



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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

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

Correct Answer: C

QUESTION 2

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 reader.

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

<input checked="" type="checkbox"/>	Iris Scanner
<input checked="" type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Proximity Badge
<input checked="" type="checkbox"/>	Smart Card Reader
<input type="checkbox"/>	One Time Password Token
<input checked="" type="checkbox"/>	Pin Pad

Public Cafe
Available Security Controls

<input checked="" type="checkbox"/>	128-bit key
<input checked="" type="checkbox"/>	64-bit key
<input checked="" type="checkbox"/>	Pre-share Key
<input checked="" type="checkbox"/>	PKI certificate
<input checked="" type="checkbox"/>	SSH Key
<input checked="" type="checkbox"/>	Pin Pad



Help Desk
Available Security Controls

<input type="checkbox"/>	Iris Scanner
<input type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Password
<input checked="" type="checkbox"/>	Proximity Badge
<input type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

Data Center
Available Security Controls

<input type="checkbox"/>	Iris Scanner
<input type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Mantrap
<input checked="" type="checkbox"/>	Smart Card Reader
<input type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

CEO's Office
Available Security Controls

<input checked="" type="checkbox"/>	Iris Scanner
<input checked="" type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Username/Password
<input type="checkbox"/>	Smart Card Reader
<input checked="" type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad



Correct Answer:

See the solution below.

PII Processing Office
Available Security Controls

<input checked="" type="checkbox"/>	Iris Scanner
<input checked="" type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Proximity Badge
<input checked="" type="checkbox"/>	Smart Card Reader
<input type="checkbox"/>	One Time Password Token
<input checked="" type="checkbox"/>	Pin Pad

Reset All Save Exit

Public Cafe
Available Security Controls

<input checked="" type="checkbox"/>	128-bit key
<input checked="" type="checkbox"/>	64-bit key
<input checked="" type="checkbox"/>	Pre-share Key
<input checked="" type="checkbox"/>	PKI certificate
<input checked="" type="checkbox"/>	SSH Key
<input checked="" type="checkbox"/>	Pin Pad

Reset All Save Exit



Help Desk
Available Security Controls

<input type="checkbox"/>	Iris Scanner
<input type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Password
<input checked="" type="checkbox"/>	Proximity Badge
<input type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

Data Center
Available Security Controls

<input type="checkbox"/>	Iris Scanner
<input type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Mantrap
<input checked="" type="checkbox"/>	Smart Card Reader
<input type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

CEO's Office
Available Security Controls

<input checked="" type="checkbox"/>	Iris Scanner
<input checked="" type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Username/Password
<input type="checkbox"/>	Smart Card Reader
<input checked="" type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad



QUESTION 3

When configuring settings in a mandatory access control environment, which of the following specifies the subjects that can access specific data objects?

- A. Owner
- B. System
- C. Administrator
- D. User

Correct Answer: C

QUESTION 4

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

Correct Answer: CF

QUESTION 5

A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org. Which of the following commands should the security analyst use? (Select two.)



- A. `nslookup`
`comptia.org`
`set type=ANY`
`ls-d example.org`
- B. `nslookup`
`comptia.org`
`set type=MX`
`example.org`
- C. `dig -axfr comptia.org @example.org`
- D. `ipconfig /flushDNS`
- E. `ifconfig eth0 down`
`ifconfig eth0 up`
`dhclient renew`
- F. `dig @example.org comptia.org`

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

F. Option F

Correct Answer: AC

[RC0-501 VCE Dumps](#)

[RC0-501 Study Guide](#)

[RC0-501 Exam Questions](#)