Questo comando ci permette di fare una ricognizione generica del target

- **sudo nmap -sn -PE 192.168.50.100/24**

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 03:12 EDT
Nmap scan report for 192.168.50.1
Host is up (0.0016s latency).
Nmap scan report for 192.168.50.100
Host is up (0.00066s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 1.76 seconds
```

procediamo con la ricerca di host attivi nella rete

- **netdiscover -r 192.168.50.100**

```
Currently scanning: Finished!   |   Screen View: Unique Hosts
2 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 120
_____________________________________________________________________________
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.2     08:00:27:3c:7d:35      2     120  PCS Systemtechnik GmbH
```

ora procediamo scansionando le prime 10 porte aperte della macchina metasploitable

- **nmap 192.168.50.100 --top-ports 10 --open**

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 03:51 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0024s 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
```

con la specifica “--reason” ci viene restituito il “perchè” una porta viene contrassegnata come “open/closed/filtered”

- **nmap 192.168.50.100 -p- -sV --reason --dns-server ns**

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 03:52 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 192.168.50.100
Host is up, received syn-ack (0.00035s latency).
Not shown: 65460 closed tcp ports (conn-refused), 45 filtered tcp ports (no-response)
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 netkit-rsh rexecd
513/tcp  open  login?      syn-ack
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  X11         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)
35412/tcp open  java-rmi    syn-ack GNU Classpath grmiregistry
41224/tcp open  mountd      syn-ack 1-3 (RPC #100005)
42247/tcp open  status      syn-ack 1 (RPC #100024)
58782/tcp open  nlockmgr    syn-ack 1-4 (RPC #100021)
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 164.54 seconds
```

Continuiamo con una scansione con unicornscan, che ci permette di fare una scansione TCP/UDP in SYN, definendo quanti pacchetti al secondo mandare (3000 nel nostro caso)

- **sudo us -mT -Iv 192.168.50.100:a -r 3000 -R 3 && sudo us -mU -Iv 192.168.50.100:a -r 3000 -R 3**

```
adding 192.168.50.100/32 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 192.168.50.100:1099  ttl 63
TCP open 192.168.50.100:42247  ttl 63
TCP open 192.168.50.100:22  ttl 63
TCP open 192.168.50.100:80  ttl 63
TCP open 192.168.50.100:513  ttl 63
TCP open 192.168.50.100:6667  ttl 63
TCP open 192.168.50.100:2049  ttl 63
TCP open 192.168.50.100:5432  ttl 63
TCP open 192.168.50.100:139  ttl 63
TCP open 192.168.50.100:3632  ttl 63
TCP open 192.168.50.100:41224  ttl 63
TCP open 192.168.50.100:35412  ttl 63
TCP open 192.168.50.100:445  ttl 63
TCP open 192.168.50.100:8009  ttl 63
TCP open 192.168.50.100:58782  ttl 63
TCP open 192.168.50.100:512  ttl 63
TCP open 192.168.50.100:2121  ttl 63
TCP open 192.168.50.100:25  ttl 63
TCP open 192.168.50.100:5900  ttl 63
TCP open 192.168.50.100:8787  ttl 63
TCP open 192.168.50.100:21  ttl 63
TCP open 192.168.50.100:111  ttl 63
TCP open 192.168.50.100:514  ttl 63
TCP open 192.168.50.100:23  ttl 63
TCP open 192.168.50.100:8180  ttl 63
TCP open 192.168.50.100:3306  ttl 63
TCP open 192.168.50.100:53  ttl 63
TCP open 192.168.50.100:6697  ttl 63
sender statistics 2944.1 pps with 196608 packets sent total
listener statistics 87193 packets recieved 0 packets droped and 0 interface drops
TCP open                     ftp[   21]         from 192.168.50.100  ttl 63
TCP open                     ssh[   22]         from 192.168.50.100  ttl 63
TCP open                  telnet[   23]         from 192.168.50.100  ttl 63
TCP open                    smtp[   25]         from 192.168.50.100  ttl 63
TCP open                  domain[   53]         from 192.168.50.100  ttl 63
TCP open                    http[   80]         from 192.168.50.100  ttl 63
TCP open                  sunrpc[  111]         from 192.168.50.100  ttl 63
TCP open             netbios-ssn[  139]         from 192.168.50.100  ttl 63
TCP open            microsoft-ds[  445]         from 192.168.50.100  ttl 63
TCP open                    exec[  512]         from 192.168.50.100  ttl 63
TCP open                   login[  513]         from 192.168.50.100  ttl 63
TCP open                   shell[  514]         from 192.168.50.100  ttl 63
TCP open             rmiregistry[ 1099]         from 192.168.50.100  ttl 63
TCP open                   shilp[ 2049]         from 192.168.50.100  ttl 63
TCP open           scientia-ssdb[ 2121]         from 192.168.50.100  ttl 63
TCP open                   mysql[ 3306]         from 192.168.50.100  ttl 63
TCP open                  distcc[ 3632]         from 192.168.50.100  ttl 63
TCP open              postgresql[ 5432]         from 192.168.50.100  ttl 63
TCP open                  winvnc[ 5900]         from 192.168.50.100  ttl 63
TCP open                     irc[ 6667]         from 192.168.50.100  ttl 63
TCP open                 unknown[ 6697]         from 192.168.50.100  ttl 63
TCP open            unknown[ 8009]      from 192.168.50.100  ttl 63
TCP open            unknown[ 8180]      from 192.168.50.100  ttl 63
TCP open            msgsrvr[ 8787]     from 192.168.50.100  ttl 63
TCP open            unknown[35412]      from 192.168.50.100  ttl 63
TCP open            unknown[41224]      from 192.168.50.100  ttl 63
TCP open            unknown[42247]      from 192.168.50.100  ttl 63
TCP open            unknown[58782]      from 192.168.50.100  ttl 63
adding 192.168.50.100/32 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 192.168.50.100:111  ttl 63
UDP open 192.168.50.100:137  ttl 63
UDP open 192.168.50.100:2049  ttl 63
UDP open 192.168.50.100:53  ttl 63
UDP open 192.168.50.100:36376  ttl 63
sender statistics 2950.7 pps with 196635 packets sent total
listener statistics 9 packets recieved 0 packets droped and 0 interface drops
UDP open                 domain[   53]      from 192.168.50.100  ttl 63
UDP open                 sunrpc[  111]      from 192.168.50.100  ttl 63
UDP open             netbios-ns[  137]      from 192.168.50.100  ttl 63
UDP open                  shilp[ 2049]      from 192.168.50.100  ttl 63
UDP open                unknown[36376]      from 192.168.50.100  ttl 63
```

avviamo una scansione senza stabilire una connessione TCP. Mandiamo un pacchetto SYN, se la porta risponde, SYN/ACK, la porta è aperta

- **sudo nmap -sS -sV -T4 192.168.50.100**

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 03:59 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00061s 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?
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  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  unknown     Apache-Coyote/1.1
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 20.53 seconds
```

Scansione con HPING3

- **sudo hping3 --scan known 192.168.50.100**

```
[sudo] password for kali:
Scanning 192.168.50.100 (192.168.50.100), port known
264 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
*** buffer overflow detected ***: terminated
zsh: IOT instruction  sudo hping3 --scan known 192.168.50.100
```

scansione con netcat, -n serve a specificare di non usare il DNS

- **nc -nvz 192.168.50.100 1-1024**

```
(UNKNOWN) [192.168.50.100] 514 (shell) open
(UNKNOWN) [192.168.50.100] 513 (login) open
(UNKNOWN) [192.168.50.100] 512 (exec) open
(UNKNOWN) [192.168.50.100] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.100] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.100] 111 (sunrpc) open
(UNKNOWN) [192.168.50.100] 80 (http) open
(UNKNOWN) [192.168.50.100] 53 (domain) open
(UNKNOWN) [192.168.50.100] 25 (smtp) open
(UNKNOWN) [192.168.50.100] 23 (telnet) open
(UNKNOWN) [192.168.50.100] 22 (ssh) open
(UNKNOWN) [192.168.50.100] 21 (ftp) open
```

per ogni porta rilevata in precedenza possiamo andare a vederne il banner, rilevando nome e versione del servizio sulla porta

- **nc -nv 192.168.50.100 22**

```
(UNKNOWN) [192.168.50.100] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

con questo comando chiedo a nmap di rifare uno scan sulle porte edestrapolare piu' informazioni sui servizi e sulle porte aperte

- **nmap -sV 192.168.50.100**

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 04:04 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0021s 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      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  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       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
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 11.44 seconds
```

con questo comando vado a fare una scasione nmap con pacchetti ridotti in maniera da essere meno visibile dai sistemi di sicurezza

- **sudo nmap -f --mtu=512 192.168.50.100**

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 04:07 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00056s 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
```

```
/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

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

- **sudo masscan 192.168.50.1/24 -p80 --banners --source-ip 192.168.50.100**

```
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-08-26 08:08:42 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
```