



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.geekcert.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

Which of the following can be provided to an AAA system for the identification phase?

- A. Username
- B. Permissions
- C. One-time token
- D. Private certificate

Correct Answer: A

QUESTION 2

A security analyst is reviewing the following output from an IPS: Given this output, which of the following can be concluded? (Select two.)

```
[**] [1:2467:7] EXPLOIT IGMP IGAP message overflow attempt [**]  
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]  
07/30-19:45:02.238185 250.19.18.71 -> 250.19.18.22  
IGMP TTL:255 TOS: 0x0 ID: 9742 IpLen:20 DgmLen: 502 MF  
Frag offset: 0x1FFF Frag Size: 0x01E2  
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0367]
```

- A. The source IP of the attack is coming from 250.19.18.22.
- B. The source IP of the attack is coming from 250.19.18.71.
- C. The attacker sent a malformed IGAP packet, triggering the alert.
- D. The attacker sent a malformed TCP packet, triggering the alert.
- E. The TTL value is outside of the expected range, triggering the alert.

Correct Answer: BC

QUESTION 3

A director of IR is reviewing a report regarding several recent breaches. The director compiles the following statistics:

Initial IR engagement time frame

Length of time before an executive management notice went out Average IR phase completion

The director wants to use data to shorten the response time. Which of the following would accomplish this?

- A. CSIRT



- B. Containment phase
- C. Escalation notifications
- D. Tabletop exercise

Correct Answer: D

QUESTION 4

An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection. Which of the following AES modes of operation would meet this integrity-only requirement?

- A. HMAC
- B. PCBC
- C. CBC
- D. GCM
- E. CFB

Correct Answer: A

QUESTION 5

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

[Latest RC0-501 Dumps](#)

[RC0-501 VCE Dumps](#)

[RC0-501 Exam Questions](#)