**NMAP:** Nmap is **a network scanner**, not a magical bypass tool. It can help **detect firewalls/IDS/IPS/AV**, but bypassing them is illegal unless done in your own lab or with explicit authorization (VAPT/Red Team).

---

### 1. How can bypass all types of firewalls?

👉 Real-world: You **cannot bypass ALL firewalls** with Nmap. You can attempt to **evade detection** by using timing, fragmentation, decoys, spoofing.

```
nmap -Pn -f -T2 -D RND:10 <target>
```

- -Pn → Skip host discovery (firewalls may block ICMP ping).
- -f → Fragment packets (bypass packet filters).
- -T2 → Slow timing (avoid detection by IDS/IPS).
- -D RND:10 → Use 10 decoy IPs (hide your real IP).

---

### 2. How can identify which type of firewall is detected?

Use **firewalk**-like scanning (--traceroute) + TTL analysis.

**Command:**

```
nmap -Pn -p 80,443 --traceroute <target>
```

- Check where packets drop → indicates firewall hop.

Or test with different scan types:

```
nmap -sS -p 80 <target>   # SYN Scan
nmap -sA -p 80 <target>   # ACK Scan (firewall stateful?)
nmap -sN -p 80 <target>   # Null Scan
```

- SYN works but ACK drops? → Stateful firewall.
- All blocked? → Stateless packet filter.

---

### 3. How can scan a network so firewall does not detect Nmap?

**Stealth + evasion techniques:**

```
nmap -sS -T0 -f -D RND:5 --data-length 50 <target>
```

- -sS → Stealth SYN scan.
- -T0 → Very slow (harder to detect).
- --data-length 50 → Add junk data (evade IDS signatures).

---

### 4. How to scan all services?

```
nmap -sV <target>
```

- -sV → Service version detection.

---

### 5. How to scan all ports?

```
nmap -p- <target>
```

- -p- → Scan all 65,535 TCP ports.

---

### 6. How to scan all open IP/hosts in a network?

```
nmap -sn 192.168.1.0/24
```

- -sn → Ping scan (discover live hosts).

---

### 7. How to scan only open ports?

```
nmap --open -p- <target>
```

- --open → Show only open ports.

---

### 8. How to scan only closed ports?

```
nmap -p- --reason <target> | grep "closed"
```

- Nmap normally doesn't show closed-only → use --reason & filter.

---

### 9. How to identify if firewall is active or not?

```
nmap -sA -p 80 <target>
```

- -sA (ACK scan) → If "filtered" → firewall present.
- If "unfiltered" → no firewall.

---

### 10. How to identify if firewall is configured or not?

**Compare -sS vs -sA results:**

- If -sS blocked but -sA works → firewall configured.

- If both work → no firewall.

---

### 11. How to scan/detect that endpoint has antivirus?

👉 **Nmap alone cannot directly detect AV.**
**But some NSE scripts try:**

```
nmap --script av* <target>
```

(rarely reliable, mostly SNMP/WMI dependent).

---

### 12. How to detect which type of antivirus endpoint has?

👉 Nmap **cannot fingerprint specific AV products**. You need **EDR/Endpoint agent logs** or **privilege access**.

Bypass: Use evasion **scans (-f, -D, --data-length).**

---

### 13. How to scan which type of OS is running?

```
nmap -O <target>
```

- -O → OS fingerprinting.
- --osscan-guess → Aggressive guess.

---

### 14. How to detect if IDS/IPS configured or not?

Test normal scan vs stealth scan:

```
nmap -sS <target>
```

```
nmap -sN <target>
```

- If normal blocked but null/fragment works → IDS/IPS present.

**Bypass:**

```
nmap -f -sS -T1 <target>
```

---

### 15. How to scan running services versions?

```
nmap -sV <target>
```

- Gets software + version (e.g., Apache 2.4.41).

---

### 16. Can we scan closed/stopped services versions?

❌ No.

- If service is **closed/stopped**, it doesn't respond → version cannot be fingerprinted.
- You only see closed or filtered.

---

### ✅ Summary Table

| **Task** | **Command** |
|---|---|
| Bypass FW | nmap -Pn -f -D RND:10 <target> |
| Detect FW type | nmap -sA -p 80 <target> |
| Evade detection | nmap -sS -T0 -f --data-length 50 <target> |
| All services | nmap -sV <target> |
| All ports | nmap -p- <target> |
| Live hosts | nmap -sn 192.168.1.0/24 |
| Only open ports | nmap --open -p- <target> |
| Only closed ports | ` nmap -p- --reason <target> |
| Firewall active? | nmap -sA -p 80 <target> |
| Firewall configured? | Compare -sS vs -sA |
| Detect AV | nmap --script av* <target> (limited) |
| Detect AV type | ❌ Not reliable with Nmap |
| OS detection | nmap -O <target> |
| IDS/IPS detection | Compare scans (-sS vs -sN) |
| Running services versions | nmap -sV <target> |
| Closed service versions | ❌ Not possible |