RC0-501 Q&As

CompTIA Security+ Recertification Exam

Pass CompTIA RC0-501 Exam with 100% Guarantee

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

https://www.passapply.com/rc0-501.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

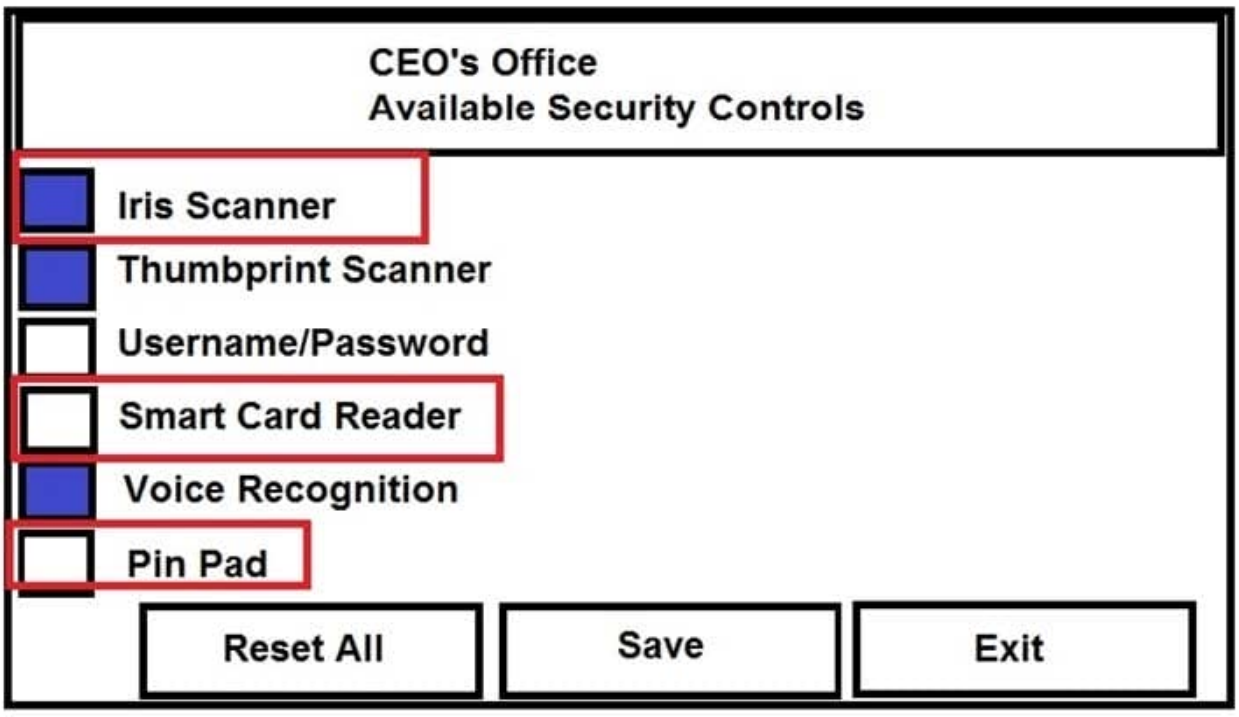

CEO's Office
Available Security Controls
Iris Scanner
Thumbprint Scanner
Username/Password
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit

Correct Answer:

See the solution below.


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 2

After a user reports stow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.

The systems administrator reviews the output below:

```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address     Foreign Address         State
TCP   0.0.0.0:135       0.0.0.0:0               LISTENING       RpcSs [svchost.exe]
TCP   0.0.0.0:445       0.0.0.0:0               LISTENING       [svchost.exe]

TCP   192.168.1.10:5000 10.37.213.20            ESTABLISHED     winserver.exe
UDP   192.168.1.10:1900 *.*                                     SSDPSVR
```

Based on the above information, which of the following types of malware was installed on the user\\'s computer?

A. RAT

B. Keylogger

C. Spyware

D. Worm

E. Bot

Correct Answer: A

QUESTION 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

Correct Answer: C

QUESTION 4

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)

Correct Answer: E

QUESTION 5

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

Correct Answer: C