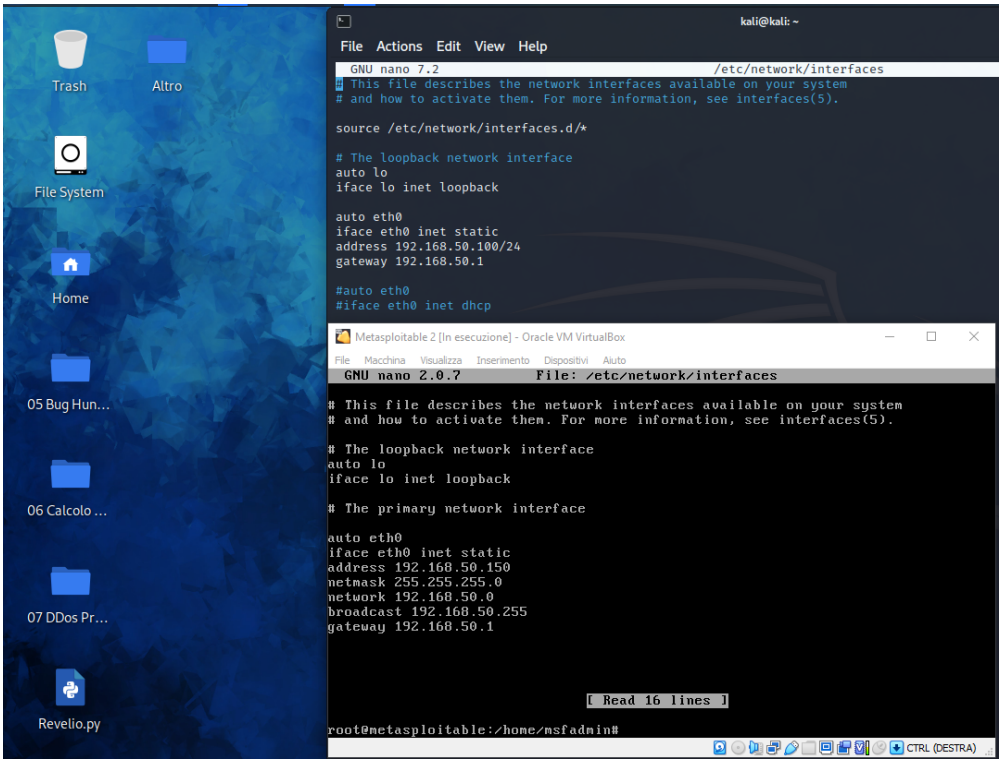
Scansione dei Servizi con Nmap

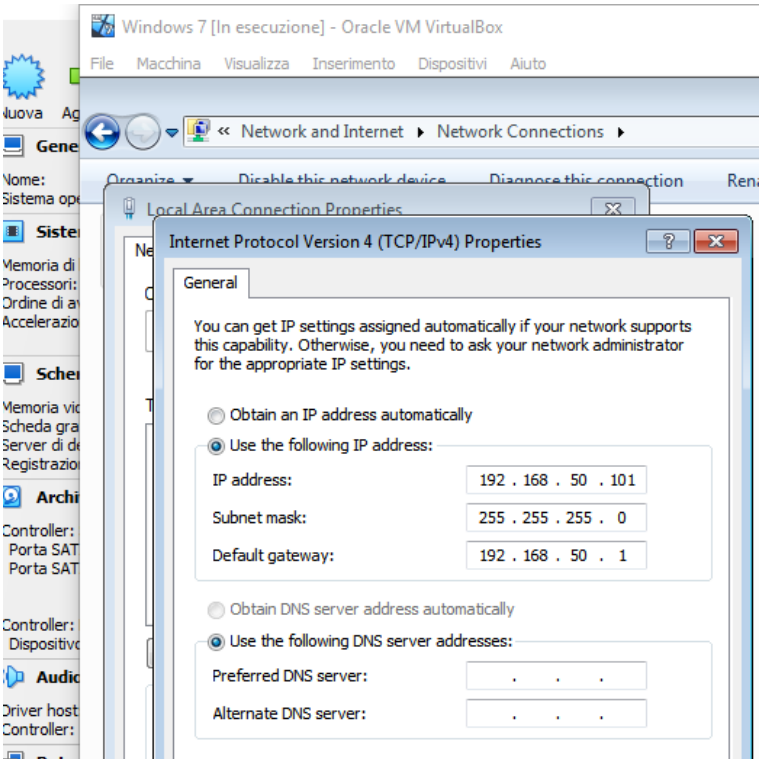
Obiettivo: Scansionare con Nmap da Kali Linux le seguenti macchine virtuali:

- **Metasploitable** - **IP** 192.168.50.150
- **Windows** 7 - **IP** 192.168.50.101

1) Configurazione Indirizzi IP

Per cominciare ho modificato gli indirizzi IP di Kali e delle due macchine da scansionare in modo che fossero sulla stessa rete.





2) Utilizzo del tool Nmap su Metasploitable

Da Kali Linux ho elevato i miei privilegi a quelli di root per semplificare l'esecuzione dei comandi. L'esercizio diceva di dover effettuare diverse scansioni sulla macchina Metasploitable tra le quali:

- *OS fingerprint* (usando il comando nmap **-O**)
- *Syn scan* (comando nmap **-sS**)
- *TCP scan* (comando nmap **-sT**)
- *Version Detection* (comando **-sV**)

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:21 EDT
Nmap scan report for 192.168.50.150
Host is up (0.00076s 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: 08:00:27:36:5C:81 (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 15.99 seconds
```

L'OS fingerprint in questo caso ci indica che il sistema operativo di Metasploitable è Linux.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:24 EDT
Nmap scan report for 192.168.50.150
Host is up (0.00012s 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: 08:00:27:36:5C:81 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kern
el

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.24 seconds
```

La scansione con -sV invece esegue il "banner grabbing", ovvero mostra i servizi attivi dell'host e la loro versione.

Tra le due scansioni **SYN** e **TCP** non c'è quasi nessuna differenza a meno che non si vogliano analizzare con il programma Wireshark. Le porte aperte sono le stesse che si possono vedere negli screen precedenti con la sola differenza che le *997 porte* chiuse, nella scansione con **-sS** la connessione viene resettata, mentre nella scansione con **-sT** viene rifiutata.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.50.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:21 EDT
Nmap scan report for 192.168.50.150
Host is up (0.00031s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:21 EDT
Nmap scan report for 192.168.50.150
Host is up (0.00020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
```

PS: Ho salvato in file separati ogni scansione effettuata per avere una documentazione leggibile anche in un secondo momento e li ho uniti in un unico report con il comando **cat**.

3) Scansione di Windows 7

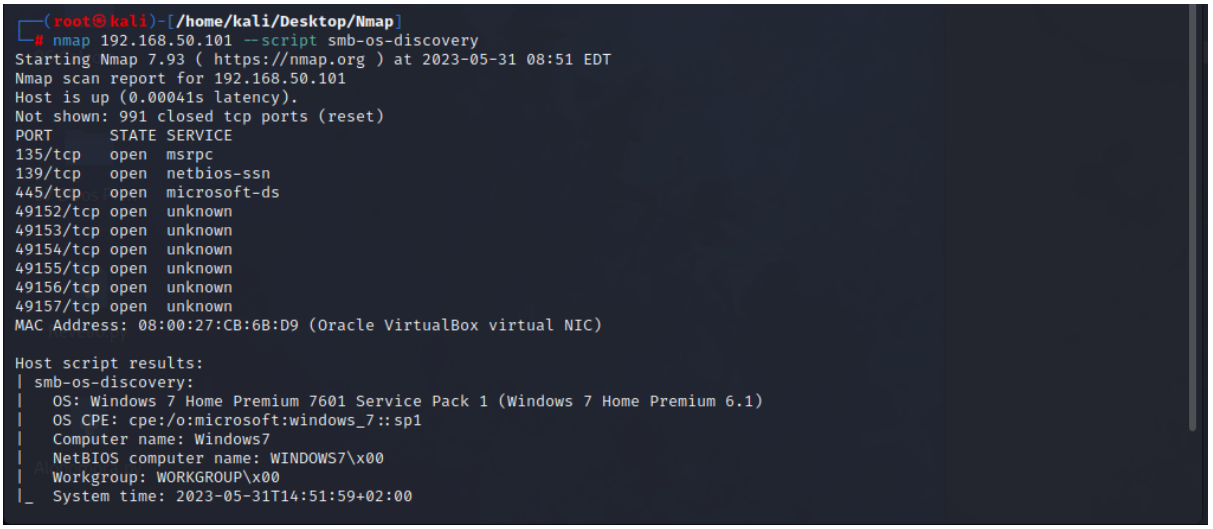
L'esercizio dettava inoltra di dover scansionare con Nmap una macchina virtuale con sopra Windows 7 per poter trovare il sistema operativo. In un primo momento utilizzando lo stesso comando con cui ho trovato l'OS di Metasploitable il risultato è stato particolare, ovvero mi indicava che il bersaglio avesse varie versioni di Windows (addirittura Phone o Vista).

```
root@kali: /home/kali/Desktop/Nmap
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/kali/Desktop/Nmap]
└─# nmap -O 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:50 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00032s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
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:CB:6B:D9 (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:micr
osoft: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 Updat
e 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 17.10 seconds
```

Per ovviare a questo problema ho utilizzato uno script di **Nmap** per poter verificare la versione precisa del Sistema Operativo del bersaglio (il codice è eseguito con privilegi di root)

nmap 192.168.50.101 –script smb-os-discovery



Come possiamo vedere alla fine della scansione **Nmap** ci indica che il bersaglio è una macchina con sopra **Sistema Operativo Windows 7 Home Premium Service Pack 1**.

PS: anche in questo caso ho salvato la scansione effettuata su un file di testo.