Scanning

Scanning is the second phase of the hacking methodology and comes right after reconnaissance (or footprinting). While reconnaissance gathers passive and active information about a target, scanning focuses on actively identifying open ports, services, and potential vulnerabilities in systems.

What is Scanning?

Scanning involves using tools and techniques to **probe a target system/network** for open ports, live hosts, services, and vulnerabilities. This helps the attacker (or ethical hacker) understand how to exploit the system.

Types of Scanning

1. Port Scanning
    - Identifies open ports on a target system.
    - Helps determine which services are running.
    - Common tools: Nmap, Netcat, Angry IP Scanner.
    - Example types:
        - TCP Connect Scan
        - SYN Scan (Half-open)
        - UDP Scan
        - Stealth Scan

2. Network Scanning
    - Identifies active devices on a network and maps the topology.
    - Helps detect live hosts, IP addresses, and shared resources.
    - Tools: Nmap, Angry IP Scanner, Advanced IP Scanner.

3. Vulnerability Scanning
    - Scans systems for known vulnerabilities (missing patches, misconfigurations).
    - Helps in finding exploits.
    - Tools: Nessus, OpenVAS, Nikto, Qualys.

4. Banner Grabbing
    - Retrieves information about the software version running on open ports.
    - Helps identify outdated or vulnerable services.

Common Tools:

- Nmap – Port and network scanning.
- **Netcat** – Port scanning and banner grabbing.
- **Nessus/OpenVAS** – Vulnerability assessment.
- **Nikto** – Web server vulnerability scanning.
- **Wireshark** – Packet capture and analysis.

Purpose of Scanning:

- Identify entry points for attack (open ports, services).
- Assess the security posture of the target.
- Map the target network structure.
- Prepare for the next phase: **Gaining Access**.

Nmap

Nmap is a network scanning and security auditing tool used to discover devices, identify open ports, detect services and their versions, and determine operating systems on a network.

Some commands I practice in class while leaning the nmap tool…

I. nmap 192.168.1.9

It shows all the open ports present in targeted machine.

```
┌──(kali㉿kali)-[~]
└─$ nmap  192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 01:56 EDT
Nmap scan report for 192.168.1.9
Host is up (0.027s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 28.50 seconds
```

II. nmap -p22 192.168.1.9

It shows specific port in this example namp is only checking for port 22.

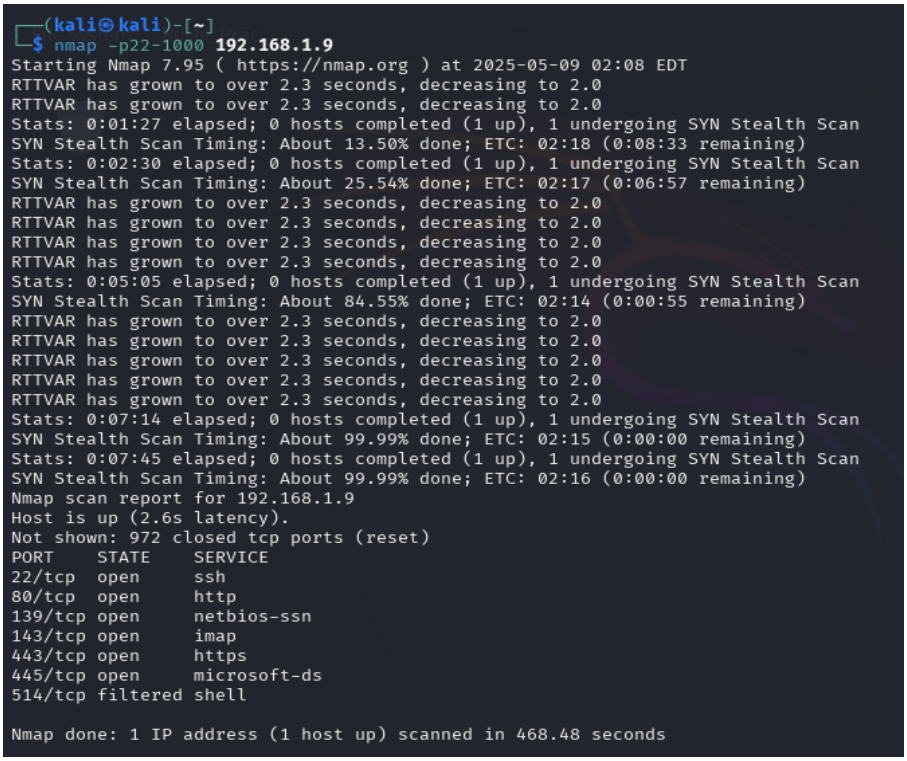
```
┌──(kali㉿kali)-[~]
└─$ nmap -p22 198.162.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:02 EDT
Nmap scan report for 198.162.1.9
Host is up (0.00066s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 5.75 seconds
```

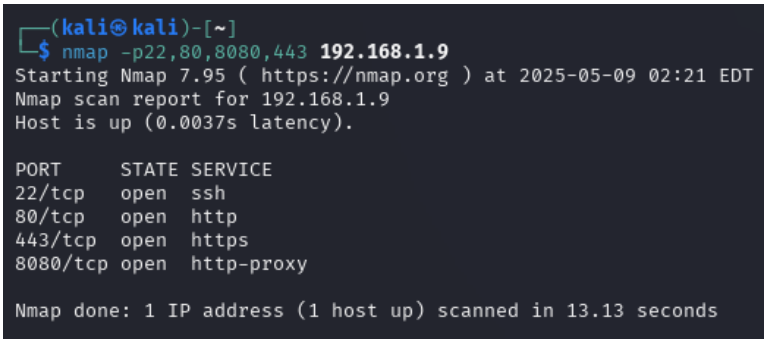
III. nmap -p22–1000 192.168.1.9

In this command we give the range of ports we want to check.



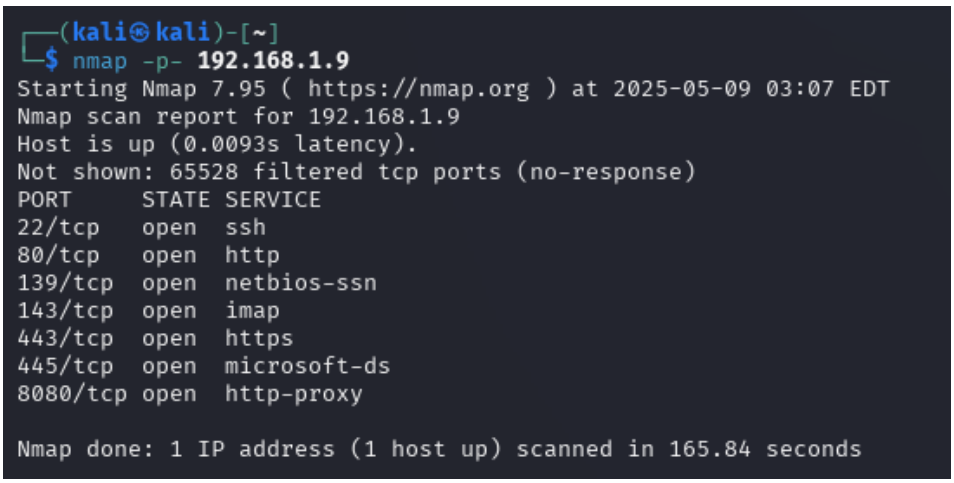
IV. nmap -p22,80,8080,443

This command is use to scan given specific ports.



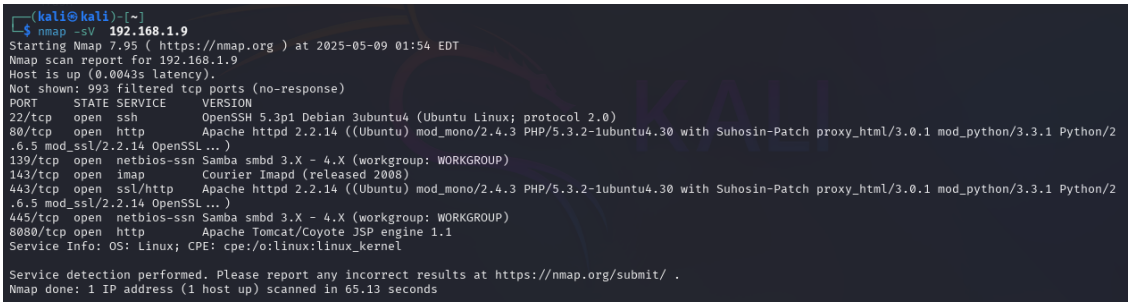
V. nmap -p- 192.168.1.9

This command scans all the port of targeted machine.



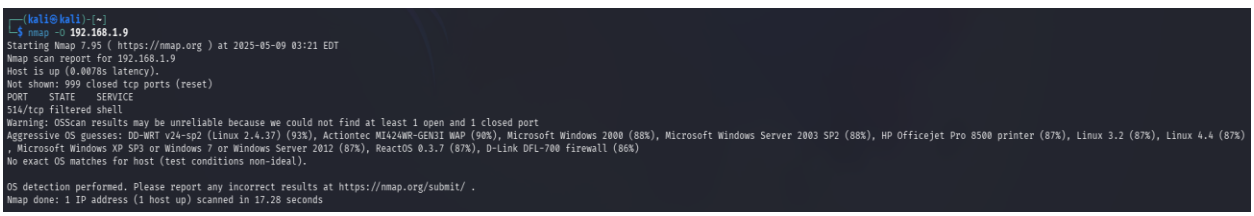
VI. nmap -sV 192.168.1.9

This command shows the service versions of ports of targeted machine.



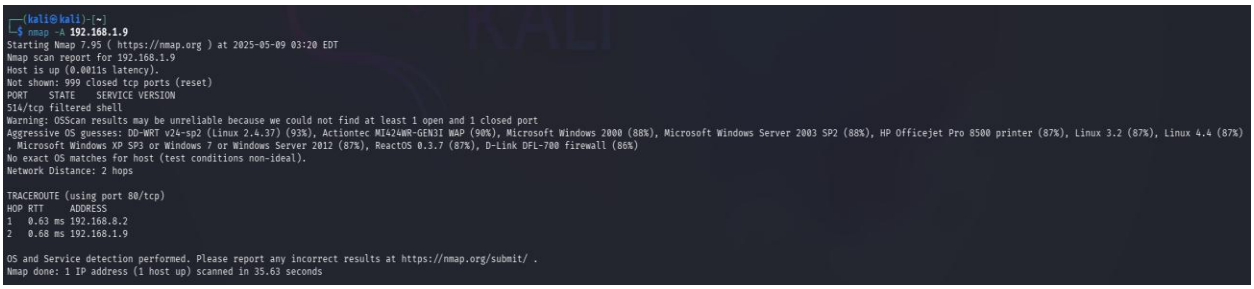
VII. nmap -O 192.168.1.9

This command is for scanning and it shows the operating system of targeted machine.



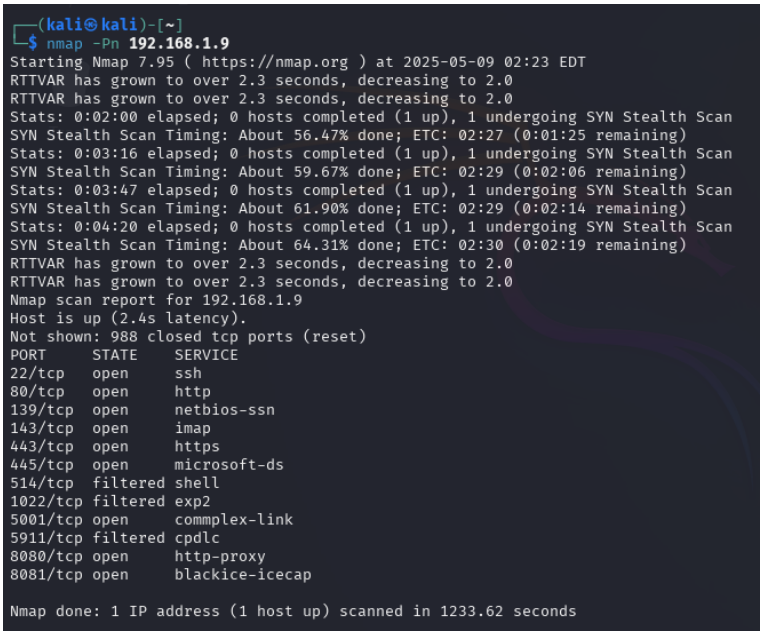
VIII. nmap -A 192.168.1.9

This Command shows the Operating System, Service version and Trace route of targeted machine.



IX. nmap -Pn 192.168.1.9

This command is for checking the ping block or any of the option is block.



X. nmap -Sn 192.168.1.9

For checking the Ping

XI. nmap -sC 192.168.1.9

For finding a basic vulnerability it scans a machine.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:51 EDT
Nmap scan report for 192.168.1.9
Host is up (0.044s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http
|_http-title: owaspbwa OWASP Broken Web Applications
139/tcp  open  netbios-ssn
143/tcp  open  imap
|_imap-capabilities: SORT CHILDREN OK IMAP4rev1 THREAD=REFERENCES CAPABILITY completed ACL2=UNIONA0001 UIDPLUS ACL QUOTA IDLE THREAD=ORDEREDSUBJECT NAMESPACE
443/tcp  open  https
| http-methods:
|_  Potentially risky methods: TRACE
| ssl-cert: Subject: commonName=owaspbwa
| Not valid before: 2013-01-02T21:12:38
|_Not valid after:  2022-12-31T21:12:38
|_ssl-date: 2025-05-09T06:52:08+00:00; +7s from scanner time.
|_http-title: owaspbwa OWASP Broken Web Applications
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy
|_http-title: Site doesn't have a title.
8081/tcp open  blackice-icecap

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: OWASPBWA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 6s, deviation: 0s, median: 6s
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 68.51 seconds
```

XII. nmap -v 192.168.1.9

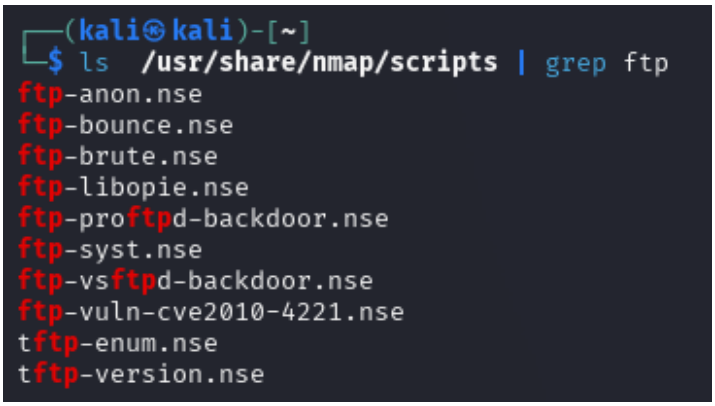
Verbosity for viewing a proper running command.

```
┌──(kali㉿kali)-[~]
└─$ nmap -v 192.168.1.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 02:54 EDT
Initiating Ping Scan at 02:54
Scanning 192.168.1.9 [4 ports]
Completed Ping Scan at 02:54, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:54
Completed Parallel DNS resolution of 1 host. at 02:54, 0.04s elapsed
Initiating SYN Stealth Scan at 02:54
Scanning 192.168.1.9 [1000 ports]
Discovered open port 8080/tcp on 192.168.1.9
Discovered open port 143/tcp on 192.168.1.9
Discovered open port 443/tcp on 192.168.1.9
Discovered open port 80/tcp on 192.168.1.9
Discovered open port 445/tcp on 192.168.1.9
Discovered open port 139/tcp on 192.168.1.9
Completed SYN Stealth Scan at 02:54, 21.75s elapsed (1000 total ports)
Nmap scan report for 192.168.1.9
Host is up (0.0020s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 22.00 seconds
           Raw packets sent: 3008 (132.268KB) | Rcvd: 203 (8.144KB)
```

XIII. ls/usr/share/nmap/script | grep “ftp”

This command is for accessing the inbuild Script of nmap we can use for hacking any machine. In this example (Command) we are specifically finding the exploit for ftp service.



XIV. nmap –script =___address_of_script_____ 192.168.1.9

In this command we are running script that we take from inbuild nmap scripts for targeted machine.