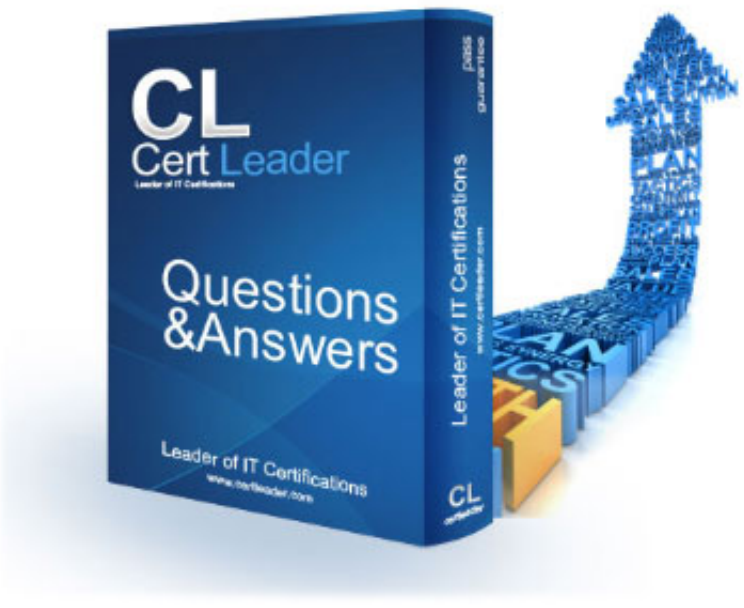
# SY0-501 Dumps

# CompTIA Security+ Certification Exam

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



**NEW QUESTION 1**
- (Exam Topic 1)
Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications. Which of the following best describes what she will do?

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

**Answer:** A

**NEW QUESTION 2**
- (Exam Topic 1)
A company has 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 3**
- (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 4**
- (Exam Topic 1)
A company wants to host a publicity available server that performs the following functions:
Evaluates MX record lookup
Can perform authenticated requests for A and AAA records
Uses RRSIG
Which of the following should the company use to fulfill the above requirements?

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

**Answer:** B

**NEW QUESTION 5**
- (Exam Topic 1)
A user clicked an email link that led to a website than infected the workstation with a virus. The virus encrypted all the network shares to which the user had access. The virus was not deleted or blocked by the company’s email filter, website filter, or antivirus. Which of the following describes what occurred?

A. The user’s account was over-privileged.
B. Improper error handling triggered a false negative in all three controls.
C. The email originated from a private email server with no malware protection.
D. The virus was a zero-day attack.

**Answer:** A

**NEW QUESTION 6**
- (Exam Topic 1)
Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

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

**Answer:** A

**NEW QUESTION 7**
- (Exam Topic 1)
Which of the following best describes routine in which semicolons, dashes, quotes, and commas are removed from a string?

A. Error handling to protect against program exploitation
B. Exception handling to protect against XSRF attacks.
C. Input validation to protect against SQL injection.
D. Padding to protect against string buffer overflows.

**Answer:** C

**NEW QUESTION 8**
- (Exam Topic 1)
An information security specialist is reviewing the following output from a Linux server.

```
user@server:~$ crontab -1
5 * * * *  /usr/local/bin/backup.sh
user@server: ~$ cat /usr/local/bin/backup.sh
#!/bin/bash
if ! grep - - quiet joeuser/etc/passwd
then rm –rf /
fi
```

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

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

**Answer:** C

**NEW QUESTION 9**
- (Exam Topic 1)
A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network. Which of the following should be implemented in the administrator does not want to provide the wireless password or he certificate to the employees?

A. WPS
B. 802.1x
C. WPA2-PSK
D. TKIP

**Answer:** A

**NEW QUESTION 10**
- (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)
Which of the following can be provided to an AAA system for the identification phase?

A. Username
B. Permissions
C. One-time token
D. Private certificate

**Answer:** A

**NEW QUESTION 15**
- (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 17**
- (Exam Topic 1)
A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

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

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

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

**Answer:** ACG

**NEW QUESTION 22**
- (Exam Topic 1)
A high-security defense installation recently begun utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation. Which of the following types of controls does this BEST describe?

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

**Answer:** A

**NEW QUESTION 26**
- (Exam Topic 1)
Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Which of the following should be used to sign the user's certificates?

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

**Answer:** B

**NEW QUESTION 29**
- (Exam Topic 1)
An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT?

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

**Answer:** A

**NEW QUESTION 32**
- (Exam Topic 1)
A company determines that it is prohibitively expensive to become compliant with new credit card regulations. Instead, the company decides to purchase insurance to cover the cost of any potential loss. Which of the following is the company doing?

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

**Answer:** A

**NEW QUESTION 34**
- (Exam Topic 1)
Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone. Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Select two.)

A. Near-field communication.
B. Rooting/jailbreaking
C. Ad-hoc connections
D. Tethering
E. Sideloading

**Answer:** BE

**NEW QUESTION 37**
- (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 39**
- (Exam Topic 1)
Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords. Which of the following technical controls would help prevent these policy violations? (Select two.)

A. Password expiration
B. Password length
C. Password complexity
D. Password history
E. Password lockout

**Answer:** CD

**NEW QUESTION 43**
- (Exam Topic 1)
A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees.
Which of the following would provide strong security and backward compatibility when accessing the wireless network?

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

**Answer:** C

**NEW QUESTION 47**
- (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 48**
- (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

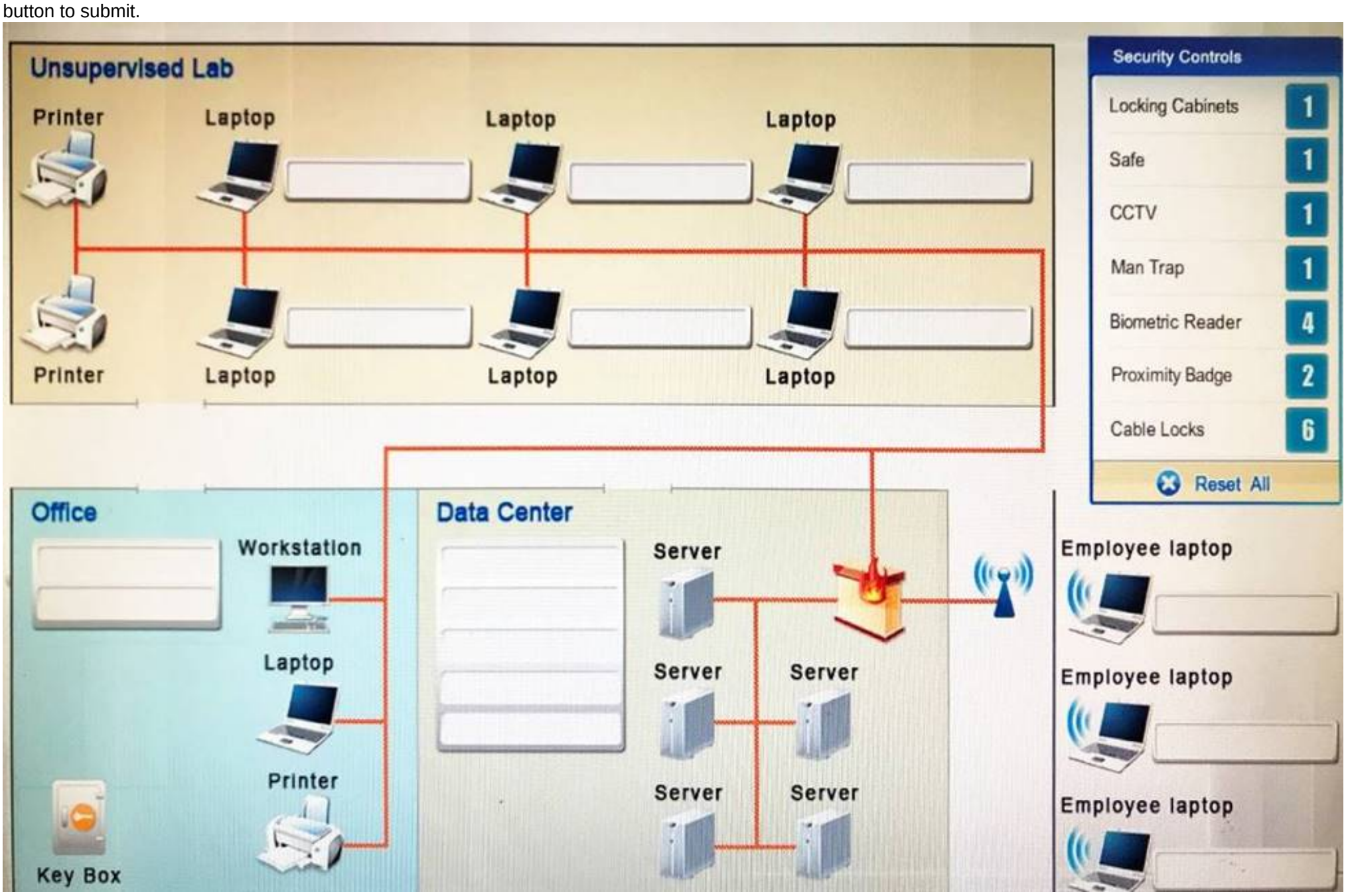
**Answer:** B

**NEW QUESTION 51**
- (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)
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 60**
- (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 64**
- (Exam Topic 1)
Which of the following encryption methods does PKI typically use to securely project keys?

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

**Answer:** C

**NEW QUESTION 68**
- (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 72**
- (Exam Topic 1)
A security analyst is reviewing the following output from an IPS:

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

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

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

**Answer:** BC

**NEW QUESTION 73**
- (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 74**
- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 75**
- (Exam Topic 1)
An organization needs to implement a large PKI. Network engineers are concerned that repeated transmission of the OCSP will impact network performance. Which of the following should the security analyst recommend is lieu of an OCSP?

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

**Answer:** B

**NEW QUESTION 77**
- (Exam Topic 1)
A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select two.)

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

**Answer:** AD

**NEW QUESTION 78**
- (Exam Topic 1)
An employer requires that employees use a key-generating app on their smartphones to log into corporate applications. In terms of authentication of an individual, this type of access policy is BEST defined as:

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

**Answer:** A

**NEW QUESTION 79**
- (Exam Topic 1)
A penetration tester is crawling a target website that is available to the public. Which of the following represents the actions the penetration tester is performing?

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

**Answer:** B

**NEW QUESTION 84**
- (Exam Topic 1)
A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

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

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

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

**Answer:** C

**NEW QUESTION 87**
- (Exam Topic 1)
When 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 90**
- (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 91**
- (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 95**
- (Exam Topic 2)
Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

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

**Answer:** D

**NEW QUESTION 96**
- (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 98**
- (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 101**
- (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 102**
- (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 107**
- (Exam Topic 2)
Which of the following AES modes of operation provide authentication? (Select two.)

A. CCM
B. CBC
C. GCM
D. DSA
E. CFB

**Answer:** AC

**NEW QUESTION 111**
- (Exam Topic 2)
A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a
brute force attack on all accounts that has been previously logged into that machine.
Which of the following can be implemented to reduce the likelihood of this attack going undetected?

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

**Answer:** B

**NEW QUESTION 112**
- (Exam Topic 2)
Which of the following differentiates a collision attack from a rainbow table attack?

A. A rainbow table attack performs a hash lookup
B. A rainbow table attack uses the hash as a password
C. In a collision attack, the hash and the input data are equivalent
D. In a collision attack, the same input results in different hashes

**Answer:** A

**NEW QUESTION 115**
- (Exam Topic 2)
A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle.
Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle?

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

**Answer:** D

**NEW QUESTION 119**
- (Exam Topic 2)
A company is developing a new system that will unlock a computer automatically when an authorized user sits in front of it, and then lock the computer when the user leaves. The user does not have to perform any action for this process to occur. Which of the following technologies provides this capability?

A. Facial recognition
B. Fingerprint scanner
C. Motion detector
D. Smart cards

**Answer:** A

**NEW QUESTION 120**
- (Exam Topic 2)
Before an infection was detected, several of the infected devices attempted to access a URL that was similar to the company name but with two letters transposed.
Which of the following BEST describes the attack vector used to infect the devices?

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

**Answer:** C

**NEW QUESTION 125**
- (Exam Topic 2)
A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account. This is an example of which of the following attacks?

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

**Answer:** C

**NEW QUESTION 127**
- (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 128**
- (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 129**
- (Exam Topic 2)
The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN.
Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance
C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

**Answer:** C

**NEW QUESTION 133**
- (Exam Topic 2)
A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts.
Which of the following subnets would BEST meet the requirements?

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

**Answer:** B

**NEW QUESTION 135**
- (Exam Topic 2)
A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization. Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?

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

**Answer:** B

**NEW QUESTION 139**
- (Exam Topic 2)
The availability of a system has been labeled as the highest priority. Which of the following should be focused on the MOST to ensure the objective?

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

**Answer:** B

**NEW QUESTION 144**
- (Exam Topic 2)
An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request.
Which of the following secure protocols is the developer MOST likely to use?

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

**Answer:** C

**NEW QUESTION 146**
- (Exam Topic 2)
A user of the wireless network is unable to gain access to the network. The symptoms are:
1.) Unable to connect to both internal and Internet resources
2.) The wireless icon shows connectivity but has no network access
The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.
Which of the following is the MOST likely cause of the connectivity issues?

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

**Answer:** A

**NEW QUESTION 149**
- (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 152**
- (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 153**
- (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 158**
- (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 163**
- (Exam Topic 2)
A security administrator is configuring a new network segment, which contains devices that will be accessed by external users, such as web and FTP server. Which of the following represents the MOST secure way to configure the new network segment?

A. The segment should be placed on a separate VLAN, and the firewall rules should be configured to allow external traffic.
B. The segment should be placed in the existing internal VLAN to allow internal traffic only.
C. The segment should be placed on an intranet, and the firewall rules should be configured to allow external traffic.
D. The segment should be placed on an extranet, and the firewall rules should be configured to allow both internal and external traffic.

**Answer:** A

**NEW QUESTION 165**
- (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 166**
- (Exam Topic 3)
An organization is moving its human resources system to a cloud services provider.

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

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

**Answer:** D

**NEW QUESTION 169**
- (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 174**
- (Exam Topic 3)
Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain. Which of the following tools would aid her to decipher the network traffic?

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

**Answer:** C

**NEW QUESTION 176**
- (Exam Topic 3)
An employee uses RDP to connect back to the office network. If RDP is misconfigured, which of the following security exposures would this lead to?

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

**Answer:** D

**NEW QUESTION 181**
- (Exam Topic 3)
The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.
Which of the following categories BEST describes what she is looking for?

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

**Answer:** D

**NEW QUESTION 186**
- (Exam Topic 3)
Given the log output:
Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS:
Login Success [user: msmith] [Source: 10.0.12.45] [localport: 23] at 00:15:23:431 CET Sun Mar 15 2015
Which of the following should the network administrator do to protect data security?

A. Configure port security for logons
B. Disable telnet and enable SSH
C. Configure an AAA server
D. Disable password and enable RSA authentication

**Answer:** B

**NEW QUESTION 191**
- (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 193**
- (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 194**
- (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 195**
- (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 199**
- (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 200**
- (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 204**
- (Exam Topic 3)
A technician must configure a firewall to block external DNS traffic from entering a network. Which of the following ports should they block on the firewall?

A. 53
B. 110
C. 143

D. 443

**Answer:** A

**NEW QUESTION 209**
- (Exam Topic 3)
Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data. Which of the following controls can be implemented to mitigate this type of inside threat?

A. Digital signatures
B. File integrity monitoring
C. Access controls
D. Change management
E. Stateful inspection firewall

**Answer:** B

**NEW QUESTION 214**
- (Exam Topic 3)
The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred. By doing which of the following is the CSO most likely to reduce the number of incidents?

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

**Answer:** C

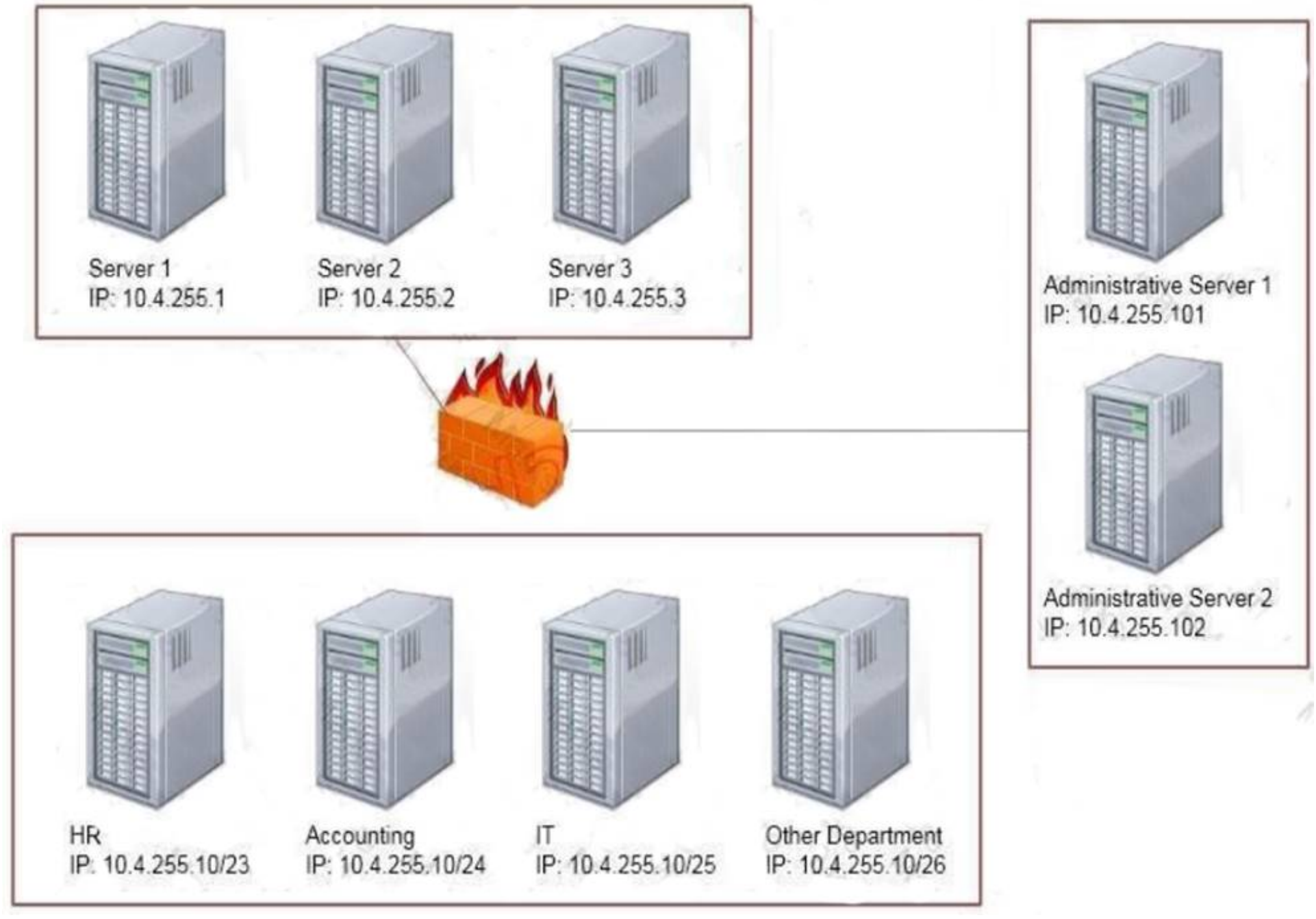
**NEW QUESTION 218**
- (Exam Topic 3)
An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection. Which of the following AES modes of operation would meet this integrity-only requirement?

A. HMAC
B. PCBC
C. CBC
D. GCM
E. CFB

**Answer:** A

**NEW QUESTION 223**
- (Exam Topic 3)
Task: Configure the firewall (fill out the table) to allow these four rules:

- Only allow the Accounting computer to have HTTPS access to the Administrative server.
- Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
- Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2




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

A. Mastered
B. Not Mastered

**Answer:** A

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

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

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria:
Block the connection Allow the connection Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent.
Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session.
When the session ends, the connection is torn down.
UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP.
The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications.
The primary purpose of UDP is to send small packets of information.
The application is responsible for acknowledging the correct reception of the data. Port 22 is used by both SSH and SCP with UDP.
Port 443 is used for secure web connections? HTTPS and is a TCP port.
Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)
Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between: 10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)
10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

**NEW QUESTION 226**
- (Exam Topic 3)
The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected. Which of the following is required to complete the certificate chain?

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

**Answer:** B

**NEW QUESTION 227**
- (Exam Topic 3)
A security administrator is evaluating three different services: radius, diameter, and Kerberos. Which of the following is a feature that is UNIQUE to Kerberos?

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

**Answer:** B

**NEW QUESTION 230**
- (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 233**
- (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 234**
- (Exam Topic 3)
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

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

**Answer:** C

**NEW QUESTION 236**
- (Exam Topic 3)
A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued. Which of the following should the administrator submit to receive a new certificate?

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

**Answer:** D

**NEW QUESTION 237**
- (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 241**
- (Exam Topic 3)
Having adequate lighting on the outside of a building is an example of which of the following security controls?

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

**Answer:** A

**NEW QUESTION 242**
- (Exam Topic 4)
A datacenter manager has been asked to prioritize critical system recovery priorities. Which of the following is the MOST critical for immediate recovery?

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

**Answer:** B

**NEW QUESTION 243**
- (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 245**
- (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 249**
- (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 251**
- (Exam Topic 4)
A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

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

**Answer:** C

**NEW QUESTION 252**
- (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 254**
- (Exam Topic 4)
A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert. Which of the following methods has MOST likely been used?

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

**Answer:** E

**NEW QUESTION 255**
- (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 257**
- (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 261**
- (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 266**
- (Exam Topic 4)
Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select Two)

A. SQL injection
B. Session hijacking
C. Cross-site scripting
D. Locally shared objects
E. LDAP injection

**Answer:** BC

**NEW QUESTION 267**
- (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 268**
- (Exam Topic 4)
An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography. Discovery of which of the following would help catch the tester in the act?

A. Abnormally high numbers of outgoing instant messages that contain obfuscated text
B. Large-capacity USB drives on the tester's desk with encrypted zip files
C. Outgoing emails containing unusually large image files
D. Unusual SFTP connections to a consumer IP address

**Answer:** C

**NEW QUESTION 273**
- (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 277**
- (Exam Topic 4)
A member of the admins group reports being unable to modify the "changes" file on a server. The permissions on the file are as follows:
Permissions User Group File
-rwxrw-r--+ Admins Admins changes
Based on the output above, which of the following BEST explains why the user is unable to modify the "changes" file?

A. The SELinux mode on the server is set to "enforcing."
B. The SELinux mode on the server is set to "permissive."
C. An FACL has been added to the permissions for the file.
D. The admins group does not have adequate permissions to access the file.

**Answer:** C

**NEW QUESTION 282**
- (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 285**
- (Exam Topic 4)
The security administrator has noticed cars parking just outside of the building fence line. Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Select TWO)

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

**Answer:** DE

**NEW QUESTION 288**
- (Exam Topic 4)
Which of the following would allow for the QUICKEST restoration of a server into a warm recovery site in a case in which server data mirroring is not enabled?

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

**Answer:** C

**NEW QUESTION 290**
- (Exam Topic 4)
A web developer improves client access to the company's REST API. Authentication needs to be tokenized but not expose the client's password. Which of the following methods would BEST meet the developer's requirements?

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

**Answer:** A

**NEW QUESTION 293**
- (Exam Topic 4)
A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system.
Which of the following methods should the security administrator select the best balances security and efficiency?

A. Temporarily permit outbound internet access for the pacs so desktop sharing can be set up
B. Have the external vendor come onsite and provide access to the PACS directly
C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing
D. Set up a web conference on the administrator's pc; then remotely connect to the pacs

**Answer:** C

**NEW QUESTION 295**
- (Exam Topic 4)
A wireless network has the following design requirements:

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

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

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

**Answer:** BE

**NEW QUESTION 297**
- (Exam Topic 4)
Security administrators attempted corrective action after a phishing attack. Users are still experiencing trouble logging in, as well as an increase in account lockouts. Users' email contacts are complaining of an increase in spam and social networking requests. Due to the large number of affected accounts, remediation must be accomplished quickly. Which of the following actions should be taken FIRST? (Select TWO)

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

**Answer:** EF

**Explanation:**
Sender Policy Framework (SPF) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators. n a Small Business Server environment, you may have to prevent your Microsoft Exchange Server-based server from being used as an open relay SMTP server for unsolicited commercial e-mail messages, or spam.
You may also have to clean up the Exchange server's SMTP queues to delete the unsolicited commercial email messages.
If your Exchange server is being used as an open SMTP relay, you may experience one or more of the following symptoms:
The Exchange server cannot deliver outbound SMTP mail to a growing list of e-mail domains. Internet browsing is slow from the server and from local area network (LAN) clients.
Free disk space on the Exchange server in the location of the Exchange information store databases or the Exchange information store transaction logs is reduced more rapidly than you expect.
The Microsoft Exchange information store databases spontaneously dismount. You may be able to manually mount the stores by using Exchange System Manager, but the stores may dismount on their own after they run for a short time. For more information, click the following article number to view the article in the Microsoft Knowledge Base.

**NEW QUESTION 299**
- (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 301**
- (Exam Topic 4)
A security analyst is investigating a security breach. Upon inspection of the audit an access logs, the analyst notices the host was accessed and the /etc/passwd file was modified with a new entry for username “gotcha” and user ID of 0. Which of the following are the MOST likely attack vector and tool the analyst should use to determine if the attack is still ongoing? (Select TWO)

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

**Answer:** BD

**NEW QUESTION 305**

- (Exam Topic 4)
Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

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

**Answer:** BD

**NEW QUESTION 307**
- (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 310**
- (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 312**
- (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 315**
- (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 320**
- (Exam Topic 5)
The help desk received a call after hours from an employee who was attempting to log into the payroll server remotely. When the help desk returned the call the next morning, the employee was able to log into the server remotely without incident. However, the incident occurred again the next evening. Which of the following BEST describes the cause of the issue?

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

**Answer:** C

**NEW QUESTION 322**

- (Exam Topic 5)
An office manager found a folder that included documents with various types of data relating to corporate clients. The office manager notified the data included dates of birth, addresses, and phone numbers for the clients. The office manager then reported this finding to the security compliance officer. Which of the following portions of the policy would the security officer need to consult to determine if a breach has occurred?

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

**Answer:** D

**NEW QUESTION 325**
- (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 329**
- (Exam Topic 5)
When sending messages using symmetric encryption, which of the following must happen FIRST?

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

**Answer:** C

**NEW QUESTION 334**
- (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 335**
- (Exam Topic 5)
Which of the following would be considered multifactor authentication?

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

**Answer:** C

**NEW QUESTION 337**
- (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 338**

- (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 340**
- (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 345**
- (Exam Topic 5)
While troubleshooting a client application connecting to the network, the security administrator notices the following error: Certificate is not valid. Which of the following is the BEST way to check if the digital certificate is valid?

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

**Answer:** B

**NEW QUESTION 349**
- (Exam Topic 5)
A user typically works remotely over the holidays using a web-based VPN to access corporate resources. The user reports getting untrusted host errors and being unable to connect. Which of the following is MOST likely the case?

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

**Answer:** A

**NEW QUESTION 351**
- (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 353**
- (Exam Topic 5)
While working on an incident, Joe, a technician, finished restoring the OS and applications on a workstation from the original mediA. Joe is about to begin copying the user's files back onto the hard drive. Which of the following incident response steps is Joe working on now?

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

**Answer:** A

**NEW QUESTION 357**
- (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 362**
- (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 365**
- (Exam Topic 5)
A security administrator is trying to eradicate a worm, which is spreading throughout the organization, using an old remote vulnerability in the SMB protocol. The worm uses Nmap to identify target hosts within the company. The administrator wants to implement a solution that will eradicate the current worm and any future attacks that may be using zero-day vulnerabilities. Which of the following would BEST meet the requirements when implemented?

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

**Answer:** C

**NEW QUESTION 369**
- (Exam Topic 5)
A security administrator installed a new network scanner that identifies new host systems on the network. Which of the following did the security administrator install?

A. Vulnerability scanner
B. Network-based IDS
C. Rogue system detection
D. Configuration compliance scanner

**Answer:** C

**NEW QUESTION 371**
- (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 372**
- (Exam Topic 5)
An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.
Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?

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

**Answer:** B

**NEW QUESTION 375**
- (Exam Topic 5)
An external auditor visits the human resources department and performs a physical security assessment. The auditor observed documents on printers that are unclaimed. A closer look at these documents reveals employee names, addresses, ages, and types of medical and dental coverage options each employee has selected. Which of the following is the MOST appropriate actions to take?

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

**Answer:** D

**NEW QUESTION 379**
- (Exam Topic 5)
An organization has several production-critical SCADA supervisory systems that cannot follow the normal 30-day patching policy. Which of the following BEST maximizes the protection of these systems from malicious software?

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

**Answer:** A

**NEW QUESTION 383**
- (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 385**
- (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 386**
- (Exam Topic 5)
A security administrator has written a script that will automatically upload binary and text-based configuration files onto a remote server using a scheduled task. The configuration files contain sensitive information. Which of the following should the administrator use? (Select TWO)

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

**Answer:** CE

**NEW QUESTION 387**
- (Exam Topic 5)
Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter. Which of the following is being described?

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

**Answer:** A

**NEW QUESTION 391**
- (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 395**
- (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 396**
- (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 400**
- (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 402**
- (Exam Topic 5)
A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized. Which of the following solutions would BEST meet these requirements?

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

**Answer:** B

**NEW QUESTION 403**
- (Exam Topic 5)
Which of the following controls allows a security guard to perform a post-incident review?

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

**Answer:** C

**NEW QUESTION 404**
- (Exam Topic 5)

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

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

**Answer:** D

**Explanation:**
RADIUS generally includes 802.1X that pre-authenticates devices.

**NEW QUESTION 405**
- (Exam Topic 5)
An application was recently compromised after some malformed data came in via web form. Which of the following would MOST likely have prevented this?

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

**Answer:** A

**NEW QUESTION 407**
- (Exam Topic 5)
During a routine vulnerability assessment, the following command was successful:
echo "vrfy 'perl -e 'print "hi" x 500 ' ' " | nc www.company.com 25 Which of the following vulnerabilities is being exploited?

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

**Answer:** A

**NEW QUESTION 411**
- (Exam Topic 5)
A systems administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees. Which of the following would provide strong security and backward compatibility when accessing the wireless network?

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

**Answer:** A

**NEW QUESTION 412**
- (Exam Topic 5)
A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFIenabled baby monitor while the baby's parents were sleeping.
Which of the following BEST describes how the intruder accessed the monitor?

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

**Answer:** D

**NEW QUESTION 414**
- (Exam Topic 5)
AChief Information Officer (CIO) recently saw on the news that a significant security flaws exists with a specific version of a technology the company uses to support many critical application. The CIO wants to know if this reported vulnerability exists in the organization and, if so, to what extent the company could be harmed. Which of the following would BEST provide the needed information?

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

**Answer:** A

**NEW QUESTION 417**
.....

# 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