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:

In promiscuous mode, a network device, such as an adapter on a host system, can intercept and read all traffic on the network segment to which the adapter is connected.

a. True
b. False

Correct Answer: a

Detail Solution: In computer networking, promiscuous mode is a mode of operation, as well as a security, monitoring and administration technique which is mostly used for network analyzer tools such as Wireshark and burpsuit. In promiscuous mode, a network device, such as an adapter on a host system, can intercept and read in its entirety each network packet that arrives.

Thus the correct option is (a).

QUESTION 2:

Which of the following commands can be used to put the NIC of a machine to promiscuous mode? (Assumption: Machine IP - 192.168.43.48, IP of default gateway - 192.168.43.141, the machine is connected with eth0 interface).

a. arpspoof 192.168.43.48
b. arpspoof 192.168.43.141
c. arpspoof –i eth0 192.168.43.48
d. arpspoof –i eth0 192.168.43.141

Correct Answer: d

Detail Solution: To put any machine (say M) into promiscuous mode we need to send fake ARP messages to all devices stating that the MAC address of default gateway is changed to the MAC address of the machine M.

To achieve this, arpspoof tool is used, and the command used for the same is arpspoof –i 192.168.43.141.

The correct option is (d).

QUESTION 3:

In Wireshark, to filter all the packets used by an IP address 23.36.4.106, which of the following filter option/command can be used?

a. 23.36.4.106
b. ip == 23.36.4.106
c. ip.addr == 23.36.4.106
d. ip.address = 23.36.4.106
e. None of these.

Correct Answer: c

Detail Solution: To filter all packets "ip.addr ==" option is used along with the IP address.

The correct option is (c).

QUESTION 4:

A simple packet analyzer tool such as Wireshark can capture login credential of a user if the login page is using the following Protocol:

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

Correct Answer: a

Detail Solution: Wireshark can capture credentials of webpages which uses unsecure protocols such as HTTP, FTP.

The correct option is (a).

QUESTION 5:

How to detect whether network sniffing is probably going on in a network?

a. By checking the ARP entry.
b. By conducting TCP stealth scan on all the machines in the network.
c. By using a script that checks whether any of the machines has the network card configured in the promiscuous mode.
d. None of these.

Correct Answer: a, c

Detail Solution: By manually checking the ARP entry we can identify if any system is using same MAC address as the MAC of default gateway, which basically indicates that that particular system is configured in the promiscuous mode.

Using the following NMAP command, we can find out whether any of the network cards on the network is configured in the promiscuous mode. (It is done by broadcasting fake ARP packets)

nmap –script=sniffer-detect <IP addresses to check>

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

QUESTION 6:

What is the purpose of scanner 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 automotive crawling web applications.
e. None of these.

Correct Answer: e

Detail Solution: Scanner module is used for finding vulnerabilities in web applications.

The correct option is (e).

QUESTION 7:

In Burp suite which of the following module is used to intercept, inspect and modify raw traffic?

a. Spider
b. Scanner
c. Intruder
d. Proxy
e. None of these.

Correct Answer: d

Detail Solution: Spider module is used for automotive 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 (d).

QUESTION 8:

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

a. Impersonation
b. Tailgating
c. Shoulder surfing
d. Chain letters
e. phishing

Correct Answer: d, e

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

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

QUESTION 9:

How does Slowloris attack work?

a. It sends a single large ping packet to victim system.
b. It sends multiple HTTP requests to the victim system but never completes the request.
c. It sends large number ARP packet to the victim system.
d. None of these.

Correct Answer: b

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

The correct option is (b).

QUESTION 10:

Which of the following tools can be used to mount DoS attack?

a. LOIC tool.
b. Hping3.
c. Hydra.
d. Crunch.
e. None of these.

Correct Answer: a, b,

Detail Solution: LOIC and Hping3 tools can be used for DoS attack, Hydra and Crunch are used for password attack.

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

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