SY0-501 Dumps

CompTIA Security+ Certification Exam

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

NEW QUESTION 1
- (Exam Topic 1)
A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords. The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Select two.)

A. The portal will function as a service provider and request an authentication assertion.
B. The portal will function as an identity provider and issue an authentication assertion.
C. The portal will request an authentication ticket from each network that is transitively trusted.
D. The back-end networks will function as an identity provider and issue an authentication assertion.
E. The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store.
F. The back-end networks will verify the assertion token issued by the portal functioning as the identity provider.

Answer: AB

NEW QUESTION 2
- (Exam Topic 1)
An analyst wants to implement a more secure wireless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?

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

Answer: A

Explanation:
EAP by itself is only an authentication framework.
PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated. The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel is protected. As a result, when EAP messages are able to be
discovered in the "clear" they do not provide the protection that was assumed when the protocol was originally authored.
PEAP, EAP-TTLS, and EAP-TLS "protect" inner EAP authentication within SSL/TLS sessions.

NEW QUESTION 3
- (Exam Topic 1)
An organization finds that most help desk calls are regarding account lockout due to a variety of applications running on different systems. Management is looking for a solution to reduce the number of account lockouts while improving security. Which of the following is the BEST solution for this organization?

A. Create multiple application accounts for each user.
B. Provide secure tokens.
C. Implement SSO.
D. Utilize role-based access control.

Answer: C

NEW QUESTION 4
- (Exam Topic 1)
Which of the following types of keys is found in a key escrow?

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

Answer: B

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

NEW QUESTION 5
- (Exam Topic 1)
In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?

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

Answer: A

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

NEW QUESTION 6
- (Exam Topic 1)
An organization's file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

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

Answer: C

NEW QUESTION 7
- (Exam Topic 1)
After a user reports stow 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
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 *.*                                      SSDPSVR
```

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 8
- (Exam Topic 1)
An attacker compromises a public CA and issues unauthorized X.509 certificates for Company.com. In the future, Company.com wants to mitigate the impact of similar incidents. Which of the following would assist Company.com with its goal?

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

Answer: A

NEW QUESTION 9
- (Exam Topic 1)
Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened.
The network and security teams perform the following actions:
▶ Shut down all network shares.
▶ Run an email search identifying all employees who received the malicious message.
▶ Reimage all devices belonging to users who opened the attachment.
Next, the teams want to re-enable the network shares. Which of the following BEST describes this phase of the incident response process?

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

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
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 10
- (Exam Topic 1)
A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

● All access must be correlated to a user account.

● All user accounts must be assigned to a single individual.

● User access to the PHI data must be recorded.

● Anomalies in PHI data access must be reported.

● Logs and records cannot be deleted or modified.

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

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

Answer: ACG

NEW QUESTION 12
- (Exam Topic 1)
Which of the following would MOST likely appear in an uncredentialed vulnerability scan?

A. Self-signed certificates
B. Missing patches
C. Auditing parameters
D. Inactive local accounts

Answer: D

NEW QUESTION 17
- (Exam Topic 1)
A high-security defense installation recently begun utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation. Which of the following types of controls does this BEST describe?

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

Answer: A

NEW QUESTION 22
- (Exam Topic 1)
Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Select two.)

A. Rainbow table attacks greatly reduce compute cycles at attack time.
B. Rainbow tables must include precomputed hashes.
C. Rainbow table attacks do not require access to hashed passwords.
D. Rainbow table attacks must be performed on the network.
E. Rainbow table attacks bypass maximum failed login restrictions.

Answer: BE

NEW QUESTION 25
- (Exam Topic 1)
Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Which of the following should be used to sign the user's certificates?

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

Answer: B

NEW QUESTION 26
- (Exam Topic 1)
An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

A. RTO
B. RPO

C. MTBF
D. MTTR

Answer: A

NEW QUESTION 30
- (Exam Topic 1)
In terms of encrypting data, which of the following is BEST described as a way to safeguard password data by adding random data to it in storage?

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

Answer: A

NEW QUESTION 34
- (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 38
- (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 40
- (Exam Topic 1)
A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

A. An attacker can access and change the printer configuration.
B. SNMP data leaving the printer will not be properly encrypted.
C. An MITM attack can reveal sensitive information.
D. An attacker can easily inject malicious code into the printer firmware.
E. Attackers can use the PCL protocol to bypass the firewall of client computers.

Answer: B

NEW QUESTION 41
- (Exam Topic 1)
A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant. Which of the following represents the authentication architecture in use?

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

Answer: D

NEW QUESTION 45
- (Exam Topic 1)
Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?

A. Privilege escalation
B. Pivoting
C. Process affinity
D. Buffer overflow

Answer: A

NEW QUESTION 49

- (Exam Topic 1)
A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

A. 1
B. 2
C. 3
D. 4

Answer: B

NEW QUESTION 50
- (Exam Topic 1)
A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

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

Answer: C

NEW QUESTION 55
- (Exam Topic 1)
A 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 60
- (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 63
- (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.
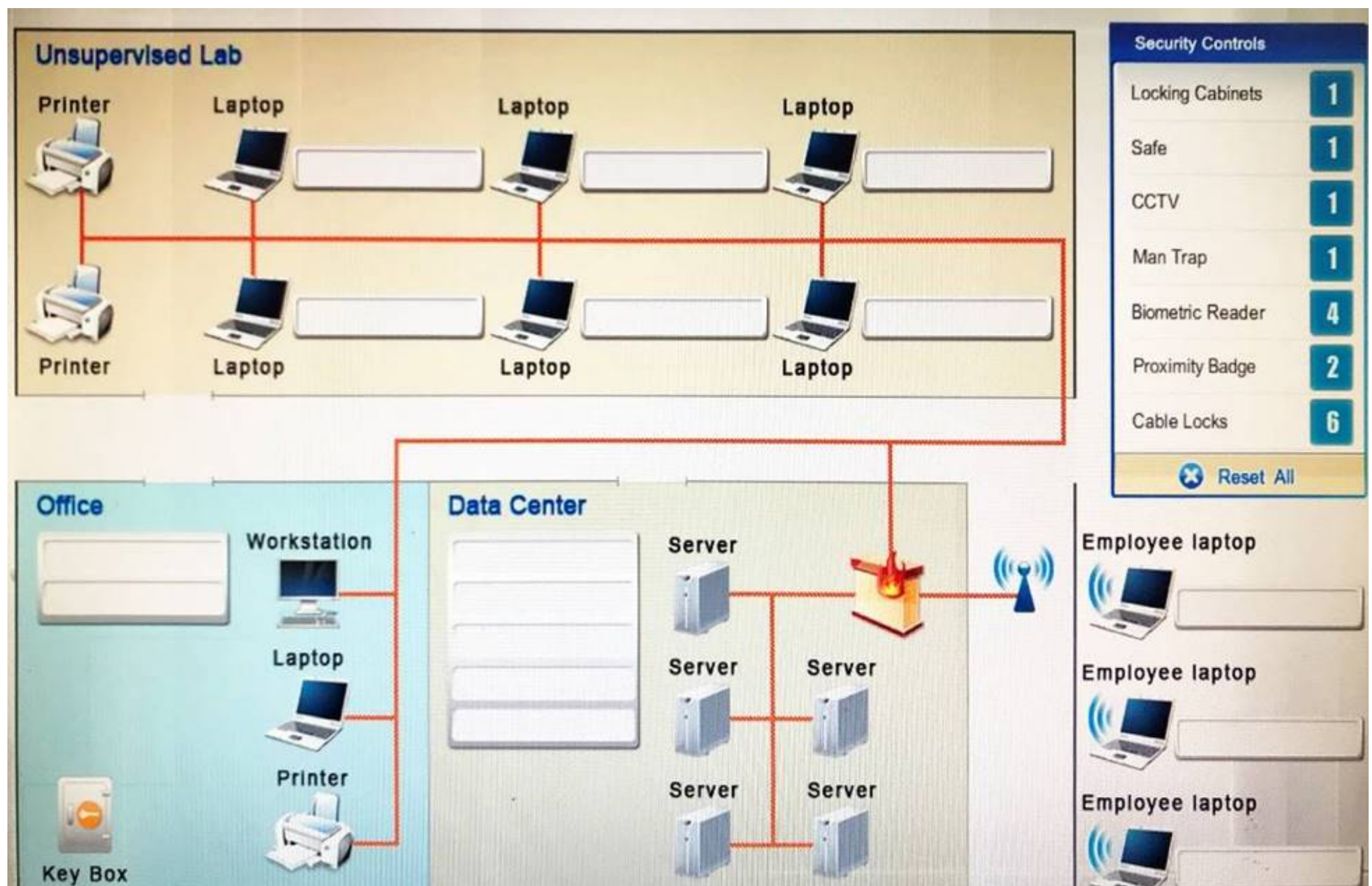
A. Mastered
B. Not Mastered

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 64
- (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.
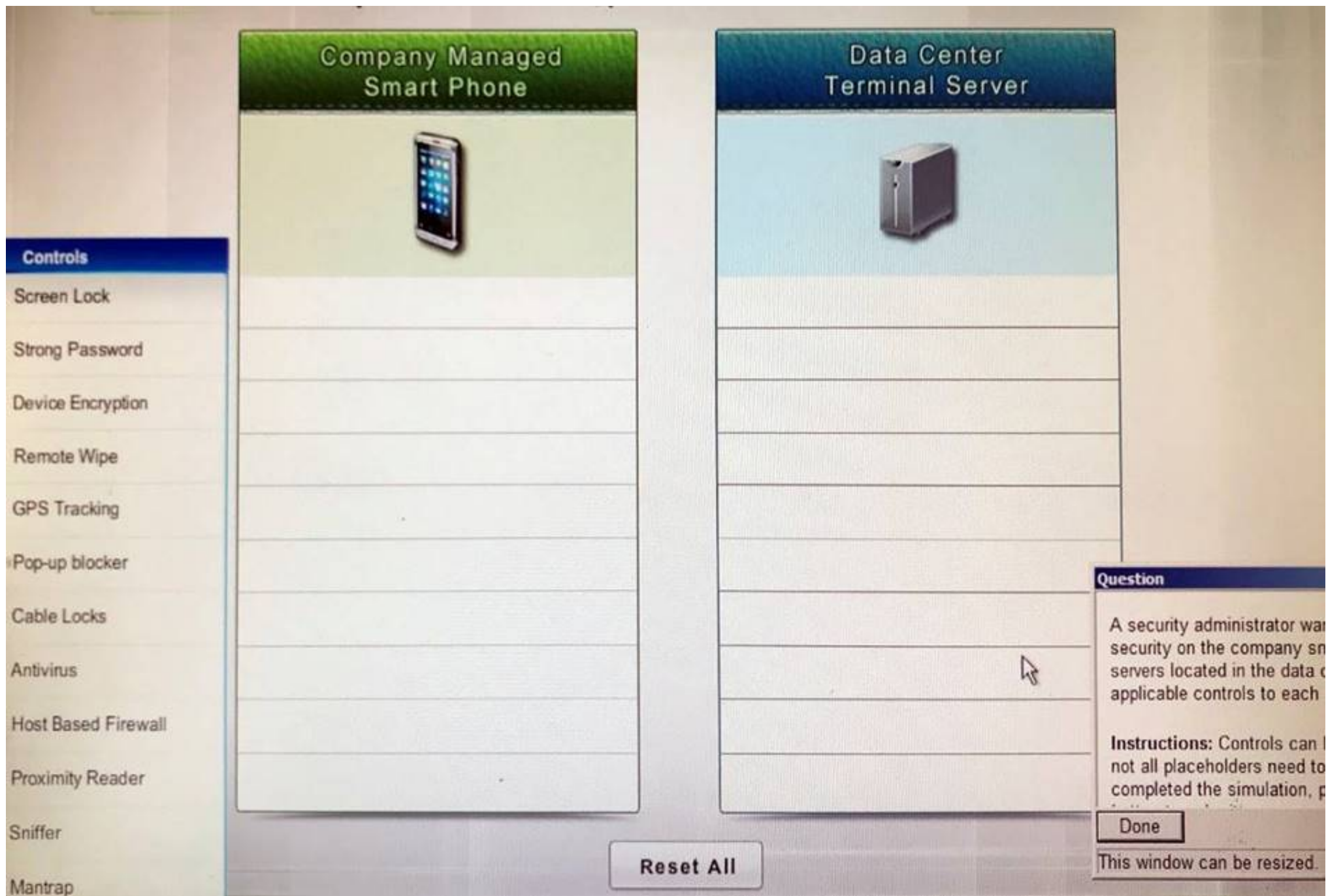
A. Mastered
B. Not Mastered

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 68
- (Exam Topic 1)
When trying to log onto a company's new ticketing system, some employees receive the following message: Access denied: too many concurrent sessions. The ticketing system was recently installed on a small VM with only the recommended hardware specifications. Which of the following is the MOST likely cause for this error message?

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

Answer: C

NEW QUESTION 73
- (Exam Topic 1)
An auditor wants to test the security posture of an organization by running a tool that will display the following:

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

Which of the following commands should be used?

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

Answer: A

NEW QUESTION 77
- (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 79
- (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 82
- (Exam Topic 1)
An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

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

Answer: C

NEW QUESTION 87
- (Exam Topic 1)
An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call.
The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

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

Answer: C

NEW QUESTION 89
- (Exam Topic 1)
A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials. Which of the following account types is the systems administrator using?

A. Shared account
B. Guest account
C. Service account
D. User account

Answer: C

NEW QUESTION 92
- (Exam Topic 1)
Which of the following technologies employ the use of SAML? (Select two.)

A. Single sign-on
B. Federation
C. LDAP

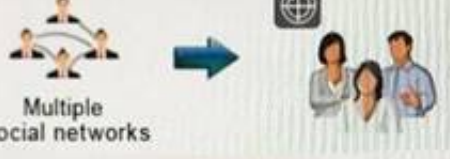D. Secure token
E. RADIUS

Answer: AB

NEW QUESTION 94
- (Exam Topic 1)
Select the appropriate attack from each drop down list to label the corresponding illustrated attack.
Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.

Attack Vector		Target	Identified Attack
Attacker gains confidential company information	→	Targeted CEO and board members	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker posts link to fake AV software	→ Multiple social networks →	Broad set of victims	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker collecting credit card details	→	Phone-based victim	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker mass-mails product information to parties that have already opted out of receiving advertisements	→	Broad set of recipients	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker redirects name resolution entries from legitimate site to fraudulent site	→	Fraudulent site / Legitimate site / Victims	WHALING / SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK

A. Mastered
B. Not Mastered

Answer: A

Explanation:

1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

2: The Hoax in this question is designed to make people believe that the fake AV (anti- virus) software is genuine.

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

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

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

5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

References:
http://searchsecurity.techtarget.com/definition/spear-phishing http://www.webopedia.com/TERM/V/vishing.html http://www.webopedia.com/TERM/P/phishing.html http://www.webopedia.com/TERM/P/pharming.html

NEW QUESTION 95
- (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 100
- (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 105
- (Exam Topic 1)
A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

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

Answer: B

NEW QUESTION 107
- (Exam Topic 1)
An organization needs to implement a large PKI. Network engineers are concerned that repeated transmission of the OCSP will impact network performance. Which of the following should the security analyst recommend is lieu of an OCSP?

A. CSR
B. CRL
C. CA
D. OID

Answer: B

NEW QUESTION 111
- (Exam Topic 1)
Adhering to a layered security approach, a controlled access facility employs security guards who verify the authorization of all personnel entering the facility. Which of the following terms BEST describes the security control being employed?

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

Answer: C

NEW QUESTION 114
- (Exam Topic 1)
An employer requires that employees use a key-generating app on their smartphones to log into corporate applications. In terms of authentication of an individual, this type of access policy is BEST defined as:

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

Answer: A

NEW QUESTION 118
- (Exam Topic 1)
Which of the following attack types BEST describes a client-side attack that is used to manipulate an HTML iframe with JavaScript code via a web browser?

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

Answer: C

NEW QUESTION 120
- (Exam Topic 1)
A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?

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

Answer: C

NEW QUESTION 125
- (Exam Topic 1)
A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

```
Hostname      IP address       MAC                  MAC filter
DadPC         192.168.1.10     00:1D:1A:44:17:B5    On
MomPC         192.168.1.15     21:13:D6:C5:42:A2    Off
JuniorPC      192.168.2.16     42:A7:D1:25:11:52    On
Unknown       192.168.1.18     10:B3:22:1A:FF:21    Off
```

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

A. Apply MAC filtering and see if the router drops any of the systems.
B. Physically check each of the authorized systems to determine if they are logged onto the network.
C. Deny the "unknown" host because the hostname is not known and MAC filtering is not applied to this host.
D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

Answer: C

NEW QUESTION 128
- (Exam Topic 1)
When identifying a company's most valuable assets as part of a BIA, which of the following should be the FIRST priority?

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

Answer: A

NEW QUESTION 131
- (Exam Topic 1)
A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

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

Answer: B

Explanation:
Only Kerberos that can do Mutual Auth and Delegation.

NEW QUESTION 133
- (Exam Topic 2)
A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls.
Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

A. Password complexity policies
B. Hardware tokens
C. Biometric systems
D. Role-based permissions
E. One time passwords
F. Separation of duties
G. Multifactor authentication
H. Single sign-on
I. Lease privilege

Answer: DFI

NEW QUESTION 134
- (Exam Topic 2)
Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

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

Answer: D

NEW QUESTION 138
- (Exam Topic 2)
A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online. Which of the following methods would have MOST likely prevented the data from being exposed?

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

Answer: D

NEW QUESTION 142
- (Exam Topic 2)
A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have cause many executives in the company to travel with mini tablet devices instead of laptops.
These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network.
Which of the following should be implemented in order to meet the security policy requirements?

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

Answer: E

NEW QUESTION 144
- (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 145
- (Exam Topic 2)
A security analyst wants to harden the company's VoIP PBX. The analyst is worried that credentials may be intercepted and compromised when IP phones authenticate with the BPX. Which of the following would best prevent this from occurring?

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

Answer: D

NEW QUESTION 148
- (Exam Topic 2)
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 ono 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 149
- (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 153
- (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 sing 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 156
- (Exam Topic 2)
Which of the following are methods to implement HA in a web application server environment? (Select two.)

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

Answer: AB

NEW QUESTION 160
- (Exam Topic 2)
To reduce disk consumption, an organization's legal department has recently approved a new policy setting the data retention period for sent email at six months. Which of the following is the BEST way to ensure this
goal is met?

A. Create a daily encrypted backup of the relevant emails.
B. Configure the email server to delete the relevant emails.
C. Migrate the relevant emails into an "Archived" folder.
D. Implement automatic disk compression on email servers.

Answer: A

NEW QUESTION 164
- (Exam Topic 2)
A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening. In order to implement a true separation of duties approach the bank could:

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

Answer: C

NEW QUESTION 168
- (Exam Topic 2)
A security analyst is investigating a suspected security breach and discovers the following in the logs of the potentially compromised server:

```
Time         Source          Destination       Account Name    Action
11:01:31     18.12.98.145    10.15.21.100      Joe             Logon Failed
11:01:32     18.12.98.145    10.15.21.100      Joe             Logon Failed
11:01:33     18.12.98.145    10.15.21.100      Joe             Logon Failed
11:01:34     18.12.98.145    10.15.21.100      Joe             Logon Failed
11:01:35     18.12.98.145    10.15.21.100      Joe             Logon Failed
11:01:36     18.12.98.145    10.15.21.100      Joe             Logon Failed
11:01:37     18.12.98.145    10.15.21.100      Joe             Logon Failed
11:01:38     18.12.98.145    10.15.21.100      Joe             Logon Successful
```

Which of the following would be the BEST method for preventing this type of suspected attack in the future?

A. Implement password expirations
B. Implement restrictions on shared credentials
C. Implement account lockout settings
D. Implement time-of-day restrictions on this server

Answer: C

NEW QUESTION 169
- (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 174
- (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 176
- (Exam Topic 2)
A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten
application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another. Which of
the following should the security administrator do to rectify this issue?

A. Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
B. Recommend classifying each application into like security groups and segmenting the groups from one another
C. Recommend segmenting each application, as it is the most secure approach
D. Recommend that only applications with minimal security features should be segmented to protect them

Answer: B

NEW QUESTION 180
- (Exam Topic 2)
Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

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

Answer: A

NEW QUESTION 182
- (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 187
- (Exam Topic 2)
A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must
collect the most volatile date first. Which of the following is the correct order in which Joe should collect the data?

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

Answer: D

NEW QUESTION 191
- (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 193
- (Exam Topic 2)
A security analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the
following should the security analyst do NEXT?

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

Answer: D

NEW QUESTION 196
- (Exam Topic 2)
A manager suspects that an IT employee with elevated database access may be knowingly modifying financial transactions for the benefit of a competitor. Which of the following practices should the manager implement to validate the concern?

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

Answer: A

NEW QUESTION 200
- (Exam Topic 2)
AChief Information Officer (CIO) drafts an agreement between the organization and its employees. The agreement outlines ramifications for releasing information without consent and/or approvals. Which of the following BEST describes this type of agreement?

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

Answer: B

NEW QUESTION 203
- (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 208
- (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 213
- (Exam Topic 2)
A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer. Which of the following is the BEST way to accomplish this?

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

Answer: A

NEW QUESTION 216
- (Exam Topic 2)
A security analyst has received the following alert snippet from the HIDS appliance:

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

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

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

Answer: B

NEW QUESTION 220
- (Exam Topic 2)
A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him. Which of the following BEST describes what occurred?

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

Answer: D

NEW QUESTION 223
- (Exam Topic 2)
A penetration tester finds that a company's login credentials for the email client were being sent in clear text. Which of the following should be done to provide encrypted logins to the email server?

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

Answer: D

NEW QUESTION 226
- (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 231
- (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 236
- (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 241

- (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 243
- (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 246
- (Exam Topic 2)
A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

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

Answer: D

NEW QUESTION 250
- (Exam Topic 2)
Company policy requires the use if passphrases instead if 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 254
- (Exam Topic 2)
An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization's security policy, the employee's access to all network resources is terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server. Which of the following represents the BEST course of action?

A. Approve the former employee's request, as a password reset would give the former employee access to only the human resources server.
B. Deny the former employee's request, since the password reset request came from an external email address.
C. Deny the former employee's request, as a password reset would give the employee access to all network resources.
D. Approve the former employee's request, as there would not be a security issue with the former employee gaining access to network resources.

Answer: C

NEW QUESTION 259
- (Exam Topic 2)
A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Select two.)

A. Ping
B. Ipconfig
C. Tracert
D. Netstat
E. Dig
F. Nslookup

Answer: BC

NEW QUESTION 264
- (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 267
- (Exam Topic 2)
Which of the following vulnerability types would the type of hacker known as a script kiddie be MOST dangerous against?

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

Answer: B

NEW QUESTION 269
- (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 273
- (Exam Topic 2)
An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP. Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

A. Use a honeypot
B. Disable unnecessary services
C. Implement transport layer security
D. Increase application event logging

Answer: B

NEW QUESTION 276
- (Exam Topic 3)
A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

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

Answer: B

NEW QUESTION 277
- (Exam Topic 3)
A security team wants to establish an Incident Response plan. The team has never experienced an incident. Which of the following would BEST help them establish plans and procedures?

A. Table top exercises
B. Lessons learned
C. Escalation procedures
D. Recovery procedures

Answer: A

NEW QUESTION 279
- (Exam Topic 3)
A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non- repudiation. Which of the following implements all these requirements?

A. Bcrypt
B. Blowfish
C. PGP

D. SHA

Answer: C

NEW QUESTION 284
- (Exam Topic 3)
The chief security officer (CS0) 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 288
- (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 291
- (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 292
- (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 297
- (Exam Topic 3)
For each of the given items, select the appropriate authentication category from the drop down choices. Select the appropriate authentication type for the following items:

Item	Response

Fingerprint scan

Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication

Hardware token

Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication

Smart card

Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication

Password

Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication

PIN number

Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication

Retina Scan

Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Item	Response
Fingerprint scan	**Biometric authentication**
	One Time Password
	Multi-factor
	PAP authentication
	PAP authentication
	Biometric authentication
Hardware token	Biometric authentication
	One Time Password
	Multi-factor
	PAP authentication
	PAP authentication
	Biometric authentication
Smart card	Biometric authentication
	One Time Password
	Multi-factor
	PAP authentication
	PAP authentication
	Biometric authentication
Password	Biometric authentication
	One Time Password
	Multi-factor
	PAP authentication
	PAP authentication
	Biometric authentication
PIN number	Biometric authentication
	One Time Password
	Multi-factor
	PAP authentication
	PAP authentication
	Biometric authentication

Retina Scan

Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication

NEW QUESTION 301
- (Exam Topic 3)
A security administrator has been asked to implement a VPN that will support remote access over IPSEC. Which of the following is an encryption algorithm that would meet this requirement?

A. MD5
B. AES
C. UDP
D. PKI

Answer: B

NEW QUESTION 304
- (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 309
- (Exam Topic 3)
Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network. This is MOST likely which of the following types of attacks?

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

Answer: A

NEW QUESTION 314
- (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 317
- (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 320
- (Exam Topic 3)
A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations. Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)

A. SCP
B. TFTP
C. SNMP
D. FTP
E. SMTP
F. FTPS

Answer: AF

NEW QUESTION 325
- (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 328
- (Exam Topic 3)
Which of the following is the summary of loss for a given year?

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

Answer: B

NEW QUESTION 331
- (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 332
- (Exam Topic 3)
A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code. Which of the following assessment techniques is BEST described in the analyst's report?

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

Answer: D

NEW QUESTION 337
- (Exam Topic 3)
Which of the following can affect electrostatic discharge in a network operations center?

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

Answer: D

NEW QUESTION 339
- (Exam Topic 3)
Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

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

Answer: D

NEW QUESTION 340
- (Exam Topic 3)
While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security?

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

Answer: A

NEW QUESTION 343
- (Exam Topic 3)
A computer on a company network was infected with a zero-day exploit after an employee accidently opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidently opened it. Which of the following should be done to prevent this scenario from occurring again in the future?

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

Answer: C

NEW QUESTION 345
- (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 348
- (Exam Topic 3)
During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions. Which of the following would help reduce the amount of risk the organization incurs in this situation in the future?

A. Time-of-day restrictions
B. User access reviews
C. Group-based privileges
D. Change management policies

Answer: B

NEW QUESTION 349
- (Exam Topic 3)
Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

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

Answer: B

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

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

NEW QUESTION 353
- (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 356
- (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 360
- (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 365
- (Exam Topic 3)
During an application design, the development team specifics 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 369
- (Exam Topic 3)
An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient.
Which of the following capabilities would be MOST appropriate to consider implementing is response to the new requirement?

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

Answer: D

NEW QUESTION 370
- (Exam Topic 3)
Which of the following is the GREATEST risk to a company by allowing employees to physically bring their personal smartphones to work?

A. Taking pictures of proprietary information and equipment in restricted areas.
B. Installing soft token software to connect to the company's wireless network.
C. Company cannot automate patch management on personally-owned devices.
D. Increases the attack surface by having more target devices on the company's campus

Answer: A

NEW QUESTION 372
- (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 severs at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?
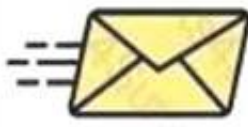
A. Implement deduplication at the network level between the two locations
B. Implement deduplication on the storage array to reduce the amount of drive space needed
C. Implement deduplication on the server storage to reduce the data backed up
D. Implement deduplication on both the local and remote servers

Answer: B

NEW QUESTION 375
- (Exam Topic 3)
Task: Determine the types of attacks below by selecting an option from the dropdown list.

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 376
- (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 379
- (Exam Topic 3)
The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administer has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled. Which of the following would further obscure the presence of the wireless network?

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

Answer: D

NEW QUESTION 383
- (Exam Topic 3)
A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks. Which of the following is the reason the manager installed the racks this way?

A. To lower energy consumption by sharing power outlets
B. To create environmental hot and cold isles
C. To eliminate the potential for electromagnetic interference
D. To maximize fire suppression capabilities

Answer: B

NEW QUESTION 388
- (Exam Topic 3)
An administrator discovers the following log entry on a server: Nov 12 2013 00:23:45 httpd[2342]:
GET/app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadow
Which of the following attacks is being attempted?

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

Answer: B

NEW QUESTION 389
- (Exam Topic 3)
Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop. Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's laptop directly?

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

Answer: B

NEW QUESTION 393
- (Exam Topic 3)
A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage.
Which of the following should be implemented?

A. Recovery agent
B. Ocsp
C. Crl
D. Key escrow

Answer: B

NEW QUESTION 397
- (Exam Topic 3)
AChief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net). Which of the following rules is preventing the CSO from accessing the site?
Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

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

Answer: C

NEW QUESTION 402
- (Exam Topic 3)
Drag and drop the correct protocol to its default port.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
FTP uses TCP port 21. Telnet uses port 23. SSH uses TCP port 22.
All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). SMTP uses TCP port 25. Port 69 is used by TFTP. SNMP makes use of UDP ports 161 and 162. http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION 407
- (Exam Topic 3)
After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

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

Answer: D

NEW QUESTION 411
- (Exam Topic 3)
Which of the following are MOST susceptible to birthday attacks?

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

Answer: A

NEW QUESTION 415
- (Exam Topic 3)
A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.
Which of the following has the administrator been tasked to perform?

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

Answer: D

NEW QUESTION 420
- (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 424
- (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 428
- (Exam Topic 4)
In determining when it may be necessary to perform a credentialed scan against a system instead of a noncredentialed scan, which of the following requirements is MOST likely to influence this decision?

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

D. The scanner must be able to audit file system permissions

Answer: D

NEW QUESTION 431
- (Exam Topic 4)
A security administrator wants to implement a logon script that will prevent MITM attacks on the local LAN. Which of the following commands should the security administrator implement within the script to accomplish this task?

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

Answer: A

NEW QUESTION 436
- (Exam Topic 4)
To determine the ALE of a particular risk, which of the following must be calculated? (Select two.)

A. ARO
B. ROI
C. RPO
D. SLE
E. RTO

Answer: AD

NEW QUESTION 441
- (Exam Topic 4)
Which of the following is the BEST choice for a security control that represents a preventive and corrective logical control at the same time?

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

Answer: B

NEW QUESTION 445
- (Exam Topic 4)
A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computers without exception. Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?

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

Answer: C

NEW QUESTION 449
- (Exam Topic 4)
A security administrator suspects that data on a server has been exhilarated as a result of un- authorized remote access. Which of the following would assist the administrator in con-firming the suspicions? (Select TWO)

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

Answer: BC

NEW QUESTION 452
- (Exam Topic 4)
Which of the following strategies should a systems architect use to minimize availability risks due to insufficient storage capacity?

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

Answer: B

NEW QUESTION 456
- (Exam Topic 4)
Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

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

Answer: C

NEW QUESTION 457
- (Exam Topic 4)
Ann, a security administrator, wants to ensure credentials are encrypted in transit when implementing a RADIUS server for SSO. Which of the following are needed given these requirements? (Select TWO)

A. Public key
B. Shared key
C. Elliptic curve
D. MD5
E. Private key
F. DES

Answer: AE

NEW QUESTION 460
- (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 462
- (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 467
- (Exam Topic 4)
A security analyst is working on a project that requires the implementation of a stream cipher. Which of the following should the analyst use?

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

Answer: C

NEW QUESTION 472
- (Exam Topic 4)
An organization is trying to decide which type of access control is most appropriate for the network. The current access control approach is too complex and requires significant overhead. Management would like to simplify the access control and provide user with the ability to determine what permissions should be applied to files, document, and directories. The access control method that BEST satisfies these objectives is:

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

Answer: D

NEW QUESTION 473
- (Exam Topic 4)
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 475
- (Exam Topic 4)
A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL. Which of the following is the attacker most likely utilizing?

A. Header manipulation
B. Cookie hijacking
C. Cross-site scripting
D. Xml injection

Answer: A

NEW QUESTION 478
- (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 483
- (Exam Topic 4)
As part of a new BYOD rollout, a security analyst has been asked to find a way to securely store company data on personal devices. Which of the following would BEST help to accomplish this?

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

Answer: B

NEW QUESTION 487
- (Exam Topic 4)
Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

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

Answer: A

NEW QUESTION 492
- (Exam Topic 4)
Many employees are receiving email messages similar to the one shown below:
From IT department To employee Subject email quota exceeded Pease click on the following link http:www.website.info/email.php?quota=1Gb and provide your username and password to increase your email quotA. Upon reviewing other similar emails, the security administrator realized that all the phishing URLs have the following common elements; they all use HTTP, they all come from .info domains, and they all contain the same URI. Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?

A. BLOCKhttp://www.*.info/ "
B. DROPhttp:// "website.info/email.php?*
C. Redirecthttp://www,*.Info/email.php?quota=*TOhttp://company.com/corporate_polict.html
D. DENYhttp://*.info/email.php?quota=1Gb

Answer: D

NEW QUESTION 493
- (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 498
- (Exam Topic 4)
A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network. The access the server using RDP on a port other than the typical registered port for the RDP protocol?

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

Answer: A

NEW QUESTION 500
- (Exam Topic 4)
The POODLE attack is an MITM exploit that affects:

A. TLS1.0 with CBC mode cipher
B. SSLv2.0 with CBC mode cipher
C. SSLv3.0 with CBC mode cipher
D. SSLv3.0 with ECB mode cipher

Answer: C

Explanation:
A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
How To Protect your Server Against the POODLE SSLv3 Vulnerability On October 14th, 2014, a vulnerability in version 3 of the SSL encryption protocol was disclosed. This vulnerability, dubbed POODLE (Padding Oracle On Downgraded Legacy Encryption), allows an attacker to read information encrypted with this version of the protocol in plain text using a man-in-the-middle attack.
Although SSLv3 is an older version of the protocol which is mainly obsolete, many pieces of software still fall back on SSLv3 if better encryption options are not available. More importantly, it is possible for an attacker to force SSLv3 connections if it is an available alternative for both participants attempting a connection. The POODLE vulnerability affects any services or clients that make it possible to communicate using SSLv3. Because this is a flaw with the protocol design, and not an implementation issue, every piece of software that uses SSLv3 is vulnerable.
To find out more information about the vulnerability, consult the CVE information found at CVE-2014-3566. What is the POODLE Vulnerability?
The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-inthe-middle context to decipher the plain text content of an SSLv3 encrypted message.
Who is Affected by this Vulnerability?
This vulnerability affects every piece of software that can be coerced into communicating with SSLv3. This means that any software that implements a fallback mechanism that includes SSLv3 support is vulnerable and can be exploited.
Some common pieces of software that may be affected are web browsers, web servers, VPN servers, mail servers, etc.
How Does It Work?
In short, the POODLE vulnerability exists because the SSLv3 protocol does not adequately check the padding bytes that are sent with encrypted messages.
Since these cannot be verified by the receiving party, an attacker can replace these and pass them on to the intended destination. When done in a specific way, the modified payload will potentially be accepted by the recipient without complaint.
An average of once out of every 256 requests will accepted at the destination, allowing the attacker to decrypt a single byte. This can be repeated easily in order to progressively decrypt additional bytes. Any attacker able to repeatedly force a participant to resend data using this protocol can break the encryption in a very short amount of time.
How Can I Protect Myself?
Actions should be taken to ensure that you are not vulnerable in your roles as both a client and a server. Since encryption is usually negotiated between clients and servers, it is an issue that involves both parties.
Servers and clients should should take steps to disable SSLv3 support completely. Many applications use better encryption by default, but implement SSLv3 support as a fallback option.
This should be disabled, as a malicious user can force SSLv3 communication if both participants allow it as an acceptable method.

NEW QUESTION 505
- (Exam Topic 4)
After a security incident, management is meeting with involved employees to document the incident and its aftermath. Which of the following BEST describes this phase of the incident response process?

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

Answer: A

NEW QUESTION 510
- (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 511
- (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 514
- (Exam Topic 4)
An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity. Which of the following actions will help detect attacker attempts to further alter log files?

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

Answer: C

NEW QUESTION 517
- (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 520
- (Exam Topic 4)
The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts. Which of the following controls should be implemented to curtail this activity?

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

Answer: D

NEW QUESTION 523
- (Exam Topic 4)
Which of the following is the BEST reason for salting a password hash before it is stored in a database?

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

Answer: A

NEW QUESTION 526
- (Exam Topic 4)
Which of the following could help detect trespassers in a secure facility? (Select TWO)

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

Answer: BD

NEW QUESTION 528

- (Exam Topic 4)
Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

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

Answer: D

NEW QUESTION 530
- (Exam Topic 4)
The administrator installs database software to encrypt each field as it is written to disk. Which of the following describes the encrypted data?

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

Answer: B

NEW QUESTION 531
- (Exam Topic 4)
When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

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

Answer: C

NEW QUESTION 536
- (Exam Topic 4)
A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network. Which of the following is the MOST likely method used to gain access to the other host?

A. Backdoor
B. Pivoting
C. Persistance
D. Logic bomp

Answer: B

NEW QUESTION 537
- (Exam Topic 4)
An external contractor, who has not been given information about the software or network architecture, is conducting a penetration test. Which of the following BEST describes the test being performed?

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

Answer: A

NEW QUESTION 538
- (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 541
- (Exam Topic 4)
A network administrator adds an ACL to allow only HTTPS connections form host 192.168.2.3 to web server 192.168.5.2. After applying the rule, the host is unable to access the server. The network administrator runs the output and notices the configuration below:

```
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.1682.3 eq 443 host 192.168.5.2
```

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

A

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

B

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

C

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

D

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

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

Answer: A

NEW QUESTION 543
- (Exam Topic 4)
An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server. Which of the following will most likely fix the uploading issue for the users?

A. Create an ACL to allow the FTP service write access to user directories
B. Set the Boolean selinux value to allow FTP home directory uploads
C. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
D. Configure the FTP daemon to utilize PAM authentication pass through user permissions

Answer: A

NEW QUESTION 547
- (Exam Topic 4)
A security administrator wants to configure a company's wireless network in a way that will prevent wireless clients from broadcasting the company's SSID.
Which of the following should be configured on the company's access points?

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

Answer: F

NEW QUESTION 551
- (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 555
- (Exam Topic 5)
Which of the following metrics are used to calculate the SLE? (Select TWO)

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

Answer: BC

NEW QUESTION 560
- (Exam Topic 5)
Every morning, a systems administrator monitors failed login attempts on the company's log management server. The administrator notices the DBAdmin account has five failed username and/or password alerts during a ten-minute window. The systems administrator determines the user account is a dummy account used to attract attackers. Which of the following techniques should the systems administrator implement?

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

Answer: B

NEW QUESTION 565
- (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 570
- (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 573
- (Exam Topic 5)
A security analyst is reviewing an assessment report that includes software versions, running services, supported encryption algorithms, and permission settings. Which of the following produced the report?

A. Vulnerability scanner
B. Protocol analyzer
C. Network mapper
D. Web inspector

Answer: A

NEW QUESTION 577
- (Exam Topic 5)
A malicious system continuously sends an extremely large number of SYN packets to a server. Which of the following BEST describes the resulting effect?

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

Answer: D

NEW QUESTION 580
- (Exam Topic 5)
A security administrator is reviewing the following PowerShell script referenced in the Task Scheduler on a database server:

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

Which of the following did the security administrator discover?

A. Ransomeware
B. Backdoor
C. Logic bomb
D. Trojan

Answer: C

NEW QUESTION 581
- (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 585
- (Exam Topic 5)
A security analyst is reviewing patches on servers. One of the servers is reporting the following error message in the WSUS management console:
The computer has not reported status in 30 days.
Given this scenario, which of the following statements BEST represents the issue with the output above?

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

Answer: D

NEW QUESTION 586
- (Exam Topic 5)
Which of the following authentication concepts is a gait analysis MOST closely associated?

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

Answer: C

NEW QUESTION 591
- (Exam Topic 5)
A security architect has convened a meeting to discuss an organization's key management policy. The organization has a reliable internal key management system, and some argue that it would be best to manage the cryptographic keys internally as opposed to using a solution from a third party. The company should use:

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

Answer: C

NEW QUESTION 594
- (Exam Topic 5)
An organization has implemented an IPSec VPN access for remote users. Which of the following IPSec modes would be the MOST secure for this organization to implement?

A. Tunnel mode
B. Transport mode

C. AH-only mode
D. ESP-only mode

Answer: A

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

NEW QUESTION 596
- (Exam Topic 5)
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:
c:\nslookup - querytype=MX comptia.org
Server: Unknown Address: 198.51.100.45
comptia.org MX preference=10, mail exchanger = 92.68.102.33 comptia.org MX preference=20, mail exchanger = exchg1.comptia.org exchg1.comptia.org internet address = 192.168.102.67
Which of the following should the penetration tester conclude about the command output?

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

Answer: D

NEW QUESTION 597
- (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 602
- (Exam Topic 5)
A security analyst is hardening a WiFi infrastructure. The primary requirements are the following:

▶ The infrastructure must allow staff to authenticate using the most secure method.

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

A. Configure a captive portal for guests and WPS for staff.
B. Configure a captive portal for staff and WPA for guests.
C. Configure a captive portal for staff and WEP for guests.
D. Configure a captive portal for guest and WPA2 Enterprise for staff

Answer: D

NEW QUESTION 607
- (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 612
- (Exam Topic 5)
Which of the following types of penetration test will allow the tester to have access only to password hashes prior to the penetration test?

A. Black box
B. Gray box
C. Credentialed

D. White box

Answer: B

NEW QUESTION 615
- (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 620
- (Exam Topic 5)
A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials. Which of the following account types is the systems administrator using?

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

Answer: C

NEW QUESTION 624
- (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 627
- (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 629
- (Exam Topic 5)
Systems administrator and key support staff come together to simulate a hypothetical interruption of service. The team updates the disaster recovery processes and documentation after meeting. Which of the following
describes the team's efforts?

A. Business impact analysis
B. Continuity of operation
C. Tabletop exercise
D. Order of restoration

Answer: C

NEW QUESTION 633
- (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 636
- (Exam Topic 5)
A remote intruder wants to take inventory of a network so exploits can be researched. The intruder is looking for information about software versions on the network. Which of the following techniques is the intruder using?

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

Answer: A

NEW QUESTION 639
- (Exam Topic 5)
A security auditor is testing perimeter security in a building that is protected by badge readers. Which of the following types of attacks would MOST likely gain access?

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

Answer: C

NEW QUESTION 640
- (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 643
- (Exam Topic 5)
A software developer is concerned about DLL hijacking in an application being written. Which of the following is the MOST viable mitigation measure of this type of attack?

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

Answer: B

NEW QUESTION 646
- (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 648
- (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 652
- (Exam Topic 5)
A recent internal audit is forcing a company to review each internal business unit's VMs because the cluster they are installed on is in danger of running out of computer resources. Which of the following vulnerabilities exist?

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

Answer: C

NEW QUESTION 656
- (Exam Topic 5)
A user downloads and installs an MP3 converter, and runs the application. Upon running the application, the antivirus detects a new port in a listening state. Which of the following has the user MOST likely executed?

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

Answer: A

NEW QUESTION 657
- (Exam Topic 5)
When attempting to secure a mobile workstation, which of the following authentication technologies rely on the user's physical characteristics? (Select TWO)

A. MAC address table
B. Retina scan
C. Fingerprint scan
D. Two-factor authentication
E. CAPTCHA
F. Password string

Answer: BC

NEW QUESTION 658
- (Exam Topic 5)
Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization's incident response capabilities. Which of the following activities has the incident team lead executed?

A. Lessons learned review
B. Root cause analysis
C. Incident audit
D. Corrective action exercise

Answer: A

NEW QUESTION 663
- (Exam Topic 5)
A penetration tester has written an application that performs a bit-by-bit XOR 0xFF operation on binaries prior to transmission over untrusted mediA. Which of the following BEST describes the action performed by this type of application?

A. Hashing
B. Key exchange
C. Encryption
D. Obfusication

Answer: D

NEW QUESTION 664
- (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 669
- (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 672
- (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 674
- (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 677
- (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 682
- (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 686
- (Exam Topic 5)
A user receives an email from ISP indicating malicious traffic coming from the user's home network is detected. The traffic appears to be Linux-based, and it is targeting a website that was recently featured on the news as being taken offline by an Internet attack. The only Linux device on the network is a home surveillance camera system.
Which of the following BEST describes what is happening?

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

Answer: A

NEW QUESTION 689
- (Exam Topic 5)
Which of the following is a deployment concept that can be used to ensure only the required OS access is exposed to software applications?

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

Answer: B

NEW QUESTION 693
- (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 697
- (Exam Topic 5)
Ann, a customer, is reporting that several important files are missing from her workstation. She recently
received communication from an unknown party who is requesting funds to restore the files. Which of the following attacks has occurred?

A. Ransomware
B. Keylogger
C. Buffer overflow
D. Rootkit

Answer: A

NEW QUESTION 700
- (Exam Topic 5)
AChief 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 704
- (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 705

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 707

- (Exam Topic 5)

A bank uses a wireless network to transmit credit card purchases to a billing system.
Which of the following would be MOST appropriate to protect credit card information from being accessed by unauthorized individuals outside of the premises?

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

Answer: C

NEW QUESTION 708

- (Exam Topic 5)

Confidential emails from an organization were posted to a website without the organization's knowledge. Upon investigation, it was determined that the emails
were obtained from an internal actor who sniffed the emails in plain text. Which of the following protocols, if properly implemented, would have MOST likely
prevented the emails from being sniffed? (Select TWO)

A. Secure IMAP
B. DNSSEC
C. S/MIME
D. SMTPS
E. HTTPS

Answer: CD

NEW QUESTION 713

......

Thank You for Trying Our Product

* 100% Pass or Money Back

   All our products come with a 90-day Money Back Guarantee.

* One year free update

   You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

   We currently serve more than 30,000,000 customers.

* Shop Securely

   All transactions are protected by VeriSign!

100% Pass Your SY0-501 Exam with Our Prep Materials Via below:

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