

TASK:

Eseguire le seguenti scansioni su Metasploitable:

- OS fingerprint
- Syn Scan
- TCP connect
- Version detection

E le seguenti su Windows 7:

- OS fingerprint

Ho cominciato l'esercitazione lanciando da kali il comando `fping -a -g 192.168.50.0/24` per trovare tutte le macchine attive sulla rete 192.168.50.*. Il risultato è stato il seguente:

```
kali@kali: ~  
(kali@kali)-[~]  
$ fping -a -g 192.168.50.0/24  
192.168.50.100  
192.168.50.111
```

Ho cominciato a scansionare l'IP 192.168.50.111. Ho lanciato per primo il comando `sudo nmap -O 192.168.50.11` per trovare il fingerprint del sistema operativo associato a quell'indirizzo IP:

```
(kali@kali)-[~]  
$ sudo nmap -O 192.168.90.111  
[sudo] password for kali:  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 08:15 EST  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.91 seconds
```

Non avendo avuto i risultati sperati ho lanciato lo stesso comando aggiungendo il `-Pn`:

```
(kali@kali)-[~]  
$ sudo nmap -Pn -O 192.168.50.111  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 08:18 EST  
Nmap scan report for 192.168.50.111  
Host is up (0.0011s 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: 08:00:27:78:DE:AF (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 16.10 seconds
```

Possiamo vedere nel riquadro rosso della foto qui a sinistra il sistema operativo della macchina associata all'IP che siamo andati a scansionare e quali sono le porte attive.

Sono quindi passato a fare il SYN scan, il cui risultato può vedersi nell'immagine qui sotto:

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.111
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 08:24 EST
Nmap scan report for 192.168.50.111
Host is up (0.00064s 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: 08:00:27:78:DE:AF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

Successivamente sono quindi andato a fare il TCP scan che mi ha restituito queste informazioni:

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.50.111
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 08:25 EST
Nmap scan report for 192.168.50.111
Host is up (0.0011s 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: 08:00:27:78:DE:AF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

La differenza che ho notato è che mentre nel SYN scan per le porte chiuse dice che ha concluso la comunicazione con il reset (sottolineato in verde), nella scansione TCP la connessione alle porte chiuse è stata rifiutata (sottolineato in giallo)

Infine sono passato a fare la Version scan, che mi ha restituito queste informazioni:

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.50.111
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 08:26 EST
Nmap scan report for 192.168.50.111
Host is up (0.00045s 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: 08:00:27:78:DE:AF (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 68.13 seconds
```

Possiamo vedere nel riquadro giallo le versioni dei servizi attivi su Metasploitable.

A questo punto ho cominciato la scansione dell'altra macchina con OS Windows 7. Sono andato per prima cosa a controllare le policy del firewall non permettendo alcuna comunicazione in entrata. Ho provato prima il comando “sudo nmap -O 192.168.50.101” e successivamente il comando “sudo nmap -Pn -O 192.168.50.101” ottenendo i risultati visibili nell'immagine qui sotto:

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 10:07 EST
Nmap scan report for 192.168.50.101
Host is up (0.00051s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:41:07:69 (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 40.01 seconds

(kali@kali)-[~]
$ sudo nmap -Pn -O 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 10:09 EST
Nmap scan report for 192.168.50.101
Host is up (0.00056s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:41:07:69 (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 41.58 seconds
```

cioè non sono riuscito a scoprire il sistema operativo della macchina con indirizzo IP 192.168.50.101.

Ho quindi provato a lanciare lo script suggerito nelle slide: `sudo nmap 192.168.50.101 --script smb-os-discovery` per vedere se fosse possibile scoprire l'OS tramite uno degli script di nmap ma come si può vedere dall'immagine neanche così ho avuto successo:


```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ sudo nmap 192.168.50.101 --script smb-os-discovery
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 10:13 EST
Nmap scan report for 192.168.50.101
Host is up (0.00039s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:41:07:69 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 39.37 seconds
```

Ho quindi provato a fare lo l'OS fingerprint a T1 senza ottenere le informazioni che stavamo cercando come dimostra l'immagini qui sotto:

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ sudo nmap -O -T1 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 11:48 EST
Nmap scan report for 192.168.50.101
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:41:07:69 (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/ .
```

Andando invece a modificare le policy firewall di Windows 7 invece possiamo vedere come le scansioni restituiscono tutti i risultati che la traccia richiede. Inizialmente la scansione di tutti gli OS della rete ha restituito queste informazioni da cui non si ha la certezza della versione del sistema operativo Windows:

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.50.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 09:02 EST
Nmap scan report for 192.168.50.101
Host is up (0.00094s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:41:07:69 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Phone 7.5
Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
```

Provando invece a lanciare lo script di nmap che ho utilizzato precedentemente invece abbiamo ottenuto l'informazione che cercavamo:

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ sudo nmap 192.168.50.101 --script smb-os-discovery
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 09:09 EST
Nmap scan report for 192.168.50.101
Host is up (0.00043s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdaapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 08:00:27:41:07:69 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: admin-PC
|   NetBIOS computer name: ADMIN-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-11-23T14:09:36-08:00
Nmap done: 1 IP address (1 host up) scanned in 26.89 seconds
```

L'unico modo che ho trovato per cui da kali si possano fare le scansioni di windows 7 è abbassare totalmente il firewall o comunque implementare delle policy che permettano la comunicazione tra le 2 macchine.