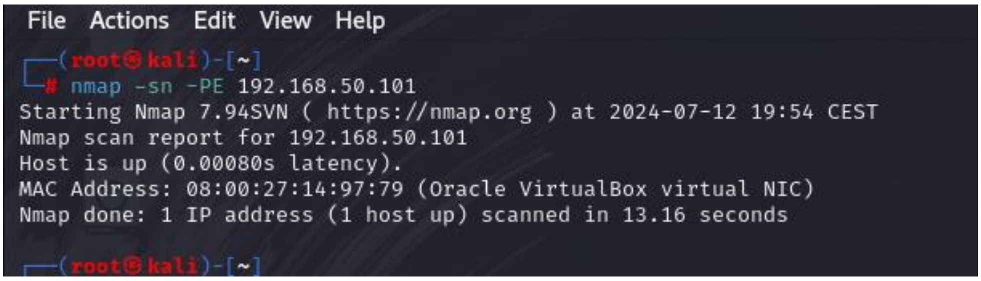
Report di scansione e rilevamento informazioni sulla macchina Metasploitable

1. nmap -sn -PE 192.168.50.101

Ping scan per determinare quali host sono attivi



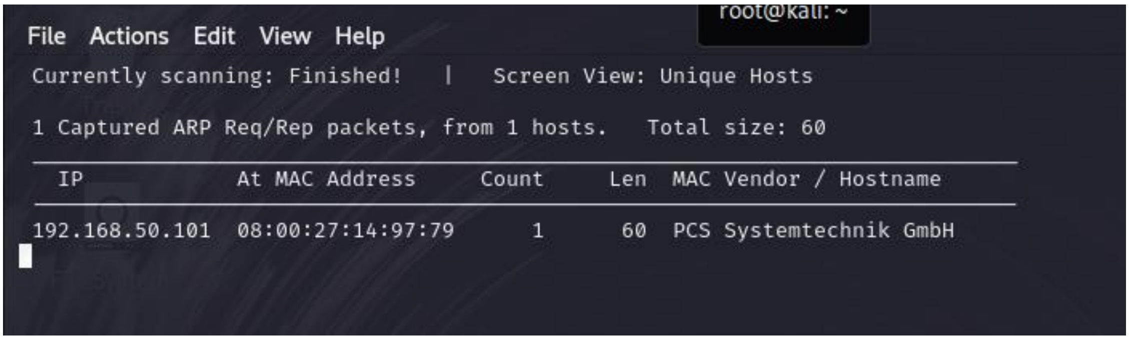
```
┌──(root㉿kali)-[~]
└─# nmap -sn -PE 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 19:54 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00080s latency).
MAC Address: 08:00:27:14:97:79 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds

┌──(root㉿kali)-[~]
```

Output: Host 192.168.50.101 is up

2. netdiscover -r 192.168.50.101/24

Scansione di rete per rilevare tutti i dispositivi attivi



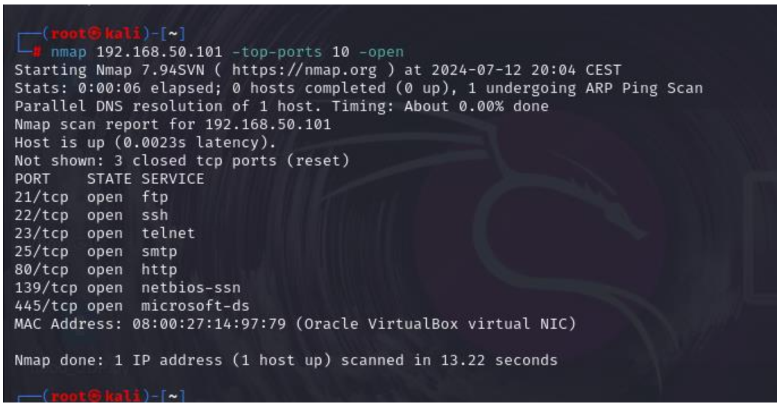
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.50.101  08:00:27:14:97:79      1      60  PCS Systemtechnik GmbH
```

Output: 1 pacchetto ARP catturato da un host.

3. nmap 192.168.50.101 -top-ports 10 -open

Scansione delle 10 porte più comuni aperte



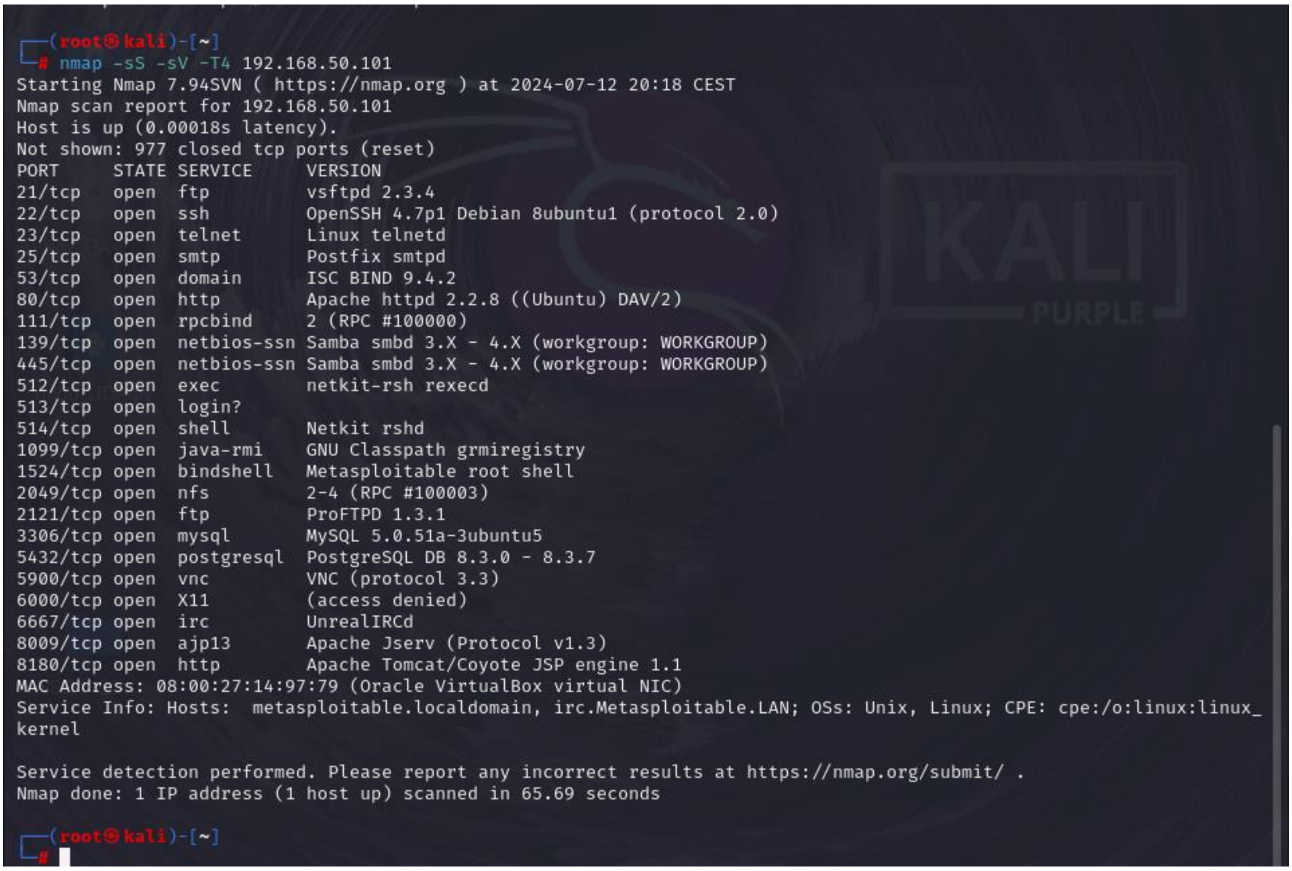
```
┌──(root㉿kali)-[~]
└─# nmap 192.168.50.101 -top-ports 10 -open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 20:04 CEST
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.50.101
Host is up (0.0023s latency).
Not shown: 3 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:14:97:79 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds

┌──(root㉿kali)-[~]
```

4. nmap -sS -sV -T4 192.168.50.101

Scansione SYN e rilevamento della versione dei servizi



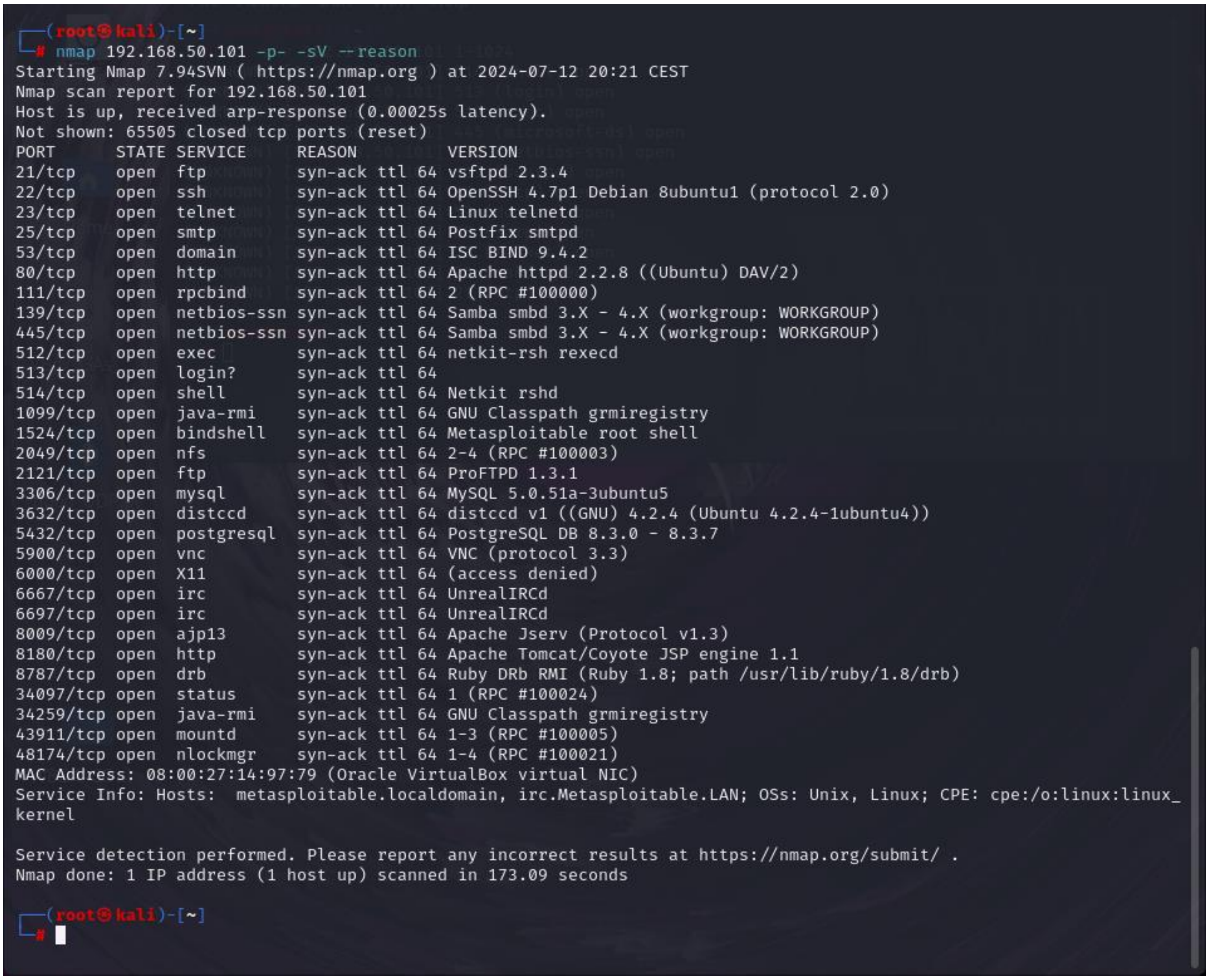
```
┌──(root㉿kali)-[~]
└─# nmap -sS -sV -T4 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 20:18 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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: 08:00:27:14:97:79 (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 65.69 seconds

┌──(root㉿kali)-[~]
└─#
```

5. nmap 192.168.50.101 -p- -sV –reason

Scansione di tutte le porte e rilevamento versione dei servizi



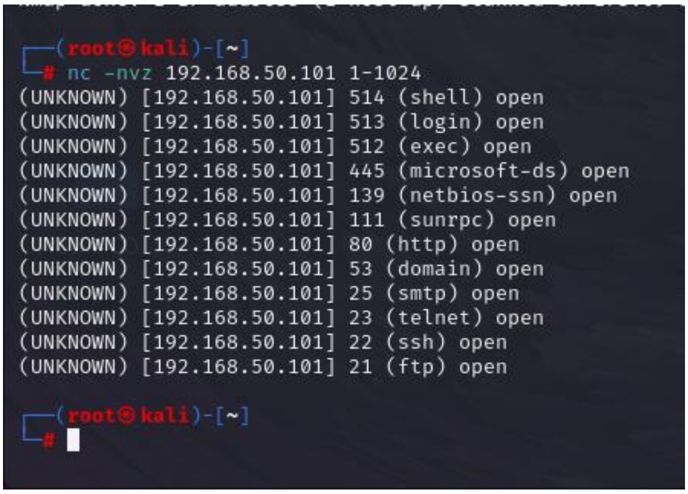
```
┌──(root㉿kali)-[~]
└─# nmap 192.168.50.101 -p- -sV --reason
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 20:21 CEST
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.00025s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  shell       syn-ack ttl 64 Netkit rshd
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64 (access denied)
6667/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
34097/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
34259/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
43911/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
48174/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
MAC Address: 08:00:27:14:97:79 (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 173.09 seconds

┌──(root㉿kali)-[~]
└─# 
```

6. nc -nvz 192.168.50.101 1-1024

Scansione delle prime 1024 porte con netcat

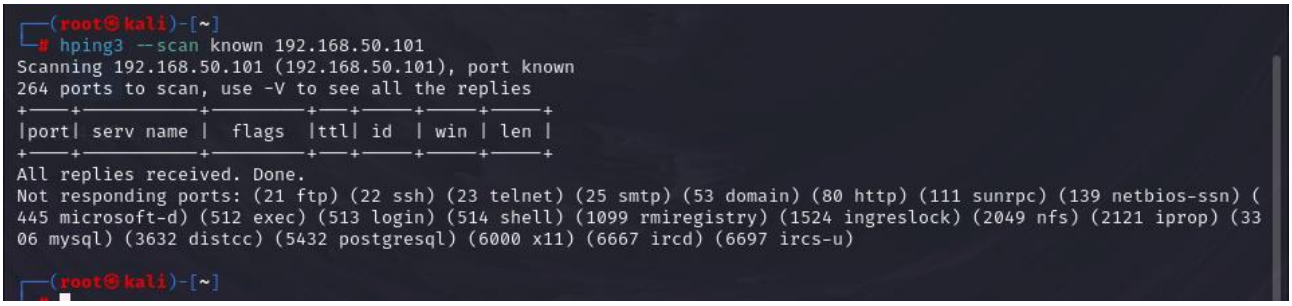


```
┌──(root㉿kali)-[~]
└─# nc -nvz 192.168.50.101 1-1024
(UNKNOWN) [192.168.50.101] 514 (shell) open
(UNKNOWN) [192.168.50.101] 513 (login) open
(UNKNOWN) [192.168.50.101] 512 (exec) open
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.101] 111 (sunrpc) open
(UNKNOWN) [192.168.50.101] 80 (http) open
(UNKNOWN) [192.168.50.101] 53 (domain) open
(UNKNOWN) [192.168.50.101] 25 (smtp) open
(UNKNOWN) [192.168.50.101] 23 (telnet) open
(UNKNOWN) [192.168.50.101] 22 (ssh) open
(UNKNOWN) [192.168.50.101] 21 (ftp) open

┌──(root㉿kali)-[~]
└─# 
```

7. hping3 –scan know 192.168.50.101

Scansione delle porte conosciute con hping3

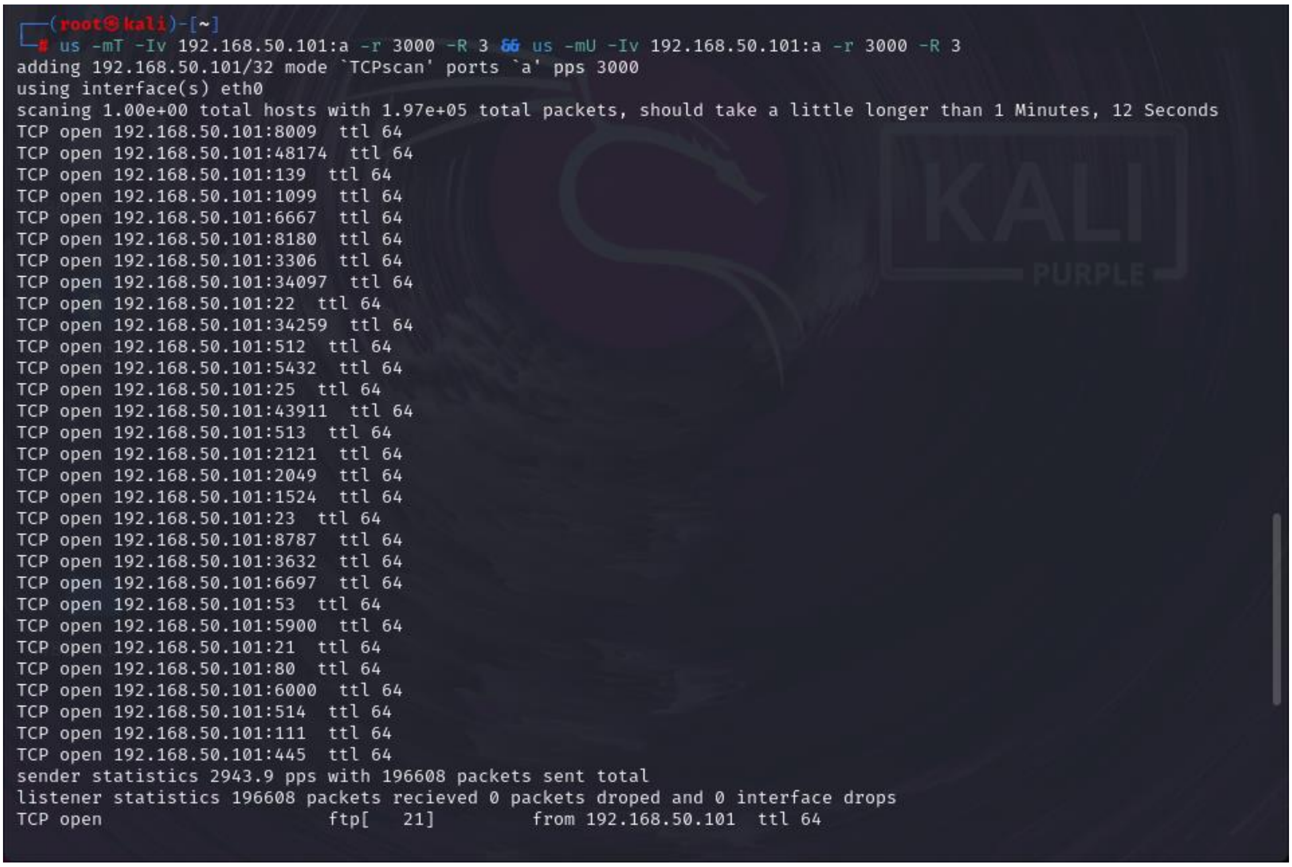


```
┌──(root㉿kali)-[~]
└─# hping3 --scan known 192.168.50.101
Scanning 192.168.50.101 (192.168.50.101), port known
264 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
All replies received. Done.
Not responding ports: (21 ftp) (22 ssh) (23 telnet) (25 smtp) (53 domain) (80 http) (111 sunrpc) (139 netbios-ssn) (
445 microsoft-d) (512 exec) (513 login) (514 shell) (1099 rmiregistry) (1524 ingreslock) (2049 nfs) (2121 iprop) (33
06 mysql) (3632 distcc) (5432 postgresql) (6000 x11) (6667 ircd) (6697 ircs-u)

┌──(root㉿kali)-[~]
```

8. us -mT -Iv 192.168.50.101:a -r 3000 -R 3 && us -mU -Iv 192.168.50.101:a -r 3000 -R 3

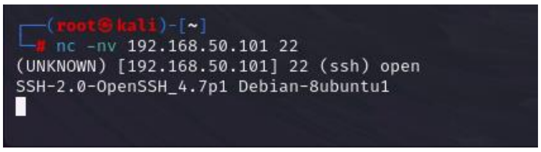
Scansione con unicornscan per TCP e UDP



```
┌──(root㉿kali)-[~]
└─# us -mT -Iv 192.168.50.101:a -r 3000 -R 3 && us -mU -Iv 192.168.50.101:a -r 3000 -R 3
adding 192.168.50.101/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
TCP open 192.168.50.101:8009  ttl 64
TCP open 192.168.50.101:48174  ttl 64
TCP open 192.168.50.101:139  ttl 64
TCP open 192.168.50.101:1099  ttl 64
TCP open 192.168.50.101:6667  ttl 64
TCP open 192.168.50.101:8180  ttl 64
TCP open 192.168.50.101:3306  ttl 64
TCP open 192.168.50.101:34097  ttl 64
TCP open 192.168.50.101:22  ttl 64
TCP open 192.168.50.101:34259  ttl 64
TCP open 192.168.50.101:512  ttl 64
TCP open 192.168.50.101:5432  ttl 64
TCP open 192.168.50.101:25  ttl 64
TCP open 192.168.50.101:43911  ttl 64
TCP open 192.168.50.101:513  ttl 64
TCP open 192.168.50.101:2121  ttl 64
TCP open 192.168.50.101:2049  ttl 64
TCP open 192.168.50.101:1524  ttl 64
TCP open 192.168.50.101:23  ttl 64
TCP open 192.168.50.101:8787  ttl 64
TCP open 192.168.50.101:3632  ttl 64
TCP open 192.168.50.101:6697  ttl 64
TCP open 192.168.50.101:53  ttl 64
TCP open 192.168.50.101:5900  ttl 64
TCP open 192.168.50.101:21  ttl 64
TCP open 192.168.50.101:80  ttl 64
TCP open 192.168.50.101:6000  ttl 64
TCP open 192.168.50.101:514  ttl 64
TCP open 192.168.50.101:111  ttl 64
TCP open 192.168.50.101:445  ttl 64
sender statistics 2943.9 pps with 196608 packets sent total
listener statistics 196608 packets recieved 0 packets droped and 0 interface drops
TCP open                     ftp[   21]         from 192.168.50.101  ttl 64
```

9. nc -nv 192.168.50.101 22

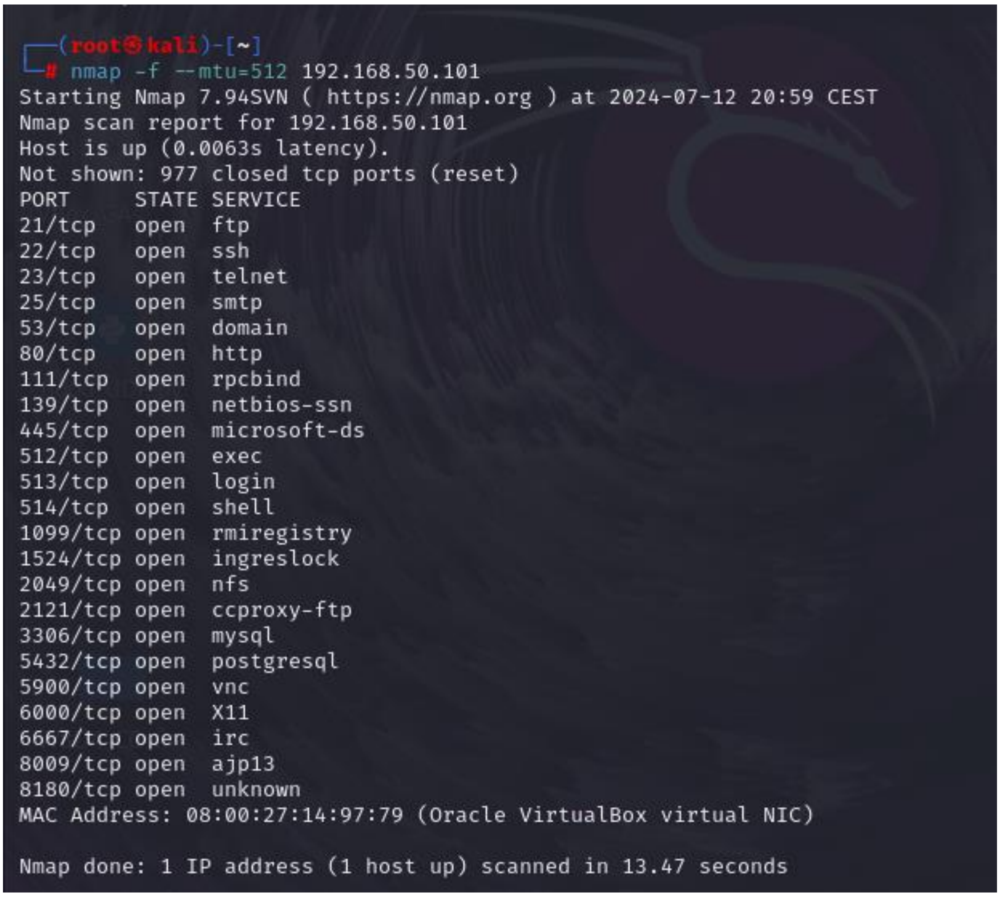
Connessione alla porta 22 SSH con netcat



```
┌──(root㉿kali)-[~]
└─# nc -nv 192.168.50.101 22
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
█
```

10. nmap -f --mtu=512 192.168.50.101

Scansione frammentata per evitare problemi di rilevamento intrusivo

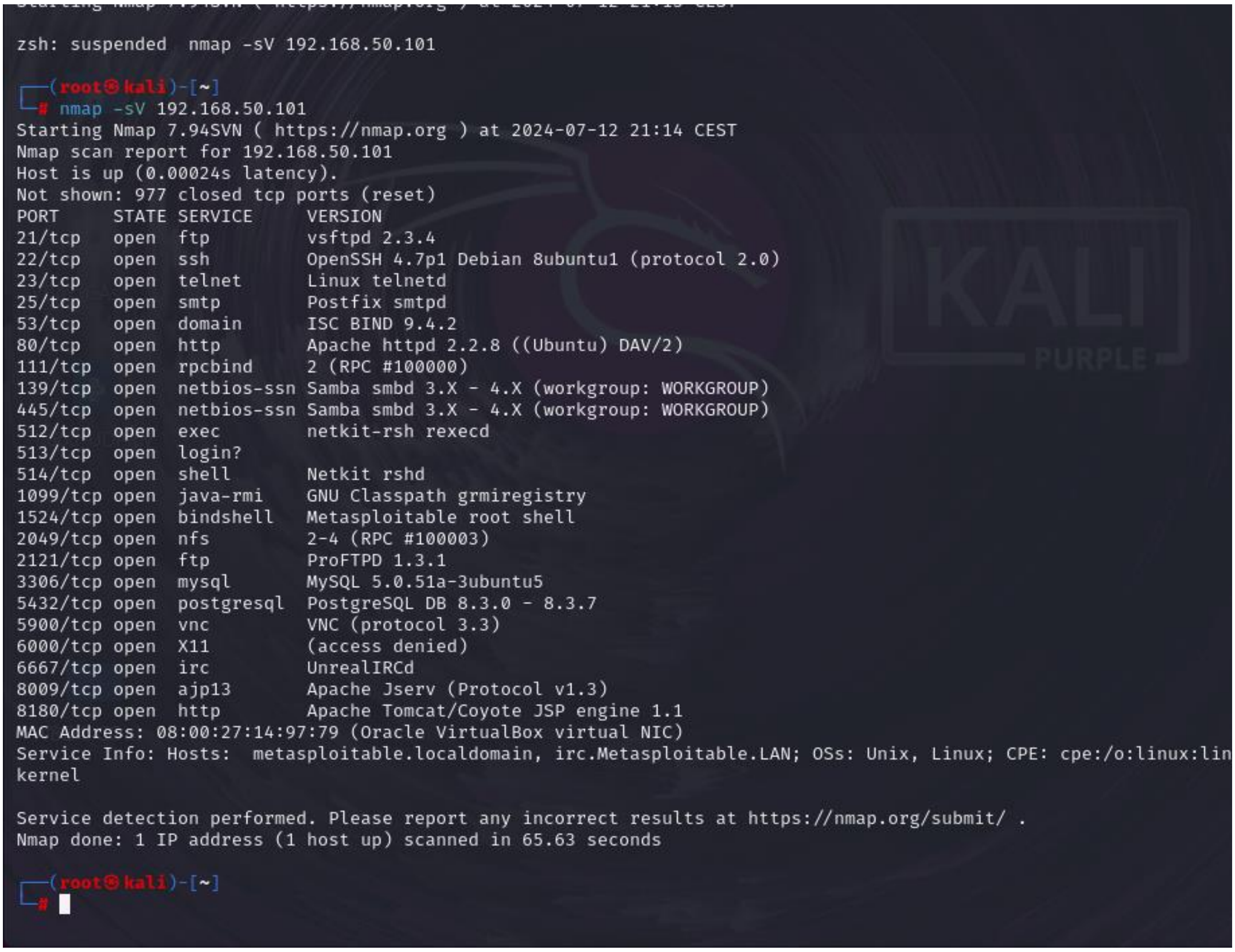


```
┌──(root㉿kali)-[~]
└─# nmap -f --mtu=512 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 20:59 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0063s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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: 08:00:27:14:97:79 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds
```

11.nmap -sV 192.168.50.101

Scansione per rilevare le versioni dei servizi in esecuzione



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 21:13 CEST

zsh: suspended  nmap -sV 192.168.50.101

┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 21:14 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00024s 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: 08:00:27:14:97:79 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:lin
kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.63 seconds

┌──(root㉿kali)-[~]
└─# 
```