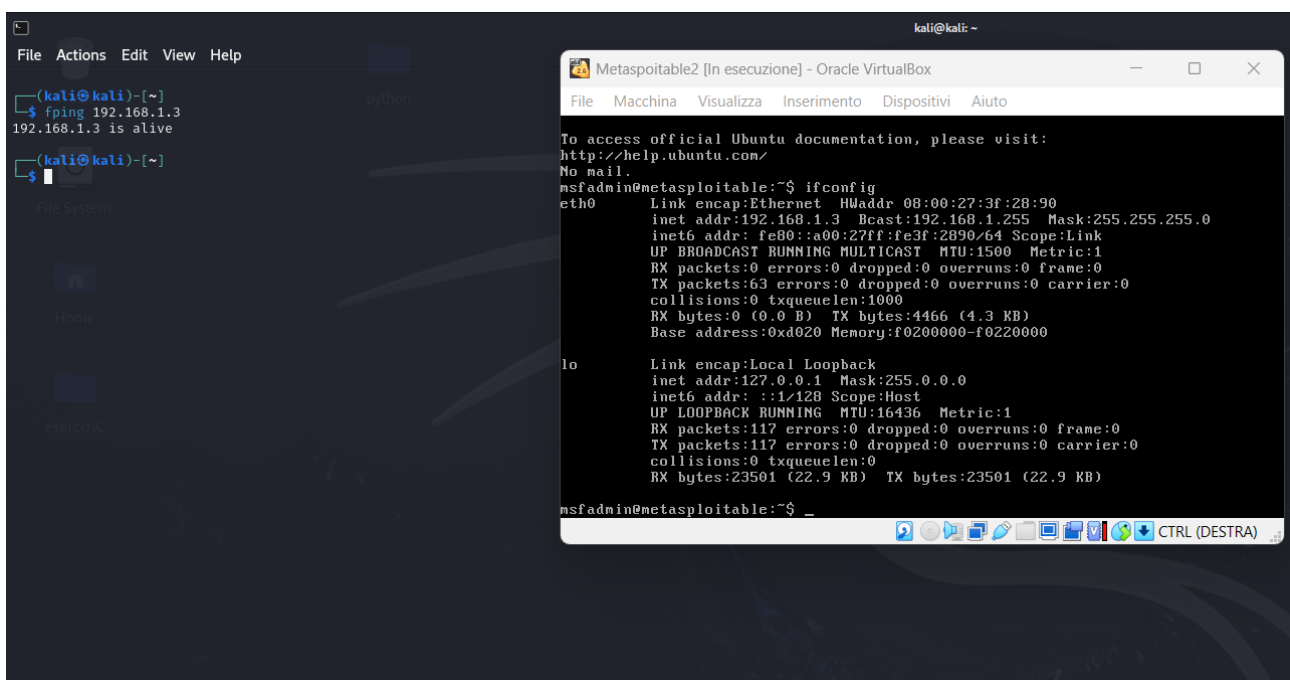


LABORATORIO 08/01/2024 S5-L2

La consegna di oggi ci chiedeva di effettuare delle scansioni con il tool NMap verso le macchine Metasploitable e Windows10.

Iniziamo quindi avviando le macchine Kali, Metasploitable e Windows configurandole in rete interna ed assegnando a tutte e tre la stessa rete.

Procediamo con il ping da Kali a Metasploitable che ci restituisce in output lo stato attivo di quest' ultima.

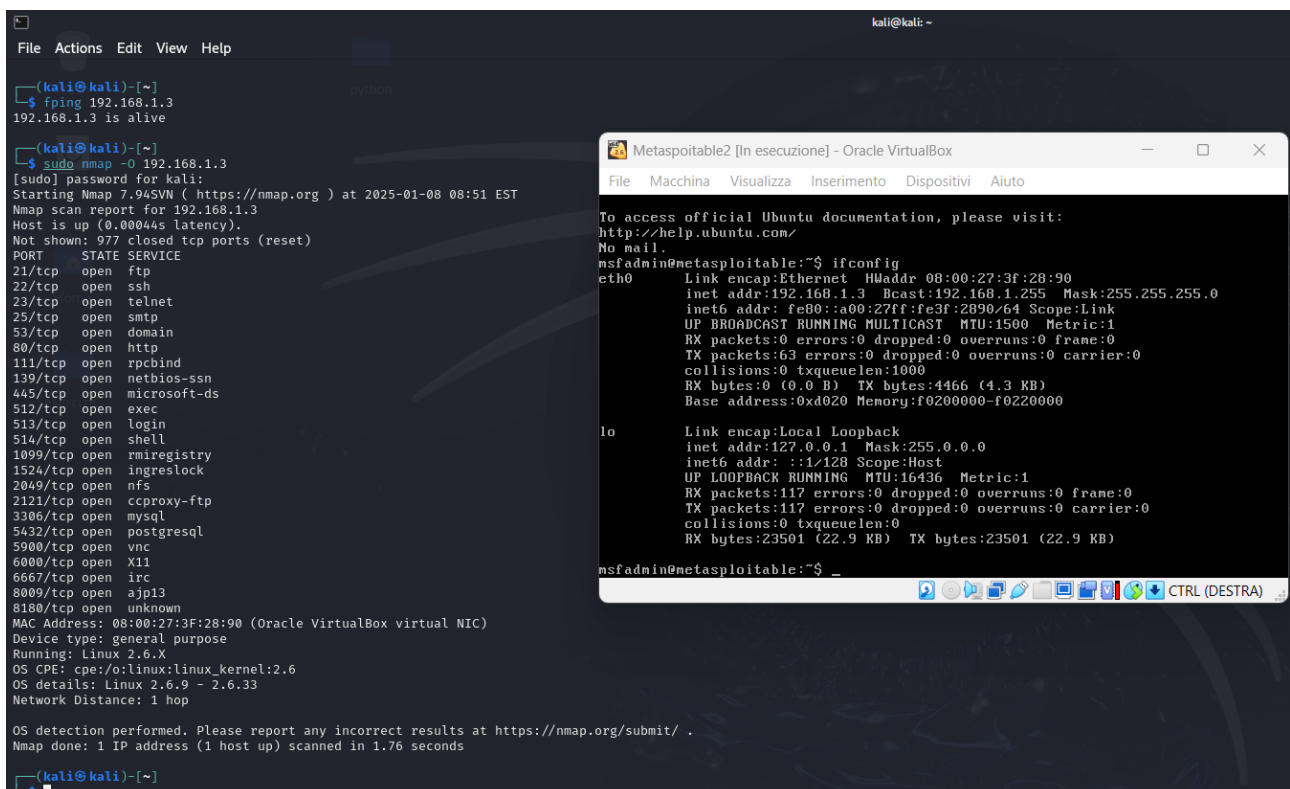


The image shows a Kali Linux terminal window on the left and a Metasploitable2 virtual machine window on the right. The terminal window displays the output of a ping command from Kali to 192.168.1.3, which is Metasploitable2. The output shows that the host is alive. The Metasploitable2 window shows the output of the 'ifconfig' command, displaying network configuration details for the 'eth0' and 'lo' interfaces.

```
(kali@kali)-[~]  
$ ping 192.168.1.3  
192.168.1.3 is alive  
$  
(kali@kali)-[~]  
$  
File System  
Home  
Desktop  
Applications
```

```
Metasploitable2 [In esecuzione] - Oracle VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:3f:28:90  
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe3f:2890/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:4466 (4.3 KB)  
          Base address:0xd020  Memory:f0200000-f0220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:23501 (22.9 KB)  TX bytes:23501 (22.9 KB)  
  
msfadmin@metasploitable:~$ _  
CTRL (DESTRA)
```

Possiamo quindi procedere con la scansione OS Fingerprint con il comando `sudo nmap -O` che ci restituirà, tra le altre cose, anche il tipo di Sistema Operativo che utilizziamo oltre al numero di porte chiuse(997).



The image shows two overlapping windows from a Kali Linux environment. The background window is a terminal with the following output:

```
(kali@kali)-[~]  
$ ping 192.168.1.3  
192.168.1.3 is alive  
  
(kali@kali)-[~]  
$ sudo nmap -O 192.168.1.3  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 08:51 EST  
Nmap scan report for 192.168.1.3  
Host is up (0.00044s 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  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-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: 08:00:27:3F:28:90 (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  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds  
  
(kali@kali)-[~]  
$
```

The foreground window is titled "Metasploitable2 [In esecuzione] - Oracle VirtualBox" and shows the output of the `ifconfig` command:

```
msfadmin@metasploitable:~$ ifconfig  
eth0: Link encap:Ethernet HWaddr 08:00:27:3f:28:90  
      inet addr:192.168.1.3 Bcast:192.168.1.255 Mask:255.255.255.0  
      inet6 addr: fe80::a00:27ff:fe3f:2890/64 Scope:Link  
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:63 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:0 (0.0 B)  TX bytes:4466 (4.3 KB)  
      Base address:0xd020 Memory:f0200000-f0220000  
  
lo: Link encap:Local Loopback  
      inet addr:127.0.0.1 Mask:255.0.0.0  
      inet6 addr: ::1/128 Scope:Host  
      UP LOOPBACK RUNNING  MTU:16436  Metric:1  
      RX packets:117 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:117 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:0  
      RX bytes:23501 (22.9 KB)  TX bytes:23501 (22.9 KB)  
  
msfadmin@metasploitable:~$
```

Utilizziamo ora il comando `sudo nmap -sS` che ha la funzione di esegue una scansione "half-open", inviando pacchetti SYN e attendendo risposte SYN/ACK.

```
kali@kali: ~  
File Actions Edit View Help  
$ sudo nmap -sS 192.168.1.3  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 08:54 EST  
Nmap scan report for 192.168.1.3  
Host is up (0.000099s 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  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-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: 08:00:27:3F:28:90 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds  
  
kali@kali: ~  
$
```

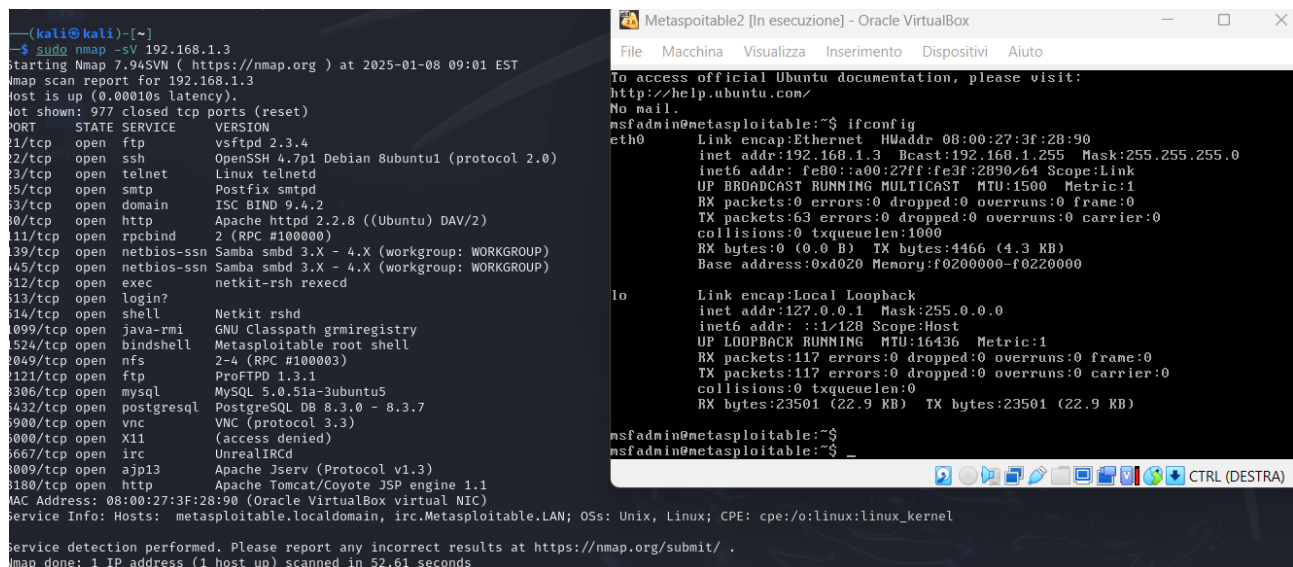
```
Metasploitable2 [In esecuzione] - Oracle VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:3f:28:90  
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe3f:2890/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:4466 (4.3 KB)  
          Base address:0xd020 Memory:f0200000-f0220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:23501 (22.9 KB)  TX bytes:23501 (22.9 KB)  
  
msfadmin@metasploitable:~$
```

Poi effettuiamo la scansione con il comando `sudo nmap -sT` che esegue una scansione che stabilisce connessioni TCP complete.

```
kali@kali: ~  
$ sudo nmap -sT 192.168.1.3  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 08:59 EST  
Nmap scan report for 192.168.1.3  
Host is up (0.0014s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
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  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-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: 08:00:27:3F:28:90 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds  
  
kali@kali: ~  
$
```

```
Metasploitable2 [In esecuzione] - Oracle VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:3f:28:90  
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe3f:2890/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:4466 (4.3 KB)  
          Base address:0xd020 Memory:f0200000-f0220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:23501 (22.9 KB)  TX bytes:23501 (22.9 KB)  
  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$
```

In ultimo procediamo con una scansione Version Detection tramite il comando `sudo nmap -sV` che in output restituirà le informazioni sull' host scansionato che appunto è Metasploitable.



The image shows two overlapping windows. The left window is a Kali Linux terminal running the command `sudo nmap -sV 192.168.1.3`. The output shows a scan report for 192.168.1.3, identifying it as a Debian 8 Ubuntu1 (protocol 2.0) with various open ports and services. The right window is a Metasploit2 VM titled "Metasploit2 [In esecuzione] - Oracle VirtualBox". It shows the output of the `ifconfig` command for the `eth0` interface, displaying IP address, netmask, and other network details. The terminal also shows the command `msfadmin@metasploitable:~$` and the prompt `msfadmin@metasploitable:~$`.

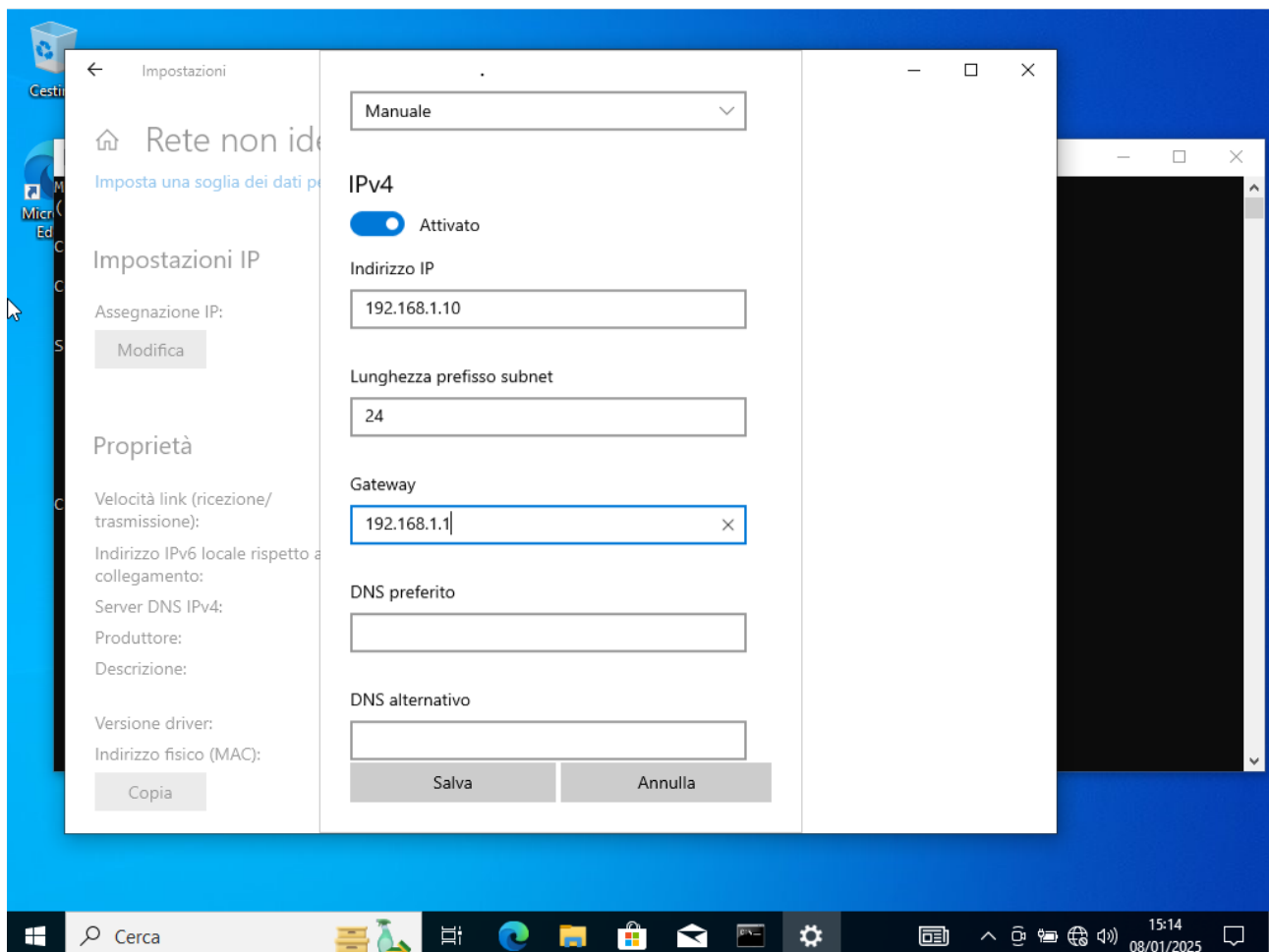
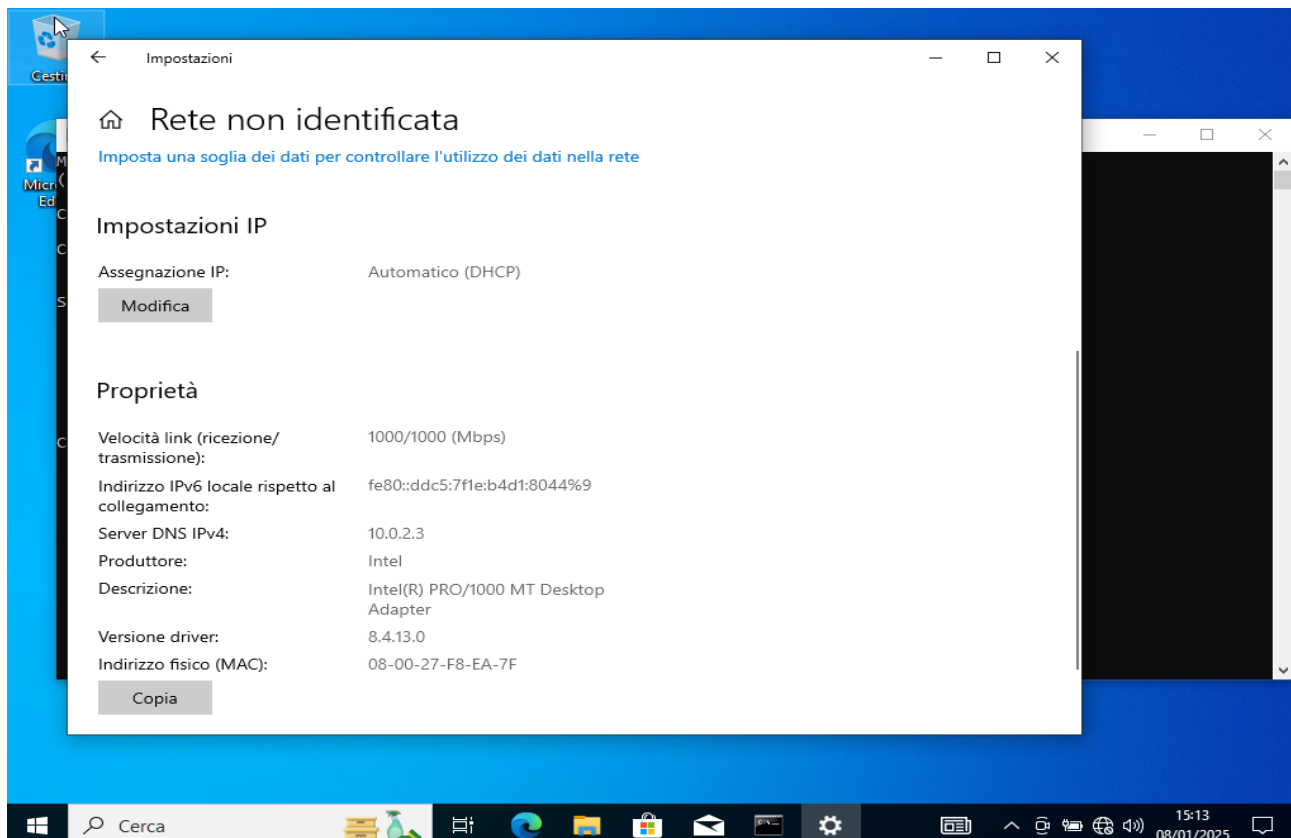
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3f:28:90
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3f:2890/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4466 (4.3 KB)
          Base address:0xd020  Memory:f0200000-f0220000

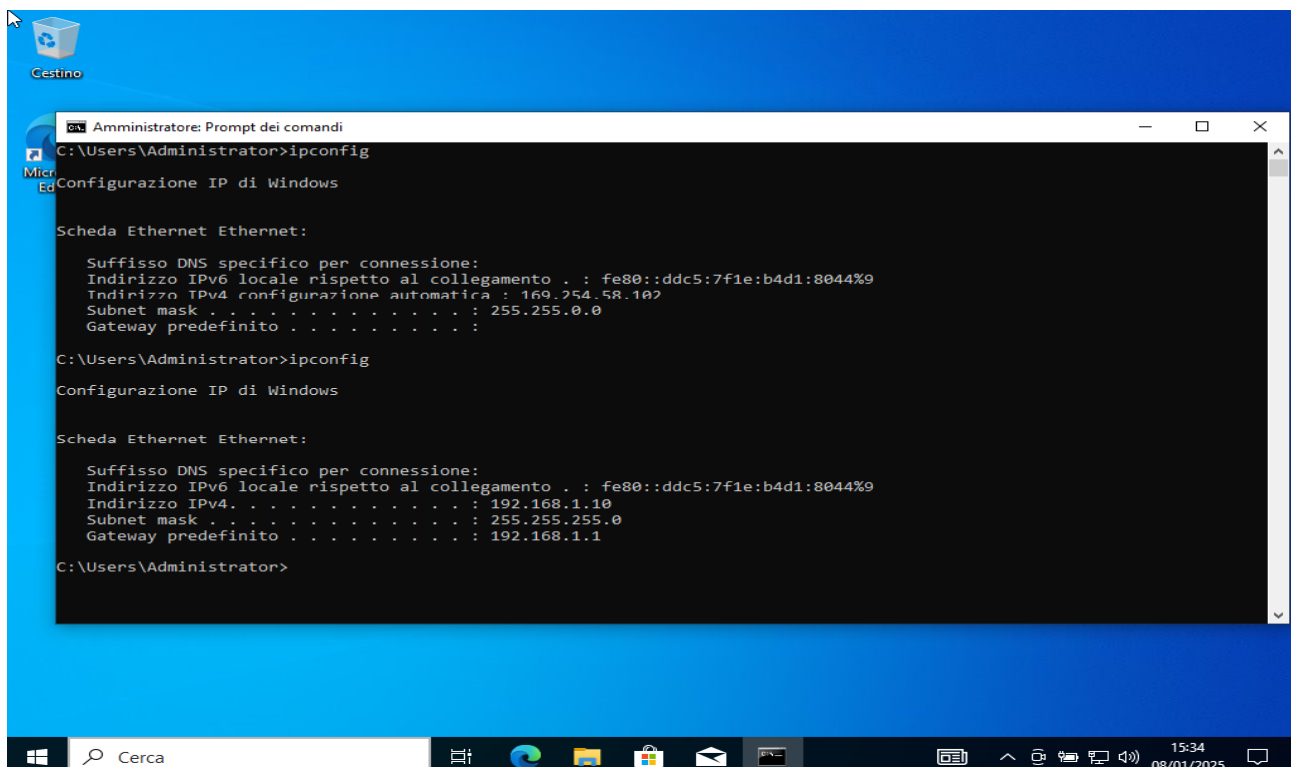
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23501 (22.9 KB)  TX bytes:23501 (22.9 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

Passiamo quindi sulla VM di Windows10 modificando l' indirizzo IP e scegliendone uno sulla stessa rete di Kali.

Per farlo dovremo assegnarlo manualmente disabilitando la funzione DHCP.





Procediamo dunque con la scansione OS Fingerprint sul target Windows10 di nuovo con il comando `sudo nmap -O` e in output avremo varie informazioni tra cui il SO del target:

