

Exam Questions SY0-501

CompTIA Security+ Certification Exam

<https://www.2passeasy.com/dumps/SY0-501/>



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 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 3

- (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 4

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 5

- (Exam Topic 1)

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

```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address          Foreign Address        State               Process
TCP    0.0.0.0:135              0.0.0.0:0               LISTENING           RpcSs [svchost.exe]
TCP    0.0.0.0:445              0.0.0.0:0               LISTENING           [svchost.exe]

TCP    192.168.1.10:5000       10.37.213.20           ESTABLISHED         winserver.exe
UDP    192.168.1.10:1900      *.*
```

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

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

Answer: D

NEW QUESTION 6

- (Exam Topic 1)

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 7

- (Exam Topic 1)

Malicious traffic from an internal network has been detected on an unauthorized port on an application server. Which of the following network-based security controls should the engineer consider implementing?

- A. ACLs
- B. HIPS
- C. NAT
- D. MAC filtering

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 9

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

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

- A. Verify the certificate has not expired on the server.
- B. Ensure the certificate has a .pfx extension on the server.
- C. Update the root certificate into the client computer certificate store.
- D. Install the updated private key on the web server.
- E. Have users clear their browsing history and relaunch the session.

Answer: AC

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 12

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 14

- (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 17

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 20

- (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 21

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 22

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 25

- (Exam Topic 1)

A system administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees.

Which of the following should the administrator implement?

- A. Shared accounts
- B. Preshared passwords
- C. Least privilege
- D. Sponsored guest

Answer: D

NEW QUESTION 30

- (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 32

- (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

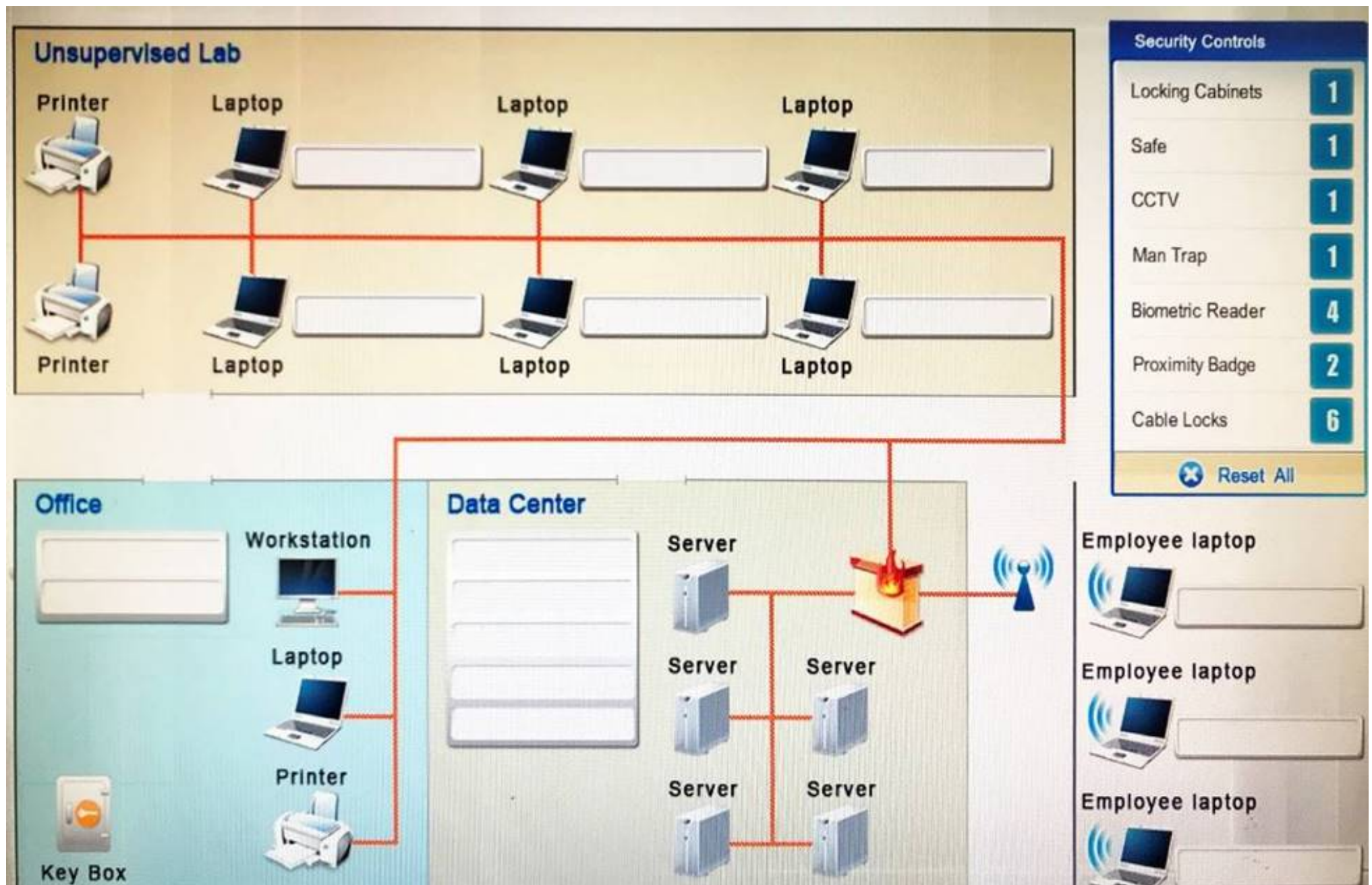
Answer: A

NEW QUESTION 37

- (Exam Topic 1)

You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.

Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away

Proximity badge + reader

Safe is a hardware/physical security measure

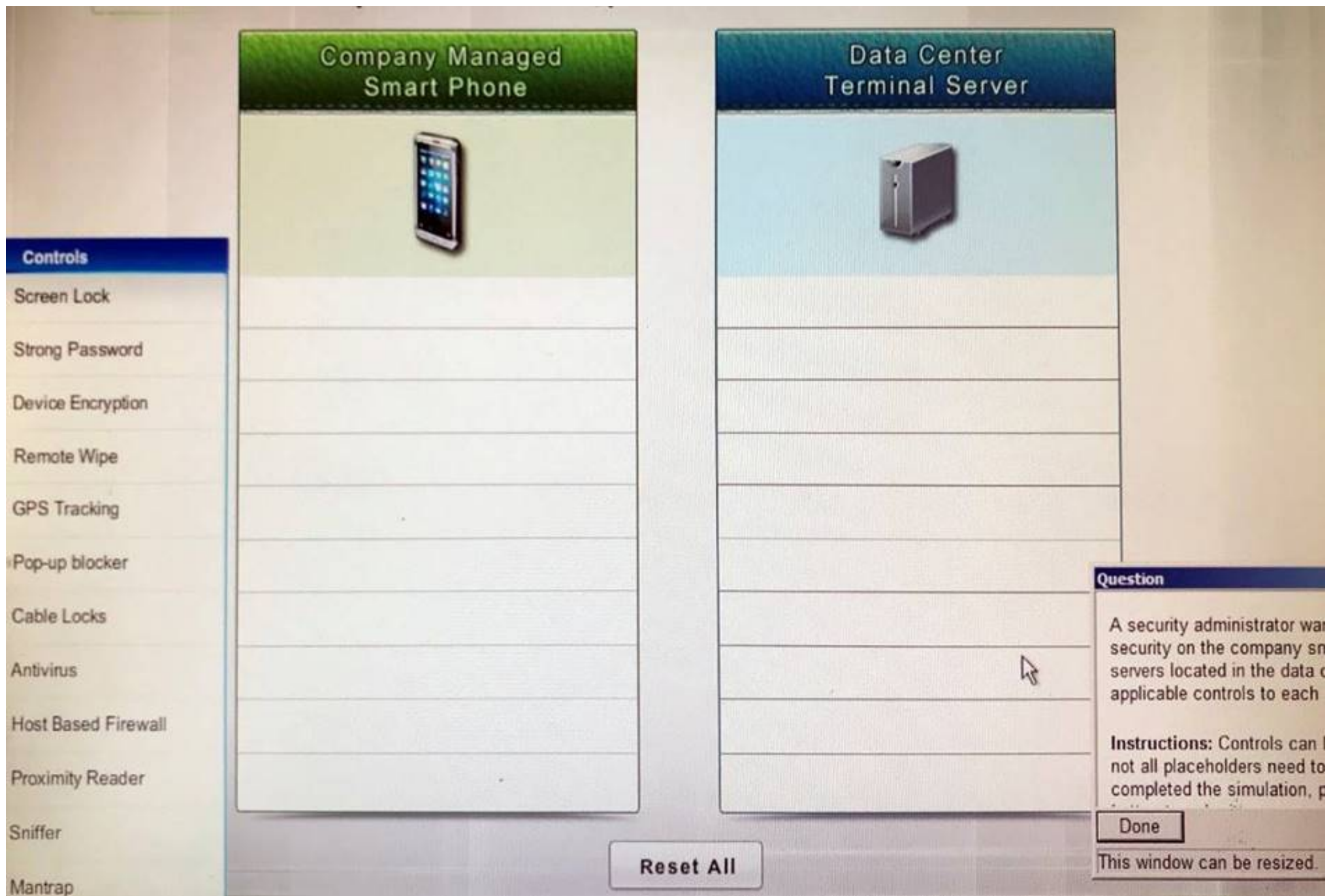
Mantrap can be used to control access to sensitive areas. CCTV can be used as video surveillance. Biometric reader can be used to control and prevent unauthorized access. Locking cabinets can be used to protect backup media, documentation and other physical artefacts.

NEW QUESTION 39

- (Exam Topic 1)

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

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 43

- (Exam Topic 1)

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

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

Which of the following vulnerabilities is present?

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

Answer: B

NEW QUESTION 44

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 45

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 47

- (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 48

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 50

- (Exam Topic 1)

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

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

Answer: AB

NEW QUESTION 55

- (Exam Topic 1)

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

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

Answer: BE

NEW QUESTION 57

- (Exam Topic 1)

A network administrator wants to implement a method of securing internal routing. Which of the following should the administrator implement?

- A. DMZ
- B. NAT
- C. VPN

D. PAT

Answer: C

NEW QUESTION 60

- (Exam Topic 1)

A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

- A. PFX
- B. PEM
- C. DER
- D. CER

Answer: B

NEW QUESTION 63

- (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 68

- (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 73

- (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 75

- (Exam Topic 1)

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

- A. Life
- B. Intellectual property
- C. Sensitive data
- D. Public reputation

Answer: A

NEW QUESTION 79

- (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 81

- (Exam Topic 2)

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

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

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

Answer: AC

NEW QUESTION 82

- (Exam Topic 2)

A security analyst wants to harden the company's VoIP PBX. The analyst is worried that credentials may be intercepted and compromised when IP phones authenticate with the PBX. Which of the following would best prevent this from occurring?

- A. Implement SRTP between the phones and the PBX.
- B. Place the phones and PBX in their own VLAN.
- C. Restrict the phone connections to the PBX.
- D. Require SIPS on connections to the PBX.

Answer: D

NEW QUESTION 84

- (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 88

- (Exam Topic 2)

Which of the following AES modes of operation provide authentication? (Select two.)

- A. CCM

- B. CBC
- C. GCM
- D. DSA
- E. CFB

Answer: AC

NEW QUESTION 92

- (Exam Topic 2)

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

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

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

Answer: B

NEW QUESTION 96

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 97

- (Exam Topic 2)

An administrator is configuring access to information located on a network file server named "Bowman". The files are located in a folder named "BalkFiles". The files are only for use by the "Matthews" division and should be read-only. The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model. Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files.

The administrator configures the file share according to the following table:

Share permissions

1	Everyone	Full control
---	----------	--------------

File system permissions

2	Bowman\Users	Modify	Inherited
3	Domain\Matthews	Read	Not inherited
4	Bowman\System	Full control	Inherited
5	Bowman\Administrators	Full control	Not inherited

Which of the following rows has been misconfigured?

- A. Row 1
- B. Row 2
- C. Row 3
- D. Row 4
- E. Row 5

Answer: D

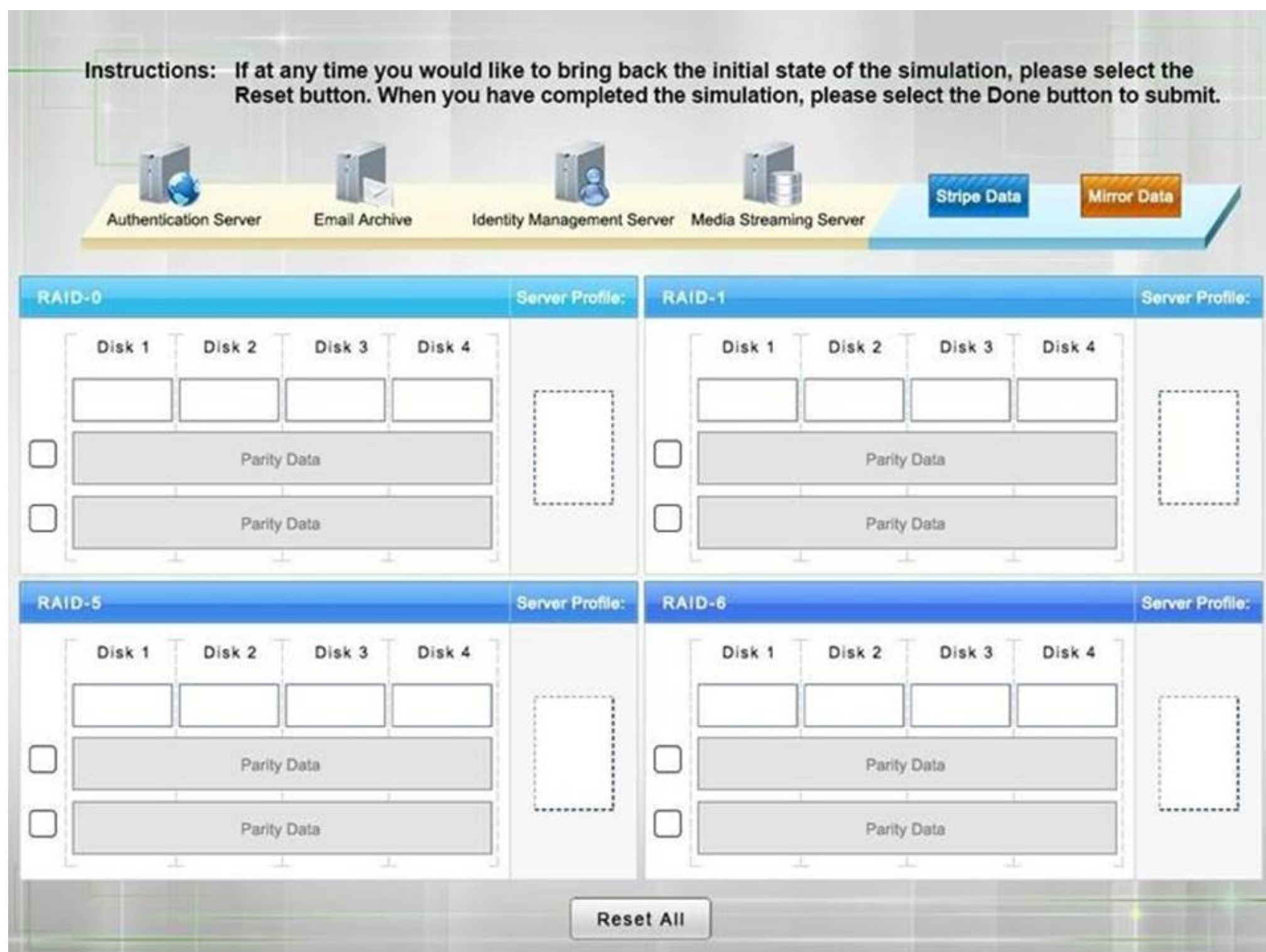
NEW QUESTION 102

- (Exam Topic 2)

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

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

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

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

NEW QUESTION 105

- (Exam Topic 2)

Before an infection was detected, several of the infected devices attempted to access a URL that was similar to the company name but with two letters transposed. Which of the following BEST describes the attack vector used to infect the devices?

- A. Cross-site scripting
- B. DNS poisoning
- C. Typo squatting
- D. URL hijacking

Answer: C

NEW QUESTION 110

- (Exam Topic 2)

A director of IR is reviewing a report regarding several recent breaches. The director compiles the following statistics:

- Initial IR engagement time frame
- Length of time before an executive management notice went out

-Average IR phase completion

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

- A. CSIRT
- B. Containment phase
- C. Escalation notifications
- D. Tabletop exercise

Answer: D

NEW QUESTION 114

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 115

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 120

- (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 124

- (Exam Topic 2)

A security analyst is performing a quantitative risk analysis. The risk analysis should show the potential monetary loss each time a threat or event occurs. Given this requirement, which of the following concepts would assist the analyst in determining this value? (Select two.)

- A. ALE
- B. AV
- C. ARO
- D. EF
- E. ROI

Answer: BD

NEW QUESTION 125

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 129

- (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 131

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 133

- (Exam Topic 2)

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

- A. Implement time-of-day restrictions.
- B. Audit file access times.
- C. Secretly install a hidden surveillance camera.
- D. Require swipe-card access to enter the lab.

Answer: D

NEW QUESTION 136

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 141

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 143

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 147

- (Exam Topic 2)

A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization. Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?

- A. Implement a DLP solution and classify the report as confidential, restricting access only to human resources staff
- B. Restrict access to the share where the report resides to only human resources employees and enable auditing
- C. Have all members of the IT department review and sign the AUP and disciplinary policies
- D. Place the human resources computers on a restricted VLAN and configure the ACL to prevent access from the IT department

Answer: B

NEW QUESTION 151

- (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 153

- (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 154

- (Exam Topic 2)

Which of the following should identify critical systems and components?

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

Answer: D

NEW QUESTION 155

- (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 158

- (Exam Topic 2)

A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols MUST the security engineer select?

- A. EAP-FAST
- B. EAP-TLS
- C. PEAP
- D. EAP

Answer: C

NEW QUESTION 163

- (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 166

- (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 167

- (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 169

- (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 173

- (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 175

- (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 176

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 178

- (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 181

- (Exam Topic 2)

A systems administrator wants to protect data stored on mobile devices that are used to scan and record assets in a warehouse. The control must automatically destroy the secure container of mobile devices if they leave the warehouse. Which of the following should the administrator implement? (Select two.)

- A. Geofencing
- B. Remote wipe
- C. Near-field communication
- D. Push notification services
- E. Containerization

Answer: AE

NEW QUESTION 185

- (Exam Topic 2)

A help desk is troubleshooting user reports that the corporate website is presenting untrusted certificate errors to employees and customers when they visit the website. Which of the following is the MOST likely cause of this error, provided the certificate has not expired?

- A. The certificate was self signed, and the CA was not imported by employees or customers
- B. The root CA has revoked the certificate of the intermediate CA
- C. The valid period for the certificate has passed, and a new certificate has not been issued
- D. The key escrow server has blocked the certificate from being validated

Answer: C

NEW QUESTION 187

- (Exam Topic 2)

Company policy requires the use of passphrases instead of passwords.

Which of the following technical controls MUST be in place in order to promote the use of passphrases?

- A. Reuse
- B. Length
- C. History
- D. Complexity

Answer: D

NEW QUESTION 188

- (Exam Topic 2)

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

Which of the following types of attacks is this?

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

Answer: D

NEW QUESTION 191

- (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 196

- (Exam Topic 2)

Which of the following must be intact for evidence to be admissible in court?

- A. Chain of custody
- B. Order of volatility
- C. Legal hold
- D. Preservation

Answer: A

NEW QUESTION 197

- (Exam Topic 2)

As part of the SDLC, a third party is hired to perform a penetration test. The third party will have access to the source code, integration tests, and network diagrams. Which of the following BEST describes the assessment being performed?

- A. Black box
- B. Regression
- C. White box
- D. Fuzzing

Answer: C

NEW QUESTION 199

- (Exam Topic 3)

The Chief Executive Officer (CEO) of a major defense contracting company is traveling overseas for a conference. The CEO will be taking a laptop. Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

- A. Remote wipe
- B. Full device encryption
- C. BIOS password
- D. GPS tracking

Answer: B

NEW QUESTION 202

- (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 206

- (Exam Topic 3)

A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources. Which of the following should be implemented?

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

Answer: B

NEW QUESTION 211

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 212

- (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 213

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 217

- (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 219

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 222

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 224

- (Exam Topic 3)

An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week.

Which of the following would be the BEST method of updating this application?

- A. Configure testing and automate patch management for the application.
- B. Configure security control testing for the application.
- C. Manually apply updates for the application when they are released.
- D. Configure a sandbox for testing patches before the scheduled monthly update.

Answer: A

NEW QUESTION 226

- (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 229

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 233

- (Exam Topic 3)

The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?

- A. Collision resistance
- B. Rainbow table
- C. Key stretching
- D. Brute force attack

Answer: C

NEW QUESTION 236

- (Exam Topic 3)

Which of the following is the LEAST secure hashing algorithm?

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

Answer: C

NEW QUESTION 238

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 239

- (Exam Topic 3)

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

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

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

Answer: C

NEW QUESTION 243

- (Exam Topic 3)

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

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

Answer: CE

NEW QUESTION 247

- (Exam Topic 3)

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

- A. Key escrow
- B. Digital signatures

- C. PKI
- D. Hashing

Answer: B

NEW QUESTION 248

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 250

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 252

- (Exam Topic 3)

Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially. Which of the following would explain the situation?

- A. An ephemeral key was used for one of the messages
- B. A stream cipher was used for the initial email; a block cipher was used for the reply
- C. Out-of-band key exchange has taken place
- D. Asymmetric encryption is being used

Answer: D

Explanation:

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

NEW QUESTION 257

- (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 260

- (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 265

- (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 266

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 271

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 272

- (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 276

- (Exam Topic 3)

A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database. Which of the following risk mitigation strategies should have been implemented when the supervisor was demoted?

- A. Incident management
- B. Routine auditing
- C. IT governance
- D. Monthly user rights reviews

Answer: D

NEW QUESTION 281

- (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 286

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 288

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 292

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

NEW QUESTION 297

- (Exam Topic 3)

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

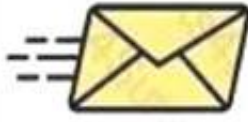









- A. Implement deduplication at the network level between the two locations
- B. Implement deduplication on the storage array to reduce the amount of drive space needed
- C. Implement deduplication on the server storage to reduce the data backed up
- D. Implement deduplication on both the local and remote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

Answer: B

NEW QUESTION 299

- (Exam Topic 3)

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

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

Spoofting

Hoax

Spam

Spim

Social Engineering

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

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

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

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

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

NEW QUESTION 304

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 307

- (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 308

- (Exam Topic 3)

Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

- A. Cloud computing
- B. Virtualization
- C. Redundancy
- D. Application control

Answer: B

Explanation:

Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

NEW QUESTION 313

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 318

- (Exam Topic 3)

A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued. Which of the following should the administrator submit to receive a new certificate?

- A. CRL
- B. OSCP
- C. PFX
- D. CSR
- E. CA

Answer: D

NEW QUESTION 322

- (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 325

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 328

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 329

- (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 333

- (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 338

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 339

- (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 342

- (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 345

- (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 347

- (Exam Topic 4)

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

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

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

Answer: C

NEW QUESTION 352

- (Exam Topic 4)

A datacenter recently experienced a breach. When access was gained, an RF device was used to access an air-gapped and locked server rack. Which of the following would BEST prevent this type of attack?

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

Answer: A

NEW QUESTION 353

- (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 356

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 360

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 363

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 366

- (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 367

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 369

- (Exam Topic 4)

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

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

Answer: AD

NEW QUESTION 373

- (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 374

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 378

- (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 379

- (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 381

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 382

- (Exam Topic 4)

A security administrator receives an alert from a third-party vendor that indicates a certificate that was installed in the browser has been hijacked at the root of a small public CA. The security administrator knows there are at least four different browsers in use on more than a thousand computers in the domain worldwide. Which of the following solutions would be BEST for the security administrator to implement to most efficiently assist with this issue?

- A. SSL
- B. CRL
- C. PKI
- D. ACL

Answer: B

NEW QUESTION 385

- (Exam Topic 4)

A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility. Which of the following configuration commands should be implemented to enforce this requirement?

- A. LDAP server 10.55.199.3
- B. CN=company, CN=com, OU=netadmin, DC=192.32.10.233
- C. SYSLOG SERVER 172.16.23.50
- D. TACAS server 192.168.1.100

Answer: B

NEW QUESTION 390

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 393

- (Exam Topic 4)

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

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

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

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

Answer: B

NEW QUESTION 397

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 402

- (Exam Topic 4)

An actor downloads and runs a program against a corporate login page. The program imports a list of usernames and passwords, looking for a successful attempt. Which of the following terms BEST describes the actor in this situation?

- A. Script kiddie
- B. Hacktivist
- C. Cryptologist
- D. Security auditor

Answer: A

NEW QUESTION 404

- (Exam Topic 4)

A wireless network has the following design requirements:

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

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

- A. PEAP

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

Answer: BE

NEW QUESTION 409

- (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 413

- (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 418

- (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 423

- (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 427

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 429

- (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 431

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 434

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 437

- (Exam Topic 5)

A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted. Which of the following types of attack is the caller performing?

- A. Phishing
- B. Shoulder surfing
- C. Impersonation
- D. Dumpster diving

Answer: C

NEW QUESTION 440

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 442

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 445

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 449

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 454

- (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 458

- (Exam Topic 5)

Which of the following locations contain the MOST volatile data?

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

Answer: D

NEW QUESTION 461

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 464

- (Exam Topic 5)

Which of the following uses precomputed hashes to guess passwords?

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

Answer: C

NEW QUESTION 468

- (Exam Topic 5)

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

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

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

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

Answer: C

NEW QUESTION 470

- (Exam Topic 5)

An organization plans to implement multifactor authentication techniques within the enterprise network architecture. Each authentication factor is expected to be a unique control. Which of the following BEST describes the proper employment of multifactor authentication?

- A. Proximity card, fingerprint scanner, PIN
- B. Fingerprint scanner, voice recognition, proximity card
- C. Smart card, user PKI certificate, privileged user certificate
- D. Voice recognition, smart card, proximity card

Answer: A

NEW QUESTION 474

- (Exam Topic 5)

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

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

File Name Source MD5 Target MD5 Status

antivirus.exe F794F21CD33E4F57890DDEA5CF267ED2 F794F21CD33E4F57890DDEA5CF267ED2

Automatic iexplore.exe 7FAAF21CD33E4F57890DDEA5CF29CCEA AA87F21CD33E4F57890DDEAEE2197333 Automatic service.exe

77FF390CD33E4F57890DDEA5CF28881F 77FF390CD33E4F57890DDEA5CF28881F Manual USB.exe E289F21CD33E4F57890DDEA5CF28EDC0

E289F21CD33E4F57890DDEA5CF28EDC0 Stopped

Based on the above output, which of the following should be reviewed?

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

Answer: B

NEW QUESTION 477

- (Exam Topic 5)

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

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

Answer: AD

NEW QUESTION 482

- (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 485

- (Exam Topic 5)

Which of the following would be considered multifactor authentication?

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

Answer: C

NEW QUESTION 488

- (Exam Topic 5)

A security manager is creating an account management policy for a global organization with sales personnel who must access corporate network resources while traveling all over the world. Which of the following practices is the security manager MOST likely to enforce with the policy? (Select TWO)

- A. Time-of-day restrictions
- B. Password complexity
- C. Location-based authentication
- D. Group-based access control
- E. Standard naming convention

Answer: BD

NEW QUESTION 490

- (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 492

- (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 495

- (Exam Topic 5)

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

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

Answer: B

Explanation:

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

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

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

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

NEW QUESTION 498

- (Exam Topic 5)

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

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

Confidence: certain

Recommendation: apply vendor patches

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

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

Answer: B

NEW QUESTION 501

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 506

- (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 507

- (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 509

- (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 512

- (Exam Topic 5)

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

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

Answer: AB

NEW QUESTION 513

- (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 518

- (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 520

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 522

- (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 526

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 530

- (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 534

- (Exam Topic 5)

To help prevent one job role from having sufficient access to create, modify, and approve payroll data, which of the following practices should be employed?

- A. Least privilege
- B. Job rotation
- C. Background checks
- D. Separation of duties

Answer: D

NEW QUESTION 539

- (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 541

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 542

- (Exam Topic 5)

A security engineer must install the same x.509 certificate on three different servers. The client application that connects to the server performs a check to ensure the certificate matches the host name. Which of the following should the security engineer use?

- A. Wildcard certificate
- B. Extended validation certificate
- C. Certificate chaining
- D. Certificate utilizing the SAN file

Answer: D

Explanation:

SAN = Subject Alternate Names

NEW QUESTION 546

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 548

- (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 551

- (Exam Topic 5)

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

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

Answer: A

Explanation:

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

NEW QUESTION 555

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 556

- (Exam Topic 5)

When attackers use a compromised host as a platform for launching attacks deeper into a company's network, it is said that they are:

- A. escalating privilege
- B. becoming persistent
- C. fingerprinting
- D. pivoting

Answer: D

NEW QUESTION 560

- (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 562

- (Exam Topic 5)

A security administrator has written a script that will automatically upload binary and text-based configuration files onto a remote server using a scheduled task. The configuration files contain sensitive information. Which of the following should the administrator use? (Select TWO)

- A. TOPT
- B. SCP
- C. FTP over a non-standard port
- D. SRTP
- E. Certificate-based authentication
- F. SNMPv3

Answer: CE

NEW QUESTION 563

- (Exam Topic 5)

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

The manager has gathered these facts:

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

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

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

Answer: D

NEW QUESTION 564

- (Exam Topic 5)

Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter. Which of the following is being described?

- A. Service level agreement
- B. Memorandum of understanding
- C. Business partner agreement
- D. Interoperability agreement

Answer: A

NEW QUESTION 567

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 569

- (Exam Topic 5)

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

- A. Implement SAML so the company's services may accept assertions from the customers' authentication servers.
- B. Provide customers with a constrained interface to manage only their users' accounts in the company's active directory server.
- C. Provide a system for customers to replicate their users' passwords from their authentication service to the company's.
- D. Use SOAP calls to support authentication between the company's product and the customers' authentication servers.

Answer: A

NEW QUESTION 574

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 576

- (Exam Topic 5)

Upon entering an incorrect password, the logon screen displays a message informing the user that the password does not match the username provided and is not the required length of 12 characters. Which of the following secure coding techniques should a security analyst address with the application developers to follow security best practices?

- A. Input validation
- B. Error handling
- C. Obfuscation
- D. Data exposure

Answer: B

NEW QUESTION 578

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 581

- (Exam Topic 5)

A new Chief Information Officer (CIO) has been reviewing the badging and decides to write a policy that all employees must have their badges rekeyed at least

annually. Which of the following controls BEST describes this policy?

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

Answer: D

NEW QUESTION 582

- (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 587

- (Exam Topic 5)

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

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

Answer: BD

NEW QUESTION 589

- (Exam Topic 5)

A systems administrator is deploying a new mission essential server into a virtual environment. Which of the following is BEST mitigated by the environment's rapid elasticity characteristic?

- A. Data confidentiality breaches
- B. VM escape attacks
- C. Lack of redundancy
- D. Denial of service

Answer: D

NEW QUESTION 590

- (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 591

- (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 596

- (Exam Topic 5)

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

wireless network?

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

Answer: A

NEW QUESTION 599

- (Exam Topic 5)

An active/passive configuration has an impact on:

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

Answer: C

NEW QUESTION 600

- (Exam Topic 5)

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

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

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

Answer: D

NEW QUESTION 605

- (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 608

- (Exam Topic 5)

A Chief Information Officer (CIO) recently saw on the news that a significant security flaw exists with a specific version of a technology the company uses to support many critical applications. The CIO wants to know if this reported vulnerability exists in the organization and, if so, to what extent the company could be harmed. Which of the following would BEST provide the needed information?

- A. Penetration test
- B. Vulnerability scan
- C. Active reconnaissance
- D. Patching assessment report

Answer: A

NEW QUESTION 611

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 615

- (Exam Topic 5)

A security analyst is acquiring data from a potential network incident. Which of the following evidence is the analyst MOST likely to obtain to determine the incident?

- A. Volatile memory capture
- B. Traffic and logs

- C. Screenshots
- D. System image capture

Answer: B

NEW QUESTION 620

- (Exam Topic 5)

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

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

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

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

Answer: D

NEW QUESTION 623

- (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 628

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SY0-501 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SY0-501 Product From:

<https://www.2passeasy.com/dumps/SY0-501/>

Money Back Guarantee

SY0-501 Practice Exam Features:

- * SY0-501 Questions and Answers Updated Frequently
- * SY0-501 Practice Questions Verified by Expert Senior Certified Staff
- * SY0-501 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SY0-501 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year