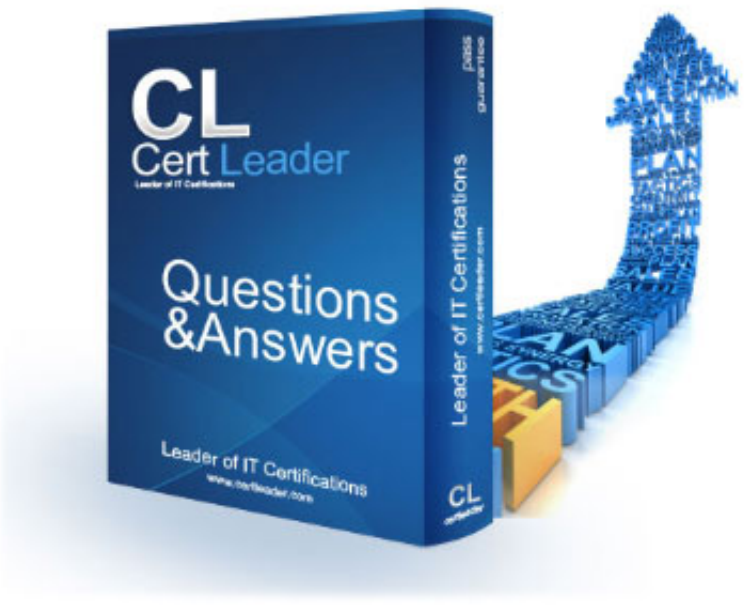
SY0-501 Dumps

CompTIA Security+ Certification Exam

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



NEW QUESTION 1
- (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 2
- (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 3
- (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 4
- (Exam Topic 1)
Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?

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

Answer: C

NEW QUESTION 5
- (Exam Topic 1)
Which of the following would a security specialist be able to determine upon examination of a server's certificate?

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

Answer: D

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

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

Answer: BC

NEW QUESTION 8
- (Exam Topic 1)
When connected to a secure WAP, which of the following encryption technologies is MOST likely to be configured when connecting to WPA2-PSK?

A. DES
B. AES
C. MD5
D. WEP

Answer: B

NEW QUESTION 9
- (Exam Topic 1)
An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment of DNSSEC at the organization?

A. LDAP
B. TPM
C. TLS
D. SSL
E. PKI

Answer: E

NEW QUESTION 10
- (Exam Topic 1)
A security analyst observes the following events in the logs of an employee workstation:

1/23	1:07:16	865	Access to C:\Users\user\temp\oasdfkh.hta has been restricted by your administrator by the default restriction policy level.
1/23	1:07:09	1034	The scan completed. No detections were found.

The security analyst reviews the file system and observes the following:

```
C:\>dir
C:\ Users\user\temp
1/23 1:07:02 oasdfkh.hta
1/23 1:07:02 update.bat
1/23 1:07:02 msg.txt
```

Given the information provided, which of the following MOST likely occurred on the workstation?

A. Application whitelisting controls blocked an exploit payload from executing.
B. Antivirus software found and quarantined three malware files.
C. Automatic updates were initiated but failed because they had not been approved.
D. The SIEM log agent was not tuned properly and reported a false positive.

Answer: A

NEW QUESTION 10
- (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 15
- (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 18
- (Exam Topic 1)
Users report the following message appears when browsing to the company's secure site: This website cannot be trusted. Which of the following actions should a security analyst take to resolve these messages? (Select two.)

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

Answer: AC

NEW QUESTION 21
- (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 25
- (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 28
- (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 31
- (Exam Topic 1)
A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.0:6666. Which of the following should the
security analyst do to determine if the compromised system still has an active connection?

A. tracert
B. netstat
C. ping
D. nslookup

Answer: B

NEW QUESTION 35
- (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 40
- (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 41
- (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 42
- (Exam Topic 1)
Ann. An employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:

Slow performance

Word documents, PDFs, and images no longer opening

A pop-up

Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?

A. Spyware
B. Crypto-malware
C. Rootkit
D. Backdoor

Answer: D

NEW QUESTION 43
- (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 46
- (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 49
- (Exam Topic 1)
A company is currently using the following configuration:

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

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

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

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

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

Answer: AC

NEW QUESTION 52
- (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 55
- (Exam Topic 1)
Which of the following attacks specifically impact data availability?

A. DDoS
B. Trojan
C. MITM
D. Rootkit

Answer: A

Explanation:
Reference: https://www.netscout.com/what-is-ddos

NEW QUESTION 59
- (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 63
- (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 64
- (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 69
- (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 73
- (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 77
- (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 78
- (Exam Topic 2)
After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition.
Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO)

A. Monitor VPN client access
B. Reduce failed login out settings
C. Develop and implement updated access control policies
D. Review and address invalid login attempts
E. Increase password complexity requirements
F. Assess and eliminate inactive accounts

Answer: CF

NEW QUESTION 80
- (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 81
- (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 82
- (Exam Topic 2)
AChief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

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

Answer: D

NEW QUESTION 84
- (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 85
- (Exam Topic 2)
A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable.
Which of the following MUST be implemented to support this requirement?

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

Answer: C

NEW QUESTION 90
- (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 92
- (Exam Topic 2)
Which of the following would meet the requirements for multifactor authentication?

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

Answer: B

NEW QUESTION 95
- (Exam Topic 2)
A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols MUST the security engineer select?

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

Answer: C

NEW QUESTION 97
- (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 100
- (Exam Topic 2)
After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

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

Answer: B

NEW QUESTION 104
- (Exam Topic 2)
A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?

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

Answer: B

NEW QUESTION 107
- (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 112
- (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 113
- (Exam Topic 3)
Phishing emails frequently take advantage of high-profile catastrophes reported in the news. Which of the following principles BEST describes the weakness being

exploited?

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

Answer: D

NEW QUESTION 115
- (Exam Topic 3)
A system administrator is configuring a site-to-site VPN tunnel. Which of the following should be configured on the VPN concentrator during the IKE phase?

A. RIPEMD
B. ECDHE
C. Diffie-Hellman
D. HTTPS

Answer: C

NEW QUESTION 119
- (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 122
- (Exam Topic 3)
After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internetbased control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence. Which of the following is the MOST likely reason the thermostat is not connecting to the internet?

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

Answer: C

NEW QUESTION 125
- (Exam Topic 3)
An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week.
Which of the following would be the BEST method of updating this application?

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

Answer: A

NEW QUESTION 126
- (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 130
- (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 131
- (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 136
- (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 141
- (Exam Topic 3)
A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results. Which of the following is the best method for collecting this information?

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

Answer: A

NEW QUESTION 145
- (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 147
- (Exam Topic 3)
Joe notices there are several user accounts on the local network generating spam with embedded malicious code. Which of the following technical control should Joe put in place to BEST reduce these incidents?

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

Answer: A

NEW QUESTION 148
- (Exam Topic 3)
A Security Officer on a military base needs to encrypt several smart phones that will be going into the field. Which of the following encryption solutions should be deployed in this situation?

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

Answer: D

NEW QUESTION 149
- (Exam Topic 3)
An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure areA. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are. The controls used by the receptionist are in place to prevent which of the following types of attacks?

A. Tailgating
B. Shoulder surfing
C. Impersonation
D. Hoax

Answer: C

NEW QUESTION 152
- (Exam Topic 3)
A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN. Which of the following protocols should be used?

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

Answer: A

NEW QUESTION 156
- (Exam Topic 3)
A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols. Which of the following summarizes the BEST response to the programmer's proposal?

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

Answer: B

NEW QUESTION 161
- (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 165
- (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 169
- (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 174
- (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 177
- (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 180
- (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 181
- (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 185
- (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 189
- (Exam Topic 4)
A security analyst has set up a network tap to monitor network traffic for vulnerabilities. Which of the following techniques would BEST describe the approach the analyst has taken?

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

Answer: D

NEW QUESTION 191
- (Exam Topic 4)
A company would like to prevent the use of a known set of applications from being used on company computers. Which of the following should the security administrator implement?

A. Whitelisting

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

Answer: D

NEW QUESTION 195
- (Exam Topic 4)
Due to regulatory requirements, a security analyst must implement full drive encryption on a Windows file server. Which of the following should the analyst implement on the system to BEST meet this requirement? (Choose two.)

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

Answer: BD

NEW QUESTION 200
- (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 201
- (Exam Topic 4)
The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems.
The help desk is receive reports that users are experiencing the following error when attempting to log in to their previous system:
Logon Failure: Access Denied
Which of the following can cause this issue?

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

Answer: C

NEW QUESTION 204
- (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 207
- (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 208
- (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 211
- (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 214
- (Exam Topic 4)
During a recent audit, it was discovered that many services and desktops were missing security patches. Which of the following BEST describes the assessment that was performed to discover this issue?

A. Network mapping
B. Vulnerability scan
C. Port Scan
D. Protocol analysis

Answer: B

NEW QUESTION 219
- (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 222
- (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 224
- (Exam Topic 4)
Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

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

Answer: D

NEW QUESTION 226
- (Exam Topic 4)
A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?

A. Put the desktops in the DMZ.
B. Create a separate VLAN for the desktops.
C. Air gap the desktops.
D. Join the desktops to an ad-hoc network.

Answer: C

NEW QUESTION 229
- (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 230
- (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 234
- (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 235
- (Exam Topic 5)
A security technician is configuring an access management system to track and record user actions. Which of the following functions should the technician configure?

A. Accounting
B. Authorization

C. Authentication
D. Identification

Answer: A

NEW QUESTION 239
- (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 243
- (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 248
- (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 250
- (Exam Topic 5)
AChief Information Officer (CIO) asks the company's security specialist if the company should spend any funds on malware protection for a specific server. Based on a risk assessment, the ARO value of a malware infection for a server is 5 and the annual cost for the malware protection is $2500. Which of the following SLE values warrants a recommendation against purchasing the malware protection?

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

Answer: A

NEW QUESTION 255
- (Exam Topic 5)
A technician is configuring a load balancer for the application team to accelerate the network performance of their applications. The applications are hosted on multiple servers and must be redundant. Given this scenario, which of the following would be the BEST method of configuring the load balancer?

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

Answer: D

NEW QUESTION 258
- (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 260
- (Exam Topic 5)
A hacker has a packet capture that contains:

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

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

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

Answer: A

NEW QUESTION 261
- (Exam Topic 5)
Which of the following is the BEST reason to run an untested application is a sandbox?

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

Answer: C

NEW QUESTION 265
- (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 267
- (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 268
- (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 269
- (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 271
- (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 275
- (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 279
- (Exam Topic 5)
An audit reported has identifies a weakness that could allow unauthorized personnel access to the facility at its main entrance and from there gain access to the network. Which of the following would BEST resolve the vulnerability?

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

Answer: C

NEW QUESTION 283
- (Exam Topic 5)
A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. After network enumeration, the analyst's NEXT step is to perform:

A. a risk analysis.
B. a vulnerability assessment.
C. a gray-box penetration test.
D. an external security audit.
E. a red team exercise.

Answer: C

NEW QUESTION 285
- (Exam Topic 5)
A procedure differs from a policy in that it:

A. is a high-level statement regarding the company's position on a topic.
B. sets a minimum expected baseline of behavior.
C. provides step-by-step instructions for performing a task.
D. describes adverse actions when violations occur.

Answer: C

NEW QUESTION 290
- (Exam Topic 5)
Several workstations on a network are found to be on OS versions that are vulnerable to a specific attack. Which of the following is considered to be a corrective action to combat this vulnerability?

A. Install an antivirus definition patch
B. Educate the workstation users
C. Leverage server isolation
D. Install a vendor-supplied patch
E. Install an intrusion detection system

Answer: D

NEW QUESTION 293
- (Exam Topic 5)
To help prevent one job role from having sufficient access to create, modify, and approve payroll data, which of the following practices should be employed?

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

Answer: D

NEW QUESTION 294
- (Exam Topic 5)
When it comes to cloud computing, if one of the requirements for a project is to have the most control over the systems in the cloud, which of the following is a service model that would be BEST suited for this goal?

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

Answer: A

NEW QUESTION 298
- (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 301
- (Exam Topic 5)
Due to regulatory requirements, server in a global organization must use time synchronization. Which of the following represents the MOST secure method of time synchronization?

A. The server should connect to external Stratum 0 NTP servers for synchronization
B. The server should connect to internal Stratum 0 NTP servers for synchronization
C. The server should connect to external Stratum 1 NTP servers for synchronization
D. The server should connect to external Stratum 1 NTP servers for synchronization

Answer: B

NEW QUESTION 303
- (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 305
- (Exam Topic 5)
A cybersecurity analyst is looking into the payload of a random packet capture file that was selected for analysis. The analyst notices that an internal host had a socket established with another internal host over a non-standard port.
Upon investigation, the origin host that initiated the socket shows this output:

```
usera@host>history
mkdir /local/usr/bin/somedirectory
nc -1 192.168.5.1 -p 9856
ping -c 30 8.8.8.8 -a 600
rm /etc/dir2/somefile
rm -rm /etc/dir2/

traceroute 8.8.8.8

pakill pid 9487

usera@host>
```

Given the above output, which of the following commands would have established the questionable socket?

A. traceroute 8.8.8.8
B. ping -1 30 8.8.8.8 -a 600
C. nc -1 192.168.5.1 -p 9856
D. pskill pid 9487

Answer: C

NEW QUESTION 309
- (Exam Topic 5)
An organization wants to upgrade its enterprise-wide desktop computer solution. The organization currently has 500 PCs active on the network. the Chief Information Security Officer (CISO) suggests that the organization employ desktop imaging technology for such a large scale upgrade. Which of the following is a security benefit of implementing an imaging solution?

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

Answer: B

NEW QUESTION 313
- (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 318
- (Exam Topic 5)
A company offers SaaS, maintaining all customers' credentials and authenticating locally. Many large customers have requested the company offer some form of federation with their existing authentication infrastructures. Which of the following would allow customers to manage authentication and authorizations from within their existing organizations?

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

Answer: A

NEW QUESTION 323
- (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 326
- (Exam Topic 5)
A bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions. in addition, the perimeter router can only handle 1Gbps of

traffic.
Which of the following should be implemented to prevent a DoS attacks in the future?

A. Deploy multiple web servers and implement a load balancer
B. Increase the capacity of the perimeter router to 10 Gbps
C. Install a firewall at the network to prevent all attacks
D. Use redundancy across all network devices and services

Answer: D

NEW QUESTION 327
- (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 328
- (Exam Topic 5)
A forensic expert is given a hard drive from a crime scene and is asked to perform an investigation. Which of the following is the FIRST step the forensic expert needs to take the chain of custody?

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

Answer: D

NEW QUESTION 332
- (Exam Topic 5)
Ann is the IS manager for several new systems in which the classification of the systems' data are being decided. She is trying to determine the sensitivity level of the data being processed. Which of the following people should she consult to determine the data classification?

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

Answer: D

NEW QUESTION 337
- (Exam Topic 5)
A systems administrator found a suspicious file in the root of the file system. The file contains URLs, usernames, passwords, and text from other documents being edited on the system. Which of the following types of malware would generate such a file?

A. Keylogger
B. Rootkit
C. Bot
D. RAT

Answer: A

NEW QUESTION 341
- (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 342
- (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 346
- (Exam Topic 5)
Which of the following is an asymmetric function that generates a new and separate key every time it runs?

A. RSA
B. DSA
C. DHE
D. HMAC
E. PBKDF2

Answer: C

NEW QUESTION 349
- (Exam Topic 5)
A technician is investigating a potentially compromised device with the following symptoms:

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

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

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

Answer: D

NEW QUESTION 350
.....

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