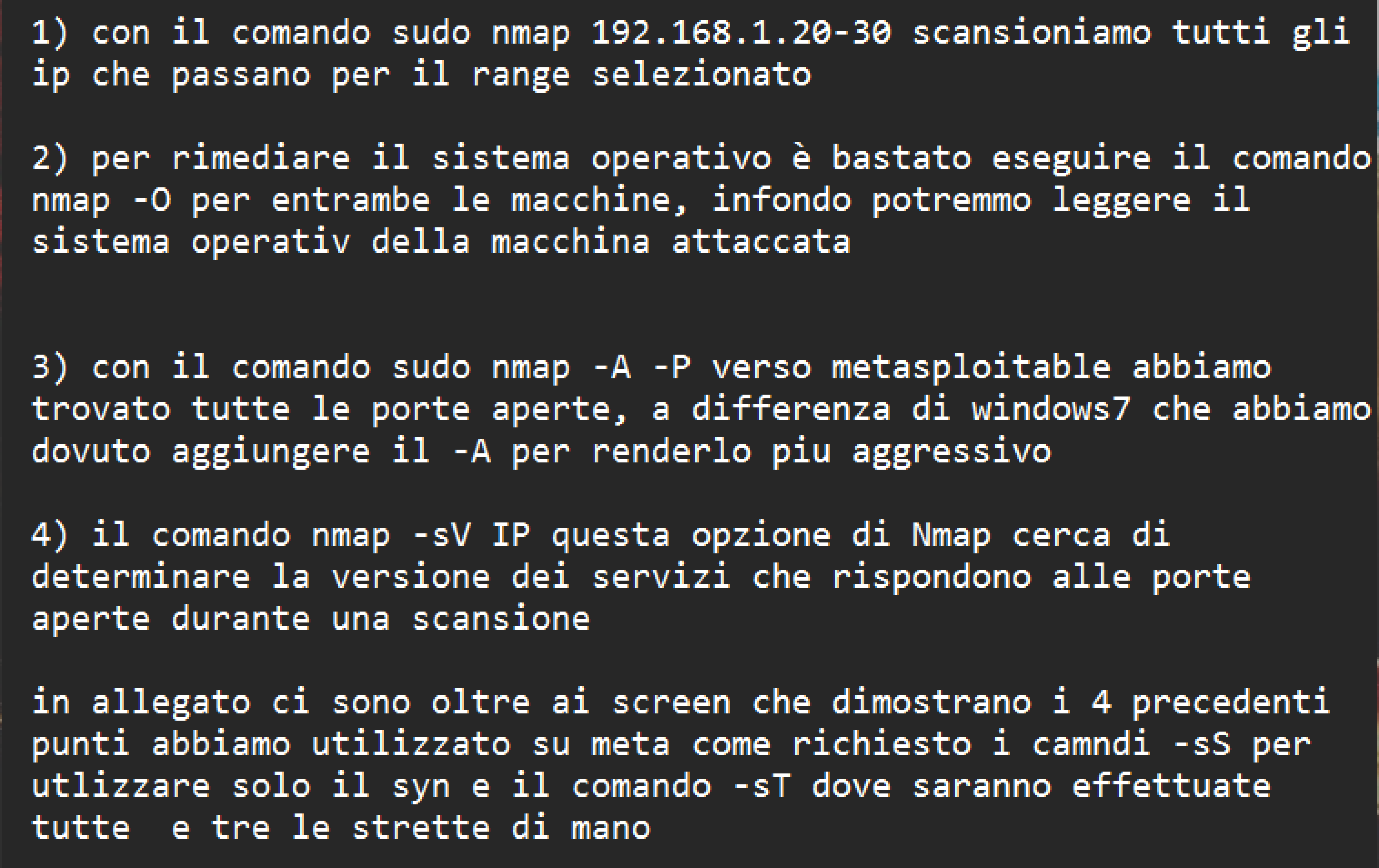


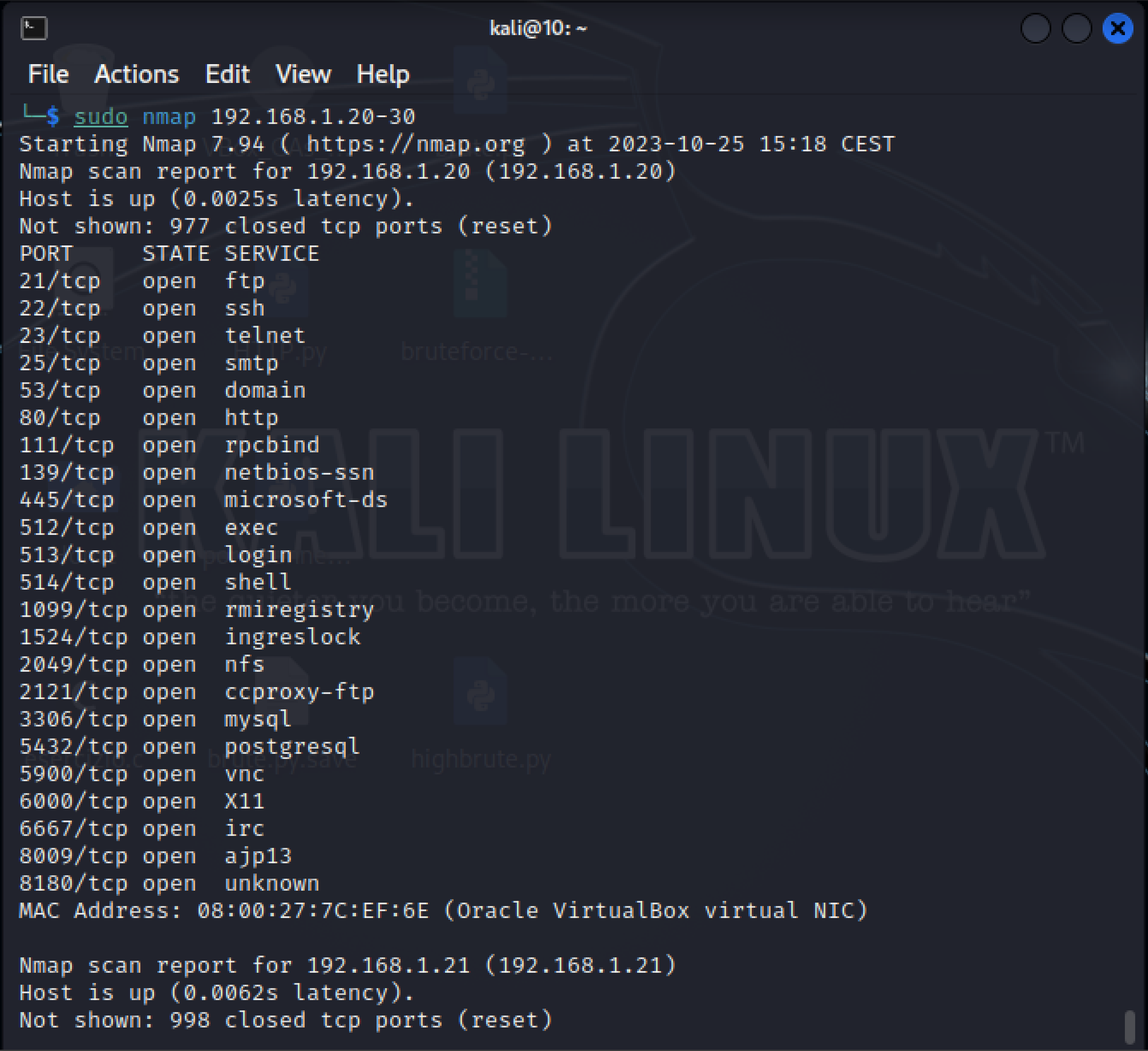
1) con il comando sudo nmap 192.168.1.20-30 scansioniamo tutti gli ip che passano per il range selezionato

2) per rimediare il sistema operativo è bastato eseguire il comando nmap -O per entrambe le macchine, infondo potremmo leggere il sistema operativ della macchina attaccata

3) con il comando sudo nmap -A -P verso metasploitable abbiamo trovato tutte le porte aperte, a differenza di windows7 che abbiamo dovuto aggiungere il -A per renderlo piu aggressivo

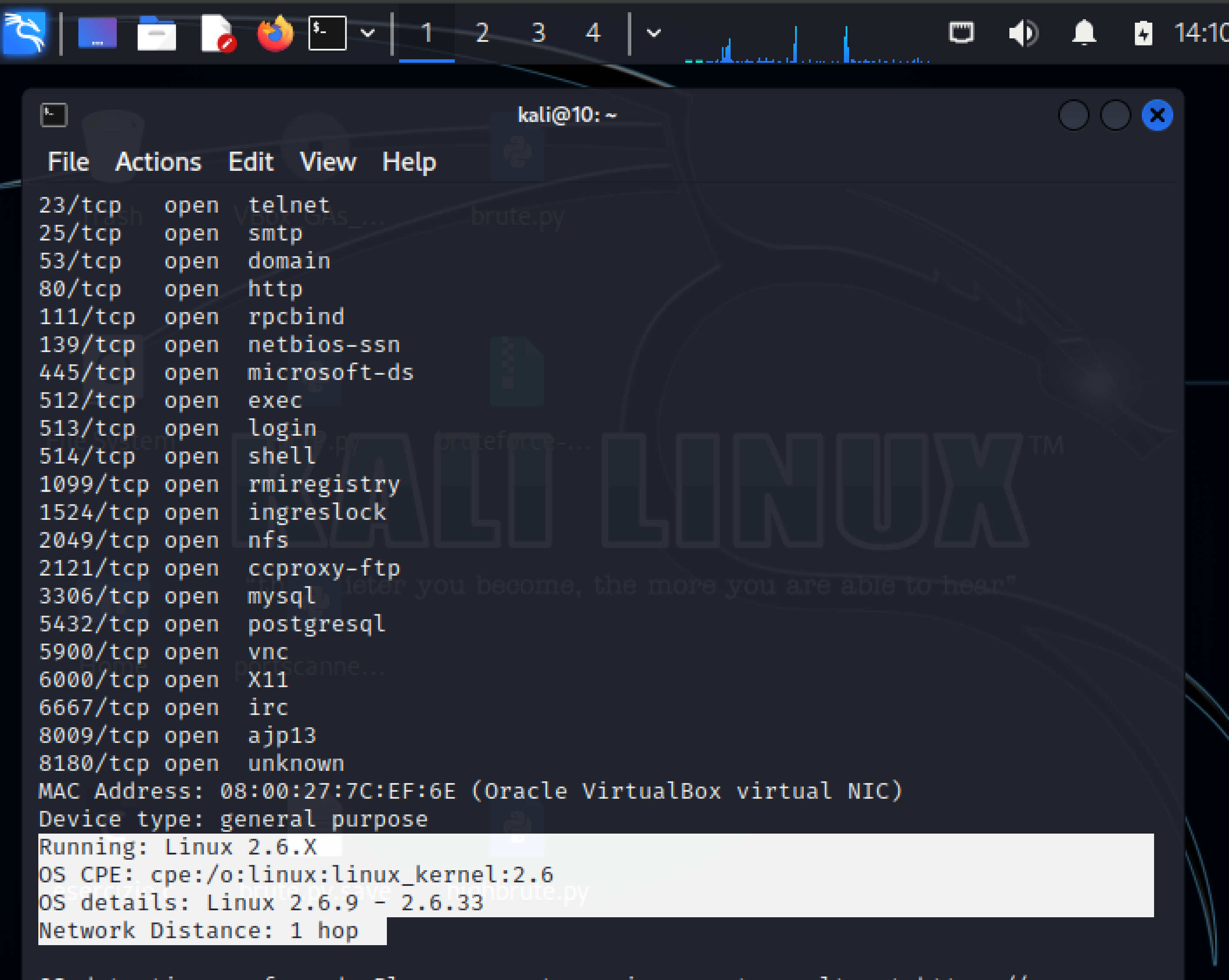
4) il comando nmap -sV IP questa opzione di Nmap cerca di determinare la versione dei servizi che rispondono alle porte aperte durante una scansione

in allegato ci sono oltre ai screen che dimostrano i 4 precedenti punti abbiamo utilizzato su meta come richiesto i camndi -sS per utlizzare solo il syn e il comando -sT dove saranno effettuate tutte e tre le strette di mano

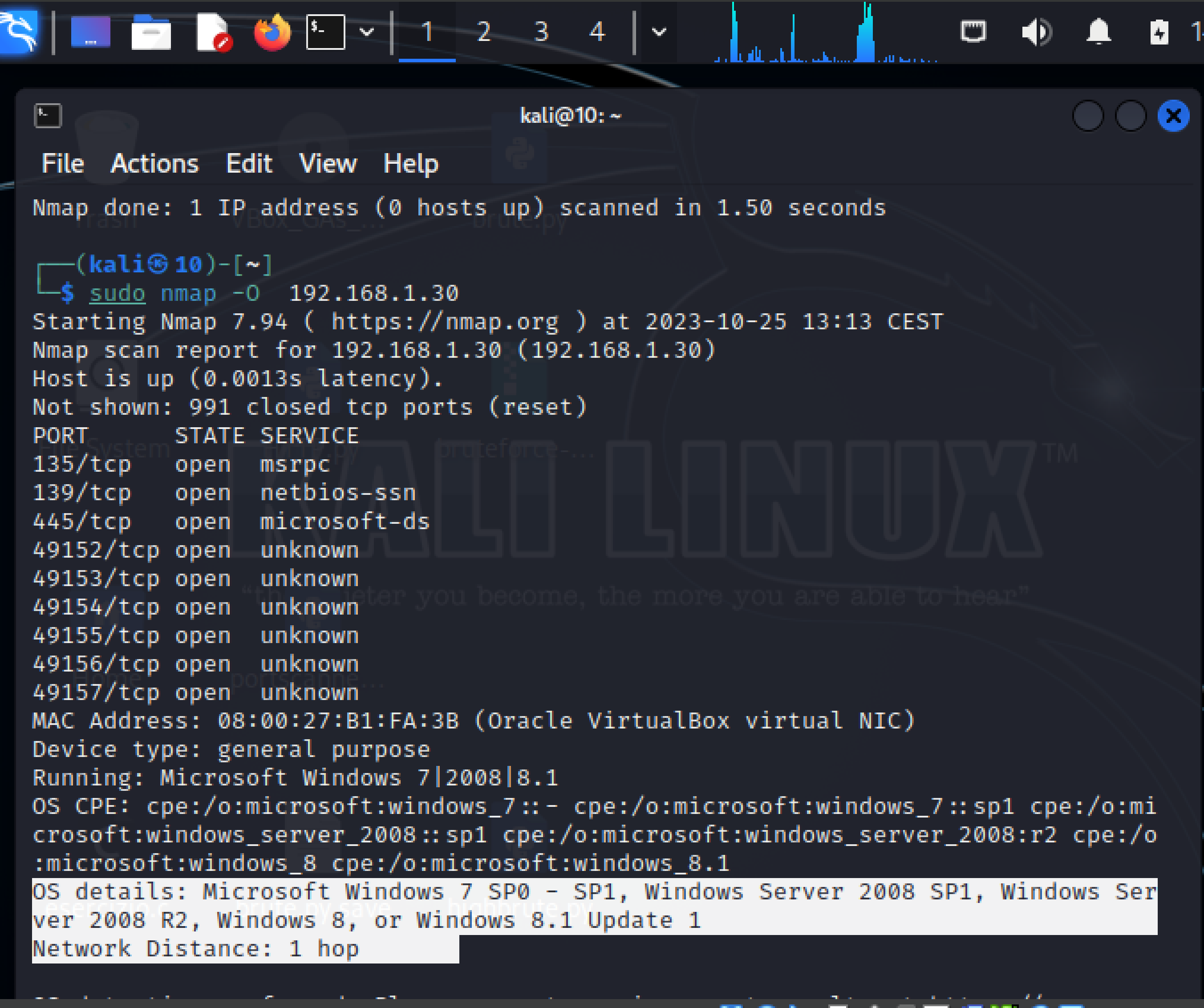


```
└─$ sudo nmap 192.168.1.20-30
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:18 CEST
Nmap scan report for 192.168.1.20 (192.168.1.20)
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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: 08:00:27:7C:EF:6E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.21 (192.168.1.21)
Host is up (0.0062s latency).
Not shown: 998 closed tcp ports (reset)
```

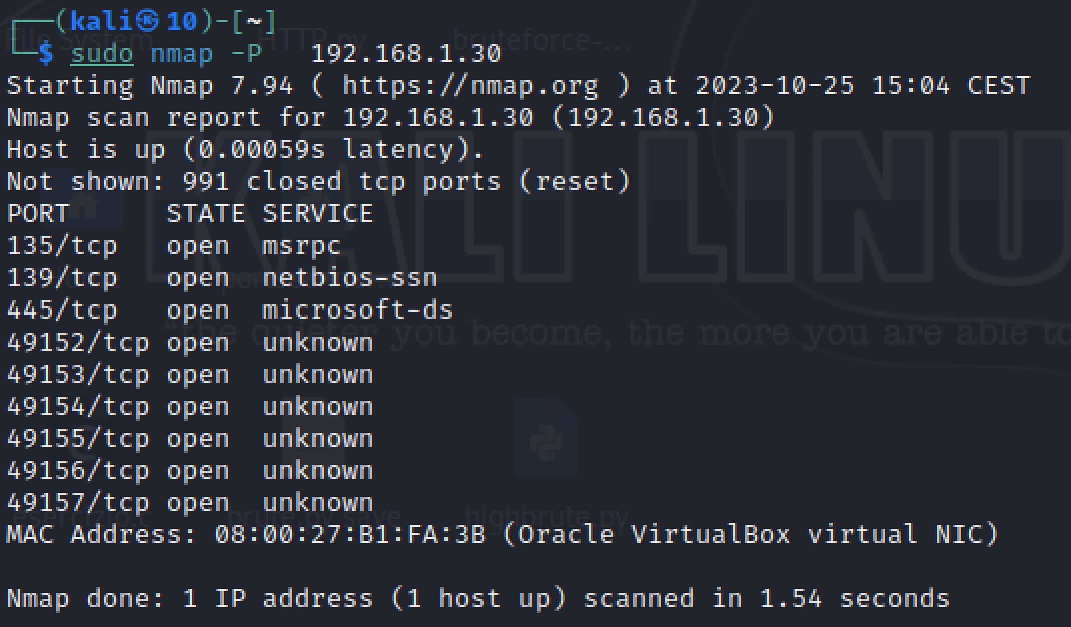


```
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp 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: 08:00:27:7C:EF:6E (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
```



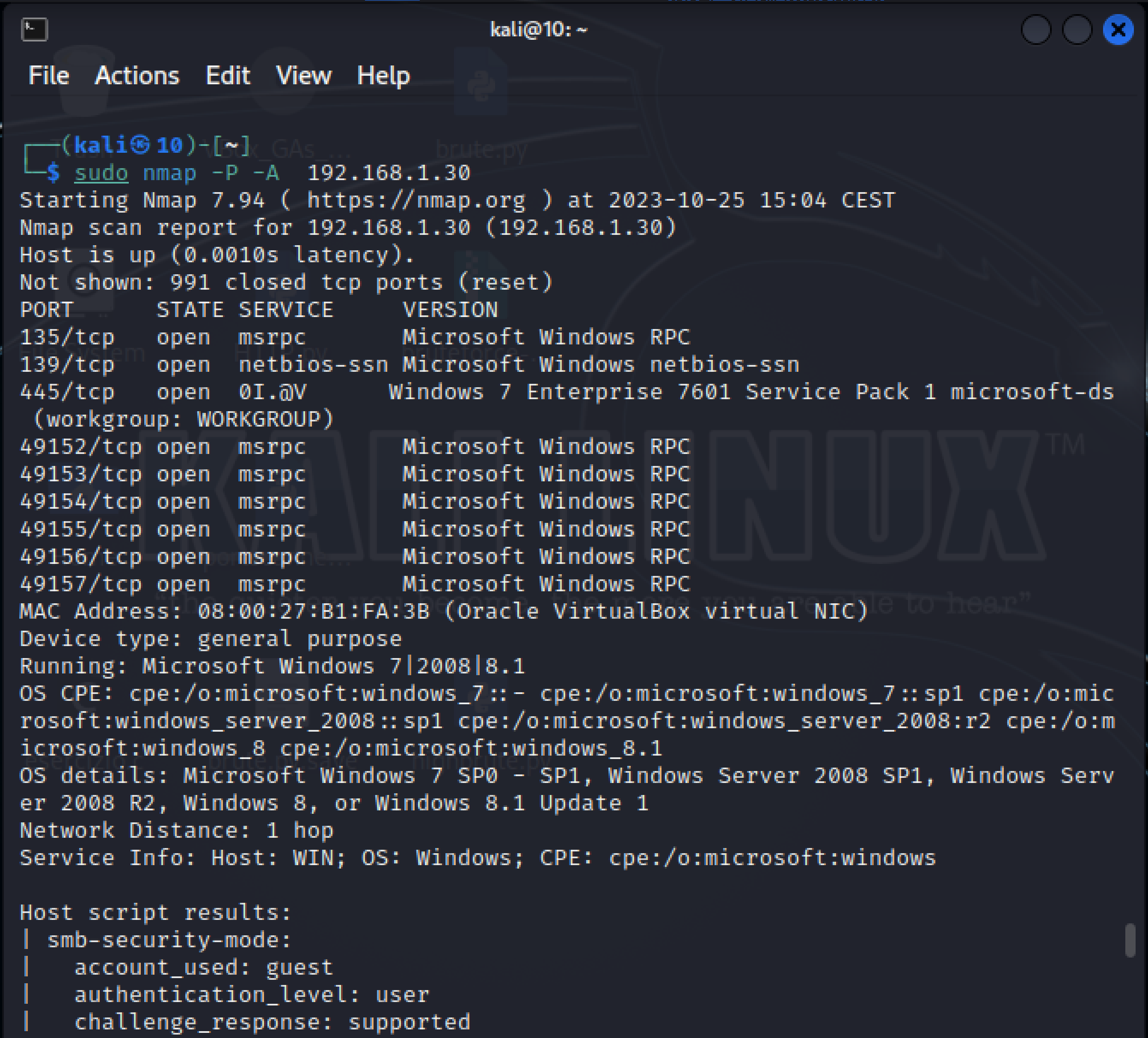
```
Nmap done: 1 IP address (0 hosts up) scanned in 1.50 seconds

┌──(kali㉿10)-[~]
└─$ sudo nmap -O  192.168.1.30
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 13:13 CEST
Nmap scan report for 192.168.1.30 (192.168.1.30)
Host is up (0.0013s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:B1:FA:3B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:mi
crosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o
:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Ser
ver 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
```



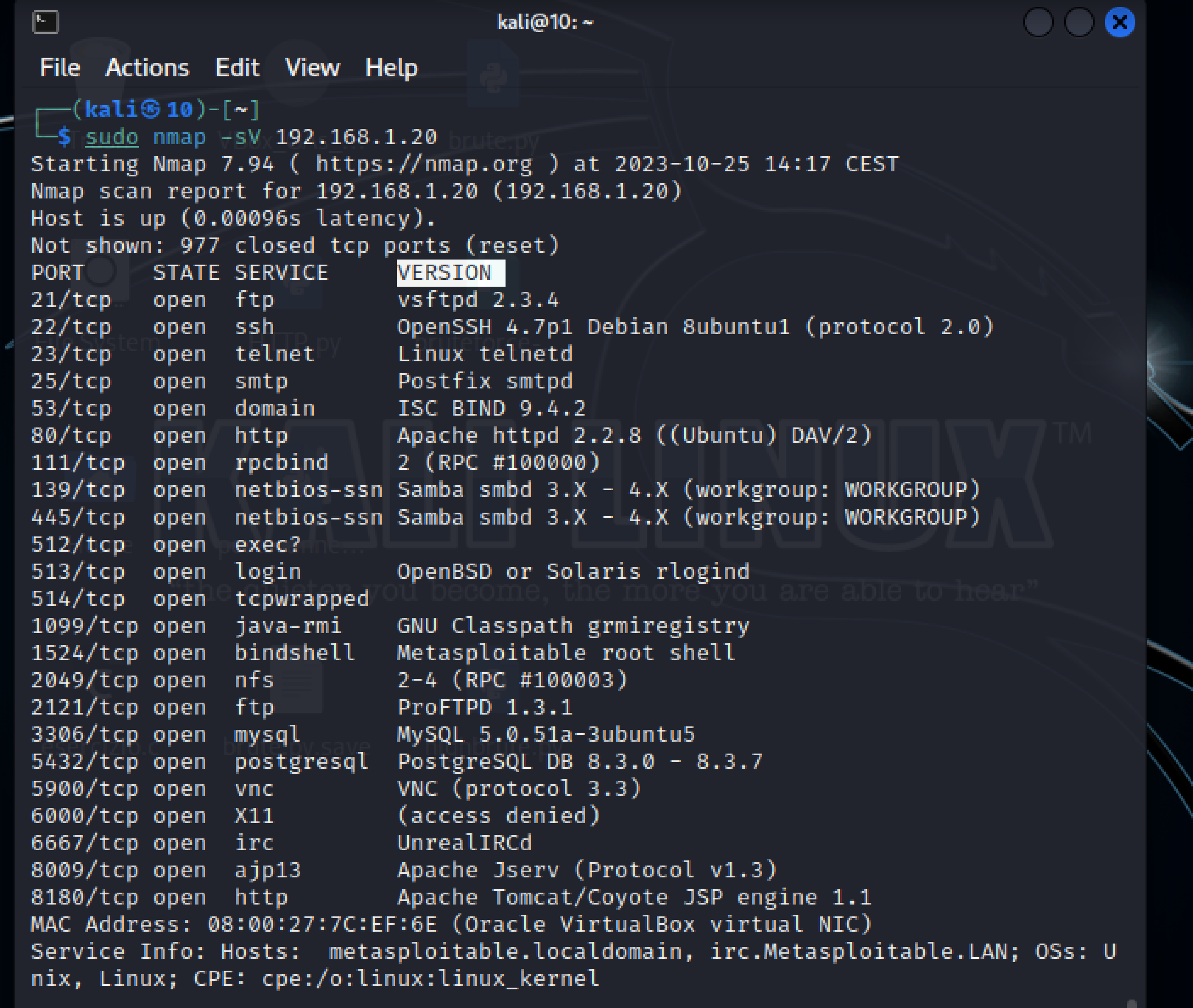
```
┌──(kali㉿10)-[~]
└─$ sudo nmap -P   192.168.1.30
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:04 CEST
Nmap scan report for 192.168.1.30 (192.168.1.30)
Host is up (0.00059s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:B1:FA:3B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

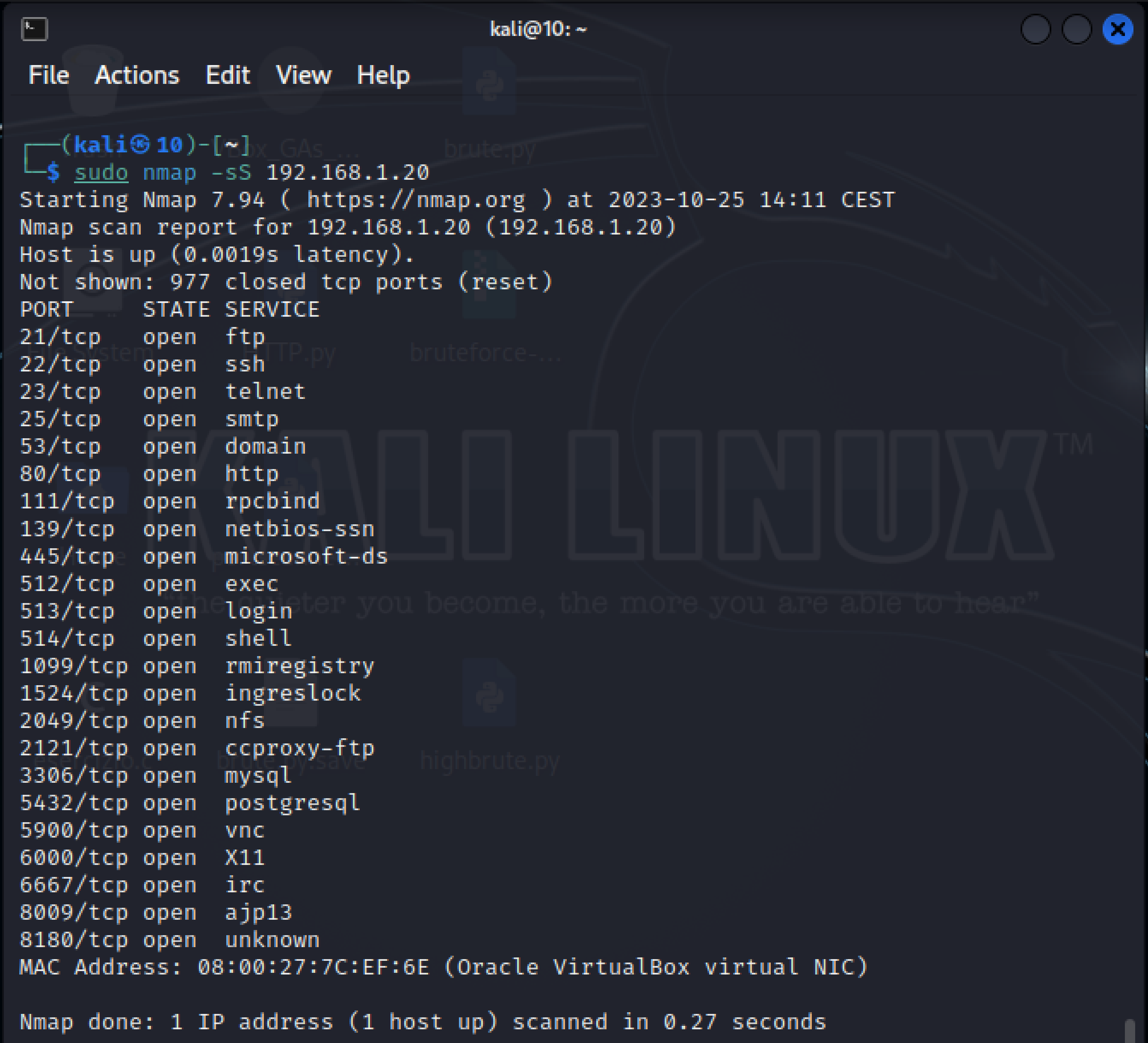


```
┌──(kali㉿10)-[~]
└─$ sudo nmap -P -A  192.168.1.30
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:04 CEST
Nmap scan report for 192.168.1.30 (192.168.1.30)
Host is up (0.0010s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  0I.@V      Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds
 (workgroup: WORKGROUP)
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49156/tcp open  msrpc       Microsoft Windows RPC
49157/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 08:00:27:B1:FA:3B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:mic
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:m
icrosoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Serv
er 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

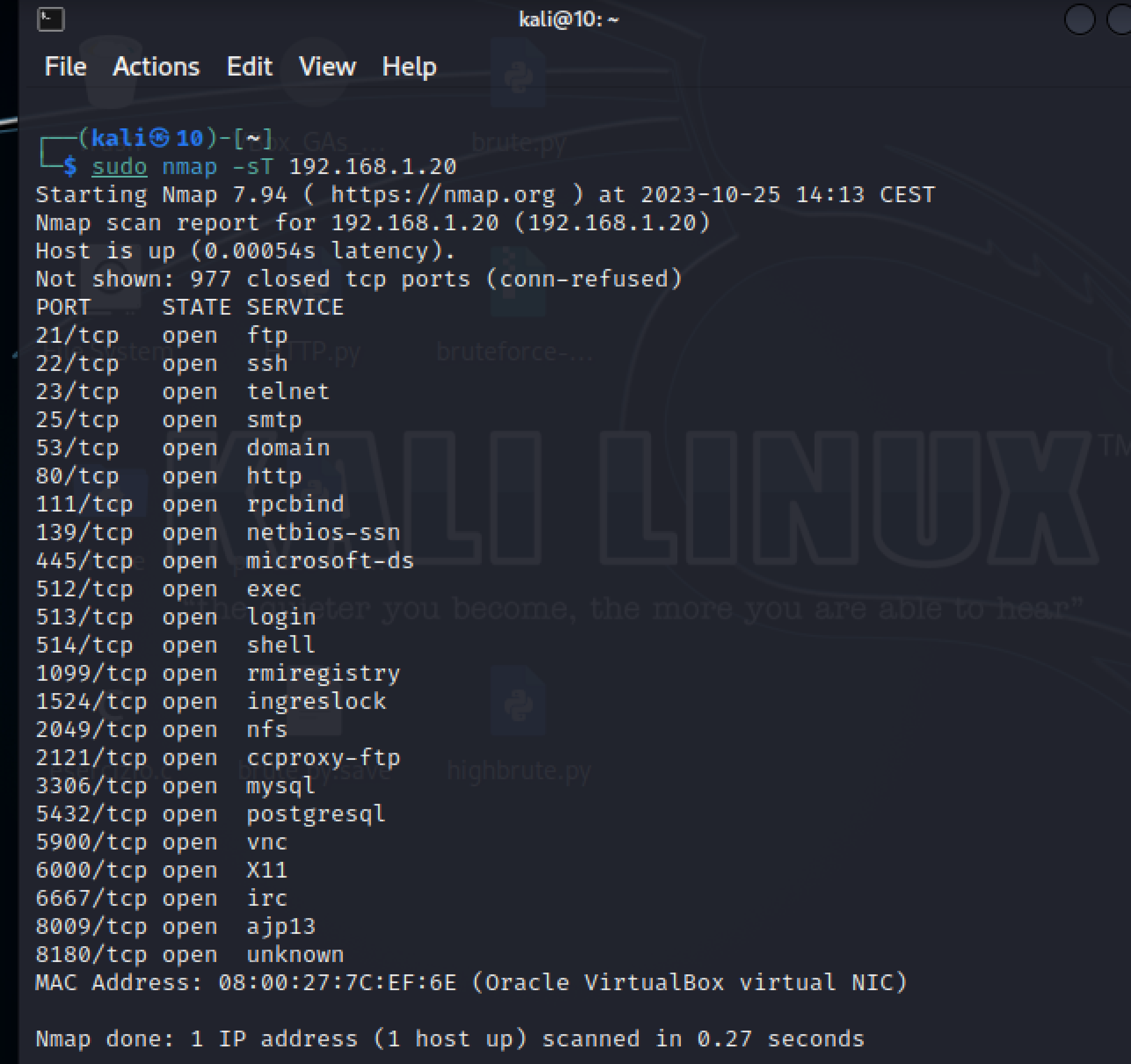


```
┌──(kali㉿10)-[~]
└─$ sudo nmap -sV 192.168.1.20
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:17 CEST
Nmap scan report for 192.168.1.20 (192.168.1.20)
Host is up (0.00096s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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: 08:00:27:7C:EF:6E (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: U
nix, Linux; CPE: cpe:/o:linux:linux_kernel
```



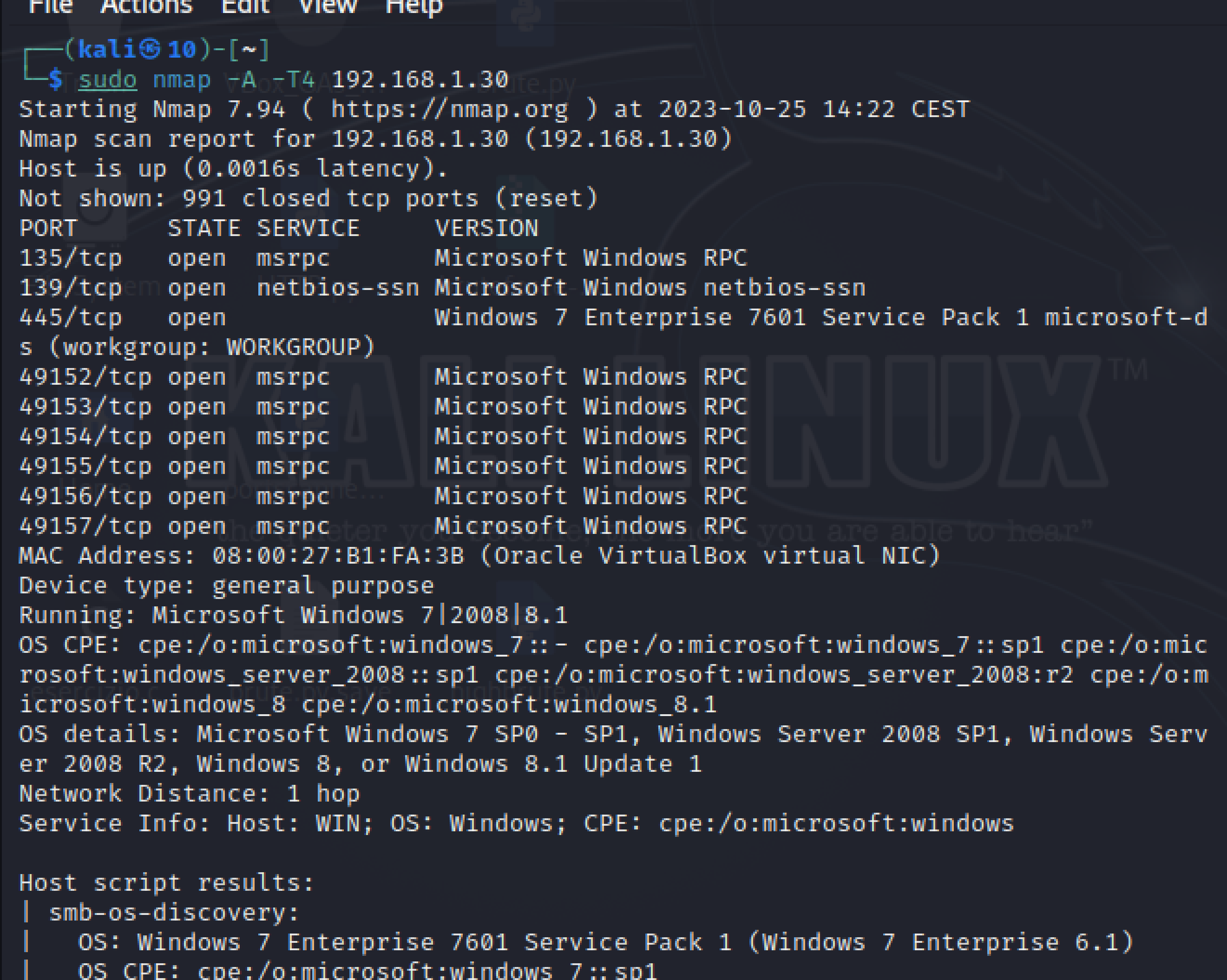
```
┌──(kali㉿10)-[~]
└─$ sudo nmap -sS 192.168.1.20
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:11 CEST
Nmap scan report for 192.168.1.20 (192.168.1.20)
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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: 08:00:27:7C:EF:6E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```



```
┌──(kali㉿10)-[~]
└─$ sudo nmap -sT 192.168.1.20
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:13 CEST
Nmap scan report for 192.168.1.20 (192.168.1.20)
Host is up (0.00054s 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: 08:00:27:7C:EF:6E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```



```
┌──(kali㉿10)-[~]
└─$ sudo nmap -A -T4 192.168.1.30
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:22 CEST
Nmap scan report for 192.168.1.30 (192.168.1.30)
Host is up (0.0016s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open              Windows 7 Enterprise 7601 Service Pack 1 microsoft-d
s (workgroup: WORKGROUP)
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49156/tcp open  msrpc       Microsoft Windows RPC
49157/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 08:00:27:B1:FA:3B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:mic
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:m
icrosoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Serv
er 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
```