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.leads4pass.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 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

QUESTION 2

An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by explogting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP. Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

A. Use a honeypot

B. Disable unnecessary services

C. Implement transport layer security

D. Increase application event logging

Correct Answer: B

QUESTION 3

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 4

A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host. Which of the following is preventing the remote user from being able to access the workstation?

A. Network latency is causing remote desktop service request to time out

B. User1 has been locked out due to too many failed passwords

C. Lack of network time synchronization is causing authentication mismatches

D. The workstation has been compromised and is accessing known malware sites

E. The workstation host firewall is not allowing remote desktop connections

Correct Answer: B

QUESTION 5

A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant. Which of the following represents the authentication architecture in use?

A. Open systems authentication

B. Captive portal

C. RADIUS federation

D. 802.1x

Correct Answer: D

Latest RC0-501 Dumps   RC0-501 VCE Dumps   RC0-501 Study Guide