NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment Solution- Week 9

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following statement(s) is/are true for sniffing?

a. It is a process of analyzing network activity by capturing network traffic.
b. It is a process of finding the vulnerability in a network.
c. It is a process used for user enumeration.
d. None of these.

Correct Answer: a

Detail Solution: Sniffing is a process of analyzing network activity by capturing network traffic. Using a sniffing tool we can capture network data and display them in a readable format; we can capture network log for forensics and evidence.

Thus the correct option is (a).

QUESTION 2 :

Consider the following statements.
(i) Burp suite is a popular tool used for sniffing.
(ii) Using Burp suite we can perform password attack on web applications.

a. Only (i) is true.
b. Only (ii) is true.
c. Both (i) and (ii) are true.
d. Both (i) and (ii) are false.

Correct Answer: c

Detail Solution: Burp suite is a tool that can be used for sniffing. With the help of payload option available in intruder module, we can also perform password attack on web applications.

The correct option is (c).

QUESTION 3:

What is the purpose of repeater module available in burp suite?

a. It is used to mount password attack.
b. It is used for manipulating and reissuing packets and to analyze their response.
c. It is used for creating dictionary.
d. None of these.

Correct Answer: b

Detail Solution: Repeater module is used for manipulation and reissuing packets, it analyzes the response of manipulated packet.

The correct option is (b).

QUESTION 4:

Which of the following approach(es) cannot protect against sniffing?

a. Restrict physical access to the network media.
b. Permanently add the MAC address of gateway to ARP cache.
c. Use encryption to protect confidential information.
d. Use dynamic IP address and ARP entries.
e. None of these.

Correct Answer: d

Detail Solution: To protect against sniffing following countermeasures can be used:

(a) Restrict the physical access to the network media to ensure that a packet sniffer cannot be installed; (b) Use encryption to protect confidential information; (c) Permanently add the MAC address of the gateway to the ARP cache; (d) Use static IP addresses and static ARP tables to prevent attackers from adding spoofed ARP entries for their machines to the network; (e) Turn off network identification broadcasts, and if possible, restrict the network to authorized users in order to protect the network from being discovered with sniffing tools; (f) Use the IPv6 instead of the IPv4 protocol; (g) Use encrypted sessions such as Secure Shell (ssh) instead of Telnet; (h) Use Secure Copy (scp) instead of a file transfer protocol (ftp); (i) Use Secure Socket Layer (SSL) for email connections.

However if we use dynamic IP address and ARP entries then an attacker can mount arpspoof attack and can change the NIC of the system in promiscuous mode.

The correct option is (d).

QUESTION 5:

Which of the following is/are example(s) of human-based social engineering attack?

a. Impersonation
b. Piggybacking
c. Shoulder surfing
d. Pop-up windows
e. Chain letters
f. phishing

Correct Answer: a, b, c

Detail Solution: The options (a), (b) and (c) are example of human-based social engineering attacks, while d, e and f are examples of computer-based social engineering attack.

The correct options are (a), (b) and (c).

QUESTION 6:

Which of the following tools can be used for social engineering attack?

a. Dnsenum
b. Hydra
c. Crunch
d. SEToolkit
e. Arpspoof

Correct Answer: d

Detail Solution: Social Engineering Toolkit (SEToolkit) is used to perform social engineering attacks. Whereas Dnsenum is used for user enumeration; Hydra and Crunch are used for password attack; arpspoof tool is used for arpspoofing.

The correct option is (d).

QUESTION 7:

Which of the following protocols is/are not vulnerable to sniffing attack?

a. HTTP
b. Telnet
c. SSH
d. SSL

Correct Answer: c, d

Detail Solution: SSH and SSL exchange data over secure channel, HTTP, Telnet, rlogin and FTP protocols exchange data in plain text (unsecured form), thus it is vulnerable to sniffing attack.

The correct options are (c) and (d).

QUESTION 8:

Which of the following can be used as a countermeasure for DoS/DDoS attack?

a. Replicate servers to provide additional failsafe protection.
b. Increase bandwidth on critical connections.
c. Secure the infrastructure using approaches such as anti-spam, content filtering, anti-trojan, firewalls, and load balancing.
d. Shut down all services until the attack has subsided.
e. None of this.

Correct Answer: a, b, c, d

Detail Solution: All measures given in option (a) to (d) can be used to protect against DoS/DDoS attacks.

The correct options are (a), (b), (c) and (d).

QUESTION 9:

Which of the following tool/approach cannot be used to perform DoS attack?

a. Hping3 tool
b. “http-slowloris” nmap script
c. LOIC tool
d. Hydra and Crunch.

Correct Answer: d

Detail Solution: We can perform DoS attack using Slowloris script, Hping tool as well as using LOIC tool. Hydra and Crunch tool are used for password cracking.

The correct option is (d).

QUESTION 10:

For mounting DoS attack using hping3 tool how many packets will be send per second if we use --faster option?

a. 10
b. 100
c. 1000
d. 10000

Correct Answer: b

Detail Solution: -- faster option allows the sending 100 packets in a second.

The correct option is (b).

**************END*********