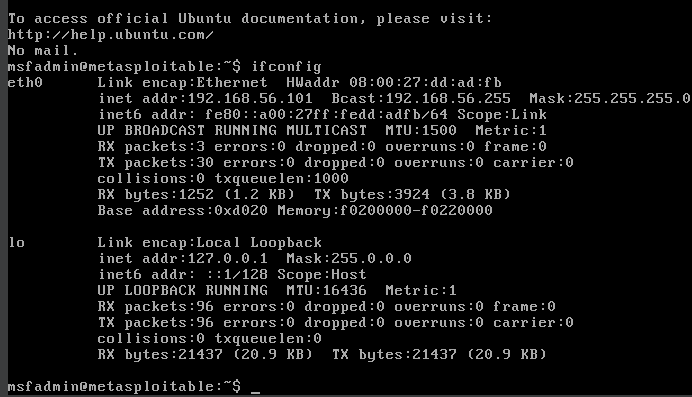
Home work – Lab1

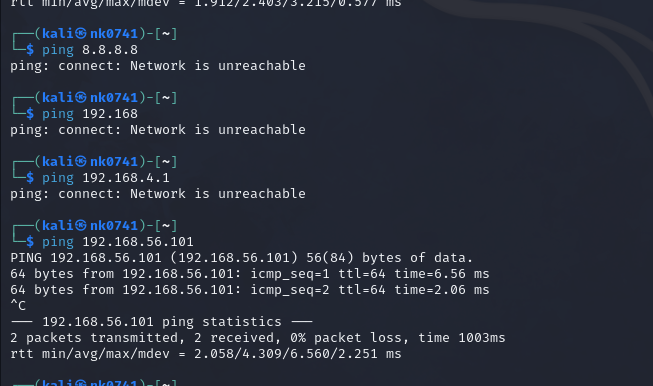
Installed kali:



Installed Metasploitable 2:



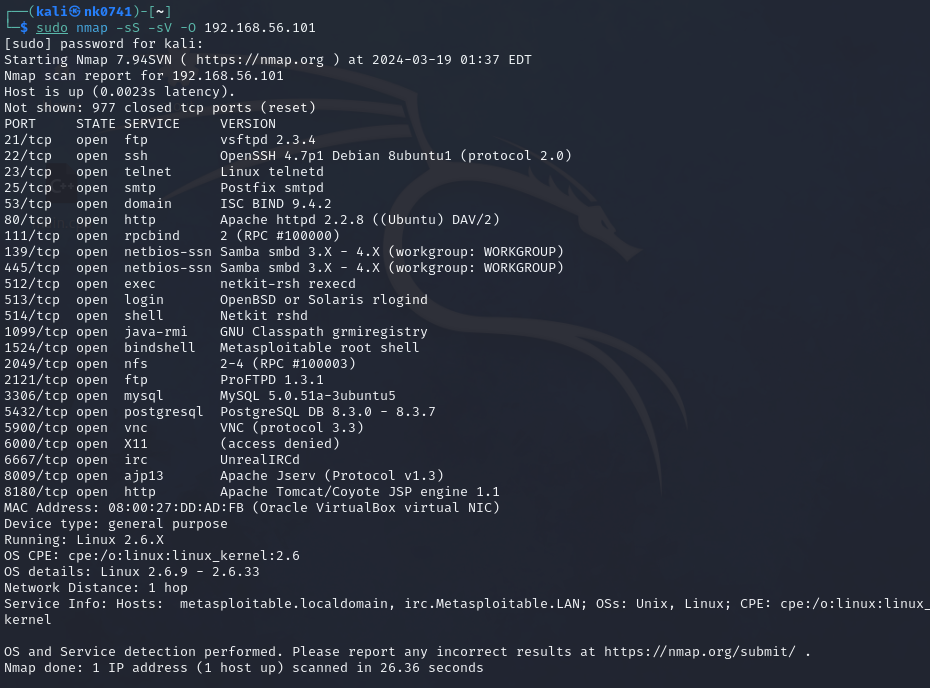
From the above screenshot, we can see I’m able to communicate to metasploitable through kali.



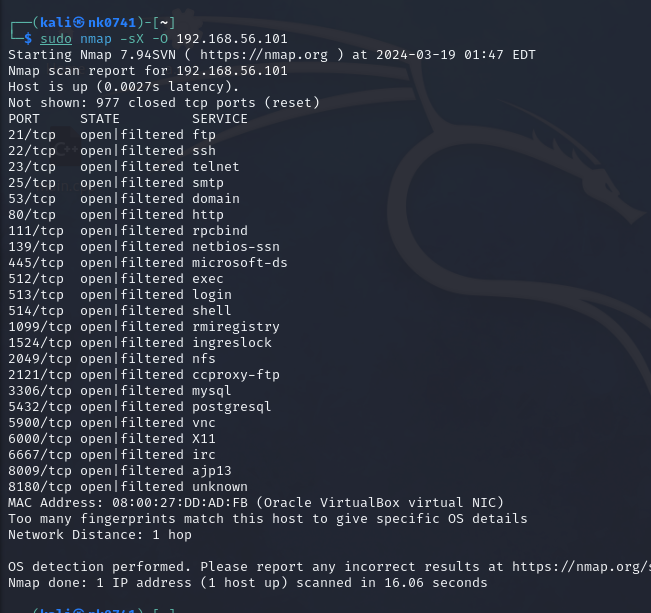
From the above screenshot we can confirm both the systems are connected and isolated from external.

I have run nmap –sS –sV -0 command on metasploitable ip address found out 23 ports are open on metasploitable. Along with that we also get information regarding the NIC card used by the machine and it’s mac address.

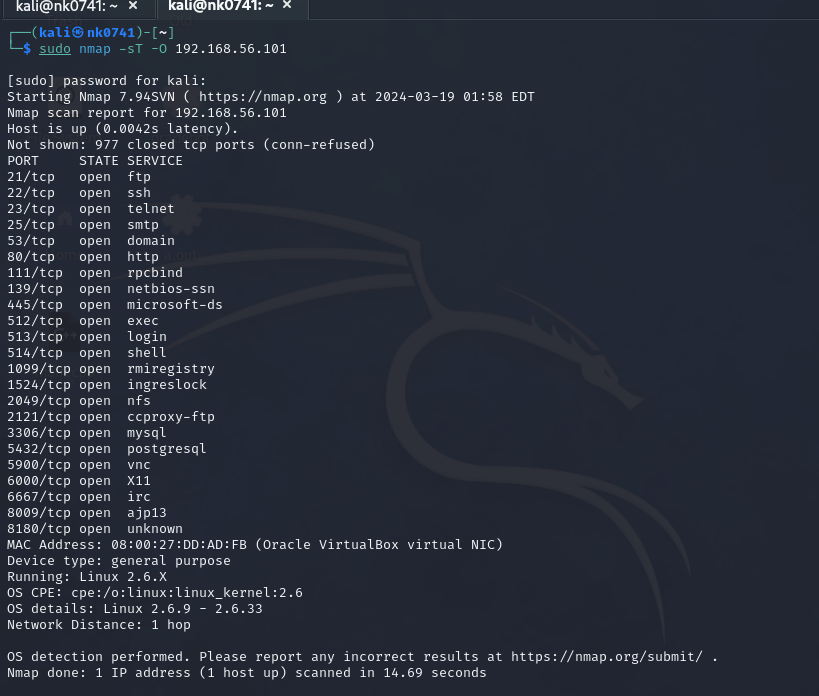
We can use that information to find any known vulnerabilities on the NIC card. We can also see the connection is 1 hop because they are connected based on point-to-point.



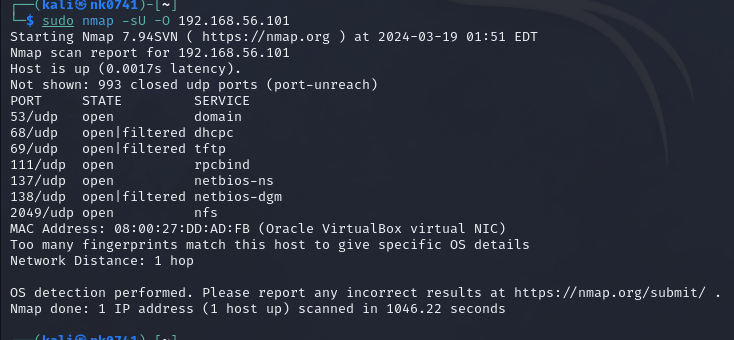
Using Xmas scan:



Using –sT TCP scans:



UDP Scans:



From the above all scans the udp scan to took long time. The Ports 68,69,137 and 138 are only available for udp connection.

So , In total we found 27 ports which open on metaspoiltable.

We can use “-scan-delay “ or “-sF” for doing scans quietly or slowly, So, that the scans are not detected.

For a normal public domain, In general the number of pings from a single Ip may be limited to 20-25 per second. So, the Server or Network administrator might block our ip address for certain amount of time. So, to avoid that case we the above mentioned tags to scan the network more passively.

If nmap command is not available to us. We can use necat or telnet and try to connect each open to check whether they are open to connection or not. We can also use wireshark or tcpdump to scan the network traffic and analyse the traffic to know which ports are open or in use.

Here I tried using Telnet to check if I’m able to connect to some ports are not.

Using Telnet command:

