NMAP and Its Scanning Techniques

Before Moving to the NMAP you should clear your basics of Network and its Connection establish Processes: -

-Network Protocols

-Network Well-known Ports

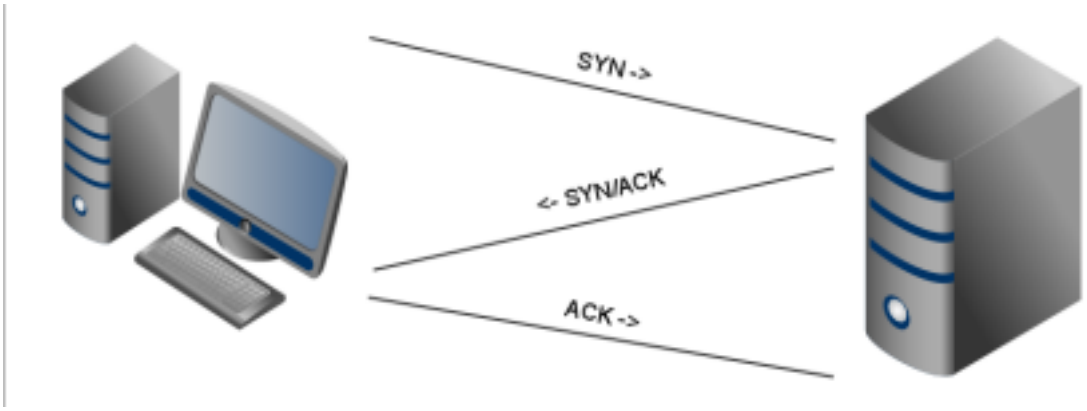
-Connection Establishes Processes

Lets start with the Essential Process for Network:-

Connection Establishes Processes: -

TCP three-way handshake

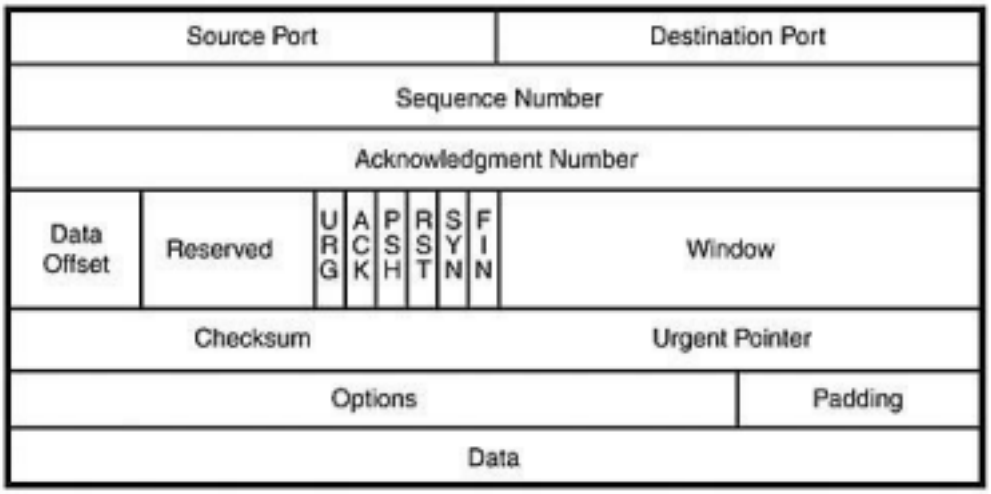
RST The TCP three-way handshake in Transmission Control Protocol is the method used by TCP set up a TCP/IP connection over an Internet Protocol based network. TCP's three-way handshaking technique is often referred to as "SYN-SYN-ACK" (or more accurately SYN, SYN-ACK, ACK)



TCP Communication Flags

In TCP most popular flags are the "SYN", "ACK" and "FIN" which are used to establish connections, acknowledge successful segment transfers and finally terminate connections. In addition to these 3 flags there are other 3 additional flags which are used for the below purposes

- — Aborts a connection in response to an error
- **URG,PSH** — Data contained in the packets should be processed immediately



Let’s Move to Nmap

What is nmap?

NMAP is a free and open source utility for network discovery and security auditing. Like there are too many devices connected to the network and a pentester or network administrators will gather a information like which type of devices, their services uptimes, live systems, which kind of services are running their with the help of this utility.

How its work?

The raw IP packets which is used by NMAP for determine what hosts are available on the network, what services (application name and version) those host are offering, which operating systems and its versions are running, what type of packet filters or firewall are implemented, and lots of other tasks.

Scanning Techniques: -

Cheatsheet

Switch Description Example

-sS TCP SYN port scan. nmap -sS 192.168.1.1

-sT TCP Connect port scan nmap -sT 192.168.1.1

-sU UDP port scan. nmap -sU 192.168.1.1

-sA TCP ACK port scan. nmap -sA 192.168.1.1
Switch Description Example

-Pn Only port scan. nmap -Pn 192.168.1.1
-sn Only host discovery. nmap -sn 192.168.1.1
-PR ARP discovery on local network. nmap -PR 192.168.1.1
-n Disable DNS resolution. nmap -n 192.168.1.1

HOST Scan: - This Scan is used to find or identify active host in the network by sending ARP request packets to all system in that network. And in result it will show a message "Host is up" by Receiving MAC address from Each active host

Syntax: - nmap -sP target_ip_range

nmap -sn target_ip_range

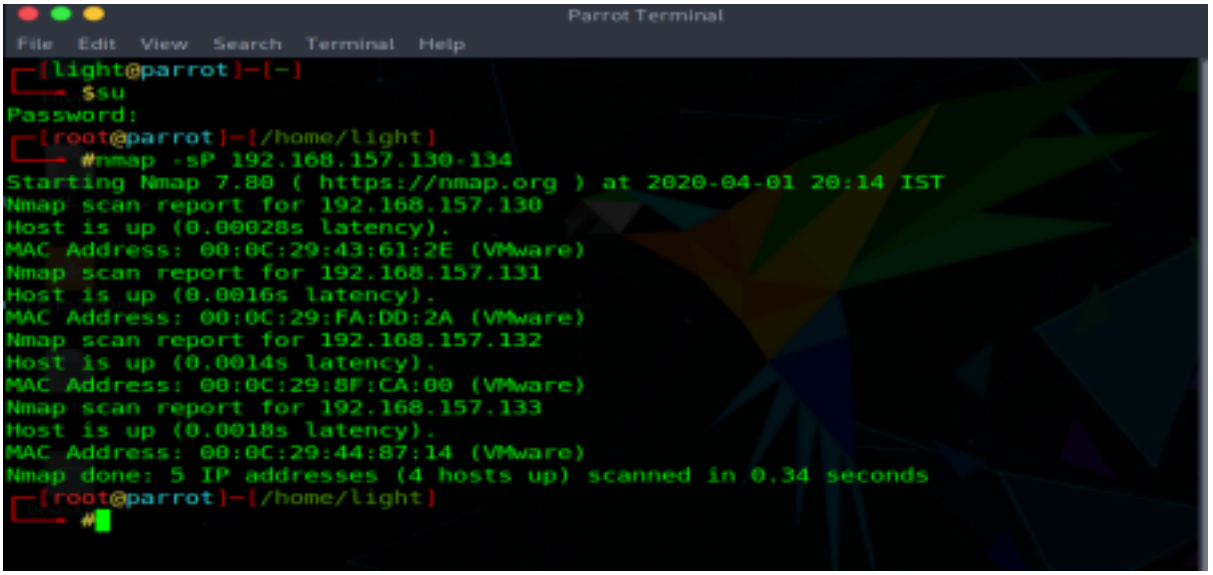
How it works?

-Sp/-sn stand for **Nmap Sweep Ping**

-sP/-sn for host scan and broadcast ARP request Packet to Identify IP allocated to particular host machine.

-By default, PING scan sends the ICMP echo request and gets an ICMP echo request and if system is alive then PING scan by default send and ARP packet and gets a response to check if the host is up.

It will broadcast ARP request for particular IP or its range. After then active host will unicast ARP packet by sending its MAC address as reply which gives a message Host is up.



Port Scan/TCP Scan/Stealth Scan: -
With the help of this scan USER can Identify open or close state of a particular port on target machine.

Port Status: -

Nmap uses 6 different port status: -

Open: - An open port is one that is actively accepting TCP, UDP or SCTP Connections. Open ports are what interests us the most because they are the ones that are vulnerable to attacks. Open ports also show the available services on a network.

Closed :- A port that receives and responds to Nmap probe packets but there is no application listening on that port. Useful for identifying that the host exists and for OS detection.

Filtered: - Nmap can't determine whether the port is open because packet filtering prevents its probes from reaching the port. Filtering could come from firewalls or router rules. Often little information is given from filtered ports during scans as the filters can drop the probes without responding or respond with useless error messages e.g. destination unreachable.

Unfiltered: - Port is accessible but Nmap doesn't know if its open or closed. Only used in ACK scan which is used to map firewall rulesets. Only used in ACK scan which is used to map firewall rulesets. Other scan types can be used to identify whether the port is open.

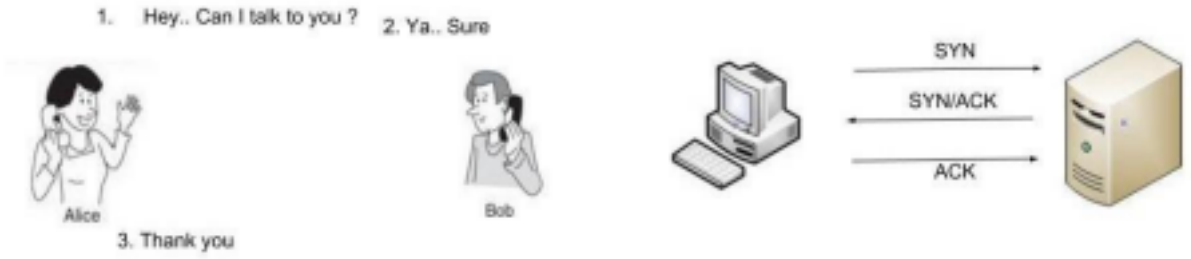
Open/filtered:- Nmap is unable to determine between open and filtered. This happens when an open port gives no response. No response means that the probe was dropped by a packet filter or any response is blocked.

Closed/filtered :- Nmap is unable to determine whether port is closed or filtered. Only used in IP ID idle scan.

Syntax :- nmap -p port_number or service_name target_IP_range

nmap -sT port_number target_IP_range

How it works :-



Port is open

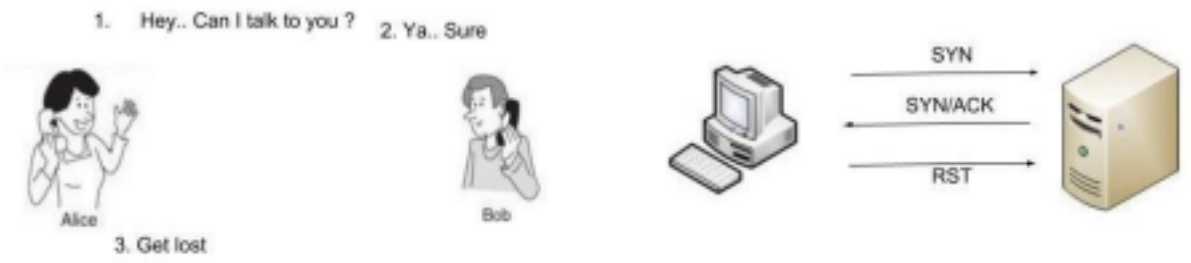
Port is closed

```
┌─[root@parrot]─[/home/light]
└──╼ #nmap -p80 192.168.157.130-134
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-01 23:52 IST
Nmap scan report for 192.168.157.130
Host is up (0.00021s latency).

PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 00:0C:29:43:61:2E (VMware)

Nmap scan report for 192.168.157.131
Host is up (0.00035s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap scan report for 192.168.157.132
Host is up (0.00039s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:8F:CA:00 (VMware)

Nmap done: 5 IP addresses (3 hosts up) scanned in 0.48 seconds
```

UDP Scan:- This method is used to list all open UDP ports on a host.
With the help of this scan penetration testers know that they often expose host essential information or can even be vulnerable moreover used to compromise a host.

Synatx:- nmap -sU target_IP

How it works :- UDP scan works by sending a UDP packet to every destination port. And it is connection less protocal. Sends 0-byte UDP packets to each target port on the victim. Receipt of an ICMP Port Unreachable message signifies the port is closed, otherwise it is assumed open.



Port is open

Port is closed

```
┌─[root@parrot]─[/home/light]
└──╼ #nmap -sU 192.168.157.130-134
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 16:50 IST
Nmap scan report for 192.168.157.130
Host is up (0.00043s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
69/udp open|filtered tftp
MAC Address: 00:0C:29:43:61:2E (VMware)

Nmap scan report for 192.168.157.131
Host is up (0.00036s latency).
Not shown: 993 closed ports
PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap scan report for 192.168.157.132
Host is up (0.00038s latency).
Not shown: 997 closed ports
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
MAC Address: 00:0C:29:8F:CA:00 (VMware)

Nmap scan report for 192.168.157.133
Host is up (0.00051s latency).
Not shown: 999 open|filtered ports
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 00:0C:29:44:87:14 (VMware)
```

XMAS SCAN: - This scan is accomplished by sending packets with the FIN, URG and PUSH flags, if the server sends RST's regardless of the port state, then that is not vulnerable to this type of scan. If the client didn't get any response, then the port is considered as open.

Xmas Scan is only workable in Linux machines and does not work on the latest version of windows

Syntax :- nmap -sX target_IP

How it works:-

In this scan manipulate the PSH, URG and FIN flags of the TCP header, Sets the FIN, PSH, and URG flags, lightning the packet up like a Christmas tree. When Source sent FIN, PUSH, and URG packet to a specific port if the port is open then destination will discard the packets and will not send any reply to the source.

Port is open

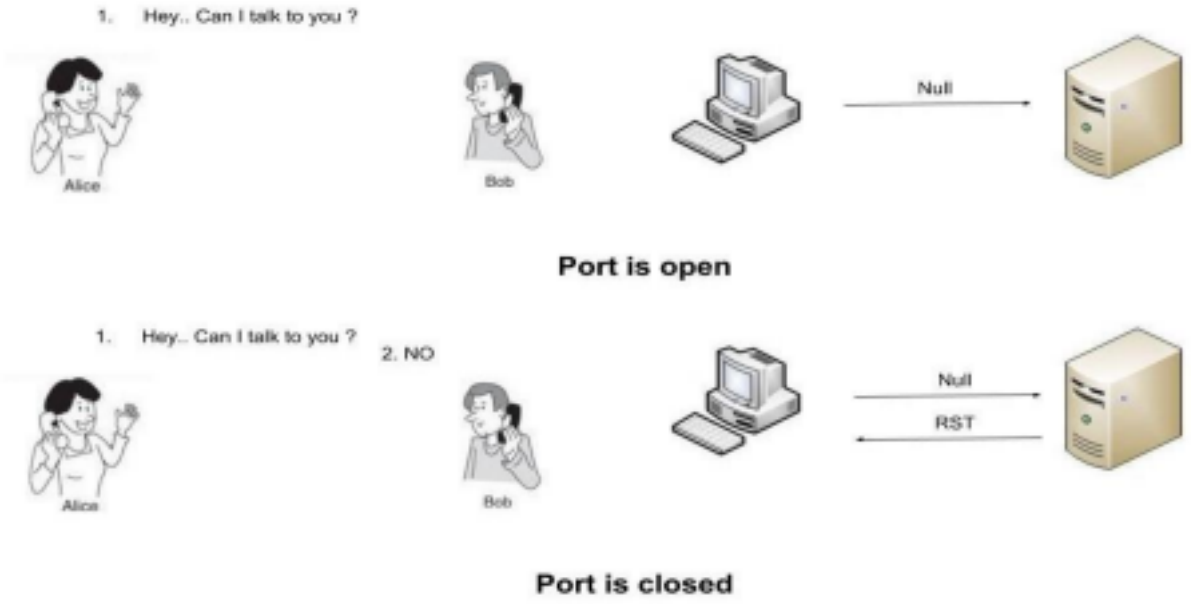
Port is closed

```
┌─[root@parrot]─[/home/light]
└──╼ #nmap -sX  192.168.157.130-134
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 17:45 IST
Nmap scan report for 192.168.157.130
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.157.130 are closed
MAC Address: 00:0C:29:43:61:2E (VMware)

Nmap scan report for 192.168.157.131
Host is up (0.0025s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)
```

NULL Scan :- Null scan sends a packet with no flags switched on, if the server sends RST'S regardless of the port state, them tha is not vulnerable to this type of scan. If the client didn't get any response, them the port is considered as open.

Syntax :- nmap -nS target_IP

How it works :- in this scan that sets all the TCP header flags to off or null.

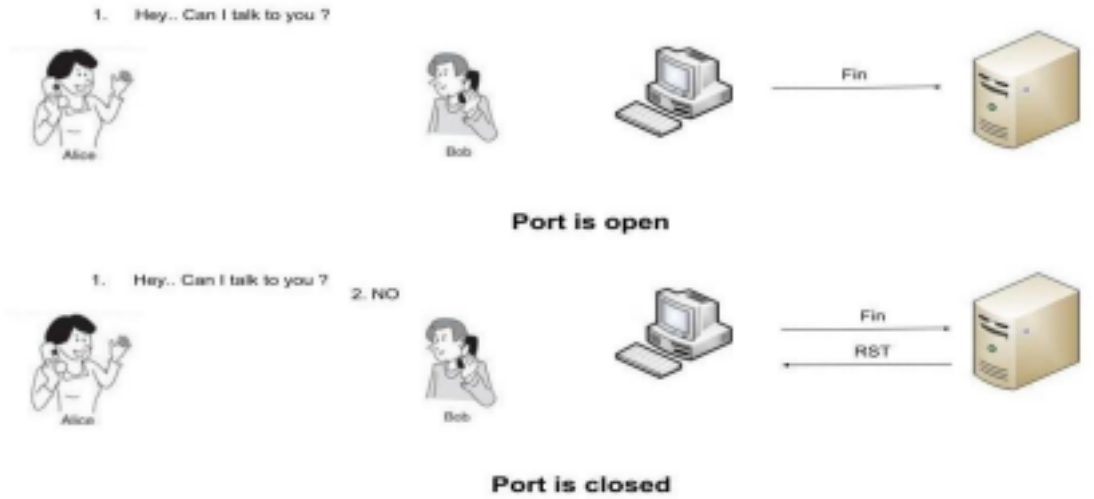



```
┌─[root@parrot]─[/home/light]
└──╼ #nmap -sN  192.168.157.131
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 18:17 IST
Nmap scan report for 192.168.157.131
Host is up (0.0031s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds
```

FIN Scan:- A FIN packet is used to terminate the tcp connection between source and destination port typically after the data transfer is complete. In the place of SYN packet, Nmap starts a FIN scan by using a FIN packet. If the port is open then no response will come from destination port when FIN packet is send through source port.

Syntax: - nmap -sF target_IP

How it works: -The Working process behind this scan is closed ports tend to reply to your FIN packet with the proper RST, if the server sends RST's regardless of the port state, then that is vulnerable to this type of scan. If the client didn't get any response, the port is considered as open.




```
┌──[root@parrot]─[/home/tight]
└──╼ #nmap -sF  192.168.157.131
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-03 12:02 IST
Nmap scan report for 192.168.157.131
Host is up (0.00013s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)
```

OS Detection SCAN :- Apart from open port enumeration nmap is quite useful in OS fingerprinting. This scan very helpful to penetration tester in order to conclude possible security vulnerabilities and determining the available system calls to set the specific exploit payloads.

Syntax: nmap -O target_ip

How it works:- **Device type:** All fingerprints are classified with one or more high-level device types, such as router, printer, firewall, general purpose. These are further described in the section called “Device and OS classification (Class lines)”. If you notice given below image here “Device Type: general purpose”.
Running: This field is also related to the OS classification scheme described in the section called “Device and OS classification (Class lines)”. It shows the OS Family (Windows in this case) and OS generation if available. If there are multiple OS families, they are separated by commas. When Nmap can’t narrow down OS generations to one specific choice, options are separated by the pipe symbol (‘|’)

Examples include OpenBSD 3.X, NetBSD 3.X|4.X and Linux 2.4.X|2.5.X|2.6.X.

If you will image given below again then here you will observe OS generations is specified as **7|2008|8.1**

OS CPE: This shows a Common Platform Enumeration (CPE) representation of the operating system when available. It may also have a CPE representation of the hardware type. OS CPE begins with cpe:/o and hardware CPE begins with cpe:/h.

OS details: This line gives the detailed description for each fingerprint that matches. While the Device type and Running lines are from predefined enumerated lists that are easy to parse by a computer, the OS details line contains free-form data which is useful to a human reading the report. This can include more exact version numbers, device models, and architectures specific to a given fingerprint.

The option -O inform Nmap to enable OS detection that identify a wide variety of systems, including residential routers, IP webcams, operating systems, and many other hardware devices

You can also execute following command for os detection

Syntax: nmap -O -p- –osscan-guess <target>

In case OS detection fails, you can use the argument –osscan-guess to try to guess the operating system:

To launch OS detection only when the scan conditions are ideal, uses the argument –osscan-limit:

Syntax: nmap -O –osscan-limit <target>

```
┌──[root㉿parrot]─[~/Home/light]
└─# nmap -O 192.168.157.131,133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-03 12:50 IST
Nmap scan report for 192.168.157.131
Host is up (0.00082s latency).
Not shown: 977 closed ports
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: 00:0C:29:FA:DD:2A (VMware)
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

Nmap scan report for 192.168.157.133
Host is up (0.00059s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2000/tcp open  cisco-sccp
MAC Address: 00:0C:29:44:B7:14 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 9.59 seconds
```