SEC504 Q&As

Hacker Tools, Techniques, Exploits and Incident Handling

Pass SANS SEC504 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/sec504.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by SANS Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

John is a malicious attacker. He illegally accesses the server of We-are-secure Inc. He then places a backdoor in the We-are-secure server and alters its log files.

Which of the following steps of malicious hacking includes altering the server log files?

A. Maintaining access

B. Covering tracks

C. Gaining access

D. Reconnaissance

Correct Answer: B

QUESTION 2

Which of the following incident response team members ensures that the policies of the organization are enforced during the incident response?

A. Information Security representative

B. Legal representative

C. Human Resource

D. Technical representative

Correct Answer: C

QUESTION 3

You want to integrate the Nikto tool with nessus vulnerability scanner. Which of the following steps will you take to accomplish the task? Each correct answer represents a complete solution. Choose two.

A. Place nikto.pl file in the /etc/nessus directory.

B. Place nikto.pl file in the /var/www directory.

C. Place the directory containing nikto.pl in root\\'s PATH environment variable.

D. Restart nessusd service.

Correct Answer: CD

QUESTION 4

Which of the following rootkits patches, hooks, or replaces system calls with versions that hide information about the attacker?

A. Library rootkit

B. Kernel level rootkit

C. Hypervisor rootkit

D. Boot loader rootkit

Correct Answer: A

QUESTION 5

Which of the following tasks can be performed by using netcat utility? Each correct answer represents a complete solution. Choose all that apply.

A. Checking file integrity

B. Creating a Backdoor

C. Firewall testing

D. Port scanning and service identification

Correct Answer: BCD