# Course Name: ETHICAL HACKING

## Assignment- Week 12

### TYPE OF QUESTION: MCQ/MSQ/SA

**Number of questions**: 10 **Total mark: 8 x 1.25 = 10**

---

**QUESTION 1:**

**NMAP command can be used for?**

a. Host Discovery
b. Port Scanning
c. Service and Version Detection
d. OS Detection
e. Vulnerability Scanning

**Correct Answer: a, b, c, d, e**

**Detail Solution:** NMAP can perform all of the above operations. Along with this we can also perform brute force attack using NMAP scripts.

---

**QUESTION 2:**

**In UDP sweep scan, a scanner sends a UDP datagram and receives an ICMP port unreachable message 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 port unreachable packet this indicates that the target is up. The correct option is (a).

---

**QUESTION 3:**

**Which NMAP options can be used for UDP sweep scan?**

a. -PS

b. -PU
c. –sU
d. -PE
e. None of these.

**Correct Answer: b, c**

**Detail Solution:** UDP sweep is carried out using the –PU or –sU option in NMAP. Hence, the correct answers are (b) and (c).

---

**QUESTION 4:**

How many host (IP) will be scanned by following NMAP command?

```
nmap -sL 192.168.62.48/24
```

a. 256
b. 1024
c. 24
d. 2

**Correct Answer: a**

**Detail Solution:** The given command will scan all hosts with IP addresses 192.168.62.0 to 192.168.62.255

Thus, a total of 256 IP addresses will be scanned. The correct option is (a).

---

**QUESTION 5:**

Consider the following statements and answers.

(i) An open port indicates that some application is running on the target system on that particular port.

(ii) A filtered port indicates that either the firewall or any other filter software is blocking nmap request.

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:** 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 the nmap request.

Thus, both statements (i) and (ii) are correct.

---

**QUESTION 6:**

By default how many ports are scanned using –F and –p option respectively?

a. 100, 1000
b. 1000, 100
c. 65536, 65536
d. None of these.

**Correct Answer: a**

**Detail Solution:** -F and –p option scans top 100 and 1000 ports respectively.

Thus, the correct option is (a).

---

**QUESTION 7:**

Which of the following NMAP commands are valid?

a. nmap 192.168.62.43
b. nmap www.nptel.ac.in
c. nmap 192.168.62.43-48
d. nmap 192.168.62.43,44,45

**Correct Answer: a, b, c, d**

**Detail Solution:** All the given nmap commands are valid.

---

**QUESTION 8:**

Which of the following statement(s) is/are false for sniffing tools like Wireshark/Burpsuite?

a. They can capture packets from almost all network protocols like TCP, IP.
b. Some sniffing tools support packet manipulation.

c. Some sniffing tools can also be used for scanning vulnerabilities in web applications.
d. None of these.

**Correct Answer: d**

**Detail Solution:** Sniffing tools can capture packets from almost all the known network protocols, some sniffing tools can be used for packet manipulation and vulnerability scanning, viz. burp suite.

The correct option is (d).

---

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