Course Name: ETHICAL HACKING

Assignment- Week 12

TYPE OF QUESTION: MCQ/MSQ/SA

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

QUESTION 1:

Which of the following can be done with the help of NMAP tool?

a. Determine the live host.
b. Determine the services running on any target system.
c. Determine the OS of the target systems.
d. Identify the vulnerabilities of the target system.

Correct Answer: a, b, c, d

Detail Solution: NMAP can perform all of the above operations (except option d). NMAP can perform password attack; however, it uses the default dictionary available in the system.

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

QUESTION 2:

Which of the following options ***cannot be used*** for host discovery using NMAP?

a. –PE
b. –PC
c. –PM
d. –PP

Correct Answer: b

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 option is (b).

QUESTION 3:

In ICMP (ECHO) sweep scan, a scanner sends an ICMP type-8 packet and receives an ICMP type-0 packet from target. What does it indicate?

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

Correct Answer: a

Detail Solution: If the sender receives ICMP type-0 packet, this indicates that the target is up. The correct option is (a).

QUESTION 4:

Which of the following NMAP options can be used for TCP sweep scan?

a. –PE
b. –PP
c. –PM
d. None of these.

Correct Answer: d

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

The correct option is (d).

QUESTION 5:

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. None of these.

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 6:

Which of the following sweep scans are automatically done when we use –sn option.

a. ICMP Echo
b. ICMP Non-Echo
c. TCP Sweep
d. UDP Sweep

Correct Answer: a, b, c

Detail Solution: All type of sweep options are used with –sn option except UDP sweep.

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

QUESTION 7:

The number of host (IP) scanned by NMAP command “nmap –sL 192.168.62.40-50” will be _____.

Correct Answer: 11

Detail Solution: The given command will scan all hosts with IP addresses 192.168.62.40 to 192.168.62.50 (including both the IPs).

Thus, a total of 11 IP addresses will be scanned.

QUESTION 8:

In NMAP by default, _____ number of ports are scanned.

Correct Answer: 1000

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

QUESTION 9:

Which of the following NMAP options treats all hosts as online (skip host discovery)?

a. –sP
b. –PO
c. –sU
d. –Pn

Correct Answer: d

Detail Solution: -sP is used for only determining if the host is online; -PO is used for IP protocol ping; -sU is used for UDP scan; -Pn is used to skip host discovery and treats all host as online

The correct option is (d).

QUESTION 10:

Which of the following NMAP options is used for Service and Version 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, for services and version detection –sV option is used.

The correct option is (e).

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