VALUTAZIONE DELLE VULNERABILITA’ (1)

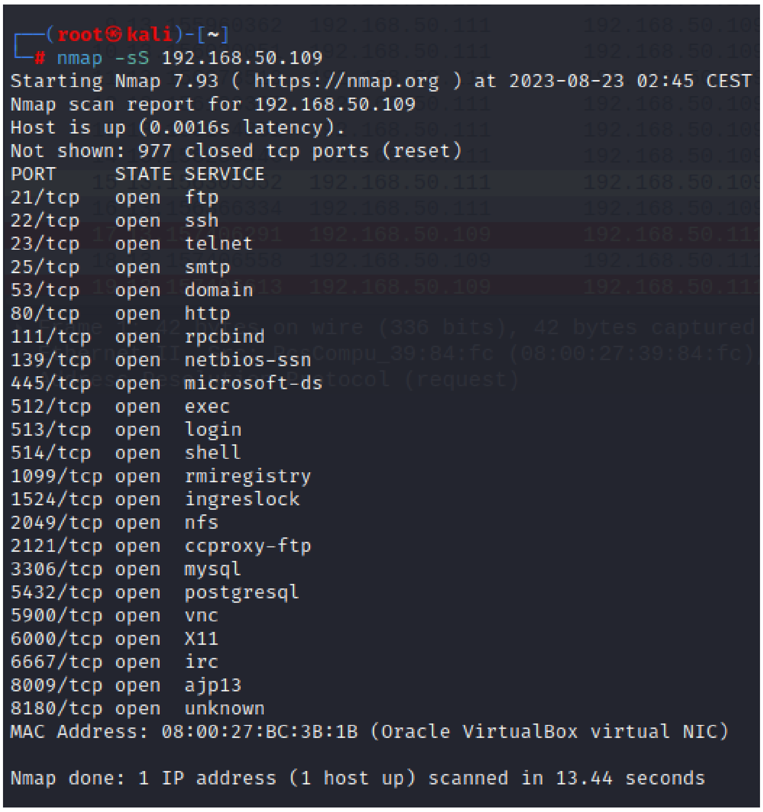
Scansione dei servizi con Nmap

Tecniche di scansione con Nmap - scansione di un host, senza e con completamento del 3-way handshake

Questo esercizio può essere utile per lo studente per prendere dimestichezza con i vari comandi di nmap.
Poiché su Linux è un potente tool di scansione della rete, si richiede di utilizzare i seguenti comandi e trascrivere i vari risultati su un report:

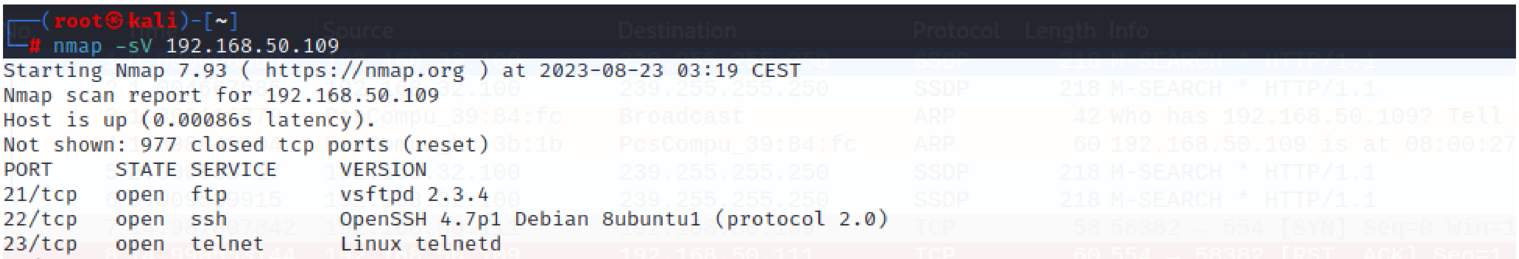
TCP: #	nmap -sS ip address
scansione completa: #	nmap -sV ip address
output su file: #	nmap -sV -oN file.txt ip address
scansione su porta: #	nmap -sS -p 8080 ip address
scansione tutte le porte: #	nmap -sS -p ip address
scansione UDP: #	nmap -sU -r -v ip address
scansione sistema operativo: #	nmap -O ip address
scansione versione servizi: #	nmap -sV ip address
scansione common 100 ports: #	nmap -F ip address
scansione tramite ARP: #	nmap -PR ip address
scansione tramite PING: #	nmap -sP ip address
scansione senza PING: #	nmap -PN ip address

TCP: nmap -sS <<ip address>>



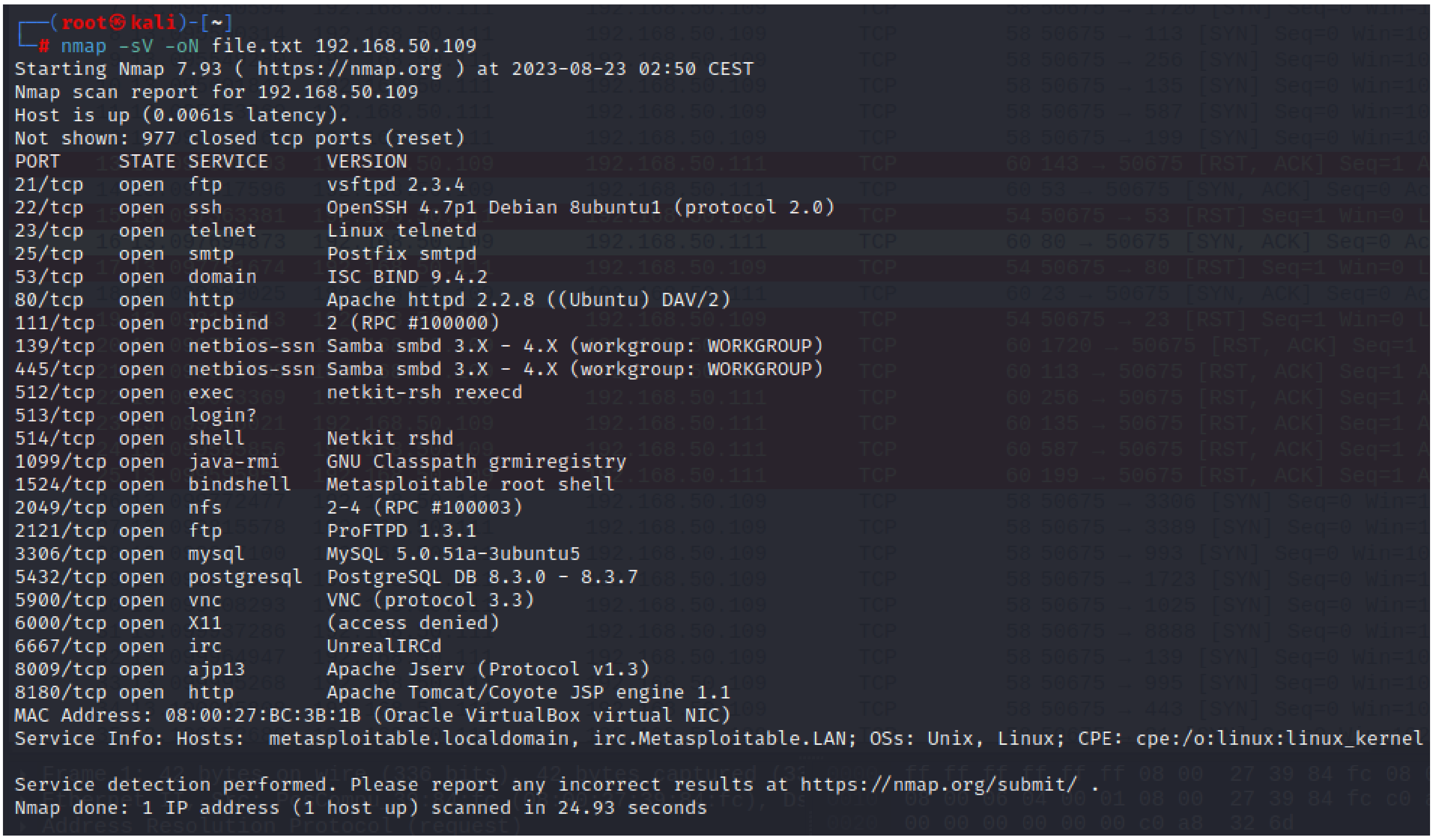
```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 02:45 CEST
Nmap scan report for 192.168.50.109
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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:BC:3B:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
```

scansione completa: nmap -sV <<ip address>>



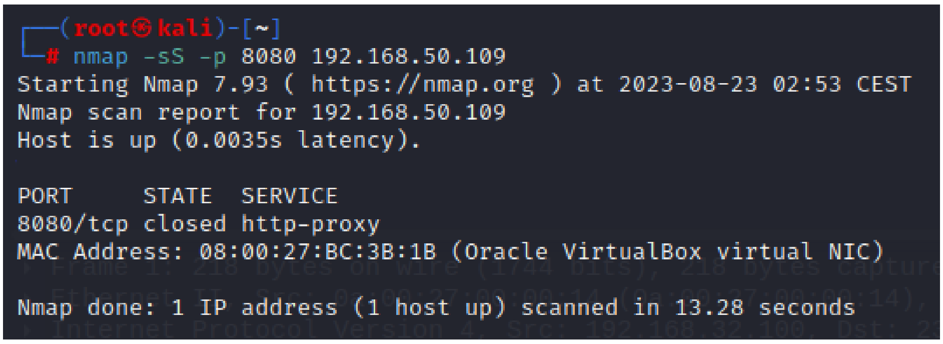
```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 03:19 CEST
Nmap scan report for 192.168.50.109
Host is up (0.00086s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
```

output su file: nmap -sV -oN file.txt. <<ip address>>



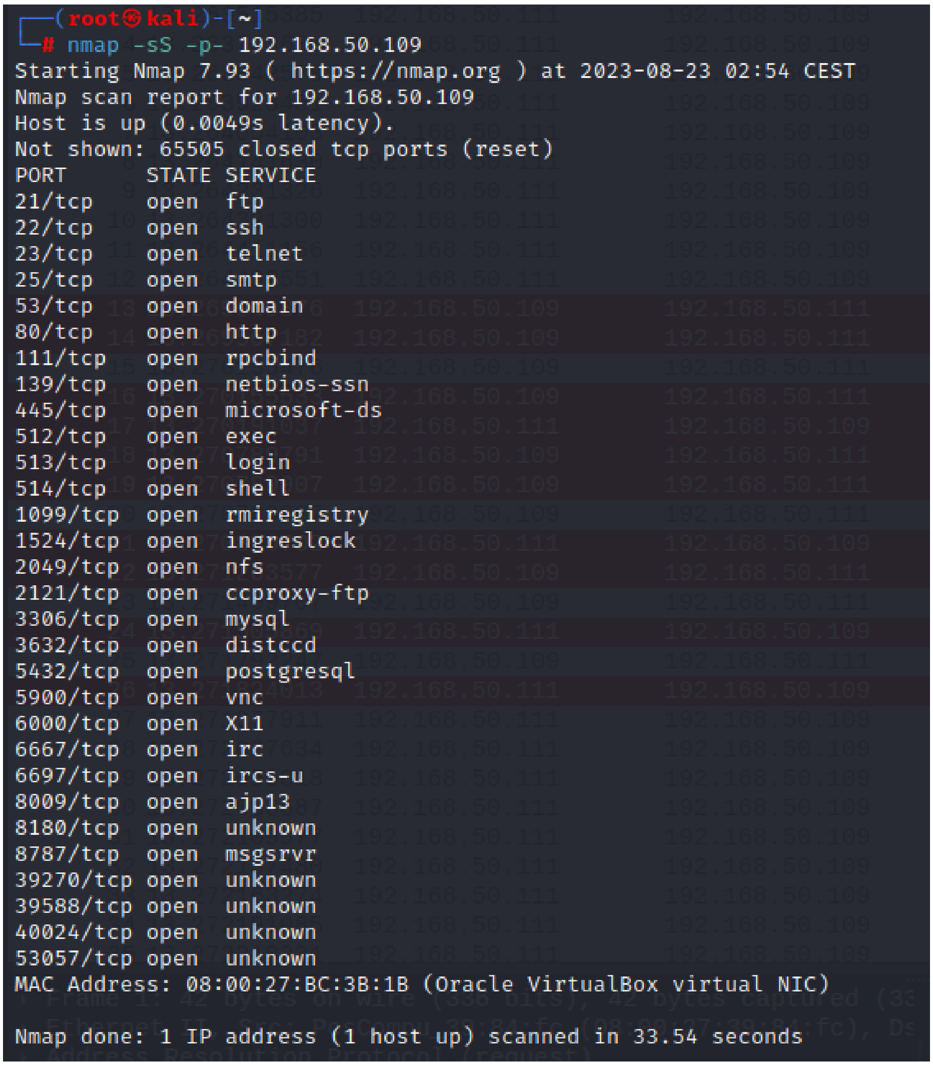
```
┌──(root㉿kali)-[~]
└─# nmap -sV -oN file.txt 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 02:50 CEST
Nmap scan report for 192.168.50.109
Host is up (0.0061s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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:BC:3B:1B (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 24.93 seconds
```

scansione su porta: nmap -sS -p 8080 <<ip address>>



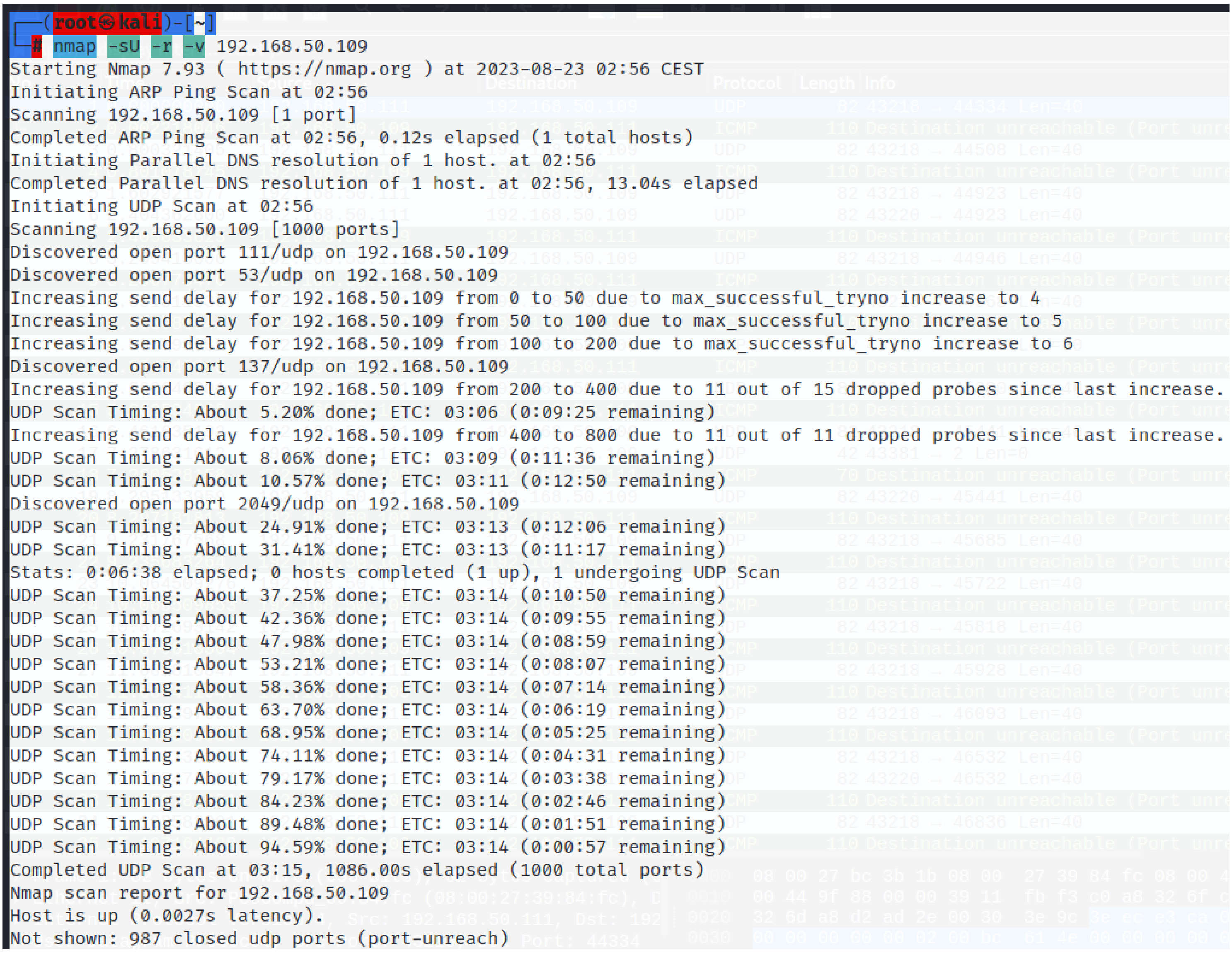
```
┌──(root㉿kali)-[~]
└─# nmap -sS -p 8080 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 02:53 CEST
Nmap scan report for 192.168.50.109
Host is up (0.0035s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 08:00:27:BC:3B:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

scansione su tutte le porte: nmap -sS -p- <<ip address>>

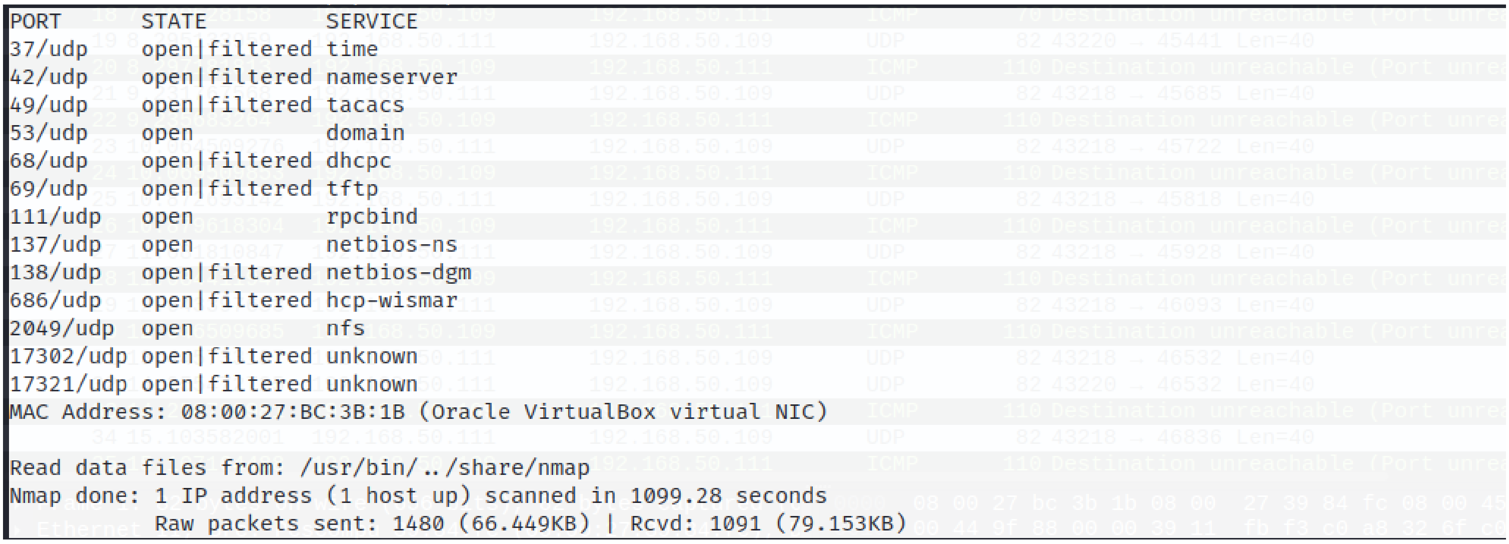


```
┌──(root㉿kali)-[~]
└─# nmap -sS -p- 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 02:54 CEST
Nmap scan report for 192.168.50.109
Host is up (0.0049s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
39270/tcp open  unknown
39588/tcp open  unknown
40024/tcp open  unknown
53057/tcp open  unknown
MAC Address: 08:00:27:BC:3B:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 33.54 seconds
```

scansione UDP: nmap -sU -r -v <<ip address>>

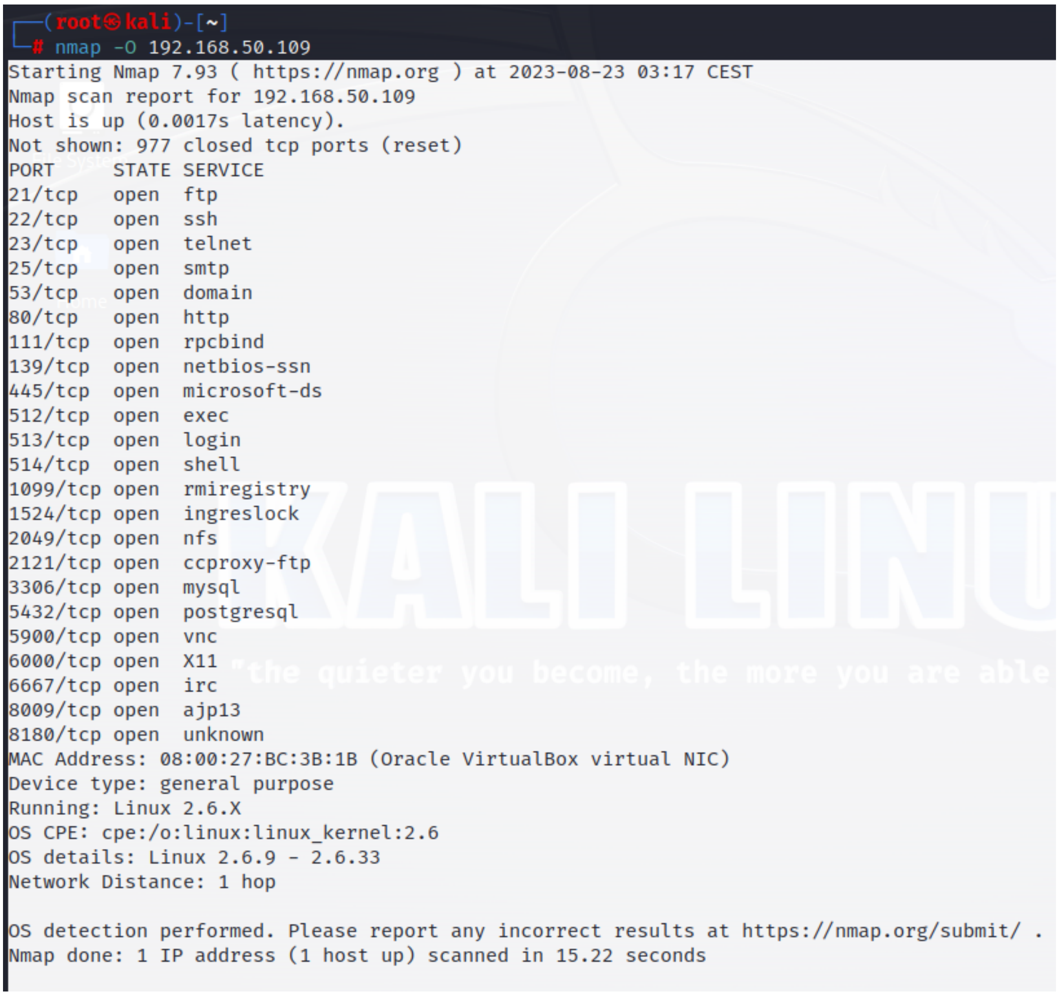


```
┌──(root㉿kali)-[~]
└─# nmap -sU -r -v 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 02:56 CEST
Initiating ARP Ping Scan at 02:56
Scanning 192.168.50.109 [1 port]
Completed ARP Ping Scan at 02:56, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:56
Completed Parallel DNS resolution of 1 host. at 02:56, 13.04s elapsed
Initiating UDP Scan at 02:56
Scanning 192.168.50.109 [1000 ports]
Discovered open port 111/udp on 192.168.50.109
Discovered open port 53/udp on 192.168.50.109
Increasing send delay for 192.168.50.109 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.50.109 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.50.109 from 100 to 200 due to max_successful_tryno increase to 6
Discovered open port 137/udp on 192.168.50.109
Increasing send delay for 192.168.50.109 from 200 to 400 due to 11 out of 15 dropped probes since last increase.
UDP Scan Timing: About 5.20% done; ETC: 03:06 (0:09:25 remaining)
Increasing send delay for 192.168.50.109 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 8.06% done; ETC: 03:09 (0:11:36 remaining)
UDP Scan Timing: About 10.57% done; ETC: 03:11 (0:12:50 remaining)
Discovered open port 2049/udp on 192.168.50.109
UDP Scan Timing: About 24.91% done; ETC: 03:13 (0:12:06 remaining)
UDP Scan Timing: About 31.41% done; ETC: 03:13 (0:11:17 remaining)
Stats: 0:06:38 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 37.25% done; ETC: 03:14 (0:10:50 remaining)
UDP Scan Timing: About 42.36% done; ETC: 03:14 (0:09:55 remaining)
UDP Scan Timing: About 47.98% done; ETC: 03:14 (0:08:59 remaining)
UDP Scan Timing: About 53.21% done; ETC: 03:14 (0:08:07 remaining)
UDP Scan Timing: About 58.36% done; ETC: 03:14 (0:07:14 remaining)
UDP Scan Timing: About 63.70% done; ETC: 03:14 (0:06:19 remaining)
UDP Scan Timing: About 68.95% done; ETC: 03:14 (0:05:25 remaining)
UDP Scan Timing: About 74.11% done; ETC: 03:14 (0:04:31 remaining)
UDP Scan Timing: About 79.17% done; ETC: 03:14 (0:03:38 remaining)
UDP Scan Timing: About 84.23% done; ETC: 03:14 (0:02:46 remaining)
UDP Scan Timing: About 89.48% done; ETC: 03:14 (0:01:51 remaining)
UDP Scan Timing: About 94.59% done; ETC: 03:14 (0:00:57 remaining)
Completed UDP Scan at 03:15, 1086.00s elapsed (1000 total ports)
Nmap scan report for 192.168.50.109
Host is up (0.0027s latency).
Not shown: 987 closed udp ports (port-unreach)
```



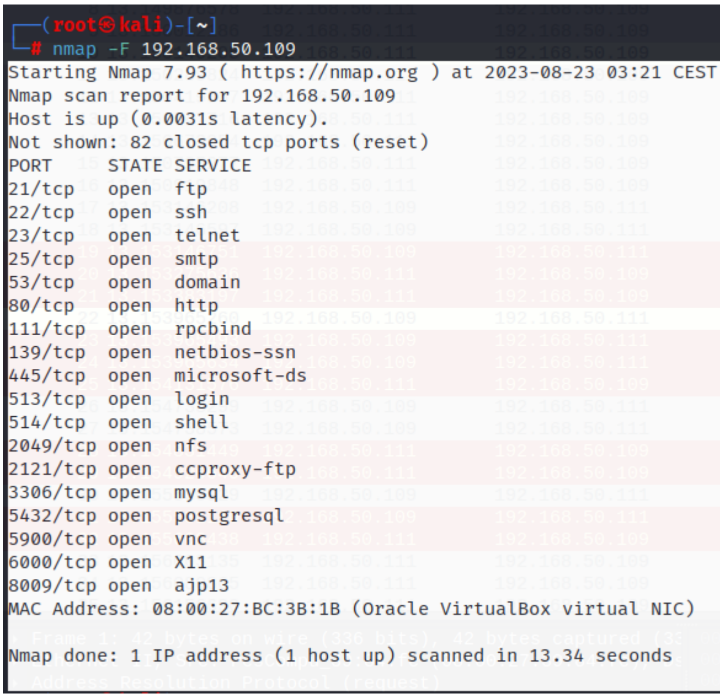
```
PORT      STATE         SERVICE
37/udp    open|filtered time
42/udp    open|filtered nameserver
49/udp    open|filtered tacacs
53/udp    open          domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open          rpcbind
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
686/udp   open|filtered hcp-wismar
2049/udp  open          nfs
17302/udp open|filtered unknown
17321/udp open|filtered unknown
MAC Address: 08:00:27:BC:3B:1B (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1099.28 seconds
           Raw packets sent: 1480 (66.449KB) | Rcvd: 1091 (79.153KB)
```

scansione tramite sistema operativo nmap -O <<ip address>>



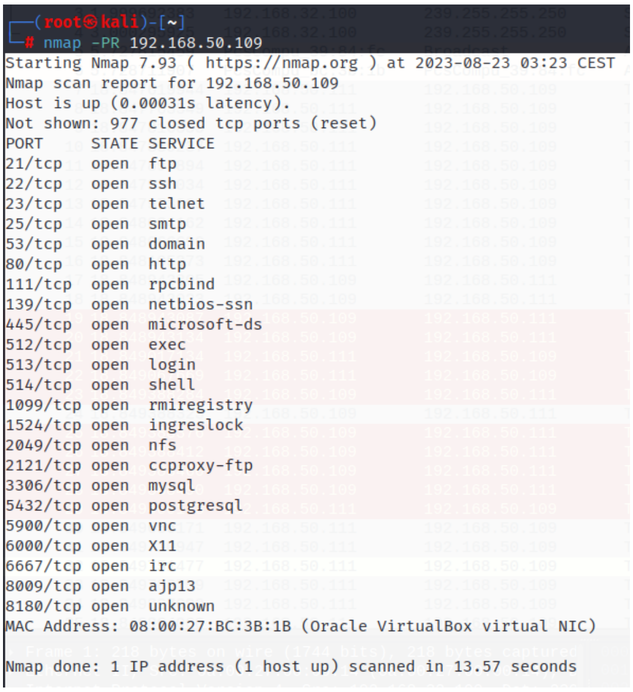
```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 03:17 CEST
Nmap scan report for 192.168.50.109
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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:BC:3B:1B (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 15.22 seconds
```

scansione common 100 ports: nmap -F <<ip address>>



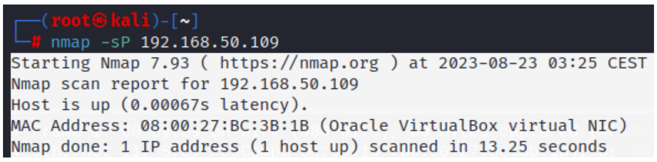
```
┌──(root㉿kali)-[~]
└─# nmap -F 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 03:21 CEST
Nmap scan report for 192.168.50.109
Host is up (0.0031s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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
513/tcp  open  login
514/tcp  open  shell
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
8009/tcp open  ajp13
MAC Address: 08:00:27:BC:3B:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

scansione tramite ARP: nmap -PR <<ip address>>



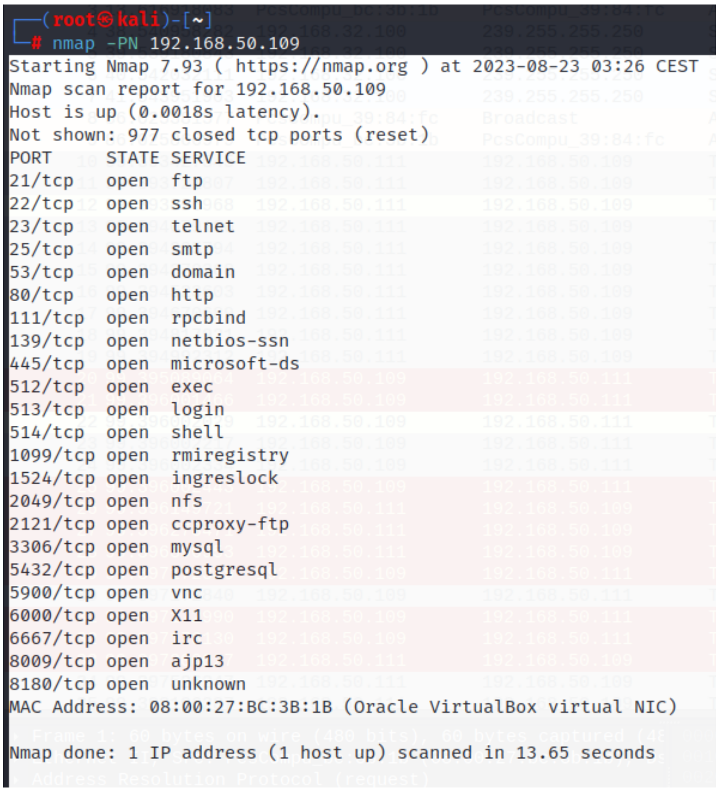
```
┌─(root㉿kali)-[~]
└─# nmap -PR 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 03:23 CEST
Nmap scan report for 192.168.50.109
Host is up (0.00031s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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:BC:3B:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.57 seconds
```

scansione tramite PING: nmap -sP <<ip address>>



```
┌─(root㉿kali)-[~]
└─# nmap -sP 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 03:25 CEST
Nmap scan report for 192.168.50.109
Host is up (0.00067s latency).
MAC Address: 08:00:27:BC:3B:1B (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

scansione senza PING: nmap -PN <<ip address>>



```
┌─(root㉿kali)-[~]
└─# nmap -PN 192.168.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-23 03:26 CEST
Nmap scan report for 192.168.50.109
Host is up (0.0018s 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:BC:3B:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds
```