

**nmap -sn -PE <target>** questo comando ci permette di scoprire quanti e quali hosts attivi ci sono sulla rete; nel nostro caso abbiamo due host attivi con IP 192.168.2.1 e 192.168.2.101

```
(root@kali)-[/home/kali]
# nmap -sn -PE 192.168.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-30 10:46 EDT
Nmap scan report for 192.168.2.1
Host is up (0.0012s latency).
Nmap scan report for 192.168.2.101
Host is up (0.0032s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 15.09 seconds
```

e successivamente con il comando **nmap -sS -sV -T4 <target>** possiamo capire che tipo di macchine sono e quali porte aperte hanno, noi abbiamo 2 host (192.168.2.1) ha 3 porte attive ed è un server, l'IP 192.168.2.101 è un client (metasploitable) ed ha svariate porte aperte.

```
(root@kali)-[/home/kali]
# nmap -sS -sV -T4 192.168.2.101/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-30 10:23 EDT
Stats: 0:02:07 elapsed; 254 hosts completed (2 up), 2 undergoing Service Scan
Service scan Timing: About 92.31% done; ETC: 10:26 (0:00:09 remaining)
Nmap scan report for 192.168.2.1
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Unbound
80/tcp    open  http         nginx
443/tcp   open  ssl/http     nginx

Nmap scan report for 192.168.2.101
Host is up (0.027s 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 rshd
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  ccproxy-ftp?
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  unknown

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: 256 IP addresses (2 hosts up) scanned in 194.16 seconds
```

Le porte aperte le possiamo vedere anche con il comando **nmap -f -mtu=512 <target>**

Anche il comando **nmap <target> -top-ports 10 --open** ci permette di vedere le porte aperte su un IP che se la scansione è più veloce e quindi meno approfondita, noi abbiamo scansionato l'IP 192.168.2.101 e ci ha mostrato le porte aperte che possiamo provare ad usare, indicandoci il tipo di servizio e il numero della porta

```
(root@kali)-[/home/kali]
# nmap 192.168.2.101 --top-port 10 --open
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-30 10:15 EDT
Nmap scan report for 192.168.2.101
Host is up (0.0040s 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

Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
```

(es. 80/TCP http)

Il comando **hping3 --scan known <target>** ci permette di fare una scansione di tutte le porte sull'IP desiderato indicando il n. della porta e il servizio (1 tcpmux).

```
(root@kali)-[/home/kali]
# hping3 --scan known 192.168.2.101
Scanning 192.168.2.101 (192.168.2.101), 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: (1 tcpmux) (2 nbp) (4 echo) (6 zip) (7 echo) (9 discard) (11 systat) (13 daytime) (15 netstat)
(17 qotd) (19 chargen) (20 ftp-data) (21 ftp) (22 ssh) (23 telnet) (25 smtp) (37 time) (43 whois) (49 tacacs) (53 d
omain) (67 bootps) (68 bootpc) (69 tftp) (70 gopher) (79 finger) (80 http) (88 kerberos) (102 iso-tsap) (104 acr-nem
a) (106 poppassd) (110 pop3) (111 sunrpc) (113 auth) (119 nntp) (123 ntp) (135 epmap) (137 netbios-ns) (138 netbios-
dgm) (139 netbios-ssn) (143 imap2) (161 snmp) (162 snmp-trap) (163 cmip-man) (164 cmip-agent) (174 mailq) (177 talk) (
179 bgp) (199 smux) (209 qmtip) (210 z3950) (213 ipx) (319 ptp-event) (320 ptp-general) (345 pawsserv) (346 zserv)
(369 rpc2portmap) (370 codaauth2) (371 clearcase) (389 ldap) (427 svrloc) (443 https) (444 snpp) (445 microsoft-d) (
464 kpasswd) (465 submissions) (487 saft) (500 isakmp) (512 exec) (513 login) (514 shell) (515 printer) (517 talk) (
518 ntalk) (520 route) (538 gdomap) (540 uucp) (543 klogin) (544 kshell) (546 dhcpv6-clie) (547 dhcpv6-serv) (548 af
povertcp) (554 rtsp) (563 nntps) (587 submission) (607 nqs) (623 asf-rmcp) (628 qmcp) (631 ipp) (636 ldaps) (646 ldp
) (655 tinc) (706 silc) (749 kerberos-ad) (750 kerberos4) (751 kerberos-ma) (752 passwd-serv) (754 krb-prop) (775 mo
ira-db) (777 moira-updat) (779 moira-ureg) (783 spamd) (853 domain-s) (871 supfilesrv) (873 rsync) (989 ftps-data) (
990 ftps) (992 telnets) (993 imaps) (995 pop3s) (1080 socks) (1093 proofd) (1094 rootd) (1099 rmiregistry) (1127 sup
filedbg) (1178 skkserv) (1194 openvpn) (1210 predict) (1236 rmtcfg) (1313 xtel) (1314 xtelw) (1352 lotusnote) (1433
ms-sql-s) (1434 ms-sql-m) (1524 ingreslock) (1645 datametrics) (1646 sa-msg-port) (1649 kermit) (1677 groupwise) (17
01 l2f) (1812 radius) (1813 radius-acct) (2000 cisco-sccp) (2049 nfs) (2086 gnutel) (2101 rctm-sc104) (2102 zephyr-s
rv) (2103 zephyr-clt) (2104 zephyr-hm) (2119 gsgatekeep) (2121 iprop) (2135 gris) (2401 cvspserver) (2430 venus) (2
431 venus-se) (2432 codasrv) (2433 codasrv-se) (2583 mon) (2600 zebrasrv) (2601 zebra) (2602 ripd) (2603 ripngd) (26
04 ospfd) (2605 bgpd) (2606 ospf6d) (2607 ospfapi) (2608 isisd) (2628 dict) (2792 f5-globals) (2811 gsift) (2947 g
psd) (3050 gds-db) (3130 icpv2) (3205 isns) (3260 iscsi-targe) (3306 mysql) (3389 ms-wbt-serv) (3493 nut) (3632 dist
cc) (3689 daap) (3690 svn) (4031 suucp) (4094 sysrqd) (4190 sieve) (4353 f5-iquery) (4369 epmd) (4373 remctl) (4460
ntske) (4500 ipsec-nat-t) (4557 fax) (4559 hylafax) (4569 iax) (4691 mtm) (4899 radmin-port) (4949 munin) (5060 sip)
(5061 sip-tls) (5222 xmpp-client) (5269 xmpp-server) (5308 cfengine) (5353 mdns) (5432 postgresql) (5555 rplay) (55
56 freeciv) (5666 nrpe) (5667 nsca) (5671 amqps) (5672 amqp) (5680 canna) (6000 x11) (6001 x11-1) (6002 x11-2) (6003
x11-3) (6004 x11-4) (6005 x11-5) (6006 x11-6) (6007 x11-7) (6346 gnutella-sv) (6347 gnutella-rt) (6379 redis) (6444
sge-qmaster) (6445 sge-execd) (6446 mysql-proxy) (6514 syslog-tls) (6566 sane-port) (6667 ircd) (6696 babel) (6697
ircs-u) (7000 bbs) (7001 afs3-callba) (7002 afs3-prserv) (7003 afs3-vlerv) (7004 afs3-kaserv) (7005 afs3-volser) (7
007 afs3-bos) (7008 afs3-update) (7009 afs3-rmtsys) (7100 font-servic) (8021 zope-ftp) (8080 http-alt) (8081 tproxy)
(8088 omniORB) (8140 puppet) (8990 clc-build-d) (9098 xinetd) (9101 bacula-dir) (9102 bacula-fd) (9103 bacula-sd) (
9418 git) (9667 xmms2) (9673 zope) (10000 webmin) (10050 zabbix-agen) (10051 zabbix-trap) (10080 amanda) (10081 kama
nda) (10082 amandaidx) (10083 amidxtape) (10809 nbd) (11112 dicom) (11371 hkp) (17001 sgi-cmsd) (17002 sgi-crsd) (17
003 sgi-gcd) (17004 sgi-cad) (17500 db-lsp) (22125 dcap) (22128 gsidcap) (22273 wnn6) (24554 blinkp) (27374 asp) (308
65 csync2) (57000 dircproxy) (60177 tfido) (60179 fido)
```

Se poi vogliamo andare ad analizzare una porta nello specifico possiamo usare il comando **nc -nv <target> <port number>**.

**nc -nv**