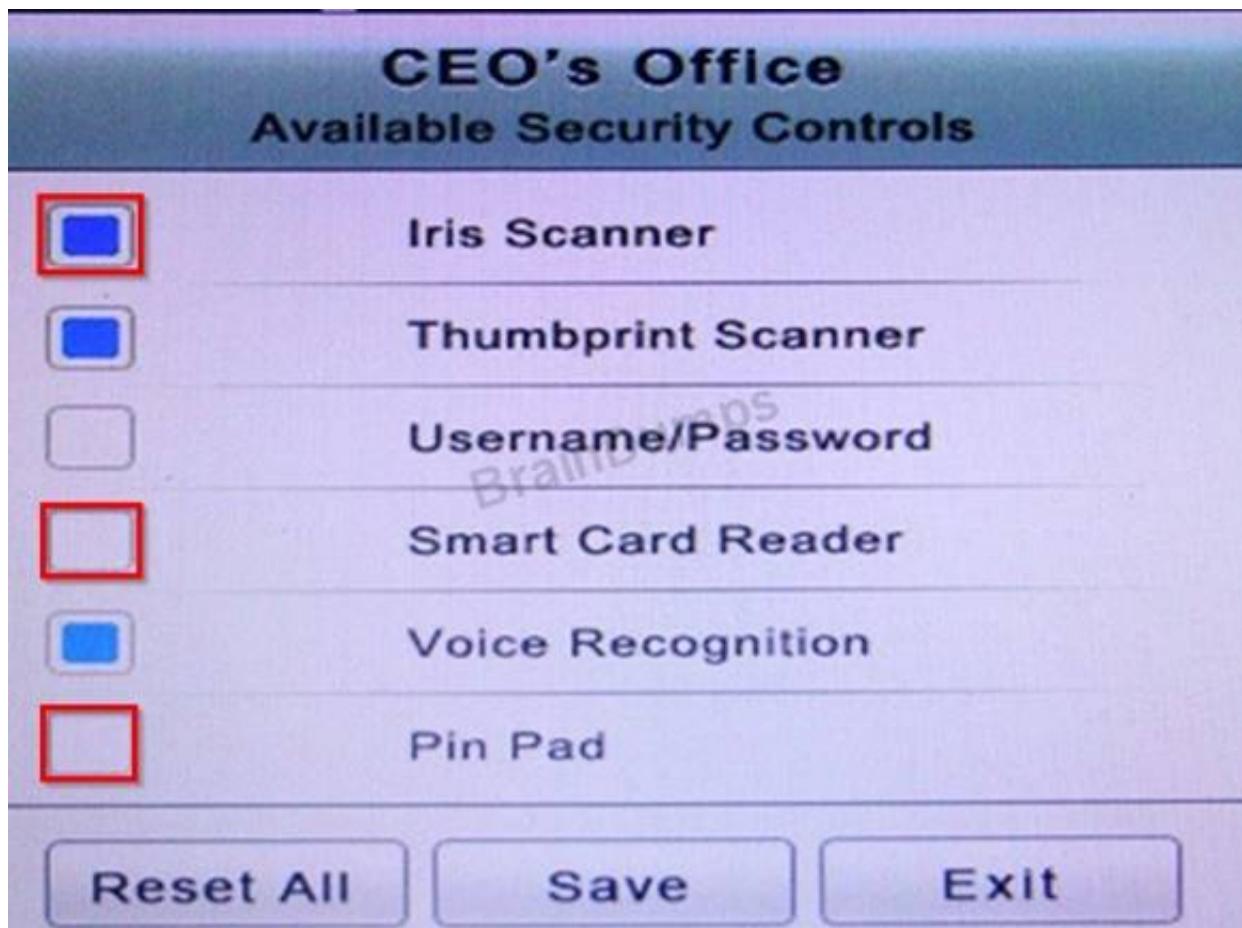
Reset All Save Exit

Data Center

Available Security Controls

<input type="checkbox"/>	Iris Scanner
<input type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Mantrap
<input checked="" type="checkbox"/>	Smart Card Reader
<input type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

Reset All Save Exit

**NEW QUESTION 171**

- (Exam Topic 3)

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 176**

- (Exam Topic 3)

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

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

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

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

Answer: D**NEW QUESTION 178**

- (Exam Topic 3)

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 180**

- (Exam Topic 4)

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 184

- (Exam Topic 4)

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. Credentialated
- D. Active

Answer: C

NEW QUESTION 185

- (Exam Topic 4)

A user needs to send sensitive information to a colleague using PKI. Which of the following concepts apply when a sender encrypts the message hash with the sender's private key? (Select TWO)

- A. Non-repudiation
- B. Email content encryption
- C. Steganography
- D. Transport security
- E. Message integrity

Answer: AE

NEW QUESTION 189

- (Exam Topic 4)

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 191

- (Exam Topic 4)

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 195

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 197

- (Exam Topic 4)

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 198

- (Exam Topic 4)

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 203

- (Exam Topic 4)

After surfing the Internet, Joe, a user, woke up to find all his files were corrupted. His wallpaper was replaced by a message stating the files were encrypted and he needed to transfer money to a foreign country to recover them. Joe is a victim of:

- A. a keylogger
- B. spyware
- C. ransomware
- D. a logic bomb

Answer: C

NEW QUESTION 205

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 206

- (Exam Topic 4)

A wireless network has the following design requirements:

- ▶ Authentication must not be dependent on enterprise directory service
- ▶ It must allow background reconnection for mobile users
- ▶ It must not depend on user certificates

Which of the following should be used in the design to meet the requirements? (Choose two.)

- A. PEAP
- B. PSK
- C. Open systems authentication
- D. EAP-TLS
- E. Captive portals

Answer: BE

NEW QUESTION 209

- (Exam Topic 4)

Security administrators attempted corrective action after a phishing attack. Users are still experiencing trouble logging in, as well as an increase in account lockouts. Users' email contacts are complaining of an increase in spam and social networking requests. Due to the large number of affected accounts, remediation must be accomplished quickly. Which of the following actions should be taken FIRST? (Select TWO)

- A. Disable the compromised accounts
- B. Update WAF rules to block social networks
- C. Remove the compromised accounts with all AD groups
- D. Change the compromised accounts' passwords
- E. Disable the open relay on the email server
- F. Enable sender policy framework

Answer: EF

Explanation:

Sender Policy Framework (SPF) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators. In a Small Business Server environment, you may have to prevent your Microsoft Exchange Server-based server from being used as an open relay SMTP server for unsolicited commercial e-mail messages, or spam.

You may also have to clean up the Exchange server's SMTP queues to delete the unsolicited commercial email messages.

If your Exchange server is being used as an open SMTP relay, you may experience one or more of the following symptoms:

The Exchange server cannot deliver outbound SMTP mail to a growing list of e-mail domains. Internet browsing is slow from the server and from local area network (LAN) clients.

Free disk space on the Exchange server in the location of the Exchange information store databases or the Exchange information store transaction logs is reduced more rapidly than you expect.

The Microsoft Exchange information store databases spontaneously dismount. You may be able to manually mount the stores by using Exchange System Manager, but the stores may dismount on their own after they run for a short time. For more information, click the following article number to view the article in the Microsoft Knowledge Base.

NEW QUESTION 212

- (Exam Topic 4)

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

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

Answer: D**NEW QUESTION 215**

- (Exam Topic 4)

A network administrator adds an ACL to allow only HTTPS connections from host 192.168.2.3 to web server 192.168.5.2. After applying the rule, the host is unable to access the server. The network administrator runs the output and notices the configuration below:

```
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.3 eq 443 host 192.168.5.2
```

Which of the following rules would be BEST to resolve the issue?

A

```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
```

B

```
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
```

C

```
accesslist 102 permit tcp host 192.168.2.3 eq 443 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
```

D

```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A**NEW QUESTION 216**

- (Exam Topic 5)

Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect against the second attack?

- A. Key risk indicators
- B. Lessons learned
- C. Recovery point objectives
- D. Tabletop exercise

Answer: B**NEW QUESTION 218**

- (Exam Topic 5)

Every morning, a systems administrator monitors failed login attempts on the company's log management server. The administrator notices the DBAdmin account has five failed username and/or password alerts during a ten-minute window. The systems administrator determines the user account is a dummy account used to attract attackers. Which of the following techniques should the systems administrator implement?

- A. Role-based access control

- B. Honeypot
- C. Rule-based access control
- D. Password cracker

Answer: B

NEW QUESTION 220

- (Exam Topic 5)

The help desk received a call after hours from an employee who was attempting to log into the payroll server remotely. When the help desk returned the call the next morning, the employee was able to log into the server remotely without incident. However, the incident occurred again the next evening. Which of the following BEST describes the cause of the issue?

- A. The password expired on the account and needed to be reset
- B. The employee does not have the rights needed to access the database remotely
- C. Time-of-day restrictions prevented the account from logging in
- D. The employee's account was locked out and needed to be unlocked

Answer: C

NEW QUESTION 225

- (Exam Topic 5)

A security engineer is configuring a wireless network with EAP-TLS. Which of the following activities is a requirement for this configuration?

- A. Setting up a TACACS+ server
- B. Configuring federation between authentication servers
- C. Enabling TOTP
- D. Deploying certificates to endpoint devices

Answer: D

NEW QUESTION 229

- (Exam Topic 5)

A security administrator is diagnosing a server where the CPU utilization is at 100% for 24 hours. The main culprit of CPU utilization is the antivirus program. Which of the following issue could occur if left unresolved? (Select TWO)

- A. MITM attack
- B. DoS attack
- C. DLL injection
- D. Buffer overflow
- E. Resource exhaustion

Answer: BE

NEW QUESTION 234

- (Exam Topic 5)

A malicious system continuously sends an extremely large number of SYN packets to a server. Which of the following BEST describes the resulting effect?

- A. The server will be unable to serve clients due to lack of bandwidth
- B. The server's firewall will be unable to effectively filter traffic due to the amount of data transmitted
- C. The server will crash when trying to reassemble all the fragmented packets
- D. The server will exhaust its memory maintaining half-open connections

Answer: D

NEW QUESTION 239

- (Exam Topic 5)

A business sector is highly competitive, and safeguarding trade secrets and critical information is paramount. On a seasonal basis, an organization employs temporary hires and contractor personnel to accomplish its mission objectives. The temporary and contract personnel require access to network resources only when on the clock. Which of the following account management practices are the BEST ways to manage these accounts?

- A. Employ time-of-day restrictions.
- B. Employ password complexity.
- C. Employ a random key generator strategy.
- D. Employ an account expiration strategy.
- E. Employ a password lockout policy

Answer: D

NEW QUESTION 240

- (Exam Topic 5)

A hacker has a packet capture that contains:

...Joe.Smith.....E289F21CD33E4F57890DDEA5CF267ED2..
...Jane.Doe.....AD1FAB10D33E4F57890DDEA5CF267ED2..
...John.Key.....3374E9E7E33E4F57890DDEA5CF267ED2..

Which of the following tools will the hacker use against this type of capture?

- A. Password cracker
- B. Vulnerability scanner
- C. DLP scanner
- D. Fuzzer

Answer: A

NEW QUESTION 242

- (Exam Topic 5)

Which of the following is the BEST reason to run an untested application in a sandbox?

- A. To allow the application to take full advantage of the host system's resources and storage
- B. To utilize the host system's antivirus and firewall applications instead of running its own protection
- C. To prevent the application from acquiring escalated privileges and accessing its host system
- D. To increase application processing speed so the host system can perform real-time logging

Answer: C

NEW QUESTION 246

- (Exam Topic 5)

A security architect has convened a meeting to discuss an organization's key management policy. The organization has a reliable internal key management system, and some argue that it would be best to manage the cryptographic keys internally as opposed to using a solution from a third party. The company should use:

- A. the current internal key management system.
- B. a third-party key management system that will reduce operating costs.
- C. risk benefits analysis results to make a determination.
- D. a software solution including secure key escrow capabilities.

Answer: C

NEW QUESTION 247

- (Exam Topic 5)

A security analyst is hardening a WiFi infrastructure. The primary requirements are the following:

- ▶ The infrastructure must allow staff to authenticate using the most secure method.
 - ▶ The infrastructure must allow guests to use an "open" WiFi network that logs valid email addresses before granting access to the Internet.
- Given these requirements, which of the following statements BEST represents what the analyst should recommend and configure?

- A. Configure a captive portal for guests and WPS for staff.
- B. Configure a captive portal for staff and WPA for guests.
- C. Configure a captive portal for staff and WEP for guests.
- D. Configure a captive portal for guest and WPA2 Enterprise for staff

Answer: D

NEW QUESTION 252

- (Exam Topic 5)

While troubleshooting a client application connecting to the network, the security administrator notices the following error: Certificate is not valid. Which of the following is the BEST way to check if the digital certificate is valid?

- A. PKI
- B. CRL
- C. CSR
- D. IPSec

Answer: B

NEW QUESTION 255

- (Exam Topic 5)

A user typically works remotely over the holidays using a web-based VPN to access corporate resources. The user reports getting untrusted host errors and being unable to connect. Which of the following is MOST likely the case?

- A. The certificate has expired
- B. The browser does not support SSL
- C. The user's account is locked out
- D. The VPN software has reached the seat license maximum

Answer: A

NEW QUESTION 258

- (Exam Topic 5)

An audit reported identifies a weakness that could allow unauthorized personnel access to the facility at its main entrance and from there gain access to the network. Which of the following would BEST resolve the vulnerability?

- A. Faraday cage

- B. Air gap
- C. Mantrap
- D. Bollards

Answer: C

NEW QUESTION 263

- (Exam Topic 5)

A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. After network enumeration, the analyst's NEXT step is to perform:

- A. a risk analysis.
- B. a vulnerability assessment.
- C. a gray-box penetration test.
- D. an external security audit.
- E. a red team exercise.

Answer: C

NEW QUESTION 268

- (Exam Topic 5)

An analyst is using a vulnerability scanner to look for common security misconfigurations on devices. Which of the following might be identified by the scanner? (Select TWO).

- A. The firewall is disabled on workstations.
- B. SSH is enabled on servers.
- C. Browser homepages have not been customized.
- D. Default administrator credentials exist on networking hardware.
- E. The OS is only set to check for updates once a day.

Answer: AB

NEW QUESTION 272

- (Exam Topic 5)

Which of the following components of printers and MFDs are MOST likely to be used as vectors of compromise if they are improperly configured?

- A. Embedded web server
- B. Spooler
- C. Network interface
- D. LCD control panel

Answer: A

NEW QUESTION 276

- (Exam Topic 5)

A security administrator installed a new network scanner that identifies new host systems on the network. Which of the following did the security administrator install?

- A. Vulnerability scanner
- B. Network-based IDS
- C. Rogue system detection
- D. Configuration compliance scanner

Answer: C

NEW QUESTION 280

- (Exam Topic 5)

An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.

Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?

- A. Firewall; implement an ACL on the interface
- B. Router; place the correct subnet on the interface
- C. Switch; modify the access port to trunk port
- D. Proxy; add the correct transparent interface

Answer: B

NEW QUESTION 282

- (Exam Topic 5)

A systems administrator has isolated an infected system from the network and terminated the malicious process from executing. Which of the following should the administrator do NEXT according to the incident response process?

- A. Restore lost data from a backup.
- B. Wipe the system.
- C. Document the lessons learned.
- D. Determine the scope of impact.

Answer: A**NEW QUESTION 284**

- (Exam Topic 5)

A user downloads and installs an MP3 converter, and runs the application. Upon running the application, the antivirus detects a new port in a listening state. Which of the following has the user MOST likely executed?

- A. RAT
- B. Worm
- C. Ransomware
- D. Bot

Answer: A**NEW QUESTION 286**

- (Exam Topic 5)

When it comes to cloud computing, if one of the requirements for a project is to have the most control over the systems in the cloud, which of the following is a service model that would be BEST suited for this goal?

- A. Infrastructure
- B. Platform
- C. Software
- D. Virtualization

Answer: A**NEW QUESTION 288**

- (Exam Topic 5)

Which of the following is a deployment concept that can be used to ensure only the required OS access is exposed to software applications?

- A. Staging environment
- B. Sandboxing
- C. Secure baseline
- D. Trusted OS

Answer: B**NEW QUESTION 290**

- (Exam Topic 5)

A security analyst is investigating a potential breach. Upon gathering, documenting, and securing the evidence, which of the following actions is the NEXT step to minimize the business impact?

- A. Launch an investigation to identify the attacking host
- B. Initiate the incident response plan
- C. Review lessons learned captured in the process
- D. Remove malware and restore the system to normal operation

Answer: D**NEW QUESTION 291**

- (Exam Topic 5)

A Chief Information Officer (CIO) has decided it is not cost effective to implement safeguards against a known vulnerability. Which of the following risk responses does this BEST describe?

- A. Transference
- B. Avoidance
- C. Mitigation
- D. Acceptance

Answer: D**NEW QUESTION 293**

- (Exam Topic 5)

Attackers have been using revoked certificates for MITM attacks to steal credentials from employees of Company.com. Which of the following options should Company.com implement to mitigate these attacks?

- A. Captive portal
- B. OCSP stapling
- C. Object identifiers
- D. Key escrow
- E. Extended validation certificate

Answer: B**NEW QUESTION 297**

- (Exam Topic 5)

An application was recently compromised after some malformed data came in via web form. Which of the following would MOST likely have prevented this?

- A. Input validation
- B. Proxy server
- C. Stress testing
- D. Encoding

Answer: A

NEW QUESTION 301

.....

Thank You for Trying Our Product

* **100% Pass or Money Back**

All our products come with a 90-day Money Back Guarantee.

* **One year free update**

You can enjoy free update one year. 24x7 online support.

* **Trusted by Millions**

We currently serve more than 30,000,000 customers.

* **Shop Securely**

All transactions are protected by VeriSign!

100% Pass Your SY0-501 Exam with Our Prep Materials Via below:

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