

In questo esercizio utilizzeremo alcuni tool su kali linux per scansionare la macchina target metasploitable.

per prima cosa dobbiamo essere certi che le 2 macchine siano sulla stessa rete.

- Kali linux :

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.2.121 netmask 255.255.255.0 broadcast 192.168.2.255  
    inet6 fe80::b3b0:a278:94ee:3bd prefixlen 64 scopeid 0<20<link>  
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)  
    RX packets 267050 bytes 16134514 (15.3 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 267529 bytes 19603487 (18.6 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 36 bytes 3288 (3.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 36 bytes 3288 (3.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

- Metasploitable

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:96:59:dc  
          inet addr:192.168.2.120 Bcast:192.168.2.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe96:59dc/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B) TX bytes:4550 (4.4 KB)  
          Base address:0xd020 Memory:f0200000-f0220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING MTU:16436 Metric:1  
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:121 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:23893 (23.3 KB) TX bytes:23893 (23.3 KB)  
  
msfadmin@metasploitable:~$
```

Adesso utilizzeremo alcuni tool per scansionare la rete di metasploitable.

- `nmap -sn -PE 192.168.2.120`

L'opzione `-sn` in **Nmap** indica di eseguire una **scansione di tipo ping** (Host Discovery) senza effettuare una scansione delle porte. In pratica, Nmap invierà pacchetti di pin per verificare se gli host specificati sono "vivi" o "attivi".

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo nmap -sn -PE 192.168.2.120
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 13:38 EDT
Nmap scan report for 192.168.2.120
Host is up (0.0027s latency).
MAC Address: 08:00:27:96:59:DC (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds

(kali@kali)-[~]
$

```

- nmap 192.168.2.120 -top-port 10 -open

Con -top-port, è possibile identificare facilmente le prime 10 porte aperte in qualsiasi rete.

```

kali@kali: ~
File Actions Edit View Help

$ sudo nmap 192.168.2.120 --top-ports 10 -open
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 13:40 EDT
Failed to resolve "-".
Bare '-': did you put a space between '--'?

(kali@kali)-[~]
$ sudo nmap 192.168.2.120 --top-ports 10 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 13:40 EDT
Nmap scan report for 192.168.2.120
Host is up (0.00069s 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: 08:00:27:96:59:DC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds

(kali@kali)-[~]
$

```

- nmap 192.168.2.120 -p- -sV -reason -dns-server ns

questo comando può essere utile per capire il motivo per cui una porta è contrassegnata come **aperto**, **chiuso**, o **filtrato** e perché l'host è contrassegnato come **vivo**.

```

kali@kali: ~
File Actions Edit View Help

$ sudo nmap 192.168.2.120 -p- -sV -reason -dns-server ns
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 13:41 EDT
Host is up (0.00069s 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: 08:00:27:96:59:DC (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds

```

- `nmap -sS -sV -T4 192.168.2.120`

questo comando utilizza una scansione semiaperta perché non si stabilisce una connessione TCP completa. Invece, invia solo un pacchetto SYN e attendiamo la risposta. Se riceviamo una risposta SYN / ACK, significa che la porta sta ascoltando. L'opzione **-Sv** Questa opzione esegue una **scansione dei servizi**, cercando di determinare le **versioni dei servizi** in esecuzione su ciascuna porta aperta.

```
(kali@kali)-[~]
$ sudo nmap -sS -sV -T4 192.168.2.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 13:44 EDT
Nmap scan report for 192.168.2.120
Host is up (0.00040s 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  http             Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:96:59:DC (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 193.25 seconds
(kali@kali)-[~]
$
```

- `nmap -f -mtu = 512 192.168.2.120`

Con l'opzione **-f e -mtu**, è possibile bypassare facilmente le restrizioni del firewall mediante la frammentazione dei pacchetti.

L'opzione **-f** fa sì che la scansione utilizzi piccoli pacchetti IP frammentati. L'idea è quella di suddividere l'intestazione TCP su diversi pacchetti per rendere più difficile per i filtri dei pacchetti, i sistemi di rilevamento delle intrusioni e altri fastidi rilevare ciò che stai facendo.

```
File Firefox ESR
Browse the WorldWide Web

(kali@kali)-[~]
$ sudo nmap -f --mtu=512 192.168.2.120
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 13:47 EDT
Nmap scan report for 192.168.2.120
Host is up (0.00025s 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: 08:00:27:96:59:DC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds

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

- hping3 – scansione known 192.168.2.120

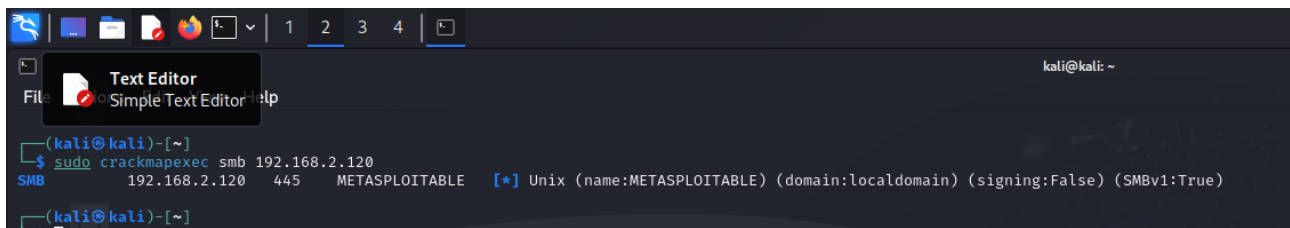
hping non è solo in grado di inviare richieste echo ICMP ma supporta anche i protocolli TCP, UDP, ICMP e RAW-IP, ha una modalità traceroute, la possibilità di inviare file tra un canale coperto e molte altre funzionalità.

```
File Actions Edit View Help
/home/kali kali@kali: ~

(kali@kali)-[~]
$ sudo hping3 --scan known 192.168.2.120
[sudo] password for kali:
Scanning 192.168.2.120 (192.168.2.120), 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)
```

- crackmapexec smb 192.168.2.120

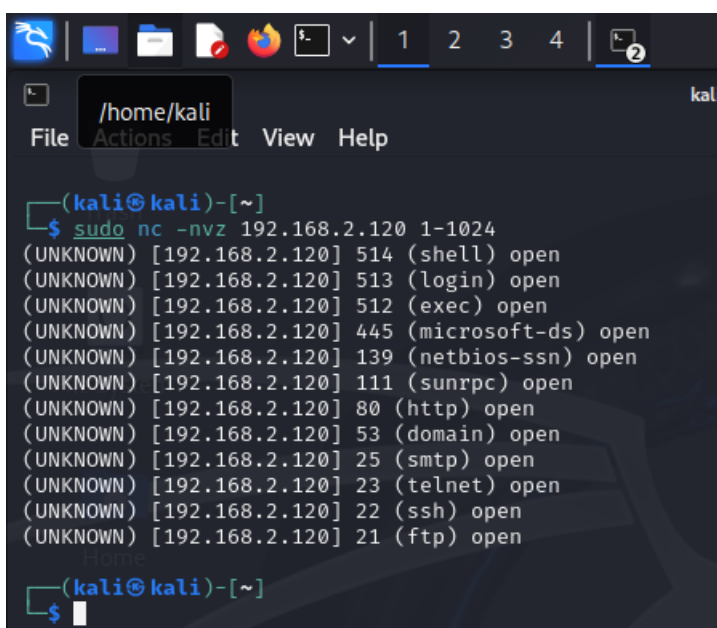
questo tool è molto interessante perchè ottiene informazioni su utenti, gruppi, condivisioni, sessioni e servizi in reti Windows, supporta diverse modalità di raccolta credenziali e identifica vulnerabilità come credenziali deboli o configurazioni di rete errate.



```
(kali@kali)-[~]
$ sudo crackmapexec smb 192.168.2.120
SMB 192.168.2.120 445 METASPLOITABLE [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)
(kali@kali)-[~]
```

- `nc -nvz 192.168.2.120 1-1024`

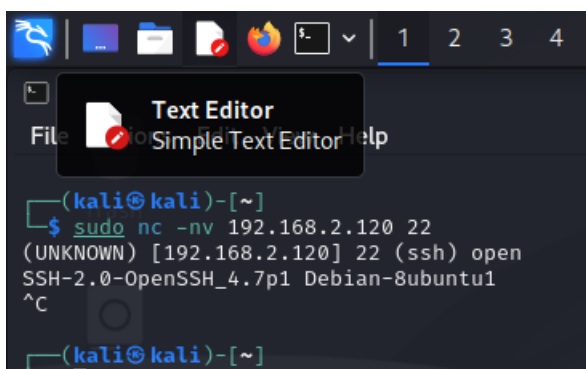
il comando esegue una scansione rapida dell'indirizzo IP specificato per verificare quali porte sono aperte e in ascolto. Non stabilisce una connessione completa né invia alcun dato.



```
(kali@kali)-[~]
$ sudo nc -nvz 192.168.2.120 1-1024
(UNKNOWN) [192.168.2.120] 514 (shell) open
(UNKNOWN) [192.168.2.120] 513 (login) open
(UNKNOWN) [192.168.2.120] 512 (exec) open
(UNKNOWN) [192.168.2.120] 445 (microsoft-ds) open
(UNKNOWN) [192.168.2.120] 139 (netbios-ssn) open
(UNKNOWN) [192.168.2.120] 111 (sunrpc) open
(UNKNOWN) [192.168.2.120] 80 (http) open
(UNKNOWN) [192.168.2.120] 53 (domain) open
(UNKNOWN) [192.168.2.120] 25 (smtp) open
(UNKNOWN) [192.168.2.120] 23 (telnet) open
(UNKNOWN) [192.168.2.120] 22 (ssh) open
(UNKNOWN) [192.168.2.120] 21 (ftp) open
(kali@kali)-[~]
$
```

- `nc -nv 192.168.2.120 22`

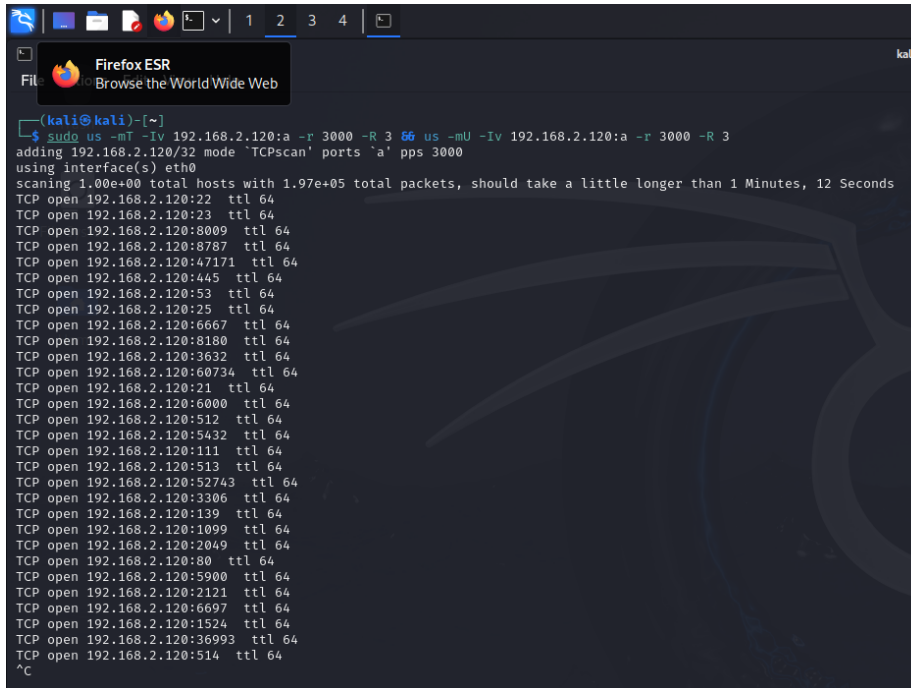
il comando tenta di stabilire una connessione alla porta specificata sull'indirizzo IP di destinazione cioè il 22 . possiamo vedere che la porta 22 sul computer remoto stampa il nome e la versione del servizio.



```
(kali@kali)-[~]
$ sudo nc -nv 192.168.2.120 22
(UNKNOWN) [192.168.2.120] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C
(kali@kali)-[~]
```

- `us -mT -lv 192.168.2.120: a -r 3000 -R 3 & us -mU -lv 102.168.2.120: a -r 3000 -R 3`

Unicorns can be configured automatically for a TCP / UDP scan, unlike nmap. By default, it sends a SYN scan. Let's say we are scanning the IP of metasploitable (192.168.169.120), looking for all ports and sending 3000 packets per second.



```
(kali@kali)-[~]
$ sudo us -mT -lv 192.168.2.120:a -r 3000 -R 3 66 us -mU -lv 192.168.2.120:a -r 3000 -R 3
adding 192.168.2.120/32 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 192.168.2.120:22 ttl 64
TCP open 192.168.2.120:23 ttl 64
TCP open 192.168.2.120:8009 ttl 64
TCP open 192.168.2.120:8787 ttl 64
TCP open 192.168.2.120:47171 ttl 64
TCP open 192.168.2.120:445 ttl 64
TCP open 192.168.2.120:53 ttl 64
TCP open 192.168.2.120:25 ttl 64
TCP open 192.168.2.120:6667 ttl 64
TCP open 192.168.2.120:8180 ttl 64
TCP open 192.168.2.120:3632 ttl 64
TCP open 192.168.2.120:60734 ttl 64
TCP open 192.168.2.120:21 ttl 64
TCP open 192.168.2.120:6000 ttl 64
TCP open 192.168.2.120:512 ttl 64
TCP open 192.168.2.120:5432 ttl 64
TCP open 192.168.2.120:111 ttl 64
TCP open 192.168.2.120:513 ttl 64
TCP open 192.168.2.120:52743 ttl 64
TCP open 192.168.2.120:3306 ttl 64
TCP open 192.168.2.120:139 ttl 64
TCP open 192.168.2.120:1099 ttl 64
TCP open 192.168.2.120:2049 ttl 64
TCP open 192.168.2.120:80 ttl 64
TCP open 192.168.2.120:5900 ttl 64
TCP open 192.168.2.120:2121 ttl 64
TCP open 192.168.2.120:6697 ttl 64
TCP open 192.168.2.120:1524 ttl 64
TCP open 192.168.2.120:36993 ttl 64
TCP open 192.168.2.120:514 ttl 64
^C
```