

REPORT NMAP

In questa esercitazione si effettueranno delle scansioni con NMAP per raccogliere informazioni.

Scansioni Target Metasploitable:

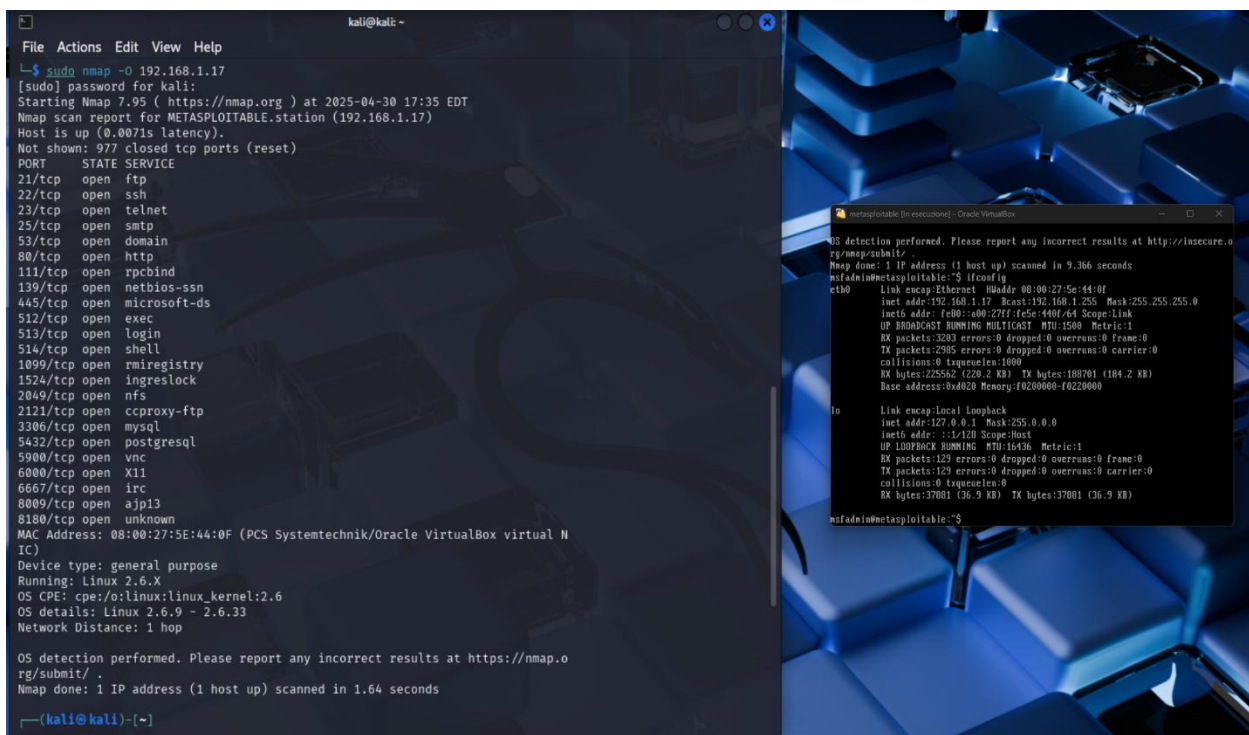
1. OS fingerprint
2. Syn Scan.
3. TCP connect
4. Versione detection

Scansioni Target Windows:

1. OS fingerprint

metasploitable

nella prima scansione si utilizzerà il comando: `nmap -O 192.168.1.17`, questo ci permette di rilevare il sistema operativo e quale versione.

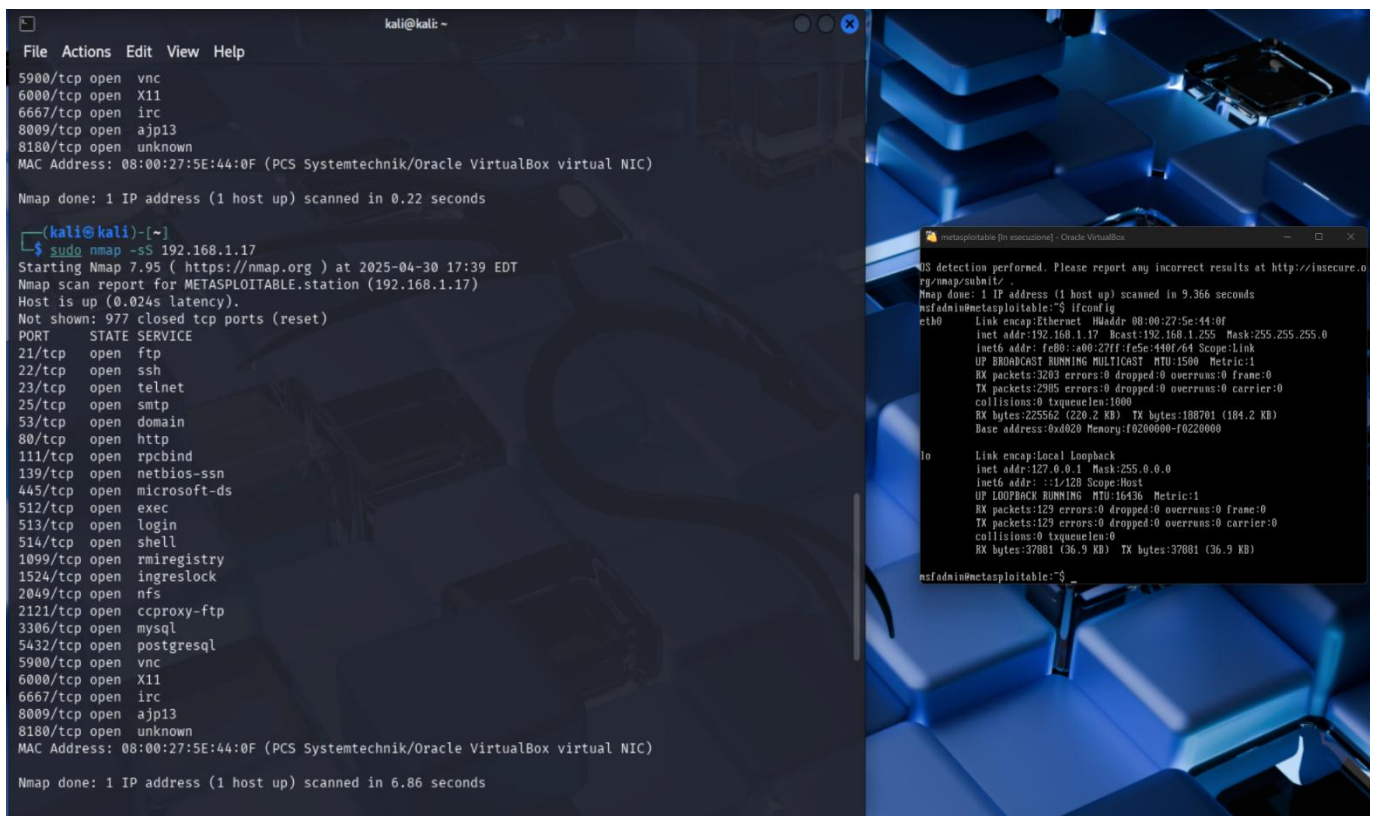


```
kali@kali: ~  
File Actions Edit View Help  
└─$ sudo nmap -O 192.168.1.17  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 17:35 EDT  
Nmap scan report for METASPLOITABLE.station (192.168.1.17)  
Host is up (0.0071s latency).  
Not shown: 977 closed tcp ports (reset)  
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: 08:00:27:5E:44:0F (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
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 1.64 seconds  
└─(kali@kali)-[~]
```

```
metasploitable [In escudo] - Oracle VirtualBox  
OS detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 9.366 seconds  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:5e:44:0f  
          inet addr: 192.168.1.17  Bcast: 192.168.1.255  Mask: 255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe5e:440f/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:3283 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2985 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:225562 (220.2 KB)  TX bytes:188701 (184.2 KB)  
          Base address: 0x0020 Memory: 16200000-16220000  
  
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:65536  Metric:1  
          RX packets:129 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:129 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:37801 (36.5 KB)  TX bytes:37801 (36.5 KB)  
  
msfadmin@metasploitable:~$
```

Otteniamo utili informazione come il MAC address, le porte aperte, il sistema operativo con la versione installata.

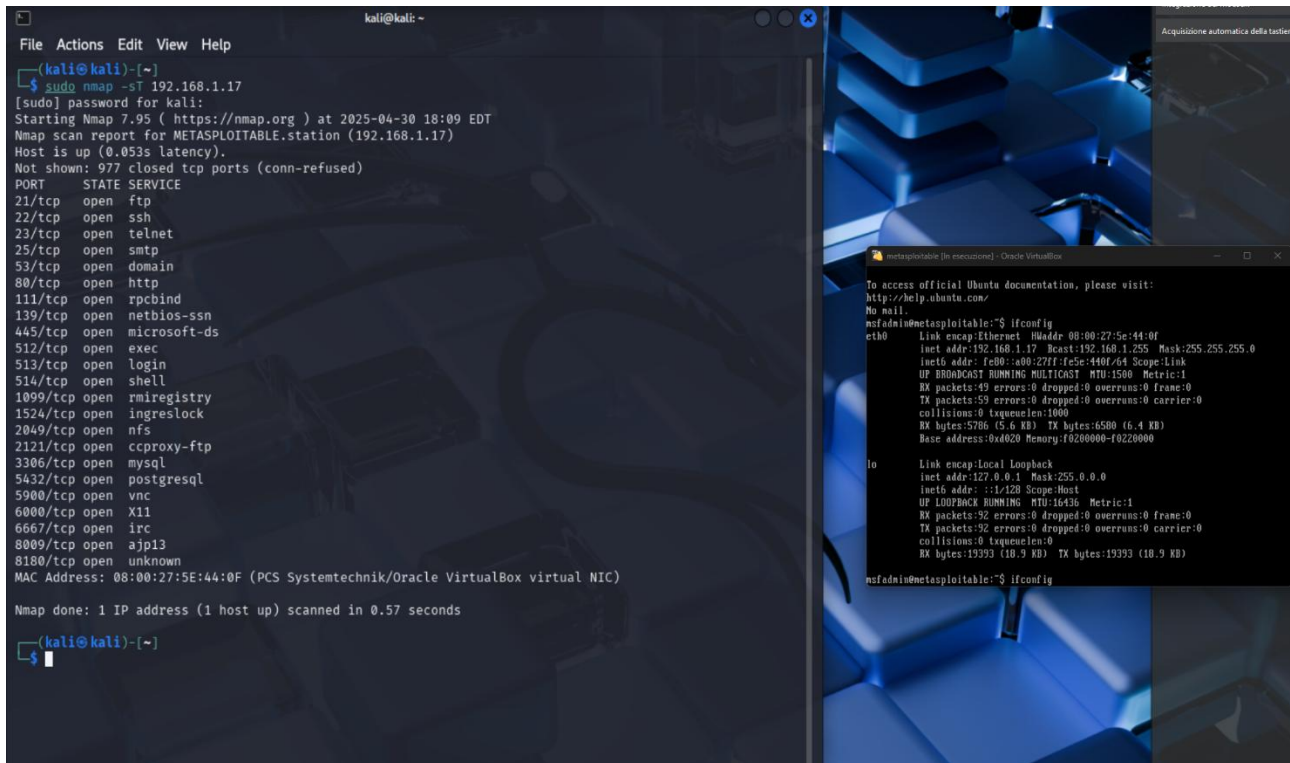
Nella seconda scansione si utilizzerà il comando: `nmap -sS 192.168.1.17`, mettendo `-sS` ci permette di vedere le porte aperte e utilizzerà pacchetti SYN attendendo un SYN/ACK



```
kali@kali: ~  
File Actions Edit View Help  
5900/tcp open  vnc  
6000/tcp open  X11  
6667/tcp open  irc  
8009/tcp open  ajp13  
8180/tcp open  unknown  
MAC Address: 08:00:27:5E:44:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds  
  
kali@kali: ~  
$ sudo nmap -sS 192.168.1.17  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 17:39 EDT  
Nmap scan report for METASPLOITABLE.station (192.168.1.17)  
Host is up (0.024s 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: 08:00:27:5E:44:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 6.86 seconds  
  
metasploitable [in esecuzione] - Oracle VirtualBox  
OS detection performed. Please report any incorrect results at http://insecure.org  
Nmap done: 1 IP address (1 host up) scanned in 9.366 seconds  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:5e:44:0f  
          inet addr:192.168.1.17  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe5e:440f/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:3203 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2905 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:225562 (220.2 KB)  TX bytes:188701 (184.2 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:129 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:129 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:37081 (36.9 KB)  TX bytes:37081 (36.9 KB)  
  
msfadmin@metasploitable:~$
```

Nella terza scansione si utilizzerà il comando `nmap -sT 192.168.1.17`

Questo comando ci permette di stabilire una connessione TCP completa a ciascuna porta di destinazione.



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

```
kali@kali: ~  
File Actions Edit View Help  
~(kali@kali)-[~]  
└─$ sudo nmap -sT 192.168.1.17  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 18:09 EDT  
Nmap scan report for METASPLOITABLE.station (192.168.1.17)  
Host is up (0.053s 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: 08:00:27:5E:44:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds  
  
~(kali@kali)-[~]  
└─$
```

The foreground window is a Metasploitable VM titled "metasploitable [in esecuzione] - Oracle VM VirtualBox". It shows the output of the `ifconfig` command:

```
msfadmin@metasploitable:~$ ifconfig  
No mail.  
eth0      Link encap:Ethernet  HWaddr 08:00:27:5e:44:0f  
          inet addr:192.168.1.17  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe5e:440f/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:49  errors:0  dropped:0  overruns:0  frame:0  
          TX packets:59  errors:0  dropped:0  overruns:0  carrier:0  
          collisions:0  txqueuelen:1000  
          RX bytes:5786 (5.6 KB)  TX bytes:6580 (6.4 KB)  
          Base address: 0x0020 Memory: f0200000-f0200000  
  
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:65536  Metric:1  
          RX packets:92  errors:0  dropped:0  overruns:0  frame:0  
          TX packets:92  errors:0  dropped:0  overruns:0  carrier:0  
          collisions:0  txqueuelen:0  
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)  
  
msfadmin@metasploitable:~$ ifconfig
```

Nella terza scansione si utilizzerà il comando `nmap -sV 192.168.1.17`

Questo comando ci permette di avere più informazioni non solo riguardanti la macchina ma anche la versione dei vari servizi. Questo può tornare utile nel caso di attacchi malevoli.

WINDOWS

In questa scansione si utilizzerà il comando: `nmap -O 192.168.1.18`

Per questa prima scansione come risultato viene che tutte le porte sono chiuse ma è riuscito a ritrovare la versione di windows e la network distance.

