

NMAP & WIRESHARK

Powerful Tools for Network Security and Analysis

part 1



Practice in LAB By: Nin Kanong

NMAP & WIRESHARK

Basic Nmap:

Nmap is a network mapper that has emerged as one of the most popular, free network discovery tools on the market. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, **perform port scanning**, ping sweeps, OS detection, and version detection.

A number of recent cyberattacks have re-focused attention on the type of network auditing that Nmap provides. Analysts have pointed out that the recent Capital One hack, for instance, **could have been detected sooner** if system administrators had been monitoring connected devices. In this guide, we'll look at what Nmap is, what it can do, and explain how to use the most common commands.

Kali> man nmap



The screenshot shows a terminal window with a dark background. At the top, it says '(k4n0ng㉿kali)-[~]'. Below that, the command '\$ man nmap' is entered. The terminal then displays the man page for nmap. The page is titled 'NMAP(1)' and is part of the 'Nmap Reference Guide'. It includes sections for NAME, SYNOPSIS, and DESCRIPTION. The NAME section says 'nmap - Network exploration tool and security / port scanner'. The SYNOPSIS section shows the command 'nmap [Scan Type ...] [Options] {target specification}'. The DESCRIPTION section provides a detailed explanation of what Nmap does, mentioning its use for network exploration and security auditing, and its ability to scan large networks or single hosts, determine host availability, service offerings, operating systems, and other characteristics.

```
NMAP(1)                               Nmap Reference Guide                               NMAP(1)

NAME
      nmap - Network exploration tool and security / port scanner

SYNOPSIS
      nmap [Scan Type ...] [Options] {target specification}

DESCRIPTION
      Nmap ("Network Mapper") is an open source tool for network exploration and
      security auditing. It was designed to rapidly scan large networks, although it
      works fine against single hosts. Nmap uses raw IP packets in novel ways to
      determine what hosts are available on the network, what services (application name
      and version) those hosts are offering, what operating systems (and OS versions)
      they are running, what type of packet filters/firewalls are in use, and dozens of
      other characteristics. While Nmap is commonly used for security audits, many
      systems and network administrators find it useful for routine tasks such as
      network inventory, managing service upgrade schedules, and monitoring host or
      service uptime.
```

What is Nmap?

Nmap is Used to Scan:

- Enterprise-scale networks
- Small business networks
- Connected devices
- IoT devices and traffic

At its core, Nmap is a network scanning tool that uses IP packets to identify all the devices connected to a network and to provide information on the services and operating systems they are running.

The program is most commonly used via a command-line interface (though GUI front-ends are also available) and is available for many different operating systems such as Linux, FreeBSD, and Gentoo. Its popularity has also been bolstered by an active and enthusiastic user support community.

Nmap was developed for enterprise-scale networks and can scan through thousands of connected devices. However, in recent years Nmap is being increasingly used by smaller companies. The rise of the IoT, in particular, now means that the networks used by these companies have become more complex **and therefore harder to secure**.

This means that Nmap is now **used in many website monitoring tools** to audit the traffic between web servers and IoT devices. The recent emergence of IoT botnets, like Mirai, has also stimulated interest in Nmap, not least because of its ability to interrogate **devices connected via the UPnP protocol** and to highlight any devices that may be malicious.

Nmap provides information on:

1. Every active IP so you can determine if an IP is being used by a legitimate service or an external attacker.
2. Your network as a whole, including live hosts, open ports, and the OS of every connected device.
3. Vulnerabilities — scan your own server to simulate the process that a hacker would use to attack your site.

- Basic scan:

kali> nmap google.com

```
(k4n0ng㉿kali)-[~]
$ nmap google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 10:06 EDT
Nmap scan report for google.com (74.125.68.113)
Host is up (0.033s latency).
Other addresses for google.com (not scanned): 74.125.68.139 74.125.68.102 74.125.68.138 74.125.68.101 74.125.68.1
00 2404:6800:4003:c02::8a 2404:6800:4003:c02::64 2404:6800:4003:c02::66 2404:6800:4003:c02::71
rDNS record for 74.125.68.113: sc-in-f113.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

kali> nmap google.com facebook.com

```
(k4n0ng㉿kali)-[~]
$ nmap google.com facebook.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 10:07 EDT
Nmap scan report for google.com (74.125.68.101)
Host is up (0.033s latency).
Other addresses for google.com (not scanned): 74.125.68.100 74.125.68.102 74.125.68.139 74.125.68.138 74.125.68.113 2404:6800:4003:c02::8a 2404:6800:4003:c02::8b 2404:6800:4003:c02::66 2404:6800:4003:c02::71
rDNS record for 74.125.68.101: sc-in-f101.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for facebook.com (57.144.160.1)
Host is up (0.037s latency).
Other addresses for facebook.com (not scanned): 2a03:2880:f350:1:face:b00c:0:25de
rDNS record for 57.144.160.1: edge-star-mini-shv-02-sin2.facebook.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

- Use metasploit for testing:

```
Metasploitable2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TX packets:511 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:228893 (223.5 KB) TX bytes:228893 (223.5 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:96:16:b6
          inet addr:192.168.100.102 Bcast:192.168.100.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe96:16b6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:390 errors:0 dropped:0 overruns:0 frame:0
          TX packets:357 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:40669 (39.7 KB) TX bytes:38017 (37.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:885 errors:0 dropped:0 overruns:0 frame:0
          TX packets:885 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:415817 (406.0 KB) TX bytes:415817 (406.0 KB)

msfadmin@metasploitable:~$
```

Because it has a lot of vulnerability and weakness.

kali> nmap 192.168.100.102

```
└─(k4n0ng㉿kali)-[~]
$ nmap 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 10:08 EDT
Nmap scan report for 192.168.100.102
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

scan single target.

Kali> nmap 192.168.100.102 192.168.100.110 192.168.100.97

```
└─(k4n0ng㉿kali)-[~]
$ nmap 192.168.100.102 192.168.100.97 192.168.100.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 10:11 EDT
Nmap scan report for 192.168.100.102
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.100.97
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.100.97 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 8C:8D:28:F4:83:96 (Intel Corporate)

Nmap scan report for 192.168.100.109
Host is up (0.000011s latency).
All 1000 scanned ports on 192.168.100.109 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

scan multiple hosts.

kali> nmap 192.168.100.1/24

```
(k4n0ng㉿kali)-[~]
$ nmap 192.168.100.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 10:59 EDT
Nmap scan report for 192.168.100.1
Host is up (0.022s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
53/tcp    open   domain
80/tcp    open   http
8022/tcp filtered oa-system
MAC Address: 64:C3:94:D6:8B:5C (Huawei Technologies)

Nmap scan report for 192.168.100.28
Host is up (0.020s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open   http
443/tcp   open   https
3306/tcp  open   mysql
MAC Address: 3C:55:76:D0:B5:EF (Cloud Network Technology Singapore PTE.)
```

is used to **scan a local network** to discover **which devices (IP addresses) are active** and gather basic information about them. Scan an IP Range or subnet.

kali> nmap 192.168.100.1-200

```
(k4n0ng㉿kali)-[~]
$ nmap 192.168.100.1-200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:00 EDT
Nmap scan report for 192.168.100.1
Host is up (0.015s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
53/tcp    open   domain
80/tcp    open   http
8022/tcp filtered oa-system
MAC Address: 64:C3:94:D6:8B:5C (Huawei Technologies)

Nmap scan report for 192.168.100.28
Host is up (0.019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open   http
443/tcp   open   https
3306/tcp  open   mysql
MAC Address: 3C:55:76:D0:B5:EF (Cloud Network Technology Singapore PTE.)
```

The command use to scan from IP 192.168.100.1 until 192.168.100.200

```
kali> nmap 192.168.100.97,102,109
```

```
(k4n0ng㉿kali)-[~]
$ nmap 192.168.100.97,102,112
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:01 EDT
Nmap scan report for 192.168.100.97
Host is up (0.000097s latency).
All 1000 scanned ports on 192.168.100.97 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 8C:8D:28:F4:83:96 (Intel Corporate)

Nmap scan report for 192.168.100.102
Host is up (0.00021s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.100.112
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.100.112 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

```
kali> vim ip.txt
```

```
(k4n0ng㉿kali)-[~]
$ vim ip.txt|
```

```
192.168.100.97
192.168.100.102
192.168.100.112
|
~
```

```
(k4n0ng㉿kali)-[~]
$ cat ip.txt
192.168.100.97
192.168.100.102
192.168.100.112
```

```
kali> nmap -iL ip.txt
```

```
(k4n0ng㉿kali)-[~]
$ nmap -iL ip.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:32 EDT
Nmap scan report for 192.168.100.97
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.100.97 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 8C:8D:28:F4:83:96 (Intel Corporate)

Nmap scan report for 192.168.100.102
Host is up (0.00024s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.100.112
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.100.112 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

-iL ip.txt: This option tells Nmap to **read input from a file**. In this case:

- ip.txt should contain a **list of IP addresses or hostnames** (one per line).
- Nmap will scan **each host listed** in that file.

Kali> nmap -iR 10

```
(heLo@HeLo)-[~]
$ nmap -iR 10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-06 12:58 EDT
Nmap scan report for v128.ce07.wdc-02.us.leaseweb.net (207.244.67.188)
Host is up (0.25s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE
5900/tcp  closed vnc
5901/tcp  closed vnc-1
5902/tcp  closed vnc-2
5903/tcp  closed vnc-3
5904/tcp  closed ag-swim
5906/tcp  closed rpas-c2
5907/tcp  closed dsd
5910/tcp  closed cm
50000/tcp closed ibm-db2
50001/tcp closed unknown
50002/tcp closed iiimsf
50003/tcp closed unknown
50006/tcp closed unknown

Nmap scan report for pool-68-134-58-205.bltmmd.fios.verizon.net (68.134.58.205)
Host is up (0.30s latency).
All 1000 scanned ports on pool-68-134-58-205.bltmmd.fios.verizon.net (68.134.58.205) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 10 IP addresses (2 hosts up) scanned in 53.74 seconds
```

-iR 10:

- -iR stands for "**input random**".
- 10 tells Nmap to **pick 10 random IP addresses** across the Internet.
- Nmap will scan each of those 10 IPs as if they were manually entered.

Kali> nmap 192.168.100.1/24 --exclude 192.168.100.150

```
(k4n0ng@kali)-[~]
$ nmap 192.168.100.1/24 --exclude 192.168.100.150
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:35 EDT
Nmap scan report for 192.168.100.1
Host is up (0.012s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
53/tcp    open   domain
80/tcp    open   http
8022/tcp filtered oa-system
MAC Address: 64:C3:94:D6:8B:5C (Huawei Technologies)

Nmap scan report for 192.168.100.7
Host is up (0.17s latency).
All 1000 scanned ports on 192.168.100.7 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 1E:3B:C3:77:E0:1A (Unknown)

Nmap scan report for 192.168.100.28
Host is up (0.0042s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open   http
443/tcp   open   https
3306/tcp  open   mysql
MAC Address: 3C:55:76:D0:B5:EF (Cloud Network Technology Singapore PTE.)
```

```
kali> nmap 192.168.1/24 --exclude 192.168.100-200
```

```
(k4n0ng㉿kali)-[~]
$ nmap 192.168.100.1/24 --exclude 192.168.100.100-250
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:37 EDT
Nmap scan report for 192.168.100.1
Host is up (0.0073s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
53/tcp    open   domain
80/tcp    open   http
8022/tcp  filtered oa-system
MAC Address: 64:C3:94:D6:8B:5C (Huawei Technologies)

Nmap scan report for 192.168.100.28
Host is up (0.014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open   http
443/tcp   open   https
3306/tcp  open   mysql
MAC Address: 3C:55:76:D0:B5:EF (Cloud Network Technology Singapore PTE.)
```

- **192.168.1.0/24**: This tells Nmap to scan **all 256 IPs** from 192.168.1.0 to 192.168.1.255.
- **--exclude**: This tells Nmap to **skip** specific IPs.
- **192.168.1.100-192.168.1.200**: Exclude **all IPs in this range**.

```
kali> nmap 192.168.1/24 -excludefile ip.txt
```

```
(k4n0ng㉿kali)-[~]
$ nmap 192.168.100.1/24 -excludefile ip.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:42 EDT
Nmap scan report for 192.168.100.1
Host is up (0.12s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
53/tcp    open   domain
80/tcp    open   http
8022/tcp  filtered oa-system
MAC Address: 64:C3:94:D6:8B:5C (Huawei Technologies)

Nmap scan report for 192.168.100.7
Host is up (0.023s latency).
All 1000 scanned ports on 192.168.100.7 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 1E:3B:C3:77:E0:1A (Unknown)
```

- 192.168.1.0/24: Tells Nmap to scan all 256 IPs in that subnet (from .0 to.255).
- **--excludefile ip.txt**: Tells Nmap to **exclude all IP addresses listed in the ip.txt file** from the scan.

Kali> nmap -sV 192.168.100.102

```
(k4n0ng㉿kali)-[~]
$ nmap -sV 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:16 EDT
Nmap scan report for 192.168.100.102
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smptd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- Service Version Detection

Detects service versions running on open ports

kali> nmap -O 192.168.100.102

```
(k4n0ng㉿kali)-[~]
$ nmap -O 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:17 EDT
Nmap scan report for 192.168.100.102
Host is up (0.00038s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Operating System detection and Attempts to detect the OS of the target machine.

```
kali> nmap -A 192.168.100.102
```

```
(k4n0ng㉿kali)-[~]
$ nmap -A 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:21 EDT
Nmap scan report for 192.168.100.102
Host is up (0.00045s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.100.112
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntui (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_
```

```
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2025-08-09T11:21:27-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s
|_nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1  0.45 ms  192.168.100.102
```

- Aggressive Scan (combines version, OS, script scanning)
- Enables OS detection, version detection, script scanning, and traceroute

Kali> nmap -v 192.168.100.102

```
(k4n0ng㉿kali)-[~]
$ nmap -v 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:26 EDT
Initiating ARP Ping Scan at 11:26
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 11:26, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:26
Completed Parallel DNS resolution of 1 host. at 11:26, 0.01s elapsed
Initiating SYN Stealth Scan at 11:26
Scanning 192.168.100.102 [1000 ports]
Discovered open port 80/tcp on 192.168.100.102
Discovered open port 22/tcp on 192.168.100.102
Discovered open port 21/tcp on 192.168.100.102
Discovered open port 53/tcp on 192.168.100.102
Discovered open port 23/tcp on 192.168.100.102
Discovered open port 139/tcp on 192.168.100.102
```

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13
8180/tcp	open	unknown
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)		

- Scan with Verbose Output
adds verbosity, shows scan progress.

Kali> nmap -vv 192.168.100.102

```
(k4n0ng㉿kali)-[~]
$ nmap -vv 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:53 EDT
Initiating ARP Ping Scan at 11:53
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 11:53, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:53
Completed Parallel DNS resolution of 1 host. at 11:53, 0.00s elapsed
Initiating SYN Stealth Scan at 11:53
Scanning 192.168.100.102 [1000 ports]
Discovered open port 5900/tcp on 192.168.100.102
Discovered open port 23/tcp on 192.168.100.102
Discovered open port 111/tcp on 192.168.100.102
```

PORT	STATE	SERVICE	REASON
21/tcp	open	ftp	syn-ack ttl 64
22/tcp	open	ssh	syn-ack ttl 64
23/tcp	open	telnet	syn-ack ttl 64
25/tcp	open	smtp	syn-ack ttl 64
53/tcp	open	domain	syn-ack ttl 64
80/tcp	open	http	syn-ack ttl 64
111/tcp	open	rpcbind	syn-ack ttl 64
139/tcp	open	netbios-ssn	syn-ack ttl 64
445/tcp	open	microsoft-ds	syn-ack ttl 64
512/tcp	open	exec	syn-ack ttl 64
513/tcp	open	login	syn-ack ttl 64

kali> nmap -T4 192.168.100.102

```
(k4n0ng㉿kali)-[~]
$ nmap -T4 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 11:55 EDT
Nmap scan report for 192.168.100.102
Host is up (0.000087s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
```

- **T0 (Paranoid):** Waits a long time between probes, sends packets slowly to avoid detection.
Used against IDS/IPS systems to sneak in.
- **T1 (Sneaky):** Slower than default but less than paranoid. Still tries to avoid detection.
- **T2 (Polite):** Reduces bandwidth and load, nice to network admins, still reasonably fast.
- **T3 (Normal):**
Default timing, balanced for most situations.
- **T4 (Aggressive):** Speeds up scanning, assumes stable network and no IDS/IPS issues. May cause dropped packets or detection. Fast scan(recommend).
- **T5 (Insane):** Max speed, can flood network and cause problems or get blocked quickly.

We can combine this with all scan.

Option	Example	Description
-T0	nmap 192.168.1.1 -T0	Paranoid (0) Intrusion Detection System evasion
-T1	nmap 192.168.1.1 -T1	Sneaky (1) Intrusion Detection System evasion
-T2	nmap 192.168.1.1 -T2	Polite (2) slows down the scan to useless bandwidth and use less target machine resources
-T3	nmap 192.168.1.1 -T3	Normal (3) which is default speed
-T4	nmap 192.168.1.1 -T4	Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network
-T5	nmap 192.168.1.1 -T5	Insane (5) speeds scan

kali> nmap -v -p- 192.168.100.102

```
(k4n0ng㉿kali)-[~]
$ nmap -v -p- 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 12:00 EDT
Initiating ARP Ping Scan at 12:00
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 12:00, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:00
Completed Parallel DNS resolution of 1 host. at 12:00, 0.10s elapsed
Initiating SYN Stealth Scan at 12:00
Scanning 192.168.100.102 [65535 ports]
Discovered open port 53/tcp on 192.168.100.102
Discovered open port 445/tcp on 192.168.100.102
Discovered open port 139/tcp on 192.168.100.102

```

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell

- Scan all TCP ports (1-65535) on the IP.

-p- means "scan all 65535 TCP ports".

Kali> nmap -v -p 22,80,443 192.168.100.102

```
[k4n0ng㉿kali)-[~]
$ nmap -v -p 22,80,443 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 12:02 EDT
Initiating ARP Ping Scan at 12:02
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 12:02, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:02
Completed Parallel DNS resolution of 1 host. at 12:02, 0.00s elapsed
Initiating SYN Stealth Scan at 12:02
Scanning 192.168.100.102 [3 ports]
Discovered open port 80/tcp on 192.168.100.102
Discovered open port 22/tcp on 192.168.100.102
Completed SYN Stealth Scan at 12:02, 0.04s elapsed (3 total ports)
Nmap scan report for 192.168.100.102
Host is up (0.00088s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   closed https
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Scans only SSH (22), HTTP (80), and HTTPS (443).

kali> nmap -v -p 80,443-450 192.168.100.102

```
[k4n0ng㉿kali)-[~]
$ nmap -v -p 22,80,443-450 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 12:04 EDT
Initiating ARP Ping Scan at 12:04
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 12:04, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:04
Completed Parallel DNS resolution of 1 host. at 12:04, 0.00s elapsed
Initiating SYN Stealth Scan at 12:04
Scanning 192.168.100.102 [10 ports]
Discovered open port 22/tcp on 192.168.100.102
Discovered open port 445/tcp on 192.168.100.102
Discovered open port 80/tcp on 192.168.100.102
Completed SYN Stealth Scan at 12:04, 0.01s elapsed (10 total ports)
Nmap scan report for 192.168.100.102
Host is up (0.00029s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   closed https
444/tcp   closed snpp
445/tcp   open  microsoft-ds
446/tcp   closed ddm-rdb
447/tcp   closed ddm-dfm
448/tcp   closed ddm-ssl
449/tcp   closed as-servermap
450/tcp   closed tserver
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

- **-v:** Enables **verbose mode**, showing more detailed progress and results.
- **-p 80,443-450:** Tells Nmap to scan:
 - + Port **80** (HTTP),
 - + Ports **443 to 450** (a small range starting with HTTPS and nearby ports).

Kali> nmap -v --top-ports 10 192.168.100.102

```
(k4n0ng㉿kali)-[~]
└─$ nmap -v --top-ports 10 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 12:05 EDT
Initiating ARP Ping Scan at 12:05
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 12:05, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:05
Completed Parallel DNS resolution of 1 host. at 12:05, 0.01s elapsed
Initiating SYN Stealth Scan at 12:05
Scanning 192.168.100.102 [10 ports]
Discovered open port 25/tcp on 192.168.100.102
Discovered open port 139/tcp on 192.168.100.102
Discovered open port 21/tcp on 192.168.100.102
Discovered open port 445/tcp on 192.168.100.102
Discovered open port 80/tcp on 192.168.100.102
Discovered open port 22/tcp on 192.168.100.102
Discovered open port 23/tcp on 192.168.100.102
Completed SYN Stealth Scan at 12:05, 0.03s elapsed (10 total ports)
Nmap scan report for 192.168.100.102
Host is up (0.00069s latency).

PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    open     smtp
80/tcp    open     http
110/tcp   closed   pop3
139/tcp   open     netbios-ssn
443/tcp   closed   https
445/tcp   open     microsoft-ds
3389/tcp  closed   ms-wbt-server
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

- **-v:** Enables **verbose mode** (you get more details during the scan).
- **--top-ports 10:** Tells Nmap to scan the **10 most commonly used TCP ports**, based on statistical data.

- more command:

kali> nmap -v -sV --top-ports 10 192.168.100.102

Add service/version detection.

Kali> nmap -v -A --top-ports 10 192.168.100.102

Add OS detection and traceroute.

Kali> nmap -v --top-ports 10 192.168.100.102 -oN top10-scan.txt

Save output.

Kali> nmap -v -p 1-65535

```
(k4n0ng㉿kali)-[~]
└─$ nmap -v -p 1-65535 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 12:07 EDT
Initiating ARP Ping Scan at 12:07
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 12:07, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:07
Completed Parallel DNS resolution of 1 host. at 12:07, 0.00s elapsed
Initiating SYN Stealth Scan at 12:07
Scanning 192.168.100.102 [65535 ports]
Discovered open port 445/tcp on 192.168.100.102
Discovered open port 5900/tcp on 192.168.100.102
Discovered open port 139/tcp on 192.168.100.102
Discovered open port 23/tcp on 192.168.100.102
```

```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
35583/tcp open  unknown
43906/tcp open  unknown
45622/tcp open  unknown
58633/tcp open  unknown
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

kali> nmap -v -p http 192.168.100.102

```
└─(k4n0ng㉿kali)-[~]
$ nmap -v -p http 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 12:10 EDT
Initiating ARP Ping Scan at 12:10
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 12:10, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:10
Completed Parallel DNS resolution of 1 host. at 12:10, 0.02s elapsed
Initiating SYN Stealth Scan at 12:10
Scanning 192.168.100.102 [2 ports]
Discovered open port 80/tcp on 192.168.100.102
Completed SYN Stealth Scan at 12:10, 0.02s elapsed (2 total ports)
Nmap scan report for 192.168.100.102
Host is up (0.00042s latency).

PORT      STATE SERVICE
80/tcp    open  http
8008/tcp  closed http
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
kali> nmap -v -p http* 192.168.100.102
```

```
(k4n0ng㉿kali)-[~]
└─$ nmap -v -p http* 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 12:10 EDT
Initiating ARP Ping Scan at 12:10
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 12:10, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:10
Completed Parallel DNS resolution of 1 host. at 12:10, 0.03s elapsed
Initiating SYN Stealth Scan at 12:10
Scanning 192.168.100.102 [12 ports]
Discovered open port 80/tcp on 192.168.100.102
Completed SYN Stealth Scan at 12:10, 0.01s elapsed (12 total ports)
Nmap scan report for 192.168.100.102
Host is up (0.00026s latency).

PORT      STATE    SERVICE
80/tcp    open     http
280/tcp   closed   http-mgmt
443/tcp   closed   https
591/tcp   closed   http-alt
593/tcp   closed   http-rpc-epmap
4180/tcp  closed   httpx
8000/tcp  closed   http-alt
8008/tcp  closed   http
8080/tcp  closed   http-proxy
8443/tcp  closed   https-alt
8990/tcp  closed   http-wmap
8991/tcp  closed   https-wmap
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
kali> nmap -v -p 80,443,8080,8000,8443 --script http-title 192.168.100.102
```

```
(k4n0ng㉿kali)-[~]
└─$ nmap -v -p 80,443,8080,8000,8443 --script http-title 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:02 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:02
Completed NSE at 13:02, 0.00s elapsed
Initiating ARP Ping Scan at 13:02
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 13:02, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:02
Completed Parallel DNS resolution of 1 host. at 13:02, 0.02s elapsed
Initiating SYN Stealth Scan at 13:02
Scanning 192.168.100.102 [4 ports]
Discovered open port 80/tcp on 192.168.100.102
Completed SYN Stealth Scan at 13:02, 0.03s elapsed (4 total ports)
NSE: Script scanning 192.168.100.102.
Initiating NSE at 13:02
Completed NSE at 13:02, 0.06s elapsed
Nmap scan report for 192.168.100.102
Host is up (0.00070s latency).

PORT      STATE    SERVICE
80/tcp    open     http
|_http-title: Metasploitable2 - Linux
443/tcp   closed   https
8080/tcp  closed   http-proxy
8443/tcp  closed   https-alt
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Use Nmap's --script to detect HTTP services (optional).
This will also show the title of web pages, helping identify running HTTP services.

Kali> nmap -sV -p- 192.168.100.102 | grep http

```
(heLo@HeLo)-[~]
$ nmap -sV -p- 192.168.100.102 | grep http

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 08:29 EDT
80/tcp  open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
8180/tcp open  http      Apache Tomcat/Coyote JSP engine 1.1
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

-p-: Scans all 65535 ports

-sV: Detects services

grep http: Filters results to only show HTTP-related ones.

Kali> nmap -v -p T:443,445,80,U:53 192.168.100.102

```
(k4n0ng@kali)-[~]
$ nmap -v -p T:443,445,80,U:53 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:05 EDT
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Initiating ARP Ping Scan at 13:05
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 13:05, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:05
Completed Parallel DNS resolution of 1 host. at 13:05, 0.00s elapsed
Initiating SYN Stealth Scan at 13:05
Scanning 192.168.100.102 [3 ports]
Discovered open port 80/tcp on 192.168.100.102
Discovered open port 445/tcp on 192.168.100.102
Completed SYN Stealth Scan at 13:05, 0.04s elapsed (3 total ports)
Nmap scan report for 192.168.100.102
Host is up (0.00049s latency).

PORT      STATE    SERVICE
80/tcp    open     http
443/tcp   closed   https
445/tcp   open     microsoft-ds
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

- **-v:** Verbose mode - shows more output during the scan.
- **-p T:443,445,80,U:53:**
 - T: prefix specifies **TCP ports:** 443 (HTTPS), 445 (SMB), 80 (HTTP)
 - U: prefix specifies **UDP port:** 53 (DNS)

```
kali> nmap -v -sS -sU -p T:443,445,80,U:53 192.168.100.102
```

```
(k4n0ng㉿kali)-[~]
└─$ nmap -v -sS -sU -p T:443,445,80,U:53 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:06 EDT
Initiating ARP Ping Scan at 13:06
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 13:06, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:06
Completed Parallel DNS resolution of 1 host. at 13:06, 0.00s elapsed
Initiating SYN Stealth Scan at 13:06
Scanning 192.168.100.102 [3 ports]
Discovered open port 445/tcp on 192.168.100.102
Discovered open port 80/tcp on 192.168.100.102
Completed SYN Stealth Scan at 13:06, 0.04s elapsed (3 total ports)
Initiating UDP Scan at 13:06
Scanning 192.168.100.102 [1 port]
Discovered open port 53/udp on 192.168.100.102
Completed UDP Scan at 13:06, 0.24s elapsed (1 total ports)
Nmap scan report for 192.168.100.102
Host is up (0.00061s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https
445/tcp   open  microsoft-ds
53/udp    open  domain
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

This command To properly scan both TCP and UDP ports, use.

- **-sS:** TCP SYN scan (stealthy and fast)
- **-sU:** Enables UDP scan (required for U: ports to be scanned)
- **-p:** Lists TCP and UDP ports explicitly

```
kali> nmap -v -sU -p T:443,445,80,U:53 192.168.100.102
```

```
(k4n0ng㉿kali)-[~]
└─$ nmap -v -sU -p T:443,445,80,U:53 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:07 EDT
WARNING: Your ports include "T:" but you haven't specified any TCP scan type.
Initiating ARP Ping Scan at 13:07
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 13:07, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:07
Completed Parallel DNS resolution of 1 host. at 13:07, 0.00s elapsed
Initiating UDP Scan at 13:07
Scanning 192.168.100.102 [1 port]
Discovered open port 53/udp on 192.168.100.102
Completed UDP Scan at 13:07, 0.14s elapsed (1 total ports)
Nmap scan report for 192.168.100.102
Host is up (0.00050s latency).

PORT      STATE SERVICE
53/udp    open  domain
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
kali> nmap -v -sS 192.168.100.102
```

```
(k4n0ng㉿kali)-[~]
$ nmap -v -sS 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:09 EDT
Initiating ARP Ping Scan at 13:09
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 13:09, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:09
Completed Parallel DNS resolution of 1 host. at 13:09, 0.00s elapsed
Initiating SYN Stealth Scan at 13:09
Scanning 192.168.100.102 [1000 ports]
Discovered open port 23/tcp on 192.168.100.102
Discovered open port 53/tcp on 192.168.100.102
Discovered open port 22/tcp on 192.168.100.102
Discovered open port 21/tcp on 192.168.100.102
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
```

- -sS: TCP SYN scan (stealthy and fast).
- -v: Enables verbose mode, so Nmap provides more detailed output.

- after this we open wireshark

```
kali> wireshark
```

```
(k4n0ng㉿kali)-[~]
$ wireshark
** (wireshark:6760) 13:09:33.506447 [GUI ECHO] -- virtual const QPalette* Qt
6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::Syst
emPalette
** (wireshark:6760) 13:09:33.507615 [GUI ECHO] -- virtual const QPalette* Qt
6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::Tool
ButtonPalette
** (wireshark:6760) 13:09:33.507855 [GUI ECHO] -- virtual const QPalette* Qt
6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::Butt
onPalette
```

wireshark> ip.addr == 192.168.100.102 && tcp.port == 80

ip.addr == 192.168.100.102 && tcp.port == 80						
No.	Time	Source	Destination	Protocol	Length	Info
48	0.495433695	192.168.100.112	192.168.100.102	TCP	58	6281
73	0.495726878	192.168.100.102	192.168.100.112	TCP	60	80
76	0.495737336	192.168.100.112	192.168.100.102	TCP	54	6281

Frame 48: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0 at 13:13:13.000000000 EDT
Ethernet II, Src: PCSSystemtec_f7:74:f6 (192.168.100.112), Dst: 192.168.100.102 (192.168.100.102)
Internet Protocol Version 4, Src: 192.168.100.112 (192.168.100.112), Dst: 192.168.100.102 (192.168.100.102)
Transmission Control Protocol, Src Port: 54628 (192.168.100.112), Dst Port: 80 (192.168.100.102)
Data (58 bytes): 0000: 08 00 27 96 16 b6 08 00 27 f7 74 0010: 00 2c 51 6b 00 00 33 06 ec 39 c0 0020: 64 66 f5 5b 00 50 12 a7 68 be 00 0030: 04 00 d8 ed 00 00 02 04 05 b4

kali> nmap -v -sA 192.168.100.102

```
(k4n0ng㉿kali)-[~]
$ nmap -v -sA 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:13 EDT
Initiating ARP Ping Scan at 13:13
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 13:13, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:13
Completed Parallel DNS resolution of 1 host. at 13:13, 0.05s elapsed
Initiating ACK Scan at 13:13
Scanning 192.168.100.102 [1000 ports]
Completed ACK Scan at 13:13, 0.05s elapsed (1000 total ports)
Nmap scan report for 192.168.100.102
Host is up (0.00050s latency).
All 1000 scanned ports on 192.168.100.102 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

- sA: Uses an ACK scan, which sends TCP ACK packets to determine firewall rules — not whether the port is open or closed.

Kali> nmap -v -sU 192.168.100.102

```
(k4n0ng㉿kali)-[~]
$ nmap -v -sU 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:13 EDT
Initiating ARP Ping Scan at 13:13
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 13:14, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:14
Completed Parallel DNS resolution of 1 host. at 13:14, 0.01s elapsed
Initiating UDP Scan at 13:14
Scanning 192.168.100.102 [1000 ports]
Discovered open port 53/udp on 192.168.100.102
Increasing send delay for 192.168.100.102 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.100.102 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.100.102 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.100.102 from 200 to 400 due to max_successful_tryno increase to 7
```

-sU: Enables UDP scan (required for U: ports to be scanned)

wireshark> ip.addr == 192.168.100.102 && udp.port

No.	Time	Source	Destination	Protocol	Length	Info
16	6.459410469	192.168.100.102	192.168.100.112	ICMP	142	Des
17	7.260689782	192.168.100.112	192.168.100.102	UDP	42	602
18	7.261589830	192.168.100.102	192.168.100.112	ICMP	70	Des
19	7.327685160	fe80::6025:48ff:fea...	ff02::fb	MDNS	123	Sta
20	7.401735908	192.168.100.44	224.0.0.251	MDNS	103	Sta
21	7.577342163	192.168.100.1	239.255.255.250	SSDP	174	M-S

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface br0
Ethernet II, Src: PCSSystemtec_f7:74:f6 (08:00:27:96:b6:08), Dst: 224.0.0.251 (ff02::fb)
Internet Protocol Version 4, Src: 192.168.100.102 (192.168.100.102), Dst: 239.255.255.250 (ff02::1)
User Datagram Protocol, Src Port: 60228, Dst Port: 131 (53/udp)

kali> nmap -v -sU -p 53,68,67,69 192.168.100.102

Nmap 7.95 Scan Report for 192.168.100.102						
PORT	STATE	SERVICE	Source	Destination	Version	Extra
53/udp	open	domain	08:00:27:96:B6:08	192.168.100.112	192.168.100.102	
67/udp	closed	dhcp	08:00:27:96:B6:08	192.168.100.112	192.168.100.102	
68/udp	open filtered	dhcpc	08:00:27:96:B6:08	192.168.100.112	192.168.100.102	
69/udp	open filtered	tftp	08:00:27:96:B6:08	192.168.100.112	192.168.100.102	
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)						

- **-v:** Enables verbose mode for detailed output.
- **-sU:** Specifies a **UDP scan** (instead of the default TCP).
- **-p 53,68,67,69:** Scans **UDP ports**:
 - 53 → **DNS**
 - 67 → **DHCP server**
 - 68 → **DHCP client**
 - 69 → **TFTP (Trivial File Transfer Protocol)**

kali> nmap -v -sS -sU -p T:80,443,U:53,67,68,69 192.168.100.102

```
(k4n0ng㉿kali)-[~]
$ nmap -v -sS -sU -p T:80,443,U:53,67,68,69 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:17 EDT
Initiating ARP Ping Scan at 13:17
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 13:17, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:17
Completed Parallel DNS resolution of 1 host. at 13:17, 0.00s elapsed
Initiating SYN Stealth Scan at 13:17
Scanning 192.168.100.102 [2 ports]
Discovered open port 80/tcp on 192.168.100.102
Completed SYN Stealth Scan at 13:17, 0.13s elapsed (2 total ports)
Initiating UDP Scan at 13:17
Scanning 192.168.100.102 [4 ports]
Discovered open port 53/udp on 192.168.100.102
Completed UDP Scan at 13:17, 1.50s elapsed (4 total ports)
Nmap scan report for 192.168.100.102
Host is up (0.00054s latency).  

PORT      STATE      SERVICE
80/tcp    open       http
443/tcp   closed    https
53/udp    open       domain
67/udp    closed    dhcps
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Scan Both TCP and UDP Together.

Kali> nmap -v -sT -p 80 192.168.100.102

```
(k4n0ng㉿kali)-[~]
$ nmap -v -sT -p 80 192.168.100.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:18 EDT
Initiating ARP Ping Scan at 13:18
Scanning 192.168.100.102 [1 port]
Completed ARP Ping Scan at 13:18, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:18
Completed Parallel DNS resolution of 1 host. at 13:18, 0.01s elapsed
Initiating Connect Scan at 13:18
Scanning 192.168.100.102 [1 port]
Discovered open port 80/tcp on 192.168.100.102
Completed Connect Scan at 13:18, 0.00s elapsed (1 total ports)
Nmap scan report for 192.168.100.102
Host is up (0.00073s latency).  

PORT      STATE      SERVICE
80/tcp    open       http
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

wireshark> ip.addr == 192.168.100.102 && tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
7	0.321438121	192.168.100.112	192.168.100.102	TCP	74	5999
8	0.321869675	192.168.100.102	192.168.100.112	TCP	74	80
9	0.321900004	192.168.100.112	192.168.100.102	TCP	66	5999
10	0.322011130	192.168.100.112	192.168.100.102	TCP	66	5999


```
Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0
Ethernet II, Src: PCSSystemtec_f7:74:f6 (08:00:27:96:16:B6), Dst: Microsoft TCP (08:00:27:96:16:B6)
Internet Protocol Version 4, Src: 192.168.100.102 (192.168.100.102), Dst: 192.168.100.112 (192.168.100.112)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 102 (102)
```

kali> nmap -v -sT 192.168.100.102

PORT			STATE	SERVICE
21/tcp	open	ftp		
22/tcp	open	ssh		
23/tcp	open	telnet		
25/tcp	open	smtp		
53/tcp	open	domain		
80/tcp	open	http		
111/tcp	open	rpcbind		
139/tcp	open	netbios-ssn		
445/tcp	open	microsoft-ds		
512/tcp	open	exec		
513/tcp	open	login		
514/tcp	open	shell		
1099/tcp	open	rmiregistry		
1524/tcp	open	ingreslock		
2049/tcp	open	nfs		
2121/tcp	open	ccproxy-ftp		
3306/tcp	open	mysql		
5432/tcp	open	postgresql		
5900/tcp	open	vnc		
6000/tcp	open	X11		
6667/tcp	open	irc		
8009/tcp	open	ajp13		
8180/tcp	open	unknown		

MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

- **-sT: TCP Connect Scan** (also called a "full-open scan").

Kali> nmap -v -sT 192.168.100.102 -p 23

```
(heLo@HeLo)-[~] 192.168.100.109      192.168.100.102      TCP      0  
$ nmap -v -sT 192.168.100.102 -p 23  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 11:10 EDT  
Initiating ARP Ping Scan at 11:10  
Scanning 192.168.100.102 [1 port]  
Completed ARP Ping Scan at 11:10, 0.11s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 11:10  
Completed Parallel DNS resolution of 1 host. at 11:10, 0.03s elapsed  
Initiating Connect Scan at 11:10  
Scanning 192.168.100.102 [1 port]  
Discovered open port 23/tcp on 192.168.100.102  
Completed Connect Scan at 11:10, 0.00s elapsed (1 total ports)  
Nmap scan report for 192.168.100.102  
Host is up (0.0010s latency).  
PORT      STATE SERVICE  
23/tcp    open  telnet  
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

-p 23 : Scans **only port 23**, which is usually used by the **Telnet** service.

wireshark> ip.port == 192.168.100.102 && tcp.port == 23

ip.port == 192.168.100.102 && tcp.port == 23						
No.	Time	Source	Destination	Protocol	Length	Info
7	1.819256858	192.168.100.112	192.168.100.102	TCP	74	342
8	1.819640784	192.168.100.102	192.168.100.112	TCP	74	23
9	1.819664780	192.168.100.112	192.168.100.102	TCP	66	342
10	1.819804808	192.168.100.112	192.168.100.102	TCP	66	342
11	3.405426943	192.168.100.45	224.0.0.251	MDNS	103	Sta
12	3.406816895	fe80::552f:7660:6d4...	ff02::fb	MDNS	123	Sta

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface
Ethernet II, Src: PCSSystemtec_f7:74:f6 (08:00:27:96:16:B6), Dst: 224.0.0.251 (ff02::1)
Ethernet II, Src: PCSSystemtec_f7:74:f6 (08:00:27:96:16:B6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request) 00:00:00:00:00:00 c0:a8:64:01

kali> nmap -v -sT -sV 192.168.100.102

```
(k4n0ng@kali)-[~]  
$ nmap -v -sT -sV 192.168.100.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:24 EDT  
NSE: Loaded 47 scripts for scanning.  
Initiating ARP Ping Scan at 13:24  
Scanning 192.168.100.102 [1 port]  
Completed ARP Ping Scan at 13:24, 0.06s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 13:24  
Completed Parallel DNS resolution of 1 host. at 13:24, 0.01s elapsed  
Initiating Connect Scan at 13:24  
Scanning 192.168.100.102 [1000 ports]  
Discovered open port 139/tcp on 192.168.100.102  
Discovered open port 53/tcp on 192.168.100.102  
Discovered open port 22/tcp on 192.168.100.102
```

```

PORT      STATE SERVICE          VERSION
21/tcp    open  ftp   vsftpd  2.3.4
22/tcp    open  ssh   OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet Linux telnetd  2.0.0-56.250
25/tcp    open  smtp  Postfix smptd  2.10.1-2.168.100.44
53/tcp    open  domain ISC BIND 9.4.2
80/tcp    open  http  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec   netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs   2-4 (RPC #100003)
2121/tcp  open  ftp   ProFTPD 1.3.1
3306/tcp  open  mysql MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc   VNC (protocol 3.3)
6000/tcp  open  X11   (access denied)
6667/tcp  open  irc   UnrealIRCd
8009/tcp  open  ajp13 Apache Jserv (Protocol v1.3)
8180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

is used to perform a **TCP Connect Scan** with **version detection** on the target IP 192.168.100.102, and provides **verbose output**.

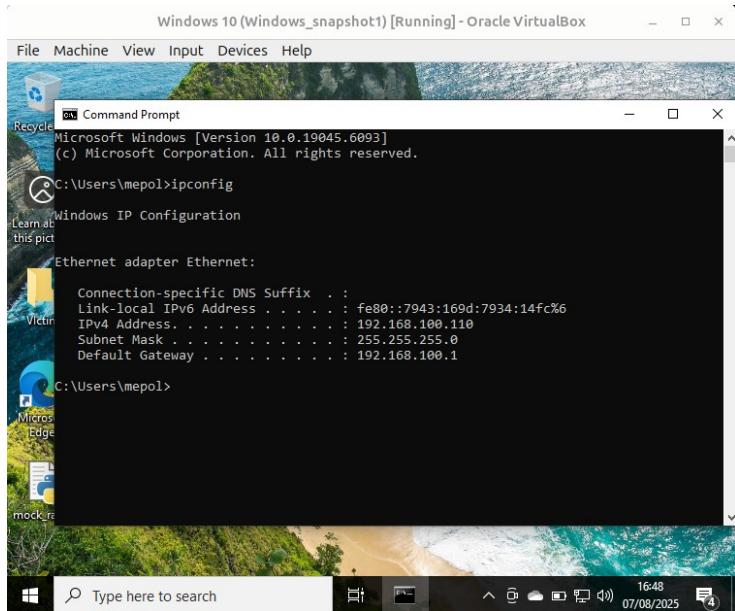
ip.port == 192.168.100.102 && tcp.port == 23						
No.	Time	Source	Destination	Protocol	Length	Info
2629	152.167218242	fe80::6025:48ff:fea...	ff02::fb	MDNS	123	Sta
2630	152.216349214	192.168.100.1	239.255.255.250	SSDP	174	M-S
2631	152.476596417	192.168.100.1	239.255.255.250	SSDP	175	M-S
2632	152.484892061	fe80::f3:23ff:fee7:...	ff02::fb	MDNS	139	Sta
2633	152.578371020	192.168.100.43	224.0.0.251	MDNS	119	Sta
2634	152.780870483	192.168.100.1	239.255.255.250	SSDP	175	M-S

▶ Frame 1: 42 bytes on wire (336 bits), 42	0000 64 c3 94 d6 8b 5c 08 00 27 f7 74
▶ Ethernet II, Src: PCSSystemtec_f7:74:f6	0010 08 00 06 04 00 01 08 00 27 f7 74
▶ Address Resolution Protocol (request)	0020 00 00 00 00 00 00 c0 a8 64 01

-sT: **TCP Connect Scan** – uses full TCP handshake to detect open ports.

-sV: **Service/version detection** – tries to determine software versions.

- Open the windows10:



we already closed firewall.

Kali> nmap -v -sT -sV -O 192.168.100.110

```
(k4n0ng㉿kali)-[~]
$ nmap -v -sT -sV -O 192.168.100.110
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 10:54 EDT
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 10:54
Scanning 192.168.100.110 [1 port]
Completed ARP Ping Scan at 10:54, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:54
Completed Parallel DNS resolution of 1 host. at 10:54, 0.00s elapsed
Initiating Connect Scan at 10:54
Scanning 192.168.100.110 [1000 ports]
Discovered open port 139/tcp on 192.168.100.110
Discovered open port 135/tcp on 192.168.100.110
Discovered open port 445/tcp on 192.168.100.110
Increasing send delay for 192.168.100.110 from 0 to 5 due to 54 out of 179

PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:ED:C4:45 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 21H2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

- **-v: Verbose mode:** Provides more detailed output. You'll see progress and additional information during the scan.

- **-sT: TCP connect scan:** Nmap completes the full TCP 3-way handshake (SYN → SYN-ACK → ACK). This is less stealthy than SYN scan (-sS) but doesn't require raw packet privileges (can be run without root).
- **-sV: Service version detection:** Nmap attempts to determine the version of services running on open ports (e.g., Apache 2.4.41, OpenSSH 8.2p1).
- **-O: Enable OS detection:** Nmap tries to guess the operating system of the target based on TCP/IP stack fingerprinting.

Kali> nmap -v -sT -sV -O -A 192.168.100.110

```
(k4n0ng㉿kali)-[~]
└─$ nmap -v -sT -sV -O -A 192.168.100.110
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 10:56 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Initiating ARP Ping Scan at 10:56
Scanning 192.168.100.110 [1 port]
Completed ARP Ping Scan at 10:56, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:56
Completed Parallel DNS resolution of 1 host. at 10:56, 0.00s elapsed
Initiating Connect Scan at 10:56
Scanning 192.168.100.110 [1000 ports]
Discovered open port 445/tcp on 192.168.100.110
Discovered open port 139/tcp on 192.168.100.110
Discovered open port 135/tcp on 192.168.100.110
Not shown: 996 closed tcp ports (conn refused)

PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?  Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 08:00:27:ED:C4:45 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 21H2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

- **-A : Aggressive mode:** Enables a suite of advanced features:
 - OS detection (-O)
 - Version detection (-sV)
 - Script scanning (--script=default)
 - Traceroute (-traceroute)

1. Overview of Nmap

- Nmap is used to provide detailed, real-time information about networks and devices connected to them.

- It helps administrators and users understand their network infrastructure, identify vulnerabilities, and protect against potential threats.

2. Primary Uses of Nmap (Three Core Processes)

a. First Use: Detailed Information on Active IPs

- Nmap provides detailed information about every active IP address on your network.
- **Process:**
 - Each IP can be scanned to determine its purpose.
 - This allows administrators to check whether an IP is being used by a legitimate service or by an external attacker.
- Helps in identifying unauthorized access or malicious activity.

b. Second Use: Network-wide Information

- Nmap provides comprehensive information about the entire network.
 - It generates a list of live hosts (active devices) and open ports.
 - It identifies the operating system (OS) of each connected device.
- **Applications:**
 - **Ongoing System Monitoring:** Tracks network activity and ensures everything is functioning as expected.
 - **Penetration Testing:** Used alongside tools like the **Metasploit Framework** to probe network vulnerabilities and repair them.
 - Example: Nmap can help identify open ports that could be exploited by attackers.

c. Third Use: Website Security

- Nmap is valuable for users looking to protect personal and business websites.
- **Process:**
 - Scanning your own web server (especially if hosted from home) simulates how a hacker might attack your site.
 - By "attacking" your own site in this way, you can identify security vulnerabilities before they are exploited by actual attackers.
- Proactive security testing to strengthen defenses.

3. Key Takeaways

1. **Network Inventory and Security:** Nmap helps administrators manage and secure their networks by providing detailed information about active IPs, live hosts, open ports, and connected devices.
2. **Integration with Other Tools:** Nmap can work alongside frameworks like Metasploit to perform advanced penetration testing and vulnerability assessment.

3. **Website Protection:** Nmap enables users to simulate attacks on their own websites, helping them identify and fix security weaknesses proactively.

Run a ping Scan

1. Overview of Ping Scan

- One of the basic functions of Nmap is to identify active hosts (devices) on your network.
- Nmap performs this by conducting a **ping scan**, which detects all IP addresses currently online without sending any packets directly to those hosts.
 - A ping scan is a non-intrusive way to discover active devices on a network.

Kali> nmap -sP 192.168.100.1/24 (old syntax)

```
(k4n0ng㉿kali)-[~]
$ nmap -sP 192.168.100.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 10:59 EDT
Nmap scan report for 192.168.100.1
Host is up (0.0028s latency).
MAC Address: 64:C3:94:D6:8B:5C (Huawei Technologies)
Nmap scan report for 192.168.100.28
Host is up (0.10s latency).
MAC Address: 3C:55:76:D0:B5:EF (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.100.33
Host is up (0.10s latency).
MAC Address: 9A:6E:94:6A:3F:15 (Unknown)
Nmap scan report for 192.168.100.36
Host is up (0.10s latency).
MAC Address: EE:E1:81:11:CE:AF (Unknown)
```

kali> nmap -sn 192.168.100.1/24 (New syntax)

```
(k4n0ng㉿kali)-[~]
$ nmap -sn 192.168.100.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 11:00 EDT
Nmap scan report for 192.168.100.1
Host is up (0.0076s latency).
MAC Address: 64:C3:94:D6:8B:5C (Huawei Technologies)
Nmap scan report for 192.168.100.28
Host is up (0.14s latency).
MAC Address: 3C:55:76:D0:B5:EF (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.100.33
Host is up (1.1s latency).
MAC Address: 9A:6E:94:6A:3F:15 (Unknown)
Nmap scan report for 192.168.100.43
Host is up (0.10s latency).
MAC Address: 02:F3:23:E7:98:B6 (Unknown)
```

- **-sn** (Ping Scan): Skips port scanning and only checks which hosts are up.
- **192.168.100.1/24**: Scans the IP range 192.168.100.0 to 192.168.100.255.
- Nmap will send **ICMP Echo Request** and sometimes **ARP requests** (on local LAN) to identify live devices.
- Output will list each detected host and its IP (and sometimes hostname + MAC address).

Scan an IPV6 Target

The -6 parameter is used to perform a scan of IP version 6 target.

Kali> nmap -6 fe80::a00:27ff:fe96:16b6

```
(k4n0ng㉿kali)-[~]
$ nmap -6 fe80::a00:27ff:fe96:16b6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 11:03 EDT
Nmap scan report for fe80::a00:27ff:fe96:16b6
Host is up (0.000075s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
2121/tcp  open  ccproxy-ftp
5432/tcp  open  postgresql
MAC Address: 08:00:27:96:16:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

End Part 1

contact:

Gmail: ninkanong200620@gmail.com