Course Name: ETHICAL HACKING

Assignment- Week 12

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 9 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following options can be used for host discovery using NMAP?

a. –PE
b. –PC
c. –PM
d. –PP

Correct Answer: a, c, d

Detail Solution: For host discovery using NMAP various options can be used, the most common option is ping sweep. –PE is used for ICMP ECHO Sweep, -PP and –PM is used for ICMP NON-ECHO ping sweep scanning. There is no option as –PC.

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

QUESTION 2:

Which of the following packets will be received in response form a target if an attacker sends out an ICMP ECHO request (Type 8) packet (Assume that the target is live).

a. ICMP Echo Request (Type 8)
b. ICMP Echo Reply (Type 0)
c. ICMP Timestamp reply (Type 14)
d. ICMP Address mask reply (Type 18)

Correct Answer: b

Detail Solution: In response to ICMP Echo request, if the host is live we will receive an ICMP Echo reply (Type 0) packet. If the host is down we will not get any response form the target system.

The correct option is (b).

QUESTION 3:

In TCP sweep scan, a scanner sends a “S” packet (Synchronization) and receives a “RA” packet (Reset) from target. What does it indicates?

a. Target is alive/up.
b. Target is down.

Correct Answer: b

Detail Solution: TCP sweep is carried out using the –PS, –PA option in NMAP. It is also done by some default options such as –sT, -p, -Pn.

In TCP sweep scan using –PS option, Synchronization packet (S) is sent from attacker system, if the attacker get an Acknowledge packet (SA) as response then it conclude the target system as up, and if it receives a Reset (RA) packet then attacker systems conclude that the target is down.

The correct option is (b).

QUESTION 4:

To see why NMAP is reporting any port as open or close (or a host as up or down) which of the following options is used?

a. --disable-arp-ping
b. --packet-trace
c. --show-reason
d. --reason

Correct Answer: d

Detail Solution: disable-arp-ping option is used to disable arp request for host scanning, packet-trace option is used to trace the incoming and outgoing packets, reason option is used to see why nmap is reporting any port as open or close or any host as up and down. There is no option called show-reason.

The correct option is (d).

QUESTION 5:

Which of the following scanning options uses all type of sweep operations (except UDP sweep)?

a. –sn
b. –PE
c. –PP
d. None of these

Correct Answer: a

Detail Solution: By default NMAP uses all type of sweep operations in common scanning options such that it can get better details about any system. Options that use all type of sweep operations are –sP, -sn, -sl, -Pn.

If we use options such as –PE and PP, then specific sweep operation (ICM sweep operation) will be performed.

The correct option is (a).

QUESTION 6:

Which of the following NMAP scans completes 3-way handshake?

a. ICMP Echo Sweep Scan
b. ICMP Non-Echo Sweep Scan
c. TCP Connect Scan
d. TCP Stealth Scan

Correct Answer: c

Detail Solution: When we do not have root privilege then for scanning we can use TCP connect scan (-sT) option which done port scanning by completing a TCP 3 way handshake process. ICMP Echo and Non-Echo sweep scan use ICMP packets. TCP stealth scan uses TCP 3 way handshake but it never completes the third step.

The correct option is (c).

QUESTION 7:

In NMAP, __________ number of ports are scanned when we use –F option.

Correct Answer: 100

Detail Solution: By default NMAP scans for top 1000 ports, if we use –F option then top 100 ports are scanned.

QUESTION 8:

Which of the following NMAP option is used for OS detection?

a. –sL
b. –sP
c. –PO
d. –sU
e. None of these.

Correct Answer: e

Detail Solution: For OS detection –O option is used, we can also use –A option which is known as aggressive scan which can be used for OS, version and vulnerability scanning.

The correct option is (e).

QUESTION 9:

Which of the following protocols are vulnerable to sniffing attack?

a. HTTP
b. HTTPS
c. SSL
d. SSH
e. FTP

Correct Answer: a, e

Detail Solution: The protocols that does not uses secure channel for data transfer such as HTTP, FTP are vulnerable to sniffing.

Thus correct options are (a) and (e).

QUESTION 10:

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

a. While running network analyzer tool such as sniffer, it is necessary to enable promiscuous mode.
b. In promiscuous mode the sniffer can read all traffic on the network segment to which the NIC is connected.
c. We do not require root privilege to set the NIC to promiscuous mode.
d. All of these.

Correct Answer: a, b

Detail Solution: In computer networking, promiscuous mode is a mode of operation, as well as a security, monitoring and administration technique that 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 (irrespective of sender and receiver). We need root privilege to enable promiscuous mode in the device.

Thus the correct option is (a).

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