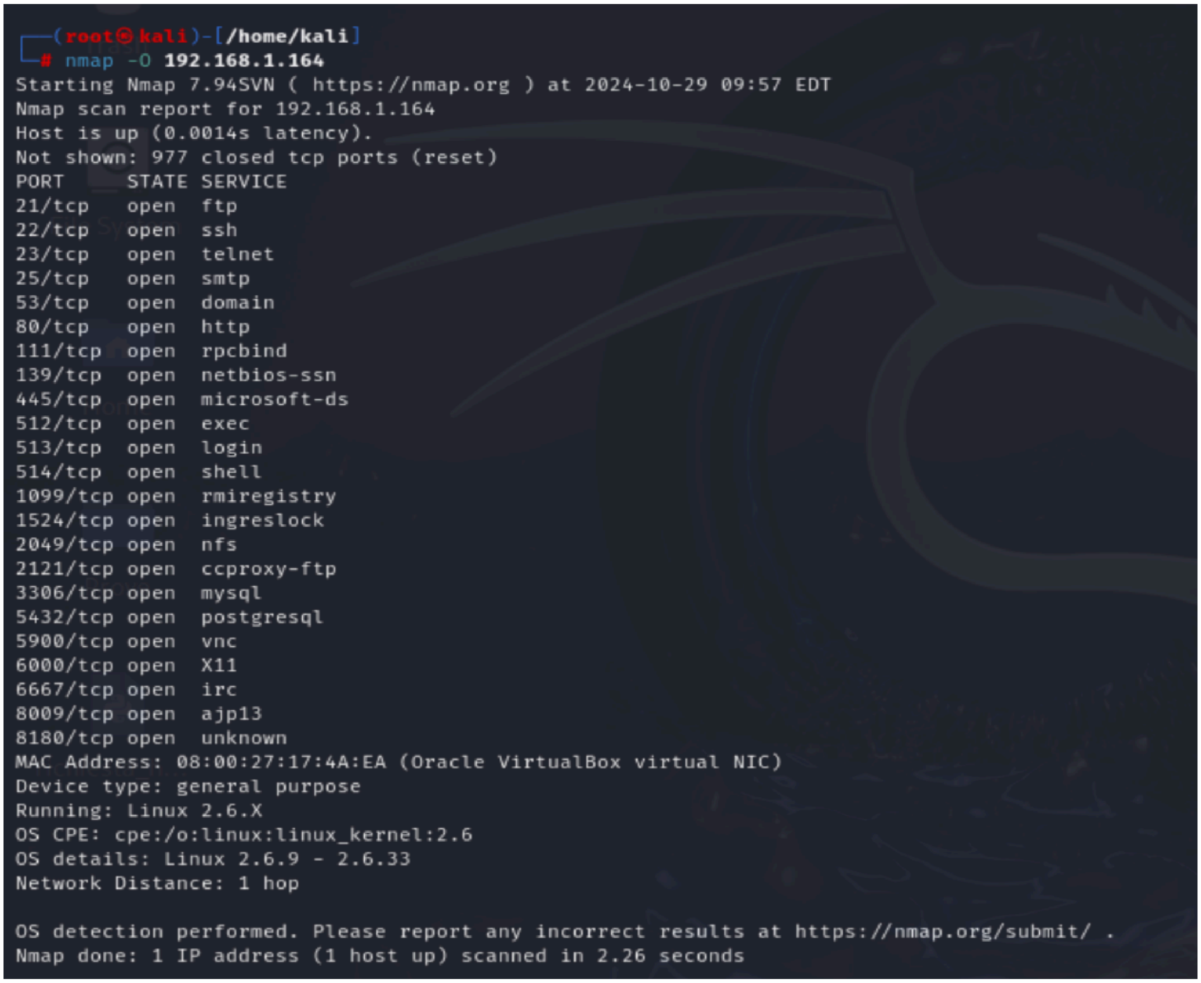
Nmap e alcuni comandi:

Nmap è uno scanner avanzato e potente che ci permette di analizzare e mappare le reti e i dispositivi associati a esse.
ricordiamo che serve l'autorizzazione prima di eseguirlo su una rete.

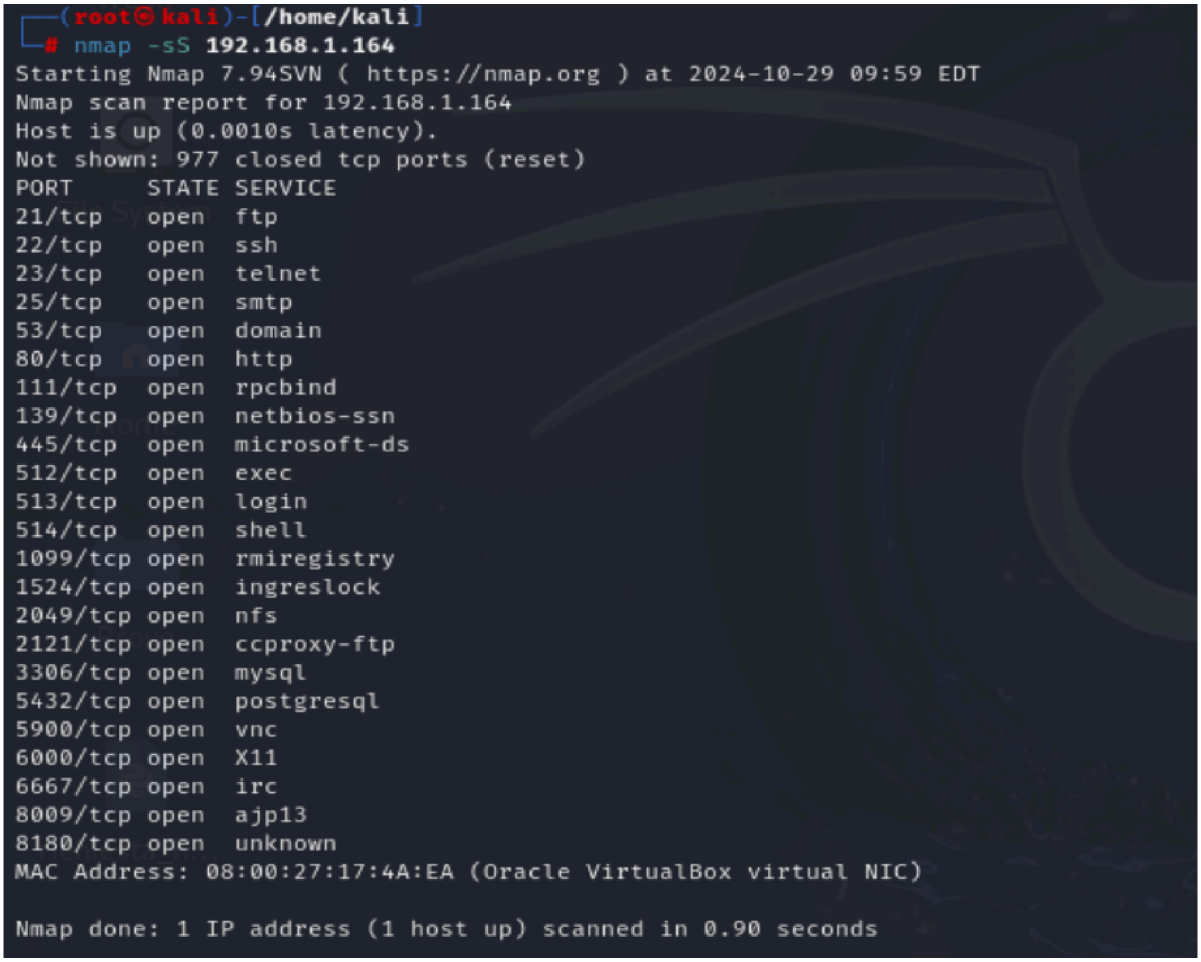
Abbiamo usato "Nmap -O <indirizzo-IP>" per mappare la rete e ricevere informazioni sullo stato delle porte aperte e il servizio (dove possibile) che offrono e il sistema operativo utilizzato.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.164
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 09:57 EDT
Nmap scan report for 192.168.1.164
Host is up (0.0014s 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: 08:00:27:17:4A:EA (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 2.26 seconds
```

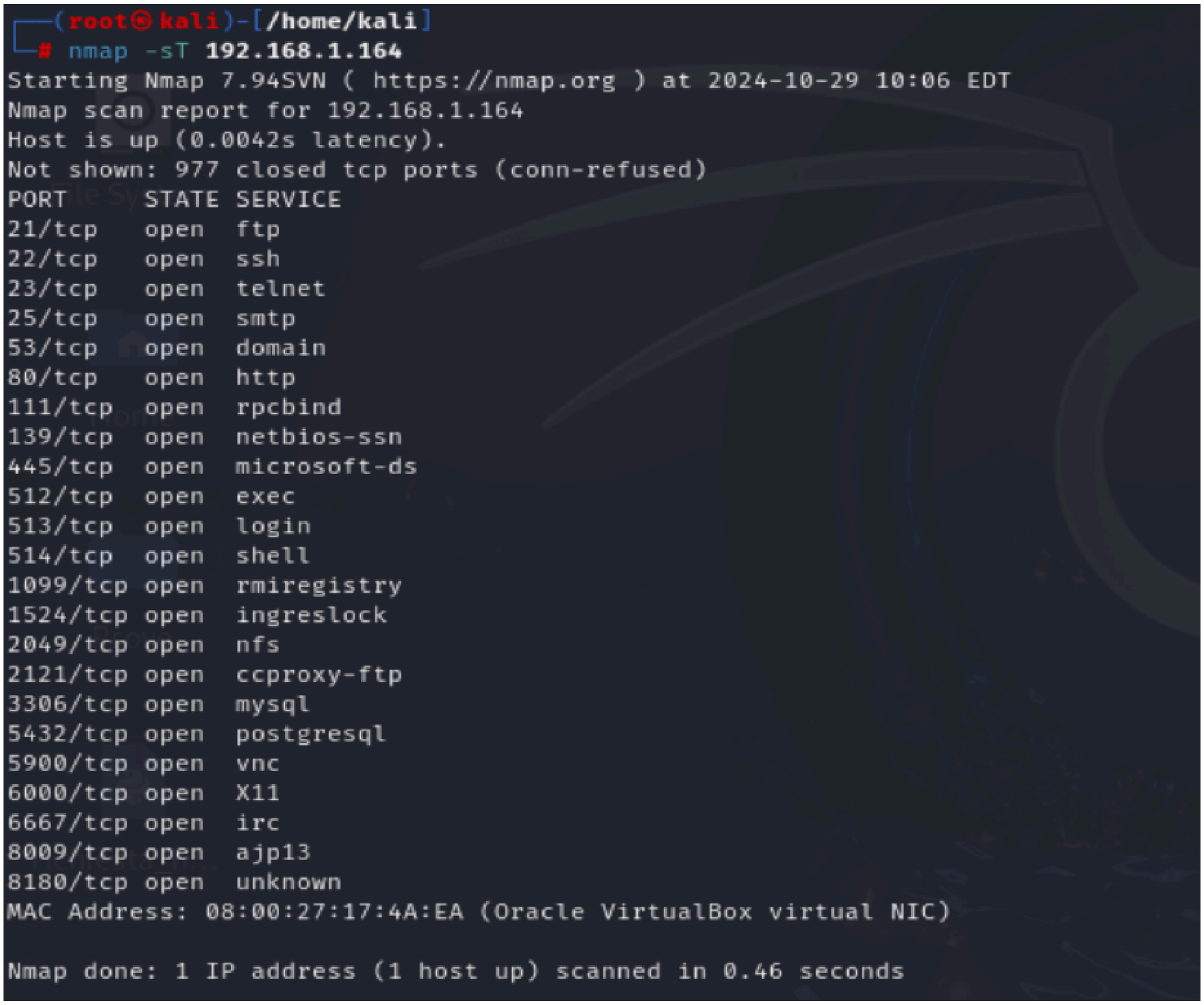
Ora proviamo a utilizzare il comando "nmap - sS <indirizzo-IP>" che serve ad avere lo stesso risultato ma con "meno rumore" perché non completa tutte le richieste del protocollo TCP cioè la "stretta di mano a tre vie" di conseguenza ci mette anche meno tempo ed è meno invadente.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.164
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 09:59 EDT
Nmap scan report for 192.168.1.164
Host is up (0.0010s 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: 08:00:27:17:4A:EA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds
```

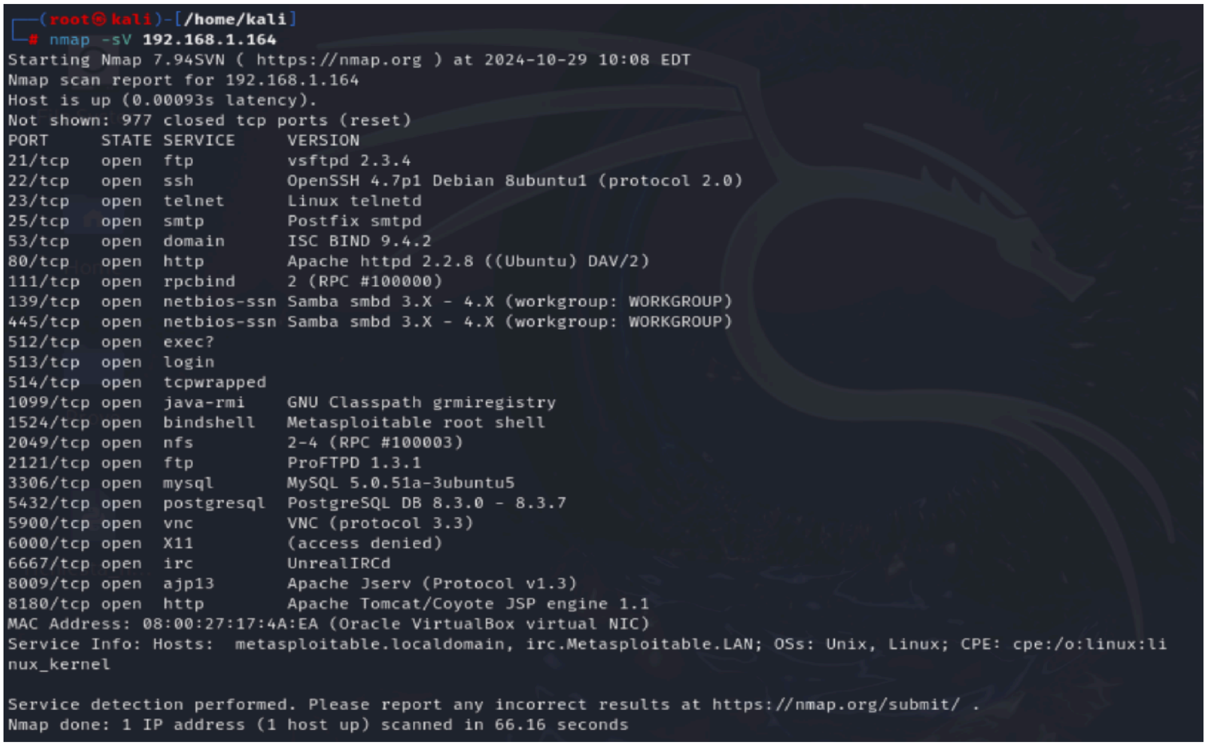
Con il comando “nmap -sT <inidirizzo-IP>” completa la procedura della “stretta di mano a 3 vie”, risulta più evidente l’intrusione ma può essere utile quando la scansione SYN non è praticabile.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.164
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:06 EDT
Nmap scan report for 192.168.1.164
Host is up (0.0042s 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: 08:00:27:17:4A:EA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

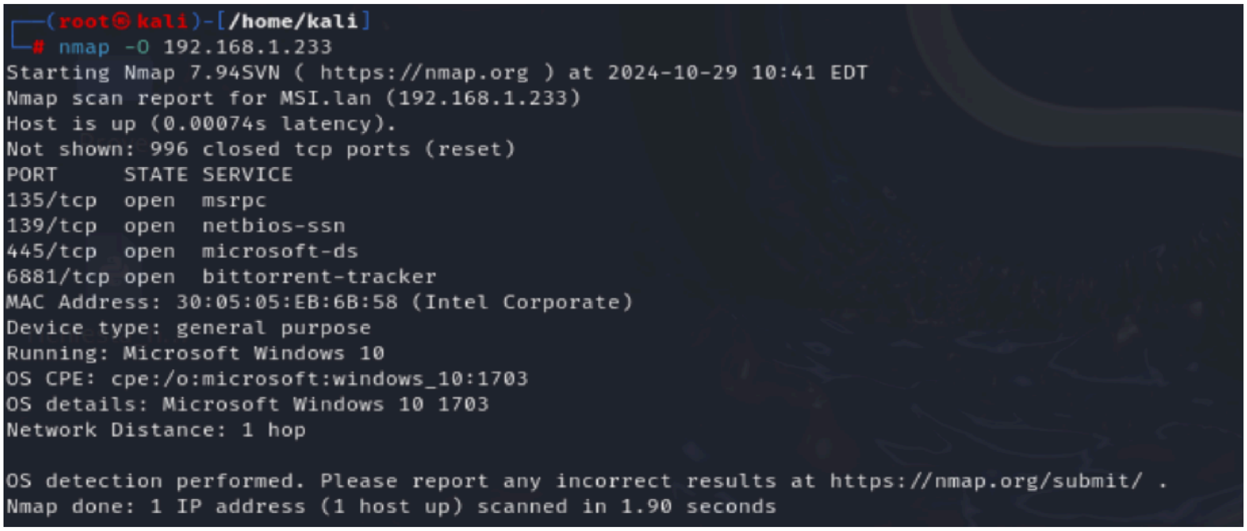
il comando “nmap -sV <indirizzo-IP>” rileva le porte, i servizi e le rispettive versioni utilizzate:



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.164
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:08 EDT
Nmap scan report for 192.168.1.164
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:17:4A:EA (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.16 seconds
```

provato anche OS fingerprint su Windows dopo aver disattivato momentaneamente le difese di windows:



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.233
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:41 EDT
Nmap scan report for MSI.lan (192.168.1.233)
Host is up (0.00074s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6881/tcp open  bittorrent-tracker
MAC Address: 30:05:05:EB:6B:58 (Intel Corporate)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
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 1.90 seconds
```

Diego Petronaci