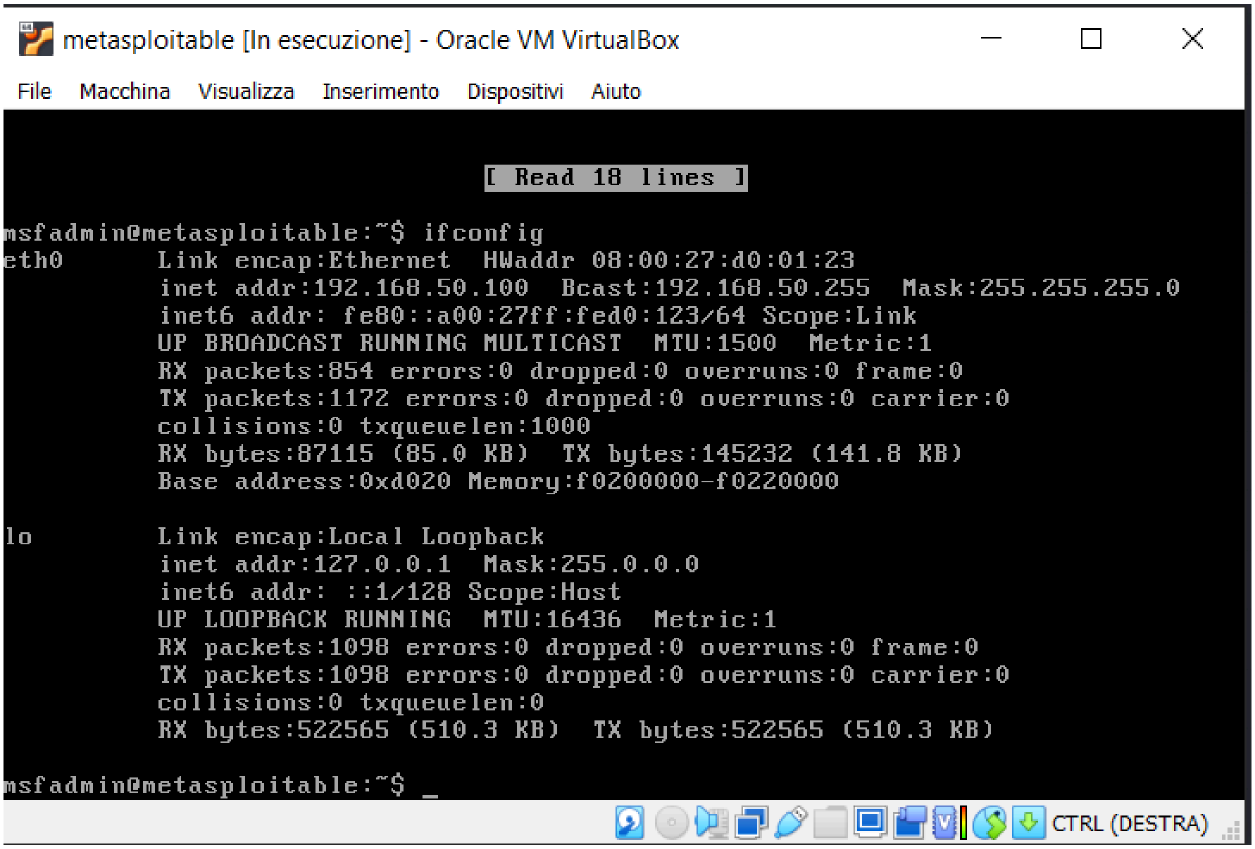
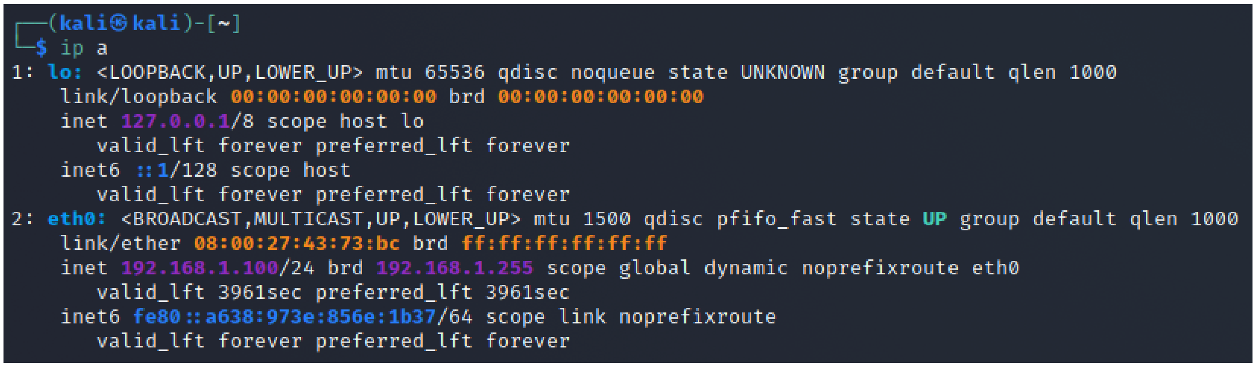
Macchina target e attaccante su reti diverse

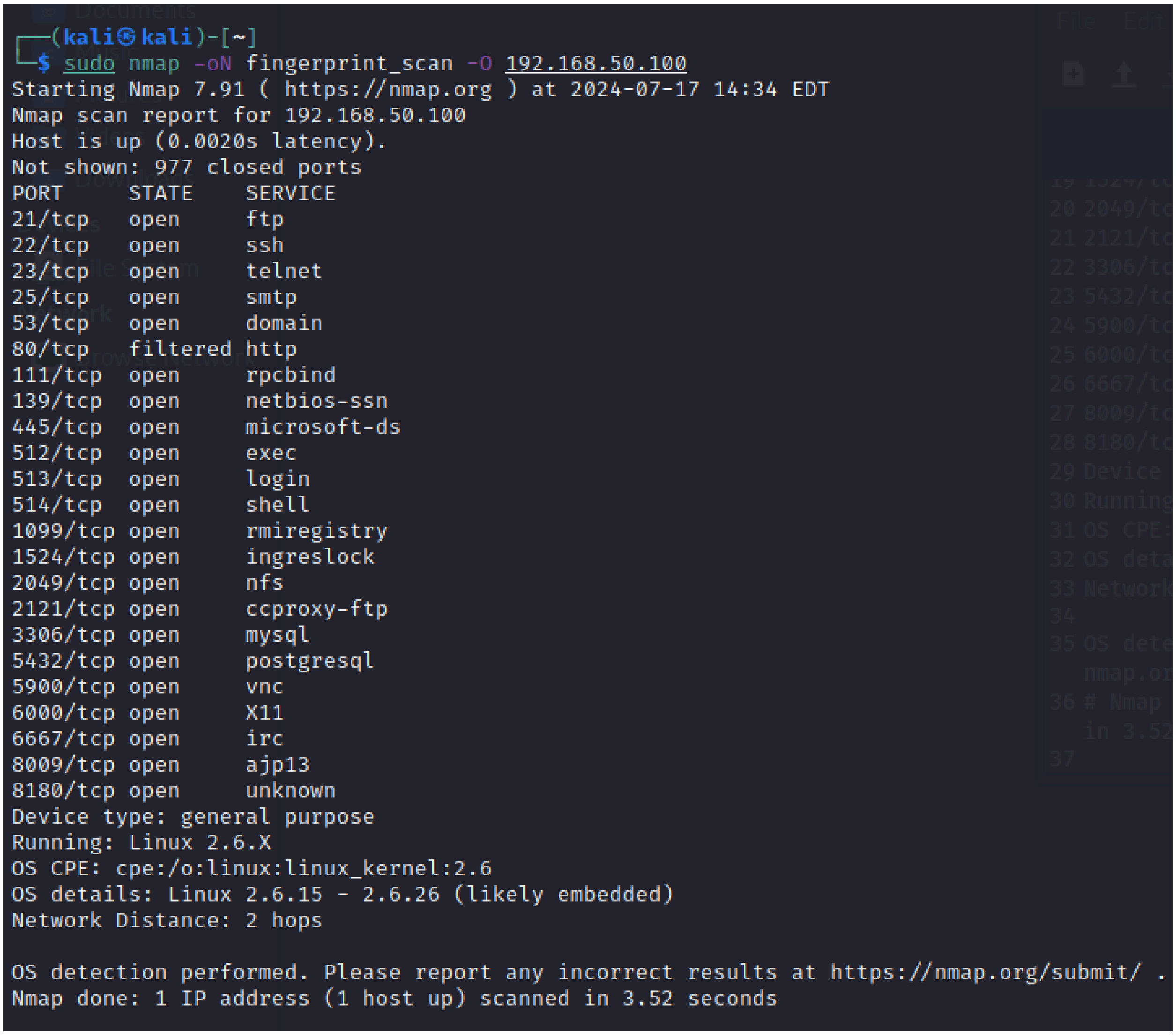


```
                          [ Read 18 lines ]

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d0:01:23
          inet addr:192.168.50.100  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed0:123/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:854 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:87115 (85.0 KB)  TX bytes:145232 (141.8 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:1098 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1098 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:522565 (510.3 KB)  TX bytes:522565 (510.3 KB)

msfadmin@metasploitable:~$ _
```

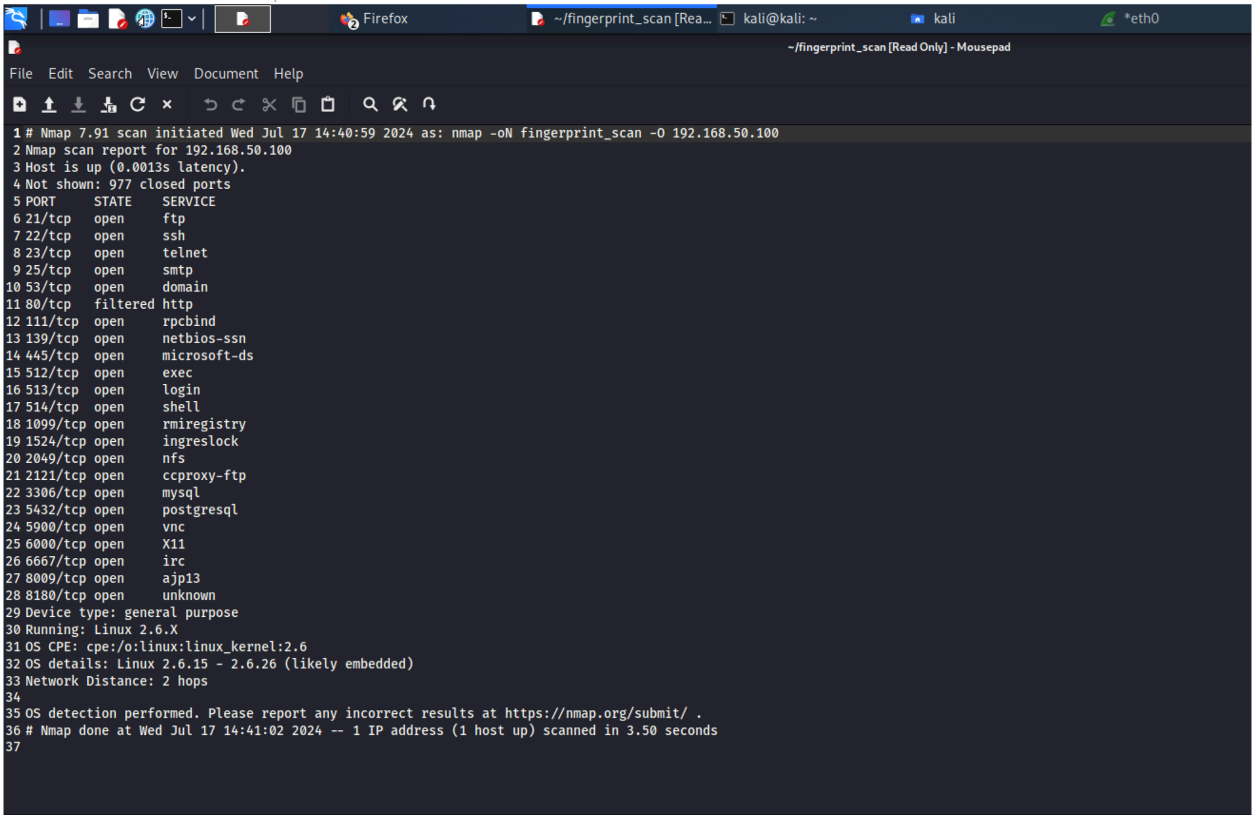


```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:43:73:bc brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 3961sec preferred_lft 3961sec
    inet6 fe80::a638:973e:856e:1b37/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

OS fingerprint con output in formato normale:



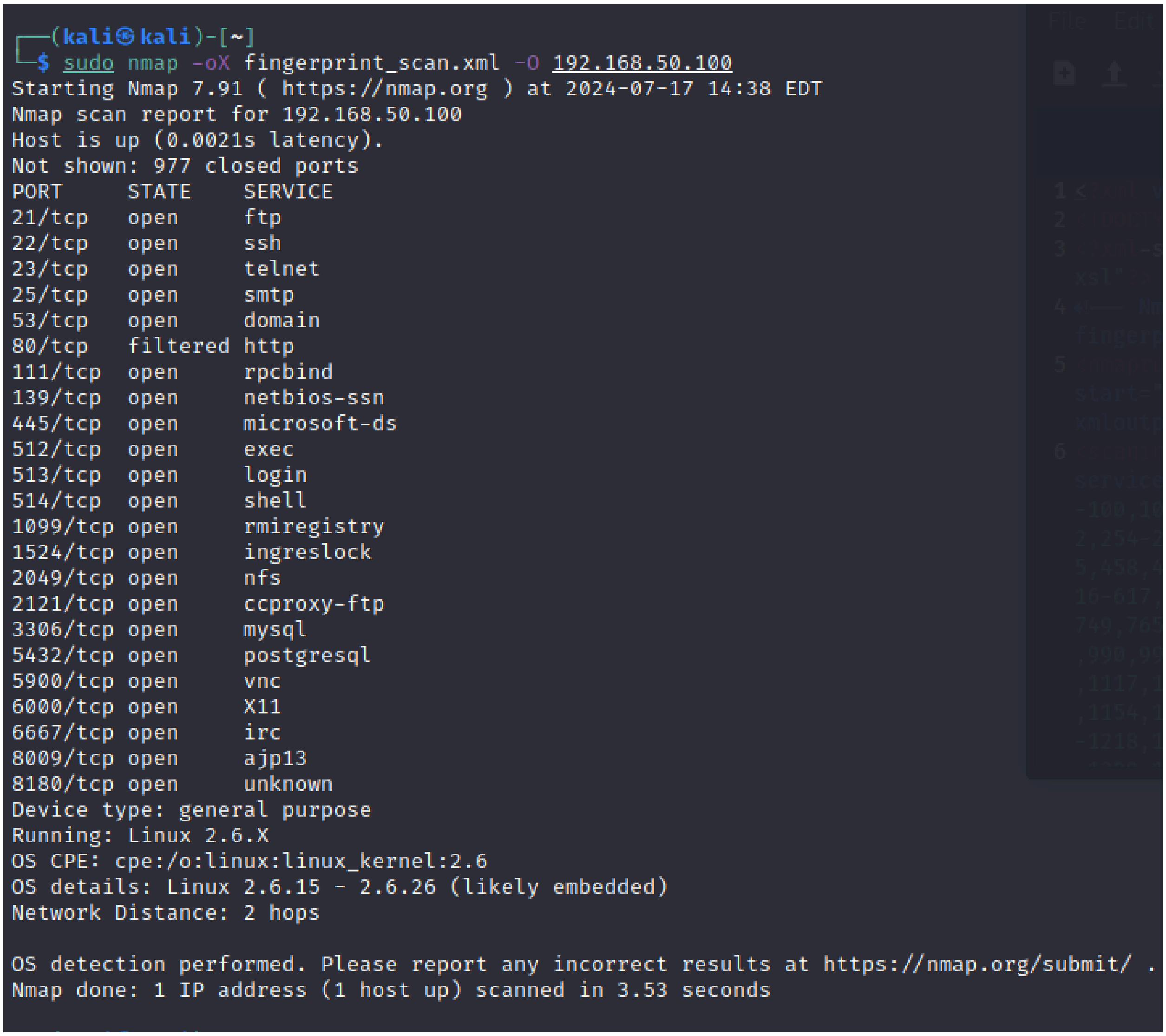
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -oN fingerprint_scan -O 192.168.50.100
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-17 14:34 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0020s latency).
Not shown: 977 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.52 seconds
```



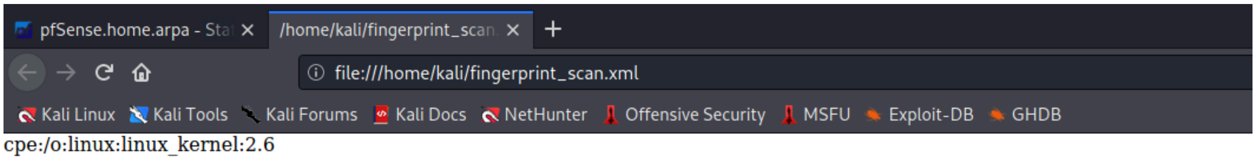
Firefox
~/fingerprint_scan [Rea...
kali@kali: ~
kali
*eth0
~/fingerprint_scan [Read Only] - Mousepad
File
Edit
Search
View
Document
Help

```
# Nmap 7.91 scan initiated Wed Jul 17 14:40:59 2024 as: nmap -oN fingerprint_scan -O 192.168.50.100
Nmap scan report for 192.168.50.100
Host is up (0.0013s latency).
Not shown: 977 closed ports
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   filtered 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jul 17 14:41:02 2024 -- 1 IP address (1 host up) scanned in 3.50 seconds
```

OS fingerprint scan in formato xml:

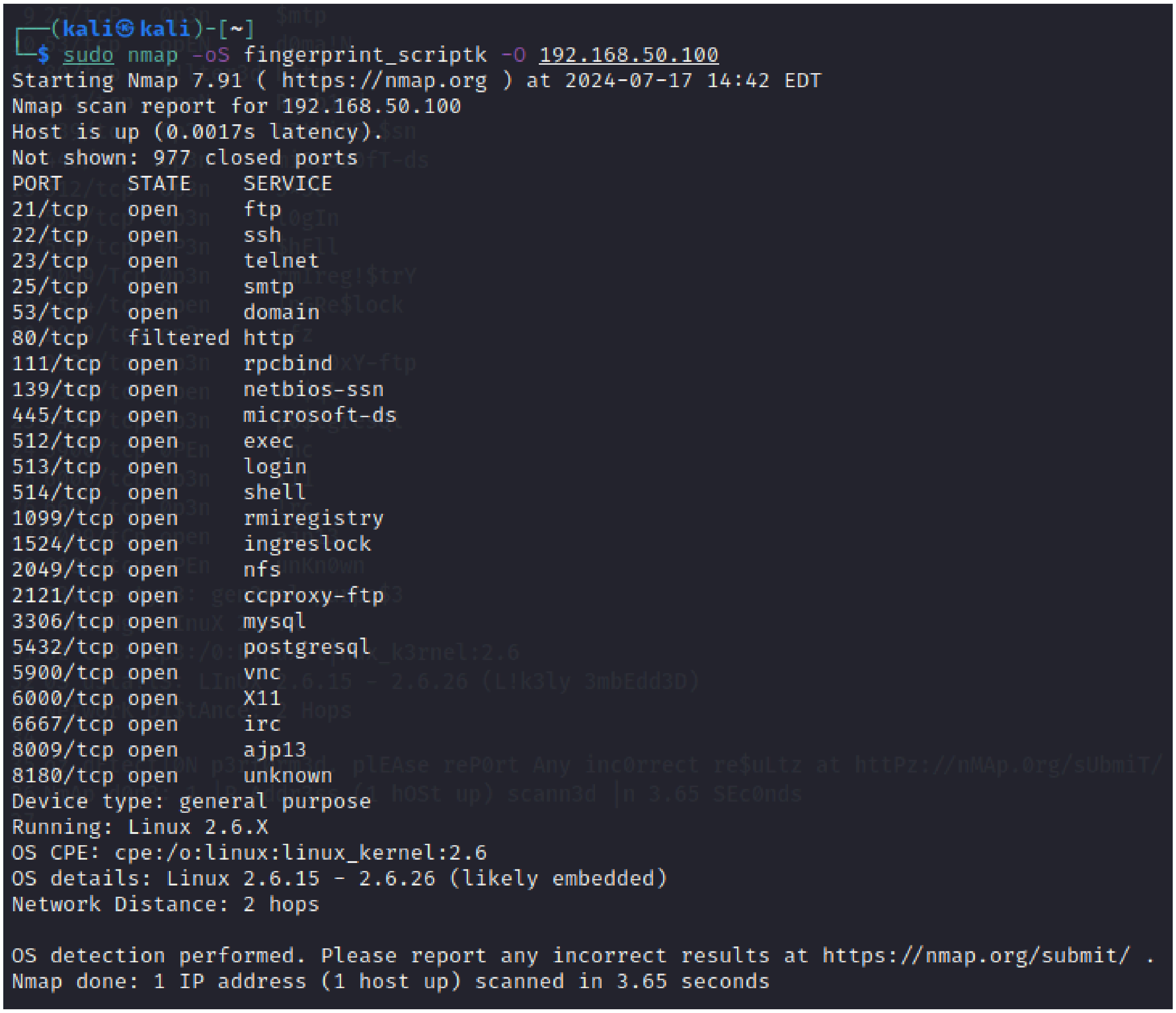


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -oX fingerprint_scan.xml -O 192.168.50.100
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-17 14:38 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0021s latency).
Not shown: 977 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.53 seconds
```

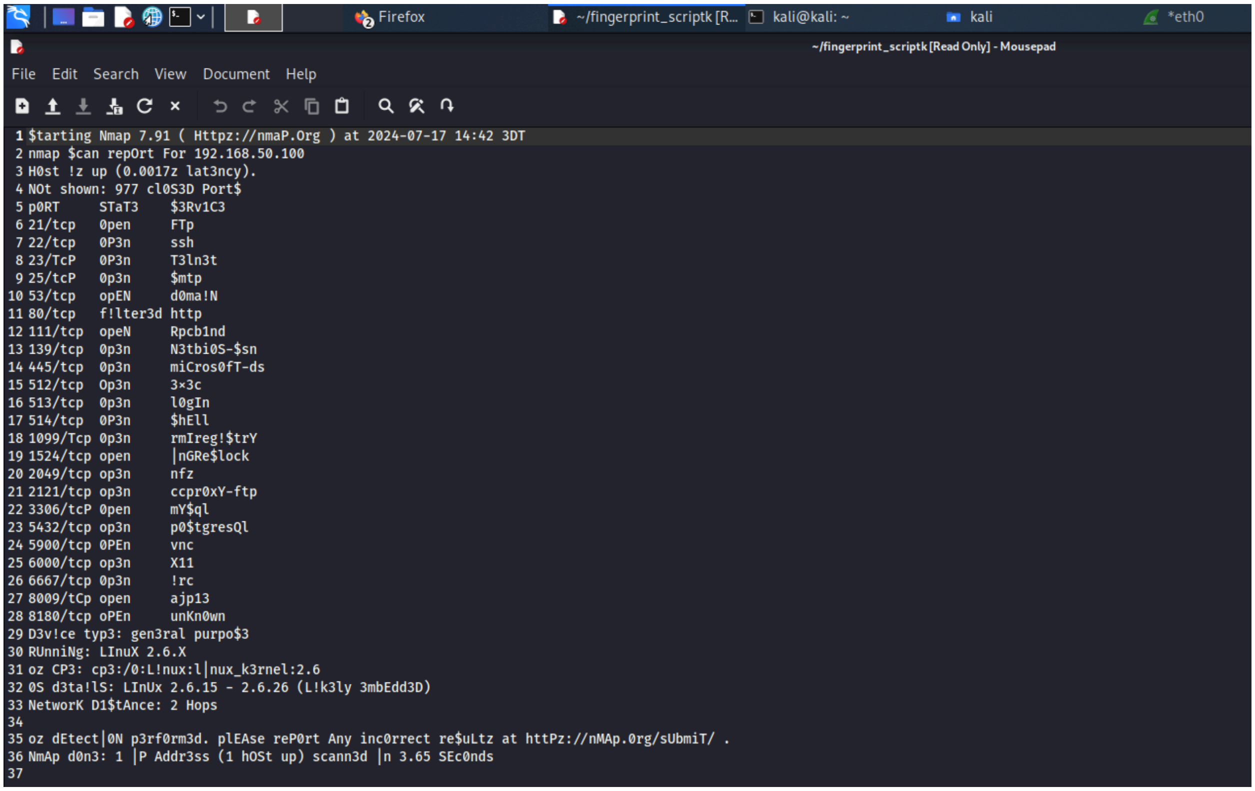


```
cpe:/o:linux:linux_kernel:2.6
```

OS fingerprint con output in formato s|<rlpt klddi3:

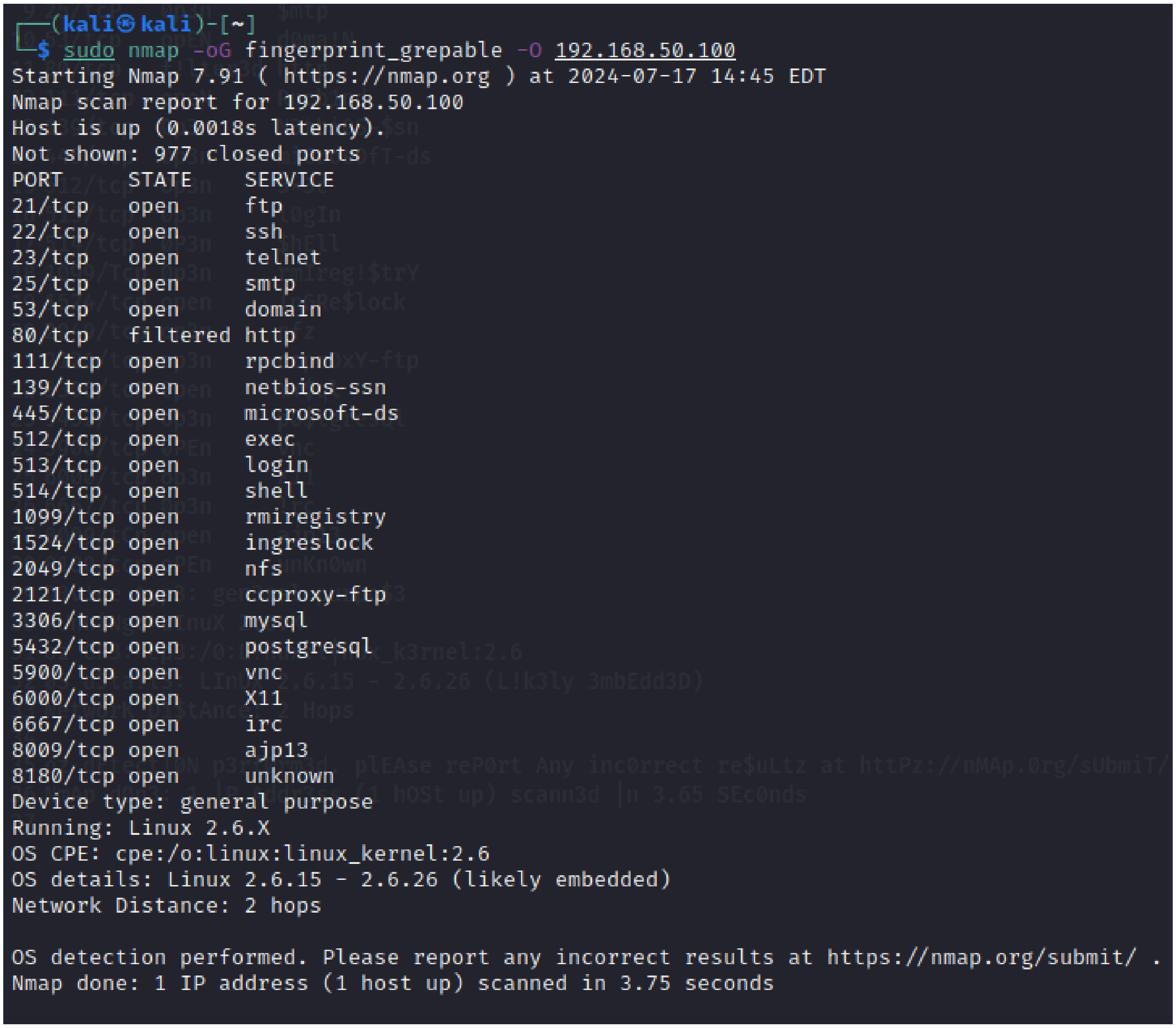


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -oS fingerprint_scriptk -O 192.168.50.100
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-17 14:42 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0017s latency).
Not shown: 977 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.65 seconds
```

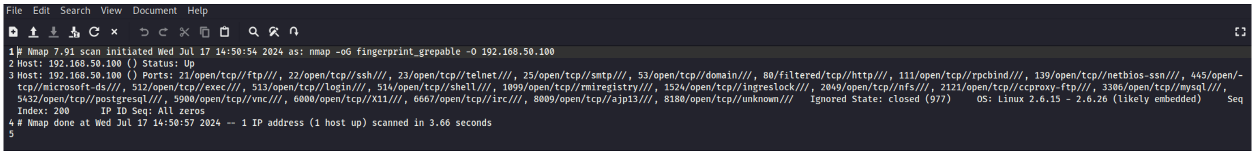

Firefox
~/fingerprint_scriptk [R...
kali@kali: ~
kali
*eth0
~/fingerprint_scriptk [Read Only] - Mousepad
File
Edit
Search
View
Document
Help

```
$tarting Nmap 7.91 ( Httpz://nmaP.Org ) at 2024-07-17 14:42 3DT
nmap $can repOrt For 192.168.50.100
H0st !z up (0.0017z lat3ncy).
NOt shown: 977 cl0S3D Port$
p0RT     STaT3    $3Rv1C3
21/tcp   0pen     FTp
22/tcp   0P3n     ssh
23/TcP   0P3n     T3ln3t
25/tcP   0p3n     $mtp
53/tcp   opEN     d0ma!N
80/tcp   f!lter3d http
111/tcp  opeN     Rpcb1nd
139/tcp  0p3n     N3tbi0S-$sn
445/tcp  0p3n     miCros0fT-ds
512/tcp  Op3n     3×3c
513/tcp  0p3n     l0gIn
514/tcp  0P3n     $hEll
1099/Tcp 0p3n     rmIreg!$trY
1524/tcp open     |nGRe$lock
2049/tcp op3n     nfz
2121/tcp op3n     ccpr0xY-ftp
3306/tcP 0pen     mY$ql
5432/tcp op3n     p0$tgresQl
5900/tcp 0PEn     vnc
6000/tcp op3n     X11
6667/tcp 0p3n     !rc
8009/tCp open     ajp13
8180/tcp oPEn     unKn0wn
D3v!ce typ3: gen3ral purpo$3
RUnniNg: LInuX 2.6.X
oz CP3: cp3:/0:L!nux:l|nux_k3rnel:2.6
0S d3ta!lS: LInUx 2.6.15 - 2.6.26 (L!k3ly 3mbEdd3D)
NetworK D1$tAnce: 2 Hops

oz dEtect|0N p3rf0rm3d. plEAse reP0rt Any inc0rrect re$uLtz at httPz://nMAp.0rg/sUbmiT/ .
NmAp d0n3: 1 |P Addr3ss (1 hOSt up) scann3d |n 3.65 SEc0nds

```

OS fingerprint con output in formato grepable:

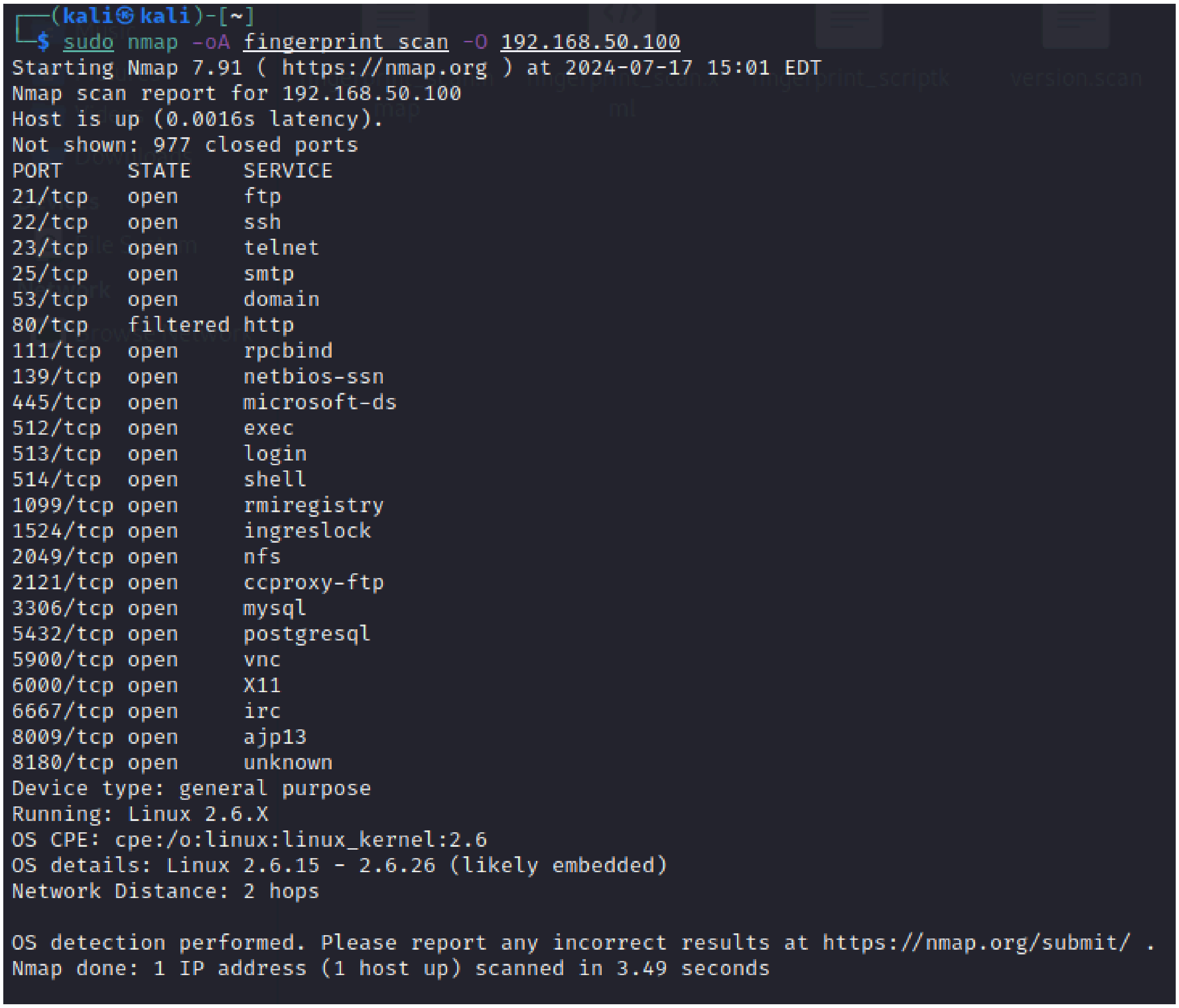


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -oG fingerprint_grepable -O 192.168.50.100
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-17 14:45 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0018s latency).
Not shown: 977 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.75 seconds
```



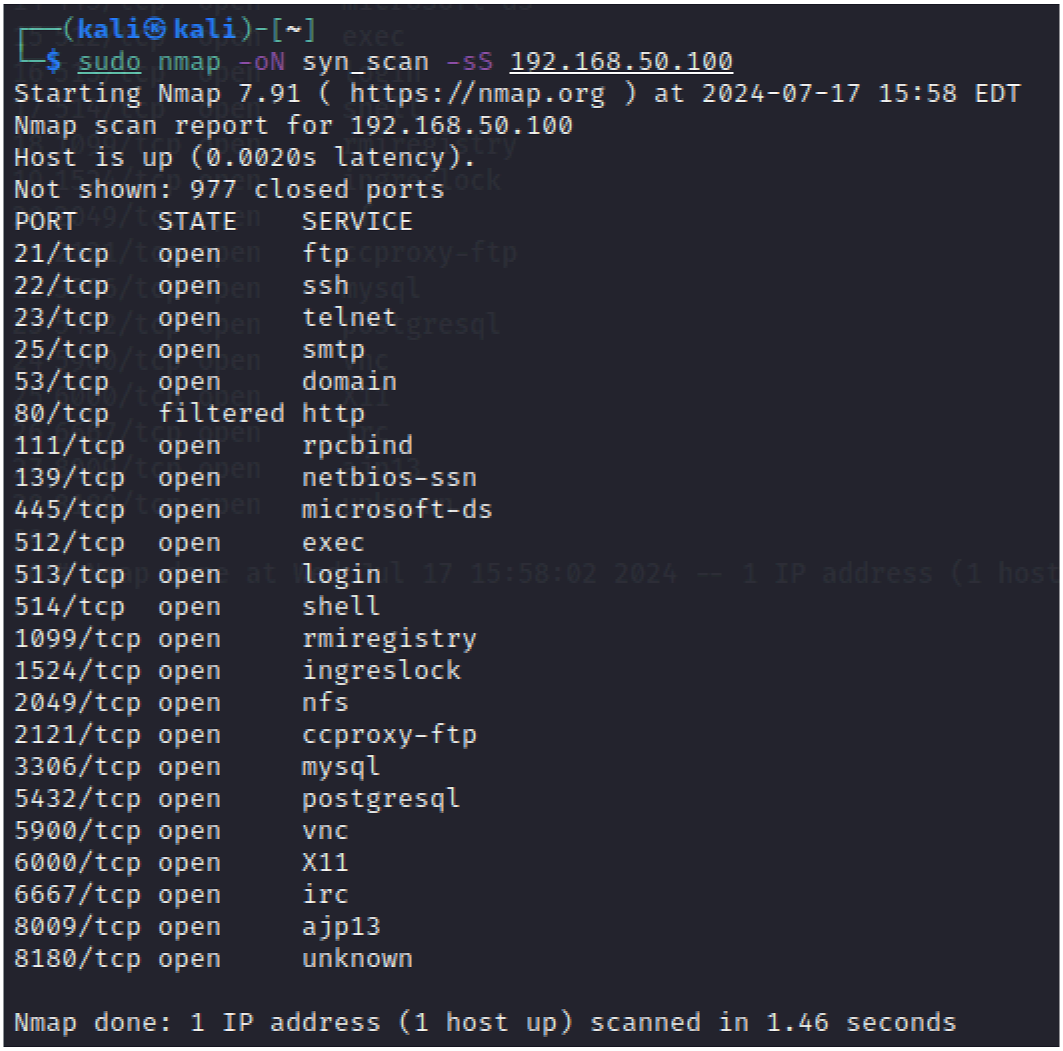
```
# Nmap 7.91 scan initiated Wed Jul 17 14:50:54 2024 as: nmap -oG fingerprint_grepable -O 192.168.50.100
Host: 192.168.50.100 () Status: Up
Host: 192.168.50.100 () Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///, 23/open/tcp//telnet///, 25/open/tcp//smtp///, 53/open/tcp//domain///, 80/filtered/tcp//http///, 111/open/tcp//rpcbind///, 139/open/tcp//netbios-ssn///, 445/open/-
tcp//microsoft-ds///, 512/open/tcp//exec///, 513/open/tcp//login///, 514/open/tcp//shell///, 1099/open/tcp//rmiregistry///, 1524/open/tcp//ingreslock///, 2049/open/tcp//nfs///, 2121/open/tcp//ccproxy-ftp///, 3306/open/tcp//mysql///,
5432/open/tcp//postgresql///, 5900/open/tcp//vnc///, 6000/open/tcp//X11///, 6667/open/tcp//irc///, 8009/open/tcp//ajp13///, 8180/open/tcp//unknown///   Ignored State: closed (977)    OS: Linux 2.6.15 - 2.6.26 (likely embedded)    Seq
Index: 200      IP ID Seq: All zeros
# Nmap done at Wed Jul 17 14:50:57 2024 -- 1 IP address (1 host up) scanned in 3.66 seconds
```

Lo switch -oA crea file di output nei tre formati più comuni (normale, xml, grepable)

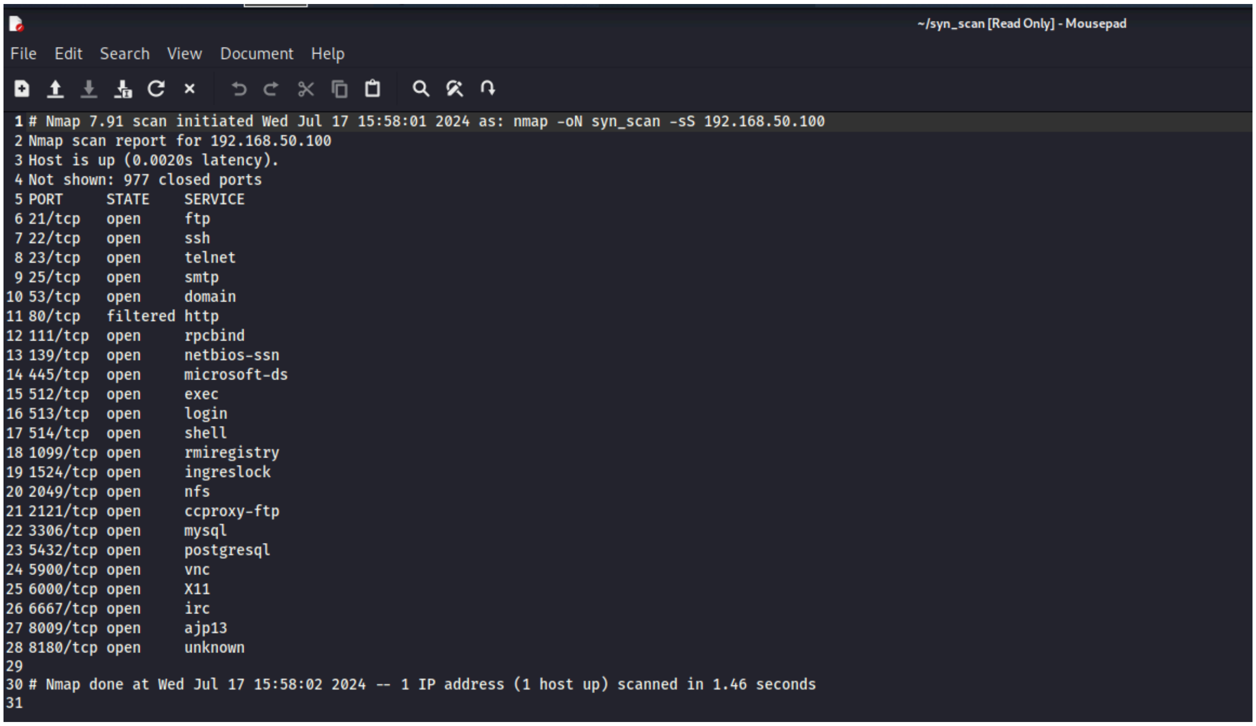


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -oA fingerprint_scan -O 192.168.50.100
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-17 15:01 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0016s latency).
Not shown: 977 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.49 seconds
```

SYN scan con report:

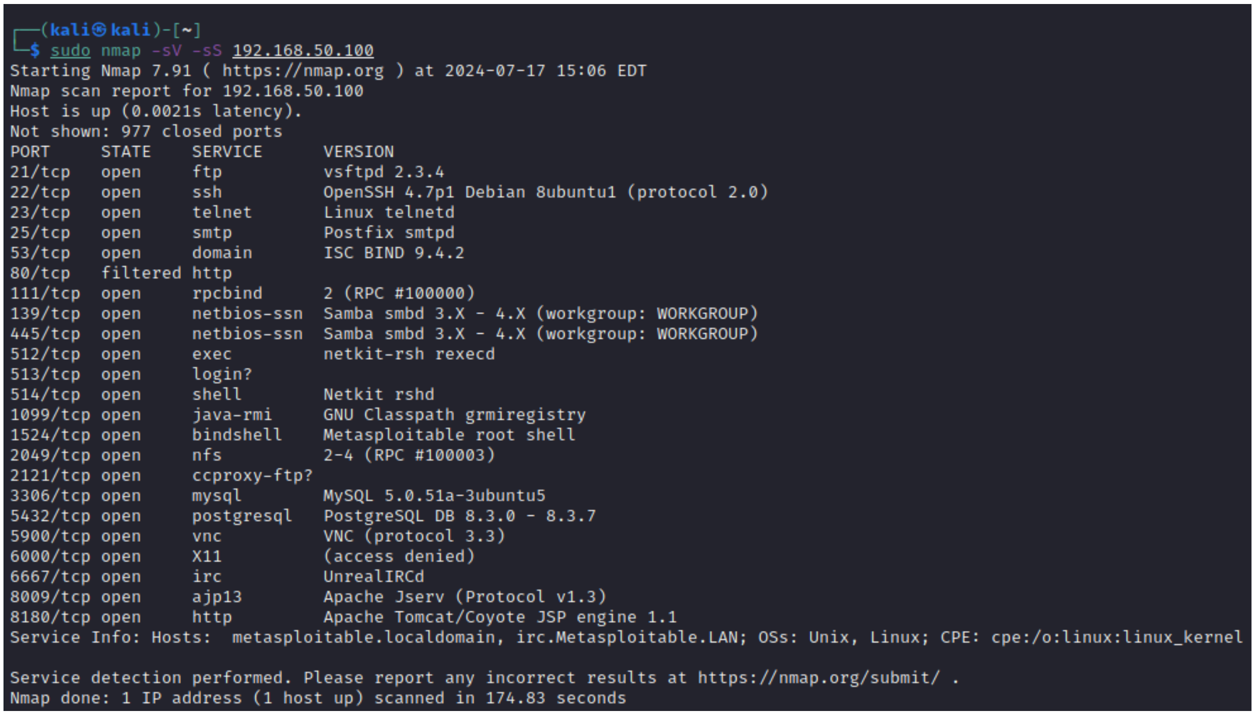


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -oN syn_scan -sS 192.168.50.100
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-17 15:58 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0020s latency).
Not shown: 977 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
```



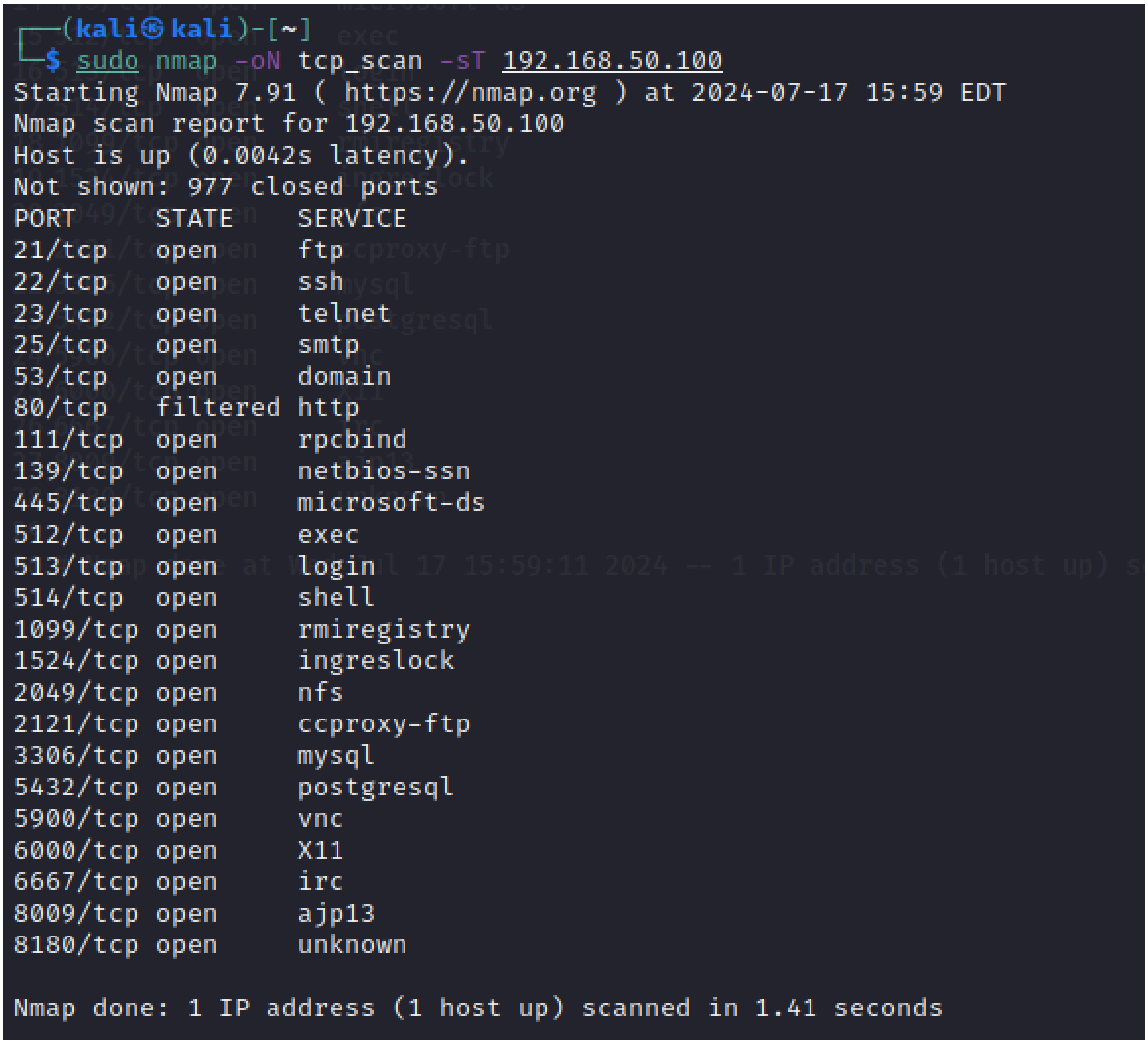
```
# Nmap 7.91 scan initiated Wed Jul 17 15:58:01 2024 as: nmap -oN syn_scan -sS 192.168.50.100
Nmap scan report for 192.168.50.100
Host is up (0.0020s latency).
Not shown: 977 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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

# Nmap done at Wed Jul 17 15:58:02 2024 -- 1 IP address (1 host up) scanned in 1.46 seconds
```

SYN Scan + version detection:

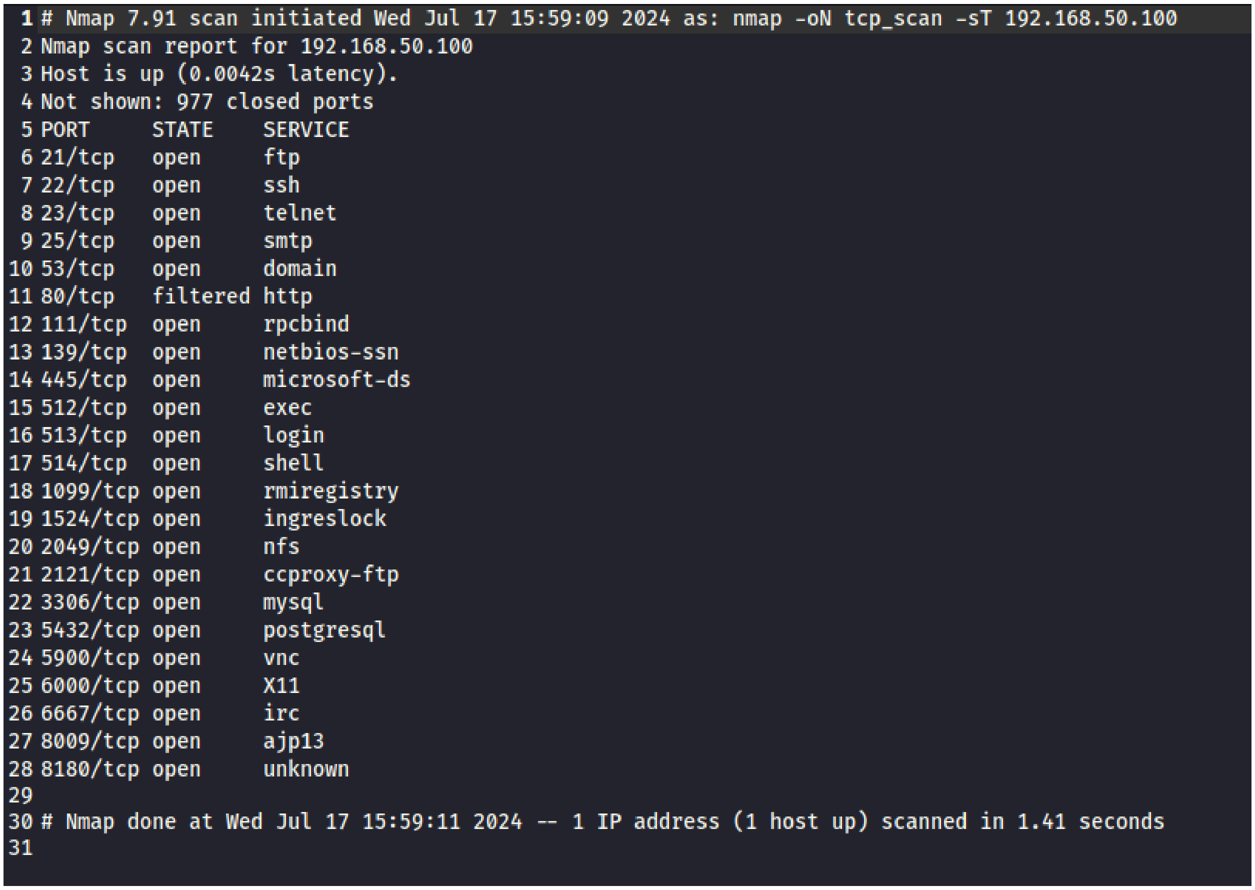


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sS 192.168.50.100
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-17 15:06 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0021s latency).
Not shown: 977 closed ports
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 2.3.4
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   filtered http
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     shell        Netkit rshd
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     ccproxy-ftp?
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 174.83 seconds
```

TCP scan con report:



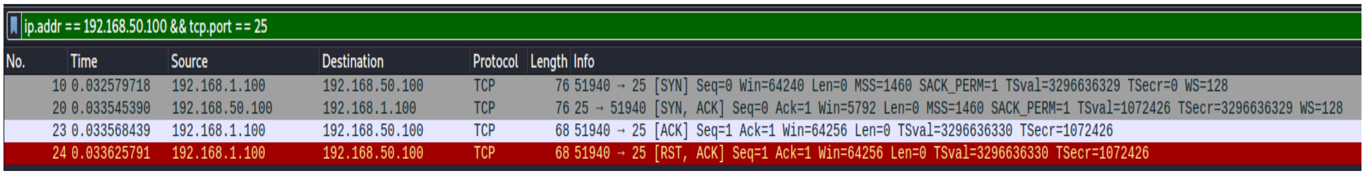
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -oN tcp_scan -sT 192.168.50.100
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-17 15:59 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0042s latency).
Not shown: 977 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered 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

Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```



```
# Nmap 7.91 scan initiated Wed Jul 17 15:59:09 2024 as: nmap -oN tcp_scan -sT 192.168.50.100
Nmap scan report for 192.168.50.100
Host is up (0.0042s latency).
Not shown: 977 closed ports
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   filtered 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

# Nmap done at Wed Jul 17 15:59:11 2024 -- 1 IP address (1 host up) scanned in 1.41 seconds
```

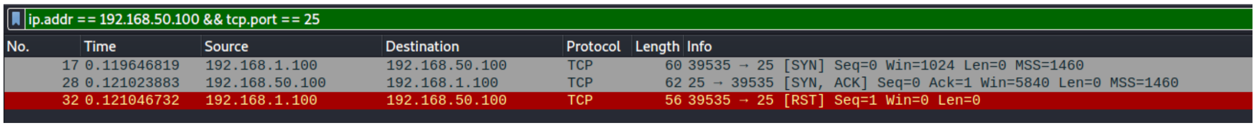
In entrambi il TCP e il SYN scan notiamo che la porta 80 risulta "filtered" e non "open" per via della regola firewall impostata su pfsense per impedire l'accesso alla DVWA su Metasploitable.

Il TCP scan completa il three-way-handshake



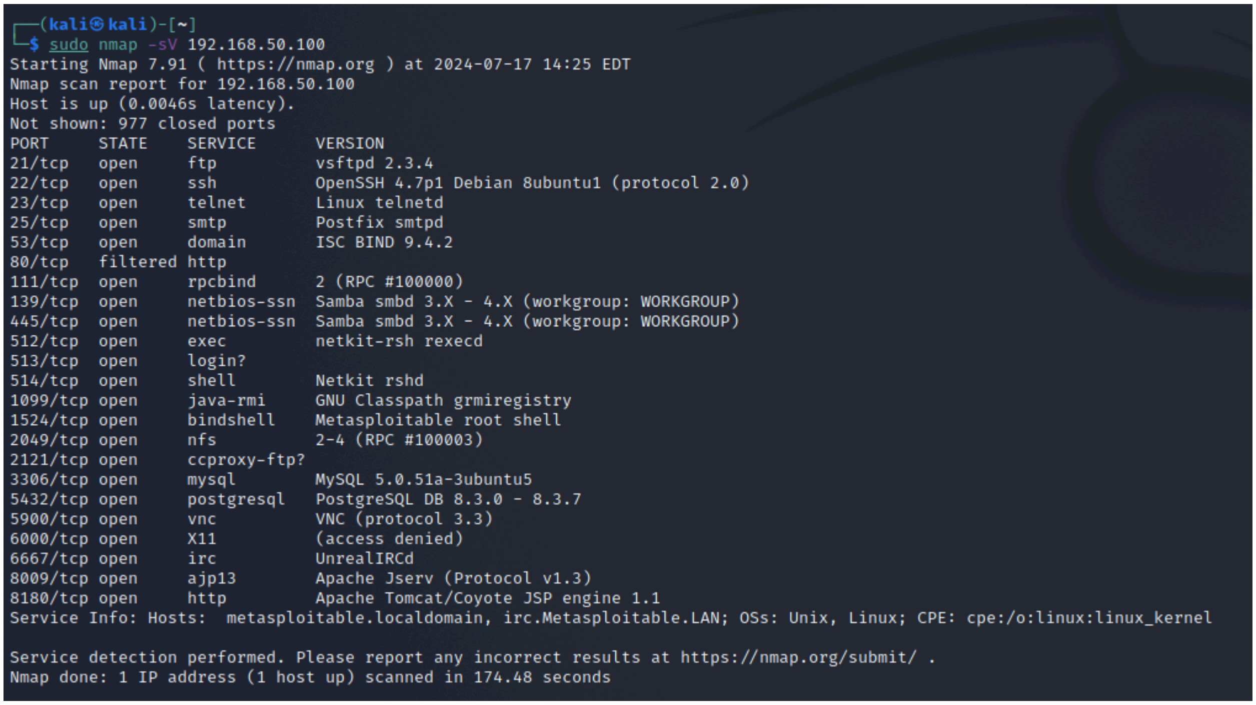
```
ip.addr == 192.168.50.100 && tcp.port == 25

No.   Time         Source          Destination     Protocol Length Info
   10 0.032579718  192.168.1.100   192.168.50.100  TCP      76 51940 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3296636329 TSecr=0 WS=128
   20 0.033545390  192.168.50.100  192.168.1.100   TCP      76 25 → 51940 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1072426 TSecr=3296636329 WS=128
   23 0.033568439  192.168.1.100   192.168.50.100  TCP      68 51940 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3296636330 TSecr=1072426
   24 0.033625791  192.168.1.100   192.168.50.100  TCP      68 51940 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3296636330 TSecr=1072426
```

Il SYN scan verifica unicamente se la porta è aperta, senza stabilire una connessione (non completando il three-way-handshake):



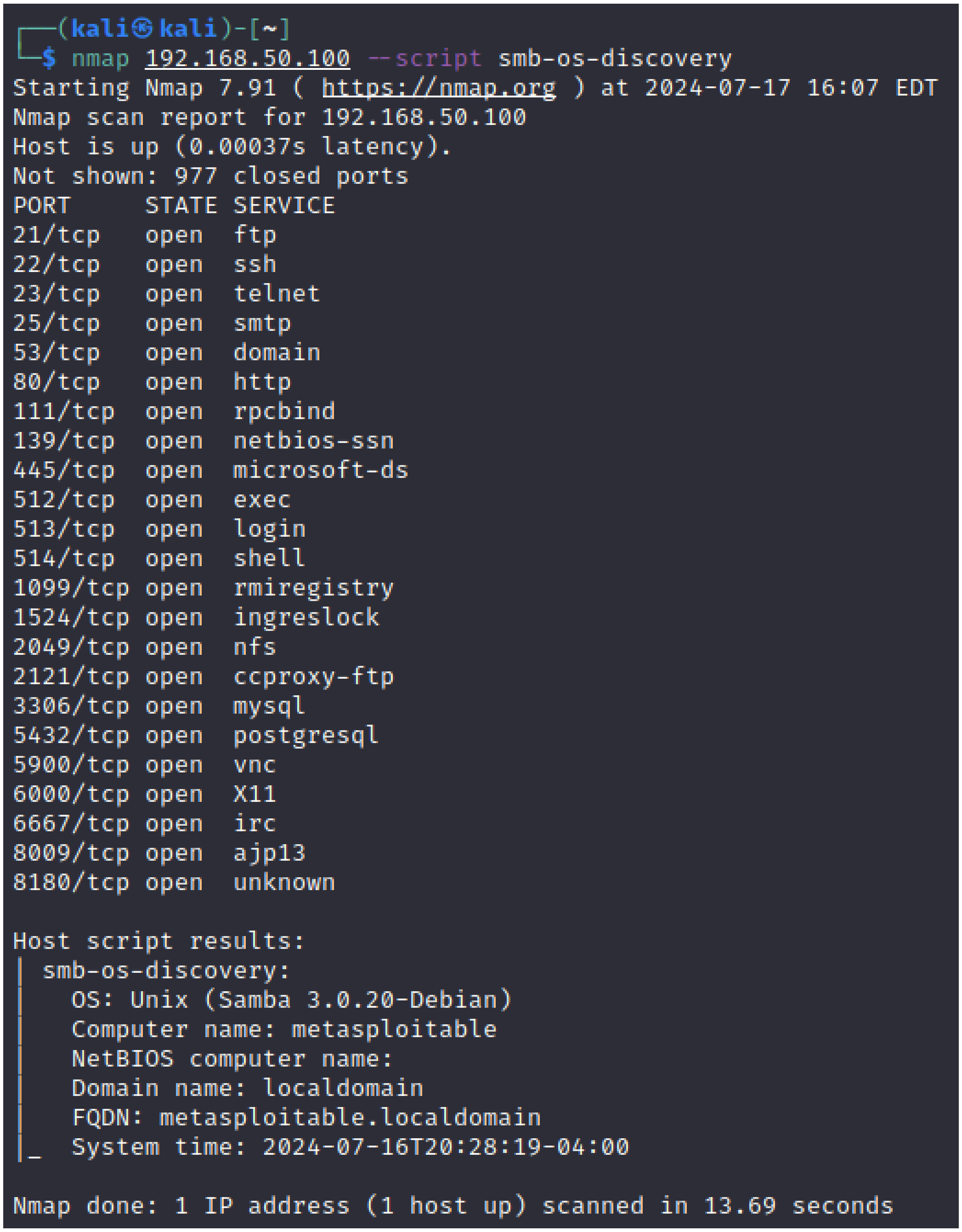
```
ip.addr == 192.168.50.100 && tcp.port == 25

No.   Time         Source          Destination     Protocol Length Info
   17 0.119646819  192.168.1.100   192.168.50.100  TCP      60 39535 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   28 0.121023883  192.168.50.100  192.168.1.100   TCP      62 25 → 39535 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
   32 0.121046732  192.168.1.100   192.168.50.100  TCP      56 39535 → 25 [RST] Seq=1 Win=0 Len=0
```

Version detection:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.100
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-17 14:25 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0046s latency).
Not shown: 977 closed ports
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   filtered http
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     shell        Netkit rshd
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     ccproxy-ftp?
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 174.48 seconds
```

Script di Nmap per determinare la versione del SO del sistema target dal banner del servizio SMB. Fornisce anche info sul tipo del sistema operativo



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.100 --script smb-os-discovery
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-17 16:07 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00037s latency).
Not shown: 977 closed ports
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

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-07-16T20:28:19-04:00

Nmap done: 1 IP address (1 host up) scanned in 13.69 seconds
```