NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

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:

With help of NMAP tool:

a. We can determine which host are alive.
b. We can determine the services running on any target system.
c. We can determine the OS of the target systems.
d. We can create a dictionary.
e. We can identify the vulnerabilities of the target system.

Correct Answer: a, b, c, e

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. For creating dictionary, secondary tools such as crunch is used.

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

QUESTION 2:

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

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 3:

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 4:

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 5:

The number of host (IP) scanned by NMAP command “nmap –sL 192.168.62.48-58” will be _____.

Correct Answer: 11

Detail Solution: The given command will scan all hosts with IP addresses 192.168.62.48 to 192.168.62.58 (including both the IPs).

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

QUESTION 6:

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

a. –sL
b. –sP
c. –PO
d. –sU
e. –Pn

Correct Answer: e

Detail Solution: -sL is used to list all IPs for scan; -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 (e).

QUESTION 7:

How many ports will be scanned using NMAP command “nmap --top-ports 5 Target_IP”?

a. 5
b. 100
c. 1000
d. 65535

Correct Answer: a

Detail Solution: --top-ports option is used to scan top ports, 5 represents that top 5 ports will be scanned by this NMAP command.

Thus correct option is (a).

QUESTION 8:

In NMAP by default _____ number of ports are scanned.

Correct Answer: 1000

Detail Solution: By default NMAP scans for top 1000 ports.

QUESTION 9:

In NMAP scan, a filtered port indicates that either the firewall or any other filter software is blocking nmap requests.

a. True.
b. False

Correct Answer: a

Detail Solution: An Open port indicates that some service are running on the port and nmap can identify this, a filtered port indicates that nmap cannot access that as some filtering software is blocking nmap request.

Thus, the correct option is (a).

QUESTION 10:

Which of the following NMAP options can be used for OS, Services and Version detection?

a. –PE
b. –PP
c. –sV
d. –O

Correct Answer: c, d

Detail Solution: For OS detection –O option is used, whereas for services and version detection –sV option is used.

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

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