



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 systems administrator is reviewing the following information from a compromised server: Given the above information, which of the following processes was MOST likely exploited via a remote buffer overflow attack?

Process	DEP	Local Address	Remote Address
LSASS	YES	0.0.0.0.	10.210.100.62
APACHE	NO	0.0.0.0	10.130.210.20
MySQL	NO	127.0.0.1	127.0.0.1
TFTP	YES	191.168.1.10	10.34.221.96

- A. Apache
- B. LSASS
- C. MySQL
- D. TFTP

Correct Answer: A

QUESTION 2

A security team wants to establish an Incident Response plan. The team has never experienced an incident. Which of the following would BEST help them establish plans and procedures?

- A. Table top exercises
- B. Lessons learned
- C. Escalation procedures
- D. Recovery procedures

Correct Answer: A

QUESTION 3

A security administrator suspects that data on a server has been exfiltrated as a result of unauthorized remote access. Which of the following would assist the administrator in confirming the suspicions? (Select TWO)

- A. Networking access control
- B. DLP alerts
- C. Log analysis



- D. File integrity monitoring
- E. Host firewall rules

Correct Answer: BC

QUESTION 4

When considering a third-party cloud service provider, which of the following criteria would be the BEST to include in the security assessment process? (Select two.)

- A. Use of performance analytics
- B. Adherence to regulatory compliance
- C. Data retention policies
- D. Size of the corporation
- E. Breadth of applications support

Correct Answer: BC

QUESTION 5

During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could best prevent this from occurring again?

- A. Credential management
- B. Group policy management
- C. Acceptable use policy
- D. Account expiration policy

Correct Answer: B

[RC0-501 PDF Dumps](#)

[RC0-501 Exam Questions](#)

[RC0-501 Braindumps](#)