In the hacking lifecycle, **Step 2: Scanning** comes right after **Reconnaissance**.

📌 In this phase, we use **Nmap** to:

* Identify **live hosts**
* Detect **open ports**
* Guess **services** and **OS types**
* Look for **vulnerabilities**

Let’s break it down for **beginners** using **real commands and scenarios**.

**🧠 What is Nmap?**

Nmap (Network Mapper) is a free, open-source tool used for **network discovery** and **security auditing**.

**🔧 Nmap Install (Optional if already done)**

**Linux (Debian/Ubuntu):**

sudo apt update && sudo apt install nmap

**Windows:**  
[Download Nmap from here](https://nmap.org/download.html)

**🚀 Typical Steps in Scanning with Nmap**

**✅ 1. Ping Sweep – Identify Live Hosts**

nmap -sn 192.168.1.0/24

* -sn: Ping scan only (no port scan).
* Finds **which devices are alive** in the subnet.

**✅ 2. Simple Port Scan**

nmap 192.168.1.10

* Scans **default 1000 ports** on the target IP.

**✅ 3. Aggressive Scan (Service & OS Detection + Traceroute)**

nmap -A 192.168.1.10

* -A: Aggressive scan = OS detection, version detection, script scanning, traceroute.
* **Great for pen-testers**; noisy for real attacks.

**✅ 4. Scan Specific Ports**

nmap -p 21,22,80,443 192.168.1.10

* -p: Specify which ports to scan (FTP, SSH, HTTP, HTTPS).

**✅ 5. Detect Service Version**

nmap -sV 192.168.1.10

* -sV: Attempts to determine **service version** (e.g., Apache 2.4.49).

**✅ 6. Operating System Detection**

nmap -O 192.168.1.10

* -O: Tries to detect **target OS** (Linux, Windows, etc.)
* Needs root privileges in many systems.

**✅ 7. Scan All Ports**

nmap -p- 192.168.1.10

* Scans **all 65535 TCP ports** instead of just top 1000.

**✅ 8. Stealth Scan (SYN Scan)**

sudo nmap -sS 192.168.1.10

* -sS: Stealthy SYN scan (also called half-open scan).
* Harder to detect by firewalls.

**✅ 9. UDP Port Scan**

sudo nmap -sU 192.168.1.10

* UDP scans can take longer but reveal services like DNS, SNMP.

**✅ 10. Scan Multiple Targets**

nmap 192.168.1.1 192.168.1.2 192.168.1.3

OR

nmap 192.168.1.1-10

**🧰 Bonus: Output Reports**

nmap -A -oN scan\_report.txt 192.168.1.10

* -oN: Saves results in **normal text format**.

nmap -A -oX scan\_report.xml 192.168.1.10

* -oX: XML output for parsing in tools like **Maltego** or **Splunk**.

**🕵️ Real-world Use Case**

Suppose you're testing a company’s internal server 192.168.1.10.

sudo nmap -A -p- -T4 192.168.1.10

* Full port scan + OS detection + service version
* -T4: Faster scan (but more noisy)

🎯 This gives you a **detailed fingerprint of the target**, which is crucial before exploitation.

**⚠️ Ethics & Caution**

Nmap is powerful and legal **only when used with permission** (e.g., CTFs, labs, pen-tests). Unauthorized scanning can lead to legal consequences.