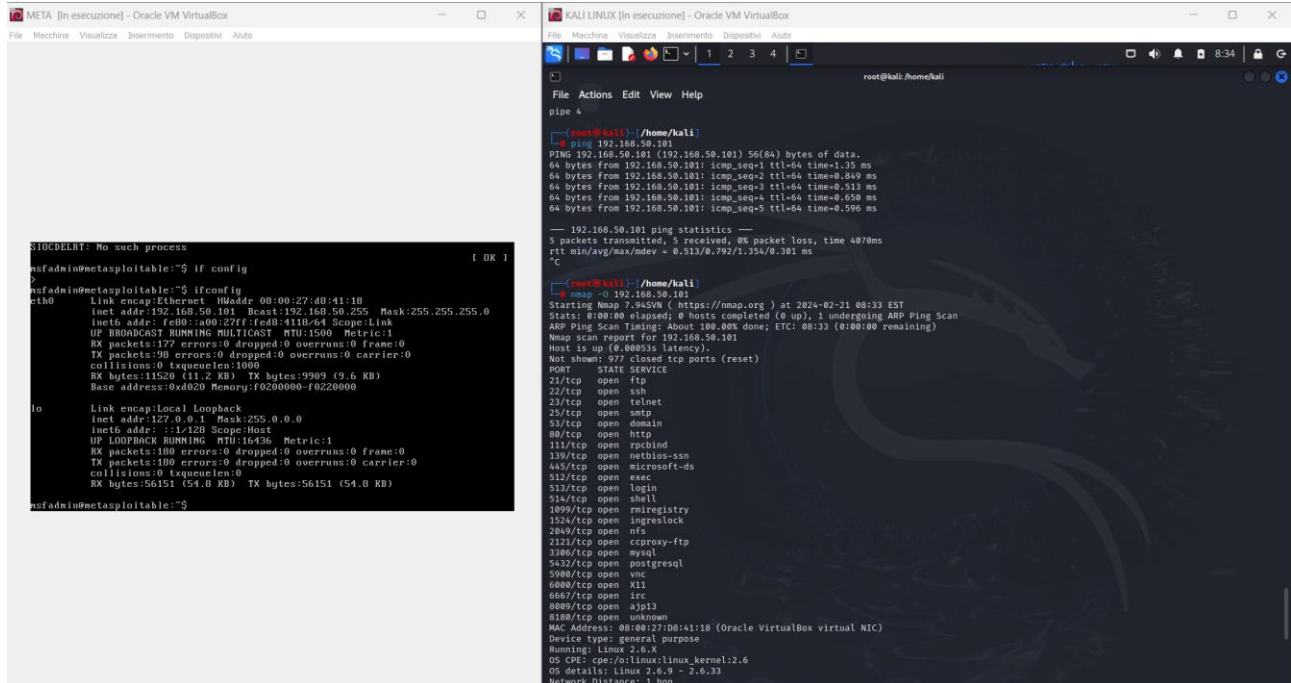


“RELAZIONE S5L3”

- ATTACCO <<"nmap">>

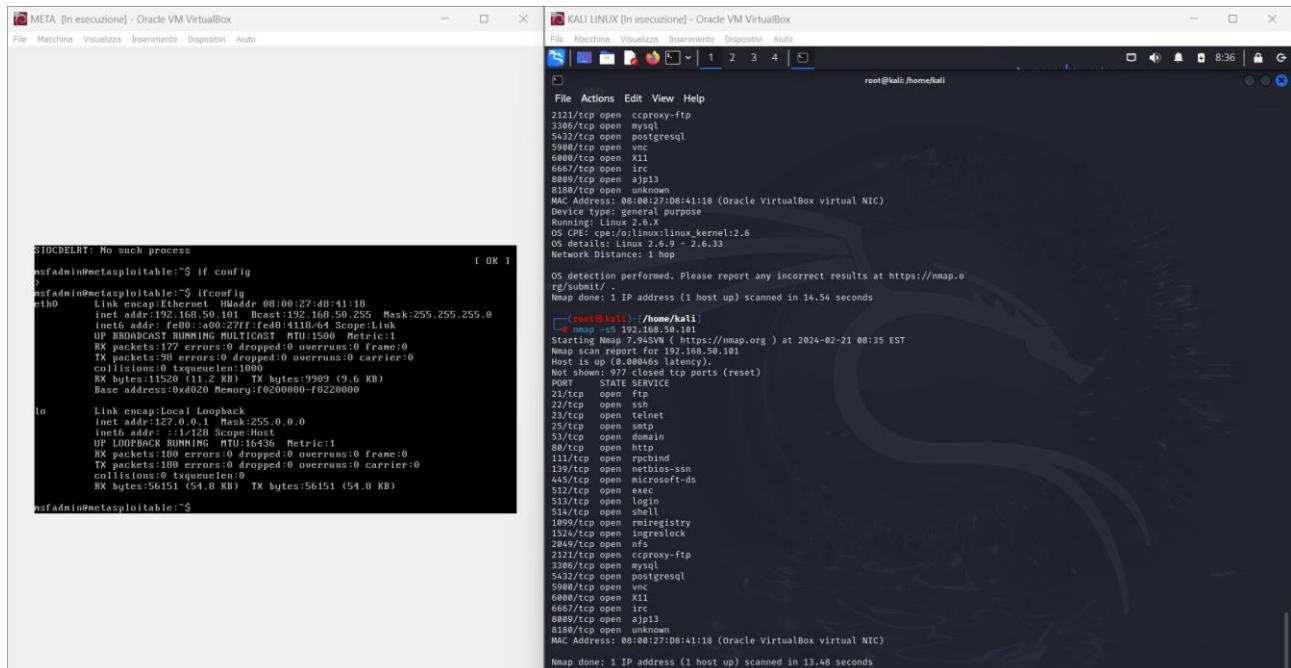
Da questo possiamo evincere le porte aperte inoltre possiamo notare il kernel : 2.6 di linux. Avendo queste info possiamo capire come effettuare il nostro attacco.



```
root@kali: /home/kali
ping 4
root@kali: /home/kali
ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data:
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.33 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.849 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.513 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.658 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=0.596 ms

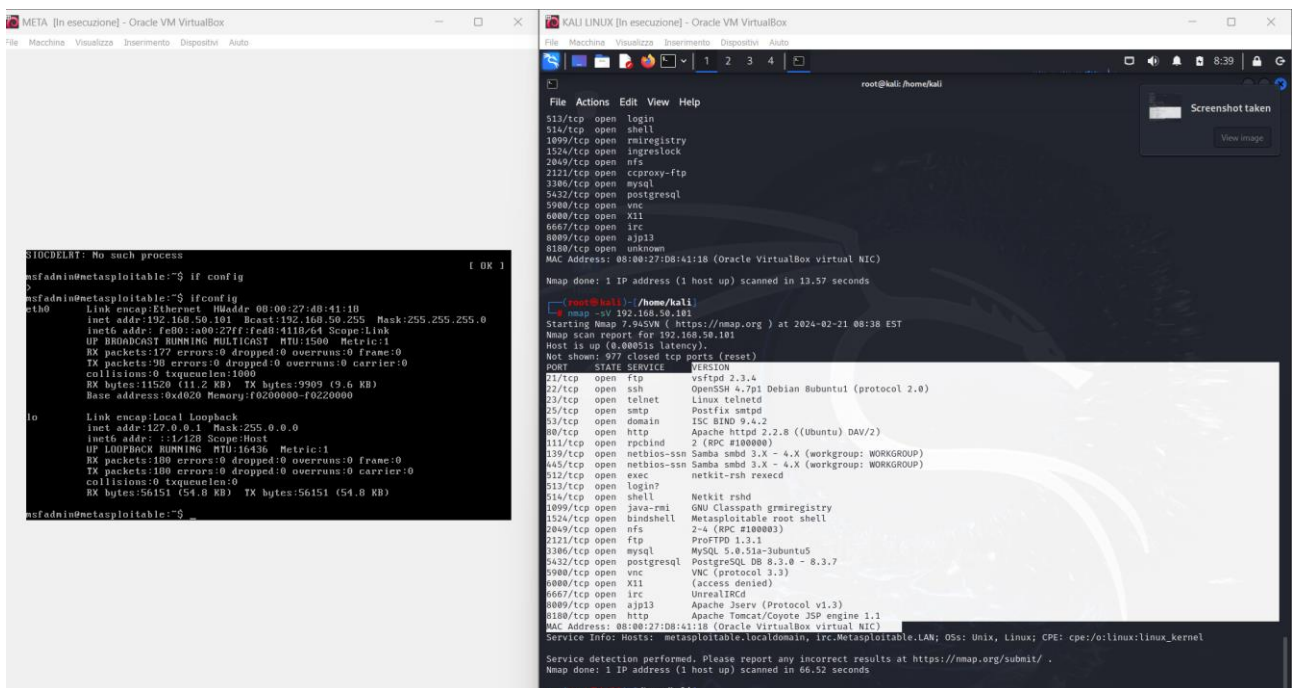
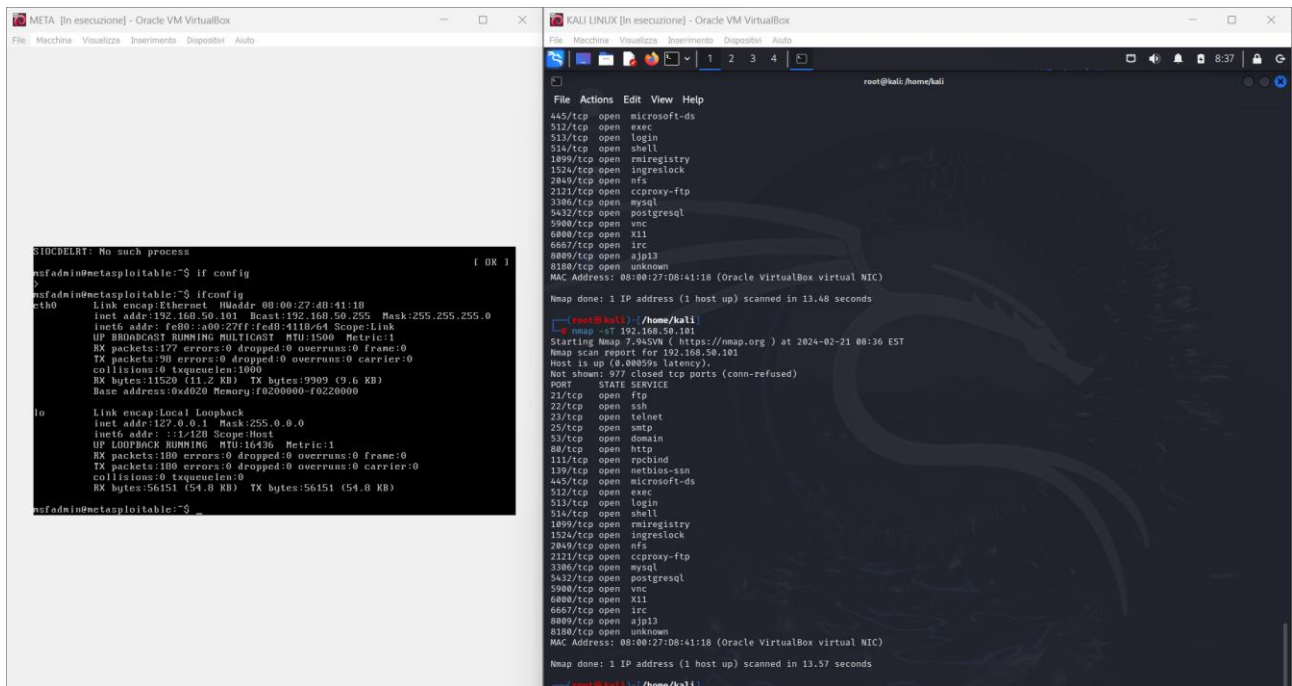
--- 192.168.50.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.513/0.792/1.354/0.301 ms
^C
root@kali: /home/kali
nmap -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 08:33 EST
State: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 00:33 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0085s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2849/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:08:41:18 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

- Attraverso il comando <<nmap -sS IP :”target”>> andiamo a eseguire la syn che mi darà risultati solo perimetrali



```
root@kali: /home/kali
nmap -sS 192.168.50.101
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 14.54 seconds
root@kali: /home/kali
nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 08:35 EST
Nmap scan report for 192.168.50.101
Host is up (0.0086s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2849/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:08:41:18 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

- CON IL COMANDO <<nmap -sT indirizzo ip >> andiamo a eseguire un controllo bruto sull'indirizzo ip



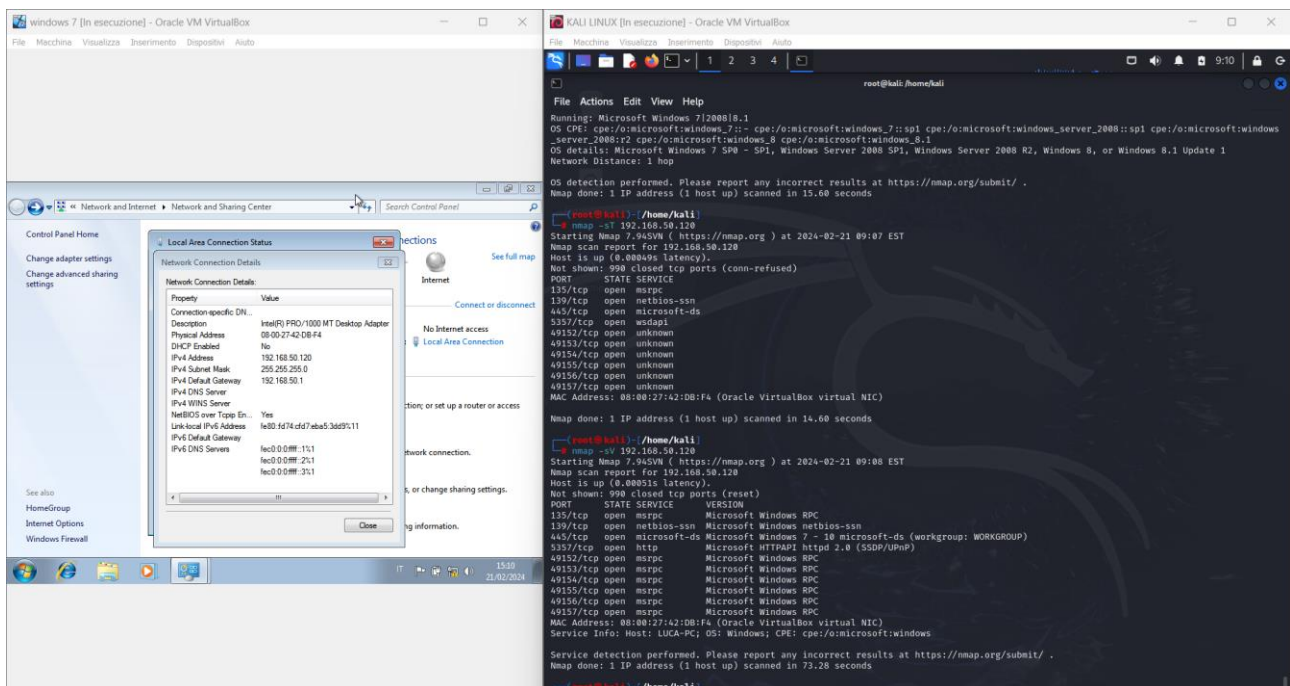
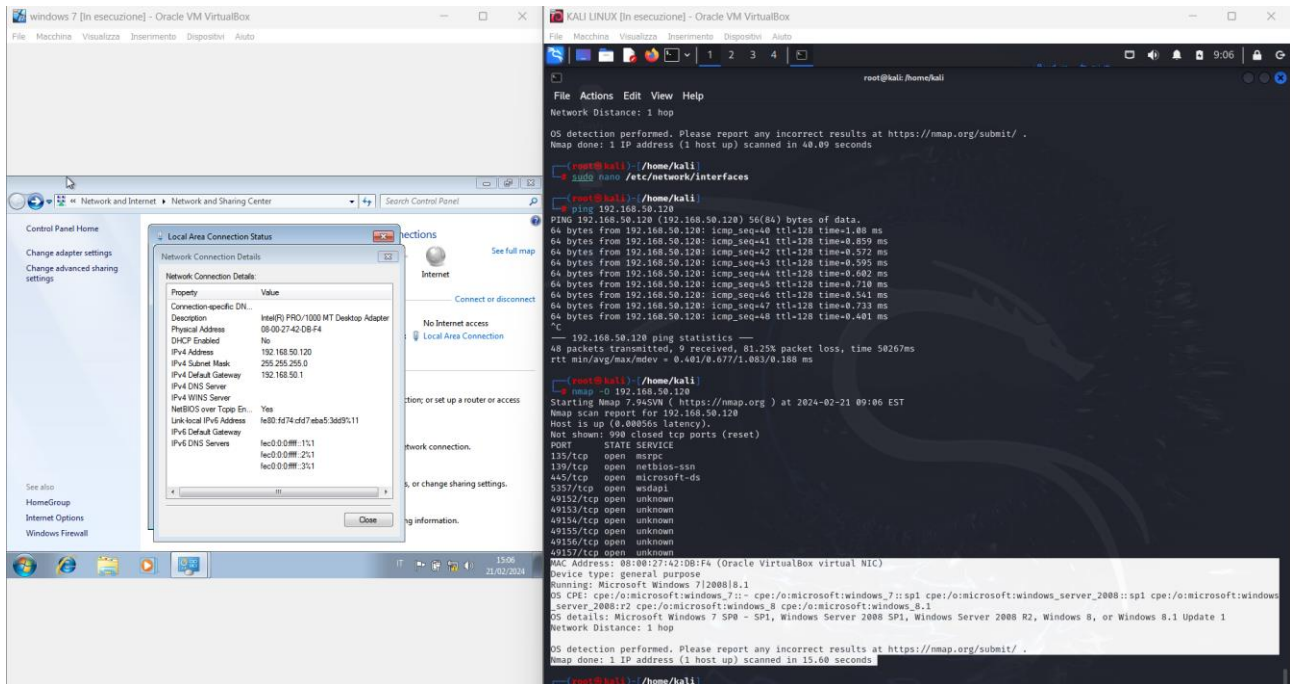
Inoltre con il comando <<nmap -sV indirizzo ip >> andiamo a esaminare in modo più approfondito infatti dai risultati possiamo evincere molte più info come la versione, per eseguire l'attacco

“Windows”

Ip : 192.168.50.120

Sistema operativo : windows 7

Servizi in ascolto : netbios-ssn; msrrpc; microsoft-ds; wsdapi;



Si consiglia di ottimizzare le regole firewall