

## 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)

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

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




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

**Answer:** C

**NEW QUESTION 3**

- (Exam Topic 1)

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

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

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

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

**Answer:** B

**NEW QUESTION 4**

- (Exam Topic 1)

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

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

**Answer:** A

**NEW QUESTION 5**

- (Exam Topic 1)

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

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

**Answer:** C

**NEW QUESTION 6**

- (Exam Topic 1)

Which of the following would a security specialist be able to determine upon examination of a server's certificate?

- A. CA public key
- B. Server private key
- C. CSR
- D. OID

**Answer:** D

**NEW QUESTION 7**

- (Exam Topic 1)

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)

A security administrator has found a hash in the environment known to belong to malware. The administrator then finds this file to be in 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	01ab28bbde63aa879b35bba62cdes283
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 9**

- (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 10**

- (Exam Topic 1)

Which of the following network vulnerability scan indicators BEST validates a successful, active scan?


- A. The scan job is scheduled to run during off-peak hours.
- B. The scan output lists SQL injection attack vectors.
- C. The scan data identifies the use of privileged-user credentials.
- D. The scan results identify the hostname and IP address.

**Answer:** D


**NEW QUESTION 13**

- (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 17

- (Exam Topic 1)

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

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

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

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

**Answer: ACG**

#### NEW QUESTION 20

- (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 22

- (Exam Topic 1)

A high-security defense installation recently begun utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation. Which of the following types of controls does this BEST describe?

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

**Answer: A**

#### NEW QUESTION 27

- (Exam Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 29

- (Exam Topic 1)

An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

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

D. MTTR

**Answer:** A

#### NEW QUESTION 32

- (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 37

- (Exam Topic 1)

A system 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:** C

#### NEW QUESTION 39

- (Exam Topic 1)

Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?

- A. Shibboleth
- B. RADIUS federation
- C. SAML
- D. OAuth
- E. OpenID connect

**Answer:** B

#### Explanation:





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

#### NEW QUESTION 40

- (Exam Topic 1)

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

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

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

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



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

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

**Answer: A**

#### NEW QUESTION 41

- (Exam Topic 1)

A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset types?

Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.

The screenshot shows a security simulation interface. On the left, there is a list of controls under the heading "Controls":

- Screen Lock
- Strong Password
- Device Encryption
- Remote Wipe
- GPS Tracking
- Pop-up blocker
- Cable Locks
- Antivirus
- Host Based Firewall
- Proximity Reader
- Sniffer
- Mantrap

On the right, there are two asset types with placeholder boxes for controls:

- Company Managed Smart Phone** (represented by a smartphone icon)
- Data Center Terminal Server** (represented by a server rack icon)

At the bottom center, there is a "Reset All" button. At the bottom right, there is a "Done" button and a text box that says "This window can be resized."

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 43**

- (Exam Topic 1)

When trying to log onto a company's new ticketing system, some employees receive the following message: Access denied: too many concurrent sessions. The ticketing system was recently installed on a small VM with only the recommended hardware specifications. Which of the following is the MOST likely cause for this error message?

- A. Network resources have been exceeded.
- B. The software is out of licenses.
- C. The VM does not have enough processing power.
- D. The firewall is misconfigured.

**Answer:** C

**NEW QUESTION 46**

- (Exam Topic 1)

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

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

Which of the following commands should be used?

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

**Answer:** A

**NEW QUESTION 50**

- (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 51**

- (Exam Topic 1)

An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call.

The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

- A. Give the application team administrator access during off-hours.
- B. Disable other critical applications before granting the team access.
- C. Give the application team read-only access.
- D. Share the account with the application team.

**Answer:** C

**NEW QUESTION 53**

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 56

- (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 58

- (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 63

- (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 66

- (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 71

- (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 75

- (Exam Topic 1)

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

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



D. Something you are.

**Answer:** A

#### NEW QUESTION 79

- (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 80

- (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 81

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 83

- (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 87

- (Exam Topic 1)

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

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

**Answer:** C

**NEW QUESTION 92**

- (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 95**

- (Exam Topic 2)

Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

- A. Encrypt it with Joe's private key
- B. Encrypt it with Joe's public key
- C. Encrypt it with Ann's private key
- D. Encrypt it with Ann's public key

**Answer:** D

**NEW QUESTION 98**

- (Exam Topic 2)

A technician suspects that a system has been compromised. The technician reviews the following log entry: WARNING- hash mismatch:

C:\Window\SysWOW64\user32.dll

WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll

Based solely on the above information, which of the following types of malware is MOST likely installed on the system?

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

**Answer:** A

**NEW QUESTION 101**

- (Exam Topic 2)

During a monthly vulnerability scan, a server was flagged for being vulnerable to an Apache Struts exploit. Upon further investigation, the developer responsible for the server informs the security team that Apache Struts is not installed on the server. Which of the following BEST describes how the security team should reach to this incident?

- A. The finding is a false positive and can be disregarded
- B. The Struts module needs to be hardened on the server
- C. The Apache software on the server needs to be patched and updated
- D. The server has been compromised by malware and needs to be quarantined.

**Answer:** A

**NEW QUESTION 104**

- (Exam Topic 2)

An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware, the attacker is provided with access to the infected machine.

Which of the following is being described?

- A. Zero-day exploit
- B. Remote code execution
- C. Session hijacking
- D. Command injection

**Answer:** A

**NEW QUESTION 108**

- (Exam Topic 2)

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

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

E. Routers

**Answer:** AB

**NEW QUESTION 110**

- (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 111**

- (Exam Topic 2)

Which of the following precautions MINIMIZES the risk from network attacks directed at multifunction printers, as well as the impact on functionality at the same time?

- A. Isolating the systems using VLANs
- B. Installing a software-based IPS on all devices
- C. Enabling full disk encryption
- D. Implementing a unique user PIN access functions

**Answer:** A

**NEW QUESTION 112**

- (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 114**

- (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 119**

- (Exam Topic 2)

Which of the following cryptographic algorithms is irreversible?

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

**Answer:** B

**NEW QUESTION 122**

- (Exam Topic 2)

A manager suspects that an IT employee with elevated database access may be knowingly modifying financial transactions for the benefit of a competitor. Which of the following practices should the manager implement to validate the concern?

- A. Separation of duties
- B. Mandatory vacations
- C. Background checks
- D. Security awareness training

**Answer:** A

**NEW QUESTION 126**

- (Exam Topic 2)

A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts.

Which of the following subnets would BEST meet the requirements?

- A. 192.168.0.16 255.25.255.248
- B. 192.168.0.16/28
- C. 192.168.1.50 255.255.25.240
- D. 192.168.2.32/27

**Answer: B**

#### NEW QUESTION 130

- (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 133

- (Exam Topic 2)

Which of the following would meet the requirements for multifactor authentication?

- A. Username, PIN, and employee ID number
- B. Fingerprint and password
- C. Smart card and hardware token
- D. Voice recognition and retina scan

**Answer: B**

#### NEW QUESTION 135

- (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 138

- (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 139

- (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 141

- (Exam Topic 2)

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

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

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

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

**Answer:** B

#### NEW QUESTION 144

- (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 147

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 152

- (Exam Topic 2)

A penetration tester finds that a company's login credentials for the email client were being sent in clear text. Which of the following should be done to provide encrypted logins to the email server?

- A. Enable IPSec and configure SMTP.
- B. Enable SSH and LDAP credentials.
- C. Enable MIME services and POP3.
- D. Enable an SSL certificate for IMAP services.

**Answer:** D

#### NEW QUESTION 153

- (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 154

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 158

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 159

- (Exam Topic 2)

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

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

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

**Answer: B**

#### NEW QUESTION 162

- (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 166

- (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 170

- (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 171

- (Exam Topic 2)

A portable data storage device has been determined to have malicious firmware. Which of the following is the BEST course of action to ensure data confidentiality?

- A. Format the device
- B. Re-image the device
- C. Perform virus scan in the device
- D. Physically destroy the device

**Answer:** C

#### NEW QUESTION 176

- (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 180

- (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 183

- (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 188

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 192

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 194**

- (Exam Topic 3)

The chief security officer (CSO) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs. Which of the following is the best solution for the network administrator to secure each internal website?

- A. Use certificates signed by the company CA
- B. Use a signing certificate as a wild card certificate
- C. Use certificates signed by a public ca
- D. Use a self-signed certificate on each internal server

**Answer:** D

**Explanation:**

This is a way to update all internal sites without incurring additional costs?

To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

**NEW QUESTION 198**

- (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 201**

- (Exam Topic 3)

A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

- A. Performance and service delivery metrics
- B. Backups are being performed and tested
- C. Data ownership is being maintained and audited
- D. Risk awareness is being adhered to and enforced

**Answer:** A

**NEW QUESTION 205**

- (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 208

- (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 213

- (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 217

- (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. Main-in-the-middle
- C. URL hijacking
- D. Transitive access

**Answer:** B

### NEW QUESTION 220

- (Exam Topic 3)

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

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

**Answer:** B

### NEW QUESTION 223

- (Exam Topic 3)

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

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

**Answer:** D

### NEW QUESTION 226

- (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 231

- (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 235

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 238

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 243

- (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 246

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 251

- (Exam Topic 3)

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



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

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 255**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 258**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 260**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 263**

- (Exam Topic 3)

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

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 264**

- (Exam Topic 3)

Which of the following use the SSH protocol?

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

F. SFTP

**Answer:** BF

**NEW QUESTION 268**

- (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 273**

- (Exam Topic 3)

A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN. Which of the following protocols should be used?

- A. RADIUS
- B. Kerberos
- C. LDAP
- D. MSCHAP

**Answer:** A

**NEW QUESTION 276**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 281**

- (Exam Topic 3)

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

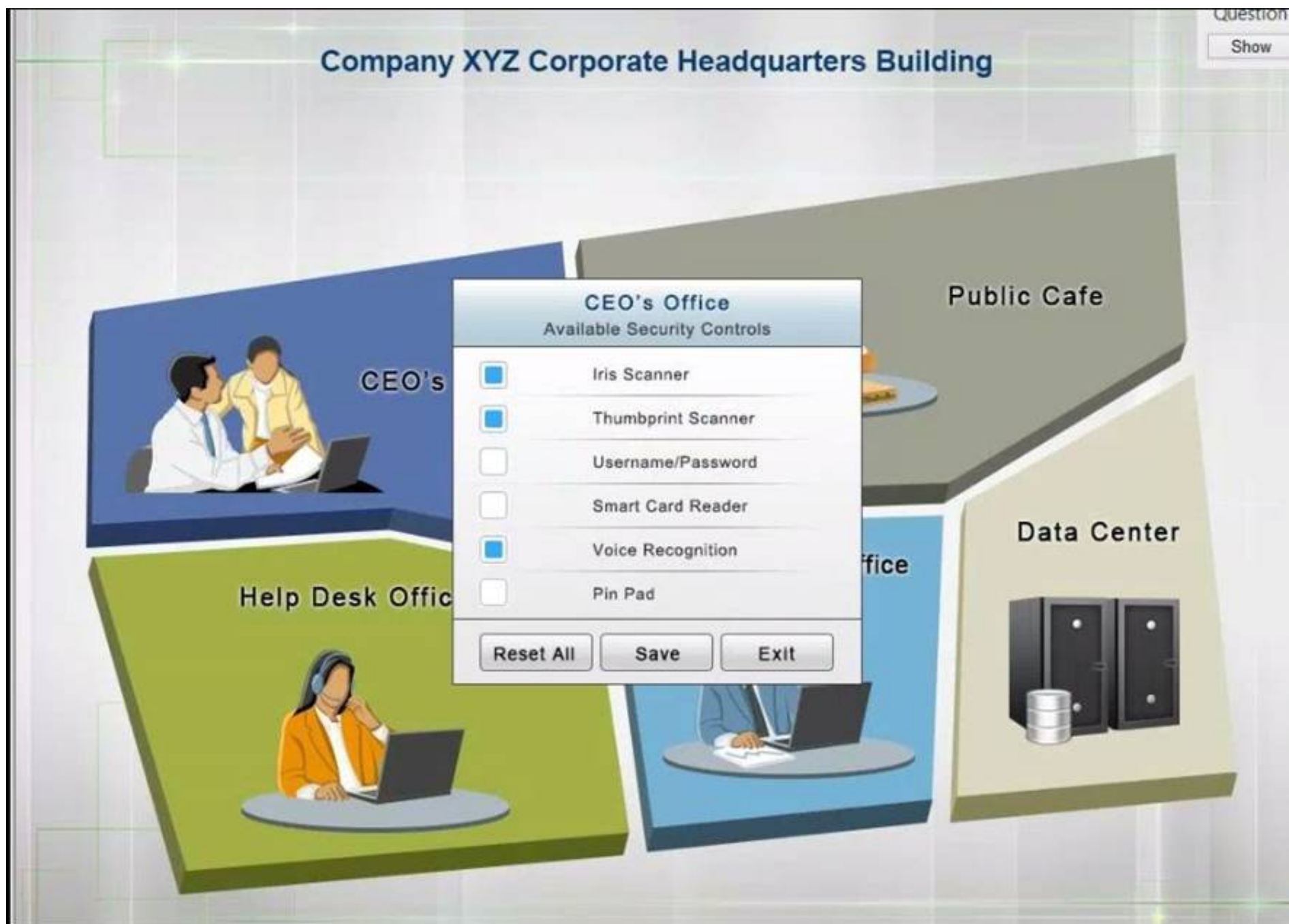
The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris reader.

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

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

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

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



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



**Public Cafe**  
Available Security Controls

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

Reset AllSaveExit

**Help Desk**  
Available Security Controls

<input type="checkbox"/>	Iris Scanner
<input type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Password
<input checked="" type="checkbox"/>	Proximity Badge
<input type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

Reset AllSaveExit

**Data Center**  
Available Security Controls

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

Reset AllSaveExit



**CEO's Office**  
**Available Security Controls**

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Solution as

**PII Processing Office**  
**Available Security Controls**

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

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



**Public Cafe**  
**Available Security Controls**

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

**Data Center**  
**Available Security Controls**

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

**CEO's Office**  
**Available Security Controls**

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

**NEW QUESTION 284**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 289**

- (Exam Topic 3)

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

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

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

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

**Answer:** D

**NEW QUESTION 290**

- (Exam Topic 3)

ACHief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net). Which of the following rules is preventing the CSO from accessing the site?

Blocked sites: \*.nonews.com, \*.rumorhasit.net, \*.mars?

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

**Answer:** C

**NEW QUESTION 294**

- (Exam Topic 3)

Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

- A. Calculate the ALE
- B. Calculate the ARO
- C. Calculate the MTBF
- D. Calculate the TCO

**Answer:** A

**NEW QUESTION 299**

- (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 300**

- (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 302**

- (Exam Topic 3)

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

- A. Deterrent

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

**Answer:** A

#### **NEW QUESTION 304**

- (Exam Topic 4)

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

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

**Answer:** B

#### **NEW QUESTION 307**

- (Exam Topic 4)

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

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

**Answer:** BC

#### **NEW QUESTION 310**

- (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 314**

- (Exam Topic 4)

A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided from the role-based authentication system in use by the company. The situation can be identified for future mitigation as which of the following?

- A. Job rotation
- B. Log failure
- C. Lack of training
- D. Insider threat

**Answer:** B

#### **NEW QUESTION 315**

- (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 318**

- (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 323**

- (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 325**

- (Exam Topic 4)

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

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

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

**Answer:** C

**NEW QUESTION 328**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 331**

- (Exam Topic 4)

The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems.

The help desk is receive reports that users are experiencing the following error when attempting to log in to their previous system:

Logon Failure: Access Denied

Which of the following can cause this issue?

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

**Answer:** C

**NEW QUESTION 334**

- (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 337**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 340**

- (Exam Topic 4)



A security administrator needs to address the following audit recommendations for a public-facing SFTP server:  
Users should be restricted to upload and download files to their own home directories only. Users should not be allowed to use interactive shell login.  
Which of the following configuration parameters should be implemented? (Select TWO).

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

**Answer:** BC

#### NEW QUESTION 344

- (Exam Topic 4)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 348

- (Exam Topic 4)

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

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

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

**Answer:** D

#### NEW QUESTION 352

- (Exam Topic 4)

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

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

**Answer:** AD

#### NEW QUESTION 356

- (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 357

- (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 362

- (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 364

- (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 14:01.10 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: cli administrator has been given the following
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]

Workstation host firewall log:
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-23 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp) (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
```

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

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

**Answer:** B

#### NEW QUESTION 368

- (Exam Topic 4)

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

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

**Answer:** D

#### NEW QUESTION 373

- (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 377

- (Exam Topic 4)

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

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

**Answer:** AE

#### NEW QUESTION 381

- (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 382

- (Exam Topic 4)

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

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

**Answer:** EF

#### Explanation:

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

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

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

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

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

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

#### NEW QUESTION 387

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 391

- (Exam Topic 4)

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

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

**Answer:** BD

#### NEW QUESTION 396

- (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 400

- (Exam Topic 4)

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

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

**Answer:** BD

#### NEW QUESTION 401

- (Exam Topic 4)

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

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

**Answer:** D

#### NEW QUESTION 404

- (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 406

- (Exam Topic 4)

A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network. Which of the following is the MOST likely method used to gain access to the other host?

- A. Backdoor
- B. Pivoting
- C. Persistence
- D. Logic bomb

**Answer:** B

#### NEW QUESTION 409

- (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 411**

- (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 414**

- (Exam Topic 5)

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

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

**Answer:** A**NEW QUESTION 419**

- (Exam Topic 5)

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

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

**Answer:** C**NEW QUESTION 422**

- (Exam Topic 5)



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

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

**Answer:** D

#### NEW QUESTION 425

- (Exam Topic 5)

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

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

**Answer:** BE

#### NEW QUESTION 427

- (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 428

- (Exam Topic 5)

A Chief Information Officer (CIO) asks the company's security specialist if the company should spend any funds on malware protection for a specific server. Based on a risk assessment, the ARO value of a malware infection for a server is 5 and the annual cost for the malware protection is \$2500. Which of the following SLE values warrants a recommendation against purchasing the malware protection?

- A. \$500
- B. \$1000
- C. \$2000
- D. \$2500

**Answer:** A

#### NEW QUESTION 432

- (Exam Topic 5)

A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production. Which of the following development methodologies is the team MOST likely using now?

- A. Agile
- B. Waterfall
- C. Scrum
- D. Spiral

**Answer:** B

#### NEW QUESTION 433

- (Exam Topic 5)

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

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

**Answer:** D

#### NEW QUESTION 435

- (Exam Topic 5)

A hacker has a packet capture that contains:

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

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

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

**Answer:** A

#### NEW QUESTION 437

- (Exam Topic 5)

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

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

**Answer:** C

#### NEW QUESTION 441

- (Exam Topic 5)

A security analyst is reviewing patches on servers. One of the servers is reporting the following error message in the WSUS management console:  
The computer has not reported status in 30 days.

Given this scenario, which of the following statements BEST represents the issue with the output above?

- A. The computer in QUESTION NO: has not pulled the latest ACL policies for the firewall.
- B. The computer in QUESTION NO: has not pulled the latest GPO policies from the management server.
- C. The computer in QUESTION NO: has not pulled the latest antivirus definitions from the antivirus program.
- D. The computer in QUESTION NO: has not pulled the latest application software updates.

**Answer:** D

#### NEW QUESTION 445

- (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 449

- (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 451

- (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 453

- (Exam Topic 5)

An organization has implemented an IPSec VPN access for remote users. Which of the following IPSec modes would be the MOST secure for this organization to

implement?

- A. Tunnel mode
- B. Transport mode
- C. AH-only mode
- D. ESP-only mode

**Answer:** A

**Explanation:**

In both ESP and AH cases with IPSec Transport mode, the IP header is exposed. The IP header is not exposed in IPSec Tunnel mode.

**NEW QUESTION 458**

- (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 459**

- (Exam Topic 5)

A company has two wireless networks utilizing captive portals. Some employees report getting a trust error in their browsers when connecting to one of the networks. Both captive portals are using the same server certificate for authentication, but the analyst notices the following differences between the two certificate details:

Certificate 1

Certificate Path: Geotrust Global CA

\*company.com Certificate 2 Certificate Path:

\*company.com

Which of the following would resolve the problem?

- A. Use a wildcard certificate.
- B. Use certificate chaining.
- C. Use a trust model.
- D. Use an extended validation certificate.

**Answer:** B

**NEW QUESTION 460**

- (Exam Topic 5)

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

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

**Answer:** B

**NEW QUESTION 464**

- (Exam Topic 5)

A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials. Which of the following account types is the systems administrator using?

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

**Answer:** C

**NEW QUESTION 468**

- (Exam Topic 5)

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

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

D. Behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed

**Answer:** D

#### NEW QUESTION 469

- (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 470

- (Exam Topic 5)

An external attacker can modify the ARP cache of an internal computer. Which of the following types of attacks is described?

- A. Replay
- B. Spoofing
- C. DNS poisoning
- D. Client-side attack

**Answer:** B

#### NEW QUESTION 471

- (Exam Topic 5)

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

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

**Answer:** A

#### NEW QUESTION 474

- (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 478

- (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 480

- (Exam Topic 5)

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

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

**Answer:** B

#### NEW QUESTION 485

- (Exam Topic 5)

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

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

**Answer:** D

#### NEW QUESTION 489

- (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 492

- (Exam Topic 5)

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

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







**Answer:** C

#### NEW QUESTION 495

- (Exam Topic 5)

A security analyst is securing smartphones and laptops for a highly mobile workforce.

Priorities include:

-  Remote wipe capabilities
-  Geolocation services
-  Patch management and reporting
-  Mandatory screen locks
-  Ability to require passcodes and pins
-  Ability to require encryption

Which of the following would BEST meet these requirements?

- A. Implementing MDM software
- B. Deploying relevant group policies to the devices
- C. Installing full device encryption
- D. Removing administrative rights to the devices

**Answer:** A

#### NEW QUESTION 498

- (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 502

- (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 503

- (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 504

- (Exam Topic 5)

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

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

**Answer:** D

#### NEW QUESTION 509

- (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 510

- (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 514

- (Exam Topic 5)

A user receives an email from ISP indicating malicious traffic coming from the user's home network is detected. The traffic appears to be Linux-based, and it is targeting a website that was recently featured on the news as being taken offline by an Internet attack. The only Linux device on the network is a home surveillance camera system.

Which of the following BEST describes what is happening?

- A. The camera system is infected with a bot.
- B. The camera system is infected with a RAT.
- C. The camera system is infected with a Trojan.
- D. The camera system is infected with a backdoor.

**Answer:** A

#### NEW QUESTION 518

- (Exam Topic 5)

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

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

**Answer:** B

**NEW QUESTION 522**

- (Exam Topic 5)

An organization wants to upgrade its enterprise-wide desktop computer solution. The organization currently has 500 PCs active on the network. the Chief Information Security Officer (CISO) suggests that the organization employ desktop imaging technology for such a large scale upgrade. Which of the following is a security benefit of implementing an imaging solution?

- A. it allows for faster deployment
- B. it provides a consistent baseline
- C. It reduces the number of vulnerabilities
- D. It decreases the boot time

**Answer: B**

**NEW QUESTION 527**

- (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 529**

- (Exam Topic 5)

A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized. Which of the following solutions would BEST meet these requirements?

- A. Multifactor authentication
- B. SSO
- C. Biometrics
- D. PKI
- E. Federation

**Answer: B**

**NEW QUESTION 530**

- (Exam Topic 5)

A forensic expert is given a hard drive from a crime scene and is asked to perform an investigation. Which of the following is the FIRST step the forensic expert needs to take the chain of custody?

- A. Make a forensic copy
- B. Create a hash of the hard rive
- C. Recover the hard drive data
- D. Update the evidence log

**Answer: D**

**NEW QUESTION 533**

- (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. tracert
- B. Fuzzer
- C. nslookup
- D. Nmap
- E. netcat

**Answer: B**

**NEW QUESTION 538**

- (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 542**

- (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 546**

- (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 551**

- (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 556**

- (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 561**

- (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 562**

- (Exam Topic 5)

An active/passive configuration has an impact on:

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

**Answer:** C

**NEW QUESTION 566**

- (Exam Topic 5)

A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFlenabled 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 571

- (Exam Topic 5)

Joe, a user, has been trying to send Ann, a different user, an encrypted document via email. Ann has not received the attachment but is able to receive the header information. Which of the following is MOST likely preventing Ann from receiving the encrypted file?

- A. Unencrypted credentials
- B. Authentication issues
- C. Weak cipher suite
- D. Permission issues

**Answer:** B

#### NEW QUESTION 575

- (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 579

- (Exam Topic 5)

A security administrator learns that PII, which was gathered by the organization, has been found in an open forum. As a result, several C-level executives found their identities were compromised, and they were victims of a recent whaling attack. Which of the following would prevent these problems in the future? (Select TWO).

- A. Implement a reverse proxy.
- B. Implement an email DLP.
- C. Implement a spam filter.
- D. Implement a host-based firewall.
- E. Implement a HIDS.

**Answer:** BC

#### NEW QUESTION 582

- (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 the 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 583

- (Exam Topic 5)

A security technician has been receiving alerts from several servers that indicate load balancers have had a significant increase in traffic. The technician initiates a system scan. The scan results illustrate that the disk space on several servers has reached capacity. The scan also indicates that incoming internet traffic to the servers has increased. Which of the following is the MOST likely cause of the decreased disk space?

- A. Misconfigured devices
- B. Logs and events anomalies
- C. Authentication issues
- D. Unauthorized software

**Answer:** D

#### NEW QUESTION 586

.....

## 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>