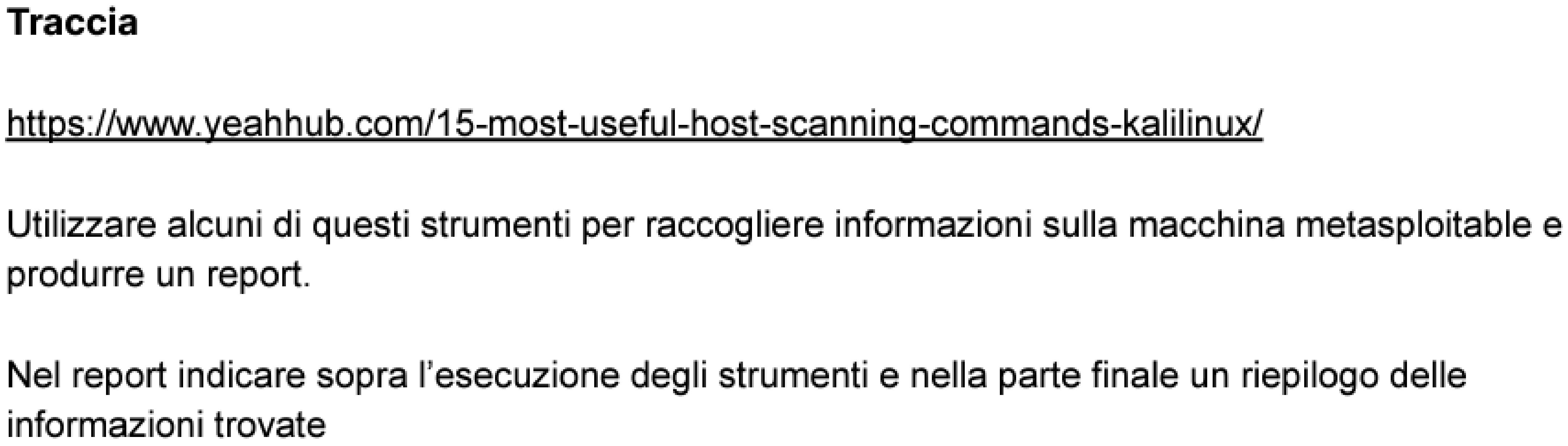
W10D4

FASE DI RACCOLTA INFORMAZIONI

La traccia



Traccia

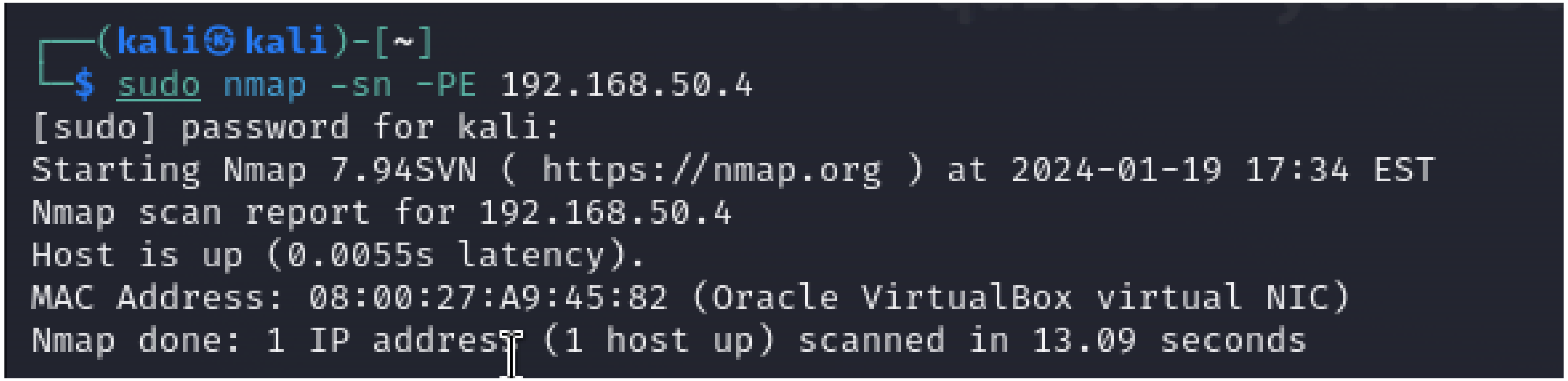
https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/

Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable e produrre un report.

Nel report indicare sopra l’esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

1) nmap -sn -PE <target>

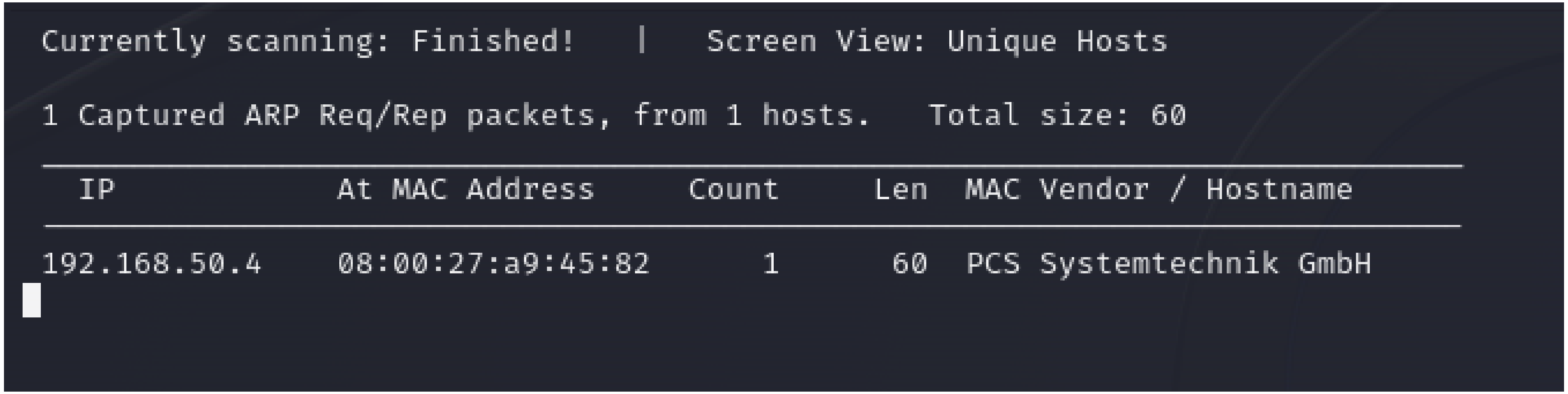
Con tale comando facciamo una scansione ping col protocollo ICMP (echo) che ci dirà semplicemente se l'host è attivo.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.50.4
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 17:34 EST
Nmap scan report for 192.168.50.4
Host is up (0.0055s latency).
MAC Address: 08:00:27:A9:45:82 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
```

2) netdiscover -r <target>

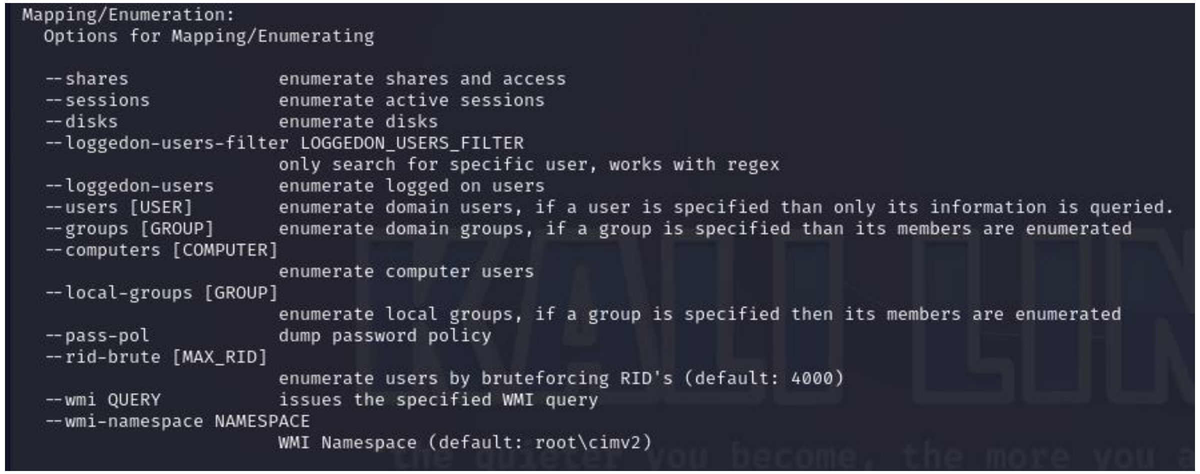
Questo è l’output di netdiscover che ci aiuta a scoprire quali host sono attivi in una rete



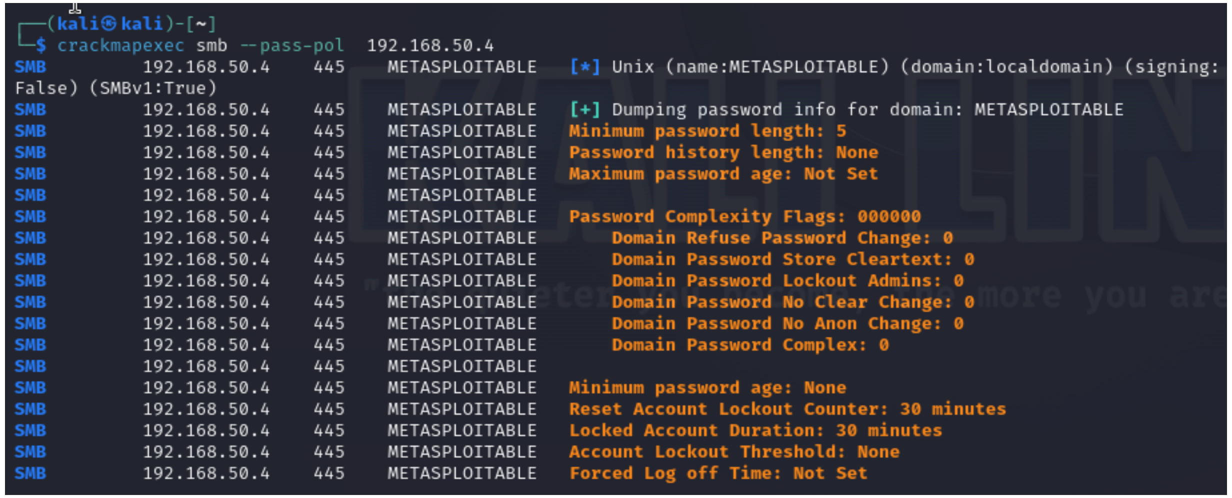
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.50.4    08:00:27:a9:45:82      1      60  PCS Systemtechnik GmbH
```

3) crackmapexec

Tra i vari comandi del modulo smb ho scelto pass-pol che serve a mostrare le policy delle password della macchina attaccata.



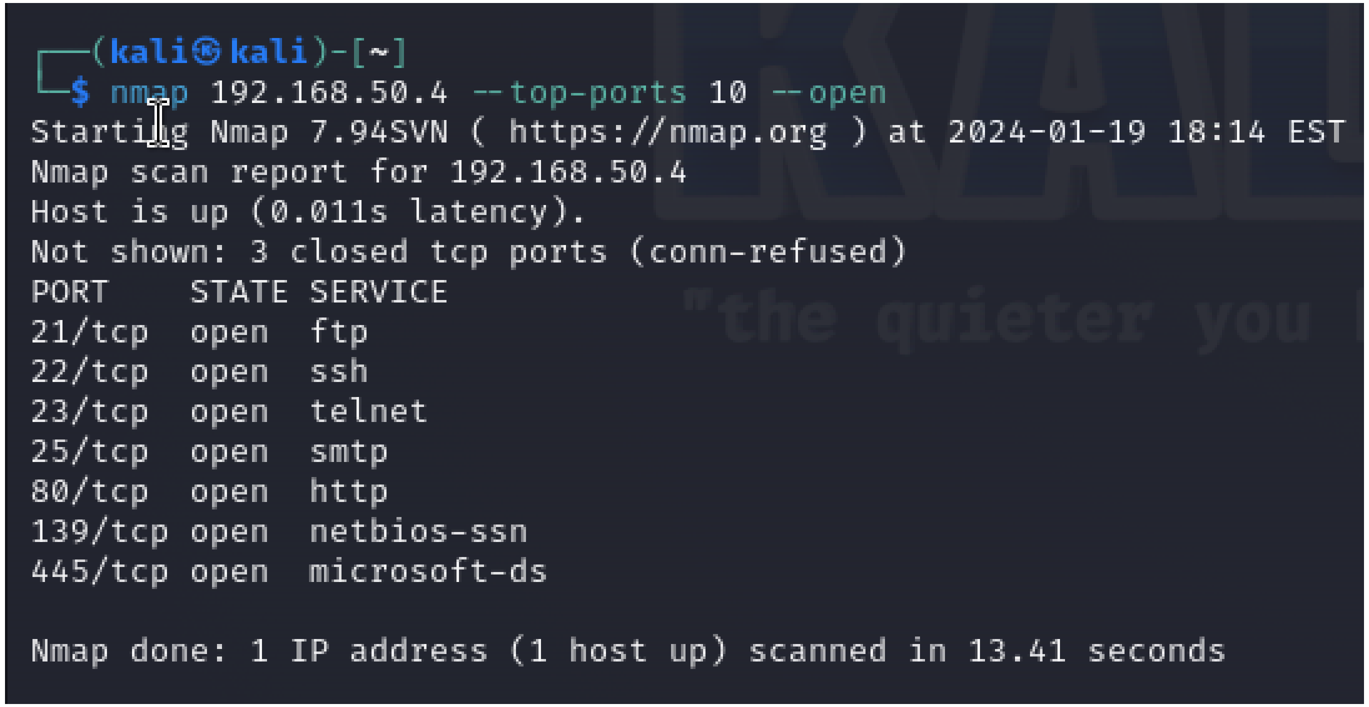
```
Mapping/Enumeration:
  Options for Mapping/Enumerating

  --shares              enumerate shares and access
  --sessions            enumerate active sessions
  --disks               enumerate disks
  --loggedon-users-filter LOGGEDON_USERS_FILTER
                        only search for specific user, works with regex
  --loggedon-users      enumerate logged on users
  --users [USER]        enumerate domain users, if a user is specified than only its information is queried.
  --groups [GROUP]      enumerate domain groups, if a group is specified than its members are enumerated
  --computers [COMPUTER]
                        enumerate computer users
  --local-groups [GROUP]
                        enumerate local groups, if a group is specified then its members are enumerated
  --pass-pol            dump password policy
  --rid-brute [MAX_RID]
                        enumerate users by bruteforcing RID's (default: 4000)
  --wmi QUERY           issues the specified WMI query
  --wmi-namespace NAMESPACE
                        WMI Namespace (default: root\cimv2)
```



```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb --pass-pol  192.168.50.4
SMB         192.168.50.4    445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:
False) (SMBv1:True)
SMB         192.168.50.4    445    METASPLOITABLE   [+] Dumping password info for domain: METASPLOITABLE
SMB         192.168.50.4    445    METASPLOITABLE   Minimum password length: 5
SMB         192.168.50.4    445    METASPLOITABLE   Password history length: None
SMB         192.168.50.4    445    METASPLOITABLE   Maximum password age: Not Set
SMB         192.168.50.4    445    METASPLOITABLE
SMB         192.168.50.4    445    METASPLOITABLE   Password Complexity Flags: 000000
SMB         192.168.50.4    445    METASPLOITABLE       Domain Refuse Password Change: 0
SMB         192.168.50.4    445    METASPLOITABLE       Domain Password Store Cleartext: 0
SMB         192.168.50.4    445    METASPLOITABLE       Domain Password Lockout Admins: 0
SMB         192.168.50.4    445    METASPLOITABLE       Domain Password No Clear Change: 0
SMB         192.168.50.4    445    METASPLOITABLE       Domain Password No Anon Change: 0
SMB         192.168.50.4    445    METASPLOITABLE       Domain Password Complex: 0
SMB         192.168.50.4    445    METASPLOITABLE
SMB         192.168.50.4    445    METASPLOITABLE   Minimum password age: None
SMB         192.168.50.4    445    METASPLOITABLE   Reset Account Lockout Counter: 30 minutes
SMB         192.168.50.4    445    METASPLOITABLE   Locked Account Duration: 30 minutes
SMB         192.168.50.4    445    METASPLOITABLE   Account Lockout Threshold: None
SMB         192.168.50.4    445    METASPLOITABLE   Forced Log off Time: Not Set
```

4) nmap <target> –top-ports 10 –open

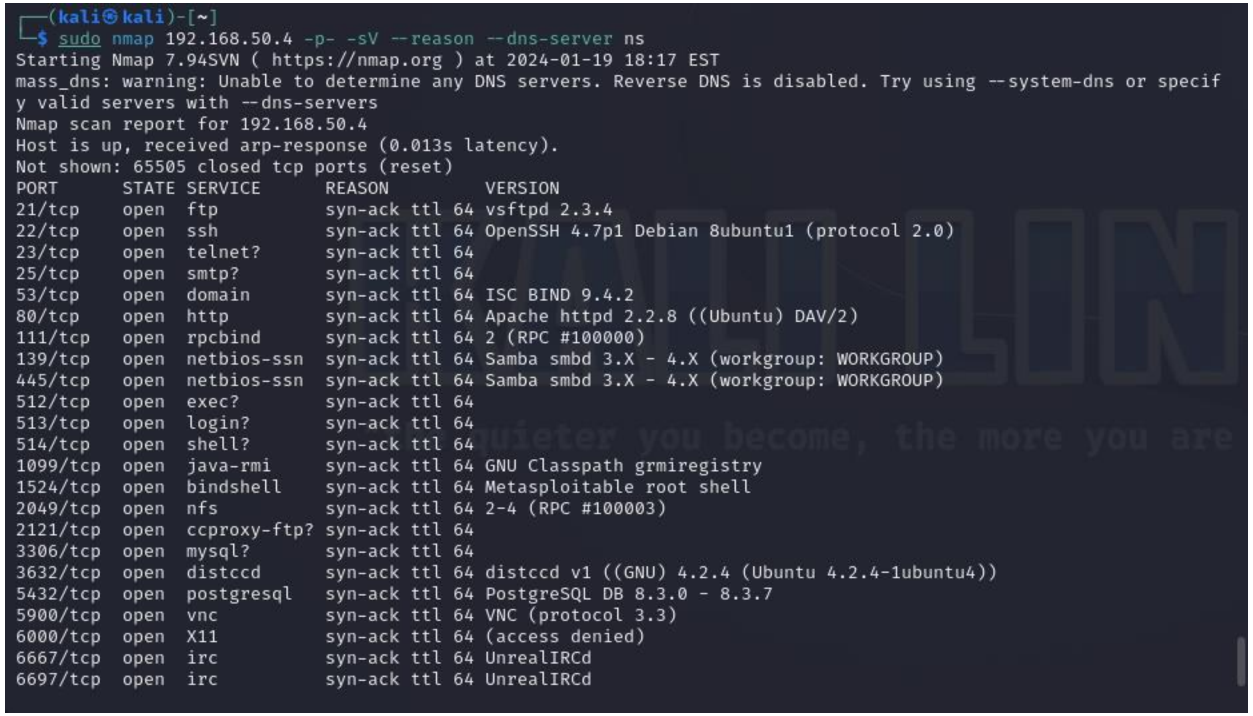
Il seguente comando mostra le 10 porte più importanti da scansionare.



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.4 --top-ports 10 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 18:14 EST
Nmap scan report for 192.168.50.4
Host is up (0.011s latency).
Not shown: 3 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

5) nmap <target> -p- -sV –reason –dns-server ns

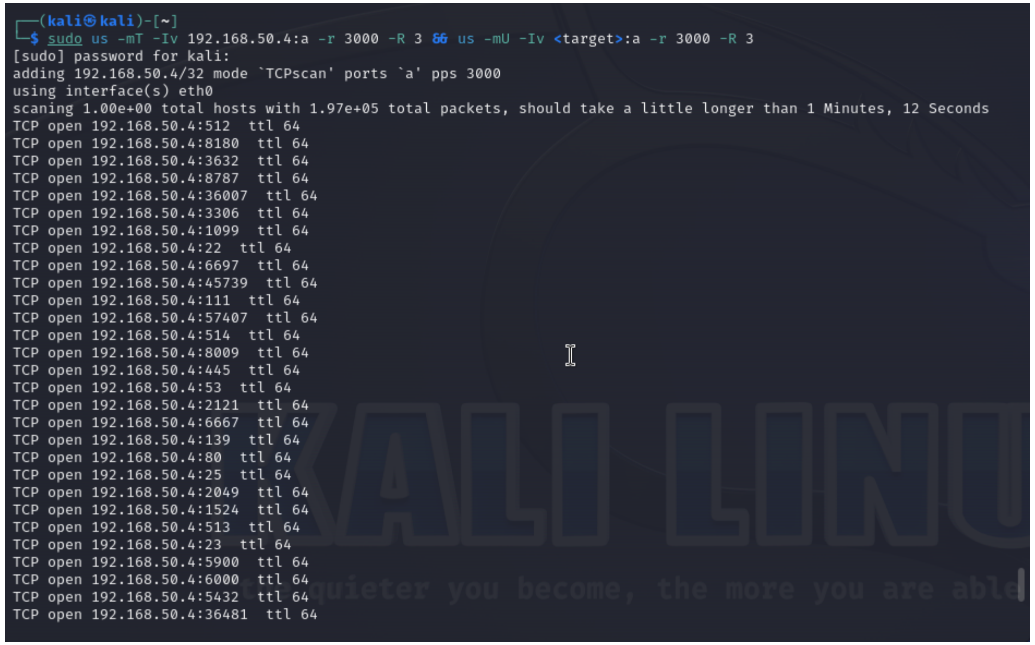
Trova se la porta scansionata è open , filtered o closed



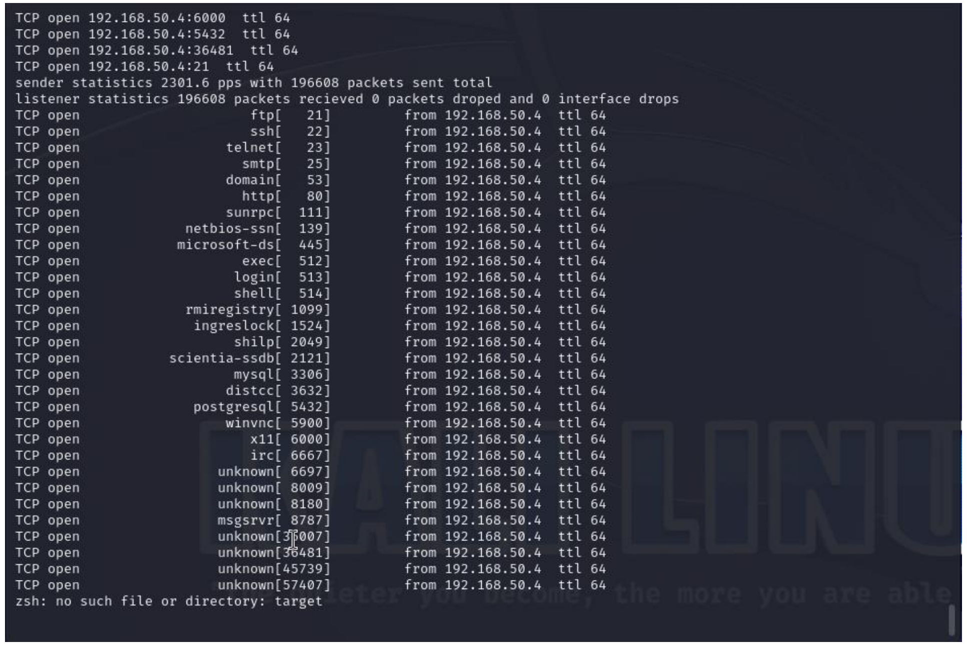
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.50.4 -p- -sV --reason --dns-server ns
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 18:17 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specif
y valid servers with --dns-servers
Nmap scan report for 192.168.50.4
Host is up, received arp-response (0.013s 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
25/tcp    open  smtp?        syn-ack ttl 64
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
513/tcp   open  login?       syn-ack ttl 64
514/tcp   open  shell?       syn-ack ttl 64
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  ccproxy-ftp? syn-ack ttl 64
3306/tcp  open  mysql?       syn-ack ttl 64
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
```

6) us -mT -Iv <target>:a -r 3000 -R 3 && us -mU -Iv <target>:a -r 3000 -R 3

Con questo comando si effettua prima una scansione TCP e poi una UDP inviando 3000 pacchetti per secondo. Unicornscan è orientato a scansioni veloci ed efficienti.



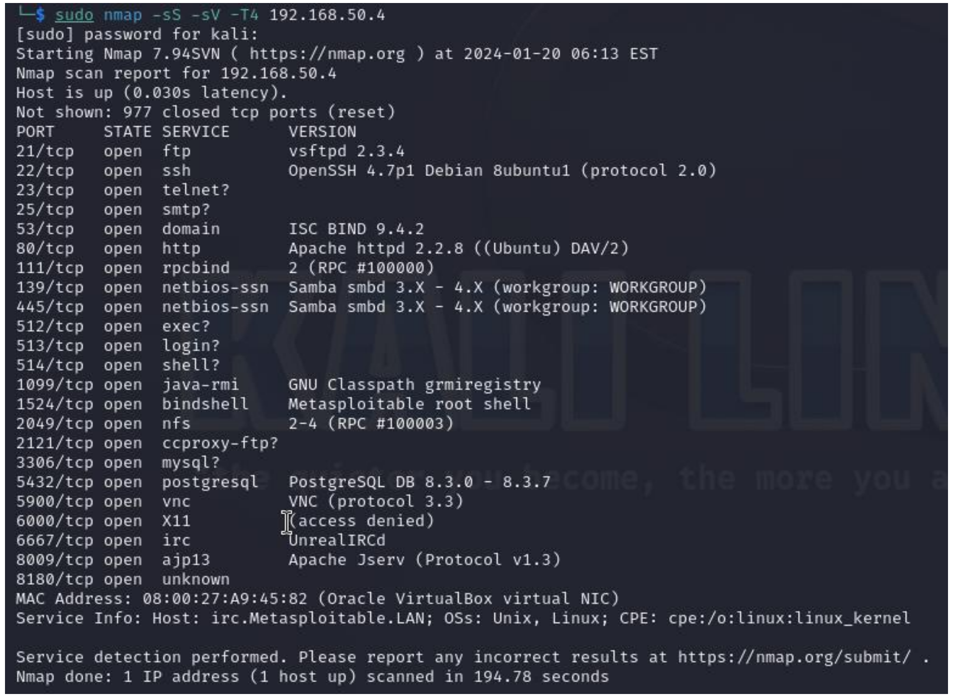
```
┌──(kali㉿kali)-[~]
└─$ sudo us -mT -Iv 192.168.50.4:a -r 3000 -R 3 && us -mU -Iv <target>:a -r 3000 -R 3
[sudo] password for kali:
adding 192.168.50.4/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
TCP open 192.168.50.4:512  ttl 64
TCP open 192.168.50.4:8180  ttl 64
TCP open 192.168.50.4:3632  ttl 64
TCP open 192.168.50.4:8787  ttl 64
TCP open 192.168.50.4:36007  ttl 64
TCP open 192.168.50.4:3306  ttl 64
TCP open 192.168.50.4:1099  ttl 64
TCP open 192.168.50.4:22  ttl 64
TCP open 192.168.50.4:6697  ttl 64
TCP open 192.168.50.4:45739  ttl 64
TCP open 192.168.50.4:111  ttl 64
TCP open 192.168.50.4:57407  ttl 64
TCP open 192.168.50.4:514  ttl 64
TCP open 192.168.50.4:8009  ttl 64
TCP open 192.168.50.4:445  ttl 64
TCP open 192.168.50.4:53  ttl 64
TCP open 192.168.50.4:2121  ttl 64
TCP open 192.168.50.4:6667  ttl 64
TCP open 192.168.50.4:139  ttl 64
TCP open 192.168.50.4:80  ttl 64
TCP open 192.168.50.4:25  ttl 64
TCP open 192.168.50.4:2049  ttl 64
TCP open 192.168.50.4:1524  ttl 64
TCP open 192.168.50.4:513  ttl 64
TCP open 192.168.50.4:23  ttl 64
TCP open 192.168.50.4:5900  ttl 64
TCP open 192.168.50.4:6000  ttl 64
TCP open 192.168.50.4:5432  ttl 64
TCP open 192.168.50.4:36481  ttl 64
```



```
TCP open 192.168.50.4:6000  ttl 64
TCP open 192.168.50.4:5432  ttl 64
TCP open 192.168.50.4:36481  ttl 64
TCP open 192.168.50.4:21  ttl 64
sender statistics 2301.6 pps with 196608 packets sent total
listener statistics 196608 packets recieved 0 packets droped and 0 interface drops
TCP open                     ftp[   21]         from 192.168.50.4  ttl 64
TCP open                     ssh[   22]         from 192.168.50.4  ttl 64
TCP open                  telnet[   23]         from 192.168.50.4  ttl 64
TCP open                    smtp[   25]         from 192.168.50.4  ttl 64
TCP open                  domain[   53]         from 192.168.50.4  ttl 64
TCP open                    http[   80]         from 192.168.50.4  ttl 64
TCP open                  sunrpc[  111]         from 192.168.50.4  ttl 64
TCP open             netbios-ssn[  139]         from 192.168.50.4  ttl 64
TCP open            microsoft-ds[  445]         from 192.168.50.4  ttl 64
TCP open                    exec[  512]         from 192.168.50.4  ttl 64
TCP open                   login[  513]         from 192.168.50.4  ttl 64
TCP open                   shell[  514]         from 192.168.50.4  ttl 64
TCP open             rmiregistry[ 1099]         from 192.168.50.4  ttl 64
TCP open              ingreslock[ 1524]         from 192.168.50.4  ttl 64
TCP open                   shilp[ 2049]         from 192.168.50.4  ttl 64
TCP open            scientia-ssdb[ 2121]         from 192.168.50.4  ttl 64
TCP open                   mysql[ 3306]         from 192.168.50.4  ttl 64
TCP open                  distcc[ 3632]         from 192.168.50.4  ttl 64
TCP open              postgresql[ 5432]         from 192.168.50.4  ttl 64
TCP open                  winvnc[ 5900]         from 192.168.50.4  ttl 64
TCP open                     x11[ 6000]         from 192.168.50.4  ttl 64
TCP open                     irc[ 6667]         from 192.168.50.4  ttl 64
TCP open                 unknown[ 6697]         from 192.168.50.4  ttl 64
TCP open                 unknown[ 8009]         from 192.168.50.4  ttl 64
TCP open                 unknown[ 8180]         from 192.168.50.4  ttl 64
TCP open                  msgsrvr[ 8787]         from 192.168.50.4  ttl 64
TCP open                 unknown[36007]         from 192.168.50.4  ttl 64
TCP open                 unknown[36481]         from 192.168.50.4  ttl 64
TCP open                 unknown[45739]         from 192.168.50.4  ttl 64
TCP open                 unknown[57407]         from 192.168.50.4  ttl 64
zsh: no such file or directory: target
```

7) nmap -sS -sV -T4 <target>

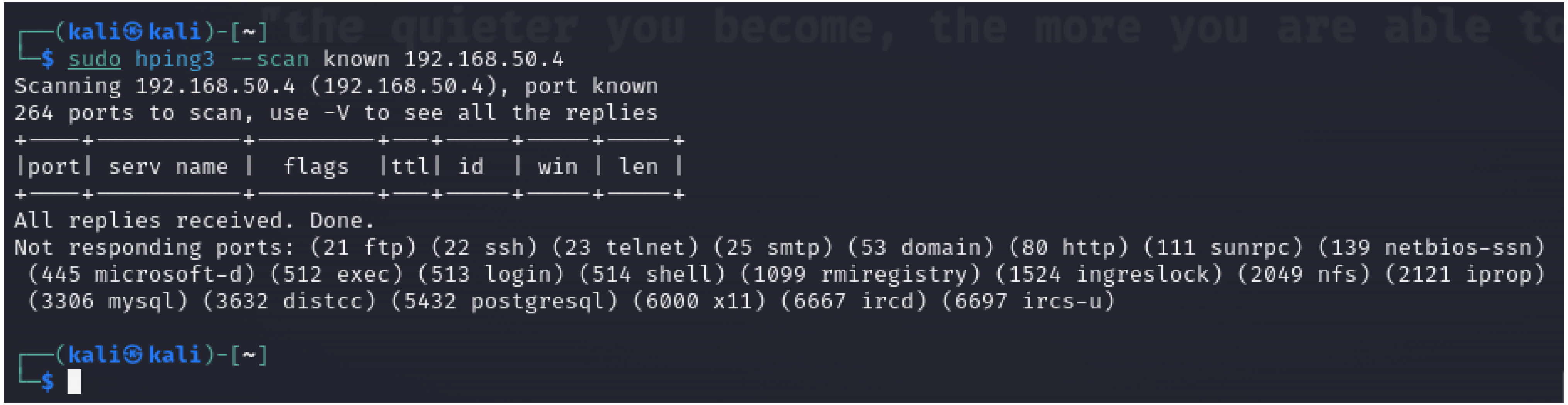
Il comando seguente determina se la porta è in ascolto. Non viene stabilita una connessione TCP completa. Si invia solo un pacchetto SYN e attendi la risposta.
Se si riceve una risposta SYN/ACK significa che la porta è in ascolto:
Con l'opzione -sV, puoi anche le porte più importanti da un elenco di database di circa 2-200.



```
└─$ sudo nmap -sS -sV -T4 192.168.50.4
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 06:13 EST
Nmap scan report for 192.168.50.4
Host is up (0.030s 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?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
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?
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  unknown
MAC Address: 08:00:27:A9:45:82 (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 194.78 seconds
```

8) hping3 –scan known <target>

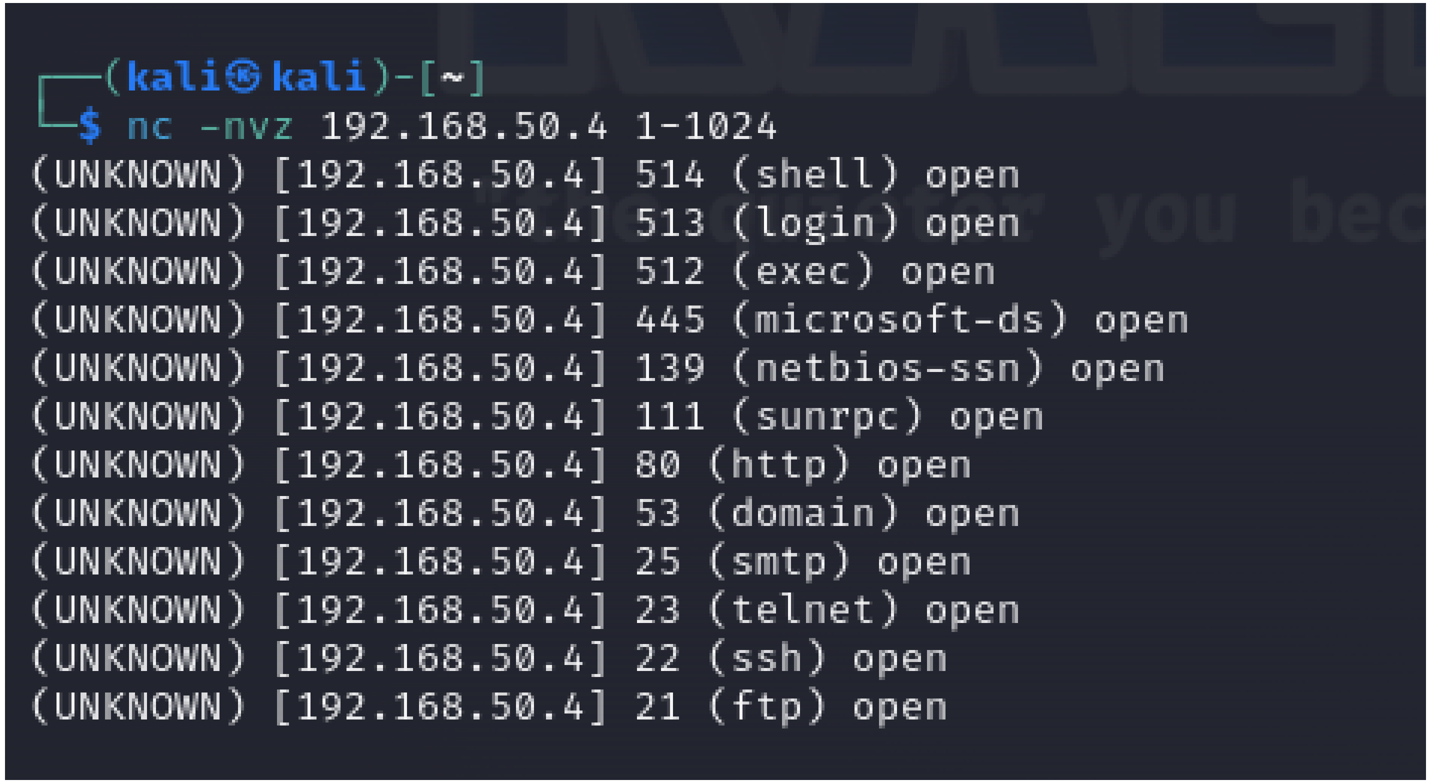
Hping3 è uno strumento che permette di testare la raggiungibilità di una porta inviando pacchetti con diversi protocolli.



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --scan known 192.168.50.4
Scanning 192.168.50.4 (192.168.50.4), 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)
 (3306 mysql) (3632 distcc) (5432 postgresql) (6000 x11) (6667 ircd) (6697 ircs-u)

┌──(kali㉿kali)-[~]
└─$ 
```

9) nc -nvz <target> 1-1024

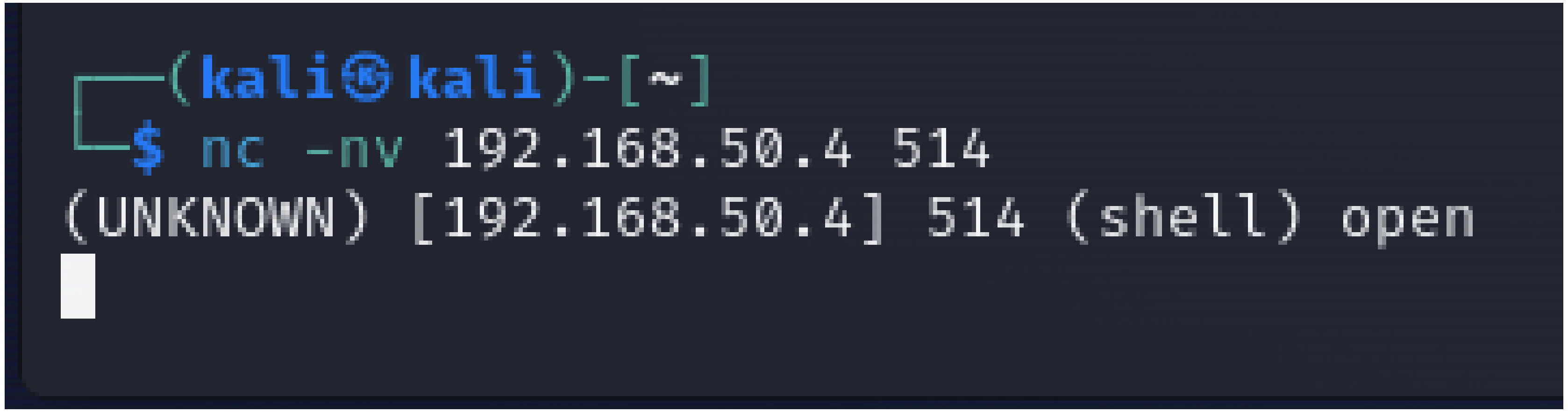
Il comando in oggetto permette di visualizzare tramite netcat quali porte sono aperte sul target.



```
┌──(kali㉿kali)-[~]
└─$ nc -nvz 192.168.50.4 1-1024
(UNKNOWN) [192.168.50.4] 514 (shell) open
(UNKNOWN) [192.168.50.4] 513 (login) open
(UNKNOWN) [192.168.50.4] 512 (exec) open
(UNKNOWN) [192.168.50.4] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.4] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.4] 111 (sunrpc) open
(UNKNOWN) [192.168.50.4] 80 (http) open
(UNKNOWN) [192.168.50.4] 53 (domain) open
(UNKNOWN) [192.168.50.4] 25 (smtp) open
(UNKNOWN) [192.168.50.4] 23 (telnet) open
(UNKNOWN) [192.168.50.4] 22 (ssh) open
(UNKNOWN) [192.168.50.4] 21 (ftp) open
```

10) nc -nv <target> <port number>

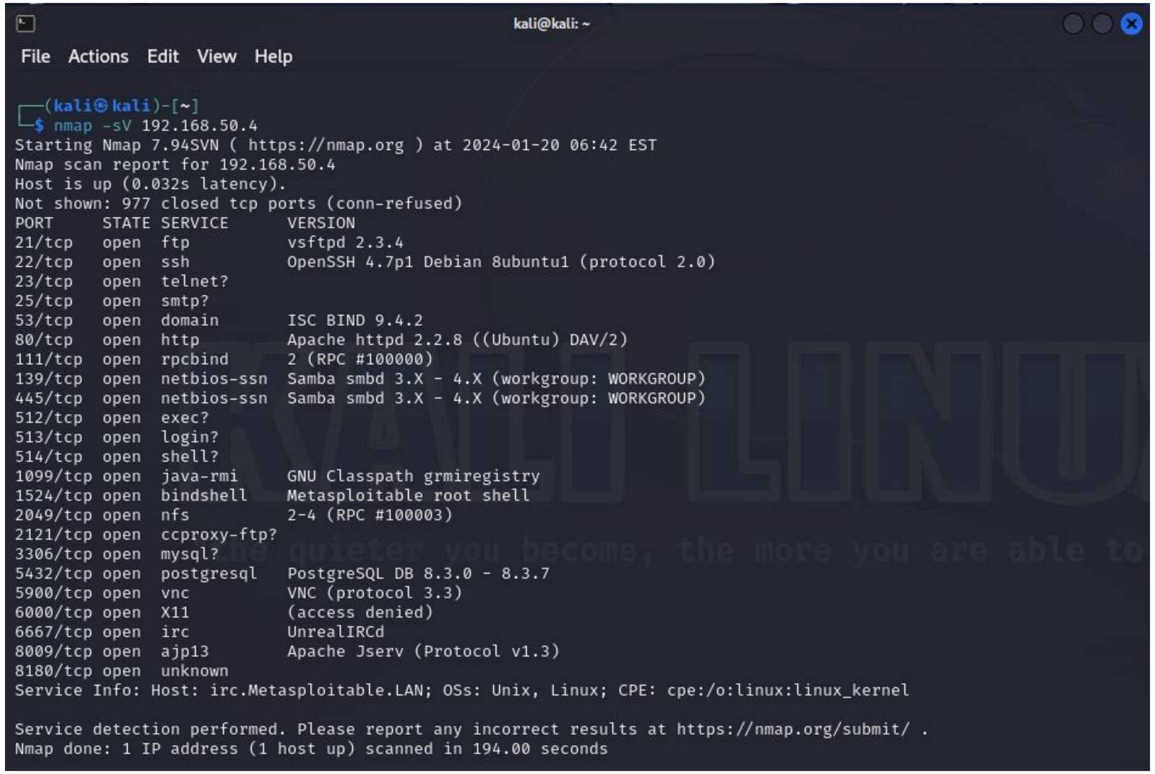
E’ come il precedente con la differenza che viene eseguito su una porta in particolare.



```
┌──(kali㉿kali)-[~]
└─$ nc -nv 192.168.50.4 514
(UNKNOWN) [192.168.50.4] 514 (shell) open
█
```

11) nmap -sV <target>

L'opzione -sV in Nmap è utilizzata per eseguire la rilevazione della versione dei servizi attivi su un host. In altre parole, quando si utilizza l'opzione -sV, Nmap cerca di identificare le versioni specifiche dei servizi che sono in ascolto sulle porte aperte dell'host.

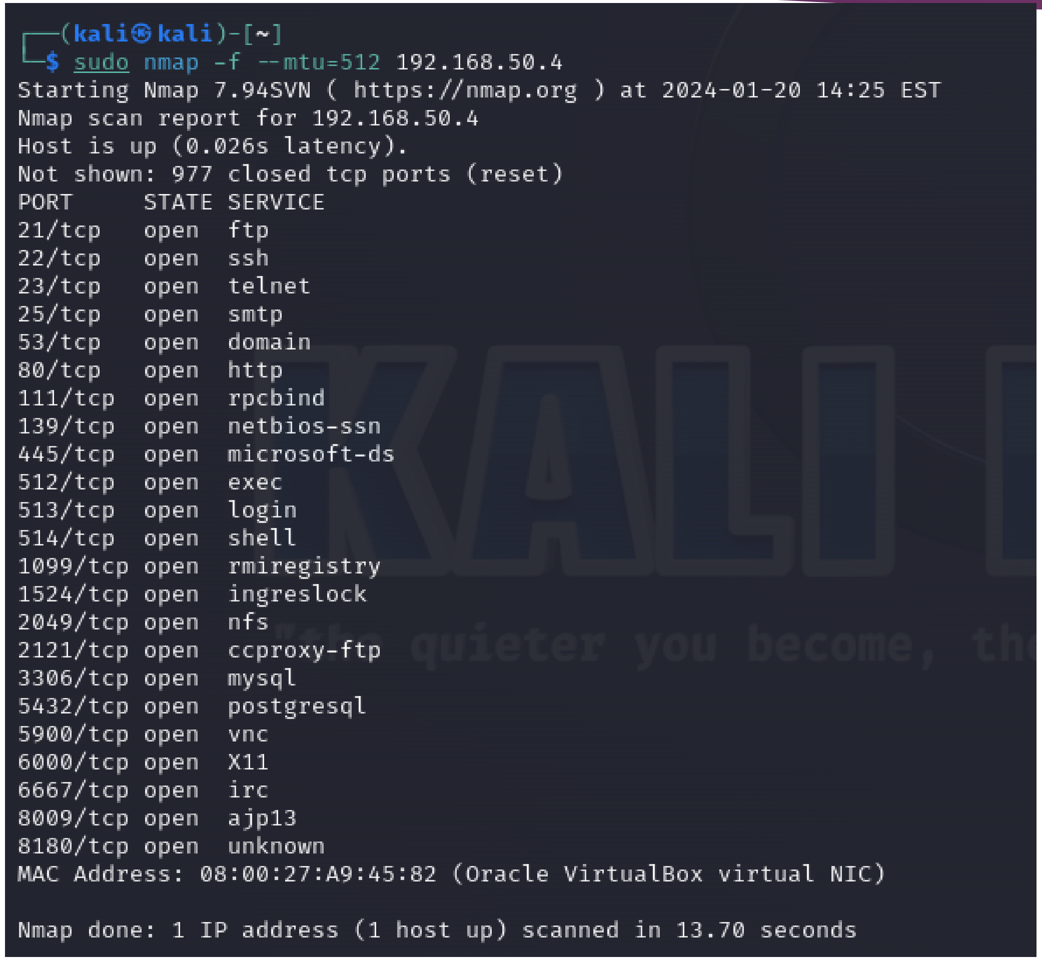


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 06:42 EST
Nmap scan report for 192.168.50.4
Host is up (0.032s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
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?
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  unknown
Service Info: Host: 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 194.00 seconds
```

12) db_import <filename.xml>

Se salvassimo i risultati delle scansioni in un db potremmo passarli a metasploit per continuare la fase di exploitation che al momento non stiamo trattando.

13) nmap -f –mtu=512 <target>

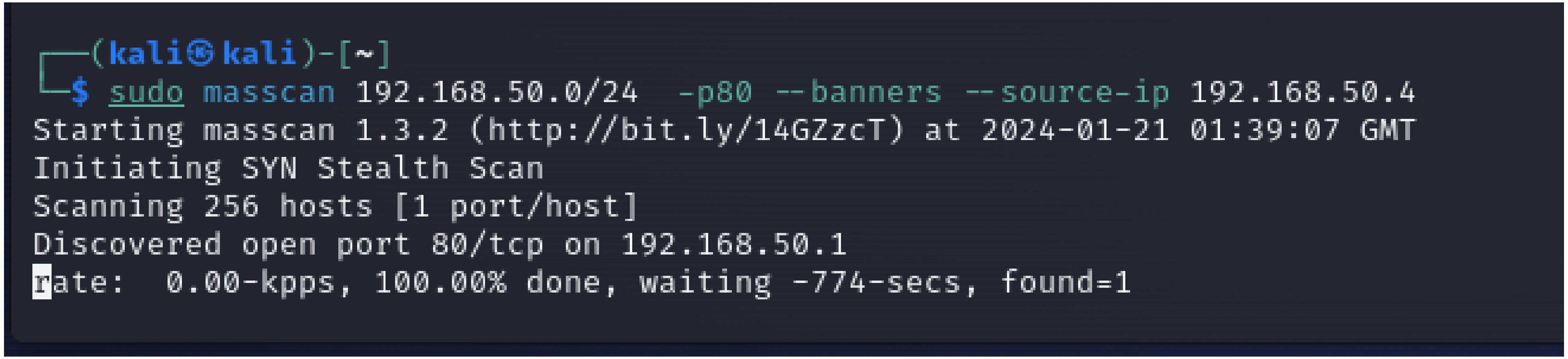


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -f --mtu=512 192.168.50.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 14:25 EST
Nmap scan report for 192.168.50.4
Host is up (0.026s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    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:A9:45:82 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.70 seconds
```

L'opzione -f fa sì che la scansione richiesta (incluse le scansioni ping) utilizzi piccoli pacchetti IP frammentati. L'idea è di suddividere l'header TCP su più pacchetti per rendere più difficile la rilevazione dai filtri dei pacchetti e dai sistemi di rilevamento delle intrusioni.

14) masscan <network> -p80 –banners –source-ip <target>

Rispetto a nmap fa delle scansioni più veloci.



```
┌──(kali㉿kali)-[~]
└─$ sudo masscan 192.168.50.0/24  -p80 --banners --source-ip 192.168.50.4
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-01-21 01:39:07 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.50.1
rate:  0.00-kpps, 100.00% done, waiting -774-secs, found=1
```