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 protocols is/are vulnerable to sniffing attack?

a. HTTP
b. Telnet
c. HTTPS
d. SSL
e. None of these.

Correct Answer: a, b

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

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

QUESTION 2:

In Wireshark, which filter will show only packets for the IP address of 192.168.1.100?

a. ip == 192.168.1.100
b. ip.addr == 192.168.1.100
c. ip.address = 192.168.1.100
d. src == 192.168.1.100.
e. None of these.

Correct Answer: b

Detail Solution: To filter all packets which belongs to a specific IP we can use “ip.addr == <IP address >” filter.

The correct option is (b).

QUESTION 3 :

Consider the following statements.
(i) Burp suite can be 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 4:

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. It is used for auto crawling web applications.
e. 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 5:

In Burp suite which of the following modules is used for auto crawling of webpages.

a. Spider
b. Scanner

c. Intruder
d. Proxy
e. None of these.

Correct Answer: a

Detail Solution: Spider module is used for auto crawling, scanner is used for vulnerability scanning, intruder is used for automatic customized attack against web application, proxy module gives a direct view of how target application works by working as proxy server. It gives facility to intercept, inspect and modify raw traffic of the application.

The correct option is (a).

QUESTION 6:

Which of the following approach(es) can protect against sniffing?

a. Permanently add the MAC address of gateway to ARP cache.
b. Use unencrypted session such as telnet, ftp.
c. Restrict physical access to the network media.
d. Use static IP addresses and static ARP tables.
e. None of these.

Correct Answer: a, c, 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.

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

QUESTION 7:

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 8:

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

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

Correct Answer: a, b, c

Detail Solution: The options (a), (b) and (c) are examples 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 9:

How does Slowloris attack work?

a. It sends a single large ping packet to victim system.
b. It sends large number ARP packet to the victim system.

c. It sends large number of ICMP packets.
d. None of these.

Correct Answer: d

Detail Solution: It sends multiple HTTP packets to connect with the victim system, but never completes the connection resulting DoS for legitimate users.

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: --fast options 10 packets for a second, -- faster option allows the sending 100 packets in a second, --flood options sends packet as fast as possible.

The correct option is (b).

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