**27-Aug-2024**

**Scanning:**

We do network scanning to find these 4 things:

1. Live Hosts on network
2. Open ports
3. Which applications/services are running on that server
4. Operating System

The main objectives are to identify weaknesses and entry points on the target network. We send probes while scanning to check the response of the site/server.

We cannot access internet with private IP because suppose we want to access google and our IP is 10.0.0.1, how does google know to which 10.0.0.1 I have to send response because millions of organizations are using this IP in their private network.

**Ports** are **Layer-4** phenomena. **Ports** are gateway to applications.

Uses 16 bits in TCP/UDP header (216 = 65535)

**Port Numbers 0-1023:**

* Well-known Ports / Fixed Ports
* Assigned to servers/web server

**Ports 1024-49151:**

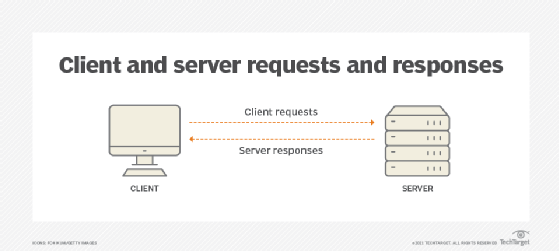
* Registered Ports

**Ports 49152-65535:**

* Random Ports / Ephemeral Ports (Temporary)

**Socket** is the combination of **IP + Port number**.

When we visit some site like cnn.com our machine gives us random port and a new socket will open in combination with our IP and Port. Then all the communication between our web browser and that site will happen within that socket. Similarly, at the same time when we open other site, our machine will open another new socket with our IP and now different random port number.



Explain the working here. Give 1 IP to client and 1 to server and then explain the working by assigning random port to client and fixed port to server.

To transfer something from your base machine into virtual machine:

* Make a shared folder. Put files into it which you want to share in virtual machine.
* Make your base machine run as an Apachee server.
* How to make your base machine work as an Apachee server:
* Run Powershell as an administrator > cd .. > cd .. > cd D: > cd .\Shared-folder > python -m http.server 80
* Now go to Virtual machine > Open browser > Type <http://150.1.7.100> > It will open that shared folder on web and will list the contents inside it > Download the content.

**Note:** Make 2nd Virtual Machine which will be Windows.

**28-Aug-2024**

Previous topic continued…..

**Determining Live Hosts using Nmap:**

We use different methods to determine how many hosts are live on network. Suppose org has banned ARP, so we have to know the other methods. We cannot rely on single command.

**ARP Ping Scan:** nmap -sn -PR 150.1.7.0/24

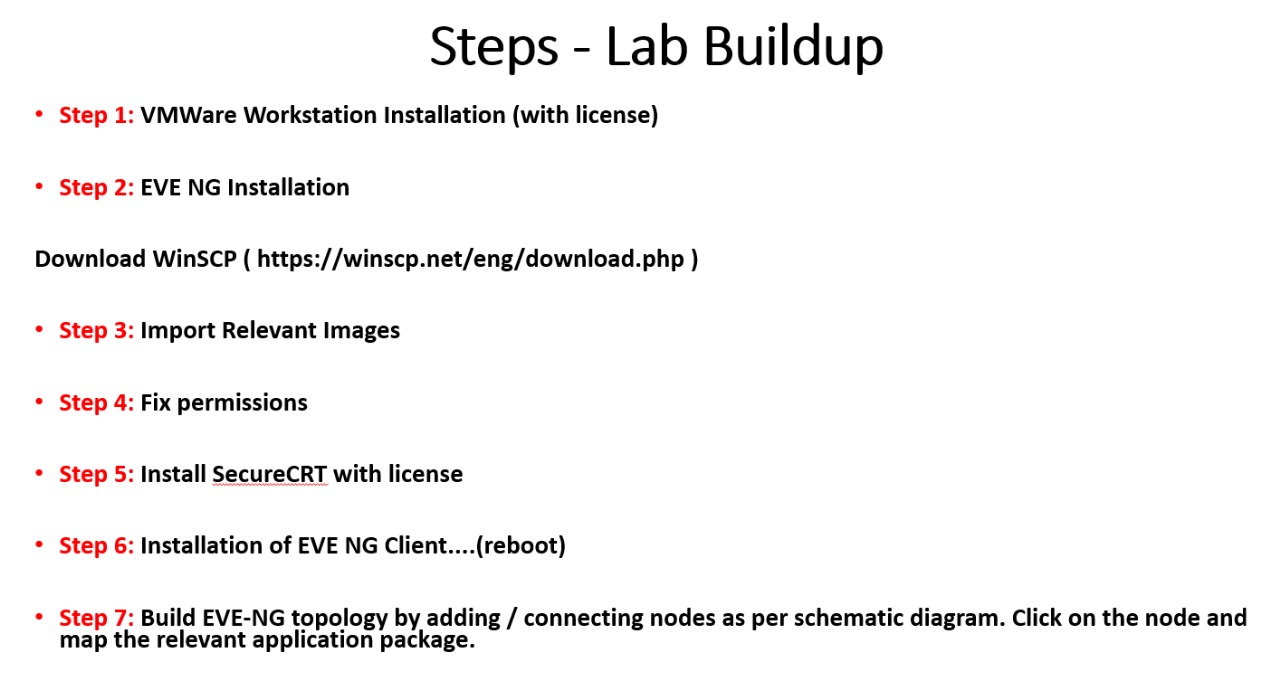
**UDP Ping Scan:** nmap -sn -PU 150.1.7.0/24

**ICMP Echo Ping Sweep:** nmap -sn -PE 150.1.7.0/24

**-sn** means **“**disable port scan**”** and **-PR**, **-PU**, **\_PE** are for **“**ARP, UDP and Ping sweep**”** respectively.

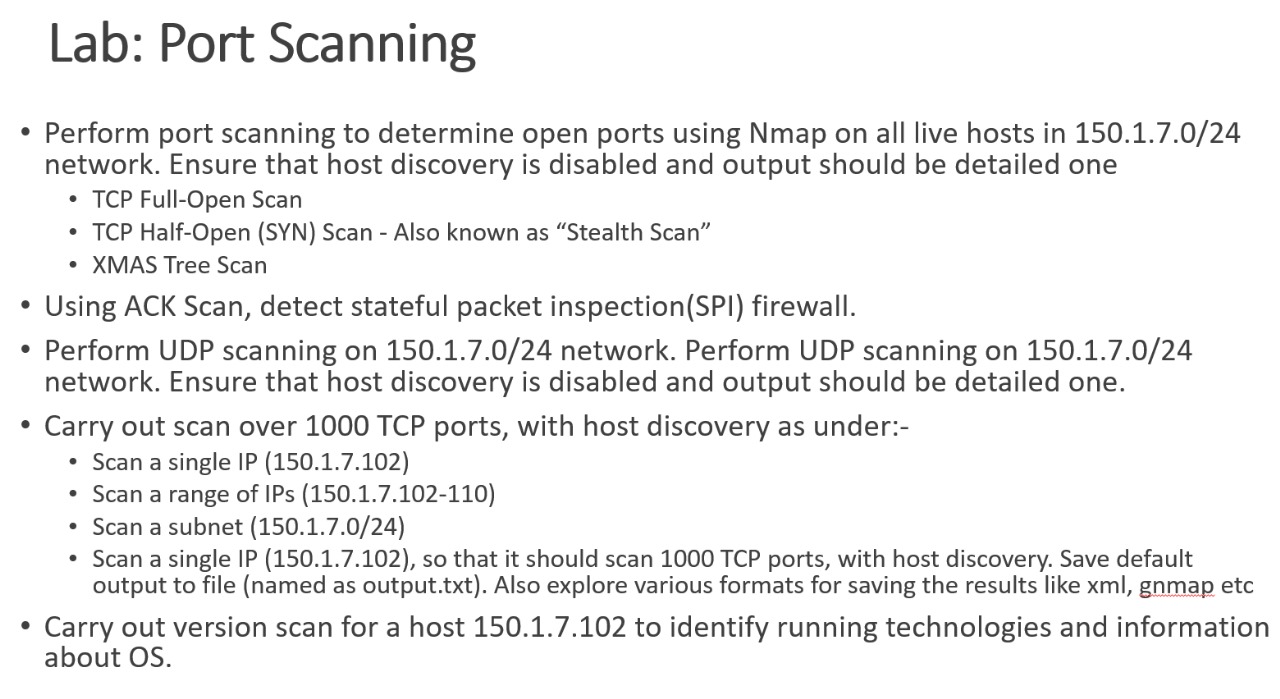
Another tool for scanning is **MITEC Network Scanner**. It is also a very powerful tool for scanning. When it gives you results, you can right click on them to explore further options.

Install 3rd VM of **Eve-ng**. Watch recorded video for installation instructions. Make sure your kali machine can ping it.



**29-Aug-2024**

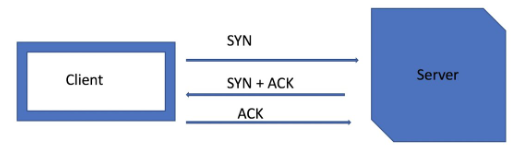
**Port Scanning:**



**nmap -sT -Pn 150.1.7.102**

-sT means TCP scan and -Pn means disable ping/host scan.

ip http server (If you put this command on router, it will start listening to port 80). You can then scan with nmap and it will show you port 80 open. **Nmap -sT 150.1.7.103** (It is the IP which we’ve given to router. It is TCP full scan which completes 3-way handshake.



**SYN** flag initiates connection.

**Nmap -sS -Pn 150.1.7.103** (This command is for TCP half open scan. It performs 3-way handshake but didn’t complete it.

**ACK Scan (Firewall Detection):**

* It is used to detect stateful packet inspection (SPI) firewalls in between.
* “ACK” scan will render:
  + A **reset** whether the port is open or closed. A reset will tell you that device can be reached with no SPI firewall in between.
  + If there is **no response**, a filtering device is between you and the destination.

**Nmap -sA -Pn 150.1.7.102 –reason**

Use this command to scan and check if you find unfiltered/reset text written. It will tell you there is no firewall between you and target.

**UDP Scanning:**

**nmap -sU -Pn 150.1.7.104**

UDP scanning takes time which can also be around 10-12 mins. We do UDP scan if you do not find anything on target like nothing then we know k UDP scan sy kch na kch mily ga hamy.

By default, **Nmap** scans 1000 mostly used Tcp ports and give you results which ports are open among them.

We can carry a single IP scan, range scan.

**nmap 150.1.7.102-110**

This will scan IP’s from 102 to 110 and give you results.

We can also scan a complete network subnet:

**nmap 150.1.7.0/24**

To save the scan output in text format in some file:

**nmap -oN myscan.txt 150.1.7.102**

If you want to save in xml format:

**nmap -oX myscan.xml 150.1.7.102**

If you want to save in all formats:

**nmap -oA combined 150.1.7.102** (It will save in all formats with the filename combined)

**To determine OS using Nmap:**

**nmap -sV 150.1.7.102** (-sV is for version. It will tell you open ports, application and their version running on specific port)

**nmap -sV -A -T4 150.1.7.102**

-A means aggressive scan and -T4 means aggressive speed scan. When you run this command in Linux only mistake it makes is it often tells you wrong information about operating system just operating system. Similarly, when you run this on windows based GUI-tool **Zenmap** it will give you more precise info about operating system. Even though it is also a nmap just with GUI.

**30-Aug-2024**

**To scan specific port scan:**

**nmap -p 80 150.1.7.102**

**To scan specific range of ports:**

**nmap -p 1-500 150.1.7.102**

**To scan 100 most common ports:**

**nmap -F 150.1.7.102**

-F means fast scan of common 100 ports.

**To scan all ports:**

**nmap -p 1-65535 150.1.7.102 OR nmap -p- 150.1.7.102**

It will take time to scan all ports.

**Linux command to find which technologies target using:**

**whatweb 150.1.7.102**

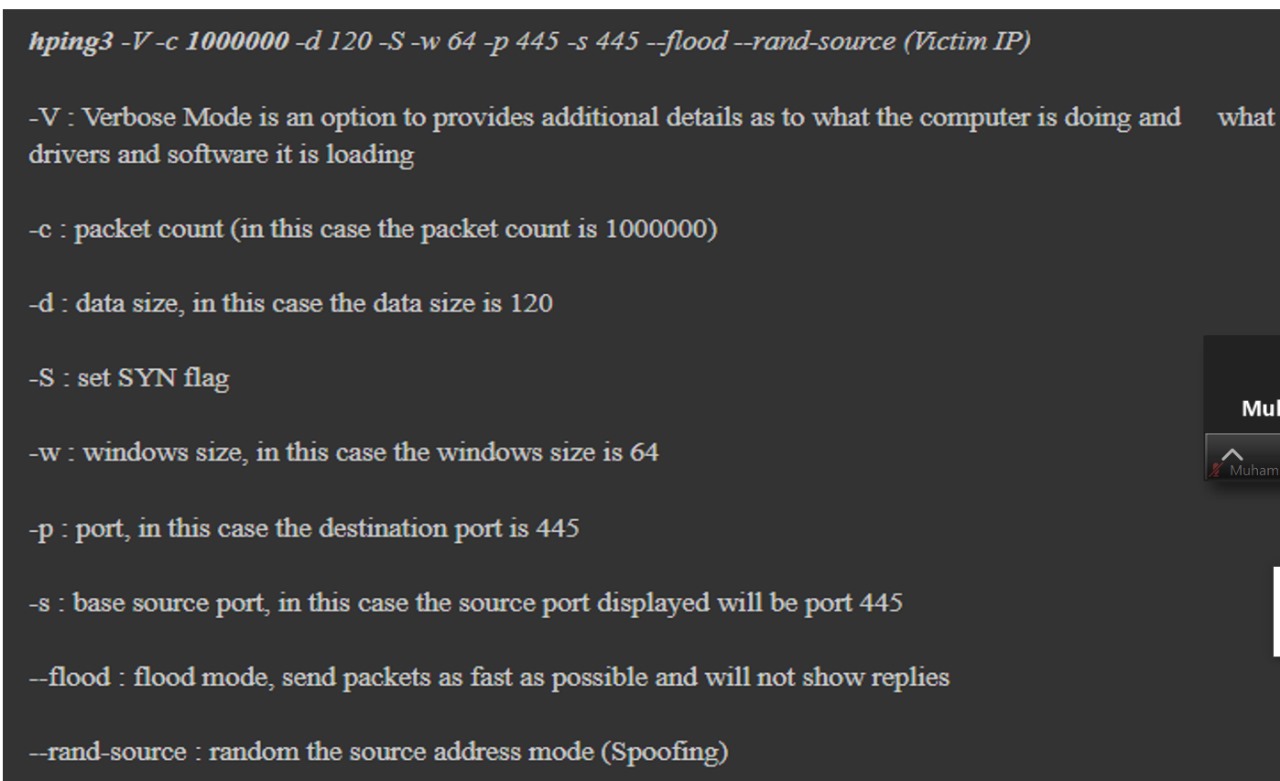
**Host discovery command in Linux:**

**fping 150.1.7.102**

**fping -g 150.1.7.102 150.1.7.110 > fpingfile.txt**

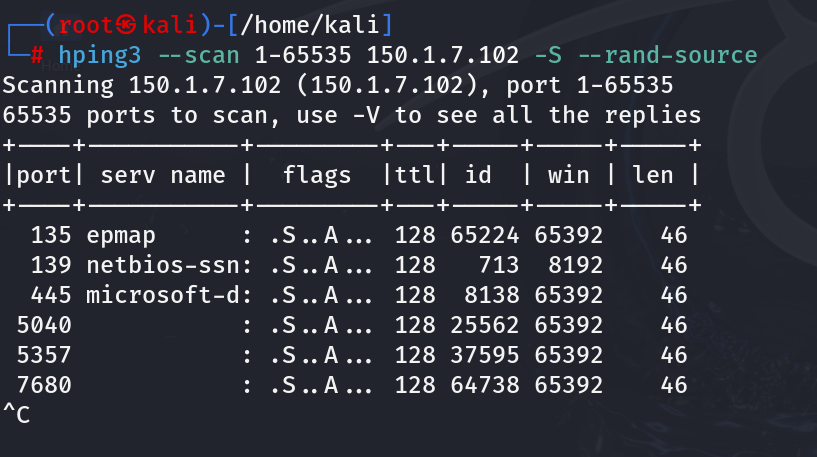
It will scan range of IP’s and will save the output in the file name fping.txt

We can also use **hping3** command to scan IP.



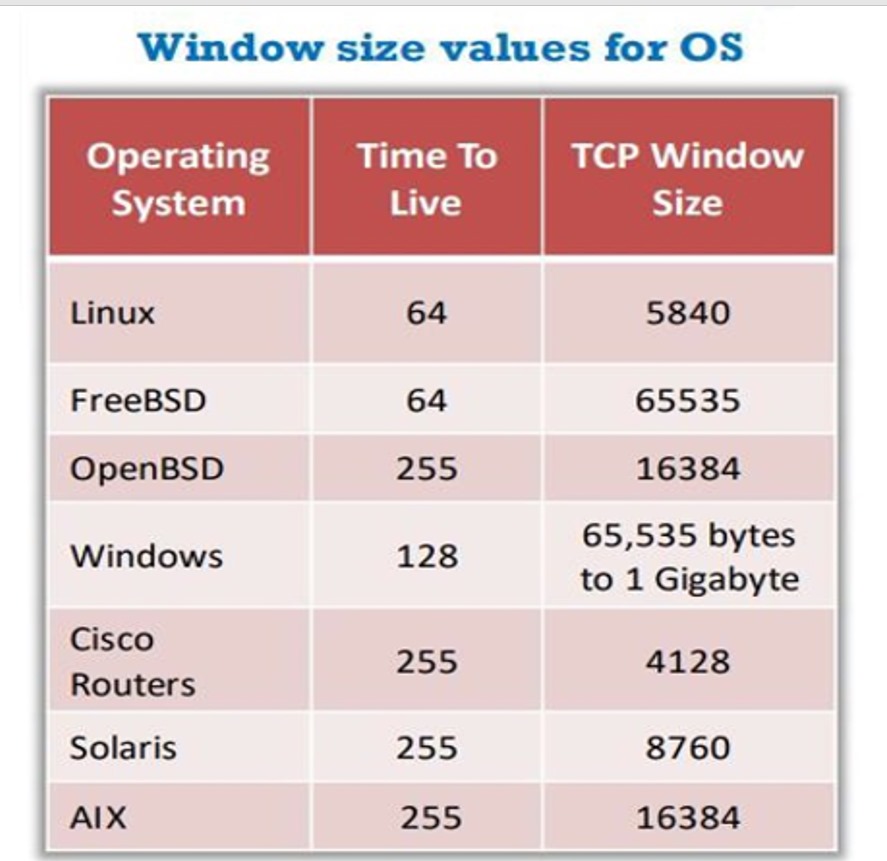
**hping3 –-scan 1-65535 150.1.7.102 -S --rand-source**

It will give us results like this:



We can know the type of Operating system via **ttl (**Time To Live)value. **128 ttl** value is for Windows OS.

Some Default **TTL** values:



**To scan the target without getting it detected by IPS/IDS, use the following command:**

**nmap -f 150.1.7.102**

This will send packets of 8 bytes and they will deceive firewall and firewall will let them pass. You can check packet size for verification using wireshark. Remember to select eth1 adapter in wireshark.

**nmap -D RND: 150.1.7.102**

This will scan the target with **decoy IP’s** like random IP’s so the target monitoring system won’t know the source IP.

You can also put IP’s of your own choice like you can put IP of someone else so target may think it is coming from that source. To do this, use the following command:

**nmap -D fake ip’s target ip**

e.g: nmap -D 150.1.7.210,150.1.7.215,150.1.7.220 **150.1.7.102**

We can also scan the target without revealing our IP. This is known as **Zombie Scan**. This technique leverages a third-party host, known as **“**zombie**”** which is used to send packets to the target.

**Advantages:**

**Stealth:** No packets are directly sent to target, making it difficult to detect.

**Bypass Firewall:** Often bypasses traditional firewall rules.

**Disadvantages:**

* Slow
* Unethical

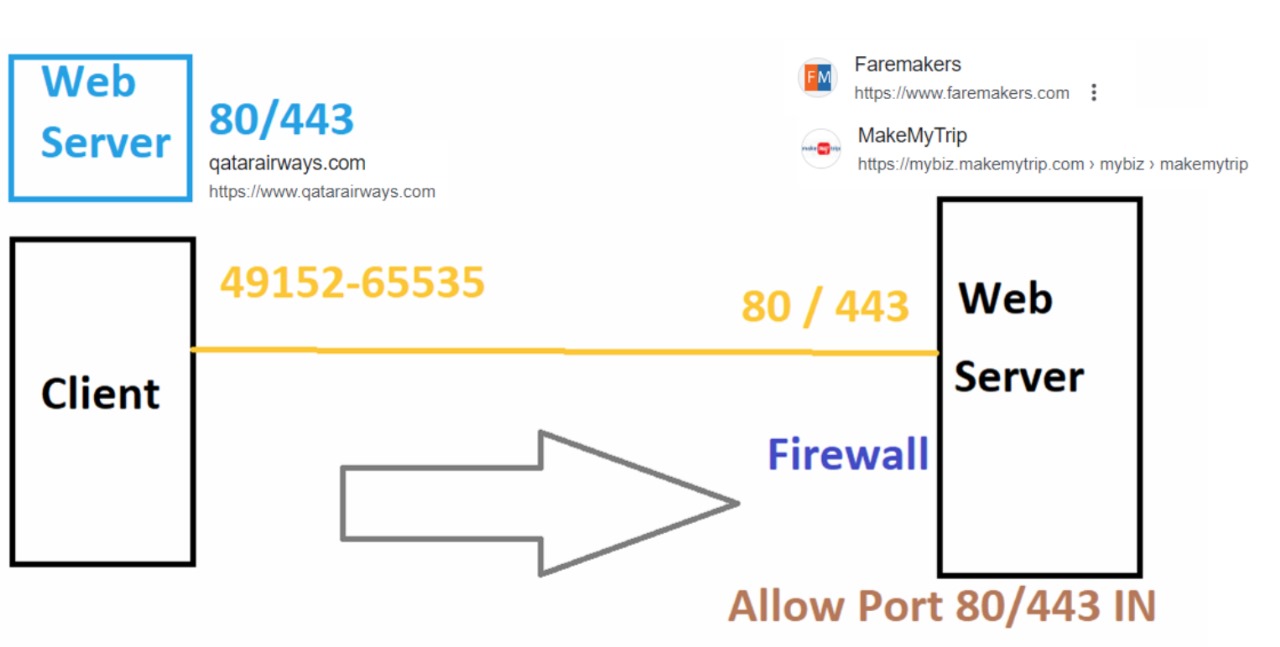
**Syntax of Command:**

**nmap -sI source ip destination ip**

e.g: nmap -sI 150.1.7.100 **150.1.7.102**

It will scan the target and show the source ip 150.1.7.100. You can verify this in wireshark.

We can also perform source port manipulation to avoid IDS/IPS detection. Understand the picture:



**nmap –source-port 80 150.1.7.102 OR nmap -g 80 150.1.7.102**

Now it will scan using our port 80. Firewalls do not block port 80 because web servers needs to communicate with each other and their default port is 80, 443. So if we manipulate our port for scanning, firewall won’t block it. This is how we deceive firewalls.