# Module 03: Scanning Networks

Scanning is the second phase of the ethical hacking methodology. While footprinting (Module 2) provides a broad overview, scanning is used to identify specific live hosts, open ports, and services running on a network.

## 1. Scanning Concepts

### The Objectives of Scanning

* **Identify Live Systems:** Determine which IP addresses are active on the network.
* **Discover Open Ports:** Identify which ports are listening for connections.
* **Identify Services:** Determine what applications and versions are running (Banner Grabbing).
* **Identify OS:** Guess the Operating System based on packet responses.
* **Identify Vulnerabilities:** Find known weaknesses in the identified services.
* **Map the Network:** Create a diagram of the target infrastructure.

### The Scanning Process (Steps)

1. **Check for Live Systems:** Use Ping Sweeps or ICMP scans.
2. **Check for Open Ports:** Perform various TCP/UDP port scans.
3. **Service/Banner Grabbing:** Interact with the port to see the software version.
4. **Vulnerability Scanning:** Use automated tools to find CVEs.
5. **Draw Network Diagrams:** Visualize the results.
6. **Prepare Proxies:** Use proxies to mask your identity during the scan.

## 2. TCP Communication & Handshakes (EXAM CRITICAL)

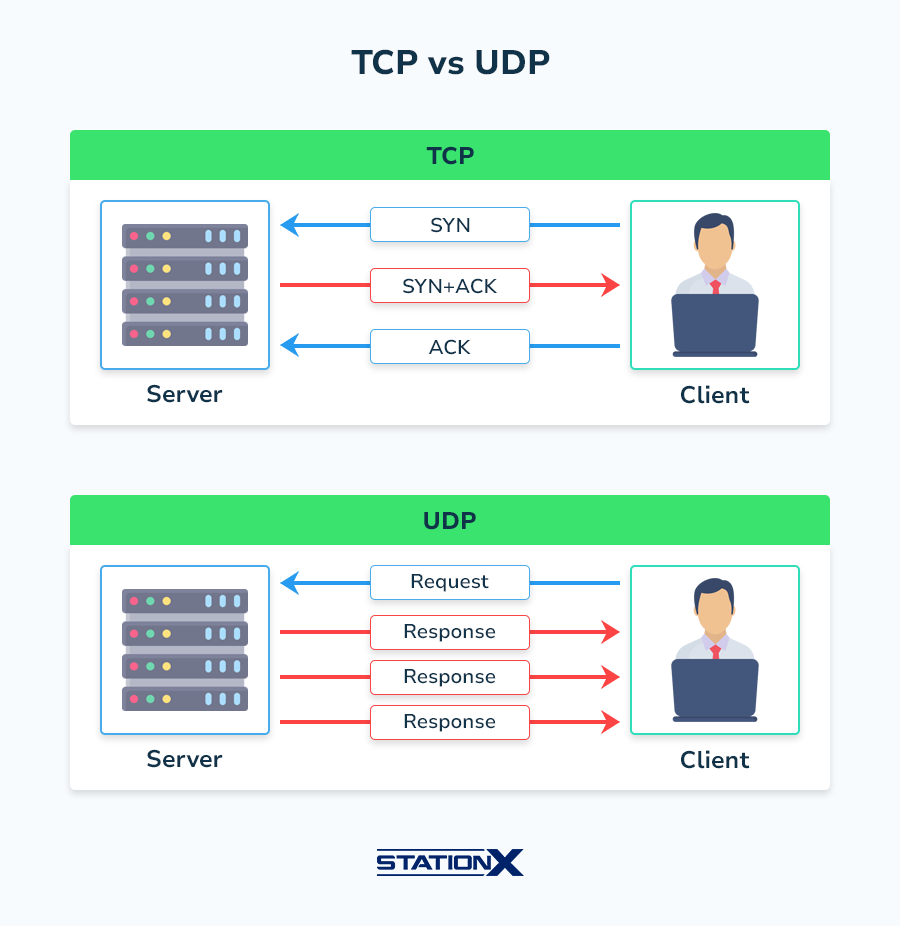
To understand Nmap scans, you must understand the **TCP 3-Way Handshake**:

1. **Client:** Sends SYN (Synchronize)
2. **Server:** Responds with SYN/ACK (Synchronize/Acknowledge)
3. **Client:** Sends ACK (Acknowledge)

### TCP Flags to Know

* **SYN:** Initiates a connection.
* **ACK:** Acknowledges receipt of a packet.
* **FIN:** Gracefully terminates a connection.
* **RST:** Resets/aborts a connection immediately.
* **PSH:** Forces data to the application layer.
* **URG:** Indicates data is urgent.

## Nmap Scanning Techniques



In Nmap, -s specifies the scan type (how the port scanning is performed).

|  |  |  |  |
| --- | --- | --- | --- |
| **Scan Type** | **Flag** | **Handshake Logic** | **Key Characteristic** |
| **TCP Connect** | -sT | SYN → SYN/ACK → ACK | Full handshake. Noisiest, easily logged. |
| **Stealth (SYN)** | -sS | SYN → SYN/ACK → RST | "Half-open." Never completes connection. Default scan. |
| **UDP Scan** | -sU | No handshake. | Slow. ICMP Unreachable means port is closed. |
| **NULL Scan** | -sN | No flags set. | Bypasses simple firewalls. Doesn't work on Windows. |
| **FIN Scan** | -sF | Only FIN set. | Inverse mapping. Doesn't work on Windows. |
| **Xmas Scan** | -sX | FIN, PSH, URG | "Lit up" flags. Doesn't work on Windows. |
| **ACK Scan** | -sA | Only ACK set. | Maps firewall rules (Filtered vs. Unfiltered). |

## 4. Scanning Tools to Memorize

Beyond Nmap, the CEH v13 curriculum requires familiarity with several specialized tools:

* **Nmap / Zenmap:** The industry standard for network discovery and security auditing.
* **Hping2 / Hping3:** Command-line oriented TCP/IP packet assembler/analyzer.
* **NetScanTools Pro:** A suite of network tools for Windows (DNS, Ping, Port Scanning).
* **Angry IP Scanner:** A very fast, cross-platform open-source network scanner.
* **Advanced IP Scanner:** A reliable and free network scanner for Windows LAN analysis.
* **Nessus:** The world's most widely used vulnerability assessment solution.
* **OpenVAS:** An open-source framework of several services and tools offering vulnerability scanning.
* **Metasploit Framework:** Contains multiple auxiliary modules specifically for port scanning and service enumeration.
* **PRTG Network Monitor:** Used for monitoring network traffic and availability.

## 5. Hping3: The Swiss Army Knife

hping3 is used for manual packet crafting. It is a favorite on the CEH exam for custom protocol testing.

|  |  |
| --- | --- |
| **Command** | **Purpose** |
| hping3 -S target.com -p 80 | Send SYN packets to port 80. |
| hping3 -1 target.com | Standard ICMP Ping. |
| hping3 -A target.com -p 80 | Send ACK packets (Firewall testing). |
| hping3 -2 target.com | UDP scan. |
| hping3 -F -P -U target.com | Xmas scan. |
| hping3 --scan 1-100 -S target.com | Port scan range 1-100. |
| hping3 -S target.com -a 1.1.1.1 | Spoof source IP to 1.1.1.1 (Decoy/Spoofing). |

## 6. Hands-On Lab Sessions (CEH v13 Practice)

### Lab 1: Host Discovery (Ping Sweep)

* **Goal:** Identify live hosts on a subnet without port scanning.
* **Tool:** Nmap
* **Command:** nmap -sn 10.10.10.0/24
* **Practical Note:** This uses ICMP Echo, Timestamp, and ARP (if local) to find active IPs.

### Lab 2: TCP Stealth Scanning and Evasion

* **Goal:** Scan a target while attempting to bypass an IDS.
* **Tool:** Nmap
* **Command:** sudo nmap -sS -f -D RND:5 10.10.10.15
* **Logic:** -sS (SYN scan), -f (Fragment packets), -D RND:5 (5 random decoys).

### Lab 3: Service Version and OS Detection

* **Goal:** Fingerprint the target's software and OS.
* **Tool:** Nmap
* **Command:** sudo nmap -sV -O -v 10.10.10.15
* **Analysis:** Observe the "Fingerprint" generated and the confidence percentage of the OS guess.

### Lab 4: Vulnerability Research with NSE

* **Goal:** Use scripts to find known weaknesses.
* **Tool:** Nmap Scripting Engine
* **Command:** nmap --script vuln 10.10.10.15
* **Common Scripts:** smb-vuln-\*, http-enum, ssl-heartbleed.

### Lab 5: Manual Packet Crafting for Firewall Auditing

* **Goal:** Determine if a firewall is stateful or stateless.
* **Tool:** Hping3
* **Command:** hping3 -A 10.10.10.15 -p 80
* **Observation:** If the firewall returns an RST, it is often a sign of a stateless firewall or that the port is "unfiltered."

### Lab 6: Vulnerability Scanning with Nessus

* **Goal:** Perform a professional-grade vulnerability assessment.
* **Tool:** Nessus
* **Action:** Create a "New Scan" -> "Basic Network Scan". Enter the target IP. Analyze the "High" and "Critical" vulnerabilities found.

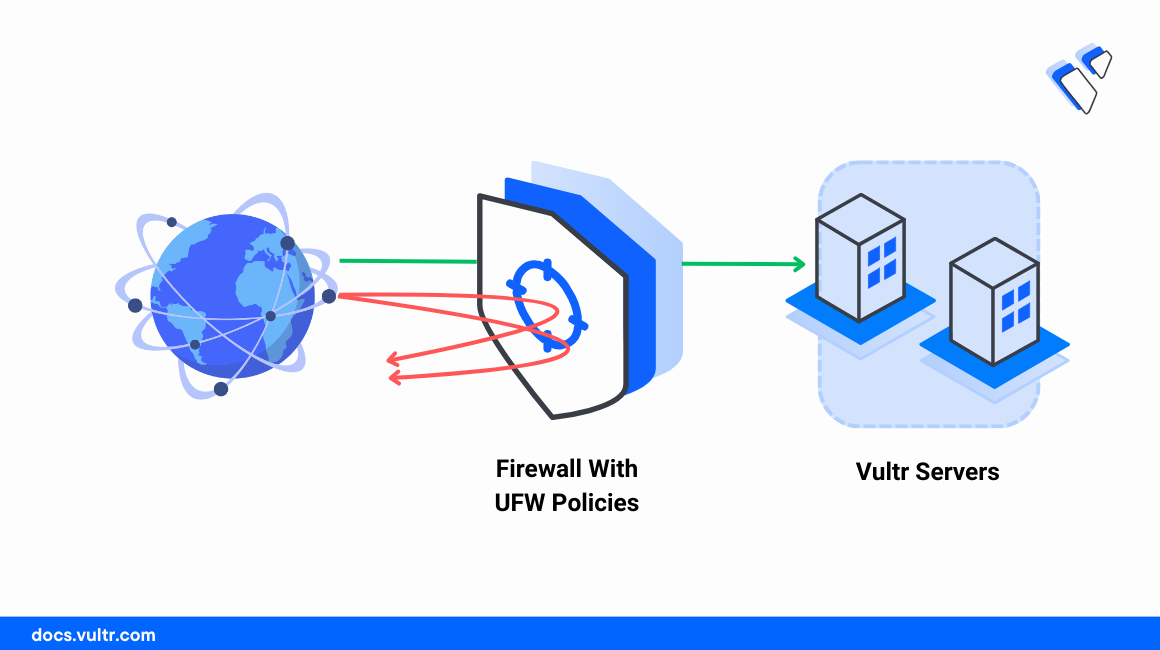
## 7. Scanning Countermeasures

* **Configure Firewalls:** Block all ICMP traffic except what is strictly necessary.
* **Intrusion Detection Systems (IDS):** Set alerts for SYN floods and "port sweeps."
* **Disable Unused Services:** Reduce the attack surface.
* **Filter Traffic:** Use Egress filtering to prevent your network from being used as a decoy.
* **Update Software:** Prevent successful banner grabbing from leading to an exploit.

**Appendix** : *Firewalls and IPS/IDS in Parrot OS*

1. *Firewall*

*Parrot OS uses* ***UFW (Uncomplicated Firewall)****, which is a front-end for iptables.*



*Check if firewall is installed*

*ufw –version*

*if not installed*

*sudo apt update*

*sudo apt install ufw -y*

*Check firewall status*

*sudo ufw status*

*If inactive then enable*

*sudo ufw enable*

*Set default rules (VERY IMPORTANT)*

*Block all incoming traffic*

*sudo ufw default deny incoming*

*Allow all outgoing*

*sudo ufw default allow outgoing*

*Allow essential services*

*sudo ufw allow ssh*

*sudo ufw allow 80/tcp*

*sudo ufw allow from 192.168.1.10*

*Verify firewall rules*

*sudo ufw status verbose*