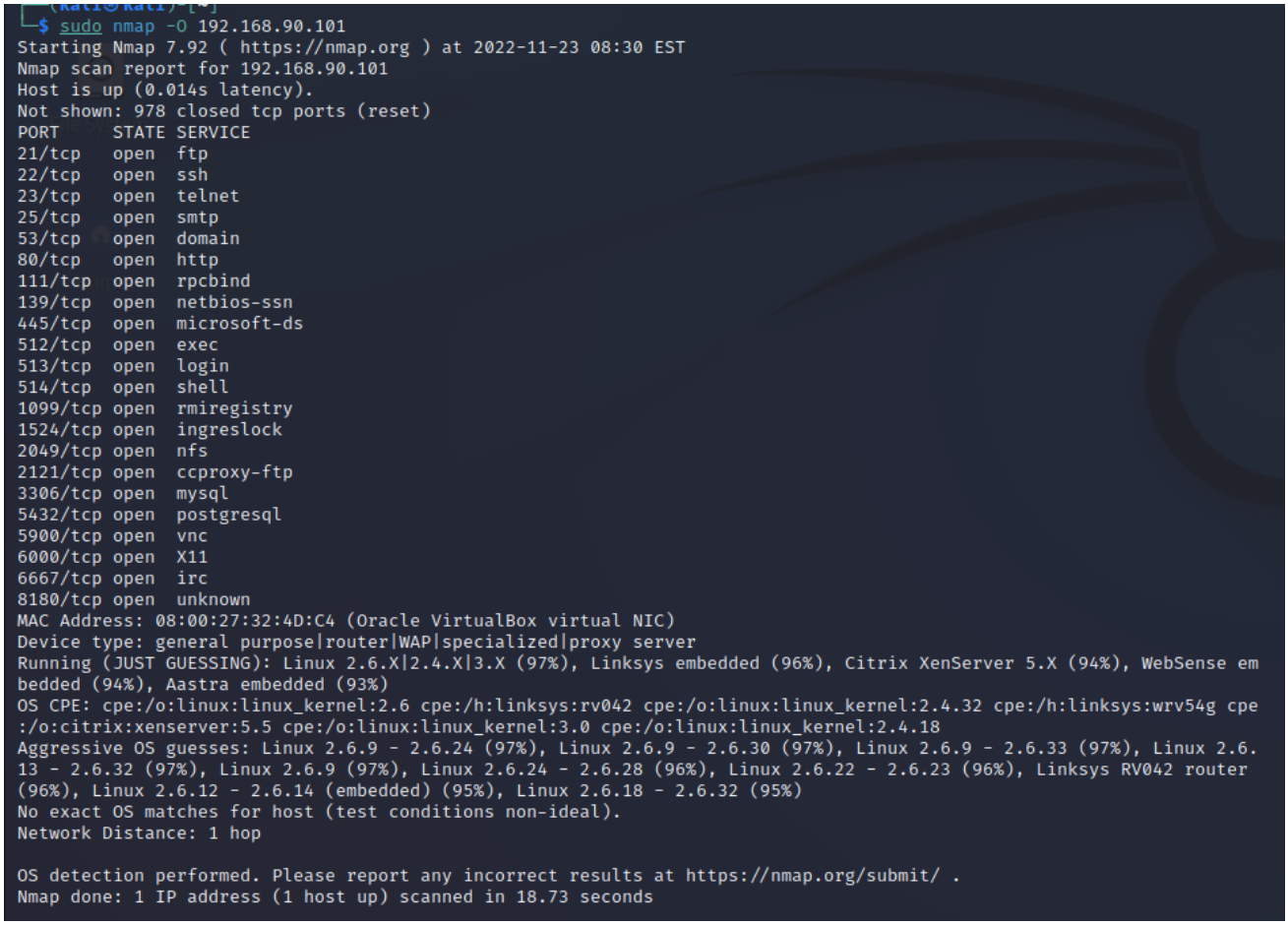
Scansione con nmap di Metasploitable e Windows 7

La Traccia di oggi di ci chiedeva di fare varie cose con lo strumento per scansioni **nmap** sia per Windows 7 e metasploitable:

1) **Metasploitable**:

- La prima richiesta per meta era quella di fare un **OS fingerprint** ,il comando per fare questo è: sudo nmap -O indirizzo ip

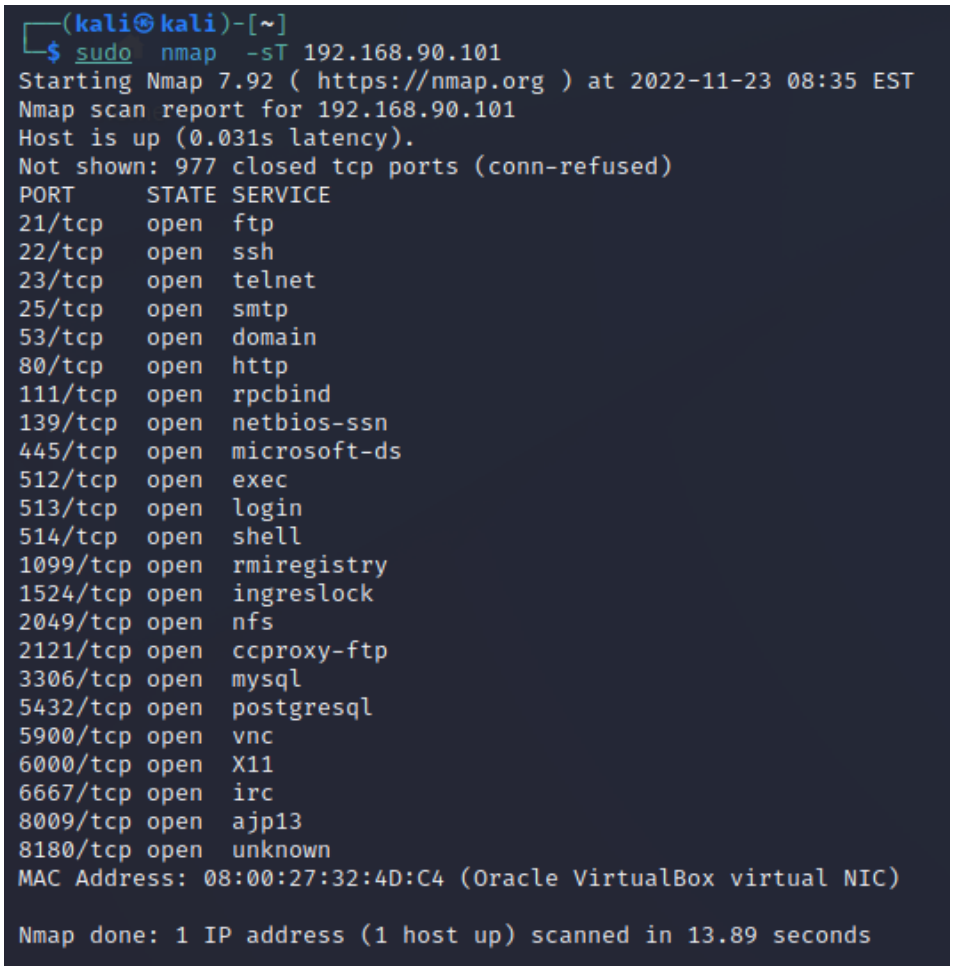


- La seconda richiesta era quella di svolgere una **SYN scan** una scansione molto meno invasiva in quanto una volta ricevuto il SYN dal server non crea un canale e chiude la
  connessione il comando è: sudo nmap **-sS** indirizzo IP**,** ci dira le porte aperte e i loro servizi.

```
└─$ sudo nmap -sS 192.168.90.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 08:32 EST
Nmap scan report for 192.168.90.101
Host is up (0.022s 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: 08:00:27:32:4D:C4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.92 seconds
```

- La terza richiesta era quella di fare una scansione **TCP connect** a differenza del SYN questa scansione è più invasiva in quanto una volta ricevuto il SYN invierà a sua volta l'ACK creando cosi una connessione col server, il comando è il seguente: sudo nmap **-sT** indirizzo IP. L' unica differenza che ho notato è che alla voce tcp ports c'è **conn-refused.**



- L’ultima richiesta della traccia era quella di eseguire una **Version Detection** una scansione ancora più invasiva in quanto aggiunge specifici test sulle porte per risalire al servizio e alla sua versione. Il comando è il seguente: sudo nmap **-sV** indirizzo ip.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.90.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 08:39 EST
Nmap scan report for 192.168.90.101
Host is up (0.021s latency).
Not shown: 977 closed tcp ports (conn-refused)
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?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
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?
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  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: 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 196.51 seconds
```

2) **Windows 7:**

La traccia ci chiedeva di svolgere l’OS fingerprint su Windows 7. Ma avendo questo il firewall attivo la scansione non avrà risultato positivo:

```
┌──(kali㉿kali)-[~]
└─$ sudo  nmap  -Pn -O 192.168.90.110
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 09:19 EST
Nmap scan report for 192.168.90.110
Host is up (0.0039s latency).
All 1000 scanned ports on 192.168.90.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:CC:25:90 (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 44.74 seconds
```

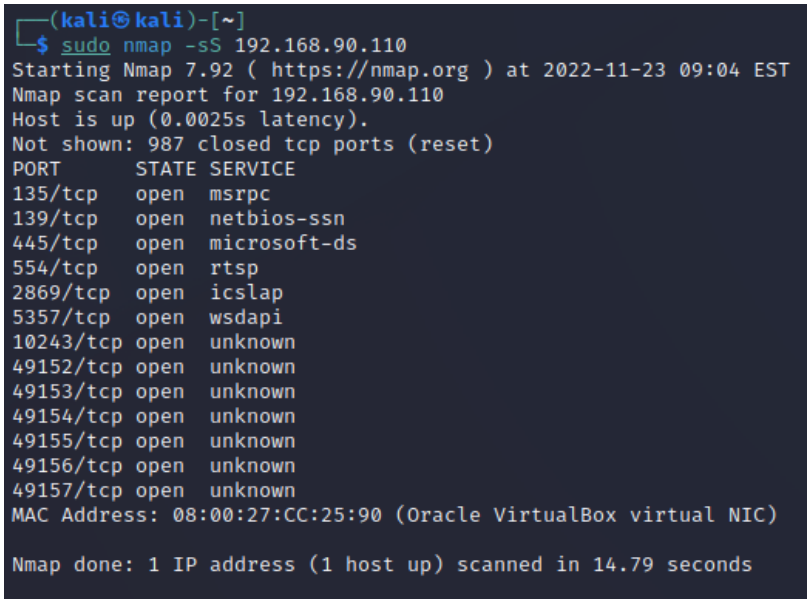
Come si vede la scansione non ha prodotto risultato positivo in quanto ci dice che l'host è attivo ma che le porte scansionate non inviato una risposta. Per ovviare a questo ci sono vari modi:

- Spegniamo il firewall di Windows.
- Aggiungiamo una regola al firewall permettendo così la comunicazione, per l'indirizzo IP di kali.
- Facendo una scansione con il timing impostato molto basso(es.T0,T1), questo dovrebbe ingannare il firewall in quanto e poco invasiva come soluzione ma anche molto lenta.

Qui ho riportato una serie di scansioni a Windows una volta applicata una delle soluzioni riportate sopra.

Os fingerprint:

SYN SCAN:



TCP connect:

```
┌──(kali㉿kali)-[~]
└─$ sudo  nmap  -sT 192.168.90.110
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 09:05 EST
Nmap scan report for 192.168.90.110
Host is up (0.0043s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
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:CC:25:90 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.58 seconds
```

Version detection:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T4 192.168.90.110
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 09:08 EST
Nmap scan report for 192.168.90.110
Host is up (0.0044s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: EMANUEL-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 141.79 seconds
```