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 attvi con IP 192.168.2.1 e 192.168.2.101

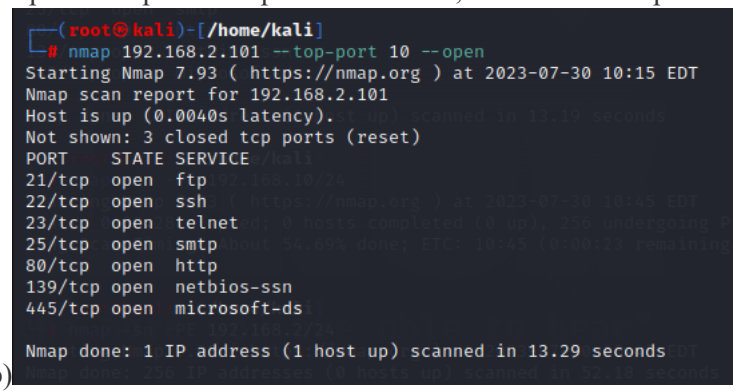
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PE 192.168.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-30 10:46 EDT
Nmap scan report for 192.168.2.1
Host is up (0.0012s latency).
Nmap scan report for 192.168.2.101
Host is up (0.0032s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned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

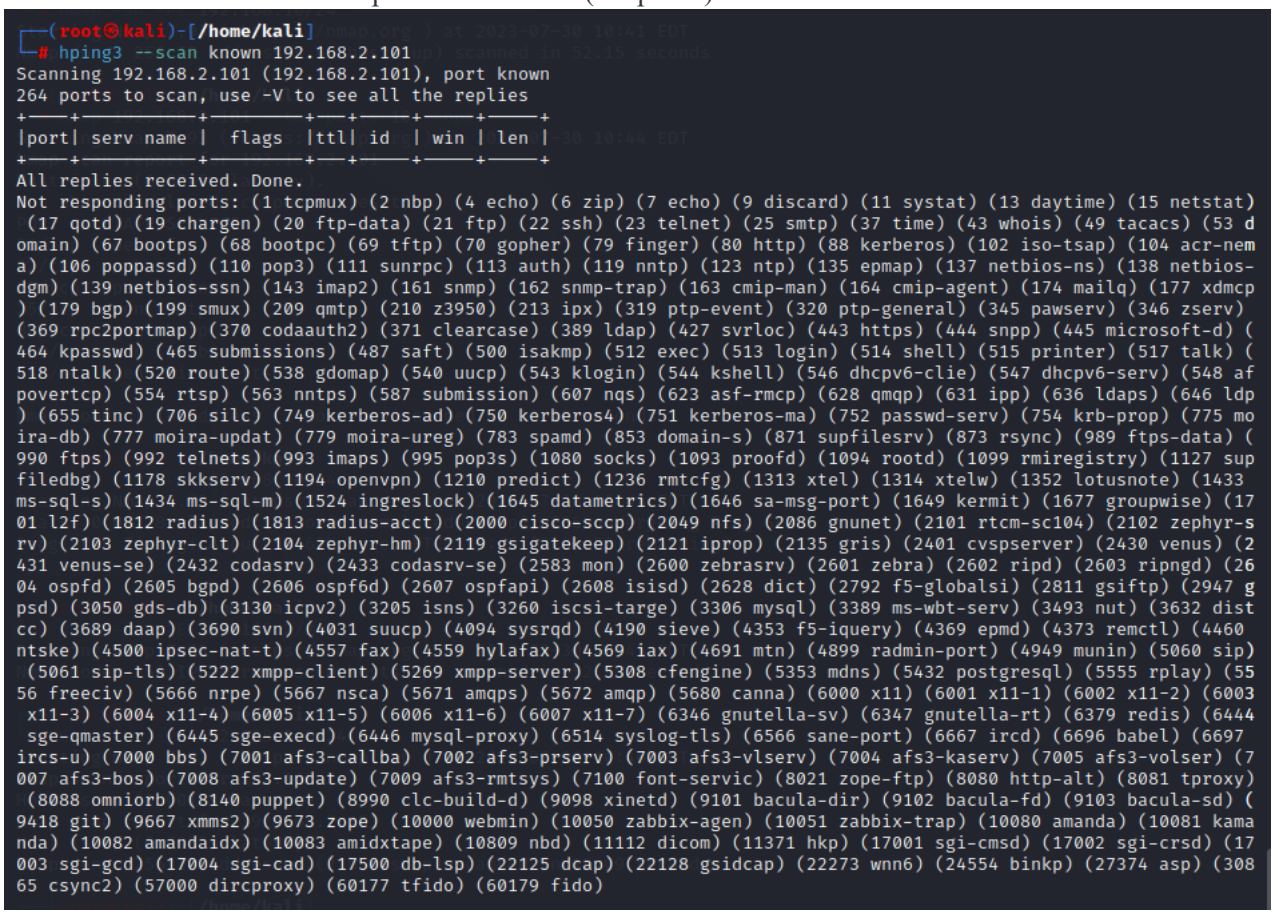
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -T4 192.168.2.101/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-30 10:23 EDT
Stats: 0:02:07 elapsed; 254 hosts completed (2 up), 2 undergoing Service Scan
Service scan Timing: About 92.31% done; ETC: 10:26 (0:00:09 remaining)
Nmap scan report for 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 rexecd
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 abbaimo 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 (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).



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