SEC504 Q&As

Hacker Tools, Techniques, Exploits and Incident Handling

QUESTION 1

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple small-sized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks.

Which of the following tools can be used to perform session splicing attacks? Each correct answer represents a complete solution. Choose all that apply.

A. Whisker

B. Fragroute

C. Nessus

D. Y.A.T.

Correct Answer: AC

QUESTION 2

Maria works as the Chief Security Officer for PassGuide Inc. She wants to send secret messages to the CEO of the company. To secure these messages, she uses a technique of hiding a secret message within an ordinary message. The technique provides \\'security through obscurity\\'.

What technique is Maria using?

A. Steganography

B. Public-key cryptography

C. RSA algorithm

D. Encryption

Correct Answer: A

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. On the We-are-secure login page, he enters =\\'or\\'\\'=\\' as a username and successfully logs in to the user page of the Web site.

The we-are-secure login page is vulnerable to a __________.

A. Dictionary attack

B. SQL injection attack

C. Replay attack

D. Land attack

Correct Answer: B

QUESTION 4

Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

A. Kernel keylogger

B. Software keylogger

C. Hardware keylogger D. OS keylogger

Correct Answer: C

QUESTION 5

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 6

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

A. It provides special tunneling, such as UDP to TCP, with the possibility of specifying all network parameters.

B. It can be used as a file transfer solution.

C. It provides outbound and inbound connections for TCP and UDP ports.

D. The nc -z command can be used to redirect stdin/stdout from a program.

Correct Answer: ABC

QUESTION 7

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

QUESTION 8

You work as a System Administrator in SunSoft Inc. You are running a virtual machine on Windows Server 2003. The virtual machine is protected by DPM. Now, you want to move the virtual machine to another host.

Which of the following steps can you use to accomplish the task? Each correct answer represents a part of the solution. Choose all that apply.

A. Remove the original virtual machine from the old server and stop the protection for the original virtual machine.

B. Run consistency check.

C. Add the copied virtual machine to a protection group.

D. Copy the virtual machine to the new server.

Correct Answer: ACD

QUESTION 9

Which of the following refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system?

A. Piggybacking

B. Hacking

C. Session hijacking

D. Keystroke logging

Correct Answer: C

QUESTION 10

Which of the following programs is used for bypassing normal authentication for securing remote access to a computer?

A. Backdoor

B. Worm

C. Adware

D. Spyware

Correct Answer: A

QUESTION 11

Which of the following is the most common vulnerability that can affect desktop applications written in native code?

A. SpyWare

B. DDoS attack

C. Malware

D. Buffer overflow

Correct Answer: D

QUESTION 12

Which of the following functions can you use to mitigate a command injection attack? Each correct answer represents a part of the solution. Choose all that apply.

A. escapeshellarg()

B. escapeshellcmd()

C. htmlentities()

D. strip_tags()

Correct Answer: AB

QUESTION 13

Which of the following actions is performed by the netcat command given below? nc 55555

A. It changes the /etc/passwd file when connected to the UDP port 55555.

B. It resets the /etc/passwd file to the UDP port 55555.

C. It fills the incoming connections to /etc/passwd file.

D. It grabs the /etc/passwd file when connected to UDP port 55555.

Correct Answer: D

QUESTION 14

Which of the following types of attacks is often performed by looking surreptitiously at the keyboard or monitor of an employee\\'s computer?

A. Buffer-overflow attack

B. Shoulder surfing attack

C. Man-in-the-middle attack

D. Denial-of-Service (DoS) attack

Correct Answer: B

QUESTION 15

Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

A. Denial of Service attack

B. Replay attack

C. Teardrop attack

D. Land attack

Correct Answer: A