Vendor:SANS

Exam Code:SEC504

Exam Name: Hacker Tools, Techniques, Exploits and Incident Handling

Version: Demo

QUESTION 1

Which of the following attacks allows an attacker to retrieve crucial information from a Web server\\'s database?

A. Database retrieval attack

B. PHP injection attack

C. SQL injection attack

D. Server data attack

Correct Answer: C

QUESTION 2

Which of the following penetration testing phases involves reconnaissance or data gathering?

A. Attack phase

B. Pre-attack phase

C. Post-attack phase

D. Out-attack phase

Correct Answer: B

QUESTION 3

OutGuess is used for _____ attack.

A. Steganography

B. Web password cracking

C. SQL injection

D. Man-in-the-middle

Correct Answer: A

QUESTION 4

Adam works as an Incident Handler for Umbrella Inc. He has been sent to the California unit to train the members of the incident response team. As a demo project he asked members of the incident response team to perform the following actions:

Remove the network cable wires.

Isolate the system on a separate VLAN

Use a firewall or access lists to prevent communication into or out of the system.

Change DNS entries to direct traffic away from compromised system

Which of the following steps of the incident handling process includes the above actions?

A. Identification

B. Containment

C. Eradication

D. Recovery

Correct Answer: B

QUESTION 5

You have forgotten your password of an online shop. The web application of that online shop asks you to enter your email so that they can send you a new password. You enter your email you@gmail.com And press the submit button. The Web application displays the server error. What can be the reason of the error?

A. You have entered any special character in email.

B. Email entered is not valid.

C. The remote server is down.

D. Your internet connection is slow.

Correct Answer: A

QUESTION 6

A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS attack are as follows:

l Saturation of network resources l Disruption of connections between two computers, thereby preventing communications between services l Disruption of services to a specific computer l Failure to access a Web site l Increase in the amount of spam Which of the following can be used as countermeasures against DoS attacks? Each correct answer

represents a complete solution. Choose all that apply.

A. Blocking undesired IP addresses

B. Applying router filtering

C. Disabling unneeded network services

D. Permitting network access only to desired traffic

Correct Answer: ABCD

QUESTION 7

Which of the following types of rootkits replaces regular application binaries with Trojan fakes and modifies the behavior of existing applications using hooks, patches, or injected code?

A. Application level rootkit

B. Hypervisor rootkit

C. Kernel level rootkit

D. Boot loader rootkit

Correct Answer: A

QUESTION 8

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

A. Use of a long random number or string as the session key reduces session hijacking.

B. It is used to slow the working of victim\\'s network resources.

C. TCP session hijacking is when a hacker takes over a TCP session between two machines.

D. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

Correct Answer: ACD

QUESTION 9

Which of the following Nmap commands is used to perform a UDP port scan?

A. nmap -sY

B. nmap -sS

C. nmap -sN

D. nmap -sU

Correct Answer: D

QUESTION 10

Which of the following functions can be used as a countermeasure to a Shell Injection attack? Each correct answer represents a complete solution. Choose all that apply.

A. escapeshellarg()

B. mysql_real_escape_string()

C. regenerateid()

D. escapeshellcmd()

Correct Answer: AD

QUESTION 11

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

Correct Answer: C

QUESTION 12

Which of the following techniques can be used to map \\'open\\' or \\'pass through\\' ports on a gateway?

A. Traceport

B. Tracefire

C. Tracegate

D. Traceroute

Correct Answer: D