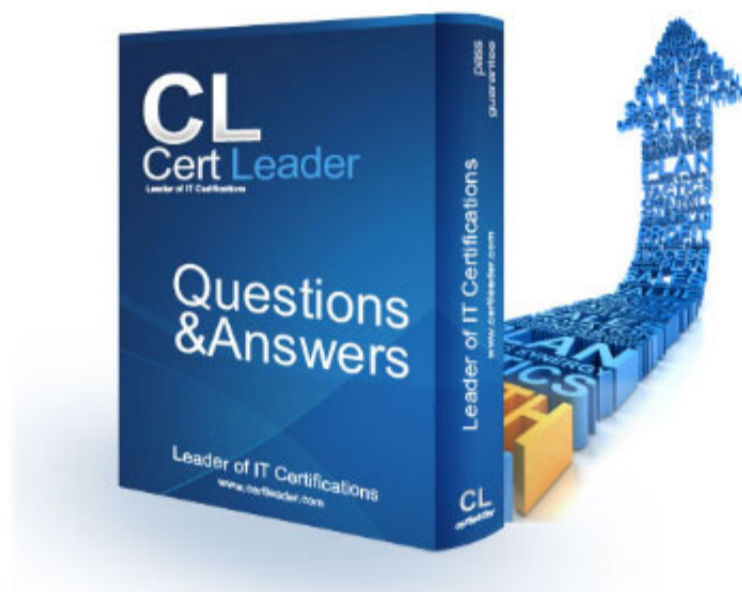


SY0-501 Dumps

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

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

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

Answer: C

NEW QUESTION 4

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 5

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 6

- (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 7

- (Exam Topic 1)

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

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

Answer: BC

NEW QUESTION 8

- (Exam Topic 1)

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

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

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

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

Answer: C

NEW QUESTION 9

- (Exam Topic 1)

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

File: winx86_adobe_flash_upgrade.exe Hash: 99ac28bede43ab869b853ba62c4ea243

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

Install Date	Package Name	Target Devices	Hash
10/10/2017	java_11.2_x64.exe	HQ PC's	01ab28bbde63aa879b35bba62cde5283
10/10/2017	winx86_adobe_flash_upgrade.exe	HQ PC's	99ac28bede43ab869b853ba62c4ea243

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

- A. The file was corrupted after it left the patch system.
- B. The file was infected when the patch manager downloaded it.

- C. The file was not approved in the application whitelist system.
- D. The file was embedded with a logic bomb to evade detection.

Answer: D

NEW QUESTION 10

- (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 10

- (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 13

- (Exam Topic 1)

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




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

Answer: A

NEW QUESTION 16

- (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 21

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 25

- (Exam Topic 1)

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

- A. Self-signed certificates

- B. Missing patches
- C. Auditing parameters
- D. Inactive local accounts

Answer: D

NEW QUESTION 27

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 30

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 35

- (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 36

- (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 37

- (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 40

- (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 43

- (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 46

- (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 48

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 53

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 55

- (Exam Topic 1)

A security analyst wishes to increase the security of an FTP server. Currently, all traffic to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modern FTP client software.

The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections. Which of the following would BEST accomplish these goals?

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

Answer: C

NEW QUESTION 57

- (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 62

- (Exam Topic 1)

Refer to the following code:

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

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

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

Answer: D

NEW QUESTION 65

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 66

- (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 71

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 75

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 76

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 80

- (Exam Topic 1)

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

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

Answer: AB

NEW QUESTION 84

- (Exam Topic 1)

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

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

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

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

Answer: BC

NEW QUESTION 87

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 88

- (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 91

- (Exam Topic 1)

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

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

Answer: BE

NEW QUESTION 94

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 97

- (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 99

- (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 103

- (Exam Topic 1)

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

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

Answer: AD

NEW QUESTION 105

- (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 109

- (Exam Topic 1)

A company is currently using the following configuration:

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

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

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

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

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

Answer: AC

NEW QUESTION 114

- (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 115

- (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 118

- (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 121

- (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 123

- (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 127

- (Exam Topic 2)

A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production.

Which of the following would correct the deficiencies?

- A. Mandatory access controls
- B. Disable remote login
- C. Host hardening
- D. Disabling services

Answer: C

NEW QUESTION 132

- (Exam Topic 2)

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

- A. Removing the hard drive from its enclosure
- B. Using software to repeatedly rewrite over the disk space
- C. Using Blowfish encryption on the hard drives
- D. Using magnetic fields to erase the data

Answer: D

NEW QUESTION 134

- (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 136

- (Exam Topic 2)

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

- A. `nslookup`
`comptia.org`
`set type=ANY`
`ls-d example.org`
- B. `nslookup`
`comptia.org`
`set type=MX`
`example.org`
- C. `dig -axfr comptia.org @example.org`
- D. `ipconfig /flushDNS`
- E. `ifconfig eth0 down`
`ifconfig eth0 up`
`dhclient renew`
- F. `dig @example.org comptia.org`

- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E
- F. Option F

Answer: AC

NEW QUESTION 140

- (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 141

- (Exam Topic 2)

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

- A. Dynamic analysis
- B. Change management
- C. Baselineing
- D. Waterfalling

Answer: B

NEW QUESTION 145

- (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 149

- (Exam Topic 2)

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

- ▶ Match each RAID type with the correct configuration and MINIMUM number of drives.
- ▶ Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements. Instructions:
- ▶ All drive definitions can be dragged as many times as necessary
- ▶ Not all placeholders may be filled in the RAID configuration boxes

▶ If parity is required, please select the appropriate number of parity checkboxes

▶ Server profiles may be dragged only once

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

Instructions: If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit.


Authentication Server


Email Archive


Identity Management Server


Media Streaming Server

Stripe Data

Mirror Data

RAID-0				Server Profile:	RAID-1				Server Profile:
Disk 1	Disk 2	Disk 3	Disk 4	<div style="border: 1px dashed gray; width: 40px; height: 40px; margin: 0 auto;"></div>	Disk 1	Disk 2	Disk 3	Disk 4	<div style="border: 1px dashed gray; width: 40px; height: 40px; margin: 0 auto;"></div>
<input type="checkbox"/>	Parity Data				<input type="checkbox"/>	Parity Data			
<input type="checkbox"/>	Parity Data				<input type="checkbox"/>	Parity Data			
RAID-5				Server Profile:	RAID-6				Server Profile:
Disk 1	Disk 2	Disk 3	Disk 4	<div style="border: 1px dashed gray; width: 40px; height: 40px; margin: 0 auto;"></div>	Disk 1	Disk 2	Disk 3	Disk 4	<div style="border: 1px dashed gray; width: 40px; height: 40px; margin: 0 auto;"></div>
<input type="checkbox"/>	Parity Data				<input type="checkbox"/>	Parity Data			
<input type="checkbox"/>	Parity Data				<input type="checkbox"/>	Parity Data			

Reset All

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

RAID-0 is known as striping. It is not a fault tolerant solution but does improve disk performance for read/write operations. Striping requires a minimum of two disks and does not use parity.

RAID-0 can be used where performance is required over fault tolerance, such as a media streaming server. RAID-1 is known as mirroring because the same data is written to two disks so that the two disks have identical data. This is a fault tolerant solution that halves the storage space. A minimum of two disks are used in mirroring and does not use parity. RAID-1 can be used where fault tolerance is required over performance, such as on an authentication server. RAID-5 is a fault tolerant solution that uses parity and striping. A minimum of three disks are required for RAID-5 with one disk's worth of space being used for parity information. However, the parity information is distributed across all the disks. RAID-5 can recover from a single disk failure.

RAID-6 is a fault tolerant solution that uses dual parity and striping. A minimum of four disks are required for RAID-6. Dual parity allows RAID-6 to recover from the simultaneous failure of up to two disks. Critical data should be stored on a RAID-6 system.

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

NEW QUESTION 151

- (Exam Topic 2)

A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle.

Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle?

- A. Architecture review
- B. Risk assessment
- C. Protocol analysis
- D. Code review

Answer: D

NEW QUESTION 155

- (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 156

- (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 159

- (Exam Topic 2)

A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening. In order to implement a true separation of duties approach the bank could:

- A. Require the use of two different passwords held by two different individuals to open an account
- B. Administer account creation on a role based access control approach
- C. Require all new accounts to be handled by someone else other than a teller since they have different duties
- D. Administer account creation on a rule based access control approach

Answer: C

NEW QUESTION 162

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 167

- (Exam Topic 2)

Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

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

Answer: A

NEW QUESTION 171

- (Exam Topic 2)

An employee receives an email, which appears to be from the Chief Executive Officer (CEO), asking for a report of security credentials for all users.

Which of the following types of attack is MOST likely occurring?

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

Answer: D

NEW QUESTION 174

- (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 179

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 181

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 184

- (Exam Topic 2)

Which of the following cryptographic algorithms is irreversible?

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

Answer: B

NEW QUESTION 186

- (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 187

- (Exam Topic 2)

A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting without the knowledge of the user. Which of the following mobile device capabilities should the user disable to achieve the stated goal?

- A. Device access control
- B. Location based services
- C. Application control
- D. GEO-Tagging

Answer: D

NEW QUESTION 192

- (Exam Topic 2)

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

in this scenario?

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

Answer: A

NEW QUESTION 197

- (Exam Topic 2)

An information security analyst needs to work with an employee who can answer QUESTION NO:s about how data for a specific system is used in the business. The analyst should seek out an employee who has the role of:

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

Answer: B

NEW QUESTION 198

- (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 200

- (Exam Topic 2)

A company's AUP requires:

- ☒ Passwords must meet complexity requirements.
- ☒ Passwords are changed at least once every six months.
- ☒ Passwords must be at least eight characters long.

An auditor is reviewing the following report:

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

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

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

Answer: C

NEW QUESTION 203

- (Exam Topic 2)

A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients. Which of the following is being used?

- A. Gray box vulnerability testing
- B. Passive scan
- C. Credentialed scan

D. Bypassing security controls

Answer: A

NEW QUESTION 205

- (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 210

- (Exam Topic 2)

An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request. Which of the following secure protocols is the developer MOST likely to use?

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

Answer: C

NEW QUESTION 214

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 219

- (Exam Topic 2)

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

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

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

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

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

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

Answer: B

NEW QUESTION 222

- (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 226

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 229

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 230

- (Exam Topic 2)

The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws.

Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

- A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers
- B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location
- C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations
- D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.

Answer: C

NEW QUESTION 233

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 238

- (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 239

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 242

- (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 243

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 244

- (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 249

- (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 254

- (Exam Topic 2)

Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field.

Which of the following has the application programmer failed to implement?

- A. Revision control system
- B. Client side exception handling
- C. Server side validation
- D. Server hardening

Answer: C

NEW QUESTION 255

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 260

- (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 264

- (Exam Topic 3)

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

- A. RSA
- B. TwoFish
- C. Diffie-Helman
- D. NTLMv2
- E. RIPEMD

Answer: B

NEW QUESTION 265

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 269

- (Exam Topic 3)

An organization is moving its human resources system to a cloud services provider.

The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a copy of the passwords. Which of the following options meets all of these requirements?

- A. Two-factor authentication
- B. Account and password synchronization
- C. Smartcards with PINS
- D. Federated authentication

Answer: D

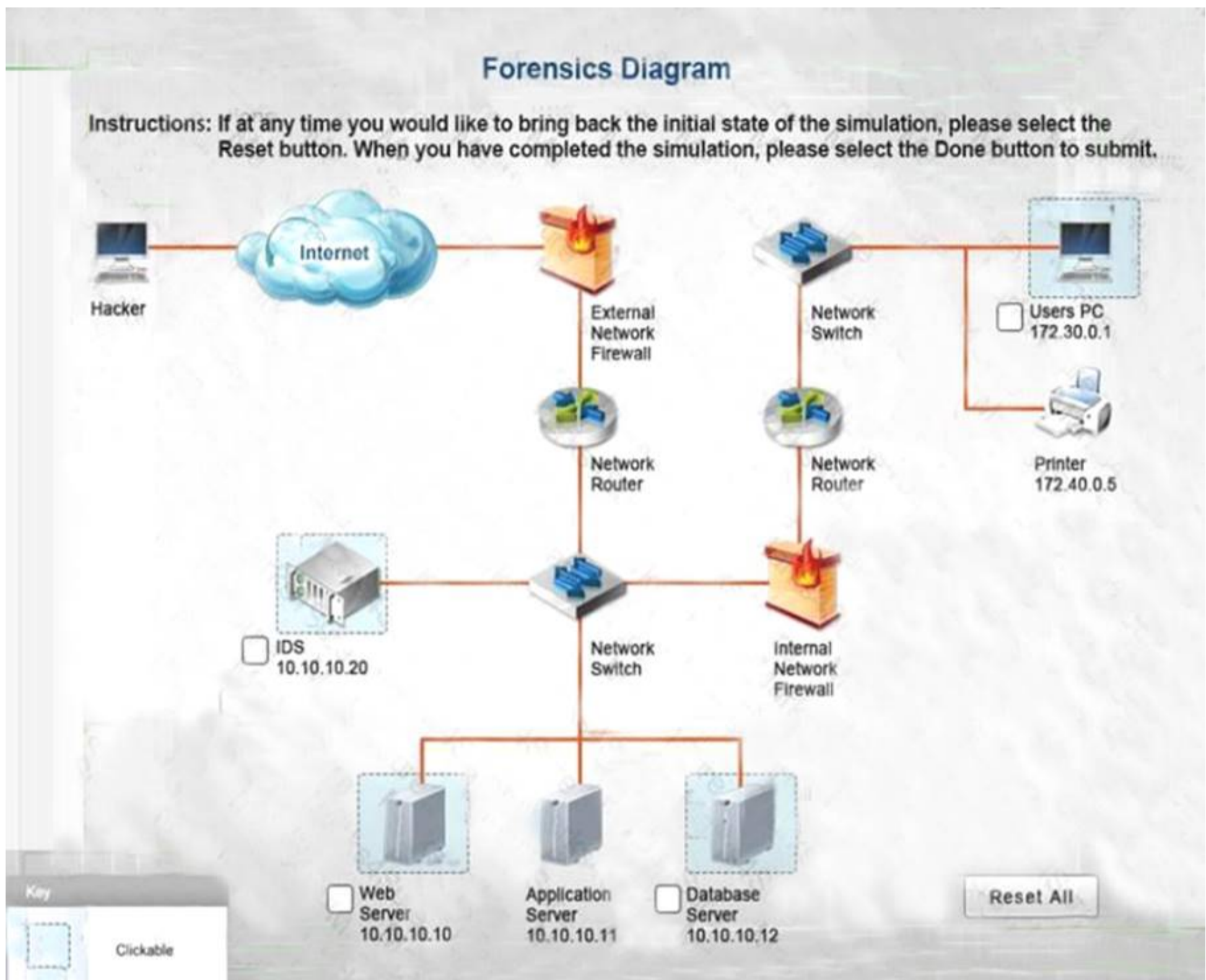
NEW QUESTION 270

- (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.

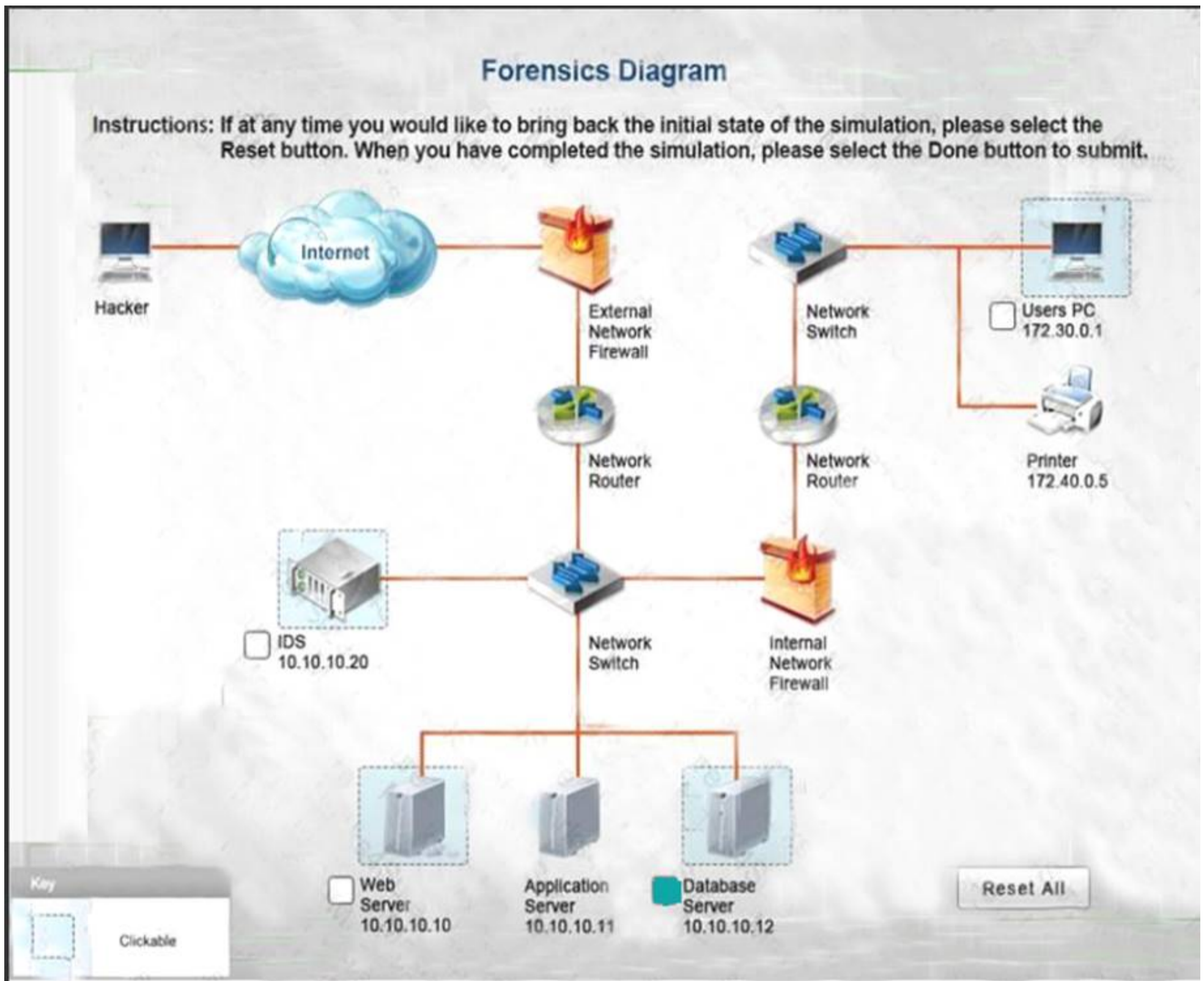


- A. Mastered
- B. Not Mastered

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. It has two tabs: 'Logs' and 'Actions'. The 'Logs' tab is selected, showing a list of log entries. Each entry contains the following information: IP address, timestamp, method, URL, status code, and user agent. The logs are filtered by a date range from 26/4/2010 00:22:49 to 26/4/2010 00:22:58. The entries are as follows:

- 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)"

The 'Actions' tab is also visible but empty. The interface includes a search bar at the top and a status bar at the bottom.

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 274

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 277

- (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 279

- (Exam Topic 3)

A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected. To protect the laptops while connected to untrusted wireless networks, which of the following would be the BEST method for reducing the risk of having the laptops compromised?

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

Answer: C

NEW QUESTION 282

- (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 283

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 287

- (Exam Topic 3)

For each of the given items, select the appropriate authentication category from the drop down choices. Select the appropriate authentication type for the following items:

Item	Response
Fingerprint scan	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
Hardware token	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
Smart card	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
Password	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
PIN number	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
Retina Scan	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Item	Response
Fingerprint scan	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
Hardware token	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
Smart card	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
Password	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
PIN number	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>

Retina Scan



NEW QUESTION 290

- (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 291

- (Exam Topic 3)

A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes.

Which of the following risk management strategies BEST describes management's response?

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

Answer: C

NEW QUESTION 294

- (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 299

- (Exam Topic 3)

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

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

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

Answer: D

NEW QUESTION 303

- (Exam Topic 3)

Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network. This is MOST likely which of the following types of attacks?

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

Answer: A

NEW QUESTION 308

- (Exam Topic 3)

A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet. Which of the following should be used in the code? (Select TWO.)

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

Answer: CE

NEW QUESTION 312

- (Exam Topic 3)

A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange white markings in different areas of the parking lot. The person is attempting which of the following types of attacks?

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

Answer: B

NEW QUESTION 315

- (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 319

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 324

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 325

- (Exam Topic 3)

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

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

Answer: B

Explanation:

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a

vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

NEW QUESTION 328

- (Exam Topic 3)

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

- A. Account logout
- B. Group Based Privileges
- C. Least privilege
- D. Password complexity

Answer: A

NEW QUESTION 332

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 336

- (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 341

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 346

- (Exam Topic 3)

An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient.

Which of the following capabilities would be MOST appropriate to consider implementing in response to the new requirement?

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

Answer: D

NEW QUESTION 350

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 353

- (Exam Topic 3)

A security administrator is developing training for corporate users on basic security principles for personal email accounts. Which of the following should be mentioned as the MOST secure way for password recovery?

- A. Utilizing a single Qfor password recovery
- B. Sending a PIN to a smartphone through text message
- C. Utilizing CAPTCHA to avoid brute force attacks
- D. Use a different e-mail address to recover password

Answer: B

NEW QUESTION 355

- (Exam Topic 3)

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

1	<input type="text"/>	RAM
2	<input type="text"/>	CPU cache
3	<input type="text"/>	Swap
4	<input type="text"/>	Hard drive

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

NEW QUESTION 357

- (Exam Topic 3)

A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability. In order to prevent similar situations in the future, the company should improve which of the following?

- A. Change management procedures
- B. Job rotation policies
- C. Incident response management
- D. Least privilege access controls

Answer: A

NEW QUESTION 359

- (Exam Topic 3)

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

- A. Upgrade the encryption to WPA or WPA2
- B. Create a non-zero length SSID for the wireless router

- C. Reroute wireless users to a honeypot
- D. Disable responses to a broadcast probe request

Answer: D

NEW QUESTION 360

- (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 364

- (Exam Topic 3)

A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols. Which of the following summarizes the BEST response to the programmer's proposal?

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

Answer: B

NEW QUESTION 367

- (Exam Topic 3)

Drag and drop the correct protocol to its default port.

FTP	<input type="text"/>	161
Telnet	<input type="text"/>	22
SMTP	<input type="text"/>	21
SNMP	<input type="text"/>	69
SCP	<input type="text"/>	25
TFTP	<input type="text"/>	23

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

FTP uses TCP port 21. Telnet uses port 23. SSH uses TCP port 22.

All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). SMTP uses TCP port 25. Port 69 is used by TFTP.

SNMP makes use of UDP ports 161 and 162. http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION 368

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 369

- (Exam Topic 3)

Which of the following are MOST susceptible to birthday attacks?

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

Answer: A

NEW QUESTION 374

- (Exam Topic 3)

A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion. Which of the following technologies would BEST be suited to accomplish this?

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

Answer: D

Explanation:

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

NEW QUESTION 376

- (Exam Topic 4)

An incident involving a workstation that is potentially infected with a virus has occurred. The workstation may have sent confidential data to an unknown internet server. Which of the following should a security analyst do FIRST?

- A. Make a copy of everything in memory on the workstation.
- B. Turn off the workstation.
- C. Consult information security policy.
- D. Run a virus scan.

Answer: A

NEW QUESTION 380

- (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 381

- (Exam Topic 4)

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

- A. arp - s 192.168.1.1 00-3a-d1-fa-b1-06

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

Answer: A

NEW QUESTION 383

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 388

- (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 390

- (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 391

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 394

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 395

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 396

- (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 399

- (Exam Topic 4)

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

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

Answer: BD

NEW QUESTION 401

- (Exam Topic 4)

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

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

Answer: AE

NEW QUESTION 403

- (Exam Topic 4)

A network technician is trying to determine the source of an ongoing network based attack. Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?

- A. Proxy
- B. Protocol analyzer
- C. Switch
- D. Firewall

Answer: B

NEW QUESTION 405

- (Exam Topic 4)

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

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

Answer: E

NEW QUESTION 410

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 415

- (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 419

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 421

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 426

- (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 429

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 431

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 432

- (Exam Topic 4)

An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography. Discovery of which of the following would help catch the tester in the act?

- A. Abnormally high numbers of outgoing instant messages that contain obfuscated text

- B. Large-capacity USB drives on the tester's desk with encrypted zip files
- C. Outgoing emails containing unusually large image files
- D. Unusual SFTP connections to a consumer IP address

Answer: C

NEW QUESTION 437

- (Exam Topic 4)

A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network. The access the server using RDP on a port other than the typical registered port for the RDP protocol?

- A. TLS
- B. MPLS
- C. SCP
- D. SSH

Answer: A

NEW QUESTION 439

- (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 443

- (Exam Topic 4)

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

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

Answer: DE

NEW QUESTION 444

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 446

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 447

- (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 448

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 449

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 453

- (Exam Topic 4)

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

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

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

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

Answer: B

NEW QUESTION 455

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 460

- (Exam Topic 4)

A wireless network has the following design requirements:

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



It must not depend on user certificates

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

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

Answer: BE

NEW QUESTION 465

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 466

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 468

- (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 469

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 472

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 473

- (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 474

- (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 477

- (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 480

- (Exam Topic 4)

A security administrator is reviewing the following network capture:

```
192.168.20.43:2043 -> 10.234.66.21:80  
POST "192.168.20.43 https://www.banksite.com<ENTER>JoeUsr<BackSPACE>erPassword<ENTER>"
```

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

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

Answer: A

NEW QUESTION 483

- (Exam Topic 4)

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

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

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

A

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

B

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

C

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

D

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

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

Answer: A**NEW QUESTION 484**

- (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 487**

- (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 490**

- (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 494**

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 498

- (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 499

- (Exam Topic 5)

A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it. The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer contact information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls. Which of the following will be the MOST efficient security control to implement to lower this risk?

- A. Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact information.
- B. Restrict screen capture features on the devices when using the custom application and the contact information.
- C. Restrict contact information storage dataflow so it is only shared with the customer application.
- D. Require complex passwords for authentication when accessing the contact information.

Answer: C

NEW QUESTION 504

- (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 505

- (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 509

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 512

- (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 514

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 517

- (Exam Topic 5)

A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks. Which of the following should the CSO conduct FIRST?

- A. Survey threat feeds from services inside the same industry.
- B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic
- C. Conduct an internal audit against industry best practices to perform a qualitative analysis.
- D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor.

Answer: A

NEW QUESTION 522

- (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 526

- (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 527

- (Exam Topic 5)

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

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

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

D. Configure a captive portal for guest and WPA2 Enterprise for staff

Answer: D

NEW QUESTION 530

- (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 534

- (Exam Topic 5)

A security analyst is attempting to identify vulnerabilities in a customer's web application without impacting the system or its data. Which of the following BEST describes the vulnerability scanning concept performed?

- A. Aggressive scan
- B. Passive scan
- C. Non-credentialed scan
- D. Compliance scan

Answer: B

Explanation:

Passive scanning is a method of vulnerability detection that relies on information gleaned from network data that is captured from a target computer without direct interaction.

Packet sniffing applications can be used for passive scanning to reveal information such as operating system, known protocols running on non-standard ports and active network applications with known bugs. Passive scanning may be conducted by a network administrator scanning for security vulnerabilities or by an intruder as a preliminary to an active attack.

For an intruder, passive scanning's main advantage is that it does not leave a trail that could alert users or administrators to their activities. For an administrator, the main advantage is that it doesn't risk causing undesired behavior on the target computer, such as freezes. Because of these advantages, passive scanning need not be limited to a narrow time frame to minimize risk or disruption, which means that it is likely to return more information.

Passive scanning does have limitations. It is not as complete in detail as active vulnerability scanning and cannot detect any applications that are not currently sending out traffic; nor can it distinguish false information put out for obfuscation.

NEW QUESTION 537

- (Exam Topic 5)

A security analyst is inspecting the results of a recent internal vulnerability scan that was performed against intranet services. The scan reports include the following critical-rated vulnerability:

Title: Remote Command Execution vulnerability in web server Rating: Critical (CVSS 10.0) Threat actor: any remote user of the web server

Confidence: certain

Recommendation: apply vendor patches

Which of the following actions should the security analyst perform FIRST?

- A. Escalate the issue to senior management.
- B. Apply organizational context to the risk rating.
- C. Organize for urgent out-of-cycle patching.
- D. Exploit the server to check whether it is a false positive.

Answer: B

NEW QUESTION 541

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 543

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 547

- (Exam Topic 5)

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

- A. Faraday cage
- B. Air gap
- C. Mantrap
- D. Bollards

Answer: C

NEW QUESTION 548

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 549

- (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 551

- (Exam Topic 5)

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

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

Answer: AB

NEW QUESTION 554

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 559

- (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 564

- (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 568

- (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 569

- (Exam Topic 5)

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

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

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

Answer: B

NEW QUESTION 572

- (Exam Topic 5)

An external auditor visits the human resources department and performs a physical security assessment. The auditor observed documents on printers that are unclaimed. A closer look at these documents reveals employee names, addresses, ages, and types of medical and dental coverage options each employee has selected. Which of the following is the MOST appropriate actions to take?

- A. Flip the documents face down so no one knows these documents are PII sensitive
- B. Shred the documents and let the owner print the new set
- C. Retrieve the documents, label them with a PII cover sheet, and return them to the printer
- D. Report to the human resources manager that their personnel are violating a privacy policy

Answer: D

NEW QUESTION 576

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 579

- (Exam Topic 5)

An organization has several production-critical SCADA supervisory systems that cannot follow the normal 30-day patching policy. Which of the following BEST maximizes the protection of these systems from malicious software?

- A. Configure a firewall with deep packet inspection that restricts traffic to the systems.
- B. Configure a separate zone for the systems and restrict access to known ports.
- C. Configure the systems to ensure only necessary applications are able to run.
- D. Configure the host firewall to ensure only the necessary applications have listening ports

Answer: A

NEW QUESTION 582

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 583

- (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 584

- (Exam Topic 5)

Which of the following threats has sufficient knowledge to cause the MOST danger to an organization?

- A. Competitors
- B. Insiders
- C. Hacktivists
- D. Script kiddies

Answer: B

NEW QUESTION 587

- (Exam Topic 5)

A systems administrator wants to generate a self-signed certificate for an internal website. Which of the following steps should the systems administrator complete prior to installing the certificate on the server?

- A. Provide the private key to a public CA.
- B. Provide the public key to the internal CA.
- C. Provide the public key to a public CA.
- D. Provide the private key to the internal CA.
- E. Provide the public/private key pair to the internal CA
- F. Provide the public/private key pair to a public CA.

Answer: D

NEW QUESTION 589

- (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 592

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 593

- (Exam Topic 5)

A company offers SaaS, maintaining all customers' credentials and authenticating locally. Many large customers have requested the company offer some form of federation with their existing authentication infrastructures. Which of the following would allow customers to manage authentication and authorizations from within their existing organizations?

- A. Implement SAML so the company's services may accept assertions from the customers' authentication servers.
- B. Provide customers with a constrained interface to manage only their users' accounts in the company's active directory server.

- C. Provide a system for customers to replicate their users' passwords from their authentication service to the company's.
- D. Use SOAP calls to support authentication between the company's product and the customers' authentication servers.

Answer: A

NEW QUESTION 595

- (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 600

- (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 603

- (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 604

- (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 605

- (Exam Topic 5)

Ann is the IS manager for several new systems in which the classification of the systems' data are being decided. She is trying to determine the sensitivity level of the data being processed. Which of the following people should she consult to determine the data classification?

- A. Steward
- B. Custodian
- C. User
- D. Owner

Answer: D

NEW QUESTION 608

- (Exam Topic 5)

A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection. Which of the following is the NEXT step the team should take?

- A. Identify the source of the active connection
- B. Perform eradication of active connection and recover
- C. Performance containment procedure by disconnecting the server
- D. Format the server and restore its initial configuration

Answer: A

NEW QUESTION 613

- (Exam Topic 5)

A systems administrator wants to implement a wireless protocol that will allow the organization to authenticate mobile devices prior to providing the user with a captive portal login. Which of the following should the systems administrator configure?

- A. L2TP with MAC filtering
- B. EAP-TTLS
- C. WPA2-CCMP with PSK
- D. RADIUS federation

Answer: D

Explanation:

RADIUS generally includes 802.1X that pre-authenticates devices.

NEW QUESTION 616

- (Exam Topic 5)

A security analyst conducts a manual scan on a known hardened host that identifies many non-compliant items. Which of the following BEST describe why this has occurred? (Select TWO)

- A. Privileged-user certificated were used to scan the host
- B. Non-applicable plugins were selected in the scan policy
- C. The incorrect audit file was used
- D. The output of the report contains false positives
- E. The target host has been compromised

Answer: BD

NEW QUESTION 620

- (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 625

- (Exam Topic 5)

A new security administrator ran a vulnerability scanner for the first time and caused a system outage. Which of the following types of scans MOST likely caused the outage?

- A. Non-intrusive credentialed scan
- B. Non-intrusive non-credentialed scan
- C. Intrusive credentialed scan
- D. Intrusive non-credentialed scan

Answer: D

NEW QUESTION 627

- (Exam Topic 5)

During a routine vulnerability assessment, the following command was successful:

echo "vrfy 'perl -e 'print "hi" x 500 ' ' ' | nc www.company.com 25 Which of the following vulnerabilities is being exploited?

- A. Buffer overflow directed at a specific host MTA
- B. SQL injection directed at a web server
- C. Cross-site scripting directed at www.company.com
- D. Race condition in a UNIX shell script

Answer: A

NEW QUESTION 628

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 629

- (Exam Topic 5)

An active/passive configuration has an impact on:

- A. confidentiality
- B. integrity
- C. availability
- D. non-repudiation

Answer: C

NEW QUESTION 630

- (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 632

- (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 637

- (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 638

- (Exam Topic 5)

Joe, a salesman, was assigned to a new project that requires him to travel to a client site. While waiting for a flight, Joe, decides to connect to the airport wireless network without connecting to a VPN, and he sends confidential emails to fellow colleagues. A few days later, the company experiences a data breach. Upon investigation, the company learns Joe's emails were intercepted. Which of the following MOST likely caused the data breach?

- A. Policy violation
- B. Social engineering
- C. Insider threat
- D. Zero-day attack

Answer: A

NEW QUESTION 643

- (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 646

- (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 650

.....

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>