Nmap – tcp and port scanning

1. Open https://nmap.org/download.html, click on OS for which you want to download
2. Then install that downloaded exe file.

TCP Scanning

Run this command in linux/unix

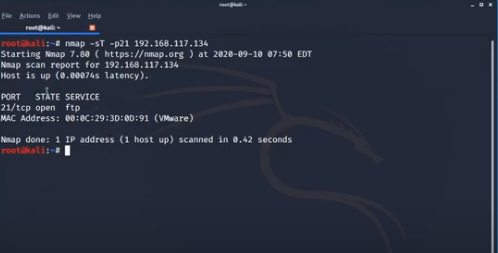
Nmap –sT –p21 192.168.117.134

-s – scan

-T – tcp scan

-p21 – given port number 21

Then ip address – target machine



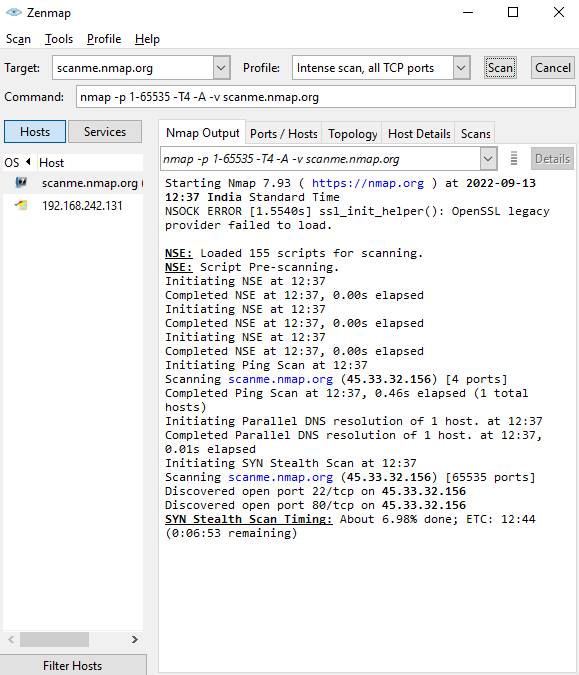
Output shows that port 21 is open and ftp service is running on that.

Now examine this in wireshark.

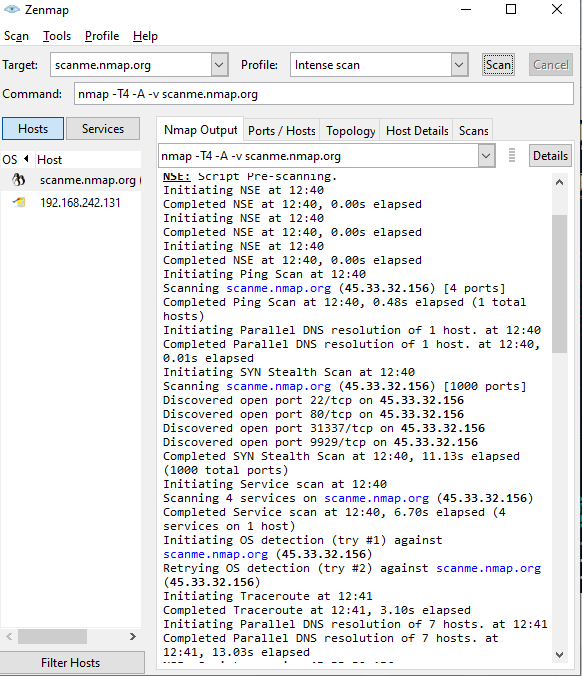
Open wireshark and then run this command again so we can see 3 way tcp handshake. So it is clear that someone is scanning my system. Some one is performing port scanning so we should block it.

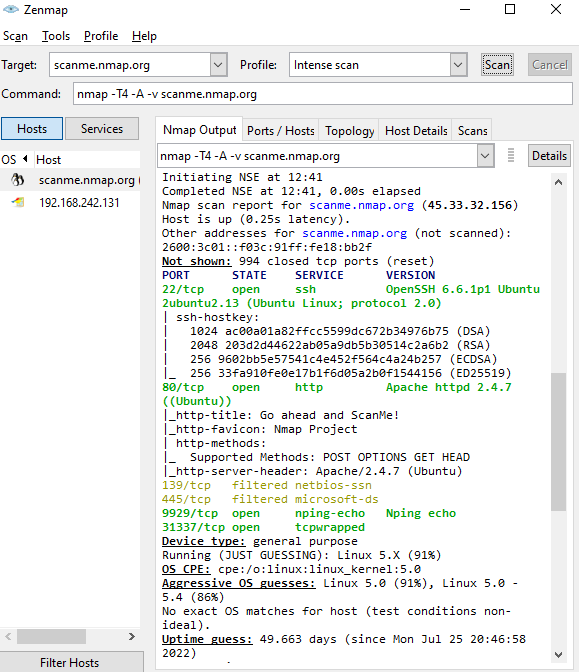
<https://www.youtube.com/watch?v=pytnN9YBTdU>

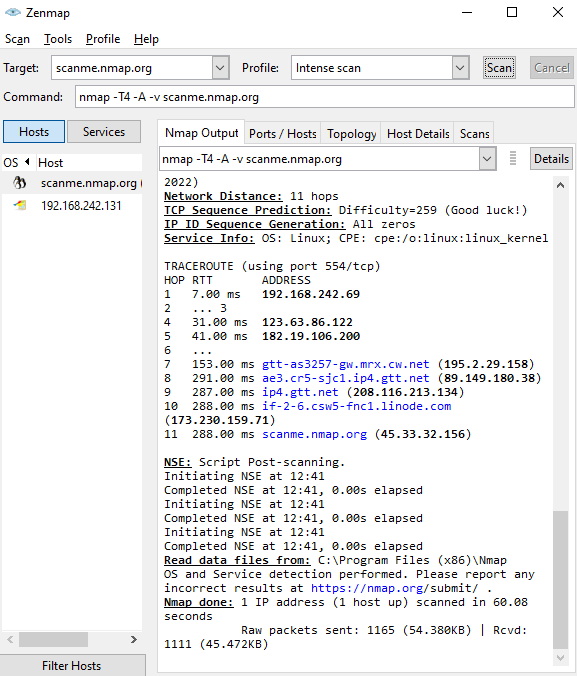
tcp scan on scanme.nmap.org



Intense scans







**Nmap with turmux**

**How to scan a Website with Nmap Termux :**

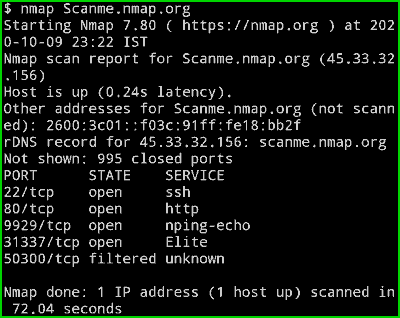
To **scan a Website** you must have permissions Else it can cause you Trouble, Nmap allows you to Scan there Test website so, in this post, we will use that website, you just have to type Nmap and then the site name you can **paste the below command** in the termux **to scan the Nmap test website.**

*nmap Scanme.nmap.org*

[How to Install and Use Nmap In Termux - 2020](https://1.bp.blogspot.com/-L7BCNUVXZj8/X4CuFdI2PLI/AAAAAAAASEo/I6rRMZ9RseAjv72jKzhK5TNv6NMwyYbrwCLcBGAsYHQ/s400/scan+website+with+nmap.png)

**Output :**

You can see that we got an**IP-Adress of the website** in the second line as well as we can see the**latency is 0.24 Seconds.**and we can also **see all the open port of the website.**



**Scan your Local Network with Nmap Termux :**

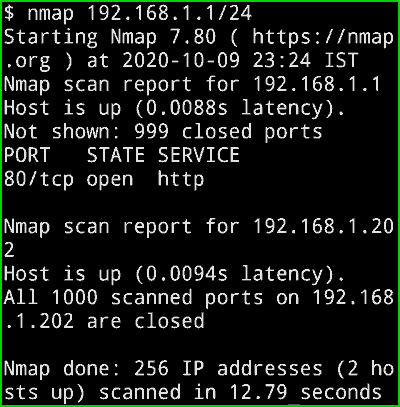
If You just wanna**scan your Local network (Your Intire subnet )**and**know How many devices are connected with your Wifi**then you can use this command. This command will give you a**list of all Devices in the network** as well as you**all the open ports**of those devices.

*nmap 192.168.1.1/24*

[How to Install and Use Nmap In Termux - 2020](https://1.bp.blogspot.com/-Lb4ItRZSfqQ/X4CuFn1DbWI/AAAAAAAASEs/Hhwrw0VVrPY-4HIG4yOW-SIo5oTG_EZpgCLcBGAsYHQ/s400/scan-a-IP-adress-in-termux-nmap.png)

**Output :**

Now you can see in the below picture,**I have 2 devices in my network.**and you can also see**all the open ports**. The 192.168.1.202**Host is up**and the **latency is 0.0025s.** If you have multiple devices on your network then it will show you a list of all the Devices.

[](https://1.bp.blogspot.com/-eLmNpSSgm88/X4CuEHupSUI/AAAAAAAASEU/KgJr4VH0D6caNY30OR0lBAq5OhezXRz6QCLcBGAsYHQ/s407/nmap-output-Ip-Scan.png)

**Aggressive scan using Nmap Termux :**

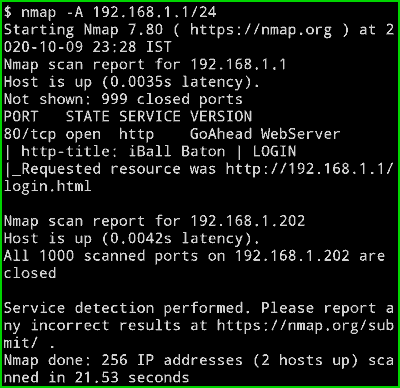
In the above Local Network scan, It won't show you detailed information but if you want to **see every possible detail**then you can use**-A argument in the command.** I am just gonna use the above command with -A argument.

*nmap -A 192.168.1.1/24*

[How to Install and Use Nmap In Termux - 2020](https://1.bp.blogspot.com/-qm_Q8fW0MW8/X4CuDIxvczI/AAAAAAAASEE/ijdgA98gJio-UwBIGMDi9Kw-HvM0OtARACLcBGAsYHQ/s400/nmap-Agressive-scan.png)

**Output :**

Now you can see **Its showing iBall Baton I Login** as well as it is showing the**URL of the login page**. This is just my local network that's why you are unable to see anything interesting but if are scanning any website then it can surely give you some extra data.



**Scan a Single port in Nmap Termux :**

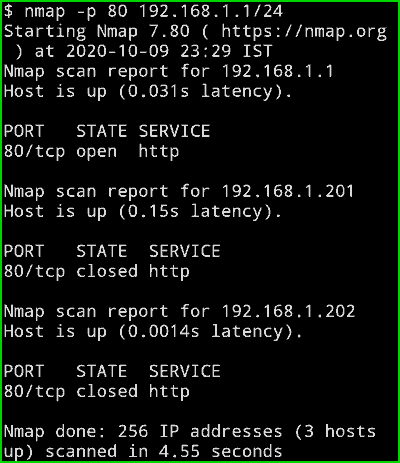
If you just wanna **scan a Single Port of a Particular Ip address** then you can do that using the below command. Here I am scanning the entire **network for the port 80**but you can put a single IP and it will work Perfectly. The advantage of scanning a single port is that it will **save you some extra time**especially when you are in a hurry.

*nmap -p 80 192.168.1.1/24*

[How to Install and Use Nmap In Termux - 2020](https://1.bp.blogspot.com/-ZMx3b9gKijQ/X4CuETRZNzI/AAAAAAAASEY/1jS0Ua1ugy0kIAQBc0ILZD4LvUJ7q0EkwCLcBGAsYHQ/s400/nmap-scan-port80.png)

**Output :**

Here you can see that Nmap is checking for **port 80 only**but on my entire network.



**Scan Multiple Port in Nmap Termux :**

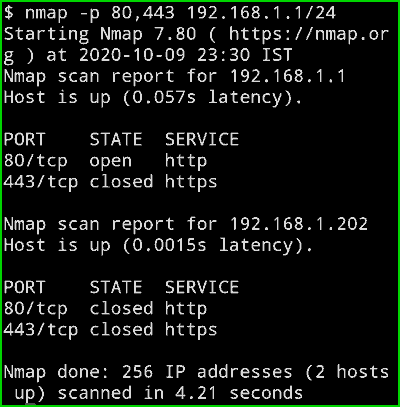
Do you know most of the time when you scan a Network and you find a device with open port 80 as well as 443 then it means that its a **WebServer**? So In the below command, I am gonna scan these two ports on my network, of course, I don't have a webserver running in my home so it won't show 443 port but if you scan it in a network where they have a webserver then it will show with this command.

*nmap -p 80,443 192.168.1.1/24*

[How to Install and Use Nmap In Termux - 2020](https://1.bp.blogspot.com/-YjOzlFJcfn4/X4CuGKm3g1I/AAAAAAAASEw/3m3dprvI3RwfkwyOzp5xyHx1s8KYVN6_gCLcBGAsYHQ/s400/scan-multiple-ports-nmap.png)

**Output :**

In the below picture you can clearly see that it is **only checking for 2 port** and as the output, we can see in my routers Ip address port 80 is open but port 443 is not. And in my second device, Both ports are closed.

****

**Ping A Website or an IP-Address with Nmap in Termux :**

If you Quickly wanna Check if a**Host is still up or not** then you can **do a Ping.** It will tell you the amount of time it took the Nmap to make a connection with the website or the Device.

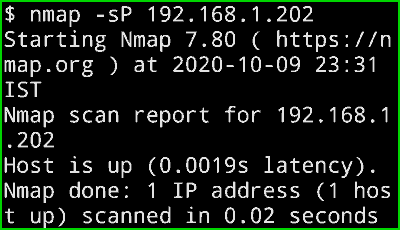
*nmap -sP 192.168.1.202*

[How to Install and Use Nmap In Termux - 2020](https://1.bp.blogspot.com/-eTqk74FjxBM/X4CuFGrPeBI/AAAAAAAASEk/BxinOZjHq1ExypC8ac7zejH-BRXJ9UQeQCLcBGAsYHQ/s400/ping-website-or-IP-using-Nmap.png)

You can also Type **Nmap -sP www.scanme.namp.org**and it will ping the google server and tell you latency.

**Output :**

You can see that the **latency is 0.02 seconds** and the**Host is still up.**

****

**Perform a Quick Scan with Nmap in Termux:**

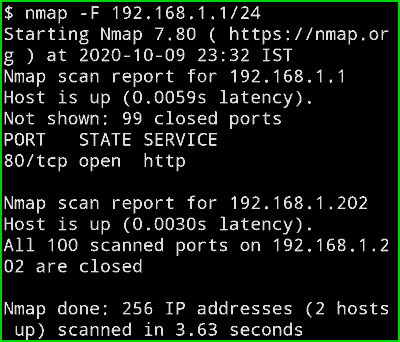
If you just wanna do a**quick scan of the network**and you only wanna know **basic information**then you can use**-F Argument**. It is much faster than the normal scan.

*nmap -F 192.168.1.1/24*

[How to Install and Use Nmap In Termux - 2020](https://1.bp.blogspot.com/-XBaNMcDoXVg/X4CuD5LPq_I/AAAAAAAASEQ/d2D35SKIDt4KGamSHXaRnJmYvqcXMSlOACLcBGAsYHQ/s400/nmap-fast-scan-termux.png)

**Output :**

Here you can see **I got the output much faster** and The**result is still good.**



Check Nmap Version in Termux :

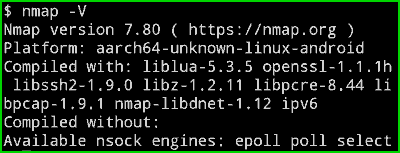
If you wanna **check the Nmap Version** then you can type the below command.

*nmap -V*

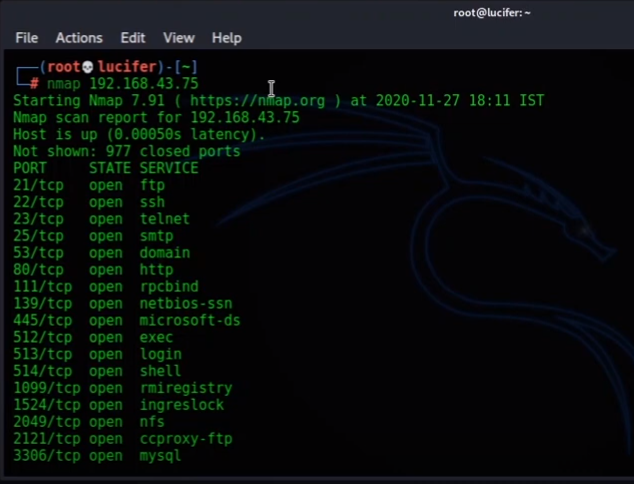
[](https://1.bp.blogspot.com/-LQ-U-6rJfzI/X4CuB08xx3I/AAAAAAAASD4/3v_2qs40Y-sWDXwjMmFQ3OJDwPf9cjS9wCLcBGAsYHQ/s400/check-nmap-version.png)

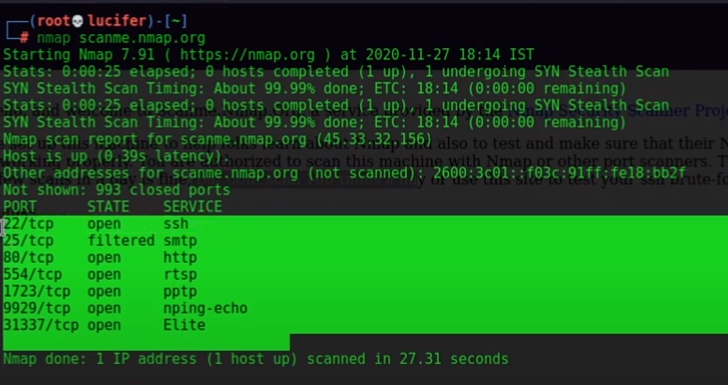
**Output :**

Now you can see the**Nmap Version in the below picture.**

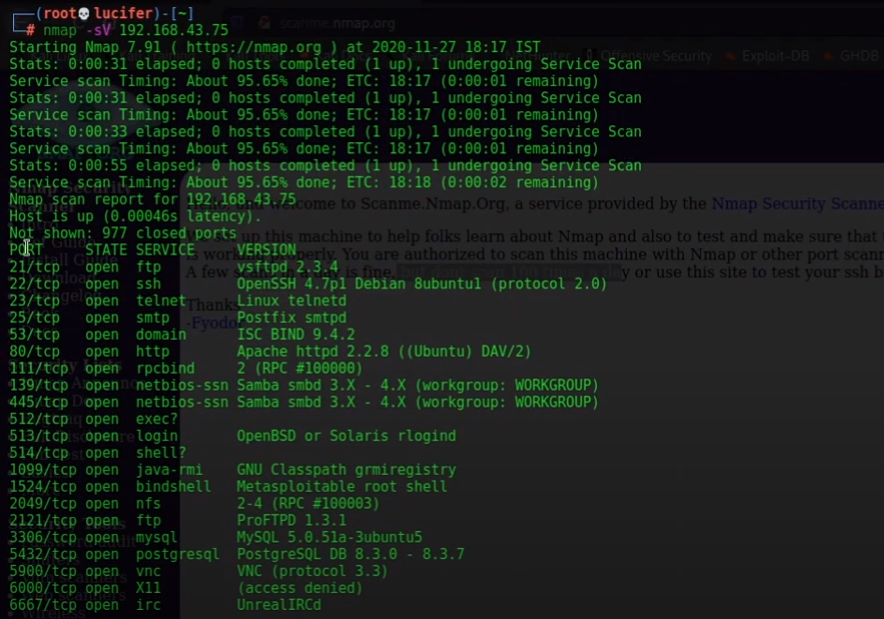


Namp in klai linux with metasploitable

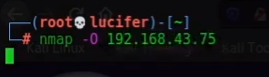


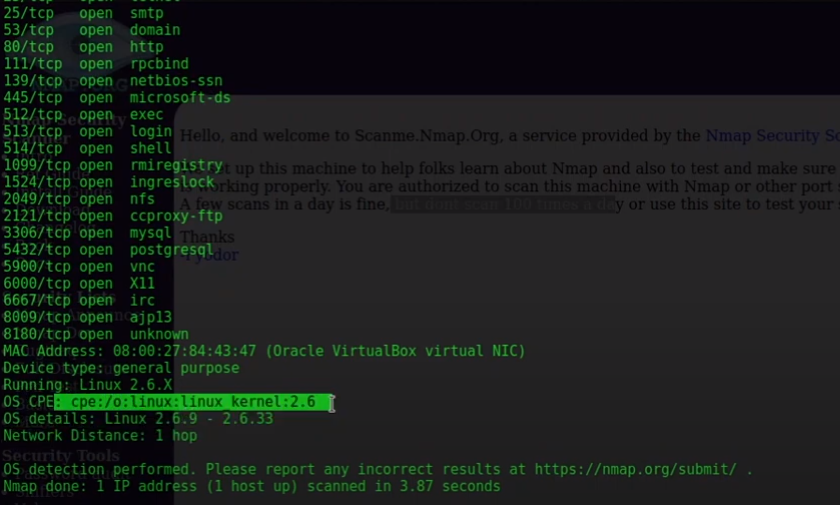


Namp to get details about services



To find operating system use capital O, it also gives details about MAC address.

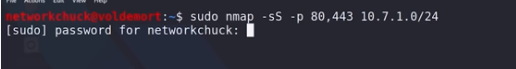




To scan entire network



Stealth scan for port 80,443 for rang of ip 10.7.1.0 to 24



To find out vulnerability use nmap script

