



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 administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and

network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production.

Which of the following would correct the deficiencies?

- A. Mandatory access controls
- B. Disable remote login
- C. Host hardening
- D. Disabling services

Correct Answer: C

QUESTION 2

After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internet-based control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence. Which of the following is the MOST likely reason the thermostat is not connecting to the internet?

- A. The company implements a captive portal
- B. The thermostat is using the incorrect encryption algorithm
- C. the WPA2 shared key is incorrect
- D. The company's DHCP server scope is full

Correct Answer: C

QUESTION 3

A company hires a third-party firm to conduct an assessment of vulnerabilities exposed to the Internet. The firm informs the company that an exploit exists for an FTP server that had a version installed from eight years ago. The company has decided to keep the system online anyway, as no upgrade exists from the vendor. Which of the following BEST describes the reason why the vulnerability exists?

- A. Default configuration
- B. End-of-life system



- C. Weak cipher suite
- D. Zero-day threats

Correct Answer: B

QUESTION 4

Ann, a college professor, was recently reprimanded for posting disparaging remarks re-grading her coworkers on a web site. Ann stated that she was not aware that the public was able to view her remarks. Which of the following security-related trainings could have made Ann aware of the repercussions of her actions?

- A. Data Labeling and disposal
- B. Use of social networking
- C. Use of P2P networking
- D. Role-based training

Correct Answer: B

QUESTION 5

After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

- A. Recovery
- B. Identification
- C. Preparation
- D. Documentation
- E. Escalation

Correct Answer: B

QUESTION 6

A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack. News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong?

- A. SoC
- B. ICS
- C. IoT



D. MFD

Correct Answer: C

QUESTION 7

Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production?

- A. Roll back changes in the test environment
- B. Verify the hashes of files
- C. Archive and compress the files
- D. Update the secure baseline

Correct Answer: B

QUESTION 8

A penetration tester finds that a company's login credentials for the email client were being sent in clear text. Which of the following should be done to provide encrypted logins to the email server?

- A. Enable IPsec and configure SMTP.
- B. Enable SSH and LDAP credentials.
- C. Enable MIME services and POP3.
- D. Enable an SSL certificate for IMAP services.

Correct Answer: D

QUESTION 9

Which of the following best describes routine in which semicolons, dashes, quotes, and commas are removed from a string?

- A. Error handling to protect against program exploitation
- B. Exception handling to protect against XSRF attacks.
- C. Input validation to protect against SQL injection.
- D. Padding to protect against string buffer overflows.

Correct Answer: C



QUESTION 10

A security analyst receives an alert from a WAF with the following payload:

```
var data= "" ++ "
```

 Which of the following types of attacks is this?

- A. Cross-site request forgery
- B. Buffer overflow
- C. SQL injection
- D. JavaScript data insertion
- E. Firewall evasion script

Correct Answer: D

QUESTION 11

Which of the following implements two-factor authentication?

- A. A phone system requiring a PIN to make a call
- B. At ATM requiring a credit card and PIN
- C. A computer requiring username and password
- D. A datacenter mantrap requiring fingerprint and iris scan

Correct Answer: B

QUESTION 12

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

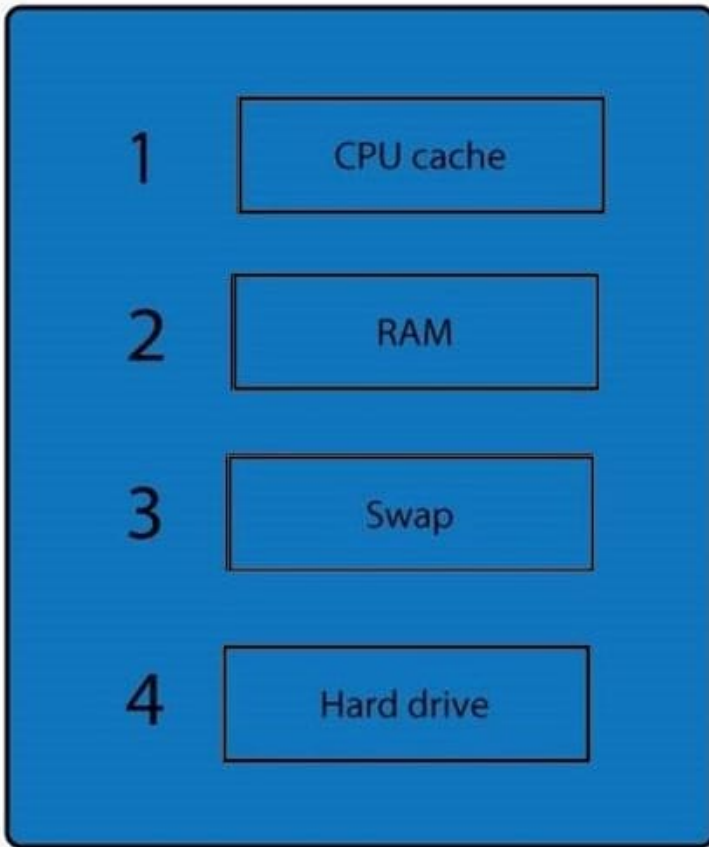
Select and Place:



1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>

- RAM
- CPU cache
- Swap
- Hard drive

Correct Answer:



When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone.

Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and

printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashees, record time offset on the systems, talk to witnesses, and track total man-hours and

expenses associated with the investigation.

QUESTION 13

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

Correct Answer: A

QUESTION 14

An audit has revealed that database administrators are also responsible for auditing database changes and backup logs. Which of the following access control methodologies would BEST mitigate this concern?

- A. Time of day restrictions
- B. Principle of least privilege
- C. Role-based access control
- D. Separation of duties

Correct Answer: D

QUESTION 15

During a recent audit, it was discovered that many services and desktops were missing security patches. Which of the following BEST describes the assessment that was performed to discover this issue?

- A. Network mapping
- B. Vulnerability scan
- C. Port Scan
- D. Protocol analysis

Correct Answer: B

[RC0-501 VCE Dumps](#)

[RC0-501 Study Guide](#)

[RC0-501 Exam Questions](#)