



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 analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the following should the security analyst do NEXT?

- A. Document and lock the workstations in a secure area to establish chain of custody
- B. Notify the IT department that the workstations are to be reimaged and the data restored for reuse
- C. Notify the IT department that the workstations may be reconnected to the network for the users to continue working
- D. Document findings and processes in the after-action and lessons learned report

Correct Answer: D

QUESTION 2

An organization needs to implement a large PKI. Network engineers are concerned that repeated transmission of the OCSP will impact network performance. Which of the following should the security analyst recommend is lieu of an OCSP?

- A. CSR
- B. CRL
- C. CA
- D. OID

Correct Answer: B

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

Which of the following is the appropriate network structure used to protect servers and services that must be provided to



external clients without completely eliminating access for internal users?

- A. NAC
- B. VLAN
- C. DMZ
- D. Subnet

Correct Answer: C

QUESTION 5

A user clicked an email link that led to a website than infected the workstation with a virus. The virus encrypted all the network shares to which the user had access. The virus was not deleted or blocked by the company's email filter, website filter, or antivirus. Which of the following describes what occurred?

- A. The user's account was over-privileged.
- B. Improper error handling triggered a false negative in all three controls.
- C. The email originated from a private email server with no malware protection.
- D. The virus was a zero-day attack.

Correct Answer: A

[Latest RC0-501 Dumps](#)

[RC0-501 PDF Dumps](#)

[RC0-501 Practice Test](#)