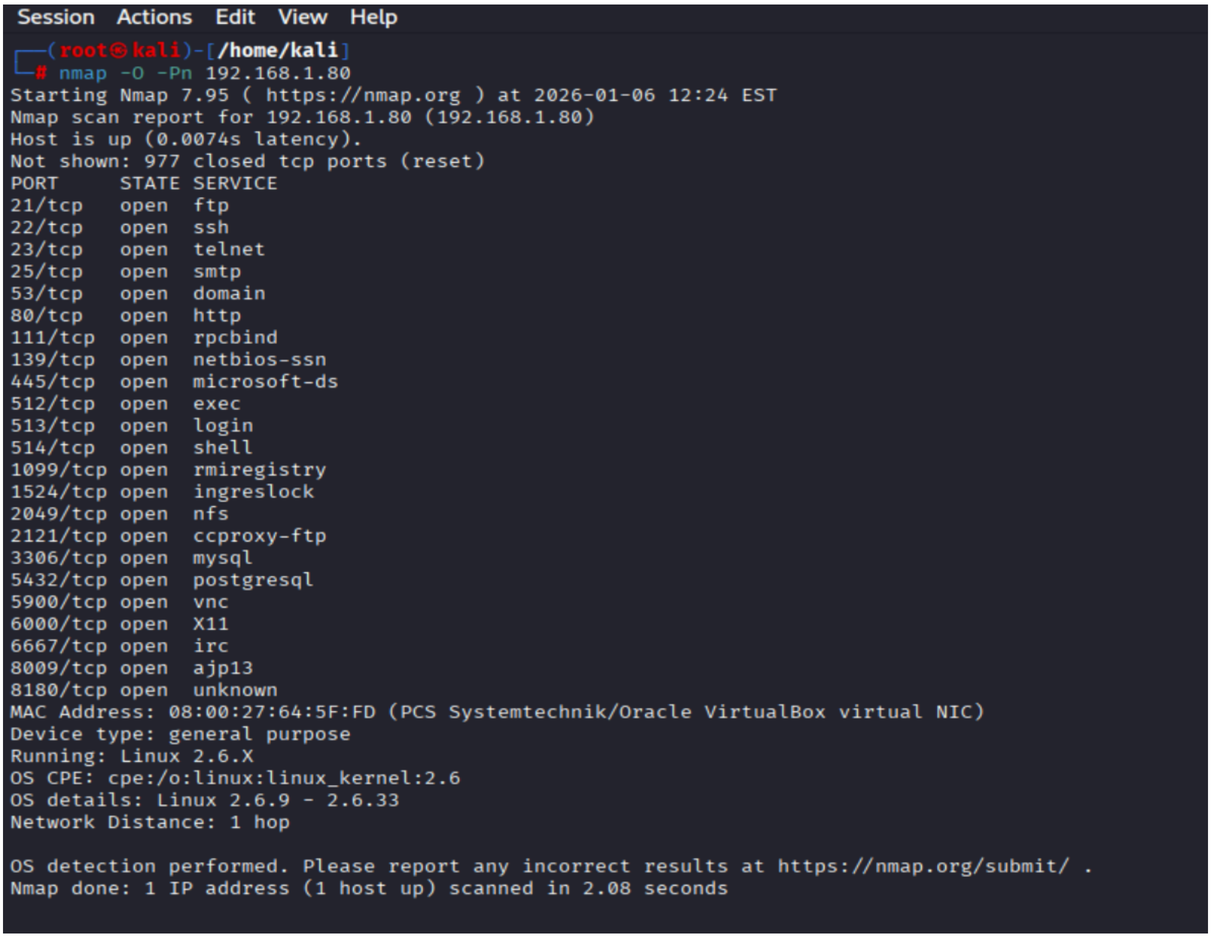
Scansione dei servizi con Nmap

Macchine Utilizzate

- **Kali Linux** con IP 192.168.1.79
- **Metaspoitable** con IP 192.168.1.80
- **Windows 7** con IP 192.168.1.81

Tecniche di scansione usate

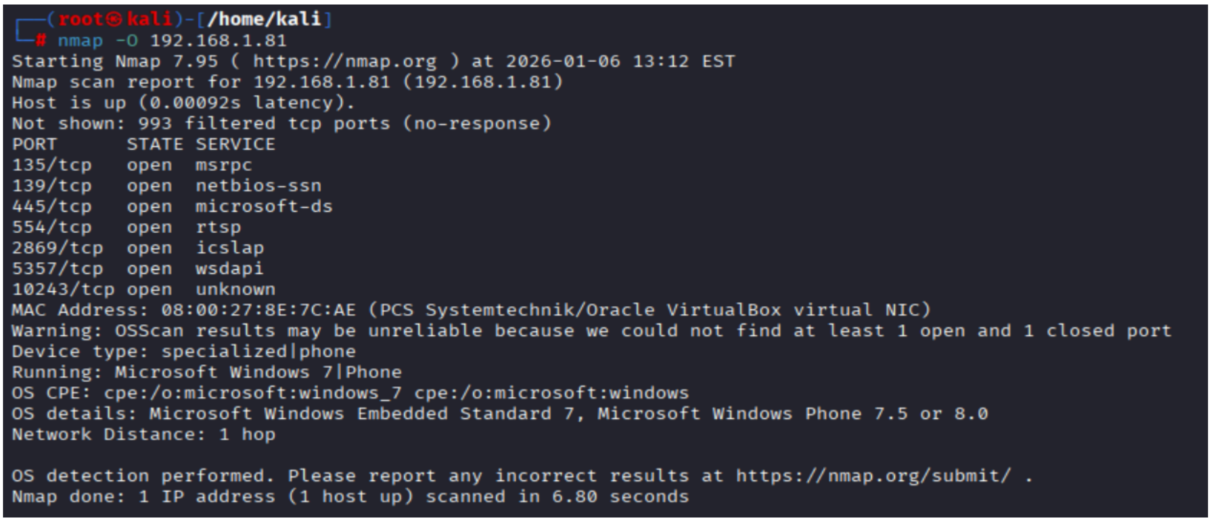
- OS fingerprint (**-O**): Nmap invia una serie di pacchetti TCP/UDP e confronta le risposte con un database di fingerprint per stimare il sistema operativo dell'host.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O -Pn 192.168.1.80
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 12:24 EST
Nmap scan report for 192.168.1.80 (192.168.1.80)
Host is up (0.0074s 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: 08:00:27:64:5F:FD (PCS Systemtechnik/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 2.08 seconds
```

(OS Fingerprint eseguito su metasploitable)

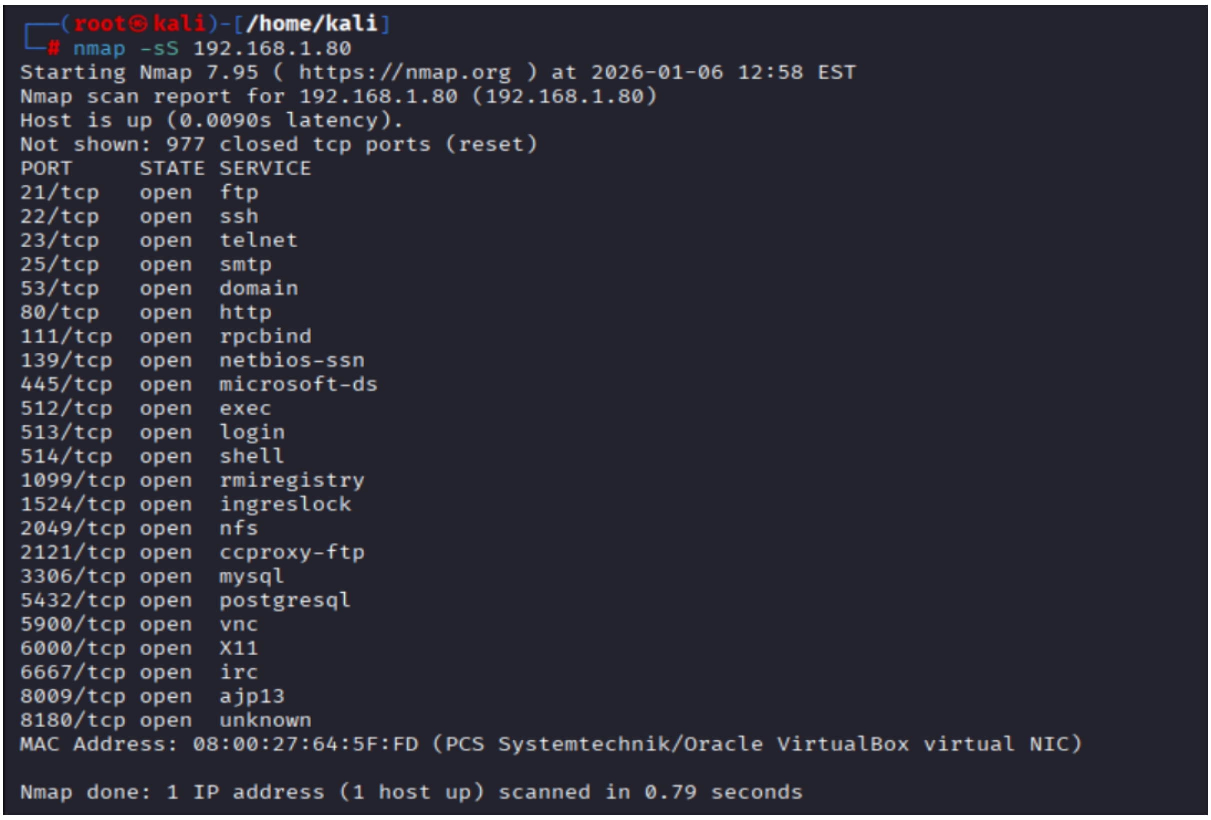


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.81
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:12 EST
Nmap scan report for 192.168.1.81 (192.168.1.81)
Host is up (0.00092s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:8E:7C:AE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
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 6.80 seconds
```

(OS Fingerprint eseguito su Windows)

- SYN scan (**-sS**): è la modalità di scansione predefinita, invia solo il SYN e non completa il three-way handshake, risultando più veloce e meno evidente nei log rispetto al connect scan.

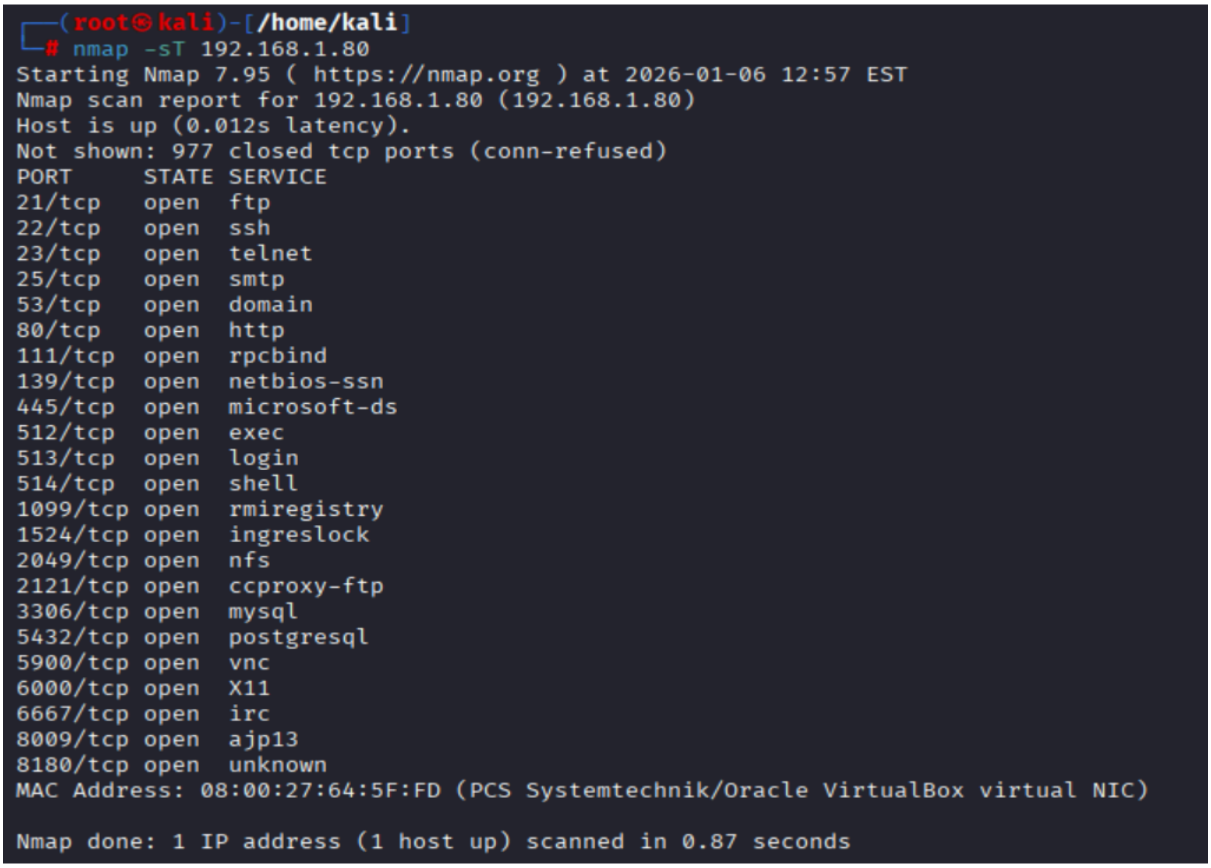


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.80
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 12:58 EST
Nmap scan report for 192.168.1.80 (192.168.1.80)
Host is up (0.0090s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
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: 08:00:27:64:5F:FD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds
```

(Syn Scan eseguito su metasploitable)

- TCP connect scan (**-sT**): chiede al sistema operativo di completare la connessione con ogni porta (three-way handshake completo), risulta più lenta e facilmente registrabile ma non richiede privilegi per pacchetti raw.

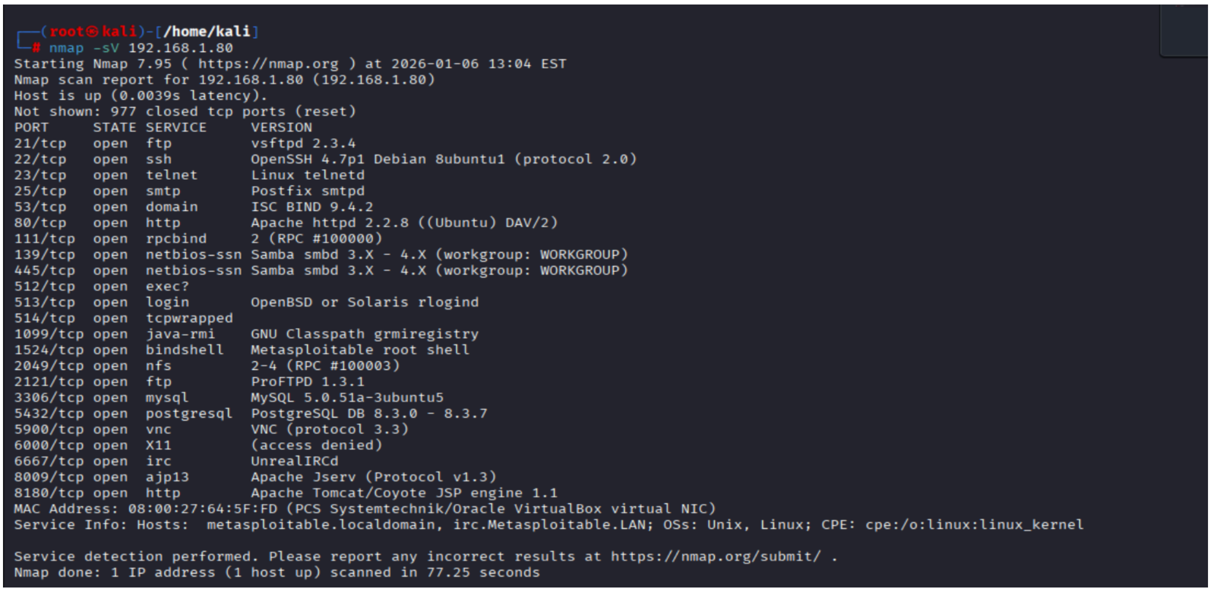


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.80
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 12:57 EST
Nmap scan report for 192.168.1.80 (192.168.1.80)
Host is up (0.012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  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: 08:00:27:64:5F:FD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

(TCP Complete Scan eseguito su metasploitable)

- Version detection (**-sV**): interroga le porte aperte con probe specifici per identificare il tipo di servizio, il nome dell’applicazione e la versione esatta, utilizzando un ampio database interno.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.80
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:04 EST
Nmap scan report for 192.168.1.80 (192.168.1.80)
Host is up (0.0039s 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       OpenBSD or Solaris rlogind
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: 08:00:27:64:5F:FD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.25 seconds
```

(Version Detection su metasploitable)

Differenze SYN scan vs TCP connect

- Nel SYN scan la connessione non viene completata: se la porta è aperta l'host risponde con SYN/ACK e Nmap risponde con RST, evitando di stabilire una sessione completa; questo riduce il rumore sui log e aumenta la furtività.
- Nel TCP connect scan Nmap ogni porta aperta genera una connessione TCP completa, rendendo la scansione più evidente e generalmente più lenta, ma più semplice da usare in assenza di privilegi elevati.