

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.geekcert.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



VCE & PDF GeekCert.com

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

2024 Latest geekcert SEC504 PDF and VCE dumps Download

QUESTION 1

Buffer overflows are one of the major errors used for exploitation on the Internet today. A buffer overflow occurs when a particular operation/function writes more data into a variable than the variable was designed to hold.

Which of the following are the two popular types of buffer everflowe? Each correct answer represents a complete

solution. Choose two.
A. Dynamic buffer overflows
B. Stack based buffer overflow
C. Heap based buffer overflow
D. Static buffer overflows
Correct Answer: BC
QUESTION 2
You send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024 using hping utility.
This attack is known as
A. Port scanning
B. Cloaking
C. Firewalking
D. Spoofing
Correct Answer: C

QUESTION 3

You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise network.

Which of the following phases of the Incident handling process should you follow next to handle this incident?

- A. Containment
- B. Preparation
- C. Recovery
- D. Identification

Correct Answer: A

VCE & PDF GeekCert.com

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

2024 Latest geekcert SEC504 PDF and VCE dumps Download

QUESTION 4

Which of the following steps can be taken as countermeasures against sniffer attacks? Each correct answer represents a complete solution. Choose all that apply.

- A. Use encrypted protocols for all communications.
- B. Use switches instead of hubs since they switch communications, which means that information is delivered only to the predefined host.
- C. Use tools such as StackGuard and Immunix System to avoid attacks.
- D. Reduce the range of the network to avoid attacks into wireless networks.

Correct Answer: ABD

QUESTION 5

Your friend plans to install a Trojan on your computer. He knows that if he gives you a new version of chess.exe, you will definitely install the game on your computer. He picks up a Trojan and joins it with chess.exe.

Which of the following tools are required in such a scenario? Each correct answer represents a part of the solution. Choose three.

- A. NetBus
- B. Absinthe
- C. Yet Another Binder
- D. Chess.exe

Correct Answer: ACD

SEC504 PDF Dumps

SEC504 Practice Test

SEC504 Braindumps