Si andranno a trovare informazioni utili sulla macchina Meta tramite strumenti di Host Scanning.

Nmap -sS esegue una scansione stealth molto veloce, in quanto non conclude il 3 way handshake ma va a fermarsi al primo passaggio, andando ad individuare le porte aperte di quell'Host.

Con -sV si andrà a visualizzare la versione di ogni servizio.

Con -T si indica la velocità con la quale si esegue il servizio.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -T4 192.168.32.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 16:34 EST
Nmap scan report for 192.168.32.102
Host is up (0.00018s 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  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  unknown
MAC Address: 08:00:27:4E:32:53 (PCS Systemtechnik/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 186.03 seconds
```

-sn mostra solo quali host sono attivi nel range che decidiamo, in questo caso si è andato ad indicare l'intera classe di rete.

-PE manda richieste ICMP, come un Ping.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -PE 192.168.32.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 16:39 EST
Nmap scan report for 192.168.32.102
Host is up (0.0019s latency).
MAC Address: 08:00:27:4E:32:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.32.100
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 29.88 seconds
```

Netdiscover -r visualizza anche lui ogni Ip presente

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.32.102  08:00:27:4e:32:53      1      60  PCS Systemtechnik GmbH

┌──(root㉿kali)-[/home/kali]
└─# netdiscover -r 192.168.32.1/24
```

nmap -A esegue un analisi molto più completa.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.32.102 -p 1-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 16:47 EST
Nmap scan report for 192.168.32.102
Host is up (0.00100s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.32.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp  open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      37793/tcp   mountd
|   100005  1,2,3      56670/udp   mountd
|   100021  1,3,4      41661/udp   nlockmgr
|   100021  1,3,4      52996/tcp   nlockmgr
|   100024  1          41455/tcp   status
|_  100024  1          57005/udp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:4E:32:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h30m07s, deviation: 3h32m08s, median: 6s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-12-05T16:48:27-05:00

TRACEROUTE
HOP RTT     ADDRESS
1   1.00 ms 192.168.32.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 88.03 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```