



**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 option is used for ICMP echo sweep in NMAP?

- a. -PE
- b. -PS
- c. -PP
- d. -PM

**Correct Answer: a**

**Detail Solution:** The -PE option is used for ICMP Echo requests (type 8). If replies are received, the host is alive.

The correct option is (a).

---

**QUESTION 2:**

In ICMP Sweep, receiving ICMP Type 0 reply indicates:

- a. Target host is down
- b. Target host is alive
- c. Target host is filtered
- d. None of these.

**Correct Answer: b**

**Detail Solution:** ICMP type 0 is Echo reply, if it is received that means the target is alive.

The correct option is (b).

---



**QUESTION 3:**

By default NMAP scans how many ports?

- a. 10
- b. 100
- c. 1000
- d. 65536

**Correct Answer: c**

**Detail Solution:** NMAP by default scans top 1000 ports.

The correct option is (c).

---

**QUESTION 4:**

Which option makes NMAP treat all host as online (skip host discovery)?

- a. -SP
- b. -PO
- c. -Pn
- d. -F

**Correct Answer: c**

**Detail Solution:** -Pn skips host discovery and treats all hosts as online.

The correct option is (c).

---

**QUESTION 5:**

Which scanning technique uses full 3-way handshake?

- a. TCP SYN scan
- b. TCP Connect scan
- c. ICMP Sweep scan
- d. FIN scan

**Correct Answer: b**



**Detail Solution:** TCP Connect scan (-sT) uses complete 3-way handshake. TCP SYN scan is half-open. FIN and ICMP are not related to TCP 3-way handshake.

The correct option is (b).

---

### **QUESTION 6:**

Assume we are running Wireshark in a host, if the NIC of the host is set in promiscuous mode, what Wireshark will do:

- a. It will capture packets only oriented to that host
- b. It will capture all packets in the same network segment in which host is connected.
- c. It will encrypt all captured packet.
- d. It will block all malicious traffic.

**Correct Answer: b**

**Detail Solution:** Promiscuous mode allows NIC to capture all packets in the network segment, not just its own traffic.

The correct option is (b).

---

### **QUESTION 7:**

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

- a. -O
- b. -TO
- c. -SO
- d. None of these

**Correct Answer: a**

**Detail Solution:** -O option enables OS detection in NMAP. There is no -TO, -SO option.

The correct option is (a).

---



### **QUESTION 8:**

Which of the following can be detected using service/version detection (-sV)?

- a. Application name
- b. Application version
- c. OS fingerprint
- d. Vulnerability status

**Correct Answer: a, b**

**Detail Solution:** The -sV option probes open ports to detect the application name and version. OS fingerprinting is done with -O, and vulnerabilities require scripts.

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

---

### **QUESTION 9:**

Which NMAP option allows scanning only the most common 10 ports?

- a. -p 10
- b. -r 10
- c. --top-ports 10
- d. -top 10

**Correct Answer: c**

**Detail Solution:** The --top-ports <N> option scans the most common N ports instead of the full range. -top is not a valid option, -r is for ordering/randomization, with -p only port 10 will be scanned.

The correct option is (c).

---

### **QUESTION 10:**

In which default format does Wireshark save captured packets?

- a. .txt
- b. .csv
- c. .xml
- d. .pcapng/.pcap



---

**Correct Answer: d**

**Detail Solution:** Wireshark saves captured packets by default in .pcapng (Packet Capture Next Generation) format (.pcap in older version). It can also export to other formats (TXT, CSV, XML, JSON), but the default is .pcapng.

The correct option is (d).

---

\*\*\*\*\*END\*\*\*\*\*