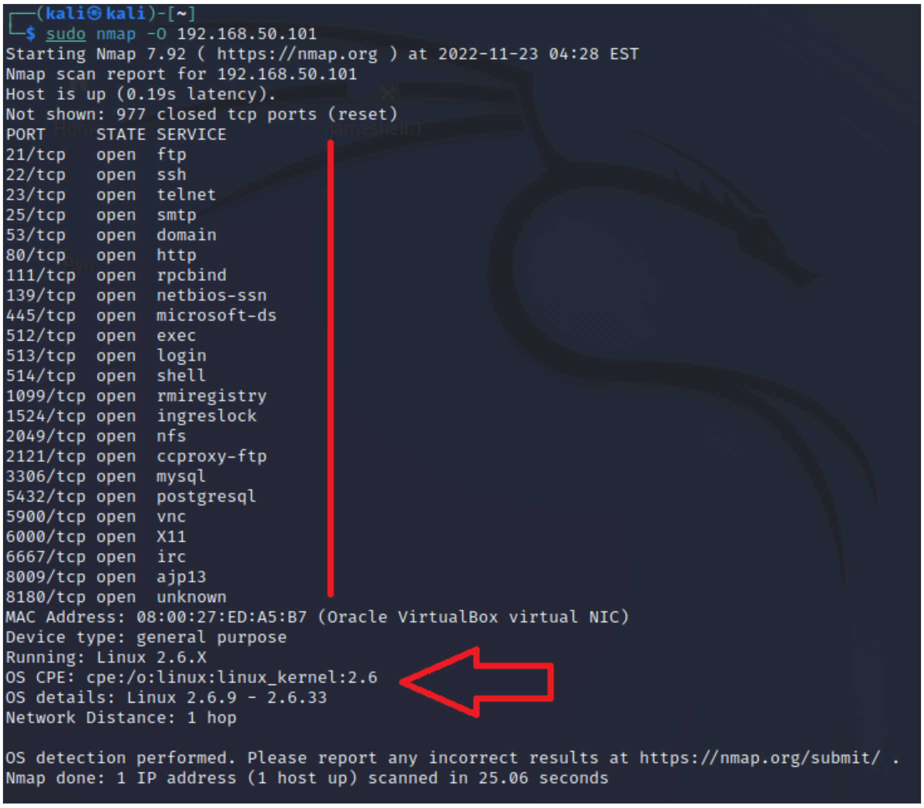
Tecniche scansione NMAP

Dopo aver di nuovo configurato le rispettive reti:

- Kali : 192.168.50.100
- Metasploitable: 192.168.50.101
- Windows: 192.168.50.103

OsFingerprint Metasploitable



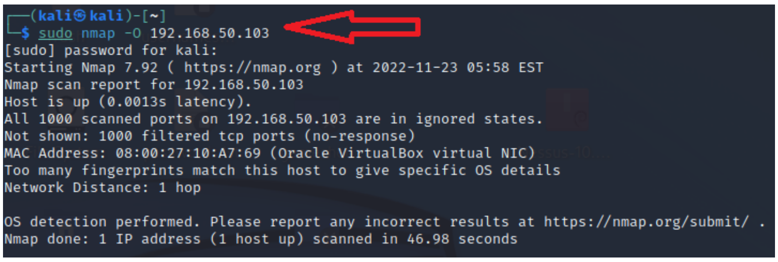
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 04:28 EST
Nmap scan report for 192.168.50.101
Host is up (0.19s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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: 08:00:27:ED:A5:B7 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.06 seconds
```

Qui possiamo vedere Metasploitable con le rispettive informazioni

- Porte Aperte
- Servizi Attivi
- Sistema Operativo

Scansione Windows :



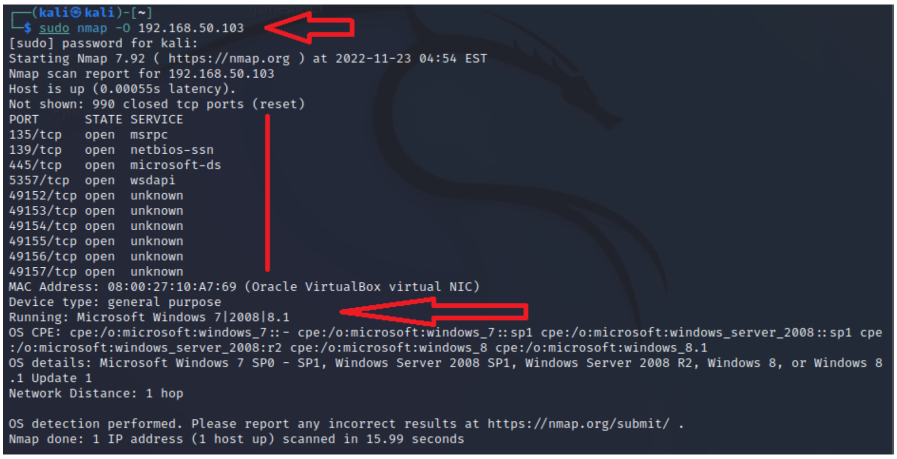
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.103
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 05:58 EST
Nmap scan report for 192.168.50.103
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.50.103 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:10:A7:69 (Oracle VirtualBox virtual NIC)
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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.98 seconds
```

Questo è il risultato ottenuto provato a scansionare Windows con il Firewall **Attivo.**

Le varie informazioni rimangono nascoste.

Se invece disattiviamo il Firewall



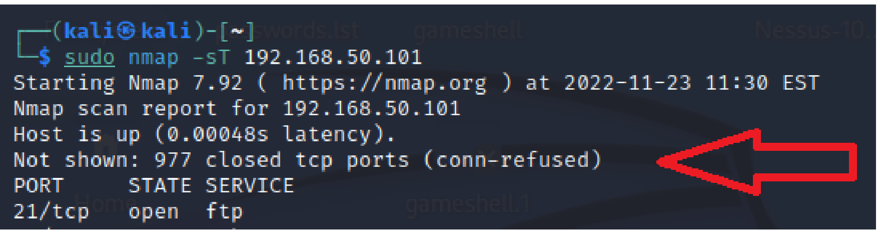
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.103
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 04:54 EST
Nmap scan report for 192.168.50.103
Host is up (0.00055s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:10:A7:69 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe
:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8
.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.99 seconds
```

Possiamo trovare tutte le informazioni che ricercavamo:

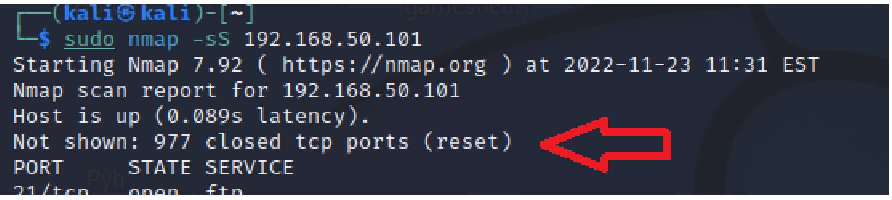
- Porte Aperte
- Servizi
- Sistema Operativo

In aggiunta possiamo trovare le due scansioni con **-sS** e **-sT**.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 11:30 EST
Nmap scan report for 192.168.50.101
Host is up (0.00048s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
```

Qui possiamo vedere come viene concluso il Three Way Handshake



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 11:31 EST
Nmap scan report for 192.168.50.101
Host is up (0.089s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
```

A differenza, qui non viene concluso bensì viene resettata la richiesta.