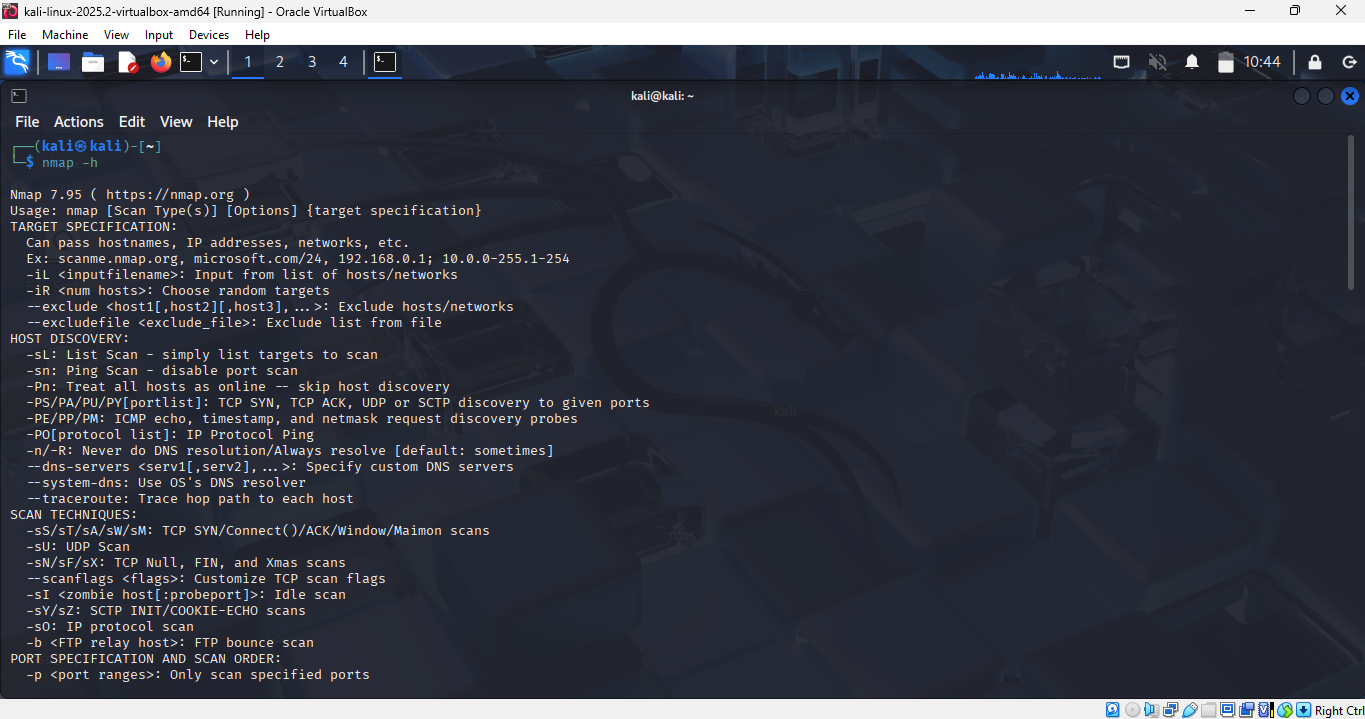
Nmap

**Nmap (Network Mapper)** is a powerful, open-source tool used for network discovery and security auditing. It helps identify live devices, open ports, running services, operating systems, and potential vulnerabilities on a network. Because of its versatility, Nmap is widely used by penetration testers, system administrators, and security researchers to assess and secure network environments.

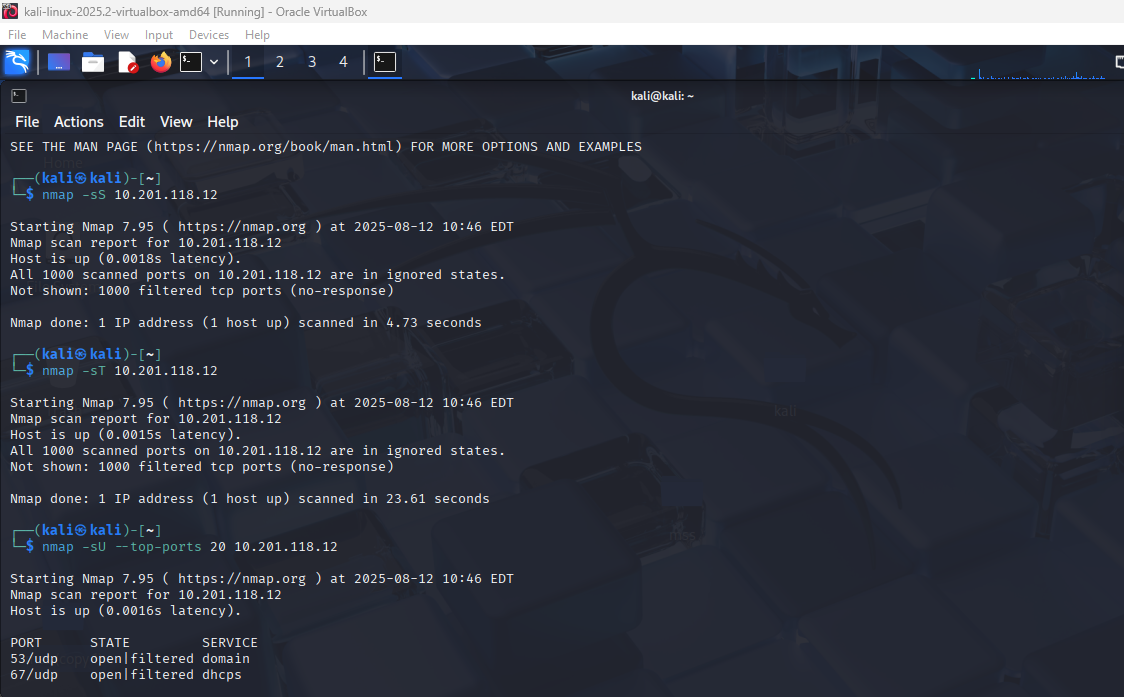
**Commands Used and Purpose:**

* **nmap -sS 10.201.118.12** → Stealth scan to find open TCP ports without completing the handshake.
* **nmap -sU 10.201.118.12** → Scan for open UDP ports.
* **nmap -O 10.201.118.12** → Identify the operating system running on the target.
* **nmap -sV 10.201.118.12** → Detect service versions on open ports.
* **nmap -vv 10.201.118.12** → Increase output detail for better analysis.
* **nmap -oA scan\_results 10.201.118.12** → Save results in all major formats.
* **nmap -A 10.201.118.12** → Perform aggressive scan (OS, version, scripts, traceroute).
* **nmap -T5 10.201.118.12** → Maximize scan speed.
* **nmap -p- 10.201.118.12** → Scan all 65,535 TCP ports.
* **nmap --script=vuln 10.201.118.12** → Run vulnerability detection scripts.

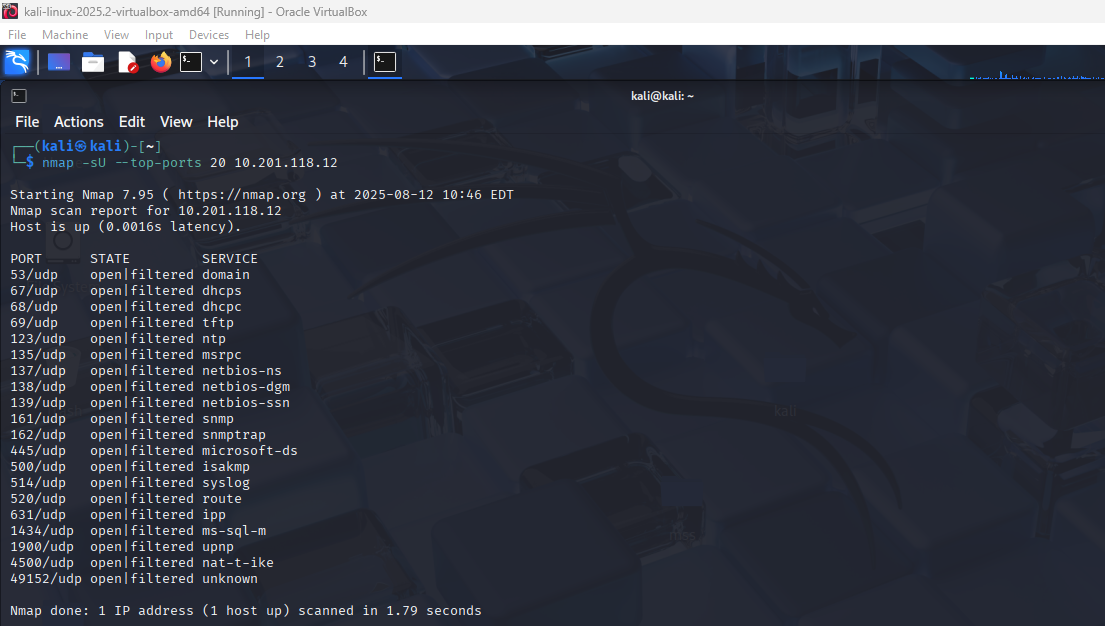
Nmap Help Menu (-h option)



TCP SYN Scan (-sS) and TCP Connect Scan (-sT)

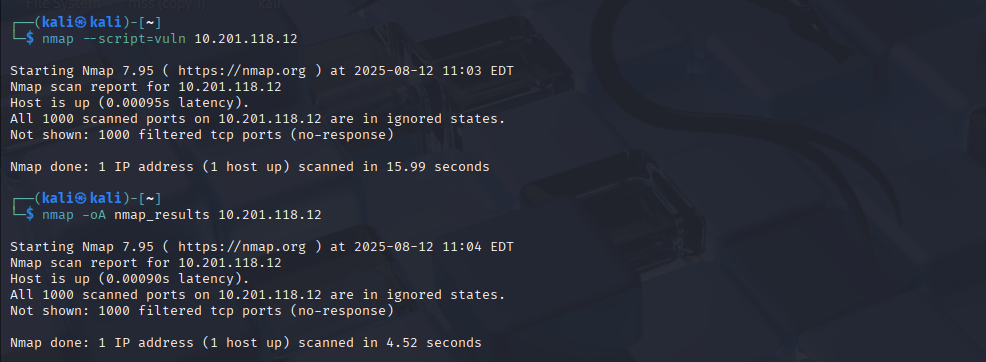


UDP Scan (-sU --top-ports 20)



Service Version Detection (-sV) and OS Detection (-O)

Aggressive Scan (-A) and Full Port Scan (-p-)



**Further Nmap**

**Task 2: Introduction**

1. Networking constructs used to direct traffic to the right application: **Ports**
2. Number of ports available: **65535**
3. Number of “well-known” ports: **1024**

**Task 3: Nmap Switches**

1. First switch listed in help menu for a SYN scan: **-sS**
2. UDP scan switch: **-sU**
3. Detect operating system: **-O**
4. Detect service version: **-sV**
5. Increase verbosity: **-v**
6. Set verbosity level two: **-vv**
7. Save results in all formats: **-oA**
8. Save results in normal format: **-oN**
9. Save results in grepable format: **-oG**
10. Enable aggressive mode: **-A**
11. Timing template level 5: **-T5**
12. Scan only port 80: **-p 80**
13. Scan ports 1000–1500: **-p 1000-1500**
14. Scan all ports: **-p-**
15. Activate a script: **--script**
16. Activate all “vuln” scripts: **--script=vuln**

**Task 5: TCP Connect Scans**

1. RFC defining TCP protocol: **RFC 793**
2. Flag sent back if port is closed: **RST**

**Task 6: SYN Scans**

1. Two other names for a SYN scan: **Half-open, Stealth**
2. Use SYN scan without sudo: **N**

**Task 7: UDP Scans**

1. No response from UDP port: **open|filtered**
2. Protocol used for “port unreachable” message: **ICMP**

**Task 8: NULL, FIN, Xmas Scans**

1. Scan type using URG flag: **Xmas**
2. Purpose: **Firewall evasion**
3. OS that responds with RST to all ports: **Microsoft Windows**

**Task 9: ICMP Network Scanning**

1. Ping sweep on **172.16.x.x/16** : **nmap -sn 172.16.0.0/16**

**Task 10: NSE Scripts Overview**

1. NSE script language: **Lua**
2. Unsafe category for production: **Intrusive**

**Task 11: Working with NSE**

1. Optional argument for ftp-anon.nse: **maxlist**

**Task 12: Searching for Scripts**

1. SMB OS discovery script filename: **smb-os-discovery.nse**
2. Depends on: **smb-brute**

**Task 13: Firewall Evasion**

1. Protocol often blocked, requiring -Pn: **ICMP**
2. Switch to append random data: **--data-length**

**Task 14: Practical**

1. Target responds to ICMP: **N**
2. Xmas scan open/filtered ports: **999**
3. Reason: **No response**
4. SYN scan (first 5000 ports) open ports: **5**
5. FTP anonymous login success: **Y**