SY0-501 Q&As

CompTIA Security+ Certification Exam

Pass CompTIA SY0-501 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

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

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A security administrator has been conducting an account permissions review that has identified several users who belong to functional groups and groups responsible for auditing the functional groups\\' actions. Several recent outages have not been able to be traced to any user. Which of the following should the security administrator recommend to preserve future audit tag integrity?

A. Enforcing stricter onboarding workflow policies.

B. Applying least privilege to user group membership.

C. Following standard naming conventions for audit group users.

D. Restricting audit group membership to service accounts.

Correct Answer: D

QUESTION 2

An analyst is concerned about data leaks and wants to restrict access to Internet services to authorized users only. The analyst also wants to control the actions each user can perform on each service Which of the following would be the

BEST technology for me analyst to consider implementing?

A. DLP

B. VPC

C. CASB

D. ACL

Correct Answer: A

QUESTION 3

Which of the following should identify critical systems and components?

A. MOU

B. BPA

C. ITCP

D. BCP

Correct Answer: D

QUESTION 4

A security analyst is reviewing the following packet capture of an attack directed at a company\\'s server located in the DMZ:

```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags [S]
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags [S]
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags [S]
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags [S]
```

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

A. DENY TCO From ANY to 172.31.64.4

B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24

C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0

D. Deny TCP from 192.168.1.10 to 172.31.67.4

Correct Answer: D

QUESTION 5

Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

A. Cloud computing

B. Virtualization

C. Redundancy

D. Application control

Correct Answer: B

Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

QUESTION 6

A security analyst is doing a vulnerability assessment on a database server. A scanning tool returns the following information:

```
Database:    CustomerAccess1
Column:      Password
Data type:   MD5 Hash
Salted?:     No
```

There have been several security breaches on the web server that accesses this database. The security team is instructed to mitigate the impact of any possible breaches. The security team is also instructed to improve the security on this database by making it less vulnerable to offline attacks. Which of the following would BEST accomplish these goals? (Choose two.)

A. Start using salts to generate MD5 password hashes

B. Generate password hashes using SHA-256

C. Force users to change passwords the next time they log on

D. Limit users to five attempted logons before they are locked out

E. Require the web server to only use TLS 1.2 encryption

Correct Answer: AC

QUESTION 7

An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations.

B. It provides insurance in case of a data breach.

C. It provides complimentary training and certification resources to IT security staff.

D. It certifies the organization can work with foreign entities that require a security clearance.

E. It assures customers that the organization meets security standards.

Correct Answer: E

QUESTION 8

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

Correct Answer: D

QUESTION 9

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

Correct Answer: AF

QUESTION 10

SIMULATION

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

The Chief Executive Officer\\'s (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.

The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.

In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.

In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.

The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.

Instructions: The original security controls for each office can be reset at any time by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.


PII Processing Office
Available Security Controls
Iris Scanner
Thumbprint Scanner
Proximity Badge
Smart Card Reader
One Time Password Token
Pin Pad
Reset All
Save
Exit


Public Cafe
Available Security Controls
128-bit key
64-bit key
Pre-share Key
PKI certificate
SSH Key
Pin Pad
Reset All
Save
Exit


Help Desk
Available Security Controls
Iris Scanner
Thumbprint Scanner
Password
Proximity Badge
Voice Recognition
Pin Pad
Reset All
Save
Exit


Data Center
Available Security Controls
Iris Scanner
Thumbprint Scanner
Mantrap
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit


CEO's Office
Available Security Controls
Iris Scanner
Thumbprint Scanner
Username/Password
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit

Correct Answer:

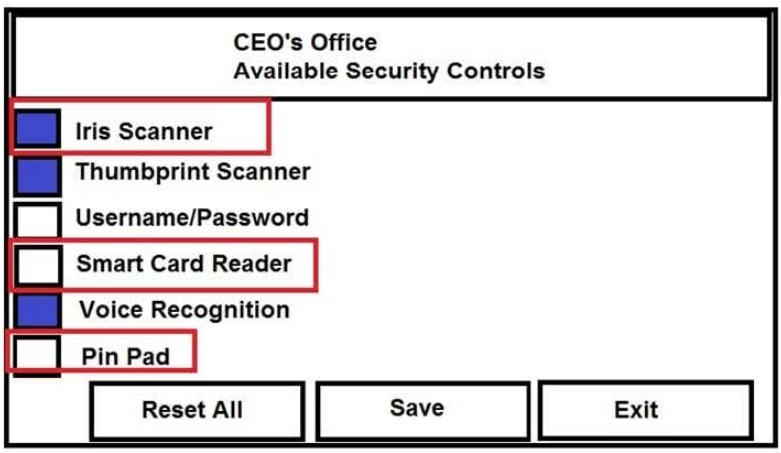
See the solution below.


PII Processing Office
Available Security Controls
Iris Scanner
Thumbprint Scanner
Proximity Badge
Smart Card Reader
One Time Password Token
Pin Pad
Reset All
Save
Exit


Public Cafe
Available Security Controls
128-bit key
64-bit key
Pre-share Key
PKI certificate
SSH Key
Pin Pad
Reset All
Save
Exit


Help Desk
Available Security Controls
Iris Scanner
Thumbprint Scanner
Password
Proximity Badge
Voice Recognition
Pin Pad
Reset All
Save
Exit


Data Center
Available Security Controls
Iris Scanner
Thumbprint Scanner
Mantrap
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit


CEO's Office
Available Security Controls
Iris Scanner
Thumbprint Scanner
Username/Password
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit

QUESTION 11

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

Correct Answer: D

QUESTION 12

During an incident, a company\\'s CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

A. Physically move the PC to a separate Internet point of presence.

B. Create and apply microsegmentation rules.

C. Emulate the malware in a heavily monitored DMZ segment.

D. Apply network blacklisting rules for the adversary domain.

Correct Answer: BA

QUESTION 13

Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.

B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.

C. Malware is trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox.

D. DNS routing tables have been compromised, and an attacker is rerouting traffic to malicious websites.

Correct Answer: D

QUESTION 14

During an audit, the auditor requests to see a copy of the identified mission-critical applications as well as their disaster recovery plans. The company being audited has an SLA around the applications it hosts. With which of the following is the auditor MOST likely concerned?

A. ARO/ALE

B. MTTR/MTBF

C. RTO/RPO

D. Risk assessment

Correct Answer: C

QUESTION 15

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

Correct Answer: A