

SY0-501 Dumps

CompTIA Security+ Certification Exam

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



NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 2

- (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 3

- (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

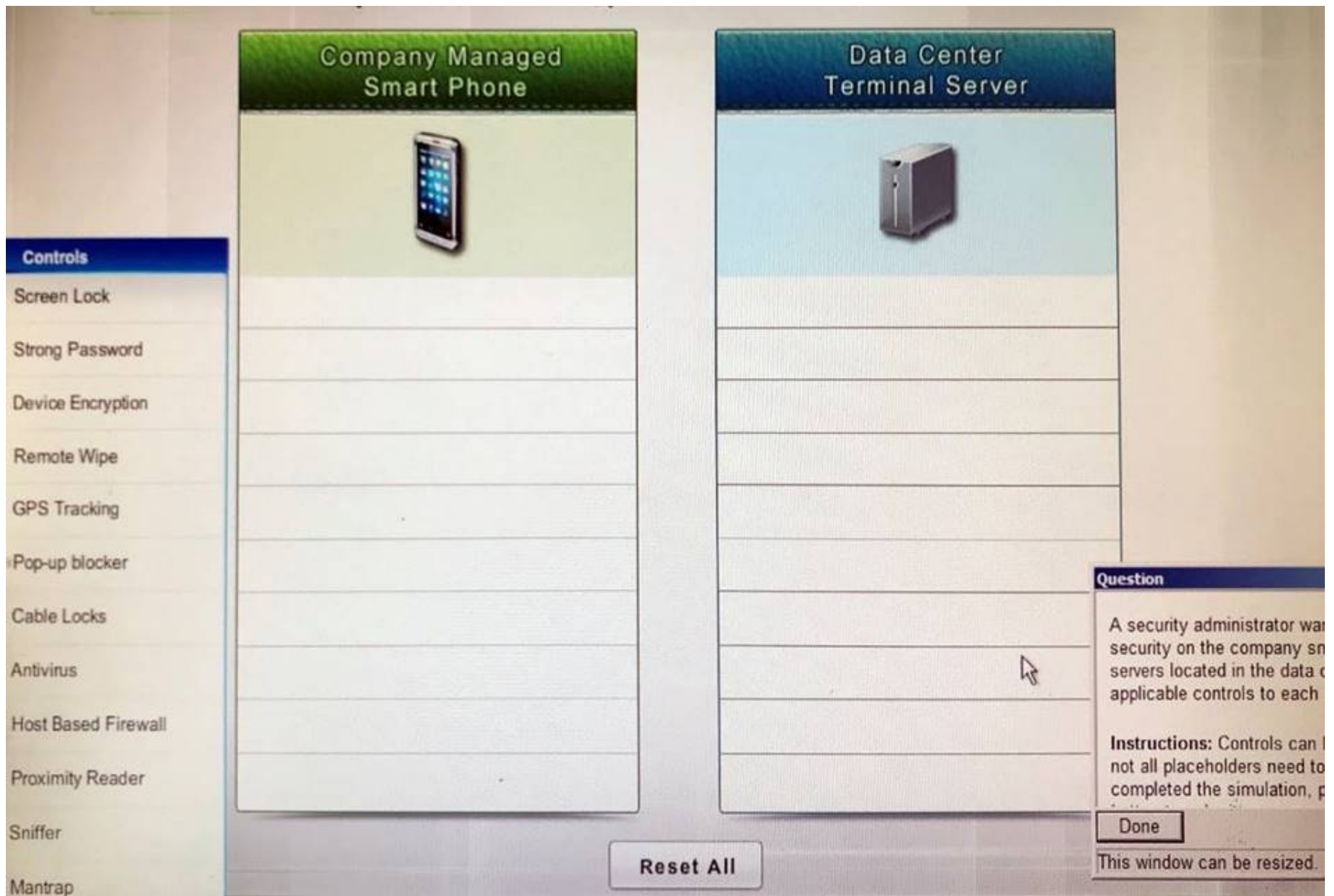
Answer: A

NEW QUESTION 4

- (Exam Topic 1)

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

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



Solution:

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

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 5

- (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 6

- (Exam Topic 2)

During a monthly vulnerability scan, a server was flagged for being vulnerable to an Apache Struts exploit. Upon further investigation, the developer responsible for the server informs the security team that Apache Struts is not installed on the server. Which of the following BEST describes how the security team should reach to this incident?

- A. The finding is a false positive and can be disregarded
- B. The Struts module needs to be hardened on the server
- C. The Apache software on the server needs to be patched and updated
- D. The server has been compromised by malware and needs to be quarantined.

Answer: A

NEW QUESTION 7

- (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 8

- (Exam Topic 2)

A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile data first. Which of the following is the correct order in which Joe should collect the data?

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

Answer: D

NEW QUESTION 9

- (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 10

- (Exam Topic 2)

An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts BEST represents the risk described in this scenario?

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

Answer: A

NEW QUESTION 11

- (Exam Topic 3)

A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

- A. Performance and service delivery metrics
- B. Backups are being performed and tested
- C. Data ownership is being maintained and audited
- D. Risk awareness is being adhered to and enforced

Answer: A

NEW QUESTION 12

- (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 13

- (Exam Topic 4)

Which of the following are used to increase the computing time it takes to brute force a password using an offline attack? (Select TWO)

- A. XOR
- B. PBKDF2
- C. bcrypt
- D. HMAC
- E. RIPEMD

Answer: BC

NEW QUESTION 14

- (Exam Topic 4)

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

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

Answer: AE

NEW QUESTION 15

- (Exam Topic 4)

A user needs to send sensitive information to a colleague using PKI. Which of the following concepts apply when a sender encrypts the message hash with the sender's private key? (Select TWO)

- A. Non-repudiation
- B. Email content encryption
- C. Steganography
- D. Transport security
- E. Message integrity

Answer: AE

NEW QUESTION 16

- (Exam Topic 4)

Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

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

Answer: A

NEW QUESTION 17

- (Exam Topic 4)

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 18

- (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 19

- (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 20

- (Exam Topic 5)

A company has noticed multiple instances of proprietary information on public websites. It has also observed an increase in the number of email messages sent to random employees containing malicious links and PDFs. Which of the following changes should the company make to reduce the risks associated with phishing attacks? (Select TWO)

- A. Install an additional firewall
- B. Implement a redundant email server
- C. Block access to personal email on corporate systems
- D. Update the X.509 certificates on the corporate email server
- E. Update corporate policy to prohibit access to social media websites
- F. Review access violation on the file server

Answer: CE

NEW QUESTION 21

.....

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>