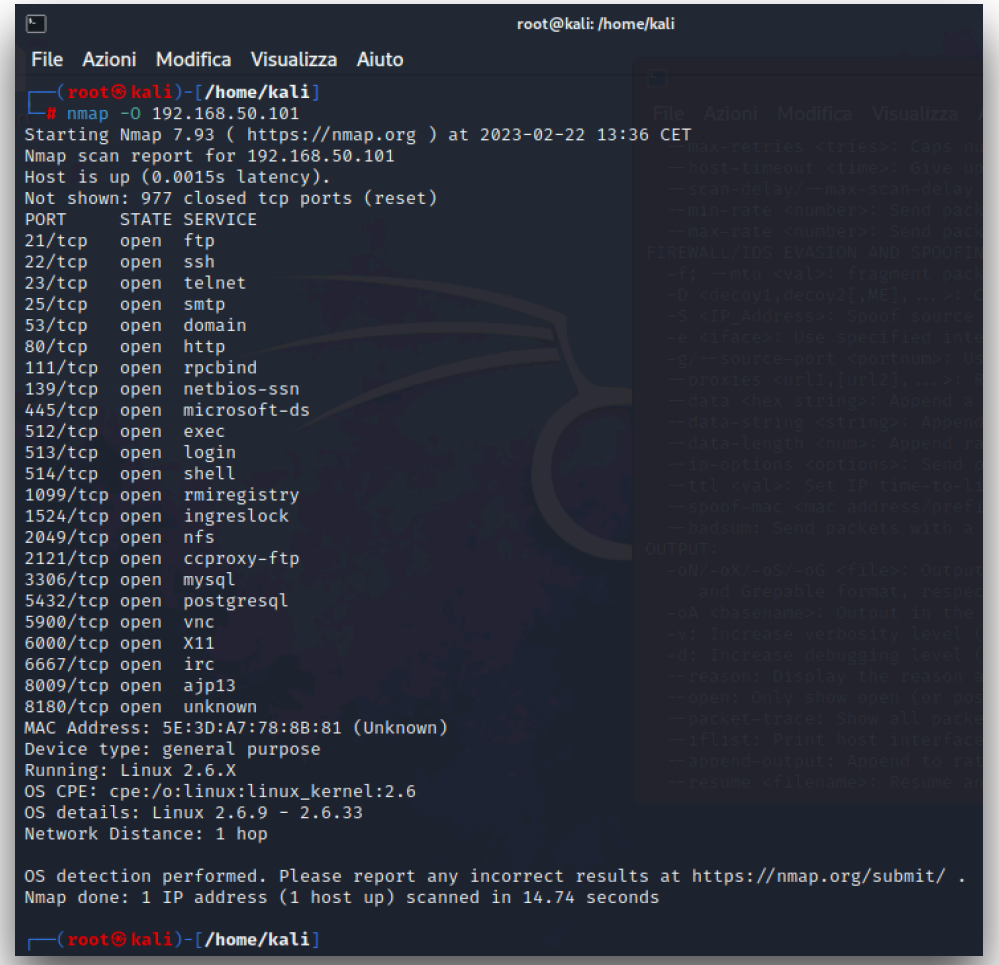
3. Identificazione servizi e scansione

-Scansioni su target Metasploitable

Ip: 192.168.50.101
Sistema operativo:
nmap 192.168.50.101 --script smb-os-discovery

```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-02-22T09:26:46-05:00
```

OS Fingerprint



Ci restituisce le porte aperte e i servizi corrispondenti ad ogni porta.

Syn Scan

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 13:42 CET
Nmap scan report for 192.168.50.101
Host is up (0.00094s 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: 5E:3D:A7:78:8B:81 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

TCP Connect

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 13:45 CET
Nmap scan report for 192.168.50.101
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (conn-refused)
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: 5E:3D:A7:78:8B:81 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

La differenza sostanziale tra i due è la latenza che varia.
Il SYN scan non completa il 3-way-handshake e per questo ha un latenza minore rispetto al TCP Connect dove abbiamo però una precisione maggiore.

Version Detection

Col seguente comando possiamo trovare i servizi in ascolto sulle porte e le loro relative versioni

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 13:46 CET
Stats: 0:02:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 13:49 (0:00:07 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00077s 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: 5E:3D:A7:78:8B:81 (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 185.83 seconds
```

Nmap output per la creazione di file report

Es. nmap -sT -oN reportmeta2.txt 192.168.50.101

```
┌──(root㉿kali)-[/home/kali]
└─# ls
Documenti  Modelli  Pubblici         reportmeta2.txt  reportmeta.txt  Scrivania
Immagini   Musica   reportmeta1.txt  reportmeta3.txt  Scaricati       Video
```

-Scansione su target Windows 7

Indirizzo ip: 192.168.50.103

OS Fingerprint

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 14:49 CET
Nmap scan report for 192.168.50.103
Host is up (0.0017s latency).
All 1000 scanned ports on 192.168.50.103 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: CE:DA:C0:90:40:80 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 37.10 seconds
```

Come possiamo vedere non riusciamo a trovare risultati.
La motivazione per cui non abbiamo un risultato è il fatto che Windows blocca il ping effettuato dallo scan di nmap attraverso un firewall.
Per questa ragione non basterà un semplice scan per riuscire ad ottenere delle informazioni ma bisognerà adottare un metodo di evasione.
Possiamo quindi utilizzare il Timing per gestire le tempistiche con cui nmap invia richieste al target ed anche una scansione su una porta sorgente che potrebbe essere aperta come la porta 80.
Per quanto riguarda l'utilizzo del **-T1**, richiederebbe un tempo elevato per poter avere un riscontro.

Es. port 80

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 80 192.168.50.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 16:15 CET
Nmap scan report for 192.168.50.103
Host is up (0.0014s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: CE:DA:C0:90:40:80 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds
```