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

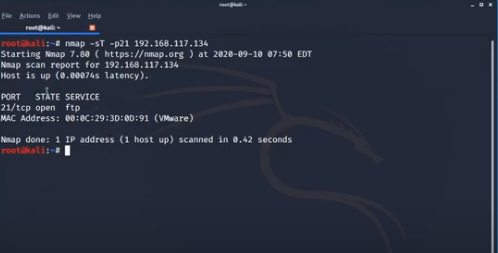
Nmap –sT –p21 192.168.117.134

-s – scan

-T – tcp scan

-p21 – given port number 21

Then ip address – target machine



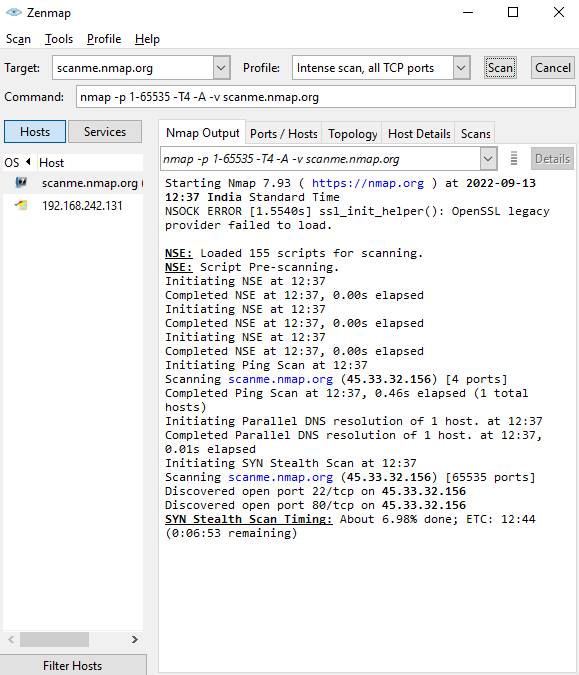
Output shows that port 21 is open and ftp service is running on that.

Now examine this in wireshark.

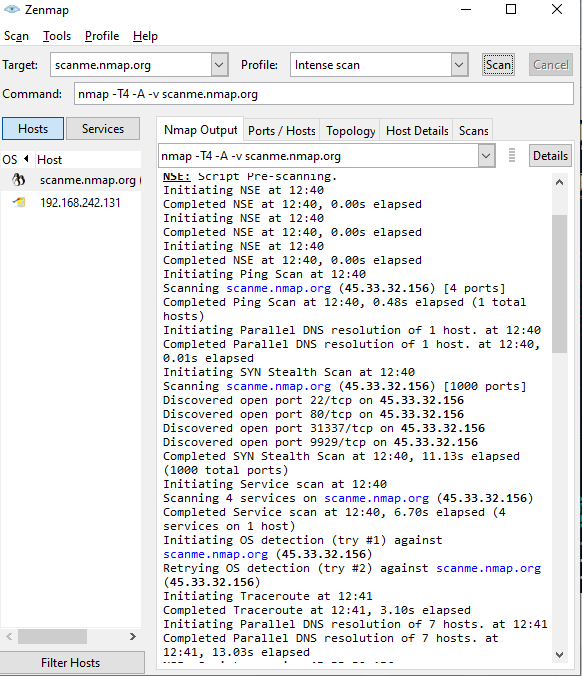
Open wireshark and then run this command again so we can see 3 way tcp handshake. So it is clear that someone is scanning my system. Some one is performing port scanning so we should block it.

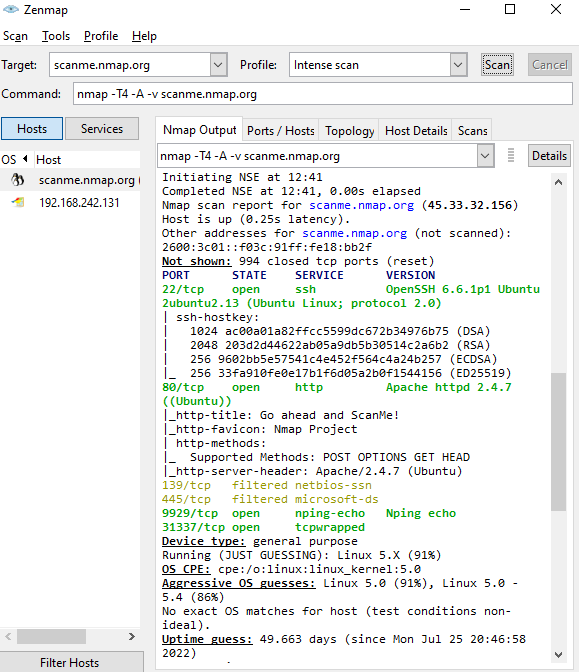
<https://www.youtube.com/watch?v=pytnN9YBTdU>

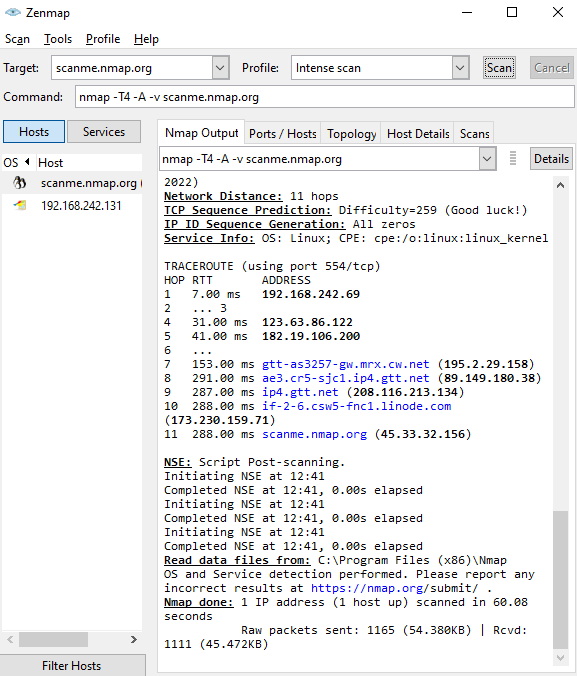
tcp scan on scanme.nmap.org



Intense scans







**How To Run a Ping Scan**

One of the most basic functions of Nmap is to identify active hosts on your network. Nmap does this by using a ping scan. This identifies all of the IP addresses that are currently online without sending any packets to these hosts.

To run a ping scan, run the following command:

# nmap -sp 192.100.1.1/24

This command then returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands (see below) to investigate them further.

**How To Run A Host Scan**

A more powerful way to scan your networks is to use Nmap to perform a host scan. Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address.

To run a host scan, use the following command:

# nmap -sp <target IP range>

This returns information on every host, their latency, their MAC address, and also any description associated with this address. This can be a powerful way of spotting suspicious hosts connected to your network.

If you see anything unusual in this list, you can then run a DNS query on a specific host, by using:

# namp -sL <IP address>

This returns a list of names associated with the scanned IP. This description provides information on what the IP is actually for.