CompTIA Security+ Certification SY0-501 Exam

- **Vendor: CompTIA**
- **Exam Code: SY0-501**
- **Exam Name: CompTIA Security+**

Get Complete Version Exam SY0-501 Dumps with VCE and PDF Here

https://www.passleader.com/sy0-501.html

NEW QUESTION 235
A Chief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

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

Answer: A

NEW QUESTION 236
A company hires a third-party firm to conduct an assessment of vulnerabilities exposed to the Internet. The firm informs the company that an exploit exists for an FTP server that had a version installed from eight years ago. The company has decided to keep the system online anyway, as no upgrade exists form the vendor. Which of the following BEST describes the reason why the vulnerability exists?

A. Default configuration
B. End-of-life system
C. Weak cipher suite
D. Zero-day threats

Answer: B

NEW QUESTION 237
An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization's security policy, the employee's access to all network resources is terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server. Which of the following represents the BEST course of action?

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

Answer: C

NEW QUESTION 238
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 239
A director of IR is reviewing a report regarding several recent breaches. The director compiles the following statistic's:
- Initial IR engagement time frame
- Length of time before an executive management notice went out
- Average IR phase completion
The director wants to use the data to shorten the response time. Which of the following would accomplish this?

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

Answer: D

NEW QUESTION 240
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 241
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 242
Which of the following types of attacks precedes the installation of a rootkit on a server?

A. Pharming
B. DDoS
C. Privilege escalation
D. DoS

Answer: C

NEW QUESTION 243
Which of the following cryptographic algorithms is irreversible?

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

Answer: B

NEW QUESTION 244
A security analyst receives an alert from a WAF with the following payload:
`var data= "<test test test>" ++ <../../../../../../etc/passwd>"`
Which of the following types of attacks is this?

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

Answer: D

NEW QUESTION 245
A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him. Which of the following BEST describes what occurred?

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

Answer: D

NEW QUESTION 246
A development team has adopted a new approach to projects in which feedback is iterative and multiple iterations of deployments are provided within an application's full life cycle. Which of the following software development methodologies is the development team using?

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

Answer: B

NEW QUESTION 247
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 248
An organization is comparing and contrasting migration from its standard desktop configuration to the newest version of the platform. Before this can happen, the Chief Information Security Officer (CISO) voices the need to evaluate the functionality of the newer desktop platform to ensure interoperability with existing software in use by the organization. In which of the following principles of architecture and design is the CISO engaging?

A. Dynamic analysis
B. Change management
C. Baselining
D. Waterfalling

Answer: B

NEW QUESTION 249
.....

NEW QUESTION 301
Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

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

Answer: D

NEW QUESTION 302
A network technician is trying to determine the source of an ongoing network based attack. Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?

A. Proxy
B. Protocol analyzer
C. Switch
D. Firewall

Answer: B

NEW QUESTION 303
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 304
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 confirming 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 305
A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated. Which of the following options will pro-vide the best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

A. Put the VoIP network into a different VLAN than the existing data network.
B. Upgrade the edge switches from 10/100/1000 to improve network speed.
C. Physically separate the VoIP phones from the data network.
D. Implement flood guards on the data network.

Answer: A

NEW QUESTION 306
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 307
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 308
Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate-based authentication with its users. The company uses SSL-inspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication. Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?

A. Use of OATH between the user and the service and attestation from the company domain.
B. Use of active directory federation between the company and the cloud-based service.
C. Use of smartcards that store x.509 keys, signed by a global CA.
D. Use of a third-party, SAML-based authentication service for attestation.

Answer: B

NEW QUESTION 309
Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it. Which of the following BEST describes what the company?

A. The system integration phase of the SDLC.
B. The system analysis phase of SSDSLC.
C. The system design phase of the SDLC.
D. The system development phase of the SDLC.

Answer: B

NEW QUESTION 310
A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided form the role-based authentication system in use by the company. The situation can be identified for future mitigation as which of the following?

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

Answer: B

NEW QUESTION 311
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 312
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 313
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 314
Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?

A. Egress traffic is more important than ingress traffic for malware prevention.
B. To rebalance the amount of outbound traffic and inbound traffic.
C. Outbound traffic could be communicating to known botnet sources.
D. To prevent DDoS attacks originating from external network.

Answer: B

NEW QUESTION 315
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 316
.....