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

Which of the following types of scan does not open a full TCP connection?

A. FIN scan

B. ACK scan

C. Stealth scan

D. Idle scan

Correct Answer: C

QUESTION 2

Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

A. Port scanning

B. ARP spoofing

C. Man-in-the-middle

D. Session hijacking

Correct Answer: B

QUESTION 3

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We- are-secure server. The output of the scanning test is as follows:

C:\whisker.pl -h target_IP_address -- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - = = Host: target_IP_address = Server: Apache/1.3.12 (Win32) ApacheJServ/1.1 mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22

+ 200 OK: HEAD /cgi-bin/printenv John recognizes /cgi-bin/printenv vulnerability (\\'Printenv\\' vulnerability) in the We_are_secure server. Which of the following statements about \\'Printenv\\' vulnerability are true? Each correct answer represents a

complete solution. Choose all that apply.

A. This vulnerability helps in a cross site scripting attack.

B. \\'Printenv\\' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.

C. The countermeasure to \\'printenv\\' vulnerability is to remove the CGI script.

D. With the help of \\'printenv\\' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

Correct Answer: ACD

QUESTION 4

You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux- based network. You are working as a root user on the Linux operating system. Your company is facing an IP spoofing attack.

Which of the following tools will you use to get an alert saying that an upcoming IP packet is being spoofed?

A. Despoof

B. Dsniff

C. ethereal

D. Neotrace

Correct Answer: A

QUESTION 5

John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail.

Which of the following techniques is he performing to accomplish his task?

A. Email spoofing

B. Steganography

C. Web ripping

D. Social engineering

Correct Answer: B