

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

NMAP

nmap -sn -PE 192.168.1.100

[-sn controlla attività di host tramite un ping, -PE echo request]

nmap -p 1-1024 192.168.1.100

[-p range porte]

```
(root@kali)-[/home/kali]
# nmap -sn -PE 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 15:04 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.00016s latency).
MAC Address: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

```
(root@kali)-[/home/kali]
# nmap -p 1-1024 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 15:04 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.00019s latency).
Not shown: 1012 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
MAC Address: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

```
(root@kali)-[/home/kali]
#
```

nmap [Meta IP] -sV -reason -dns-server ns

- *nmap ip*: La parte ip dovrebbe essere sostituita con l'indirizzo IP del target che desideri scansionare.
- *-sV*: Specifica di eseguire la scansione dei servizi per determinare il tipo e la versione dei servizi in esecuzione sulle porte aperte.
- *-reason*: Questo flag abilita l'output delle ragioni per lo stato di una porta, come se una porta sia aperta, chiusa o filtrata.
- *-dns-server ns*: Questo flag specifica il server DNS da utilizzare per le query DNS durante la scansione.

```

(root@kali)-[/home/kali]
# nmap 192.168.1.100 -sV -reason -dns-server ns
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 15:09 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 192.168.1.100
Host is up, received arp-response (0.000076s latency).
Not shown: 977 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
513/tcp   open  login        syn-ack ttl 64 OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped   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  ftp          syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql        syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
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
8009/tcp  open  ajp13?       syn-ack ttl 64
8180/tcp  open  http         syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:1D:D6:E8 (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 97.59 seconds

```

nmap -sS -sV -T4 [Meta ip] / [Windows IP]

- **-sS**: Specifica di utilizzare la scansione SYN. Nmap invia pacchetti SYN per determinare lo stato delle porte: se una porta risponde con un pacchetto SYN/ACK, la porta è aperta; se una porta risponde con un pacchetto RST, la porta è chiusa.
- **-sV**: Abilita il rilevamento dei servizi. Nmap cercherà di determinare il tipo e la versione dei servizi in esecuzione sulle porte aperte.
- **-T4**: Specifica il livello di aggressività della scansione. In questo caso, è impostato su "Aggressivo" (4 su una scala da 0 a 5), che indica una scansione più veloce ma anche più rumorosa e intensiva rispetto alla scansione predefinita.
- **<target>**: Specifica l'host o l'intervallo di indirizzi IP da scansionare. Sostituisci <target> con l'indirizzo IP del tuo obiettivo.

```

(root@kali)-[/home/kali]
# nmap -sS -sV -T4 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 15:13 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.000071s 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?
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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?
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:1D:D6:E8 (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 126.14 seconds

(root@kali)-[/home/kali]
#

```

nmap -f -mtu=512 [Meta ip]

- *-f: Specifica di frammentare i pacchetti durante la scansione. La frammentazione dei pacchetti può essere utile per bypassare i dispositivi di sicurezza che filtrano o analizzano i pacchetti in base alle dimensioni.*
- *-mtu=512: Specifica il valore della massima unità di trasmissione (MTU) per i pacchetti inviati durante la scansione. L'MTU è la dimensione massima in byte di un pacchetto di dati che può essere trasmesso attraverso una rete. Impostando l'MTU a 512, si imposta la dimensione massima dei pacchetti a 512 byte.*

```
(root@kali)-[/home/kali]
# nmap -f -mtu=512 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 15:22 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.000074s 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: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

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

nmap [IP] -top-ports 10 -open

100 = meta

8 = win7

```
(kali@kali)-[~]
$ nmap 192.168.1.100 -top-ports 10 -open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 09:53 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.0032s 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 0.04 seconds

(kali@kali)-[~]
$ nmap 192.168.1.8 -top-ports 10 -open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 09:53 EDT
Nmap scan report for PC192.168.1.8 (192.168.1.8)
Host is up (0.00051s latency).
Not shown: 8 closed tcp ports (conn-refused)
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

nmap 192.168.1.100 -p- -sV --reason --dns-server 8.8.8.8

- *-p-*: Questo flag indica a Nmap di scansionare tutte le porte da 1 a 65535.
- *-sV*: Questo flag abilita il rilevamento del servizio, consentendo a Nmap di tentare di determinare il tipo e la versione del servizio in esecuzione su ciascuna porta.

- *--reason*: Questo flag mostra la ragione per cui Nmap ha determinato lo stato di una porta (ad esempio, se la porta è chiusa, filtrata o aperta).
- *--dns-server <DNS_server>*: Questo flag specifica il server DNS da utilizzare per le query DNS durante la scansione (opzionale).

```
(kali@kali)-[~]
$ nmap 192.168.1.100 -p- -sV --reason --dns-server 8.8.8.8

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 11:55 EDT
Nmap scan report for 192.168.1.100
Host is up, received syn-ack (0.000032s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE REASON VERSION
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
513/tcp   open  login    syn-ack OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped syn-ack
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  XI1      syn-ack (access denied)
6667/tcp  open  irc      syn-ack UnrealIRCd
6697/tcp  open  irc      syn-ack UnrealIRCd (Admin email admin@Metasploitable.LAN)
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)
33699/tcp open  java-rmi syn-ack GNU Classpath grmiregistry
36090/tcp open  status   syn-ack 1 (RPC #100024)
48381/tcp open  nlockmgr syn-ack 1-4 (RPC #100021)
50015/tcp open  mountd   syn-ack 1-3 (RPC #100005)
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 130.23 seconds

(kali@kali)-[~]
```

NETCAT

NC -nvz IP

NC -nv IP

si scoprono servizi ed eventuali porte aperte

```
(root@kali)-[/home/kali]
# nc -nvz 192.168.1.100 1-1024
(UNKNOWN) [192.168.1.100] 514 (shell) open
(UNKNOWN) [192.168.1.100] 513 (login) open
(UNKNOWN) [192.168.1.100] 512 (exec) open
(UNKNOWN) [192.168.1.100] 445 (microsoft-ds) open
(UNKNOWN) [192.168.1.100] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.100] 111 (sunrpc) open
(UNKNOWN) [192.168.1.100] 80 (http) open
(UNKNOWN) [192.168.1.100] 53 (domain) open
(UNKNOWN) [192.168.1.100] 25 (smtp) open
(UNKNOWN) [192.168.1.100] 23 (telnet) open
(UNKNOWN) [192.168.1.100] 22 (ssh) open
(UNKNOWN) [192.168.1.100] 21 (ftp) open

(root@kali)-[/home/kali]
# nc -nv 192.168.1.100 22
(UNKNOWN) [192.168.1.100] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C

(root@kali)-[/home/kali]
```

NC -nvz [IP] 1-1024

-nvz: Queste opzioni specificano il comportamento di netcat durante la scansione dei porti:

- *-n: Disabilita la risoluzione DNS per evitare la traduzione degli indirizzi IP.*
- *-v: Abilita la modalità verbosa per visualizzare informazioni dettagliate durante la scansione.*
- *-z: Specifica di scansionare i porti senza inviare alcun dato, utile per determinare lo stato dei porti senza stabilire una connessione.*

ip: Questo è l'indirizzo IP del target che si desidera scansionare.

1-1024: Questo specifica l'intervallo di porte da 1 a 1024 che si desidera scansionare sul target. Quindi, netcat scansionerà tutte le porte comprese tra 1 e 1024 sull'host specificato.

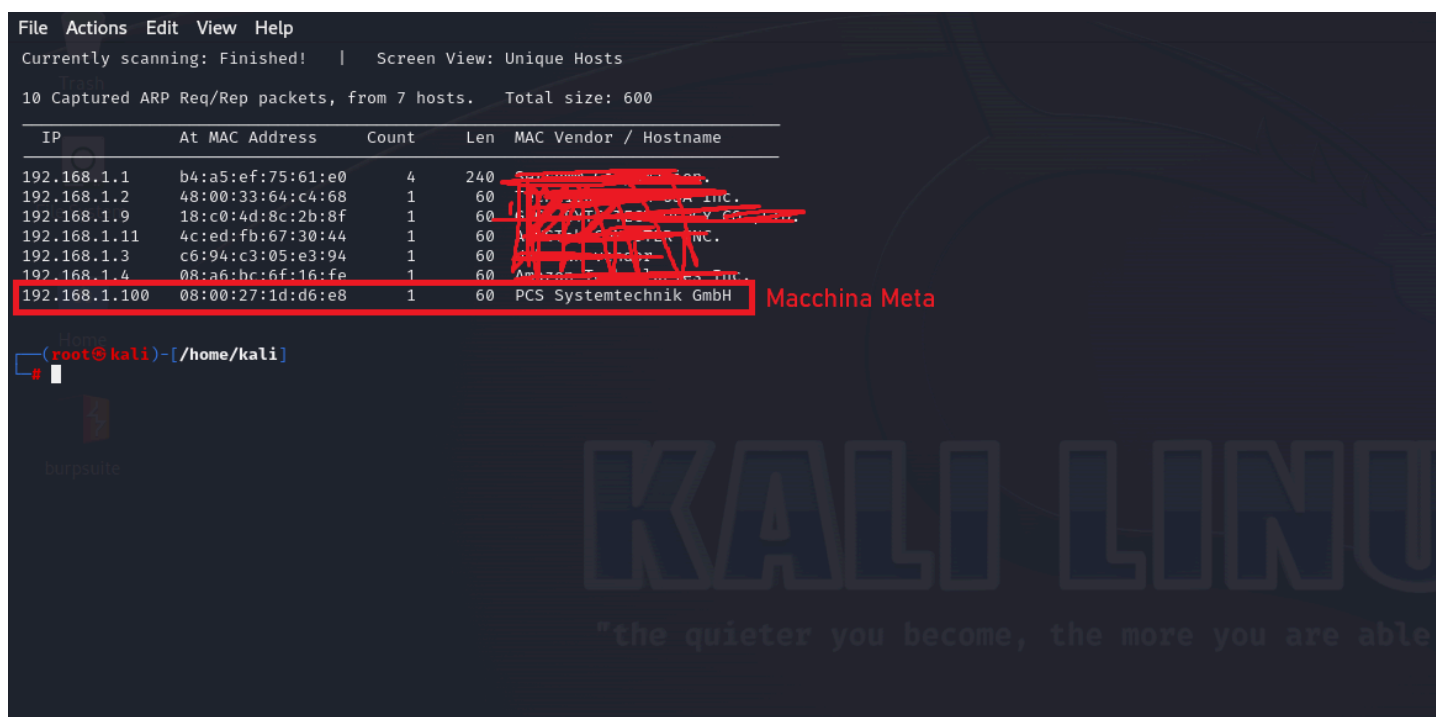
```
(root@kali)-[/home/kali]
# nc -nvz 192.168.1.100 1-1024
(UNKNOWN) [192.168.1.100] 514 (shell) open
(UNKNOWN) [192.168.1.100] 513 (login) open
(UNKNOWN) [192.168.1.100] 512 (exec) open
(UNKNOWN) [192.168.1.100] 445 (microsoft-ds) open
(UNKNOWN) [192.168.1.100] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.100] 111 (sunrpc) open
(UNKNOWN) [192.168.1.100] 80 (http) open
(UNKNOWN) [192.168.1.100] 53 (domain) open
(UNKNOWN) [192.168.1.100] 25 (smtp) open
(UNKNOWN) [192.168.1.100] 23 (telnet) open
(UNKNOWN) [192.168.1.100] 22 (ssh) open
(UNKNOWN) [192.168.1.100] 21 (ftp) open

(root@kali)-[/home/kali]
# █
```

Netdiscover

netdiscover -r [IP META]

si scoprono Mac address, ip i rete e Hostname



Crackmapexec

crackmapexec fpt [IP META / 24]

si scoprono servizi attivi e versione (in questo caso FTP vsFTPd 2.3.4 con nota vulnerabilità)

ho aggiunto anche una scansione su windows7 sul SMB (SMB1 quindi vulnerabile ad EB)



```
(kali@kali)-[~]  
$ crackmapexec smb 192.168.1.8  
SMB 192.168.1.8 445 WIN7EC [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN7EC) (domain:Win7ec) (signing:False) (SMBv1:True)  
(kali@kali)-[~]  
$
```

UnicornScan

us -mT -lv <target>:a -r 3000 -R 3 && us -mU -lv <target>:a -r 3000 -R 3

- *us: Avvia Unicorn Scan.*
- *-mT: Specifica di eseguire una scansione TCP.*
- *-lv: Abilita l'output verboso per mostrare informazioni dettagliate durante la scansione.*
- *192.168.1.100:a: Specifica l'IP del target come 192.168.1.100 con una scansione su tutte le porte.*
- *-r 3000: Limita la velocità di invio dei pacchetti a 3000 pacchetti al secondo.*
- *-R 3: Specifica un massimo di 3 ritrasmissioni per i pacchetti non confermati.*
- *&&: Operatore logico che indica di eseguire il comando successivo solo se il primo comando ha successo.*
- *us: Avvia Unicorn Scan di nuovo.*
- *-mU: Specifica di eseguire una scansione UDP.*
- *-lv: Abilita l'output verboso per mostrare informazioni dettagliate durante la scansione.*
- *<target>:a: Specifica il target per la scansione su tutte le porte UDP.*
- *-r 3000: Limita la velocità di invio dei pacchetti a 3000 pacchetti al secondo.*
- *-R 3: Specifica un massimo di 3 ritrasmissioni per i pacchetti non confermati.*

```
(root@kali)-[/home/kali]
# nmap -sT -iV 192.168.1.100:a -r 3000 -R 3 66 us -mU -iV 192.168.1.100:a -r 3000 -R 3
adding 192.168.1.100/32 mode 'TCPscan' ports 'a' pps 3000
using interface(s) eth0
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
TCP open 192.168.1.100:513    ttl 64
TCP open 192.168.1.100:8787  ttl 64
TCP open 192.168.1.100:1524  ttl 64
TCP open 192.168.1.100:80   ttl 64
TCP open 192.168.1.100:23   ttl 64
TCP open 192.168.1.100:3306  ttl 64
TCP open 192.168.1.100:22   ttl 64
TCP open 192.168.1.100:514   ttl 64
TCP open 192.168.1.100:2049  ttl 64
TCP open 192.168.1.100:512   ttl 64
TCP open 192.168.1.100:50015 ttl 64
TCP open 192.168.1.100:6000  ttl 64
TCP open 192.168.1.100:445   ttl 64
TCP open 192.168.1.100:6697  ttl 64
TCP open 192.168.1.100:53   ttl 64
TCP open 192.168.1.100:3632  ttl 64
TCP open 192.168.1.100:48381 ttl 64
TCP open 192.168.1.100:6667  ttl 64
TCP open 192.168.1.100:5900  ttl 64
TCP open 192.168.1.100:21   ttl 64
TCP open 192.168.1.100:8180  ttl 64
TCP open 192.168.1.100:36090 ttl 64
TCP open 192.168.1.100:8009  ttl 64
TCP open 192.168.1.100:33699 ttl 64
TCP open 192.168.1.100:25   ttl 64
TCP open 192.168.1.100:111   ttl 64
TCP open 192.168.1.100:139   ttl 64
TCP open 192.168.1.100:2121  ttl 64
TCP open 192.168.1.100:1099  ttl 64
TCP open 192.168.1.100:5432  ttl 64
sender statistics 2986.1 pps with 196608 packets sent total
listener statistics 196608 packets recieved 0 packets dropped and 0 interface drops
TCP open      ftp[ 21]      from 192.168.1.100  ttl 64
TCP open      ssh[ 22]      from 192.168.1.100  ttl 64
TCP open      telnet[ 23]    from 192.168.1.100  ttl 64
TCP open      smtp[ 25]     from 192.168.1.100  ttl 64
TCP open      domain[ 53]    from 192.168.1.100  ttl 64
TCP open      http[ 80]     from 192.168.1.100  ttl 64
TCP open      sunrpc[ 111]   from 192.168.1.100  ttl 64
TCP open      netbios-ssn[ 139] from 192.168.1.100  ttl 64
TCP open      microsoft-ds[ 445] from 192.168.1.100  ttl 64
TCP open      exec[ 512]    from 192.168.1.100  ttl 64
TCP open      login[ 513]   from 192.168.1.100  ttl 64
TCP open      shell[ 514]   from 192.168.1.100  ttl 64
TCP open      rmiregistry[ 1099] from 192.168.1.100  ttl 64
TCP open      ingreslock[ 1524] from 192.168.1.100  ttl 64
TCP open      shilp[ 2049]   from 192.168.1.100  ttl 64
TCP open      scientia-ssdb[ 2121] from 192.168.1.100  ttl 64
```

```

listener statistics 196608 packets recieved 0 packets dropped and 0 interface drops
TCP open          ftp[ 21]          from 192.168.1.100 ttl 64
TCP open          ssh[ 22]          from 192.168.1.100 ttl 64
TCP open          telnet[ 23]        from 192.168.1.100 ttl 64
TCP open          smtp[ 25]         from 192.168.1.100 ttl 64
TCP open          domain[ 53]        from 192.168.1.100 ttl 64
TCP open          http[ 80]         from 192.168.1.100 ttl 64
TCP open          sunrpc[ 111]       from 192.168.1.100 ttl 64
TCP open          netbios-ssn[ 139]   from 192.168.1.100 ttl 64
TCP open          microsoft-ds[ 445]  from 192.168.1.100 ttl 64
TCP open          exec[ 512]        from 192.168.1.100 ttl 64
TCP open          login[ 513]       from 192.168.1.100 ttl 64
TCP open          shell[ 514]       from 192.168.1.100 ttl 64
TCP open          rmiregistry[ 1099]  from 192.168.1.100 ttl 64
TCP open          ingreslock[ 1524]   from 192.168.1.100 ttl 64
TCP open          shilp[ 2049]       from 192.168.1.100 ttl 64
TCP open          scientia-ssdb[ 2121] from 192.168.1.100 ttl 64
TCP open          mysql[ 3306]       from 192.168.1.100 ttl 64
TCP open          distcc[ 3632]      from 192.168.1.100 ttl 64
TCP open          postgresql[ 5432]   from 192.168.1.100 ttl 64
TCP open          winvnc[ 5900]      from 192.168.1.100 ttl 64
TCP open          x11[ 6000]         from 192.168.1.100 ttl 64
TCP open          irc[ 6667]         from 192.168.1.100 ttl 64
TCP open          unknown[ 6697]     from 192.168.1.100 ttl 64
TCP open          unknown[ 8009]     from 192.168.1.100 ttl 64
TCP open          unknown[ 8180]     from 192.168.1.100 ttl 64
TCP open          msgsrvr[ 8787]     from 192.168.1.100 ttl 64
TCP open          unknown[33699]     from 192.168.1.100 ttl 64
TCP open          unknown[36090]     from 192.168.1.100 ttl 64
TCP open          unknown[48381]     from 192.168.1.100 ttl 64
TCP open          unknown[50015]     from 192.168.1.100 ttl 64
adding 192.168.1.100/32 mode `UDPscan' ports `a' pps 3000
using interface(s) eth0
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
UDP open 192.168.1.100:45580 ttl 64
UDP open 192.168.1.100:53 ttl 64
UDP open 192.168.1.100:111 ttl 64
UDP open 192.168.1.100:137 ttl 64
UDP open 192.168.1.100:2049 ttl 64
UDP open 192.168.1.100:56534 ttl 64
UDP open 192.168.1.100:53009 ttl 64
sender statistics 2975.7 pps with 196635 packets sent total
listener statistics 21 packets recieved 0 packets dropped and 0 interface drops
UDP open          domain[ 53]          from 192.168.1.100 ttl 64
UDP open          sunrpc[ 111]         from 192.168.1.100 ttl 64
UDP open          netbios-ns[ 137]      from 192.168.1.100 ttl 64
UDP open          shilp[ 2049]         from 192.168.1.100 ttl 64
UDP open          unknown[45580]       from 192.168.1.100 ttl 64
UDP open          unknown[53009]       from 192.168.1.100 ttl 64
UDP open          unknown[56534]       from 192.168.1.100 ttl 64

```

```

└─(root@kali)-[/home/kali]

```

HPING3

hping3 -S 192.168.1.100

-S: Questa opzione specifica di eseguire una scansione SYN. La scansione SYN coinvolge l'invio di pacchetti SYN ai porti di destinazione. Se la porta è aperta il sistema remoto risponderà con un pacchetto SYN/ACK, indicando che la porta è aperta e il sistema è disposto a stabilire una connessione. Se la porta è chiusa, il sistema remoto risponderà con un pacchetto RST, indicando che la porta è chiusa.

```
(root@kali)-[/home/kali]
# hping3 -S 192.168.1.100
HPING 192.168.1.100 (eth0 192.168.1.100): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.100 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=3.7 ms
len=46 ip=192.168.1.100 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=11.5 ms
len=46 ip=192.168.1.100 ttl=64 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=7.0 ms
len=46 ip=192.168.1.100 ttl=64 DF id=0 sport=0 flags=RA seq=3 win=0 rtt=10.6 ms
len=46 ip=192.168.1.100 ttl=64 DF id=0 sport=0 flags=RA seq=4 win=0 rtt=10.5 ms
len=46 ip=192.168.1.100 ttl=64 DF id=0 sport=0 flags=RA seq=5 win=0 rtt=6.5 ms
len=46 ip=192.168.1.100 ttl=64 DF id=0 sport=0 flags=RA seq=6 win=0 rtt=6.0 ms
len=46 ip=192.168.1.100 ttl=64 DF id=0 sport=0 flags=RA seq=7 win=0 rtt=5.5 ms
^C
— 192.168.1.100 hping statistic —
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 3.7/7.7/11.5 ms

(root@kali)-[/home/kali]
#
```

MASSCAN

masscan <network> -p80 -banners -source-ip <target>

<network>: Questo è il range di indirizzi IP o il singolo indirizzo IP della rete che si desidera esaminare.

-p80: Questa opzione specifica di effettuare la scansione solo sulla porta 80, che è comunemente utilizzata per il protocollo HTTP.

--banners: Questa opzione specifica di raccogliere i banner dei servizi che rispondono sulla porta 80. Un "banner" è una stringa di testo inviata dal server quando viene stabilita una connessione, che può includere informazioni sul servizio o sulla versione in esecuzione.

```
# masscan 192.168.1.100 -p80 --banners --source-ip 192.168.1.100

Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-04-26 16:49:43 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]

(root@kali)-[/home/kali]
#
```

(porta chiusa)