

SY0-501 Dumps

CompTIA Security+ Certification Exam

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



NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: A

Explanation:

EAP by itself is only an authentication framework.

PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated. The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel is protected. As a result, when EAP messages are able to be discovered in the “clear” they do not provide the protection that was assumed when the protocol was originally authored.

PEAP, EAP-TTLS, and EAP-TLS “protect” inner EAP authentication within SSL/TLS sessions.

NEW QUESTION 2

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 3

- (Exam Topic 1)

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 4

- (Exam Topic 1)

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

- A. Elasticity
- B. Scalability
- C. High availability
- D. Redundancy

Answer: A

Explanation:

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

NEW QUESTION 5

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 6

- (Exam Topic 1)

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 7

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 8

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 9

- (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 10

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

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 12

- (Exam Topic 1)

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

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

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

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

Answer: C

NEW QUESTION 14

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 17

- (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.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 21

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 26

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 29

- (Exam Topic 1)

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

- A. Verify the certificate has not expired on the server.
- B. Ensure the certificate has a .pfx extension on the server.

- C. Update the root certificate into the client computer certificate store.
- D. Install the updated private key on the web server.
- E. Have users clear their browsing history and relaunch the session.

Answer: AC

NEW QUESTION 32

- (Exam Topic 1)

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 37

- (Exam Topic 1)

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

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

Answer: BE

NEW QUESTION 42

- (Exam Topic 1)

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 47

- (Exam Topic 1)

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 49

- (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 51

- (Exam Topic 1)

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 55

- (Exam Topic 1)

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 58

- (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 organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.

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

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

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

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

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

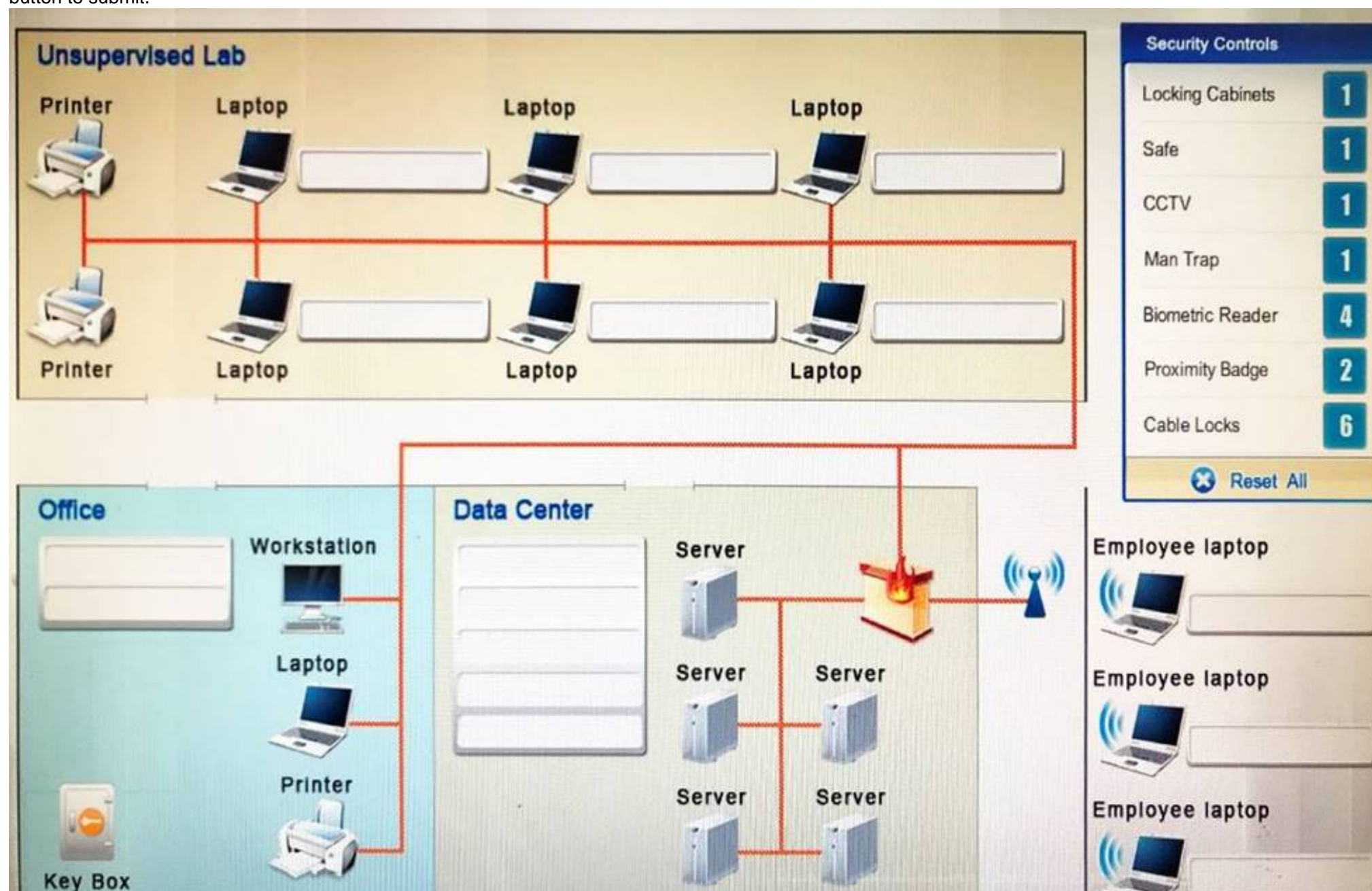
Answer: A

NEW QUESTION 59

- (Exam Topic 1)

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.



- A. Mastered
- B. Not Mastered

Answer: A

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

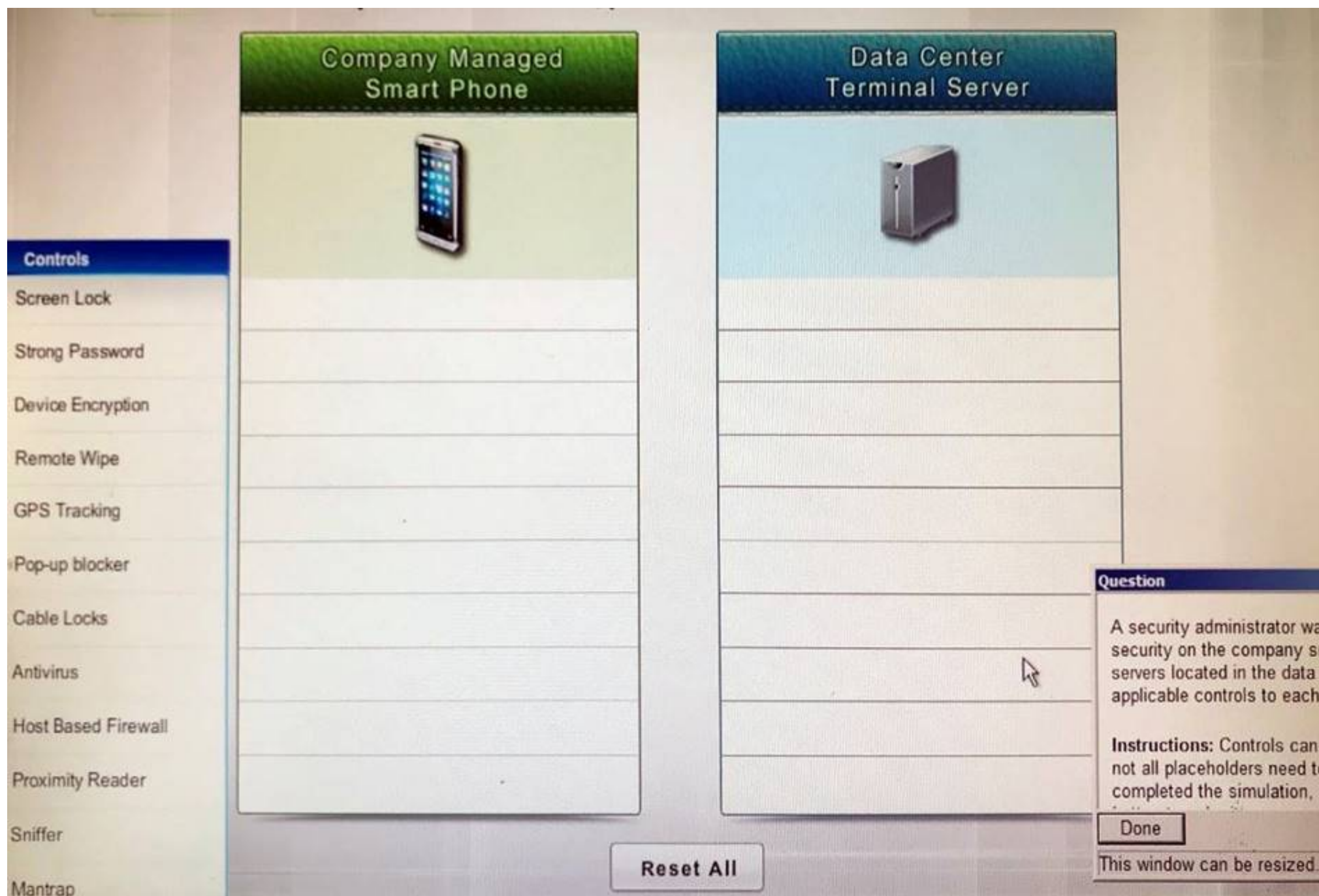
Mantrap can be used to control access to sensitive areas. CCTV can be used as video surveillance. Biometric reader can be used to control and prevent unauthorized access. Locking cabinets can be used to protect backup media, documentation and other physical artefacts.

NEW QUESTION 61

- (Exam Topic 1)

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. Mastered
- B. Not Mastered

Answer: A

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 62

- (Exam Topic 1)

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 64

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 65

- (Exam Topic 1)

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 68

- (Exam Topic 1)

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

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

Answer: AC

NEW QUESTION 72

- (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 75

- (Exam Topic 1)

Which of the following encryption methods does PKI typically use to securely project keys?

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

Answer: C

NEW QUESTION 76

- (Exam Topic 1)

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 80

- (Exam Topic 1)

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 84


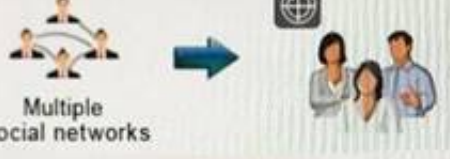




- (Exam Topic 1)

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
 <p>Attacker gains confidential company information</p>	 <p>Targeted CEO and board members</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>
 <p>Attacker posts link to fake AV software</p>	 <p>Broad set of victims</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>
 <p>Attacker collecting credit card details</p>	 <p>Phone-based victim</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>
 <p>Attacker mass-mails product information to parties that have already opted out of receiving advertisements</p>	 <p>Broad set of recipients</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>
 <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>	 <p>Victims</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>

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 86

- (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 IGAP packet, triggering the alert.
- D. The attacker sent a malformed TCP packet, triggering the alert.
- E. The TTL value is outside of the expected range, triggering the alert.

Answer: BC

NEW QUESTION 88

- (Exam Topic 1)

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 93

- (Exam Topic 1)

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 96

- (Exam Topic 1)

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 98

- (Exam Topic 1)

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 103

- (Exam Topic 1)

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 106

- (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 107

- (Exam Topic 1)

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 109

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 113

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 114

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 119

- (Exam Topic 1)

A company is currently using the following configuration:

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

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

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

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

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

Answer: AC

NEW QUESTION 122

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 124

- (Exam Topic 1)

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 128

- (Exam Topic 1)

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

- A. Life
- B. Intellectual property
- C. Sensitive data

D. Public reputation

Answer: A

NEW QUESTION 132

- (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 134

- (Exam Topic 1)

A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

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

Answer: B

Explanation:

Only Kerberos that can do Mutual Auth and Delegation.

NEW QUESTION 137

- (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. Least privilege

Answer: DFI

NEW QUESTION 140

- (Exam Topic 2)

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 143

- (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 145

- (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 148

- (Exam Topic 2)

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 153

- (Exam Topic 2)

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

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

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

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

Answer: A

NEW QUESTION 154

- (Exam Topic 2)

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 156

- (Exam Topic 2)

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 161

- (Exam Topic 2)

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 163


- (Exam Topic 2)


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.


Authentication Server


Email Archive


Identity Management Server


Media Streaming Server

Stripe Data

Mirror Data

RAID-0	Server Profile:	RAID-1	Server Profile:
<div style="display: flex; justify-content: space-between; font-size: 0.8em;"> Disk 1Disk 2Disk 3Disk 4 </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> </div> <div style="margin-top: 5px;"> <input type="checkbox"/> <div style="background-color: #d3d3d3; padding: 2px; text-align: center;">Parity Data</div> </div> <div style="margin-top: 5px;"> <input type="checkbox"/> <div style="background-color: #d3d3d3; padding: 2px; text-align: center;">Parity Data</div> </div>	<div style="border: 1px dashed #ccc; width: 40px; height: 40px; margin: 0 auto;"></div>	<div style="display: flex; justify-content: space-between; font-size: 0.8em;"> Disk 1Disk 2Disk 3Disk 4 </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> </div> <div style="margin-top: 5px;"> <input type="checkbox"/> <div style="background-color: #d3d3d3; padding: 2px; text-align: center;">Parity Data</div> </div> <div style="margin-top: 5px;"> <input type="checkbox"/> <div style="background-color: #d3d3d3; padding: 2px; text-align: center;">Parity Data</div> </div>	<div style="border: 1px dashed #ccc; width: 40px; height: 40px; margin: 0 auto;"></div>
<div style="display: flex; justify-content: space-between; font-size: 0.8em;"> Disk 1Disk 2Disk 3Disk 4 </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> </div> <div style="margin-top: 5px;"> <input type="checkbox"/> <div style="background-color: #d3d3d3; padding: 2px; text-align: center;">Parity Data</div> </div> <div style="margin-top: 5px;"> <input type="checkbox"/> <div style="background-color: #d3d3d3; padding: 2px; text-align: center;">Parity Data</div> </div>	<div style="border: 1px dashed #ccc; width: 40px; height: 40px; margin: 0 auto;"></div>	<div style="display: flex; justify-content: space-between; font-size: 0.8em;"> Disk 1Disk 2Disk 3Disk 4 </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> <div style="border: 1px solid #ccc; width: 40px; height: 20px;"></div> </div> <div style="margin-top: 5px;"> <input type="checkbox"/> <div style="background-color: #d3d3d3; padding: 2px; text-align: center;">Parity Data</div> </div> <div style="margin-top: 5px;"> <input type="checkbox"/> <div style="background-color: #d3d3d3; padding: 2px; text-align: center;">Parity Data</div> </div>	<div style="border: 1px dashed #ccc; width: 40px; height: 40px; margin: 0 auto;"></div>

Reset All

- A. Mastered
- B. Not Mastered

Answer: A

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 single 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 166

- (Exam Topic 2)

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 169

- (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 174

- (Exam Topic 2)

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 177

- (Exam Topic 2)

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 180

- (Exam Topic 2)

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

-Initial IR engagement time frame

-Length of time before an executive management notice went out

-Average IR phase completion

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

- A. CSIRT
- B. Containment phase

- C. Escalation notifications
- D. Tabletop exercise

Answer: D

NEW QUESTION 185

- (Exam Topic 2)

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 190

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 191

- (Exam Topic 2)

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 192

- (Exam Topic 2)

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 197

- (Exam Topic 2)

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 198

- (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 203

- (Exam Topic 2)

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 206

- (Exam Topic 2)

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 210

- (Exam Topic 2)

Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures.

Which of the following should be implemented to correct this issue?

- A. Decrease the room temperature
- B. Increase humidity in the room
- C. Utilize better hot/cold aisle configurations
- D. Implement EMI shielding

Answer: B

NEW QUESTION 215

- (Exam Topic 2)

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 216

- (Exam Topic 2)

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

- A. Implement time-of-day restrictions.

- B. Audit file access times.
- C. Secretly install a hidden surveillance camera.
- D. Require swipe-card access to enter the lab.

Answer: D

NEW QUESTION 219

- (Exam Topic 2)

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

- A. Document and lock the workstations in a secure area to establish chain of custody
- B. Notify the IT department that the workstations are to be reimaged and the data restored for reuse
- C. Notify the IT department that the workstations may be reconnected to the network for the users to continue working
- D. Document findings and processes in the after-action and lessons learned report

Answer: D

NEW QUESTION 223

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 225

- (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 228

- (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 232

- (Exam Topic 2)

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 234

- (Exam Topic 2)

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 237

- (Exam Topic 2)

Which of the following should identify critical systems and components?

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

Answer: D

NEW QUESTION 242

- (Exam Topic 2)

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 245

- (Exam Topic 2)

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 248

- (Exam Topic 2)

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

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

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

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

Answer: B

NEW QUESTION 249

- (Exam Topic 2)

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 251

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 253

- (Exam Topic 2)

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 258

- (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 (SAM) attribute of a certificate?

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

Answer: B

NEW QUESTION 260

- (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 265

- (Exam Topic 2)

A new firewall has been placed 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 from 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 268

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 269

- (Exam Topic 2)

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 271

- (Exam Topic 2)

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 274

- (Exam Topic 2)

Company policy requires the use of passphrases instead of 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 279

- (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 280

- (Exam Topic 2)

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 283

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 285

- (Exam Topic 3)

The Chief Executive Officer (CEO) of a major defense contracting company is 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 286

- (Exam Topic 3)

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 290

- (Exam Topic 3)

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 291

- (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 292

- (Exam Topic 3)

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

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

Answer: B

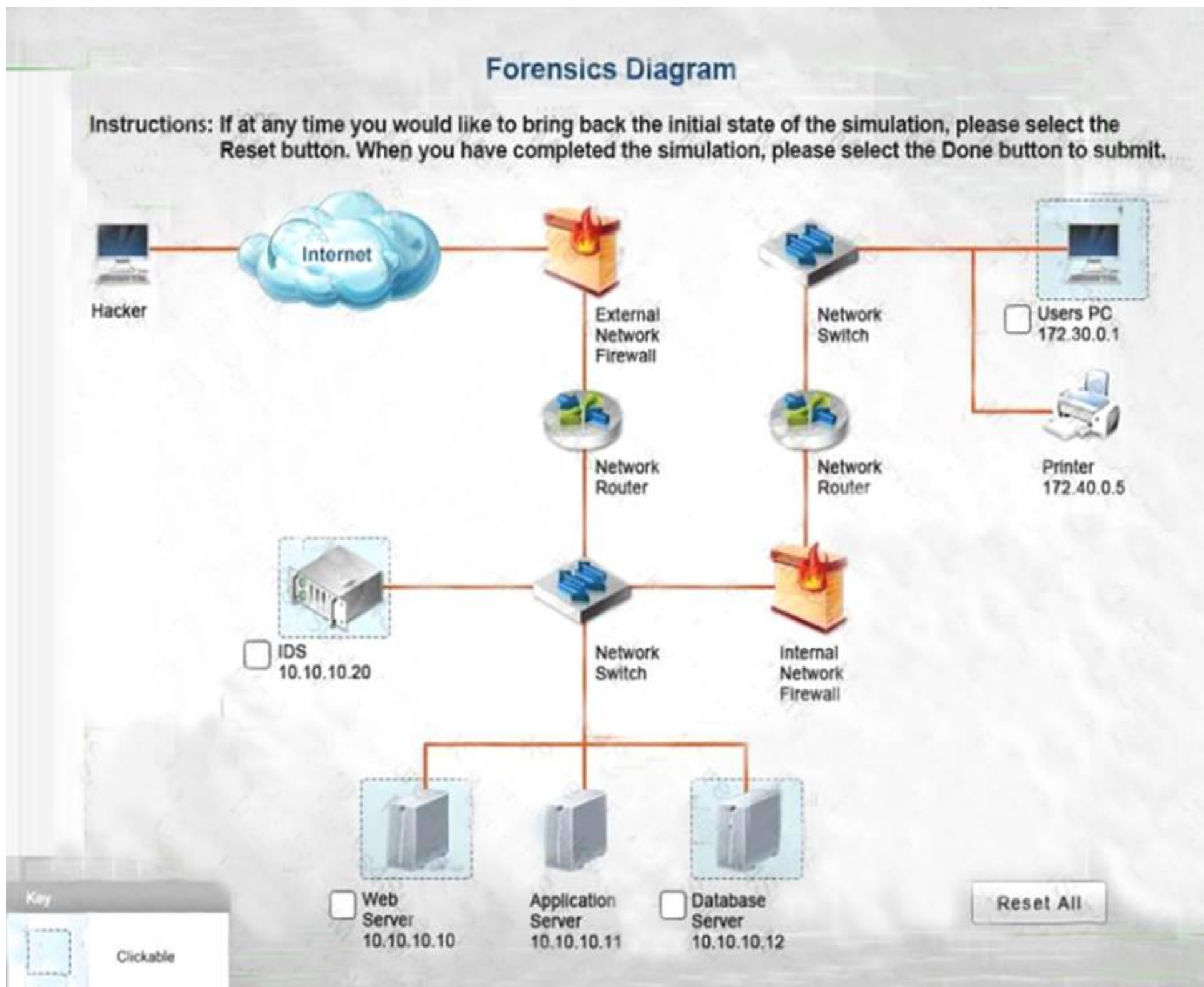
NEW QUESTION 293

- (Exam Topic 3)

A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.

You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incident responses.

Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. 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.

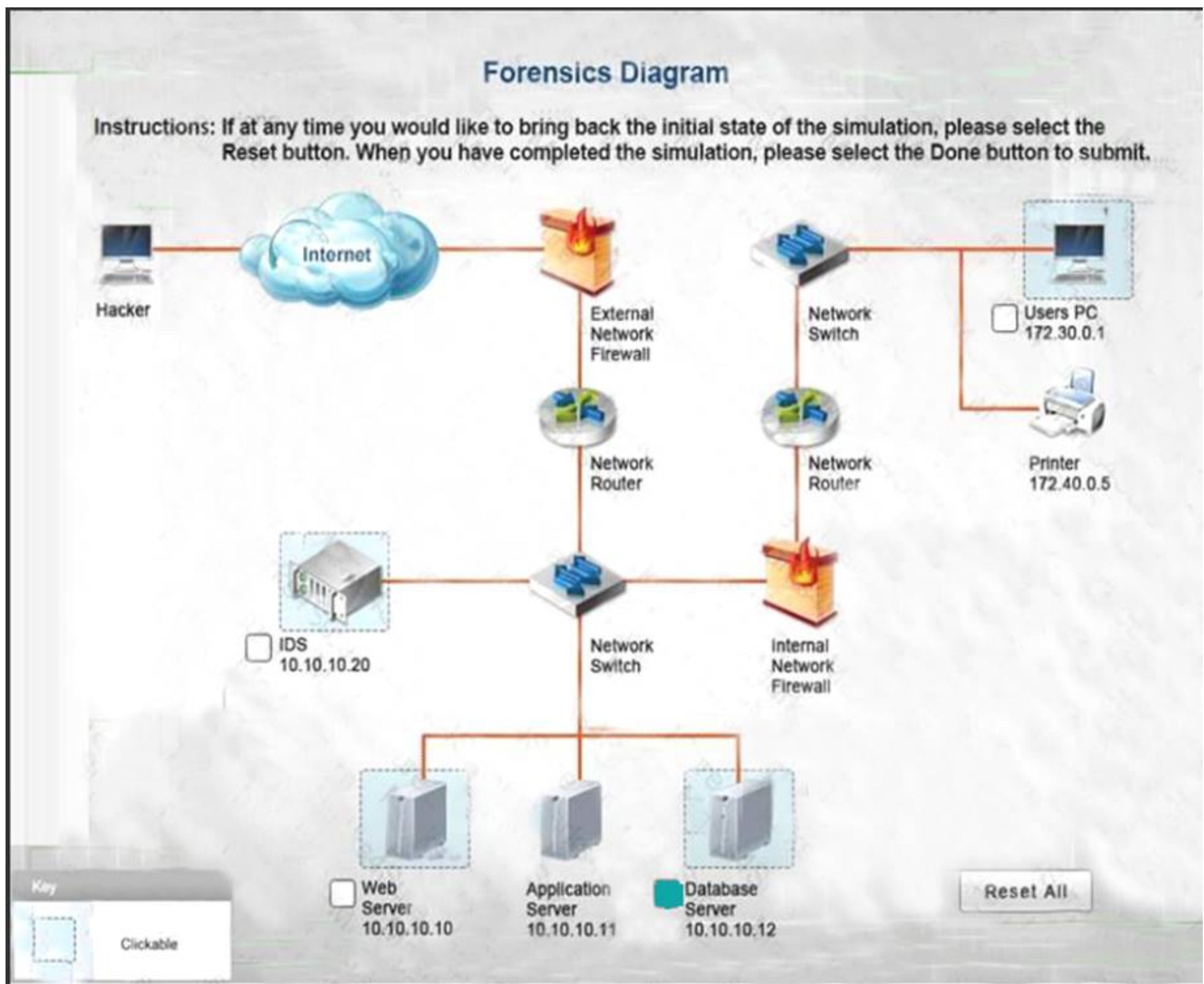


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Database server was attacked, actions should be to capture network traffic and Chain of Custody.



Logs
⚙️ Actions

Possible Actions:

- Capture Network Traffic
- Chain Of Custody
- Format
- Hash
- Image
- Record Time Offset
- System Restore

Actions Performed:

- Capture Network Traffic
- Chain Of Custody
-
-
-
-
-

IDS Server Log:

Web Server Log:

The screenshot shows a web server log viewer interface. At the top, there are two tabs: 'Logs' (selected) and 'Actions'. The 'Logs' tab displays a list of HTTP requests. Each log entry consists of two lines: the first line contains the IP address, timestamp, method, URL, status code, and size; the second line contains the referrer and user agent. The logs are organized into alternating light blue and white rows.

Log Entries (Top Section):

- fcrawler.company.com - - [26/Apr/2010:00:22:49 -0400] "GET /contacts.html HTTP/1.0" 200 4000
"FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
- 123.123.123.123 - - [26/Apr/2010:00:22:49 -0400] "GET /pics/5star2000.gif HTTP/1.0" 200 4005
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- fcrawler.company.com - - [26/Apr/2010:00:22:50 -0400] "GET /news/news.html HTTP/1.0" 200 16716 "-"
"FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
- 123.123.123.123 - - [26/Apr/2010:00:22:50 -0400] "GET /pics/5star.gif HTTP/1.0" 200 1031
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /pics/a2hlogo.jpg HTTP/1.0" 200 4282
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /cgi-bin/newcount?command=null&jafsof3&width=4&font=digital&noshw HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- ppp931.on.company.com - - [26/Apr/2010:00:22:52 -0400] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html" "Mozilla/4.7 [en]C-SYMPA (Win95; U)"
- 123.123.123.123 - - [26/Apr/2010:00:22:53 -0400] "GET /cgi-bin/newcount?command=ls HTTP/1.0" 200 36
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=whoami HTTP/1.0" 200 36
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 151.44.15.252 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863
"http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

Log Entries (Bottom Section):

- 151.44.15.252 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863
"http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=ls%20-l%20/data/finance/payroll/*.xls HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 123.123.123.123 - - [26/Apr/2010:00:23:00 -0400] "GET /cgi-bin/newcount?command=scp%20/data/finance/payroll/gi-Nov2010.xls%20root@123.123.123.123: HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
- 213.60.233.243 - - [25/May/2010:00:17:09 +1200] "GET /internet/index.html HTTP/1.1" 200 6792
"http://www.company.com/video/streaming/http.html" "Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413 Debian/1.6-5"
- 151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /js/master.js HTTP/1.1" 200 2263 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /css/master.css HTTP/1.1" 200 6123 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /images/navigation/home1.gif HTTP/1.1" 200 2735 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /data/zookeeper/co-100.gif HTTP/1.1" 200 196 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 151.44.15.252 - - [25/May/2010:00:17:22 +1200] "GET /adsense-alternate.html HTTP/1.1" 200 887 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
- 151.44.15.252 - - [25/May/2010:00:17:39 +1200] "GET /data/zookeeper/status.html HTTP/1.1" 200 4195 "http://www.company.com/cgi-bin/forum/comm"

Database Server Log:

→ Logs

Actions

X

Database Server Log

Audit Failure	2012/4/16 11:33	Microsoft Windows security auditing.	4625	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4648	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Failure	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon

Users PC Log:

**NEW QUESTION 298**

- (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 300

- (Exam Topic 3)

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 301

- (Exam Topic 3)

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 306

- (Exam Topic 3)

Which of the following is the LEAST secure hashing algorithm?

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

Answer: C

NEW QUESTION 311

- (Exam Topic 3)

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 313

- (Exam Topic 3)

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 318

- (Exam Topic 3)

Given the log output:

Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS:

Login Success [user: msmith] [Source: 10.0.12.45] [localport: 23] at 00:15:23:431 CET Sun Mar 15 2015

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

- A. Configure port security for logons
- B. Disable telnet and enable SSH
- C. Configure an AAA server
- D. Disable password and enable RSA authentication

Answer: B

NEW QUESTION 323

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 326

- (Exam Topic 3)

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 331

- (Exam Topic 3)

A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed

strange white markings in different areas of the parking lot. The person is attempting which of the following types of attacks?

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

Answer: B

NEW QUESTION 333

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 337

- (Exam Topic 3)

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 338

- (Exam Topic 3)

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 343

- (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 347

- (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 352

- (Exam Topic 3)

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

- A. Account lockout
- B. Group Based Privileges

- C. Least privilege
- D. Password complexity

Answer: A

NEW QUESTION 355

- (Exam Topic 3)

Recently several employees were victims of a phishing email that appeared to originate from the company president. The email claimed the employees would be disciplined if they did not click on a malicious link in the message. Which of the following principles of social engineering made this attack successful?

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

Answer: A

NEW QUESTION 358

- (Exam Topic 3)

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 359

- (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 362

- (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 366

- (Exam Topic 3)

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 369

- (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 371

- (Exam Topic 3)

The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred. By doing which of the following is the CSO most likely to reduce the number of incidents?

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

Answer: C

NEW QUESTION 374

- (Exam Topic 3)

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 in 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 376

- (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 380

- (Exam Topic 3)

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 383

- (Exam Topic 3)

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 386

- (Exam Topic 3)

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

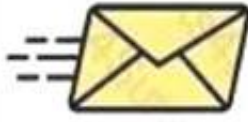









- A. Implement deduplication at the network level between the two locations
- B. Implement deduplication on the storage array to reduce the amount of drive space needed
- C. Implement deduplication on the server storage to reduce the data backed up
- D. Implement deduplication on both the local and remote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

Answer: B

NEW QUESTION 387

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

Spoofting

Hoax

Spam

Spim

Social Engineering

- 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 390

- (Exam Topic 3)

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 393

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 394

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 396

- (Exam Topic 3)

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 aisles
- C. To eliminate the potential for electromagnetic interference
- D. To maximize fire suppression capabilities

Answer: B

NEW QUESTION 400

- (Exam Topic 3)

A security administrator is evaluating three different services: radius, diameter, and Kerberos. Which of the following is a feature that is UNIQUE to Kerberos?

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

Answer: B

NEW QUESTION 405

- (Exam Topic 3)

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 409

- (Exam Topic 3)

An administrator discovers the following log entry on a server: Nov 12 2013 00:23:45 httpd[2342]:

GET/app2/prod/proc/process.php?input=change;cd%20../../etc;cat%20shadow
Which of the following attacks is being attempted?

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

Answer: B

NEW QUESTION 414

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 416

- (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 418

- (Exam Topic 3)

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 423

- (Exam Topic 3)

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 427

- (Exam Topic 3)

A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.

Which of the following has the administrator been tasked to perform?

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

Answer: D

NEW QUESTION 430

- (Exam Topic 4)

In determining when it may be necessary to perform a credentialed scan against a system instead of a noncredentialed scan, which of the following requirements

is MOST likely to influence this decision?

- A. The scanner must be able to enumerate the host OS of devices scanned.
- B. The scanner must be able to footprint the network.
- C. The scanner must be able to check for open ports with listening services.
- D. The scanner must be able to audit file system permissions

Answer: D

NEW QUESTION 431

- (Exam Topic 4)

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 433

- (Exam Topic 4)

A security administrator wants to implement a logon script that will prevent MITM attacks on the local LAN. Which of the following commands should the security administrator implement within the script to accomplish this task?

- A. arp - s 192.168.1.1 00-3a-d1-fa-b1-06
- B. dig - x@192.168.1.1 mypc.comptia.com
- C. nmap - A - T4 192.168.1.1
- D. tcpdump - Inv host 192.168.1.1 or either 00:3a:d1:fa:b1:06

Answer: A

NEW QUESTION 435

- (Exam Topic 4)

Which of the following is the BEST choice for a security control that represents a preventive and corrective logical control at the same time?

- A. Security awareness training
- B. Antivirus
- C. Firewalls
- D. Intrusion detection system

Answer: B

NEW QUESTION 440

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 441

- (Exam Topic 4)

Which of the following strategies should a systems architect use to minimize availability risks due to insufficient storage capacity?

- A. High availability
- B. Scalability
- C. Distributive allocation
- D. Load balancing

Answer: B

NEW QUESTION 446

- (Exam Topic 4)

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

- A. NAC
- B. VLAN
- C. DMZ
- D. Subnet

Answer: C

NEW QUESTION 451

- (Exam Topic 4)

A security analyst has set up a network tap to monitor network traffic for vulnerabilities. Which of the following techniques would BEST describe the approach the analyst has taken?

- A. Compliance scanning
- B. Credentialed scanning
- C. Passive vulnerability scanning
- D. Port scanning

Answer: D

NEW QUESTION 453

- (Exam Topic 4)

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 457

- (Exam Topic 4)

A penetration tester harvests potential usernames from a social networking site. The penetration tester then uses social engineering to attempt to obtain associated passwords to gain unauthorized access to shares on a network server.

Which of the following methods is the penetration tester MOST likely using?

- A. Escalation of privilege
- B. SQL injection
- C. Active reconnaissance
- D. Proxy server

Answer: C

NEW QUESTION 461

- (Exam Topic 4)

Which of the following is commonly done as part of a vulnerability scan?

- A. Exploiting misconfigured applications
- B. Cracking employee passwords
- C. Sending phishing emails to employees
- D. Identifying unpatched workstations

Answer: D

NEW QUESTION 465

- (Exam Topic 4)

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 470

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 473

- (Exam Topic 4)

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 475

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 478

- (Exam Topic 4)

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

- A. Data Labeling and disposal
- B. Use of social networking
- C. Use of P2P networking
- D. Role-based training

Answer: B

NEW QUESTION 479

- (Exam Topic 4)

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 480

- (Exam Topic 4)

As part of a new BYOD rollout, a security analyst has been asked to find a way to securely store company data on personal devices. Which of the following would BEST help to accomplish this?

- A. Require the use of an eight-character PIN.
- B. Implement containerization of company data.
- C. Require annual AUP sign-off.
- D. Use geofencing tools to unlock devices while on the premises.

Answer: B

NEW QUESTION 483

- (Exam Topic 4)

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 485

- (Exam Topic 4)

Many employees are receiving email messages similar to the one shown below:

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

- A. BLOCK http://www.*.info/ "
- B. DROP [http:// \"website.info/email.php?*](http://\)
- C. Redirect http://www,*.Info/email.php?quota=*TOhttp://company.com/corporate_policy.html
- D. DENY http://*.info/email.php?quota=1Gb

Answer: D

NEW QUESTION 487

- (Exam Topic 4)

A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party. Which of the following actions did the company take regarding risks related to its email and collaboration services?

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

Answer: A

NEW QUESTION 490

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 492

- (Exam Topic 4)

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 496

- (Exam Topic 4)

Which of the following would allow for the QUICKEST restoration of a server into a warm recovery site in a case in which server data mirroring is not enabled?

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

Answer: C

NEW QUESTION 501

- (Exam Topic 4)

The computer resource center issued smartphones to all first-level and above managers. The managers have the ability to install mobile tools. Which of the following tools should be implemented to control the types of tools the managers install?

- A. Download manager
- B. Content manager
- C. Segmentation manager
- D. Application manager

Answer: D

NEW QUESTION 504

- (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 506

- (Exam Topic 4)

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 511

- (Exam Topic 4)

A web developer improves client access to the company's REST API. Authentication needs to be tokenized but not expose the client's password. Which of the following methods would BEST meet the developer's requirements?

- A. SAML
- B. LDAP
- C. OAuth
- D. Shibboleth

Answer: A

NEW QUESTION 516

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 518

- (Exam Topic 4)

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 522

- (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 523

- (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 524

- (Exam Topic 4)

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 525

- (Exam Topic 4)

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 527

- (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 532

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 535

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 539

- (Exam Topic 4)

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 540

- (Exam Topic 4)

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 543

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 547

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 549

- (Exam Topic 4)

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

- A. Block level encryption
- B. SAML authentication
- C. Transport encryption
- D. Multifactor authentication
- E. Predefined challenge QUESTION NO:s
- F. Hashing

Answer: BD

NEW QUESTION 553

- (Exam Topic 4)

A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following should the engineer implement if the design requires client MAC address to be visible across the tunnel?

- A. Tunnel mode IPSec
- B. Transport mode VPN IPSec
- C. L2TP
- D. SSL VPN

Answer: D

NEW QUESTION 554

- (Exam Topic 4)

An external contractor, who has not been given information about the software or network architecture, is conducting a penetration test. Which of the following BEST describes the test being performed?

- A. Black box
- B. White box
- C. Passive reconnaissance
- D. Vulnerability scan

Answer: A

NEW QUESTION 558

- (Exam Topic 4)

Which of the following penetration testing concepts is being used when an attacker uses public Internet databases to enumerate and learn more about a target?

- A. Reconnaissance
- B. Initial exploitation
- C. Pivoting
- D. Vulnerability scanning
- E. White box testing

Answer: A

NEW QUESTION 563

- (Exam Topic 4)

A security administrator is reviewing the following network capture:

```
192.168.20.43:2043 -> 10.234.66.21:80
```

```
POST "192.168.20.43 https://www.banksite.com<ENTER>JoeUsr<BackSPACE>erPassword<ENTER>"
```

Which of the following malware is MOST likely to generate the above information?

- A. Keylogger
- B. Ransomware
- C. Logic bomb
- D. Adware

Answer: A

NEW QUESTION 566

- (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 571**

- (Exam Topic 4)

A security administrator wants to configure a company's wireless network in a way that will prevent wireless clients from broadcasting the company's SSID. Which of the following should be configured on the company's access points?

- A. Enable ESSID broadcast
- B. Enable protected management frames
- C. Enable wireless encryption
- D. Disable MAC authentication
- E. Disable WPS
- F. Disable SSID broadcast

Answer: F**NEW QUESTION 572**

- (Exam Topic 4)

A security analyst captures forensic evidence from a potentially compromised system for further investigation. The evidence is documented and securely stored to FIRST:

- A. maintain the chain of custody.
- B. preserve the data.
- C. obtain a legal hold.
- D. recover data at a later time.

Answer: B**NEW QUESTION 573**

- (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 577

- (Exam Topic 5)

Which of the following metrics are used to calculate the SLE? (Select TWO)

- A. ROI
- B. ARO
- C. ALE
- D. MTBF
- E. MTTF
- F. TCO

Answer: BC

NEW QUESTION 582

- (Exam Topic 5)

A security technician is configuring an access management system to track and record user actions. Which of the following functions should the technician configure?

- A. Accounting
- B. Authorization
- C. Authentication
- D. Identification

Answer: A

NEW QUESTION 587

- (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 589

- (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 594

- (Exam Topic 5)

An office manager found a folder that included documents with various types of data relating to corporate clients. The office manager notified the data included dates of birth, addresses, and phone numbers for the clients. The office manager then reported this finding to the security compliance officer. Which of the following portions of the policy would the security officer need to consult to determine if a breach has occurred?

- A. Public
- B. Private
- C. PHI
- D. PII

Answer: D

NEW QUESTION 598

- (Exam Topic 5)

An organization's employees currently use three different sets of credentials to access multiple internal resources. Management wants to make this process less complex. Which of the following would be the BEST option to meet this goal?

- A. Transitive trust
- B. Single sign-on
- C. Federation
- D. Secure token

Answer: B

NEW QUESTION 599

- (Exam Topic 5)

When sending messages using symmetric encryption, which of the following must happen FIRST?

- A. Exchange encryption key
- B. Establish digital signatures
- C. Agree on an encryption method
- D. Install digital certificates

Answer: C

NEW QUESTION 601

- (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 604

- (Exam Topic 5)

A technician is configuring a load balancer for the application team to accelerate the network performance of their applications. The applications are hosted on multiple servers and must be redundant. Given this scenario, which of the following would be the BEST method of configuring the load balancer?

- A. Round-robin
- B. Weighted
- C. Least connection
- D. Locality-based

Answer: D

NEW QUESTION 606

- (Exam Topic 5)

Which of the following uses precomputed hashes to guess passwords?

- A. Iptables
- B. NAT tables
- C. Rainbow tables
- D. ARP tables

Answer: C

NEW QUESTION 608

- (Exam Topic 5)

A security administrator is reviewing the following PowerShell script referenced in the Task Scheduler on a database server:

```
$members = GetADGroupMemeber -Identity "Domain Admins" -Recursive | Select - ExpandProperty  
name  
if ($members -notcontains "JohnDoe"){  
Remove-Item -path C:\Database -recurse -force  
}
```

Which of the following did the security administrator discover?

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

Answer: C

NEW QUESTION 613

- (Exam Topic 5)

Two users must encrypt and transmit large amounts of data between them. Which of the following should they use to encrypt and transmit the data?

- A. Symmetric algorithm
- B. Hash function
- C. Digital signature
- D. Obfuscation

Answer: A

NEW QUESTION 615

- (Exam Topic 5)

A technician receives a device with the following anomalies: Frequent pop-up ads

Show response-time switching between active programs Unresponsive peripherals The technician reviews the following log file entries:

File Name Source MD5 Target MD5 Status
antivirus.exe F794F21CD33E4F57890DDEA5CF267ED2 F794F21CD33E4F57890DDEA5CF267ED2
Automatic iexplore.exe 7FAAF21CD33E4F57890DDEA5CF29CCEA AA87F21CD33E4F57890DDEAEE2197333 Automatic service.exe
77FF390CD33E4F57890DDEA5CF28881F 77FF390CD33E4F57890DDEA5CF28881F Manual USB.exe E289F21CD33E4F57890DDEA5CF28EDC0
E289F21CD33E4F57890DDEA5CF28EDC0 Stopped
Based on the above output, which of the following should be reviewed?

- A. The web application firewall
- B. The file integrity check
- C. The data execution prevention
- D. The removable media control

Answer: B

NEW QUESTION 619

- (Exam Topic 5)

Which of the following describes the key difference between vishing and phishing attacks?

- A. Phishing is used by attackers to steal a person's identity.
- B. Vishing attacks require some knowledge of the target of attack.
- C. Vishing attacks are accomplished using telephony services.
- D. Phishing is a category of social engineering attack.

Answer: C

NEW QUESTION 623

- (Exam Topic 5)

User from two organizations, each with its own PKI, need to begin working together on a joint project. Which of the following would allow the users of the separate PKIs to work together without connection errors?

- A. Trust model
- B. Stapling
- C. Intermediate CA
- D. Key escrow

Answer: A

NEW QUESTION 626

- (Exam Topic 5)

Which of the following types of penetration test will allow the tester to have access only to password hashes prior to the penetration test?

- A. Black box
- B. Gray box
- C. Credentialed
- D. White box

Answer: B

NEW QUESTION 629

- (Exam Topic 5)

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. Local account
- B. Guest account
- C. Service account
- D. User account

Answer: C

NEW QUESTION 634

- (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 639

- (Exam Topic 5)

The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment MUST be deployed to guard against unknown threats?

- A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates
- B. Implementation of an off-site datacenter hosting all company data, as well as deployment of VDI for all client computing needs
- C. Host-based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs
- D. Behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed

Answer: D

NEW QUESTION 640

- (Exam Topic 5)

While working on an incident, Joe, a technician, finished restoring the OS and applications on a workstation from the original media. Joe is about to begin copying the user's files back onto the hard drive. Which of the following incident response steps is Joe working on now?

- A. Recovery
- B. Eradication
- C. Containment
- D. Identification

Answer: A

NEW QUESTION 645

- (Exam Topic 5)

A remote intruder wants to take inventory of a network so exploits can be researched. The intruder is looking for information about software versions on the network. Which of the following techniques is the intruder using?

- A. Banner grabbing
- B. Port scanning
- C. Packet sniffing
- D. Virus scanning

Answer: A

NEW QUESTION 649

- (Exam Topic 5)

A security auditor is testing perimeter security in a building that is protected by badge readers. Which of the following types of attacks would MOST likely gain access?

- A. Phishing
- B. Man-in-the-middle
- C. Tailgating
- D. Watering hole
- E. Shoulder surfing

Answer: C

NEW QUESTION 652

- (Exam Topic 5)

A network administrator needs to allocate a new network for the R&D group. The network must not be accessible from the Internet regardless of the network firewall or other external misconfigurations. Which of the following settings should the network administrator implement to accomplish this?

- A. Configure the OS default TTL to 1
- B. Use NAT on the R&D network
- C. Implement a router ACL
- D. Enable protected ports on the switch

Answer: A

NEW QUESTION 653

- (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 654

- (Exam Topic 5)

A procedure differs from a policy in that it:

- A. is a high-level statement regarding the company's position on a topic.
- B. sets a minimum expected baseline of behavior.
- C. provides step-by-step instructions for performing a task.
- D. describes adverse actions when violations occur.

Answer: C

NEW QUESTION 656

- (Exam Topic 5)

A software developer is concerned about DLL hijacking in an application being written. Which of the following is the MOST viable mitigation measure of this type of attack?

- A. The DLL of each application should be set individually
- B. All calls to different DLLs should be hard-coded in the application
- C. Access to DLLs from the Windows registry should be disabled
- D. The affected DLLs should be renamed to avoid future hijacking

Answer: B

NEW QUESTION 661

- (Exam Topic 5)

A company wants to ensure confidential data from storage media is sanitized in such a way that the drive cannot be reused. Which of the following method should the technician use?

- A. Shredding
- B. Wiping
- C. Low-level formatting
- D. Repartitioning
- E. Overwriting

Answer: A

NEW QUESTION 664

- (Exam Topic 5)

Which of the following scenarios BEST describes an implementation of non-repudiation?

- A. A user logs into a domain workstation and access network file shares for another department
- B. A user remotely logs into the mail server with another user's credentials
- C. A user sends a digitally signed email to the entire finance department about an upcoming meeting
- D. A user access the workstation registry to make unauthorized changes to enable functionality within an application

Answer: C

NEW QUESTION 667

- (Exam Topic 5)

A security administrator is trying to eradicate a worm, which is spreading throughout the organization, using an old remote vulnerability in the SMB protocol. The worm uses Nmap to identify target hosts within the company. The administrator wants to implement a solution that will eradicate the current worm and any future attacks that may be using zero-day vulnerabilities. Which of the following would BEST meet the requirements when implemented?

- A. Host-based firewall
- B. Enterprise patch management system
- C. Network-based intrusion prevention system
- D. Application blacklisting
- E. File integrity checking

Answer: C

NEW QUESTION 672

- (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 677

- (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 678

- (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 683

.....

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>