

# CompTIA

**Exam RC0-501**

**CompTIA Security+ Recertification Exam**

Version: Demo

**[ Total Questions: 10 ]**

**Question No : 1**

A security administrator has found a hash in the environment known to belong to malware. The administrator then finds this file to be in in the preupdate area of the OS, which indicates it was pushed from the central patch system.

File: winx86\_adobe\_flash\_upgrade.exe

Hash: 99ac28bede43ab869b853ba62c4ea243

The administrator pulls a report from the patch management system with the following output:

Install Date	Package Name	Target Devices	Hash
10/10/2017	java_11.2_x64.exe	HQ PC's	01ab28bbde63aa879b35bba62cdes283
10/10/2017	winx86_adobe_flash_upgrade.exe	HQ PC's	99ac28bede43ab869b853ba62c4ea243

Given the above outputs, which of the following MOST likely happened?

- A. The file was corrupted after it left the patch system.
- B. The file was infected when the patch manager downloaded it.
- C. The file was not approved in the application whitelist system.
- D. The file was embedded with a logic bomb to evade detection.

**Answer: D**

**Question No : 2**

An organization's file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

- A. Snapshot
- B. Full
- C. Incremental
- D. Differential

**Answer: C**

**Question No : 3 CORRECT TEXT**

## CompTIA RC0-501 : Practice Test

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 scanner.
- \* 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 anytime 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

### 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

### 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

Reset All   Save   Exit

**Answer:** Please refer to the Explanation part to solve this sim.

**Explanation:**

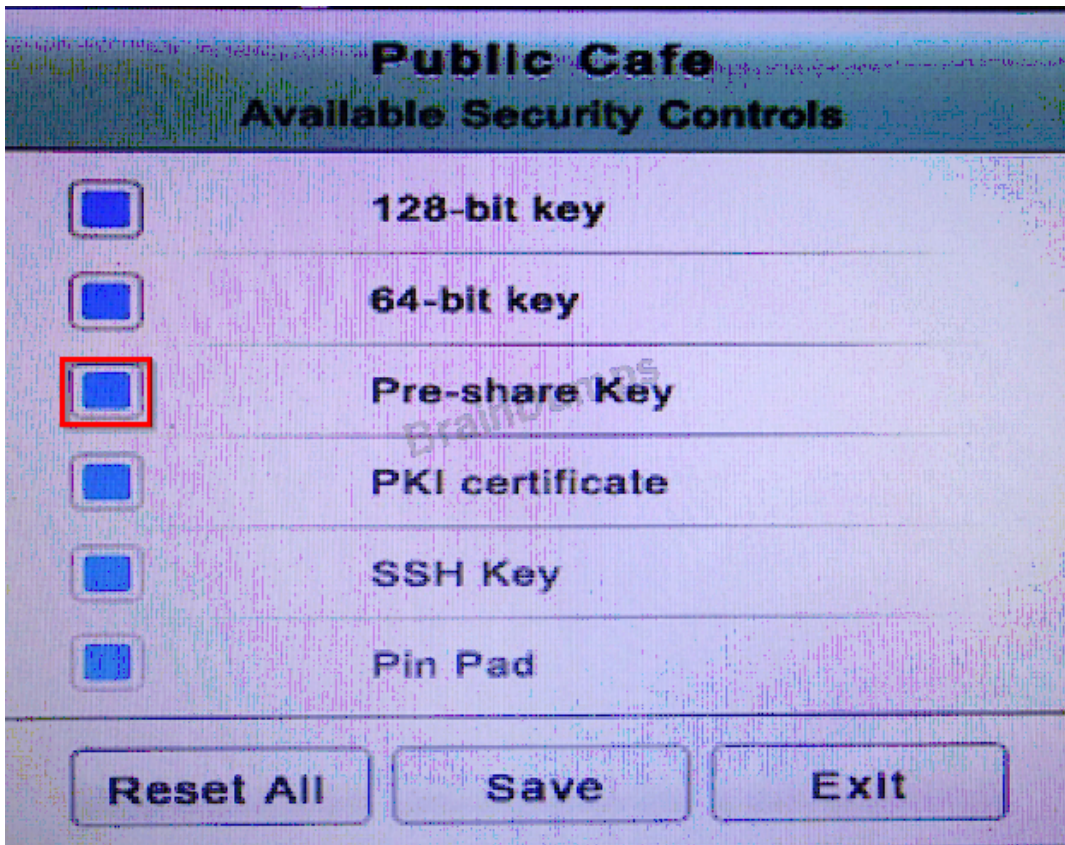
Use the following to get this sim work as :

**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





### 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

Reset All      Save      Exit





**Question No : 4**

Which of the following cryptographic algorithms is irreversible?

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

**Answer: B**

**Question No : 5**

A new firewall has been placed into service at an organization. However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network. Which of the following steps should be completed to BEST resolve the issue?

- A. The firewall should be configured to prevent user traffic from matching the implicit deny rule.
- B. The firewall should be configured with access lists to allow inbound and outbound traffic.
- C. The firewall should be configured with port security to allow traffic.
- D. The firewall should be configured to include an explicit deny rule.

**Answer: A**

**Question No : 6**

A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment?

- A. A perimeter firewall and IDS
- B. An air gapped computer network
- C. A honeypot residing in a DMZ
- D. An ad hoc network with NAT
- E. A bastion host

**Answer: B**

**Question No : 7**

Which of the following cryptographic attacks would salting of passwords render ineffective?

- A. Brute force
- B. Dictionary
- C. Rainbow tables
- D. Birthday

**Answer: B**

**Question No : 8**

The compute resource center issued smartphones to all first-level and above managers. The managers have the ability to install mobile tools. Which of the following tools should be implemented to control the types of tools the managers install?

- A. Download manager
- B. Content manager
- C. Segmentation manager
- D. Application manager

**Answer: D**

**Question No : 9**

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**

**Question No : 10**

An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked

to investigate the organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.

The IT security department finds the following security configuration for the accounts payable module:

Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?

- A.
- B.
- C.
- D.
- E. Option A
- F. Option B
- G. Option C
- H. Option D

**Answer: A**