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

Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened. The network and security teams perform the following actions:

Shut down all network shares.

Run an email search identifying all employees who received the malicious message. Reimage all devices belonging to users who opened the attachment. Next, the teams want to re-enable the network shares. Which of the following BEST

describes this phase of the incident response process?

A. Eradication

B. Containment

C. Recovery

D. Lessons learned

Correct Answer: C

QUESTION 2

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 3

A security analyst is reviewing the following packet capture of an attack directed at a company\\'s server located in the DMZ:

```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags [S]
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags [S]
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags [S]
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags [S]
```

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

A. DENY TCO From ANY to 172.31.64.4

B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24

C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0

D. Deny TCP from 192.168.1.10 to 172.31.67.4

Correct Answer: C

QUESTION 4

A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account. This is an example of which of the following attacks?

A. SQL injection

B. Header manipulation

C. Cross-site scripting

D. Flash cookie explogtation

Correct Answer: C

QUESTION 5

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

Latest RC0-501 Dumps RC0-501 Practice Test RC0-501 Exam Questions