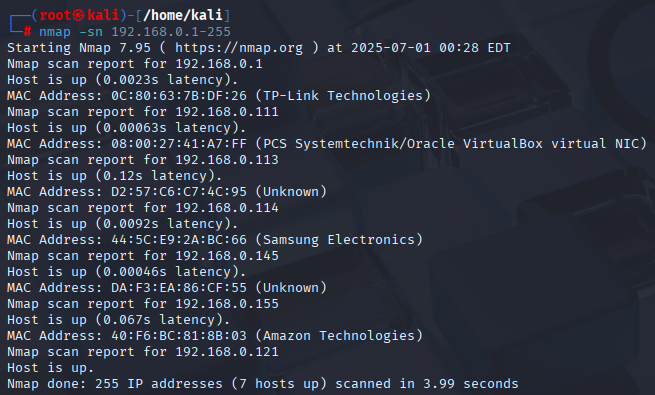
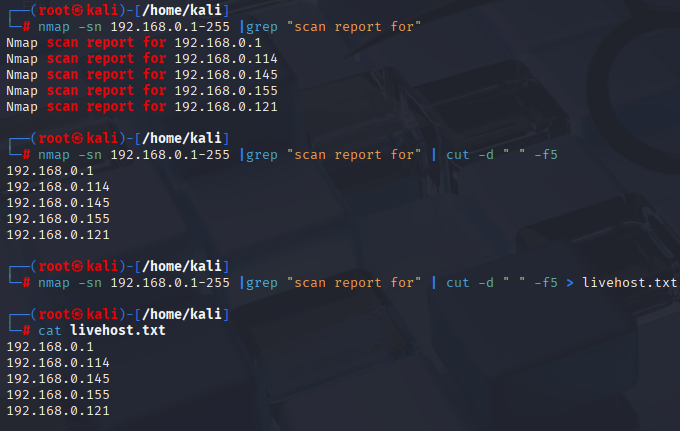
**Host Discovery Scan :** A host discovery scan, also known as a "ping scan," is a technique used to identify active hosts on a network. It involves sending network packets to a range of IP addresses and analyzing the responses to determine which devices are online and reachable. This is a crucial first step in network reconnaissance and security testing.

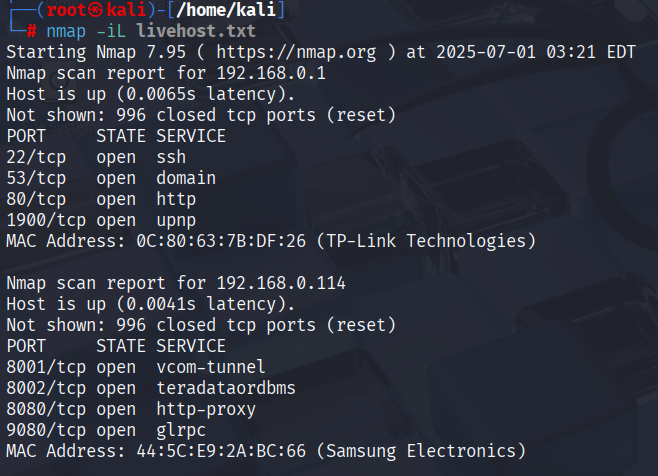


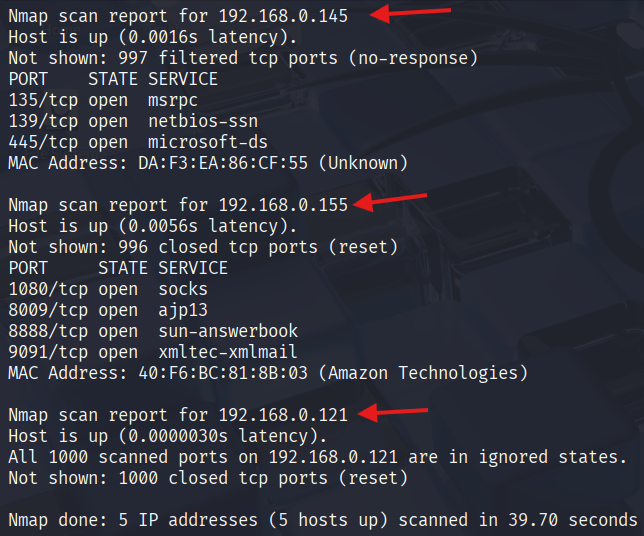
I found seven live hosts when I scanned my local network in the 192.168.0.0/24 IP address range.

**Alive Systems - Text File:** I saved all live hosts data to a particular text file called livehost.txt. In this process i removed the description for IP address using grep and cut and saved only the IP values to a text file As we can see data in the file using cat command as shown in figure.

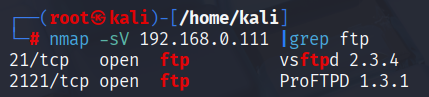


**Port Scan:** Here we are targeting whole text file of IP address to run the scan, in our case it is livehost.txt. Command : nmap -iL livehost.txt, Where small “i” is input captial “L” is list.

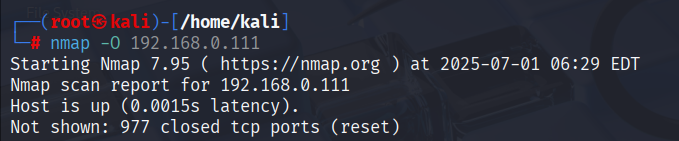


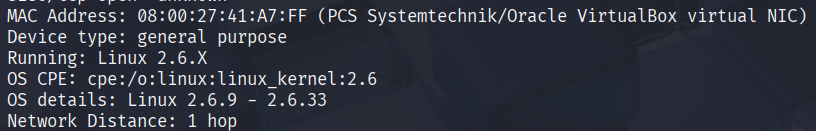


**Version Detection :** I used version + grep command to simplify the results and know the version of FTP. Similarly we can do it for any services. Command sV where small “s” is for scanning and capital “V” is for version.



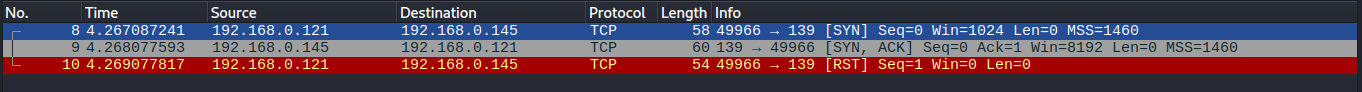
**OS Detection :** We can detect OS only if the services make the information accessible as they communicate with each other internally or while we are probing the particular port with packet transfer and calculate the time taken calculate by TTL time to live. Command “O” to detect the OS.

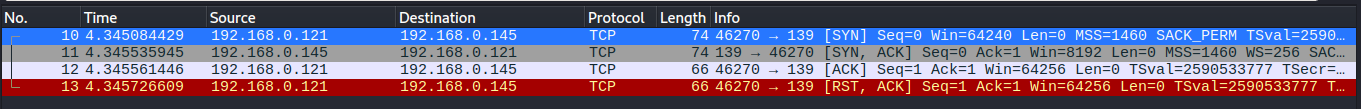




**Open| Closed| Filtered :**

An open port is a network port that is actively listening for incoming connections from other network devices.





A closed port is one that is accessible (meaning the host is reachable), but no application is actively listening on it.

Screenshot 2025-07-01 181750

A filtered port is a network port that a firewall or other security device is actively blocking or filtering traffic to, preventing it from being identified as either open or closed by port scanning tools.

Screenshot 2025-07-01 182055