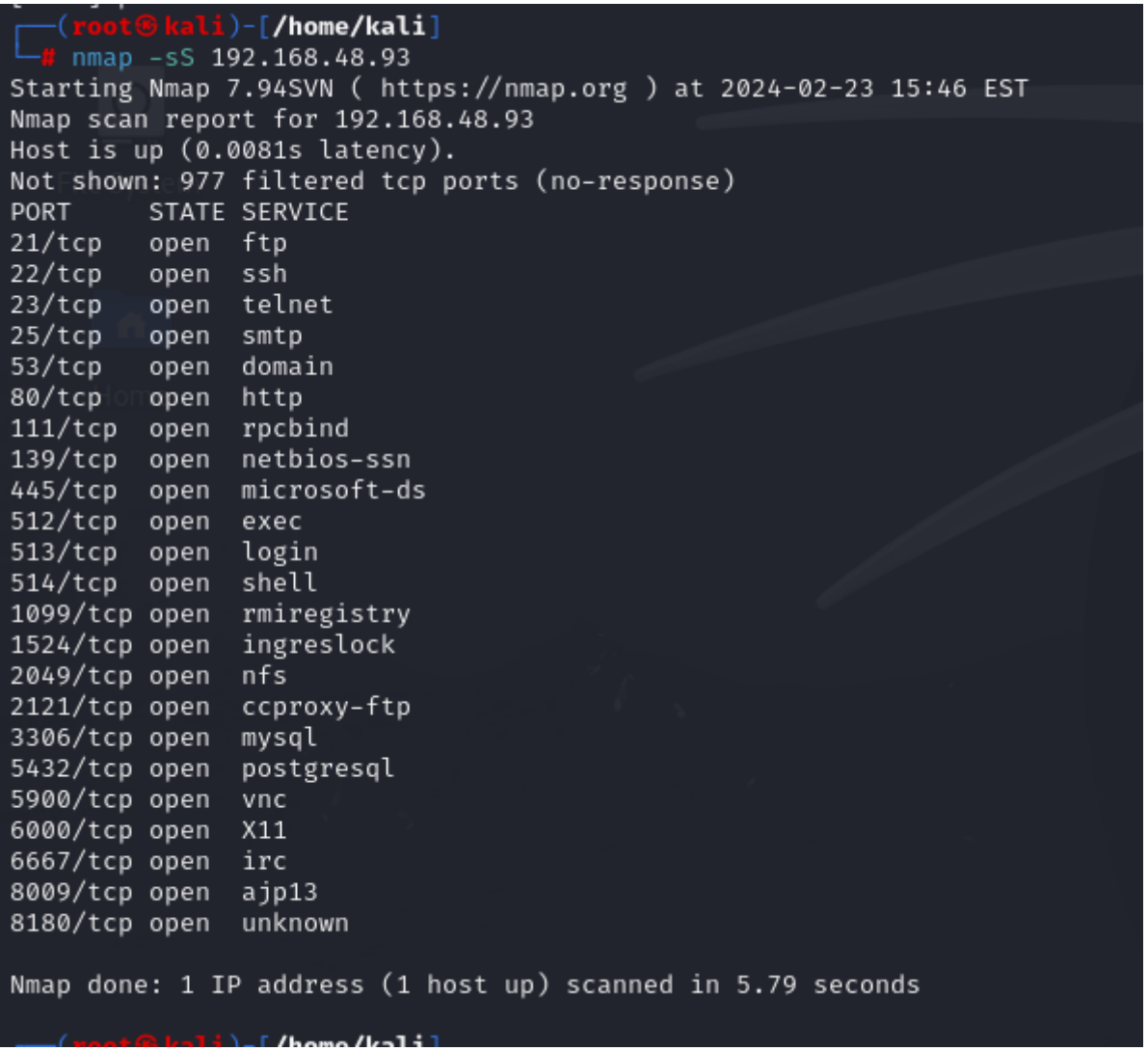
Scansione dei servizi con Nmap

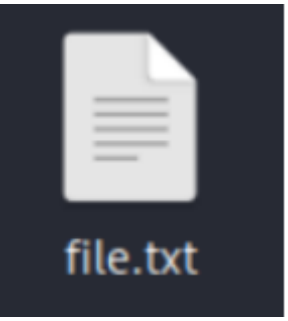


Il comando **nmap -sS 192.168.48.93** è stato utilizzato per eseguire una scansione SYN su tutte le porte della macchina con l'indirizzo IP 192.168.48.93

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 15:48 EST
Nmap scan report for 192.168.48.93
Host is up (0.0045s latency).
Not shown: 977 filtered tcp ports (no-response)
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        netkit-rsh rexecd
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
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 16.75 seconds

┌──(root㉿kali)-[/home/kali]
```

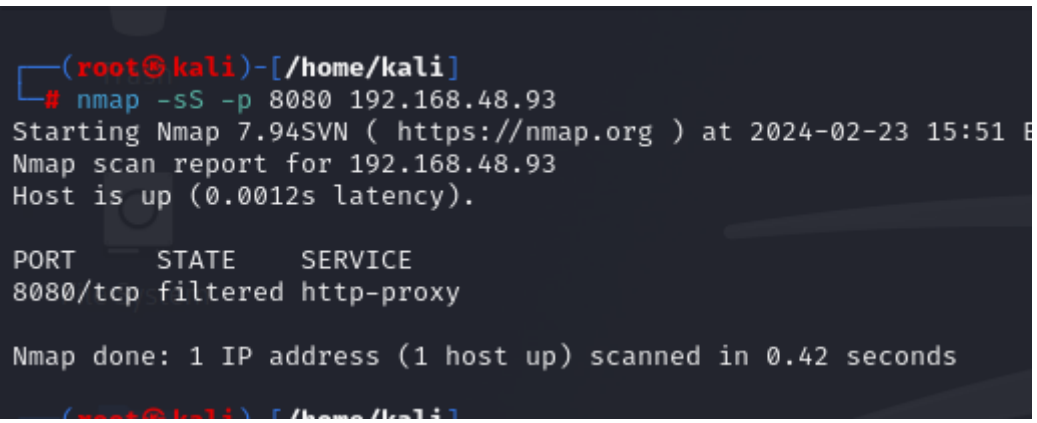
Il comando **nmap -sV 192.168.48.93** è stato utilizzato per eseguire una scansione dei servizi sulla macchina con l'indirizzo IP 192.168.48.93.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -oN file.txt 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 15:49 EST
Nmap scan report for 192.168.48.93
Host is up (0.0050s latency).
Not shown: 977 filtered tcp ports (no-response)
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        netkit-rsh rexecd
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
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 16.12 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

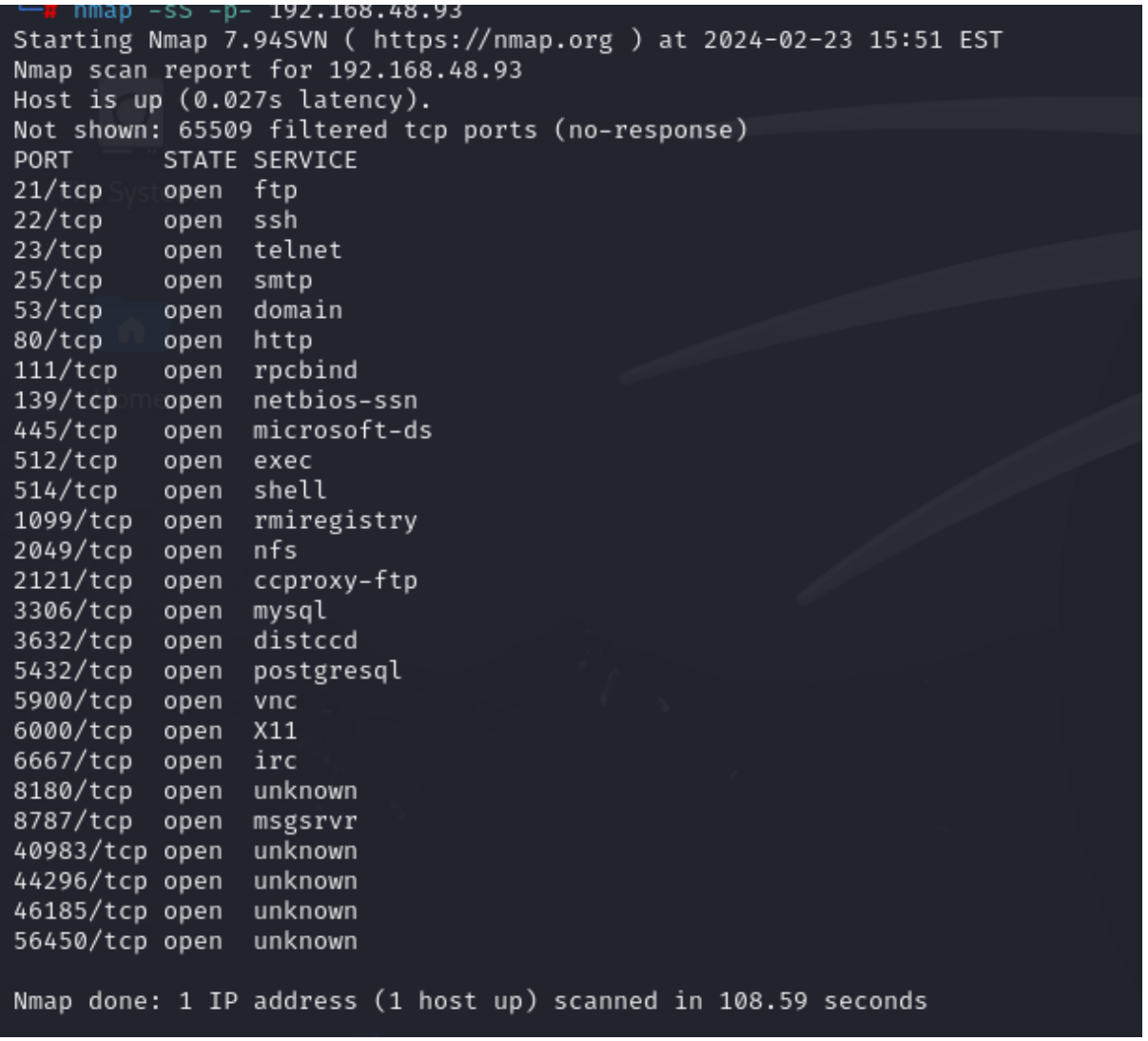


Il comando **nmap -sV -oN file.txt 192.168.48.93** è stato utilizzato per

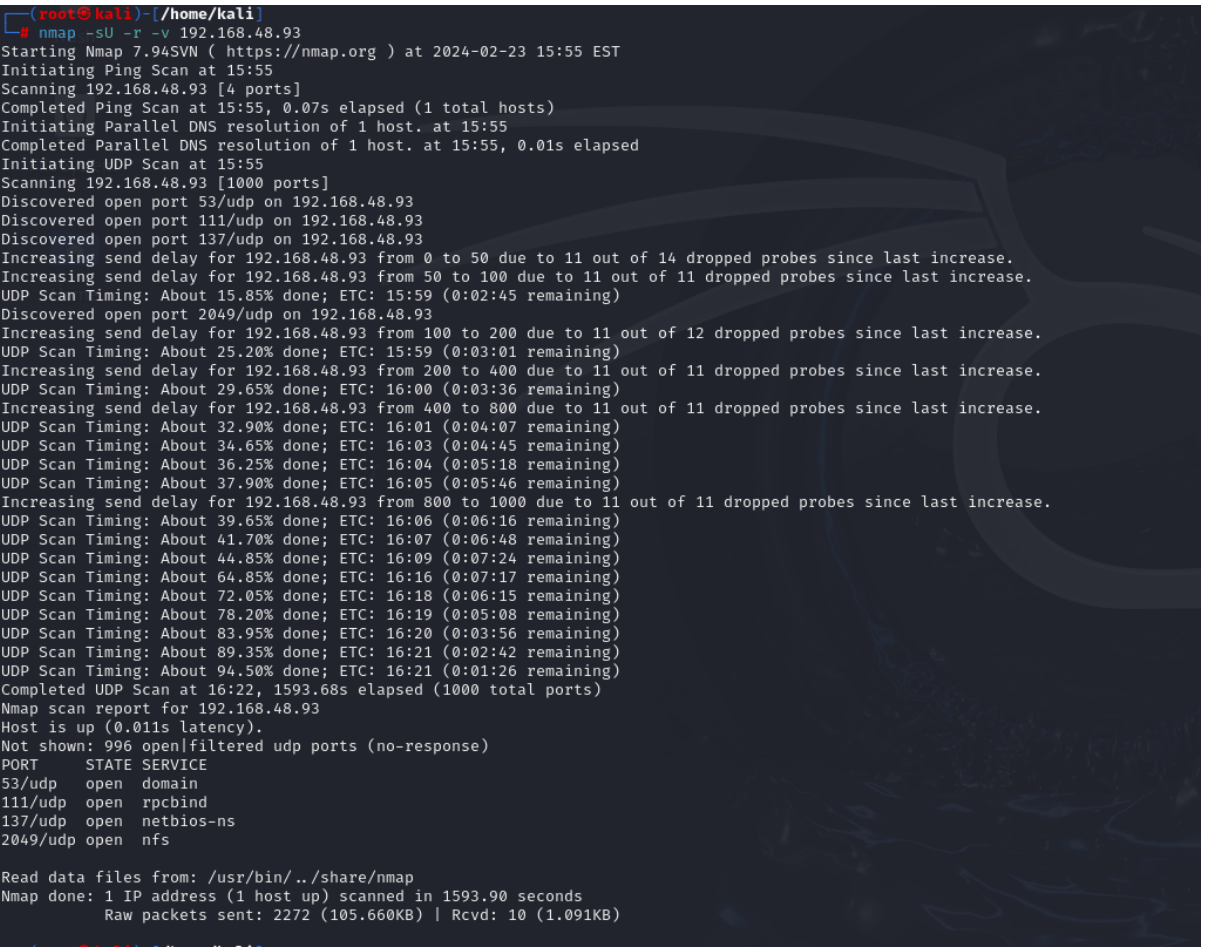
eseguire una scansione dei servizi sulla macchina con l'indirizzo IP 192.168.48.93 e salvare i risultati in un file di testo denominato "file.txt".



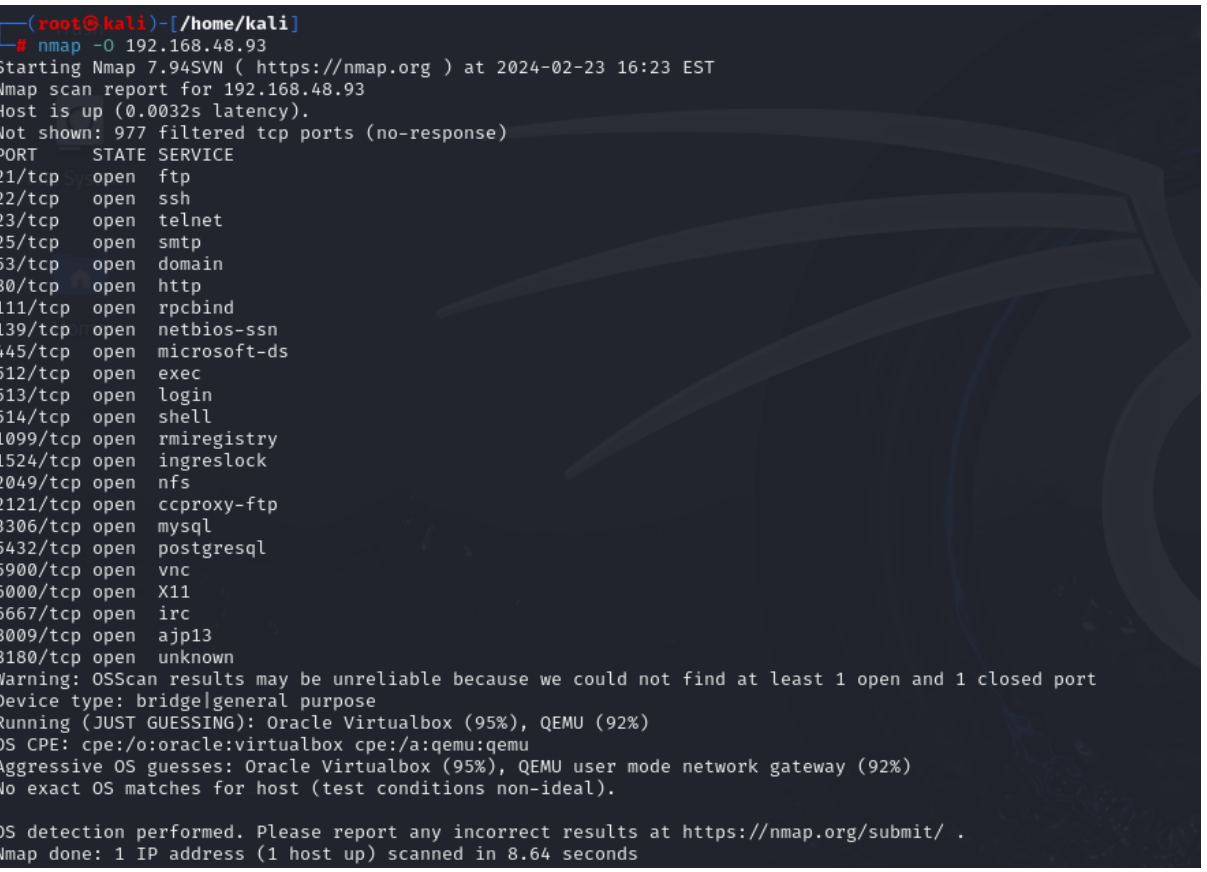
Il comando **nmap -sS -p 8080 192.168.48.93** è stato utilizzato per eseguire una scansione SYN su una specifica porta, nel caso specifico la porta 8080, sulla macchina con l'indirizzo IP 192.168.48.93



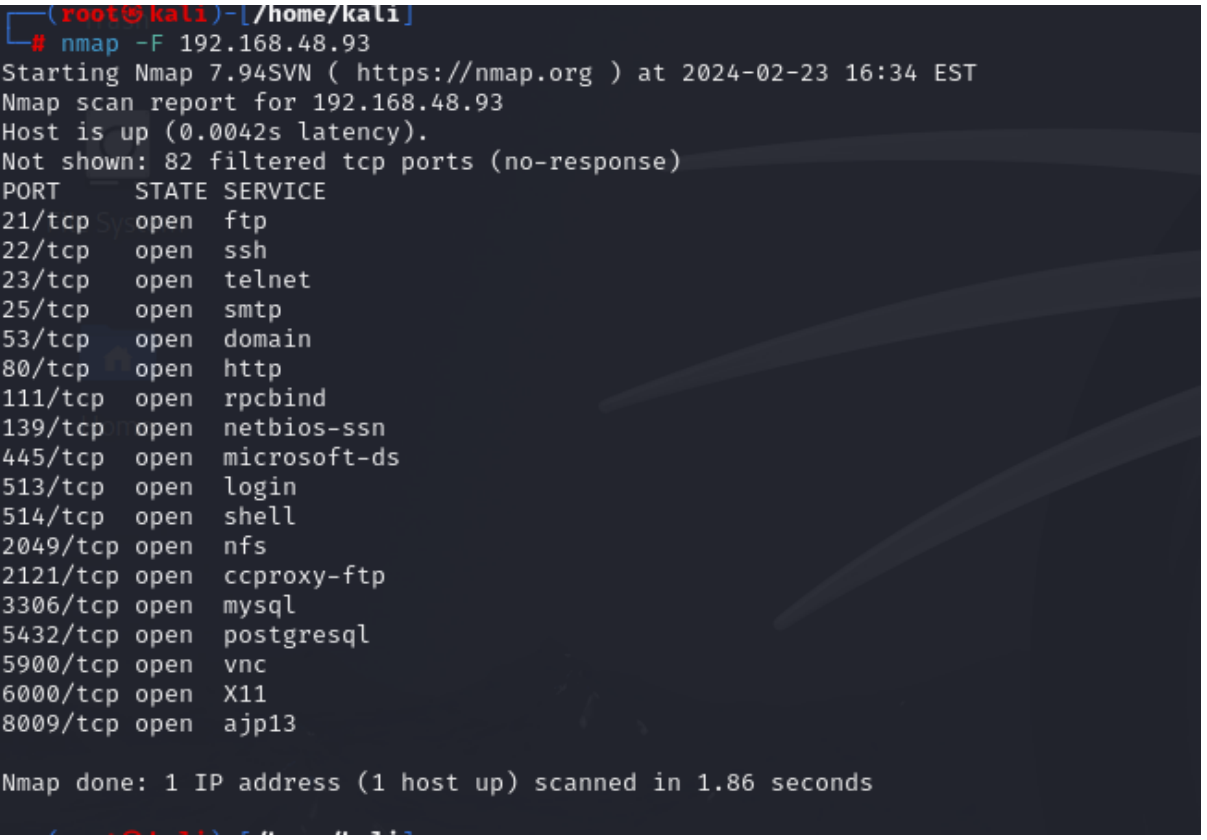
Il comando **nmap -sS -p 8080 192.168.48.93** è stato utilizzato per eseguire una scansione SYN su tutte le 65535 porte, sulla macchina con l'indirizzo IP 192.168.48.93



Il comando **nmap -sU -r -v 192.168.48.93** è stato utilizzato per eseguire una scansione UDP approfondita sulla macchina con l'indirizzo IP 192.168.48.93.



Il comando **nmap -O 192.168.48.93** è stato utilizzato per eseguire una scansione per l'identificazione del sistema operativo sulla macchina con l'indirizzo IP 192.168.48.93.



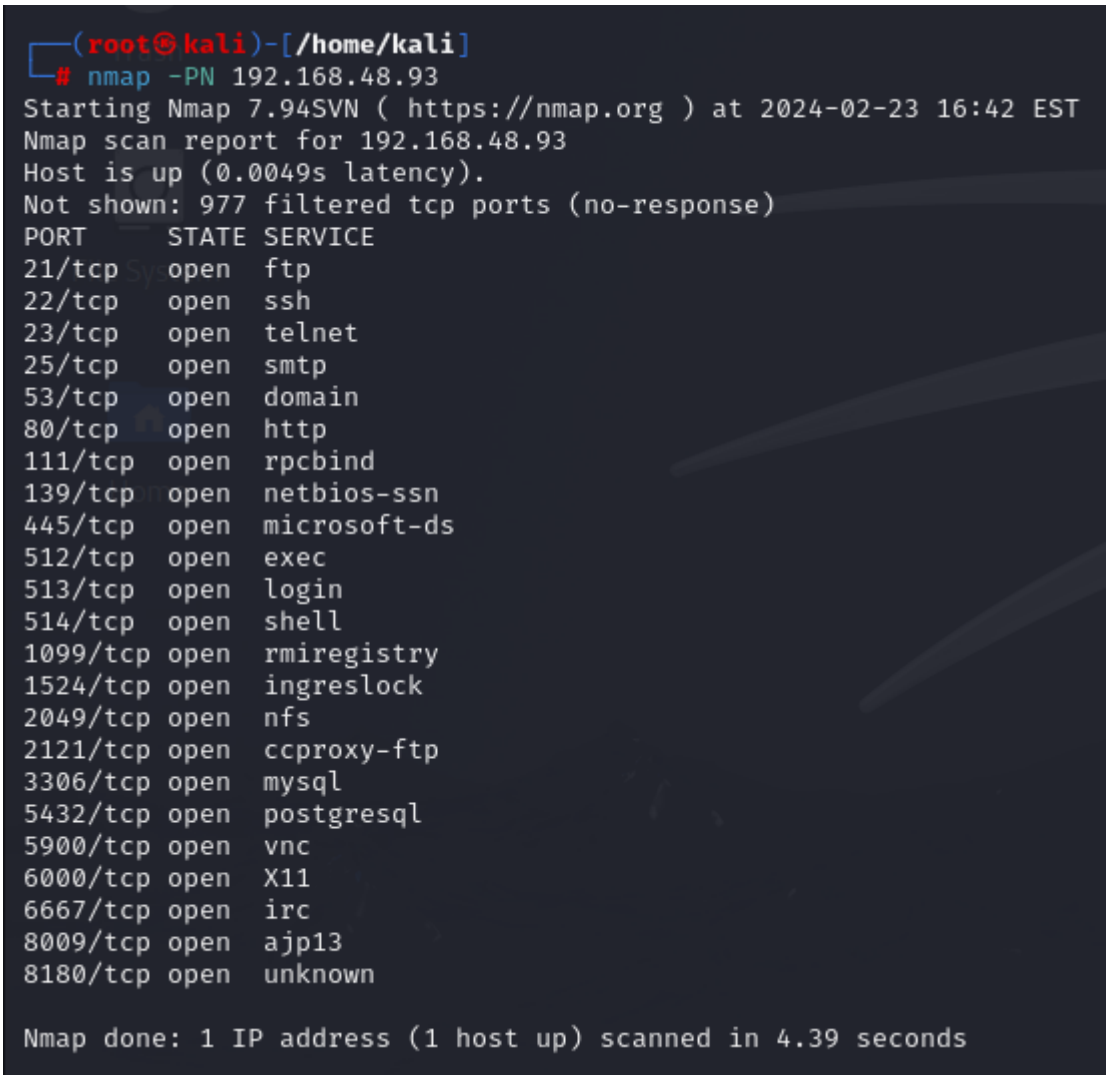
Il comando **nmap -F 192.168.48.93** è stato utilizzato per eseguire una scansione rapida delle porte più comuni sulla macchina con l'indirizzo IP 192.168.48.93.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p- 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 16:30 EST
Stats: 0:02:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.00% done; ETC: 16:32 (0:00:01 remaining)
Stats: 0:03:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.00% done; ETC: 16:33 (0:00:04 remaining)
Nmap scan report for 192.168.48.93
Host is up (0.015s latency).
Not shown: 65510 filtered tcp ports (no-response)
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        netkit-rsh rexecd
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)
6697/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
40983/tcp open  nlockmgr    1-4 (RPC #100021)
44296/tcp open  java-rmi    GNU Classpath grmiregistry
46185/tcp open  mountd      1-3 (RPC #100005)
Service Info: Host:  metasploitable.localdomain; 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 238.15 seconds
```

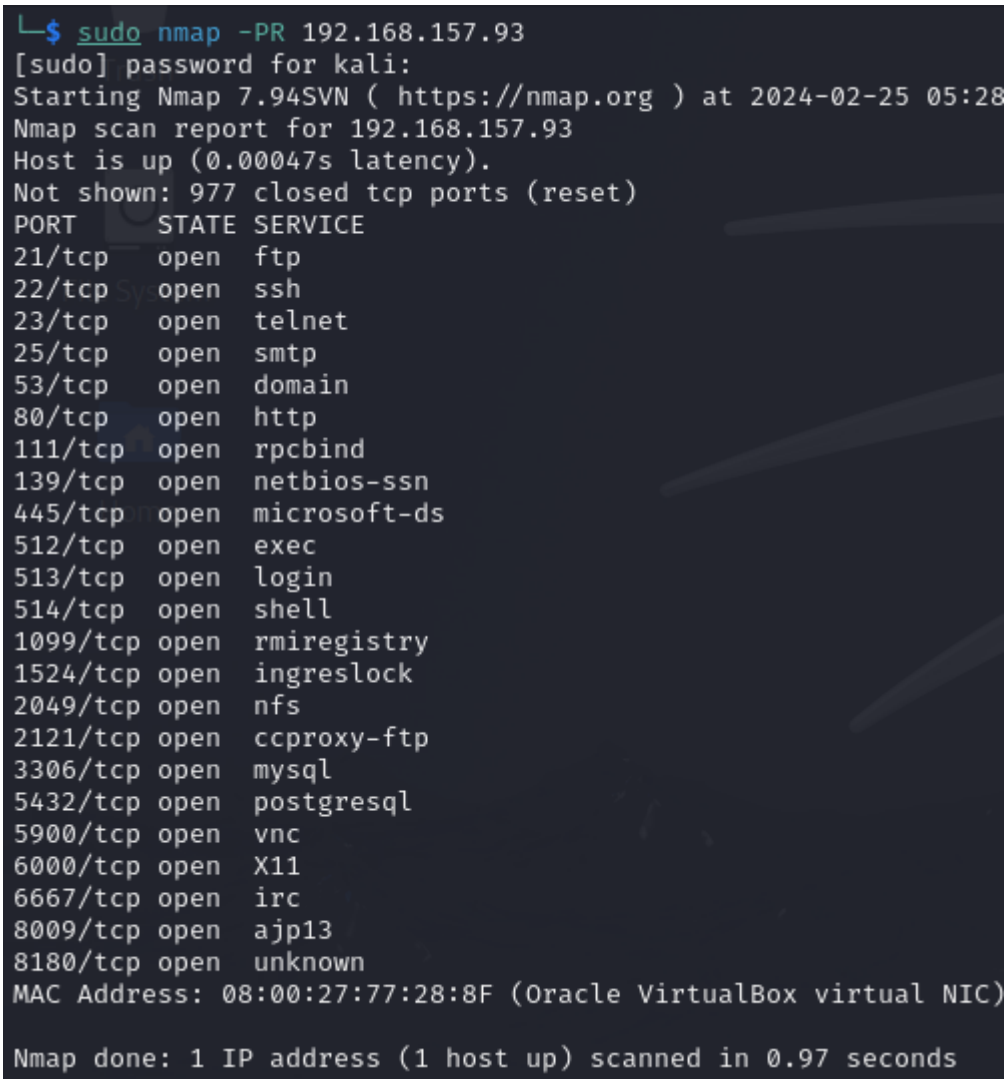
La scansione completa delle porte e il rilevamento delle versioni dei servizi eseguiti con il comando **nmap -sV -p- 192.168.48.93** hanno fornito un dettagliato elenco dei servizi in esecuzione sulla macchina con l'indirizzo IP 192.168.48.93.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sP 192.168.48.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 16:40 EST
Nmap scan report for 192.168.48.93
Host is up (0.0011s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Il comando **nmap -sP 192.168.48.93** è stato utilizzato per eseguire una scansione di discovery di host utilizzando pacchetti di tipo ping (ICMP echo request).



Il comando **nmap -PN 192.168.48.93** è stato utilizzato per eseguire una scansione della rete senza considerare il ping.



Il comando **nmap -PR 192.168.157.93** è stato utilizzato per eseguire una scansione di discovery di host mediante l'invio di pacchetti ARP (Address Resolution Protocol).

IP TARGET	OS	TIPO SCANSIONE	COMANDO	PORTE APERTE	PORTE CHIUSE	MAC ADDRESS
192.168.48.93	METASPLOITABLE	TCP	nmap -sS	23	977	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione completa	nmap -sV	23	977	08:00:27:CE:D2:42

192.168.48.93	METASPLOITABLE	output su file	nmap -sV -oN file.txt	23	977	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione su pora	nmap -sS ip -p 8080	23	977	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione tutte le porte	nmap -sS -p-	30	65505	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione udp	nmap -sU -r -v	3		08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione sistema operativo	nmap -O	-	-	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione versione servizi	nmap -sV	23	977	08:00:27:CE:D2:42
192.168.48.93	METASPLOITABLE	scansione common 100 ports	nmap -F	18	82	08:00:27:CE:D2:42
192.168.157.93	METASPLOITABLE	scansione ARP	nmap -PR	23	977	08:00:27:CE:D2:42