Nmap (Network Mapper) is a **powerful open-source tool** used for **network scanning, security auditing, and reconnaissance**. It helps cybersecurity professionals understand what devices, services, and vulnerabilities exist on a network.

Nmap can:

1. Discover Hosts

Find which machines are online (host discovery).

2. Scan Ports

Identify which ports are open, closed, or filtered.

3. Detect Services & Versions

Find out what software and version is running on each port
(e.g., Apache 2.4.41, SSH 7.9, MySQL 5.7).

4. OS Detection

Identify the operating system (Windows, Linux, etc.).

5. Run Vulnerability Scripts

Using NSE (Nmap Scripting Engine), Nmap can:

- Enumerate SMB shares
- Detect vulnerable services (e.g., MS17-010)
- Gather metadata from web servers
- Perform brute-force or authentication checks

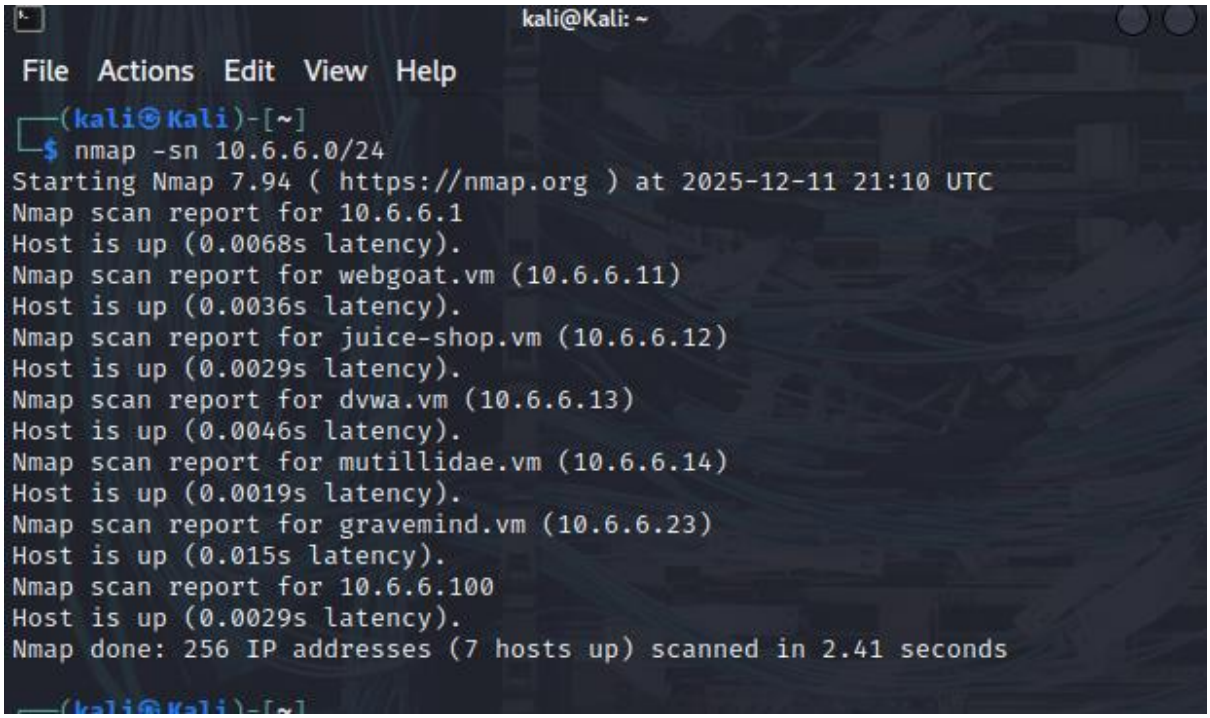
Host Discovery

nmap –sn 10.6.6.0/24

This is used to **scan a network to find which hosts are up** (ping scan).
It does **not** scan ports — only checks if devices are alive.

- -sn = “ping scan”
- Scan the whole subnet 10.6.6.0 → 10.6.6.255
- Report which hosts reply (alive machines)

output



You can use -v, -p, and -sV to find additional information about the services running on the open ports

Operating System discovery –

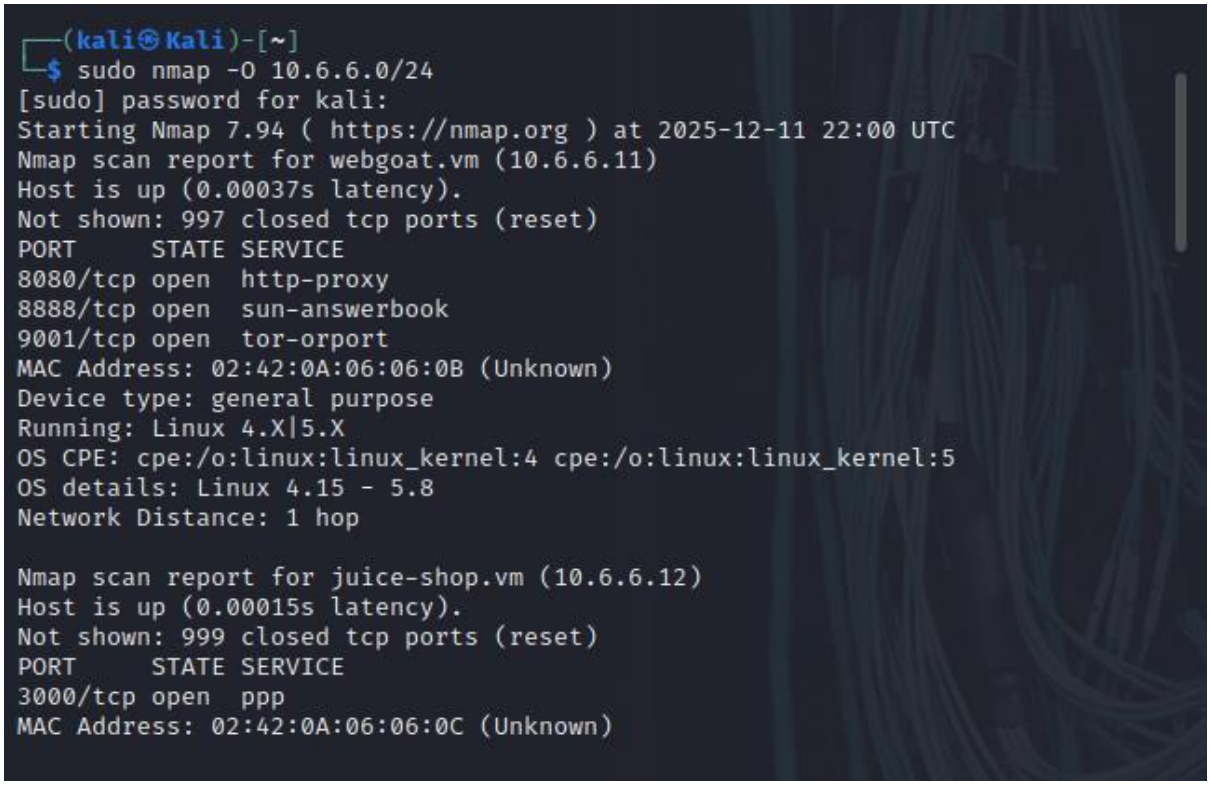
sudo nmap -O 10.6.6.23

To run this, you need root privileges

The -O option can be used to further determine information about the operating system running on the target host.

Some Nmap options require additional permissions and must be run as root or using the sudo command. To find operating system information on the target host, use the nmap -O command. Enter the password of kali when prompted.

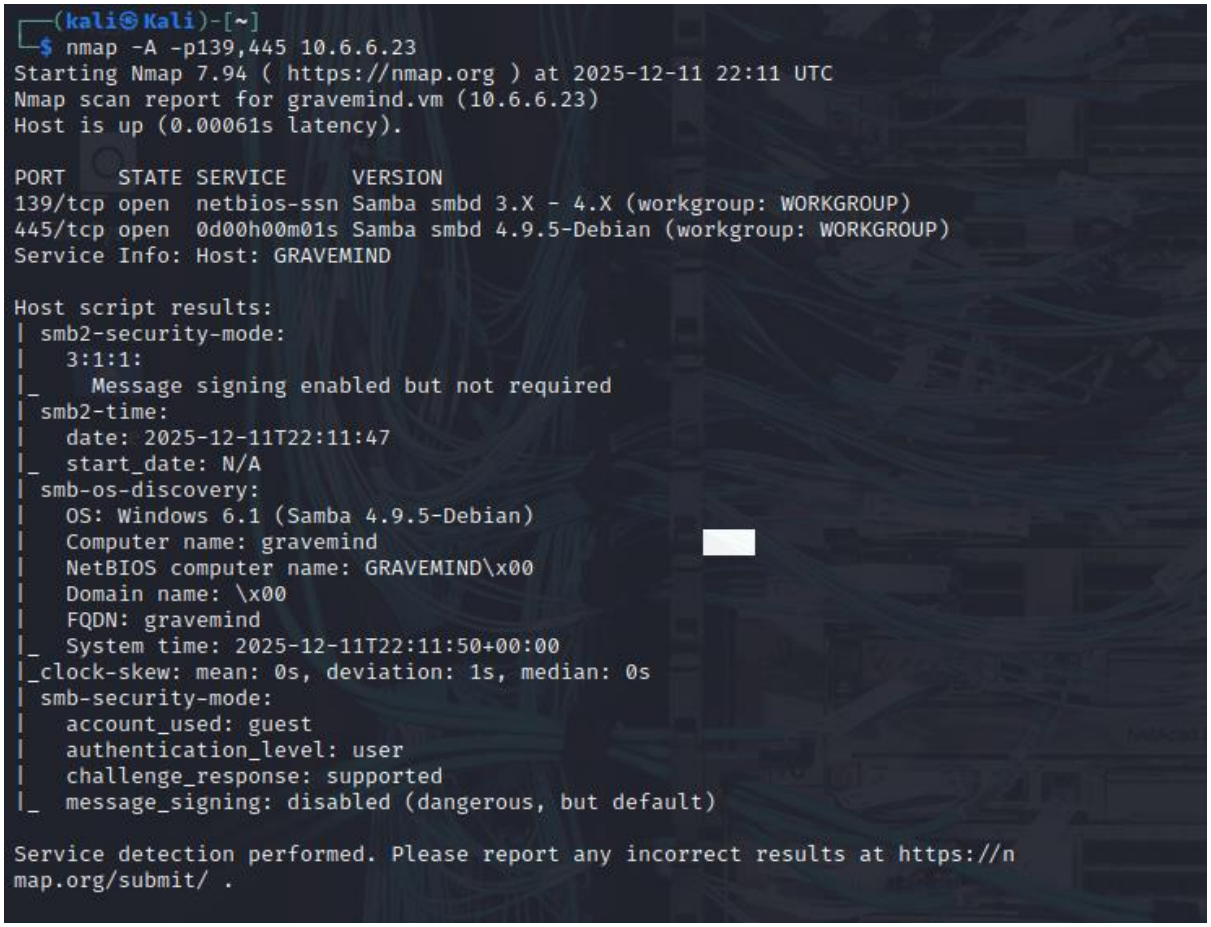
output



The -A option enables aggressive scanning, which includes OS detection, version detection, script scanning (default NSE scripts), and traceroute.
You can specify multiple ports to scan by using the -p option and listing the ports separated by commas

nmap –A –p139, 445 10.6.6.0/24

output

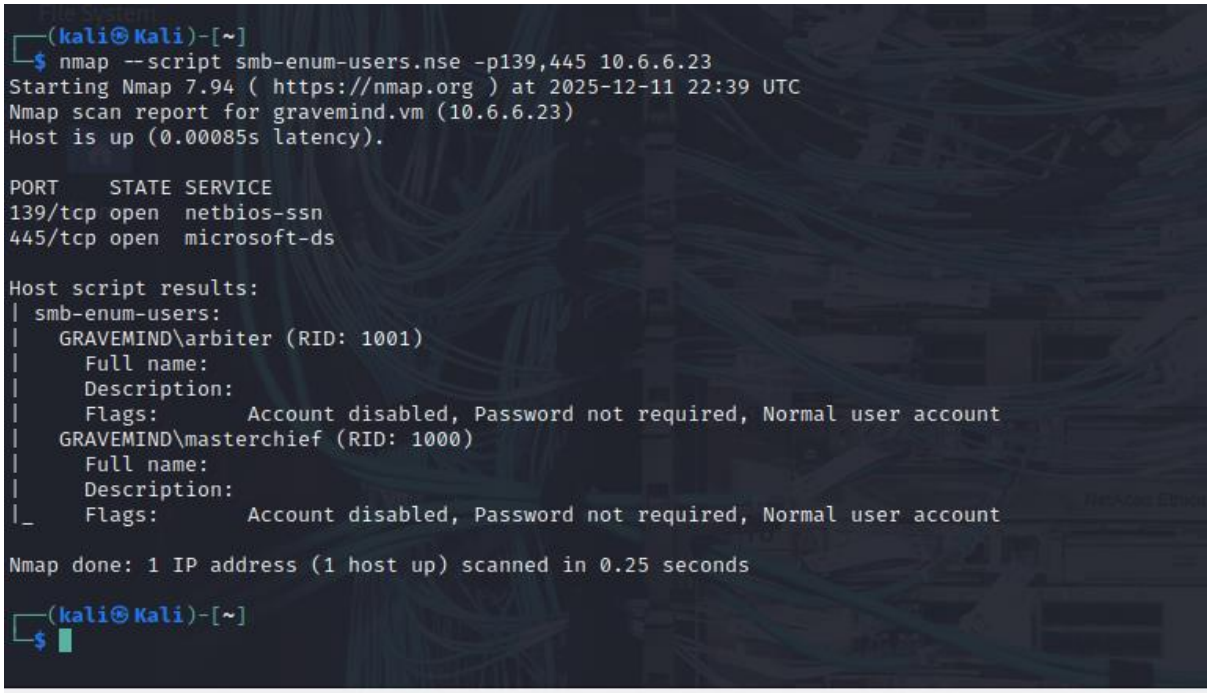


SMB Services with Scripts (Nmap)

To gather detailed information about SMB (Server Message Block) services running on a target, Nmap provides specific **SMB enumeration scripts** through the Nmap Scripting Engine (NSE). These scripts help identify SMB versions, shared folders, security settings, vulnerabilities, and authentication methods.

nmap --script smb-enum-users.nse -p139,445 10.6.6.23

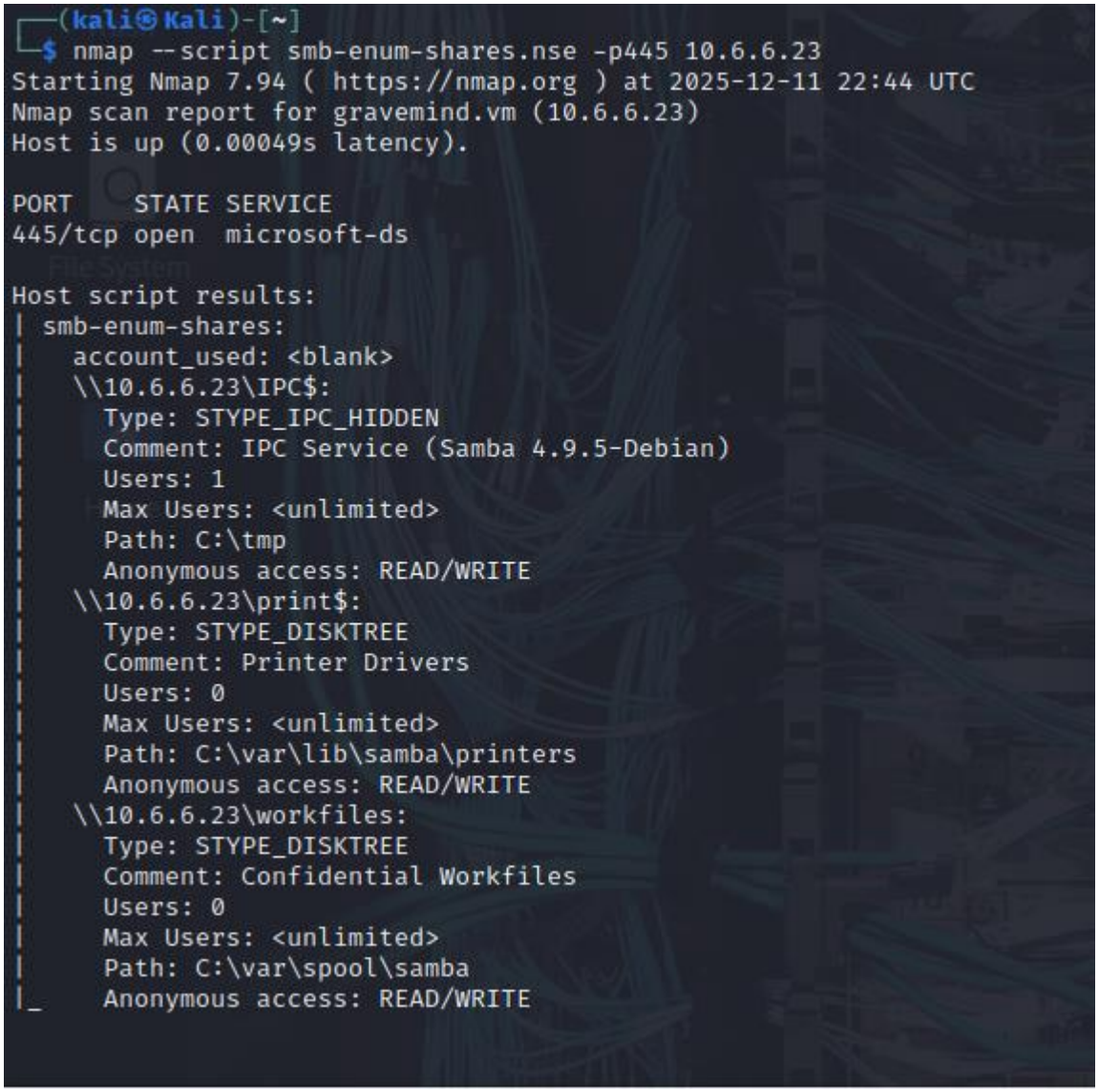
output



You can enumerate the network shares using another NSE script, smb-enum-shares.nse. To discover shared directories on the target computer. Use the Nmap share enumeration script with the command

nmap --script smb-enum-shares.nse -p445 10.6.6.23

output


(kali㉿Kali)-[~]
$ nmap --script smb-enum-shares.nse -p445 10.6.6.23
Starting Nmap 7.94 (https://nmap.org) at 2025-12-11 22:44 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00049s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
Host script results:
| smb-enum-shares:
| account_used: <blank>
| \\10.6.6.23\IPC$:
| Type: STYPE_IPC_HIDDEN
| Comment: IPC Service (Samba 4.9.5-Debian)
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: READ/WRITE
| \\10.6.6.23\print$:
| Type: STYPE_DISKTREE
| Comment: Printer Drivers
| Users: 0
| Max Users: <unlimited>
| Path: C:\var\lib\samba\printers
| Anonymous access: READ/WRITE
| \\10.6.6.23\workfiles:
| Type: STYPE_DISKTREE
| Comment: Confidential Workfiles
| Users: 0
| Max Users: <unlimited>
| Path: C:\var\spool\samba
|_ Anonymous access: READ/WRITE