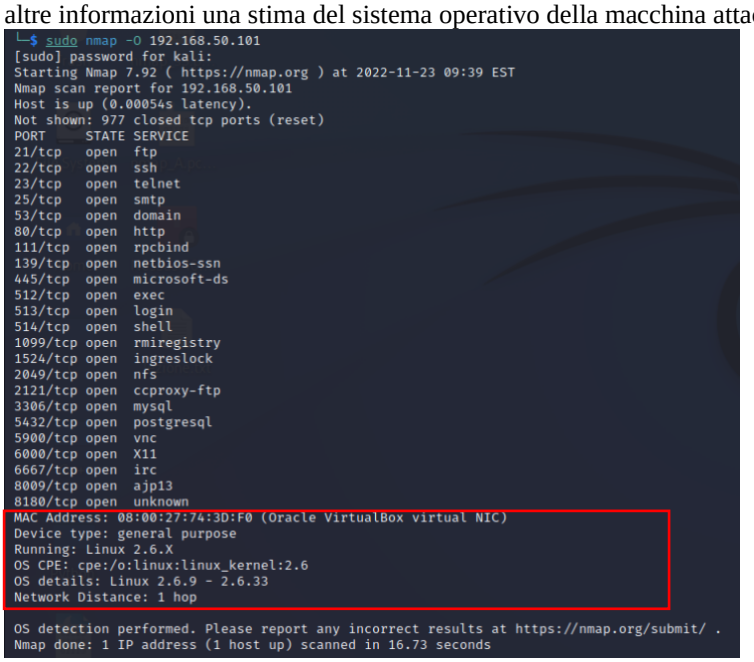
REPORT NMAP

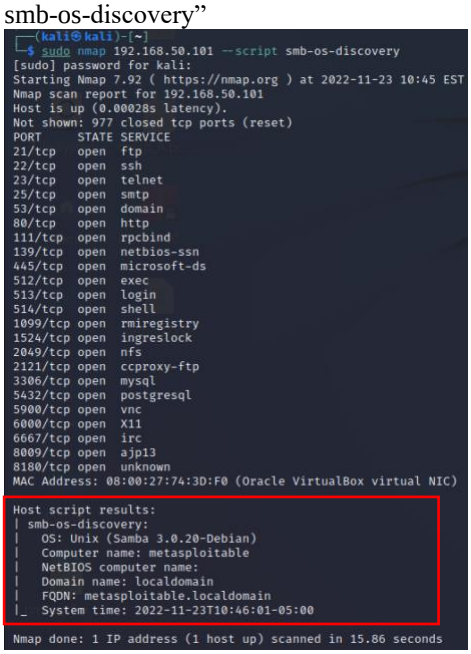
FRANCESCO PERSICHETTI

1) L'esercizio consiste nell'effettuare le seguenti scansioni con target **Metasploitable**:
   1. OS fingerprint
   2. Syn Scan
   3. TCP
   4. Version detection
2) E la seguente scansione con target **Windows 7**:
   1. OS fingerprint

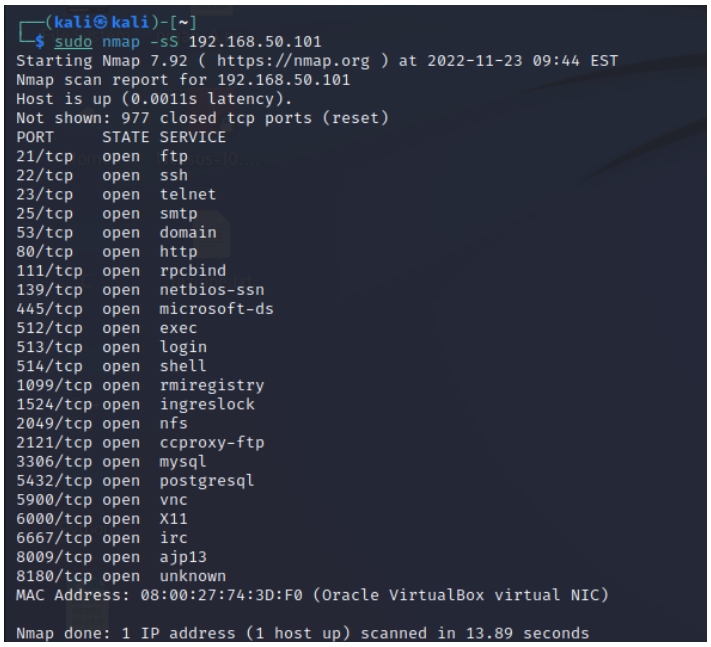
1.1
Impostiamo l'indirizzo IP della macchina Metasploitable (192.168.50.101) in modo da essere sulla stessa rete dell'indirizzo IP di kali. Dopodiché con il comando "nmap -O 192.168.50.101" si avvia la scansione che ci ridarà tra le altre informazioni una stima del sistema operativo della macchina attaccata



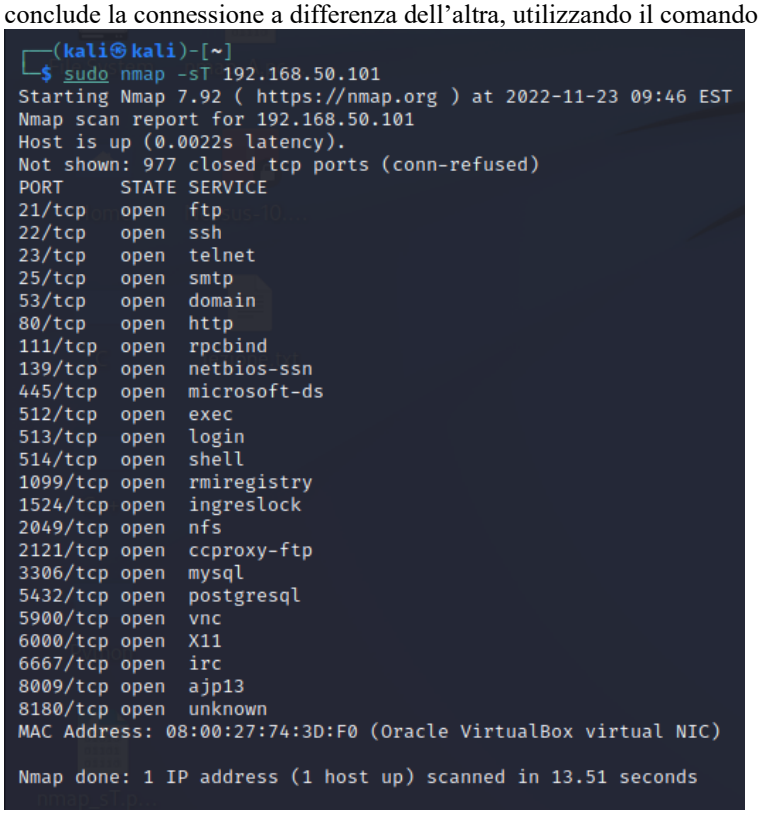
Se vogliamo essere più precisi sull'origine della macchina attaccata usiamo il comando "nmap 192.168.50.101 –script smb-os-discovery"



1.2
Per scansionare i servizi attivi sulle varie porte aperte senza essere troppo invadente usiamo il comando “nmap -sS 192.168.50.101”



1.3
Stessa operazione del punto sopra ma usando TCP che è una scansione più invadente rispetto alla SYN poiché la prima conclude la connessione a differenza dell’altra, utilizzando il comando “nmap -sT 192.168.50.101”



1.4
Infine, utilizziamo il comando “nmap -sV 192.168.50.101” per venire a conoscenza della versione dei servizi che vengono scannerizzati

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 09:47 EST
Nmap scan report for 192.168.50.101
Host is up (0.00053s 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  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:74:3D:F0 (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 67.74 seconds
```

2.1
Impostiamo l’indirizzo IP della macchina Windows 7 (192.168.50.102) in modo da essere sulla stessa rete dell’indirizzo IP di kali. Dopodiché con il comando “nmap -O 192.168.50.102” avviamo la scansione per farci ridare informazioni riguardante il sistema operativo della macchina attaccata, ma senza riuscirci dato che Windows ha il firewall attivo

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 09:17 EST
Nmap scan report for 192.168.50.102
Host is up (0.00064s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:7D:B5:0B (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 41.54 seconds
```

Per provare a farci ridare una risposta immediata abbiamo tolto il firewall e riprovando a fare lo stesso comando questa volta avremo una risposta più esaustiva

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 09:09 EST
Nmap scan report for 192.168.50.102
Host is up (0.0012s 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: 08:00:27:7D:B5:0B (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 17.76 seconds
```

Per evitare di spegnere il firewall e avere strada libera per ogni richiesta che noi andiamo a fare, un modo per poterlo aggirare potrebbe essere quello di aggiungere un timing alla nostra scansione per gestire appunto il tempo che passa da un invio di richiesta all'altro. Quelli più gettonati per poter bypassare le protezioni sono T0 e T1