W10D4 – Pratica

Epic Education Srl

Simulazione fase di raccolta informazioni pt. 2

(target Metasploitable)

Simone Giordano

22/09/2025

Contatti:

Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Sintesi esecutiva 3

Perimetro 3

Panoramica delle vulnerabilità 3

Raccolta info Metasploitable 4

Nmap -sn -PE 4

Netdiscover -r 4

Crackmapexec........ 4

NetExec........ 5

nmap --top-ports --open........ 5

nmap <IP> -p- -sV --reason --dns-server ns 5

Unicornscan........ 6

TCP Syn Scan con Nmap 8

Scansione con HPING3 9

Scansione porte con Netcat........ 9

Banner Grabbing con Netcat 10

Scansione porte con Nmap per info su servizi e versioni 10

Scansione con by-pass del Firewall con Nmap 11

Scansione con Masscan 11

Riepilogo informazioni........ 12

Metodi di evasione firewall con Nmap........ 14

NMAP con Timing 14

NMAP source port manipulation........ 14

FIN scan 15

Xmas 16

TCP Idle scanning........ 17

Fragmentation 18

Sintesi esecutiva

Questo documento riassume i risultati delle scansioni condotte sulla macchina *Metasploitable* utilizzando diversi strumenti. L'obiettivo è identificare le porte aperte e i servizi esposti ma anche di capire le differenze dei risultati delle diverse tecniche adottate.

Perimetro

Il target prefissato è la macchina Metasploitable

Panoramica delle vulnerabilità

Sono state identificate le seguenti porte aperte con i relativi servizi

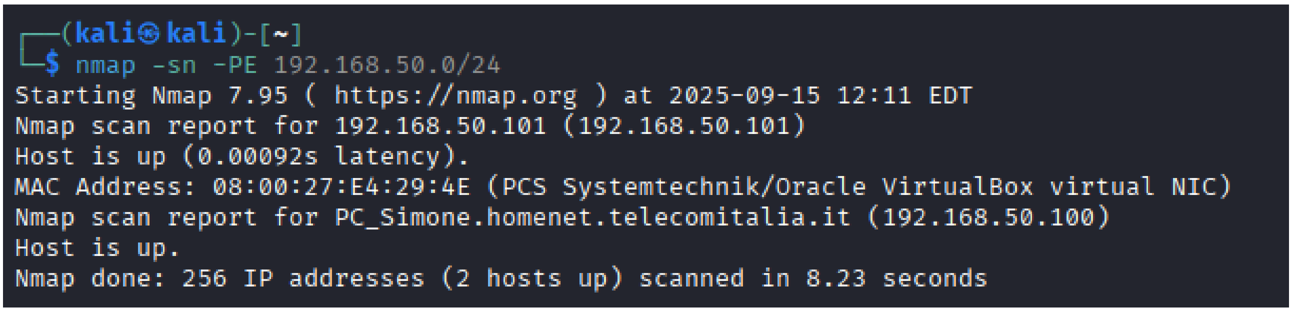
Port		Service
21	tcp	ftp
22	tcp	ssh
23	tcp	telnet
25	tcp	smtp
53	tcp	domain
80	tcp	http
111	tcp	rpcbind
139	tcp	netbios-ssn
445	tcp	netbios-ssn
512	tcp	exec
513	tcp	login
514	tcp	shell
1099	tcp	java-rmi
1524	tcp	bindshell
2049	tcp	nfs
2121	tcp	ccproxy-ftp
3306	tcp	mysql
5432	tcp	postgresql
5900	tcp	vnc
6000	tcp	X11
6667	tcp	irc
8009	tcp	ajp13
8180	tcp	http

Raccolta info Metasploitable

Nmap-sn-PE

-sn effettua un ping scan per verificare quali host sono attivi sulla rete
-PE specifica il tipo di ping ICMP Echo request da inviare, inviandolo rileverà se l’host risponde. Se risponde l’host è attivo.

Con il comando abbiamo eseguito un ping scan inviando ping echo request sulla rete 2 host: 192.168.50.100 (Kali) e 192.168.51.101 (Metasploitable).



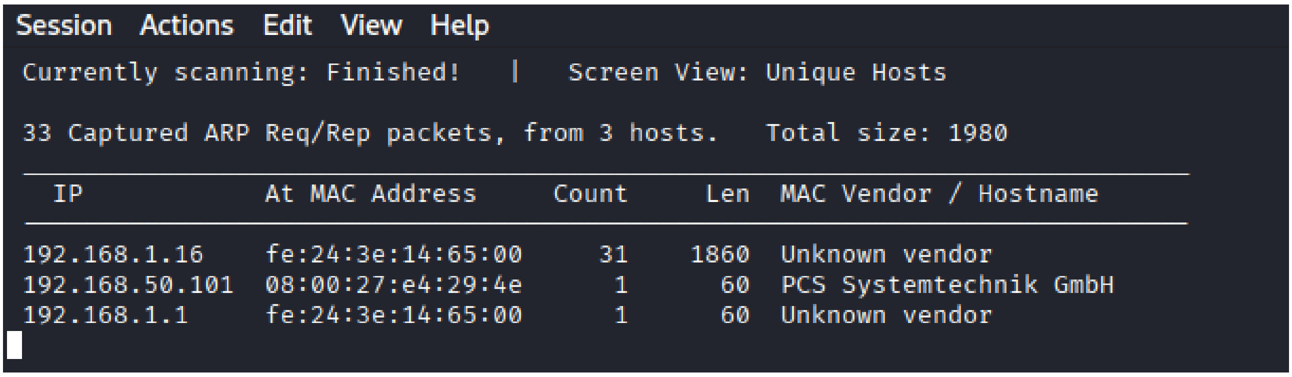
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 12:11 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00092s latency).
MAC Address: 08:00:27:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for PC_Simone.homenet.telecomitalia.it (192.168.50.100)
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 8.23 seconds
```

Netdiscover-r

sudo netdiscover -r 192.168.50.0/24

Netdiscover è uno strumento per **scoprire host nella rete locale** usando principalmente **pacchetti ARP**, -r indica il **range** (CIDR o intervallo) da scansionare

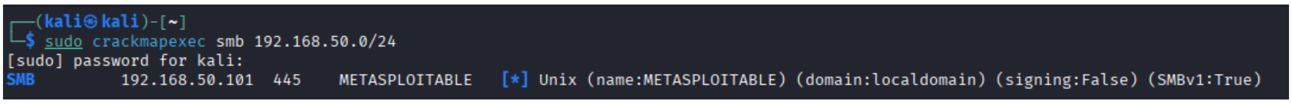
Nella nostra rete ha individuato la macchina Metasploitable 192.168.50.101



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

 33 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 1980
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.16    fe:24:3e:14:65:00     31    1860  Unknown vendor
 192.168.50.101  08:00:27:e4:29:4e      1      60  PCS Systemtechnik GmbH
 192.168.1.1     fe:24:3e:14:65:00      1      60  Unknown vendor
```

Crackmapexec

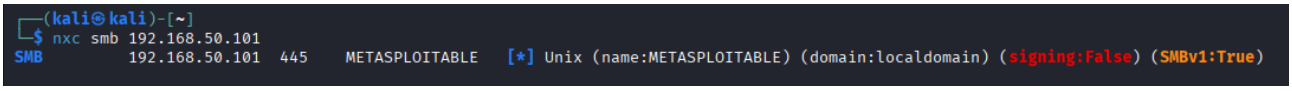
sudo crackmapexec smb 192.168.50.0/24
smb permette di fare una scansione semplice su tutta la subnet, in questo caso ha rilevato la macchina Metasploitable



```
┌──(kali㉿kali)-[~]
└─$ sudo crackmapexec smb 192.168.50.0/24
[sudo] password for kali:
SMB         192.168.50.101  445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)
```

NetExec

nxc smb 192.168.50.101

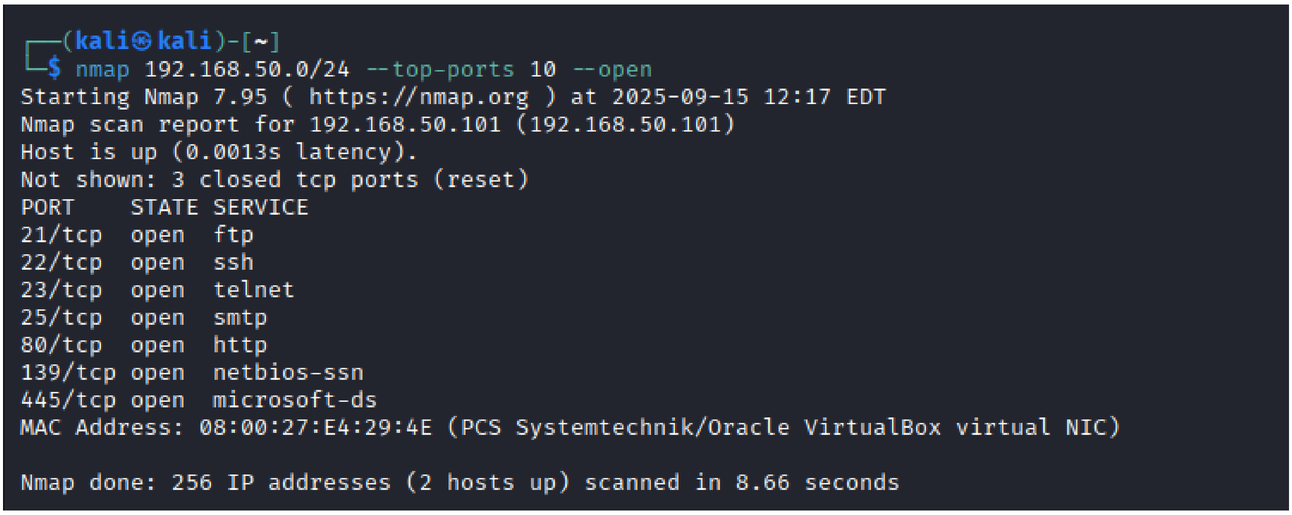


```
┌──(kali㉿kali)-[~]
└─$ nxc smb 192.168.50.101
SMB         192.168.50.101  445    METASPLOITABLE    [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)
```

nmap --top-ports --open

nmap 192.168.51.0/24 --top-ports 10 –open

--top-ports <N> dice a Nmap di scansionare **solo i N. (10) porte più comuni**, per una ricognizione rapida.
--open filtra l’output mostrando **solo le porte/host che risultano aperte/i**.

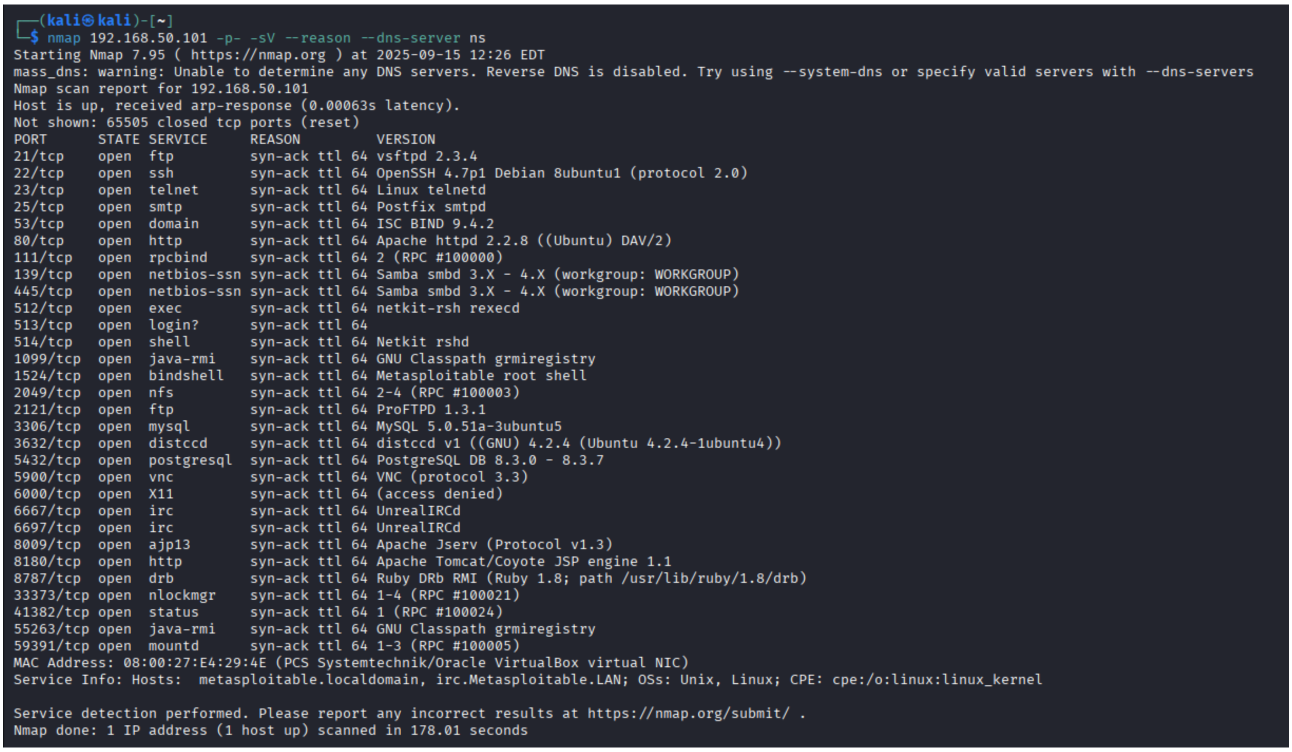


```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.0/24 --top-ports 10 --open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 12:17 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.0013s latency).
Not shown: 3 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  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:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 256 IP addresses (2 hosts up) scanned in 8.66 seconds
```

nmap <IP>-p--sV--reason--dns-server ns

nmap 192.168.50.101 -p- -sV --reason --dns-server ns

--reason ci fornisce info sul tipo di pacchetto di risposta ricevuto (reason)



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.101 -p- -sV --reason --dns-server ns
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 12:26 EDT
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, received arp-response (0.00063s 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)
33373/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
41382/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
55263/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
59391/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
MAC Address: 08:00:27:E4:29:4E (PCS Systemtechnik/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 178.01 seconds
```

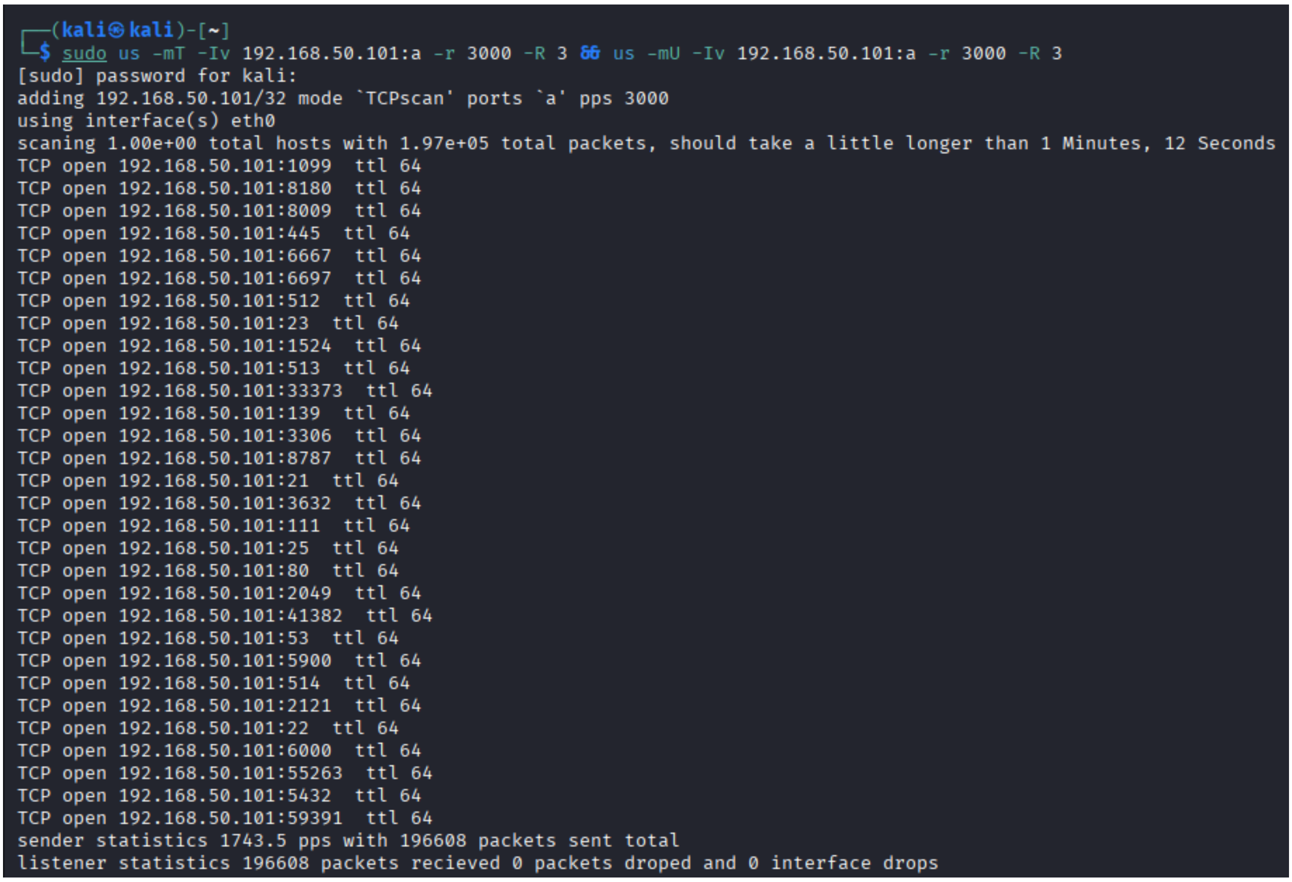
Unicornscan

Unicorn scan è uno strumento di **network reconnaissance e scanning ad alte prestazioni**.

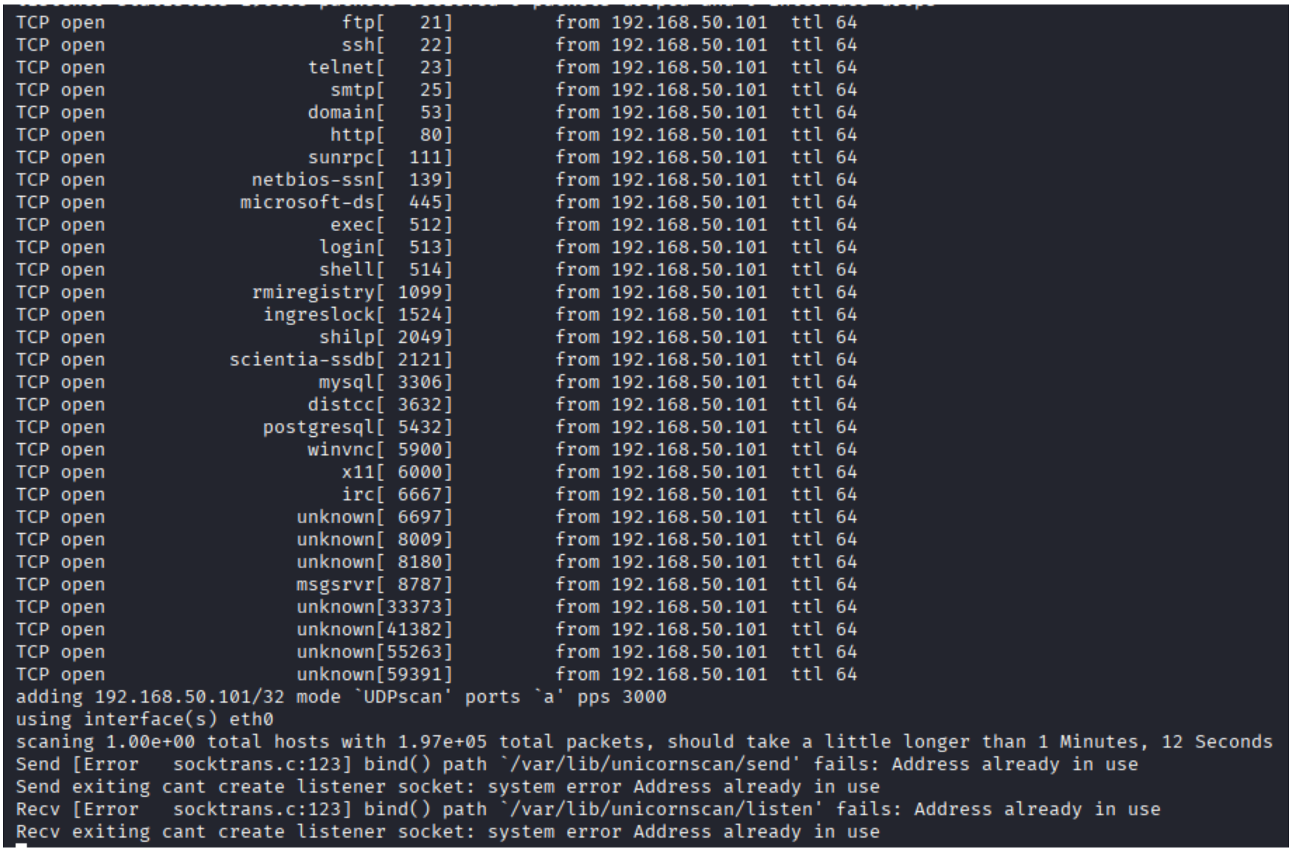
Ha scansionato tutte le porte TCP inviando 3000 pacchetti al secondo

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

us = Comado unicornscan
-mT = modalità **TCP scan**.
A = All, per scansionare tutte le porte
-mU = modalità **UDP scan**.
-r 3000 = rate ~ **3000 pacchetti al secondo**
-R 3 = retries o similar (3 ripetizioni/ tentativi).



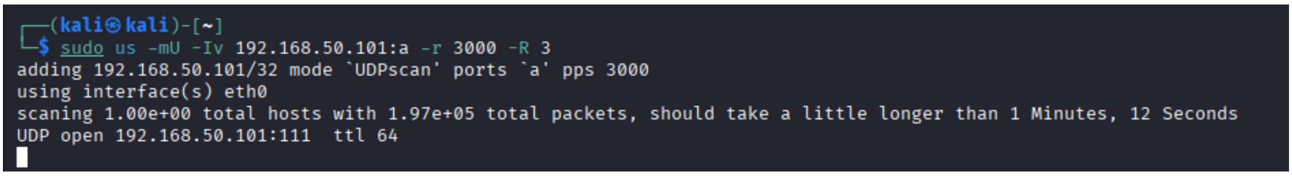
```
┌──(kali㉿kali)-[~]
└─$ sudo us -mT -Iv 192.168.50.101:a -r 3000 -R 3 && us -mU -Iv 192.168.50.101:a -r 3000 -R 3
[sudo] password for kali:
adding 192.168.50.101/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
TCP open 192.168.50.101:1099  ttl 64
TCP open 192.168.50.101:8180  ttl 64
TCP open 192.168.50.101:8009  ttl 64
TCP open 192.168.50.101:445  ttl 64
TCP open 192.168.50.101:6667  ttl 64
TCP open 192.168.50.101:6697  ttl 64
TCP open 192.168.50.101:512  ttl 64
TCP open 192.168.50.101:23  ttl 64
TCP open 192.168.50.101:1524  ttl 64
TCP open 192.168.50.101:513  ttl 64
TCP open 192.168.50.101:33373  ttl 64
TCP open 192.168.50.101:139  ttl 64
TCP open 192.168.50.101:3306  ttl 64
TCP open 192.168.50.101:8787  ttl 64
TCP open 192.168.50.101:21  ttl 64
TCP open 192.168.50.101:3632  ttl 64
TCP open 192.168.50.101:111  ttl 64
TCP open 192.168.50.101:25  ttl 64
TCP open 192.168.50.101:80  ttl 64
TCP open 192.168.50.101:2049  ttl 64
TCP open 192.168.50.101:41382  ttl 64
TCP open 192.168.50.101:53  ttl 64
TCP open 192.168.50.101:5900  ttl 64
TCP open 192.168.50.101:514  ttl 64
TCP open 192.168.50.101:2121  ttl 64
TCP open 192.168.50.101:22  ttl 64
TCP open 192.168.50.101:6000  ttl 64
TCP open 192.168.50.101:55263  ttl 64
TCP open 192.168.50.101:5432  ttl 64
TCP open 192.168.50.101:59391  ttl 64
sender statistics 1743.5 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
TCP open                     ssh[   22]         from 192.168.50.101  ttl 64
TCP open                  telnet[   23]         from 192.168.50.101  ttl 64
TCP open                    smtp[   25]         from 192.168.50.101  ttl 64
TCP open                  domain[   53]         from 192.168.50.101  ttl 64
TCP open                    http[   80]         from 192.168.50.101  ttl 64
TCP open                  sunrpc[  111]         from 192.168.50.101  ttl 64
TCP open             netbios-ssn[  139]         from 192.168.50.101  ttl 64
TCP open            microsoft-ds[  445]         from 192.168.50.101  ttl 64
TCP open                    exec[  512]         from 192.168.50.101  ttl 64
TCP open                   login[  513]         from 192.168.50.101  ttl 64
TCP open                   shell[  514]         from 192.168.50.101  ttl 64
TCP open             rmiregistry[ 1099]         from 192.168.50.101  ttl 64
TCP open              ingreslock[ 1524]         from 192.168.50.101  ttl 64
TCP open                   shilp[ 2049]         from 192.168.50.101  ttl 64
TCP open            scientia-ssdb[ 2121]        from 192.168.50.101  ttl 64
TCP open                   mysql[ 3306]         from 192.168.50.101  ttl 64
TCP open                  distcc[ 3632]         from 192.168.50.101  ttl 64
TCP open              postgresql[ 5432]         from 192.168.50.101  ttl 64
TCP open                  winvnc[ 5900]         from 192.168.50.101  ttl 64
TCP open                     x11[ 6000]         from 192.168.50.101  ttl 64
TCP open                    irc[ 6667]         from 192.168.50.101  ttl 64
TCP open                 unknown[ 6697]         from 192.168.50.101  ttl 64
TCP open                 unknown[ 8009]         from 192.168.50.101  ttl 64
TCP open                 unknown[ 8180]         from 192.168.50.101  ttl 64
TCP open                 msgsrvr[ 8787]         from 192.168.50.101  ttl 64
TCP open                 unknown[33373]         from 192.168.50.101  ttl 64
TCP open                 unknown[41382]         from 192.168.50.101  ttl 64
TCP open                 unknown[55263]         from 192.168.50.101  ttl 64
TCP open                 unknown[59391]         from 192.168.50.101  ttl 64
adding 192.168.50.101/32 mode `UDPscan' 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
Send [Error   socktrans.c:123] bind() path `/var/lib/unicornscan/send' fails: Address already in use
Send exiting cant create listener socket: system error Address already in use
Recv [Error   socktrans.c:123] bind() path `/var/lib/unicornscan/listen' fails: Address already in use
Recv exiting cant create listener socket: system error Address already in use
```

Lo scan UDP non ha funzionato, quindi ho provato a lanciarlo da solo senza concatenarlo con la scansione TCP

Dopo un’ora ancora non aveva finito la scansione



```
┌──(kali㉿kali)-[~]
└─$ sudo us -mU -Iv 192.168.50.101:a -r 3000 -R 3
adding 192.168.50.101/32 mode `UDPscan' 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
UDP open 192.168.50.101:111  ttl 64
```

TCP Syn Scan con Nmap

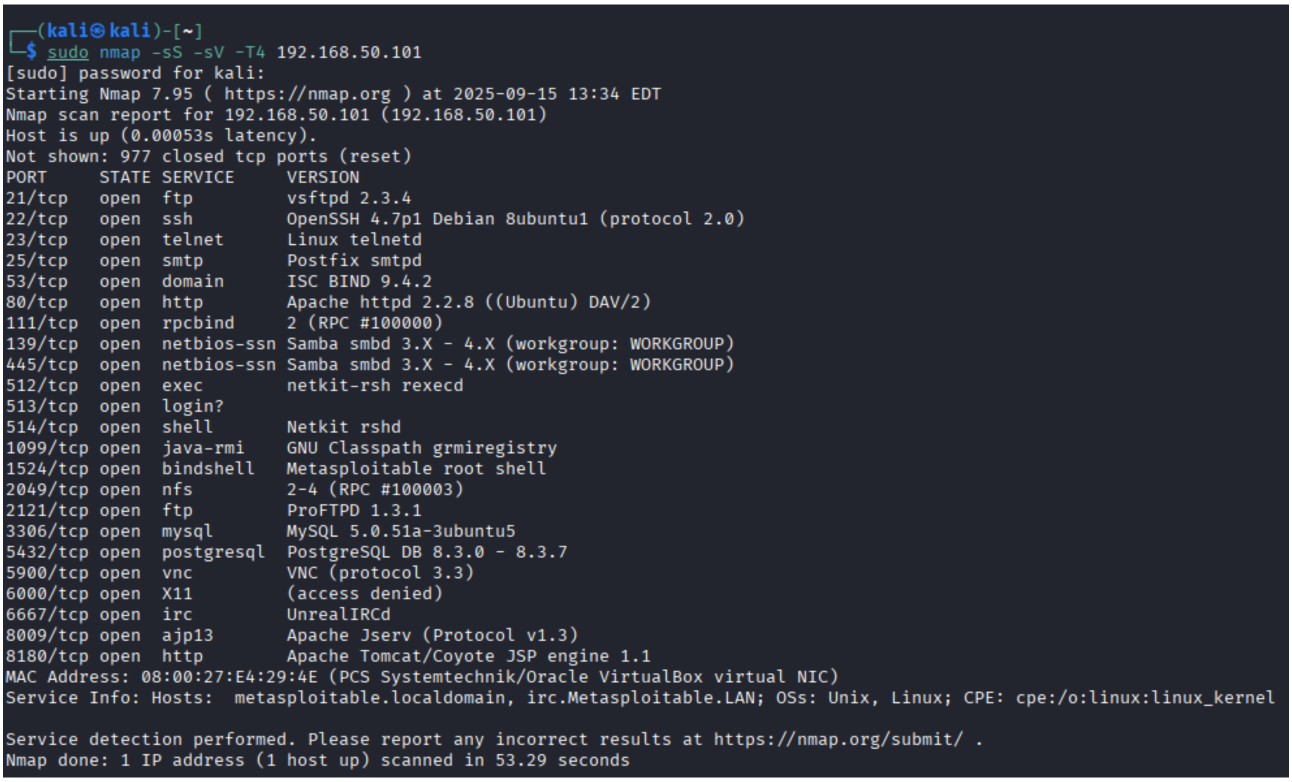
sudo nmap -sS -sV -T4 192.168.50.101

-T4 serve per accelerare la scansione, regola:

- La velocità
- Il parallelismo (più host/porte interrogate parallelamente)
- Il timeout della scansione

-T0 = paranoid (lentissimo, usato per evitare IDS)
-T1 = sneaky
-T2 = polite
-T3 = normal (default)
-T4 = aggressive (veloce, usato su LAN/ambienti affidabili)
-T5 = insane (massimo aggressività, rischioso)

In questo caso T4 accelera i risultati di -sS e -sV. Velocizzare ovviamente riduce l’affidabilità dei risultati.

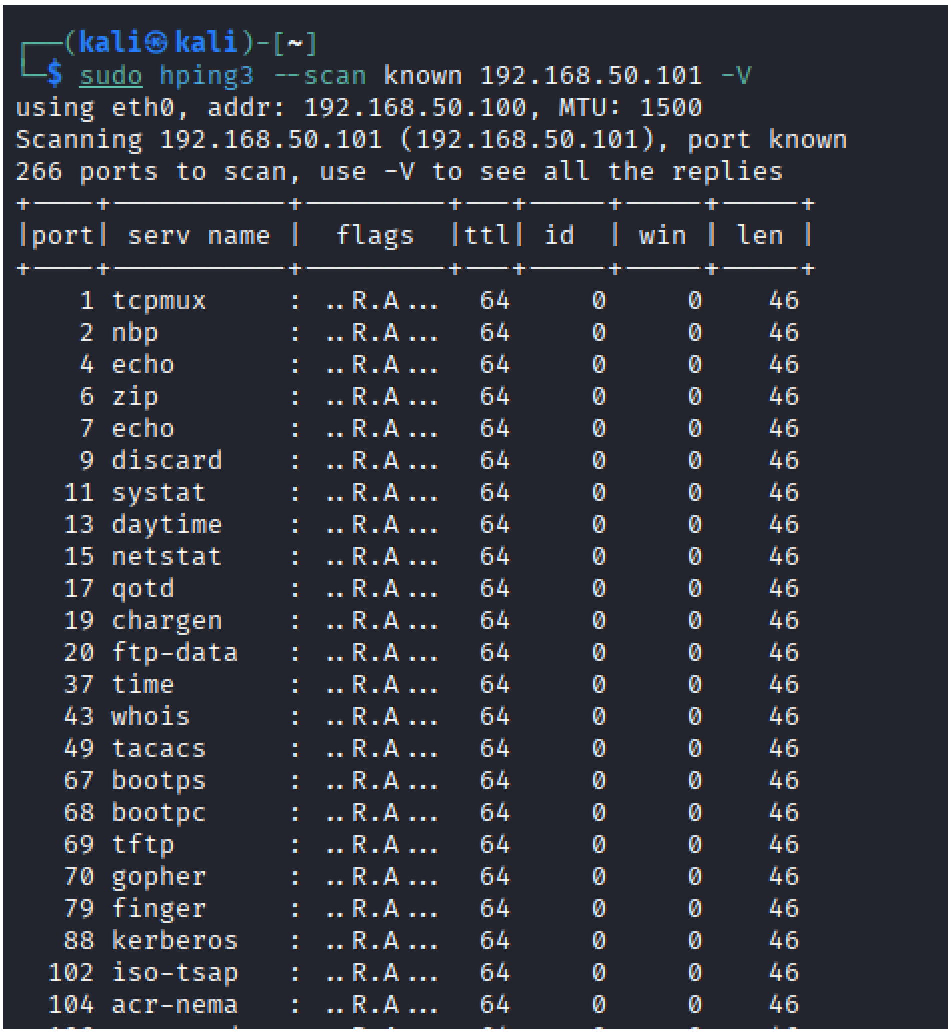


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -T4 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 13:34 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00053s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     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:E4:29:4E (PCS Systemtechnik/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 53.29 seconds
```

Scansione con HPING3

sudo hping3 --scan known 192.168.50.101

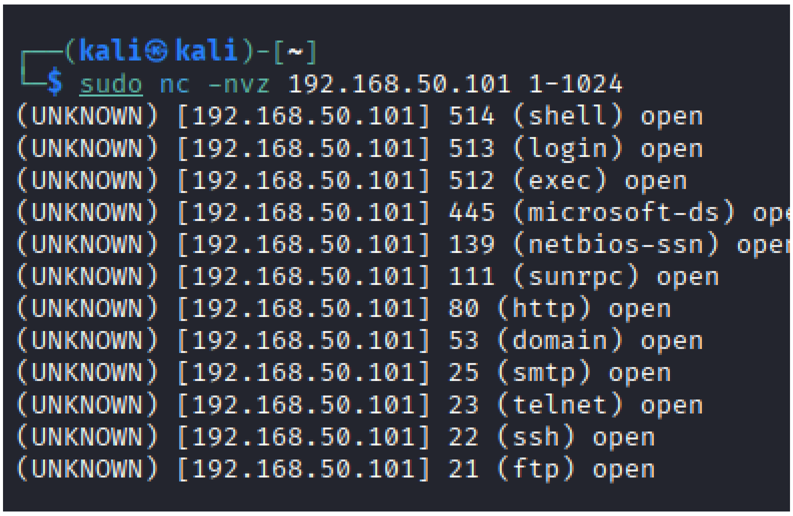
HPING, rispetto a ping è in grado di inviare non solo richieste echo ICMP ma anche TCP, UDP, ICMP e RAW-IP



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --scan known 192.168.50.101 -V
using eth0, addr: 192.168.50.100, MTU: 1500
Scanning 192.168.50.101 (192.168.50.101), port known
266 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
    1 tcpmux     : ..R.A...  64     0     0    46
    2 nbp        : ..R.A...  64     0     0    46
    4 echo       : ..R.A...  64     0     0    46
    6 zip        : ..R.A...  64     0     0    46
    7 echo       : ..R.A...  64     0     0    46
    9 discard    : ..R.A...  64     0     0    46
   11 systat     : ..R.A...  64     0     0    46
   13 daytime    : ..R.A...  64     0     0    46
   15 netstat    : ..R.A...  64     0     0    46
   17 qotd       : ..R.A...  64     0     0    46
   19 chargen    : ..R.A...  64     0     0    46
   20 ftp-data   : ..R.A...  64     0     0    46
   37 time       : ..R.A...  64     0     0    46
   43 whois      : ..R.A...  64     0     0    46
   49 tacacs     : ..R.A...  64     0     0    46
   67 bootps     : ..R.A...  64     0     0    46
   68 bootpc     : ..R.A...  64     0     0    46
   69 tftp       : ..R.A...  64     0     0    46
   70 gopher     : ..R.A...  64     0     0    46
   79 finger     : ..R.A...  64     0     0    46
   88 kerberos   : ..R.A...  64     0     0    46
  102 iso-tsap   : ..R.A...  64     0     0    46
  104 acr-nema   : ..R.A...  64     0     0    46
```

Scansione porte con Netcat

sudo nc -nvz 192.168.50.101 1-1024

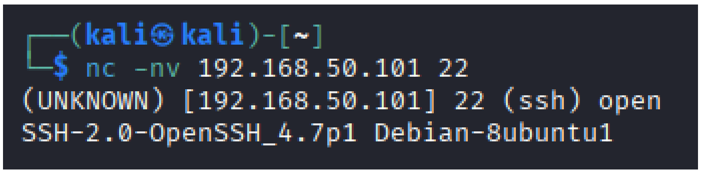


```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nvz 192.168.50.101 1-1024
(UNKNOWN) [192.168.50.101] 514 (shell) open
(UNKNOWN) [192.168.50.101] 513 (login) open
(UNKNOWN) [192.168.50.101] 512 (exec) open
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) ope
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) oper
(UNKNOWN) [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
```

Banner Grabbing con Netcat

nc -nv 192.168.50.101 22

È stata stabilita una connessione con la porta 22 ottenendo il banner SSH.

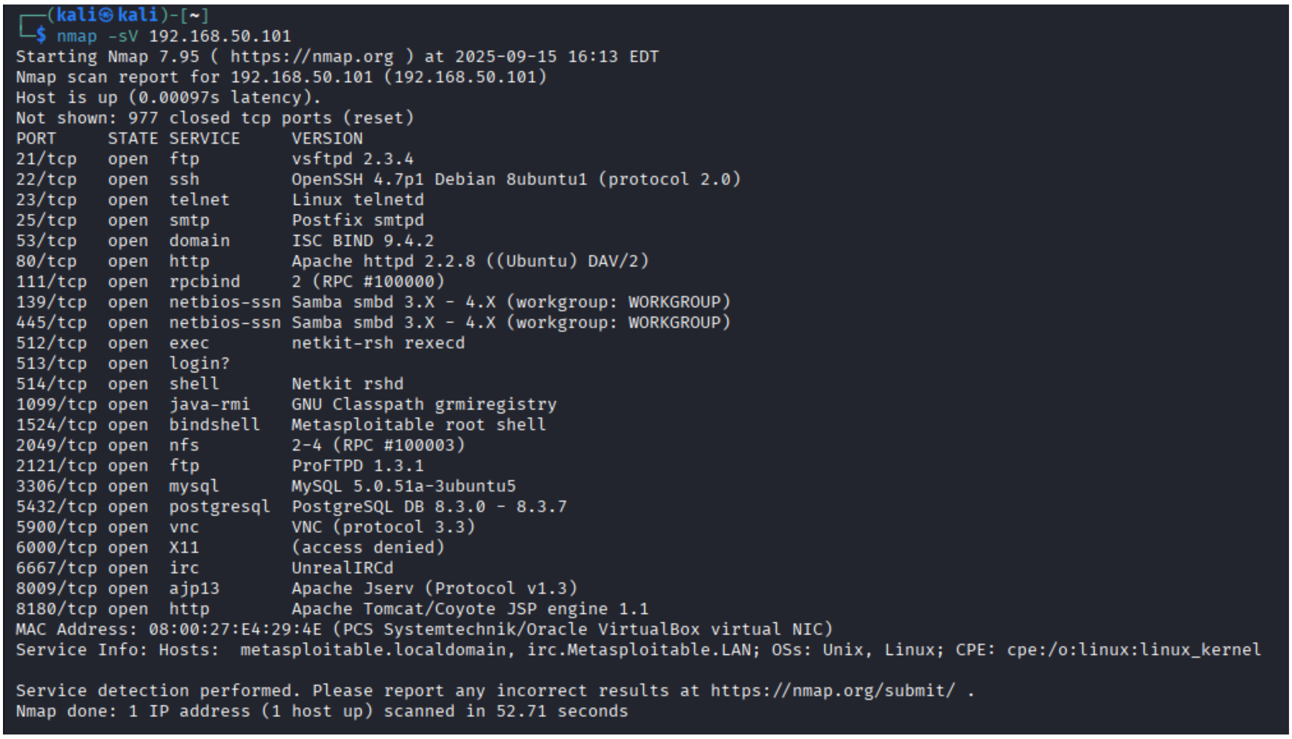


```
┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.50.101 22
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Scansione porte con Nmap per info su servizi e versioni

nmap -sV 192.168.50.101

La scansione rileva le porte aperte, i relativi servizi e le informazioni sulle versioni.

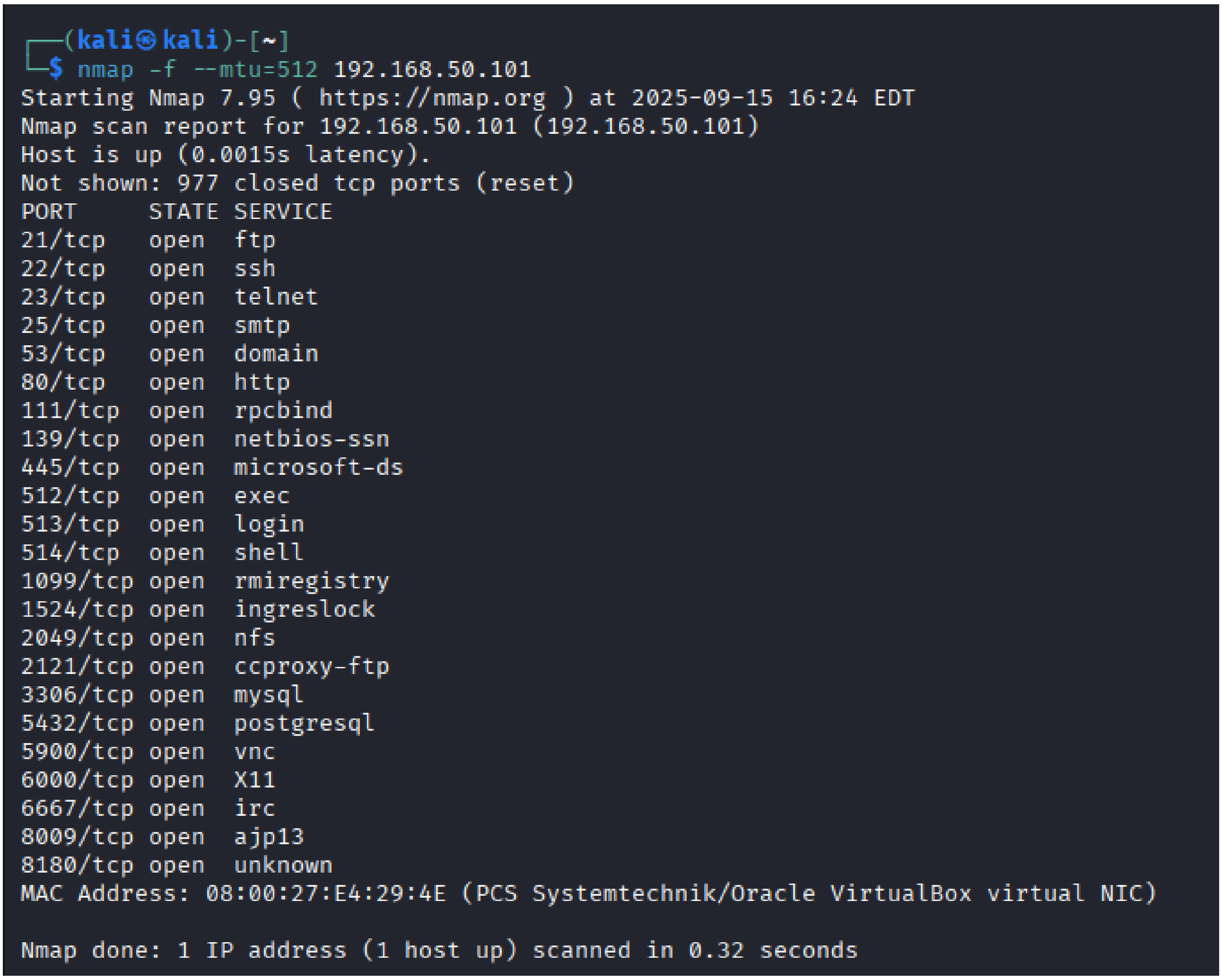


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 16:13 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00097s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         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:E4:29:4E (PCS Systemtechnik/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 52.71 seconds
```

Scansione con by-pass del Firewall con Nmap

nmap -f --mtu=512 192.168.50.101

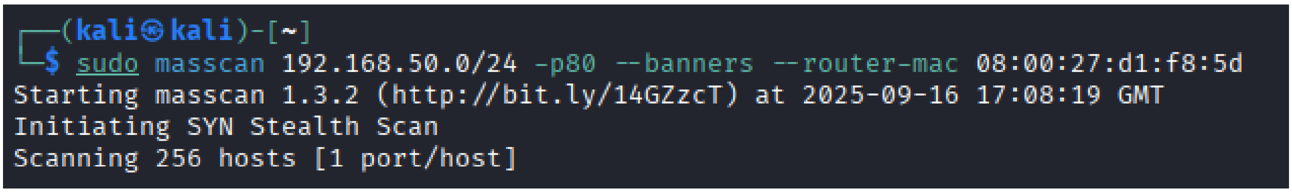
-f frammenta i pacchetti inviati da nmap
--mtu 512 imposta la dimensione (512 byte) del frammento



```
┌──(kali㉿kali)-[~]
└─$ nmap -f --mtu=512 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 16:24 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.0015s 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:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

Scansione con Masscan

Masscan è uno scanner molto veloce, per scansioni massive, scansionerà solo la porta 80 di tutti gli indirizzi della subnet 192.168.50.0/24.



```
┌──(kali㉿kali)-[~]
└─$ sudo masscan 192.168.50.0/24 -p80 --banners --router-mac 08:00:27:d1:f8:5d
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-09-16 17:08:19 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
```

Riepilogo informazioni

Host rete		Ruolo macchina	OS
192.168.50.101	METASPLOITABLE	Macchina target	Linux 2.6.X
192.168.50.100	KALI	Macchina attaccante	

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4	
22	tcp	open	ssh	syn-ack	OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0
23	tcp	open	telnet	syn-ack	Linux telnetd		
25	tcp	open	smtp	syn-ack	Postfix smtpd		
53	tcp	open	domain	syn-ack	ISC BIND	9.4.2	
80	tcp	open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
512	tcp	open	exec	syn-ack	netkit-rsh rexecd		
513	tcp	open	login	syn-ack			
514	tcp	open	shell	syn-ack	Netkit rshd		
1099	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
1524	tcp	open	bindshell	syn-ack	Metasploitable root shell		
2049	tcp	open	nfs	syn-ack		2-4	RPC #100003

2121	tcp	open	ftp	syn-ack	ProFTPD	1.3.1	
3306	tcp	open	mysql	syn-ack	MySQL	5.0.51a-3ubuntu5	
3632	tcp	open	distccd	syn-ack	distccd	v1	(GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
5432	tcp	open	postgresql	syn-ack	PostgreSQL DB	8.3.0 - 8.3.7	
5900	tcp	open	vnc	syn-ack	VNC		protocol 3.3
6000	tcp	open	X11	syn-ack			access denied
6667	tcp	open	irc	syn-ack	UnrealIRCd		
6697	tcp	open	irc	syn-ack	UnrealIRCd		
8009	tcp	open	ajp13	syn-ack	Apache Jserv		Protocol v1.3
8180	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	
8787	tcp	open	drb	syn-ack	Ruby DRb RMI		Ruby 1.8; path /usr/lib/ruby/1.8/drb
####	tcp	open	nlockmgr	syn-ack		1-4	RPC #100021
####	tcp	open	status	syn-ack		1	RPC #100024
####	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
####	tcp	open	mountd	syn-ack		1-3	RPC #100005

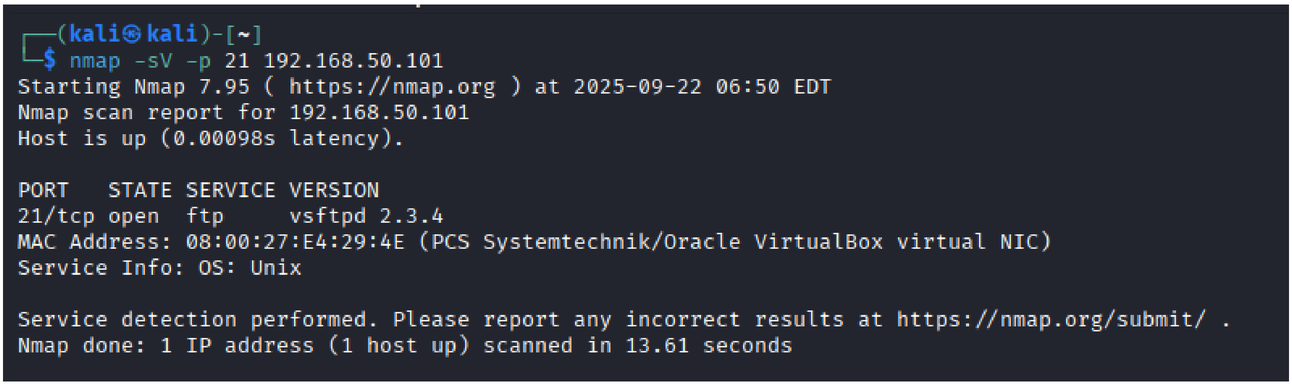
Metodi di evasione firewall con Nmap

NMAP con Timing

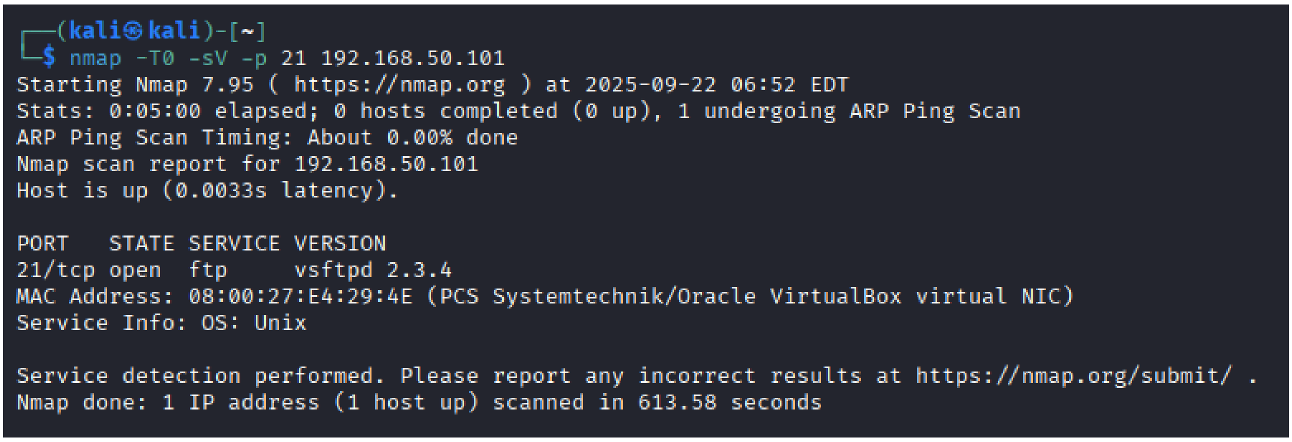
Il timing impostato a 0 allunga il tempo tra una richiesta e l'altra e il parallelismo per eludere IPS/IDS.

In questo caso ho eseguito nmap -T0 su una sola porta per evitare scansioni lunghissime.

Di seguito possiamo notare che la scansione senza il timing ha impiegato 13,61 secondi, mentre quella con il -T0 ha impiegato 613,58 secondi.



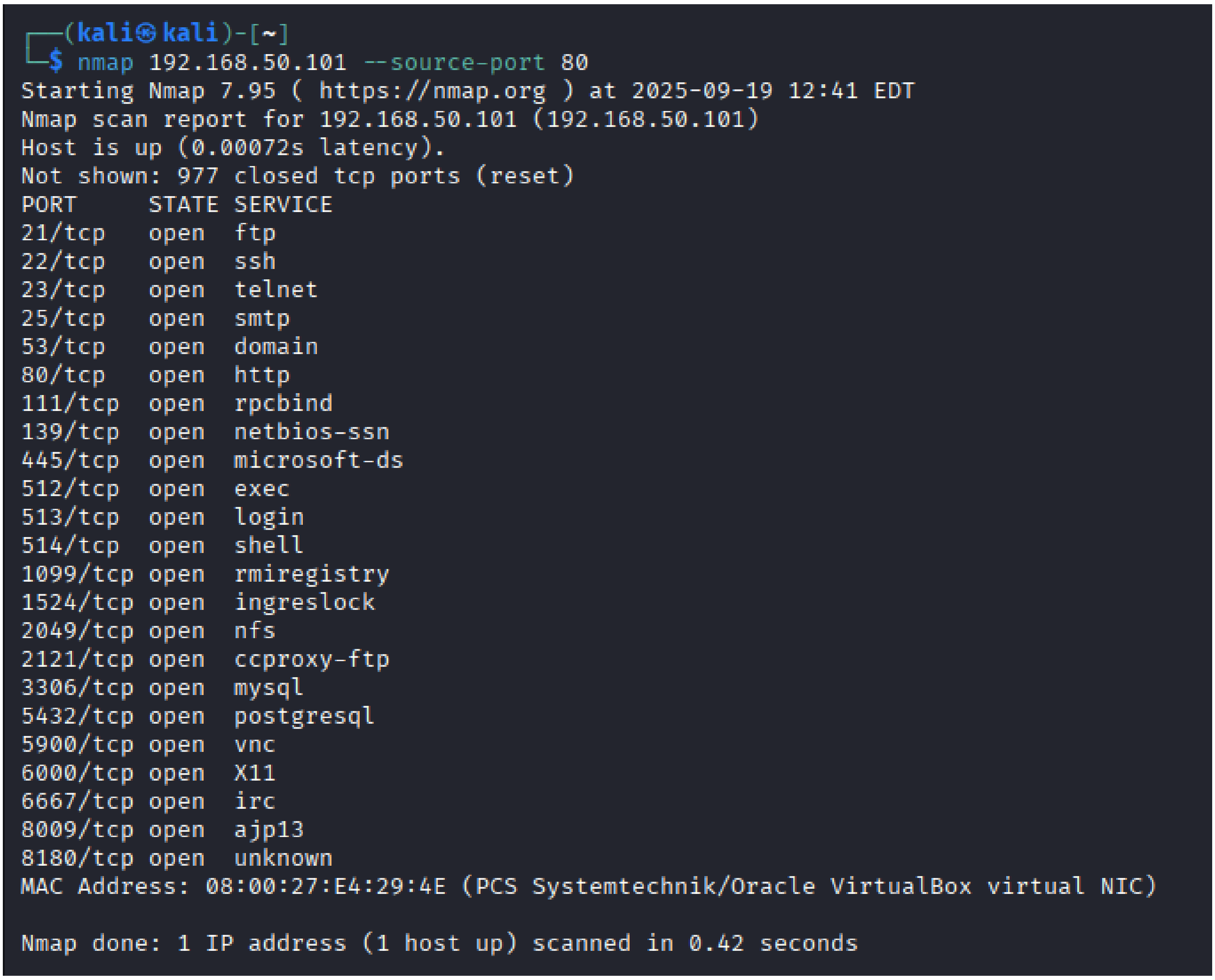
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 21 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 06:50 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00098s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 08:00:27:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.61 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -T0 -sV -p 21 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 06:52 EDT
Stats: 0:05:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 0.00% done
Nmap scan report for 192.168.50.101
Host is up (0.0033s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 08:00:27:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 613.58 seconds
```

NMAP source port manipulation

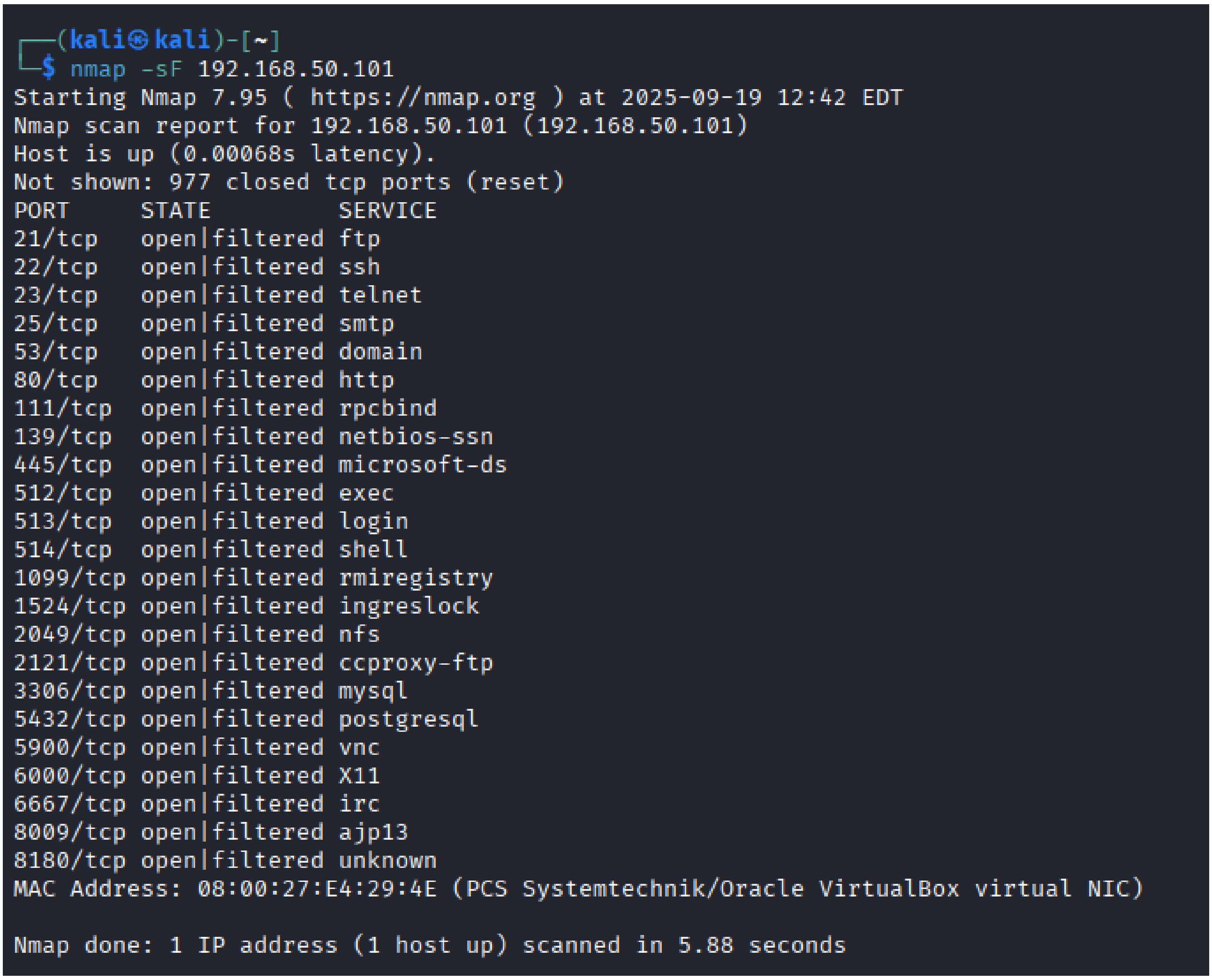
Per eludere IPS/IDS è possibile inviare pacchetti da porte note, come la porta 80.



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.101 --source-port 80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 12:41 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00072s 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:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

FIN scan

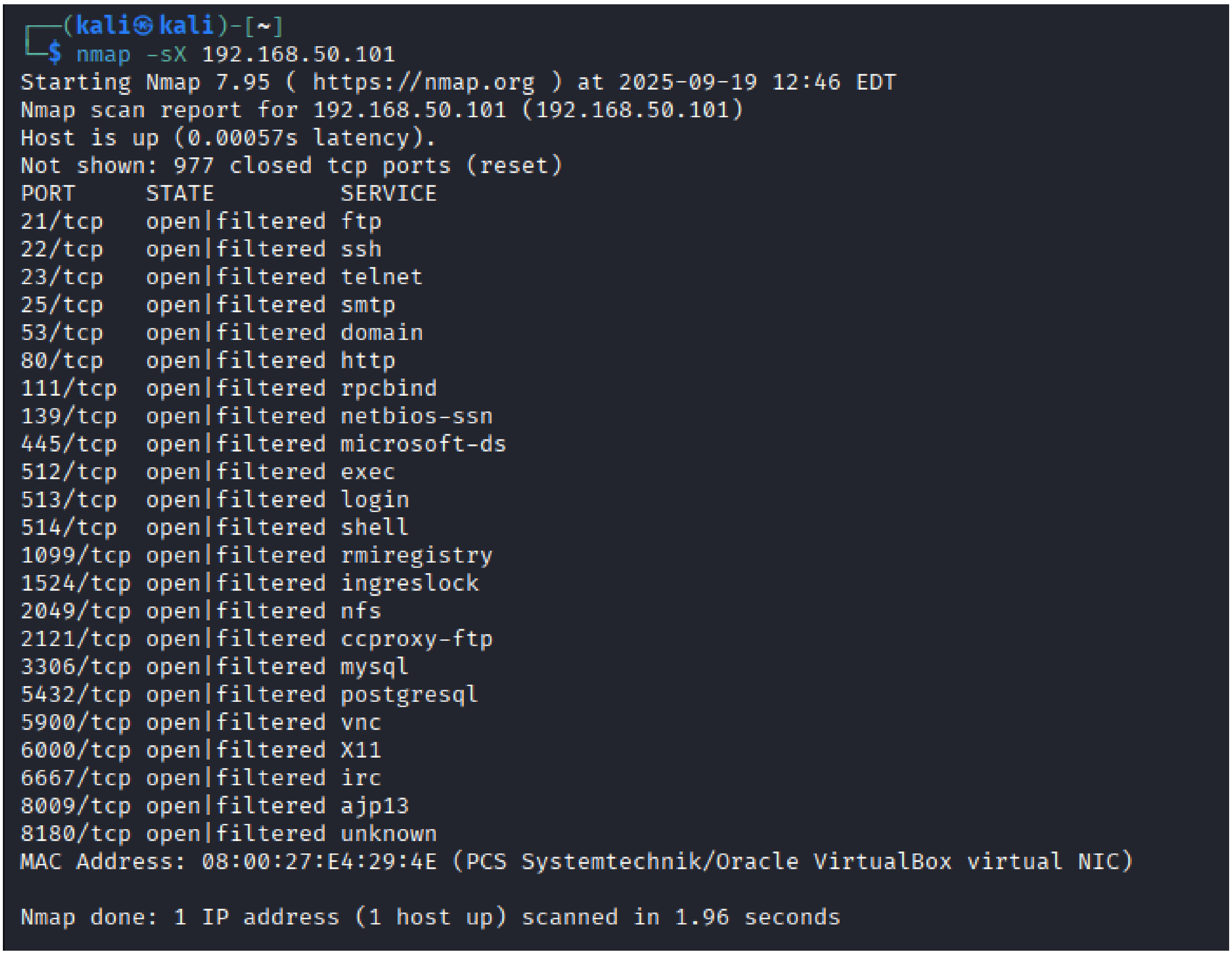
Lo scan invia un pacchetto con solo il flag FIN (per chiudere la sessione). Non seguendo il normale three-way handshake potrebbe passare più inosservato rispetto a uno scan SYN classico.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sF 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 12:42 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.88 seconds
```

Xmas

È un tipo di scan TCP che invia pacchetti con i flag FIN, PSH e URG. Anche questo scan, non seguendo il normale three-way handshake, potrebbe passare più inosservato rispetto a uno scan SYN classico.



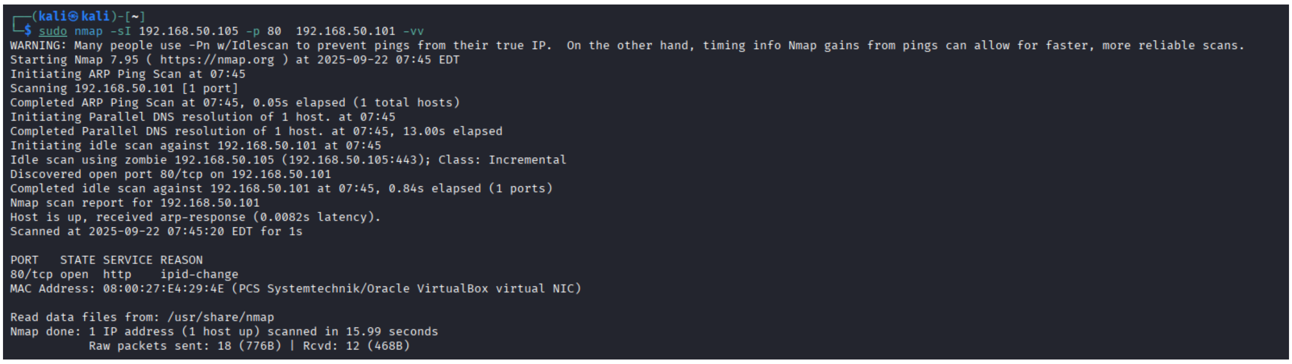
```
┌──(kali㉿kali)-[~]
└─$ nmap -sX 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 12:46 EDT
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.00057s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.96 seconds
```

TCP Idle scanning

Tecnica che sfrutta un terzo host “zombie” per nascondere lo scanning.

Lo scanner non manda i pacchetti direttamente al target ma forgia (esegue lo sproofing) pacchetti con l’IP sorgente dello zombie. Lo scanner osserva lo zombie per dedurre se il target ha risposto o meno.

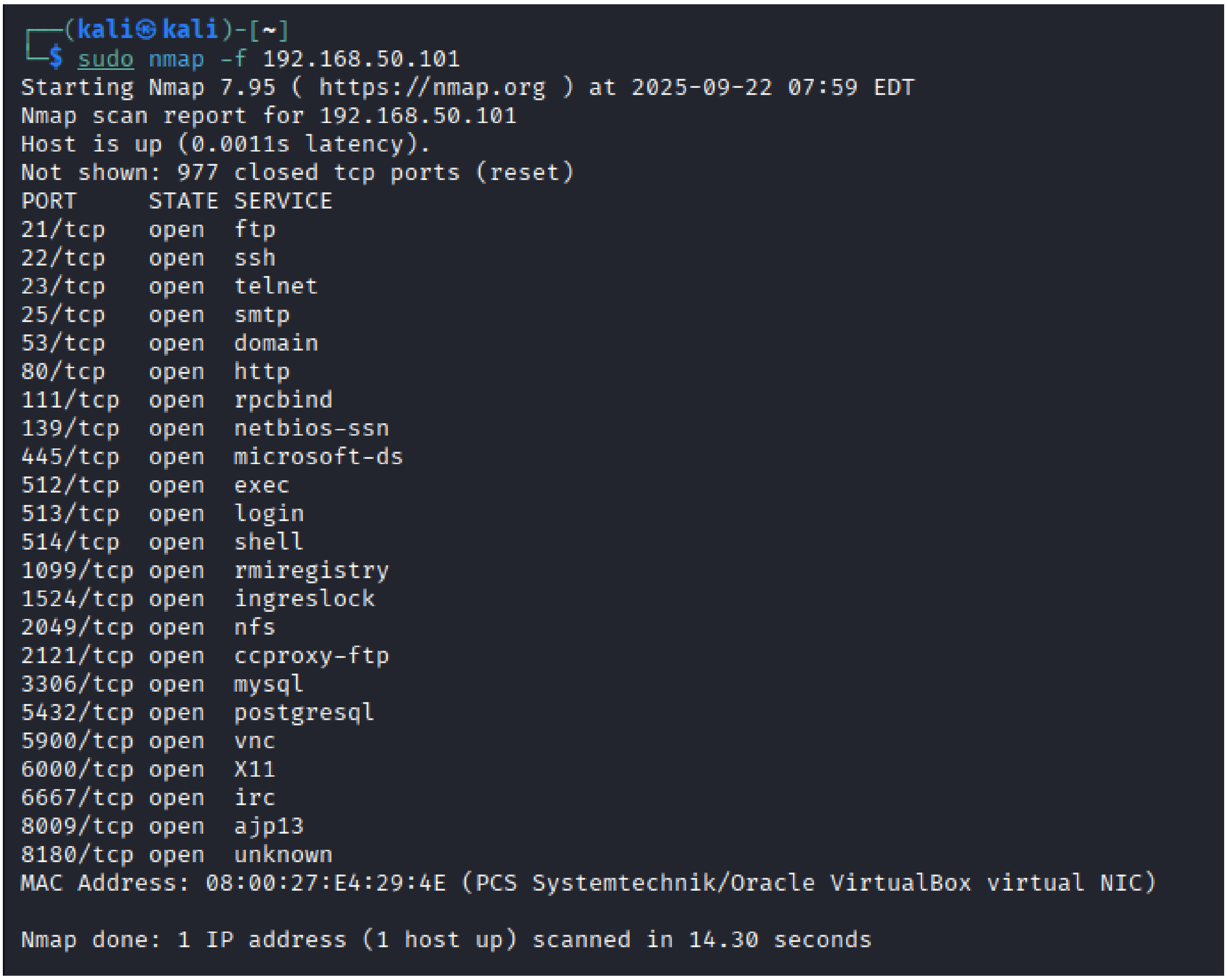
Kali (scanner): **192.168.50.100**
Metasploitable (target): **192.168.50.101**
Windows (zombie): **192.168.50.105**



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sI 192.168.50.105 -p 80  192.168.50.101 -vv
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On the other hand, timing info Nmap gains from pings can allow for faster, more reliable scans.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 07:45 EDT
Initiating ARP Ping Scan at 07:45
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 07:45, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:45
Completed Parallel DNS resolution of 1 host. at 07:45, 13.00s elapsed
Initiating idle scan against 192.168.50.101 at 07:45
Idle scan using zombie 192.168.50.105 (192.168.50.105:443); Class: Incremental
Discovered open port 80/tcp on 192.168.50.101
Completed idle scan against 192.168.50.101 at 07:45, 0.84s elapsed (1 ports)
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.0082s latency).
Scanned at 2025-09-22 07:45:20 EDT for 1s

PORT   STATE SERVICE REASON
80/tcp open  http    ipid-change
MAC Address: 08:00:27:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.99 seconds
           Raw packets sent: 18 (776B) | Rcvd: 12 (468B)
```

Fragmentation

La **frammentazione IP** consiste nel dividere un pacchetto TCP/IP in più pezzi più piccoli, prima di inviarlo alla destinazione. Questo può servire a evitare IDS/IPS, perché alcuni firewall o IDS non riassemblano correttamente i pacchetti frammentati.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -f 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 07:59 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0011s 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:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.30 seconds
```