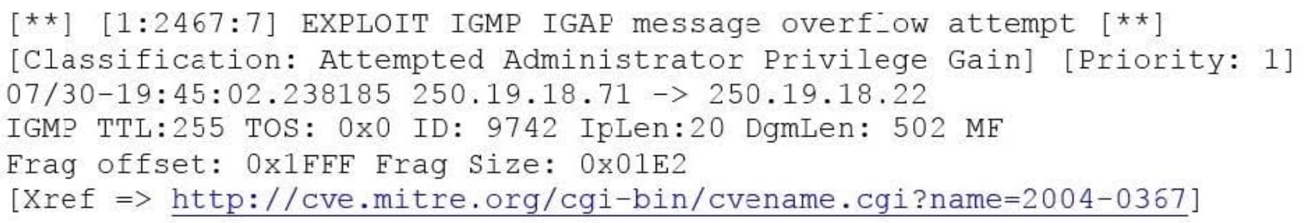
RC0-501$^{\text{Q\&As}}$

CompTIA Security+ Recertification Exam

QUESTION 1

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 2

Which of the following encryption methods does PKI typically use to securely project keys?

A. Elliptic curve

B. Digital signatures

C. Asymmetric

D. Obfuscation

Correct Answer: B

QUESTION 3

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 4

An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization\\'s security policy, the employee\\'s access to all network resources is terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server. Which of the following represents the BEST course of action?

A. Approve the former employee\\'s request, as a password reset would give the former employee access to only the human resources server.

B. Deny the former employee\\'s request, since the password reset request came from an external email address.

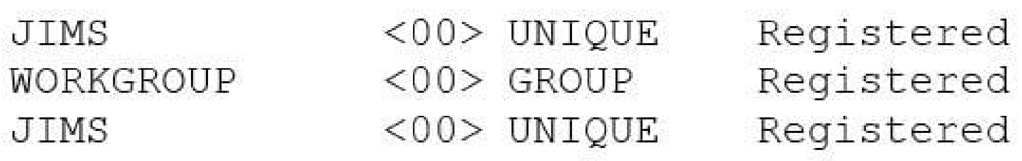
C. Deny the former employee\\'s request, as a password reset would give the employee access to all network resources.

D. Approve the former employee\\'s request, as there would not be a security issue with the former employee gaining access to network.

Correct Answer: C

QUESTION 5

An auditor wants to test the security posture of an organization by running a tool that will display the following:



```
JIMS           <00> UNIQUE    Registered
WORKGROUP      <00> GROUP     Registered
JIMS           <00> UNIQUE    Registered
```

Which of the following commands should be used?

A. nbtstat

B. nc

C. arp

D. ipconfig

Correct Answer: A