DUMPSARENA

Hacker Tools, Techniques, Exploits and Incident Handling

SANS SEC504

Version Demo

Total Demo Questions: 15

Total Premium Questions: 328

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	97
Topic 2, Volume B	96
Topic 3, Volume C	135
Total	328

QUESTION NO: 1

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.

ANSWER: B D

QUESTION NO: 2

Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to secure access to the network of the company from all possible entry points. He segmented the network into several subnets and installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except the ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Adam is still worried about the programs like Hping2 that can get into a network through covert channels.

Which of the following is the most effective way to protect the network of the company from an attacker using Hping2 to scan his internal network?

A. Block all outgoing traffic on port 21

B. Block all outgoing traffic on port 53

C. Block ICMP type 13 messages

D. Block ICMP type 3 messages

ANSWER: C

QUESTION NO: 3

Which of the following attacks are examples of Denial-of-service attacks (DoS)?

Each correct answer represents a complete solution. Choose all that apply.

A. Fraggle attack

B. Smurf attack

C. Birthday attack

D. Ping flood attack

ANSWER: A B D

QUESTION NO: 4

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

ANSWER: B

QUESTION NO: 5

Network mapping provides a security testing team with a blueprint of the organization. Which of the following steps is NOT a part of manual network mapping?

A. Gathering private and public IP addresses

B. Collecting employees information

C. Banner grabbing

D. Performing Neotracerouting

ANSWER: D

QUESTION NO: 6

Which of the following is used by attackers to obtain an authenticated connection on a network?

A. Denial-of-Service (DoS) attack

B. Replay attack

C. Man-in-the-middle attack

D. Back door

ANSWER: B

QUESTION NO: 7

Which of the following languages are vulnerable to a buffer overflow attack?

Each correct answer represents a complete solution. Choose all that apply.

A. Java

B. C++

C. C

D. Action script

ANSWER: B C

QUESTION NO: 8

What is the purpose of configuring a password protected screen saver on a computer?

A. For preventing unauthorized access to a system.

B. For preventing a system from a Denial of Service (DoS) attack.

C. For preventing a system from a social engineering attack.

D. For preventing a system from a back door attack.

ANSWER: A

QUESTION NO: 9

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.

ANSWER: A C D

QUESTION NO: 10

Adam works as a Security Analyst for Umbrella Inc. Company has a Windows-based network. All computers run on Windows XP. Manager of the Sales department complains Adam about the unusual behavior of his computer. He told Adam that some pornographic contents are suddenly appeared on his computer overnight. Adam suspects that some malicious software or Trojans have been installed on the computer. He runs some diagnostics programs and Port scanners and found that the Port 12345, 12346, and 20034 are open. Adam also noticed some tampering with the Windows registry, which causes one application to run every time when Windows start.

Which of the following is the most likely reason behind this issue?

A. Cheops-ng is installed on the computer.

B. Elsave is installed on the computer.

C. NetBus is installed on the computer.

D. NetStumbler is installed on the computer.

ANSWER: C

QUESTION NO: 11

Which of the following tools will you use to prevent from session hijacking?

Each correct answer represents a complete solution. Choose all that apply.

A. OpenSSH

B. Rlogin

C. Telnet

D. SSL

ANSWER: A D

QUESTION NO: 12

Which of the following are the limitations for the cross site request forgery (CSRF) attack?

Each correct answer represents a complete solution. Choose all that apply.

A. The attacker must determine the right values for all the form inputs.

B. The attacker must target a site that doesn't check the referrer header.

C. The target site should have limited lifetime authentication cookies.

D. The target site should authenticate in GET and POST parameters, not only cookies.

ANSWER: A B

QUESTION NO: 13

Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?

A. Preparation phase

B. Eradication phase

C. Identification phase

D. Recovery phase

E. Containment phase

ANSWER: A

QUESTION NO: 14

US Garments wants all encrypted data communication between corporate office and remote location.

They want to achieve following results:

l Authentication of users

l Anti-replay

l Anti-spoofing

l IP packet encryption

They implemented IPSec using Authentication Headers (AHs). Which results does this solution provide?

Each correct answer represents a complete solution. Choose all that apply.

A. Anti-replay

B. IP packet encryption

C. Authentication of users

D. Anti-spoofing

ANSWER: A D

QUESTION NO: 15

Adam works as a Network Administrator for PassGuide Inc. He wants to prevent the network from DOS attacks. Which of the following is most useful against DOS attacks?

A. SPI

B. Distributive firewall

C. Honey Pot

D. Internet bot

ANSWER: A