PMIT

Ethical Hacking

SCANNING NETWORK

Class no 1

Black Box 🡪 Information Gathering 🡪 Network Scanning

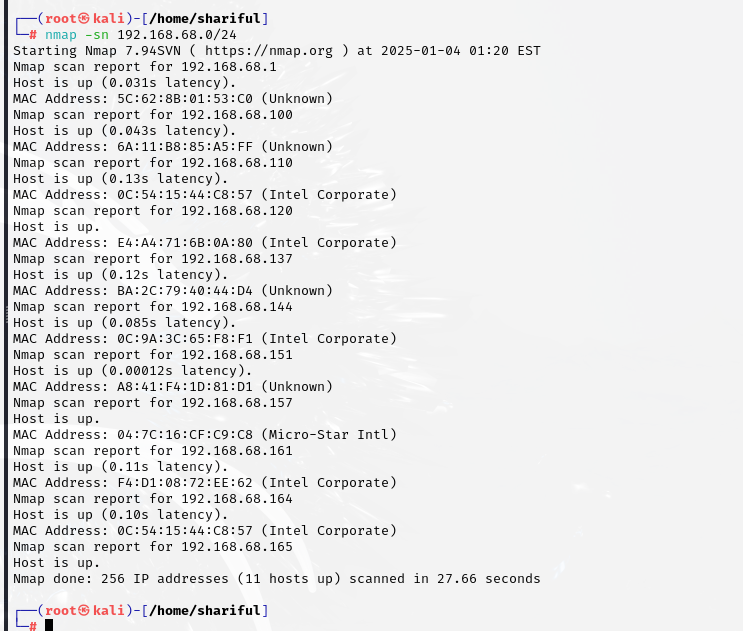
White Box 🡪 Network Scanning

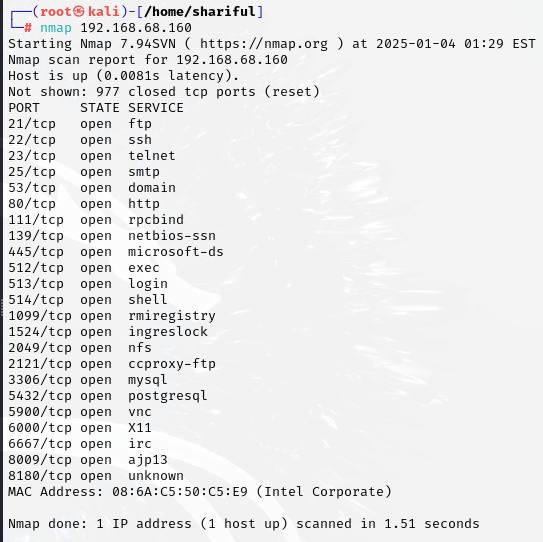
Probe Packet mean packet return without data, only structure will be send.

How to use nmap properly link: <https://nmap.org/docs.html>

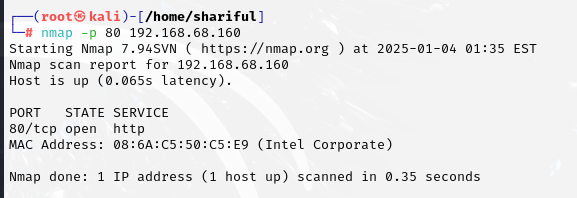
See running all port:

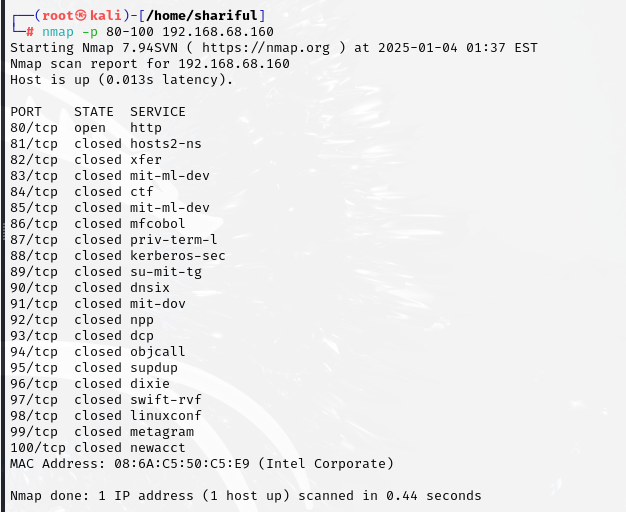
nmap -sn 192.168.68.0/24

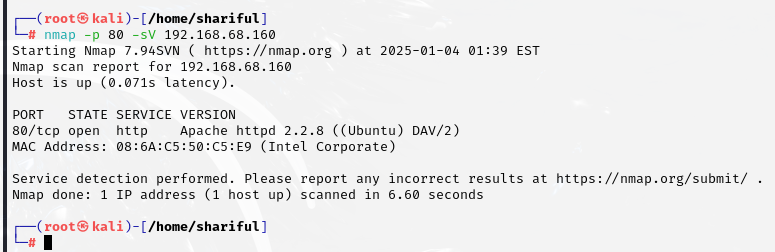




Scan specific port :



Scan a range of port: 

Check service version: 

Check operating system: 

If I send too much packet then fireware can detect and block the ip..then it’s need to send slowly.range is T1 to T6(T4 is by default,T1 is most slow and T6 is max speed): 