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.leads4pass.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

You check performance logs and note that there has been a recent dramatic increase in the amount of broadcast traffic. What is this most likely to be an indicator of?

A. Virus

B. Syn flood

C. Misconfigured router

D. DoS attack

Correct Answer: D

QUESTION 2

John works as a Network Administrator for Net Perfect Inc. The company has a Windows- based network. The company uses Check Point SmartDefense to provide security to the network of the company. On the

HTTP servers of the company, John defines a rule for dropping any kind of userdefined URLs. Which of the following types of attacks can be prevented by dropping the user-defined URLs?

A. Morris worm

B. Code red worm

C. Hybrid attacks

D. PTC worms and mutations

Correct Answer: D

QUESTION 3

Which of the following statements are correct about spoofing and session hijacking? Each correct answer represents a complete solution. Choose all that apply.

A. Spoofing is an attack in which an attacker can spoof the IP address or other identity of the target and the valid user cannot be active.

B. Spoofing is an attack in which an attacker can spoof the IP address or other identity of the target but the valid user can be active.

C. Session hijacking is an attack in which an attacker takes over the session, and the valid user\\'s session is disconnected.

D. Session hijacking is an attack in which an attacker takes over the session, and the valid user\\'s session is not disconnected.

Correct Answer: BD

QUESTION 4

Peter works as a Network Administrator for the PassGuide Inc. The company has a Windows-based network. All client computers run the Windows XP operating system. The employees of the company complain that suddenly all of the client computers have started working slowly. Peter finds that a malicious hacker is attempting to slow down the computers by flooding the network with a large number of requests.

Which of the following attacks is being implemented by the malicious hacker?

A. SQL injection attack

B. Denial-of-Service (DoS) attack

C. Man-in-the-middle attack

D. Buffer overflow attack

Correct Answer: B

QUESTION 5

Your IDS discovers that an intruder has gained access to your system. You immediately stop that access, change passwords for administrative accounts, and secure your network. You discover an odd account

(not administrative) that has permission to remotely access the network.

What is this most likely?

A. An example of privilege escalation.

B. A normal account you simply did not notice before. Large networks have a number of accounts; it is hard to track them all.

C. A backdoor the intruder created so that he can re-enter the network.

D. An example of IP spoofing.

Correct Answer: C