Macchina Kali
ip: 192.168.50.100

Macchina Metasploitable

Ip: 192.168.50.101

Porte aperte:

21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180

Macchina Windows 7

Ip: 192.168.50.102

Porte aperte:

135, 139, 445, 5357, 49152-49156

In allegato lascio gli screenshot delle varie scansioni:

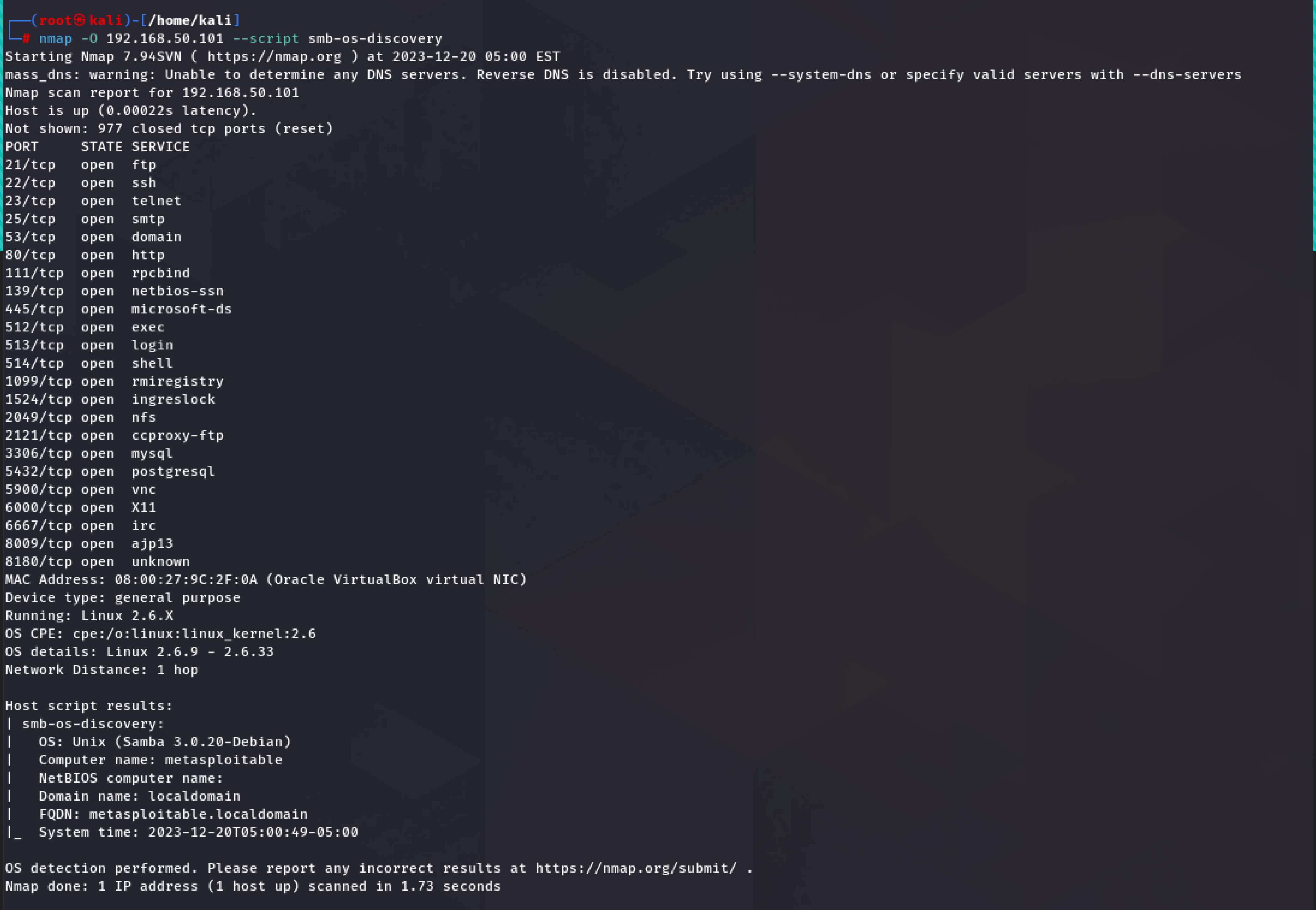
Scansioni a meta: Slide

1. Os fingerprint
2. Syn Scan
3. TCP connect
4. Version detection

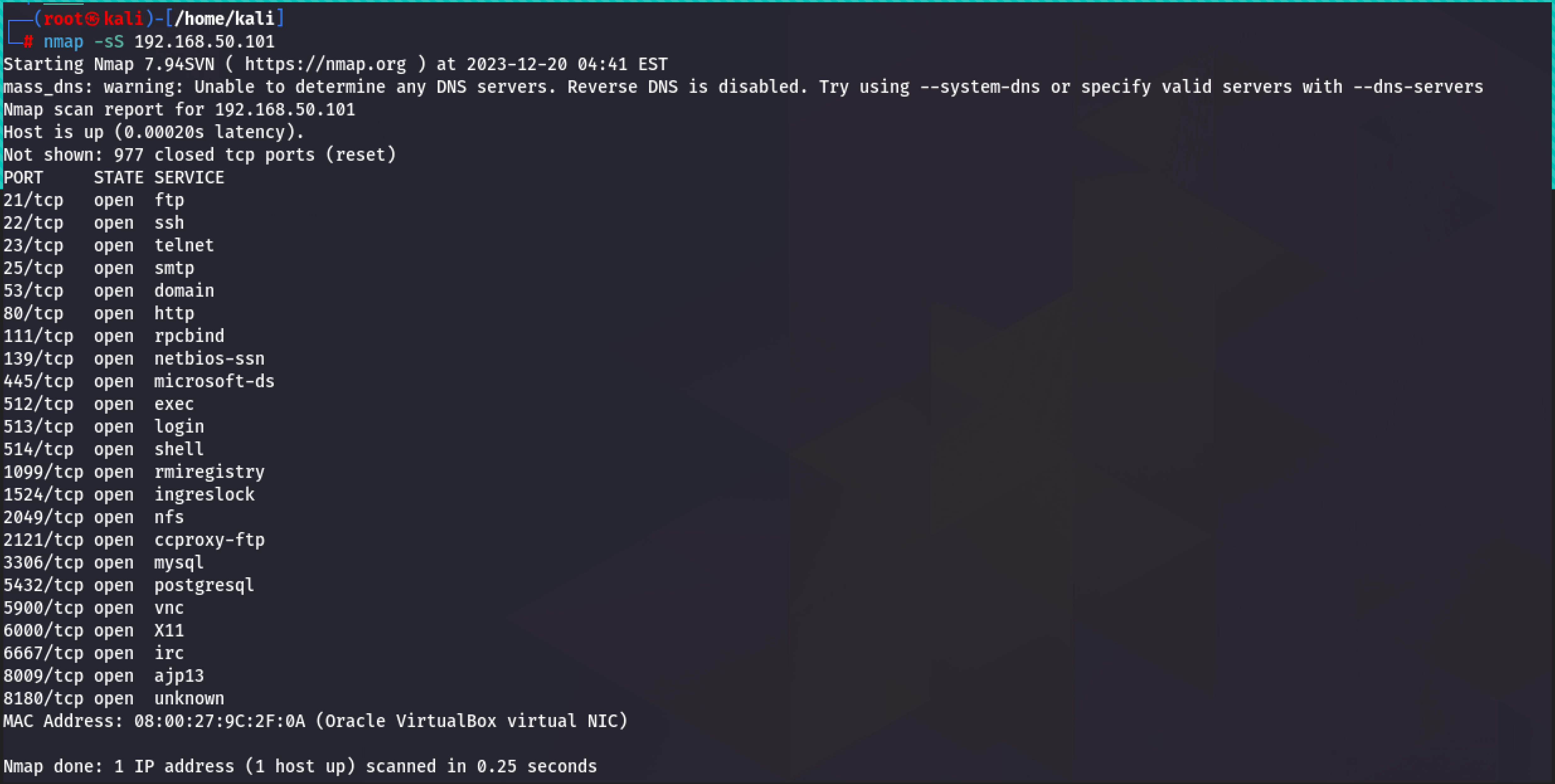
La differenza tra syn e TCP è che la prima è di tipo Reset quindi si ferma al SYN-ACK mandando poi un reset per non lasciare tracce, la seconda è conn-refused perché il Three-Way-Handshake non va a buon fine per via delle regole dei firewall

Scansioni a windows 7: Slide

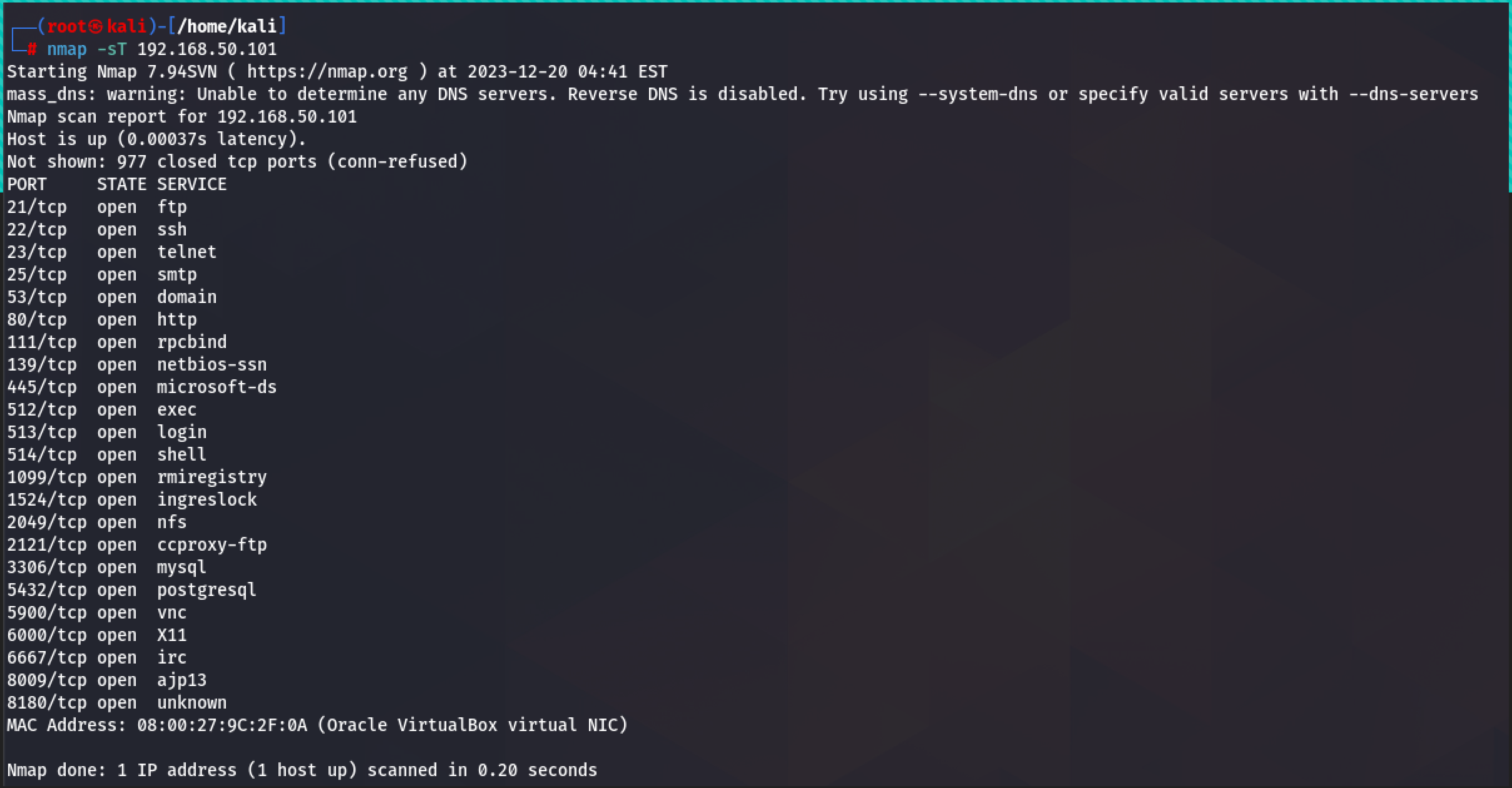
1. Os fingerprint
2. Apertura TCP/UDP nelle regole firewall in entrata
3. Apertura TCP/UDP nelle regole firewall in uscita



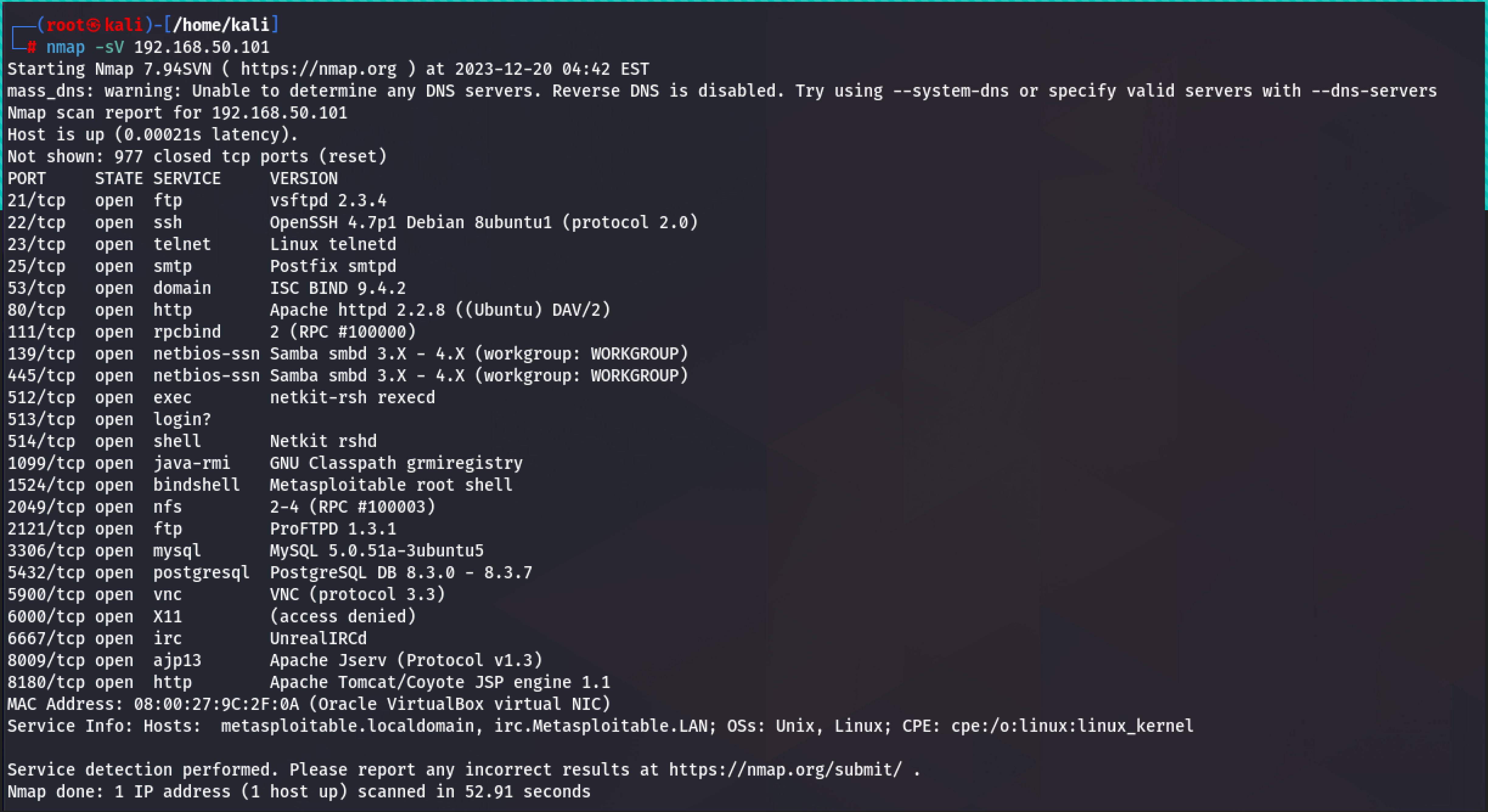
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.101 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 05:00 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00022s 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: 08:00:27:9C:2F:0A (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

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: 2023-12-20T05:00:49-05:00

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
```



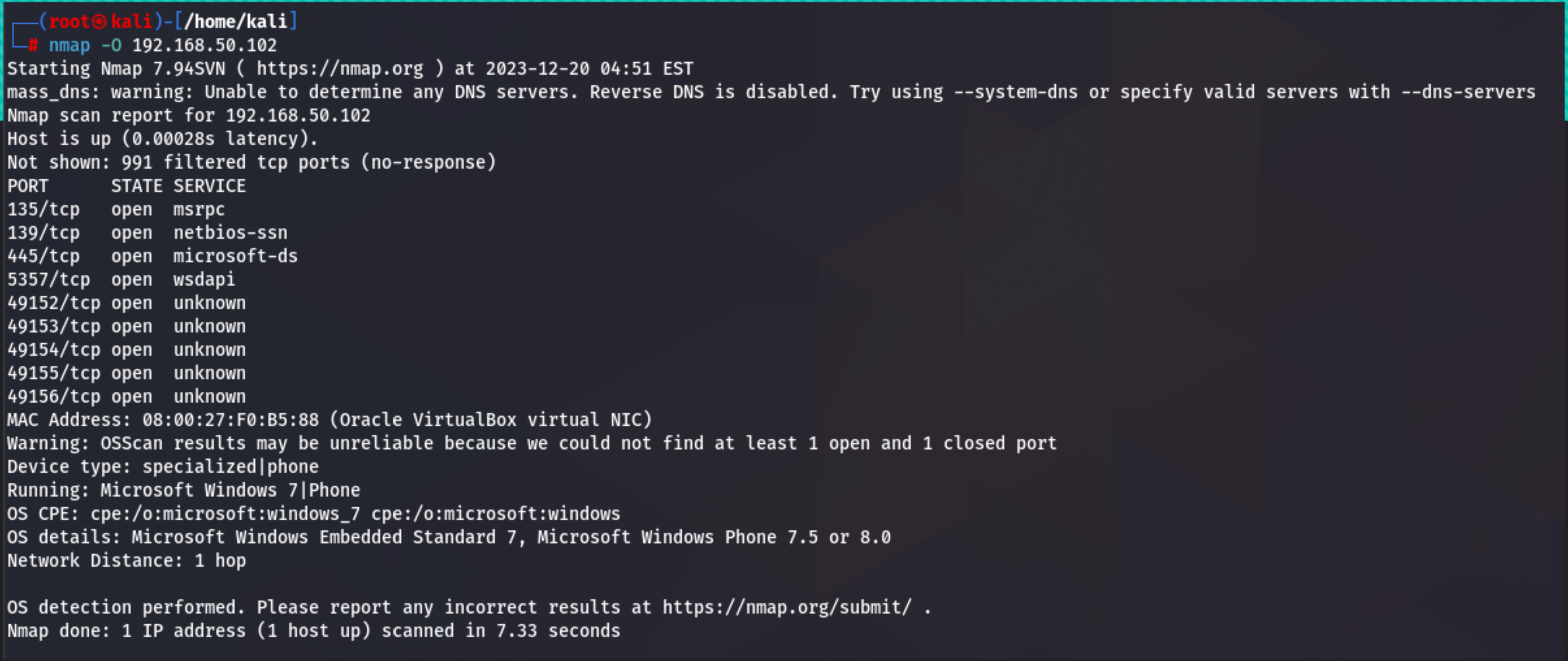
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 04:41 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00020s 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: 08:00:27:9C:2F:0A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```



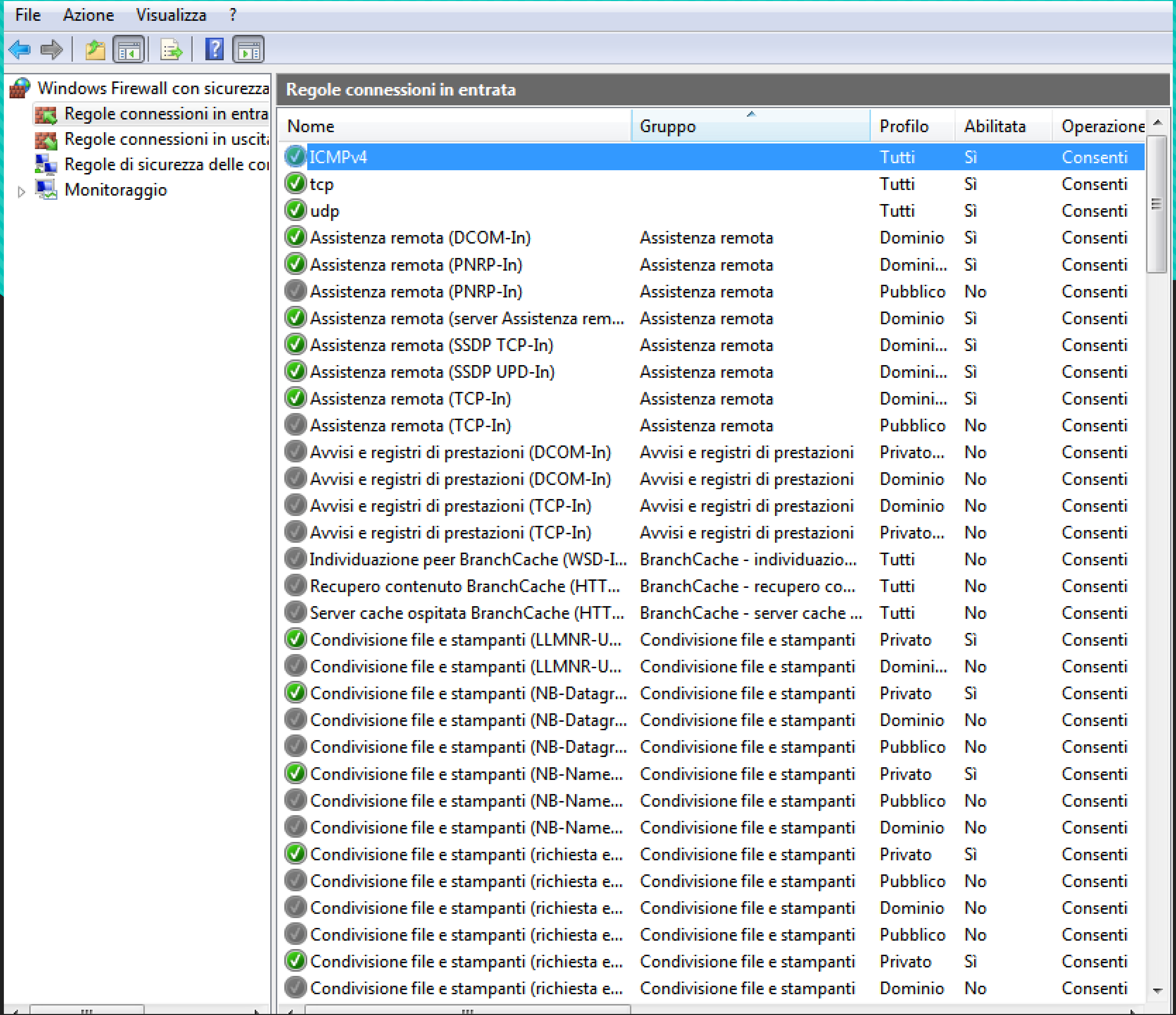
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 04:41 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00037s 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: 08:00:27:9C:2F:0A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 04:42 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00021s 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        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  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: 08:00:27:9C:2F:0A (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 52.91 seconds
```

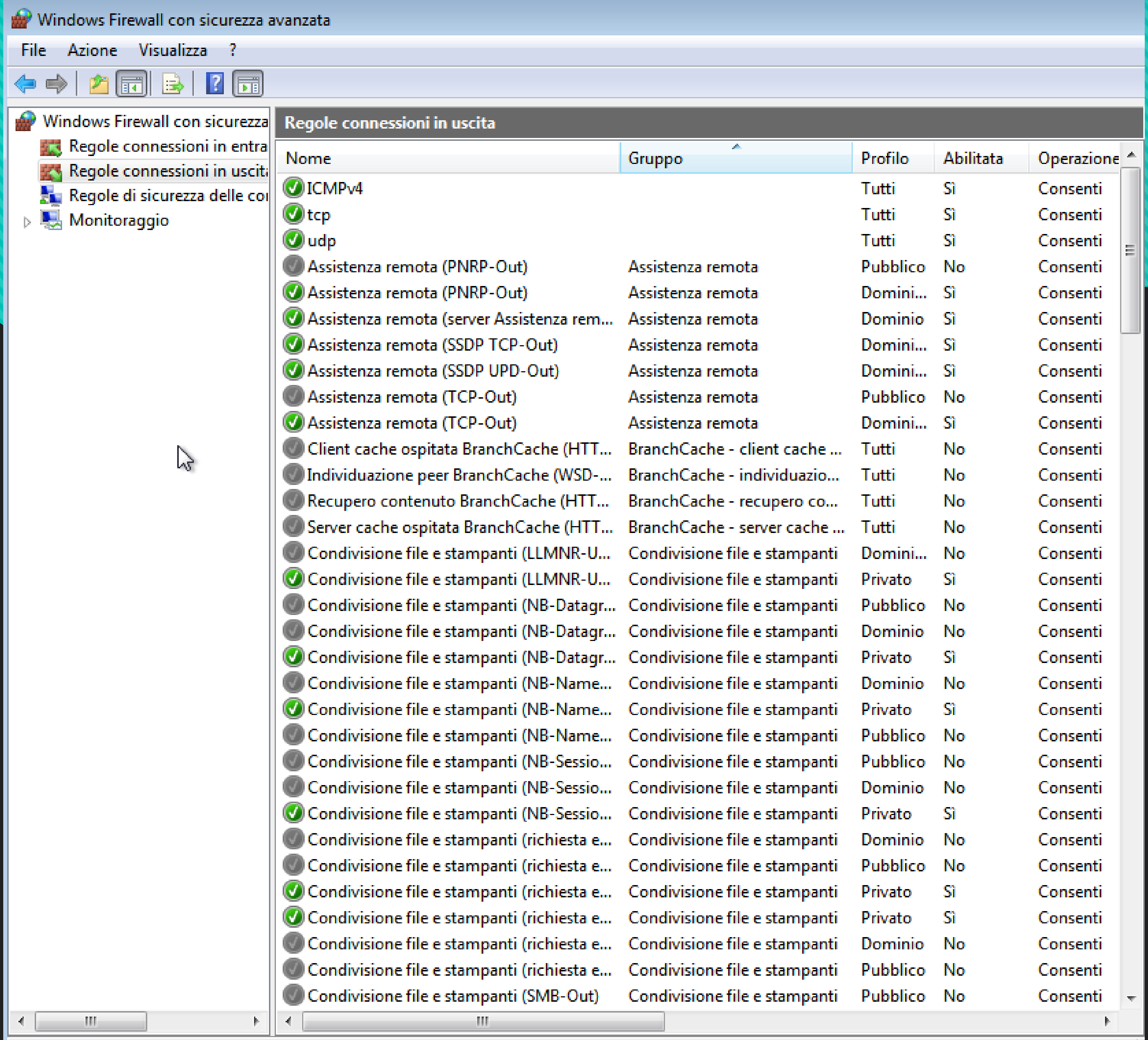


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 04:51 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.00028s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:F0:B5:88 (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 7.33 seconds
```


File
Azione
Visualizza
?
Windows Firewall con sicurezza
Regole connessioni in entra
Regole connessioni in uscit
Regole di sicurezza delle co
Monitoraggio

Regole connessioni in entrata

Nome	Gruppo	Profilo	Abilitata	Operazione
ICMPv4		Tutti	Sì	Consenti
tcp		Tutti	Sì	Consenti
udp		Tutti	Sì	Consenti
Assistenza remota (DCOM-In)	Assistenza remota	Dominio	Sì	Consenti
Assistenza remota (PNRP-In)	Assistenza remota	Domini...	Sì	Consenti
Assistenza remota (PNRP-In)	Assistenza remota	Pubblico	No	Consenti
Assistenza remota (server Assistenza rem...	Assistenza remota	Dominio	Sì	Consenti
Assistenza remota (SSDP TCP-In)	Assistenza remota	Domini...	Sì	Consenti
Assistenza remota (SSDP UPD-In)	Assistenza remota	Domini...	Sì	Consenti
Assistenza remota (TCP-In)	Assistenza remota	Domini...	Sì	Consenti
Assistenza remota (TCP-In)	Assistenza remota	Pubblico	No	Consenti
Avvisi e registri di prestazioni (DCOM-In)	Avvisi e registri di prestazioni	Privato...	No	Consenti
Avvisi e registri di prestazioni (DCOM-In)	Avvisi e registri di prestazioni	Dominio	No	Consenti
Avvisi e registri di prestazioni (TCP-In)	Avvisi e registri di prestazioni	Dominio	No	Consenti
Avvisi e registri di prestazioni (TCP-In)	Avvisi e registri di prestazioni	Privato...	No	Consenti
Individuazione peer BranchCache (WSD-I...	BranchCache - individuazio...	Tutti	No	Consenti
Recupero contenuto BranchCache (HTT...	BranchCache - recupero co...	Tutti	No	Consenti
Server cache ospitata BranchCache (HTT...	BranchCache - server cache ...	Tutti	No	Consenti
Condivisione file e stampanti (LLMNR-U...	Condivisione file e stampanti	Privato	Sì	Consenti
Condivisione file e stampanti (LLMNR-U...	Condivisione file e stampanti	Domini...	No	Consenti
Condivisione file e stampanti (NB-Datagr...	Condivisione file e stampanti	Privato	Sì	Consenti
Condivisione file e stampanti (NB-Datagr...	Condivisione file e stampanti	Dominio	No	Consenti
Condivisione file e stampanti (NB-Datagr...	Condivisione file e stampanti	Pubblico	No	Consenti
Condivisione file e stampanti (NB-Name...	Condivisione file e stampanti	Privato	Sì	Consenti
Condivisione file e stampanti (NB-Name...	Condivisione file e stampanti	Pubblico	No	Consenti
Condivisione file e stampanti (NB-Name...	Condivisione file e stampanti	Dominio	No	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Privato	Sì	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Pubblico	No	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Dominio	No	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Pubblico	No	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Privato	Sì	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Dominio	No	Consenti


Windows Firewall con sicurezza avanzata
File
Azione
Visualizza
?
Windows Firewall con sicurezza
Regole connessioni in entra
Regole connessioni in uscit
Regole di sicurezza delle co
Monitoraggio

Regole connessioni in uscita

Nome	Gruppo	Profilo	Abilitata	Operazione
ICMPv4		Tutti	Sì	Consenti
tcp		Tutti	Sì	Consenti
udp		Tutti	Sì	Consenti
Assistenza remota (PNRP-Out)	Assistenza remota	Pubblico	No	Consenti
Assistenza remota (PNRP-Out)	Assistenza remota	Domini...	Sì	Consenti
Assistenza remota (server Assistenza rem...	Assistenza remota	Dominio	Sì	Consenti
Assistenza remota (SSDP TCP-Out)	Assistenza remota	Domini...	Sì	Consenti
Assistenza remota (SSDP UPD-Out)	Assistenza remota	Domini...	Sì	Consenti
Assistenza remota (TCP-Out)	Assistenza remota	Pubblico	No	Consenti
Assistenza remota (TCP-Out)	Assistenza remota	Domini...	Sì	Consenti
Client cache ospitata BranchCache (HTT...	BranchCache - client cache ...	Tutti	No	Consenti
Individuazione peer BranchCache (WSD-...	BranchCache - individuazio...	Tutti	No	Consenti
Recupero contenuto BranchCache (HTT...	BranchCache - recupero co...	Tutti	No	Consenti
Server cache ospitata BranchCache (HTT...	BranchCache - server cache ...	Tutti	No	Consenti
Condivisione file e stampanti (LLMNR-U...	Condivisione file e stampanti	Domini...	No	Consenti
Condivisione file e stampanti (LLMNR-U...	Condivisione file e stampanti	Privato	Sì	Consenti
Condivisione file e stampanti (NB-Datagr...	Condivisione file e stampanti	Pubblico	No	Consenti
Condivisione file e stampanti (NB-Datagr...	Condivisione file e stampanti	Dominio	No	Consenti
Condivisione file e stampanti (NB-Datagr...	Condivisione file e stampanti	Privato	Sì	Consenti
Condivisione file e stampanti (NB-Name...	Condivisione file e stampanti	Dominio	No	Consenti
Condivisione file e stampanti (NB-Name...	Condivisione file e stampanti	Privato	Sì	Consenti
Condivisione file e stampanti (NB-Name...	Condivisione file e stampanti	Pubblico	No	Consenti
Condivisione file e stampanti (NB-Sessio...	Condivisione file e stampanti	Pubblico	No	Consenti
Condivisione file e stampanti (NB-Sessio...	Condivisione file e stampanti	Dominio	No	Consenti
Condivisione file e stampanti (NB-Sessio...	Condivisione file e stampanti	Privato	Sì	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Dominio	No	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Pubblico	No	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Privato	Sì	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Privato	Sì	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Dominio	No	Consenti
Condivisione file e stampanti (richiesta e...	Condivisione file e stampanti	Pubblico	No	Consenti
Condivisione file e stampanti (SMB-Out)	Condivisione file e stampanti	Pubblico	No	Consenti