Report

Quest'oggi ho utilizzato nmap per scansionare la rete di metasploitable e windows 7.

Per quanto riguarda metasploitable ho utilizzato i comandi di OS Fingerprint, Syn Scan, Tcp connect e Version Detection. Riporto tutti i test:

```
└─# nmap -O 192.168.49.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:25 EST
Nmap scan report for 192.168.49.2
Host is up (0.00092s 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.49.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:26 EST
Nmap scan report for 192.168.49.2
Host is up (0.0026s 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

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.49.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:27 EST
Nmap scan report for 192.168.49.2
Host is up (0.0038s 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

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.49.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:28 EST
Nmap scan report for 192.168.49.2
Host is up (0.0038s 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  ccproxy-ftp?
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
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 172.73 seconds
```

Abbiamo una differenza sostanziale tra TCP connect e SYN che non salta all'occhio con facilità: il TCP non fa il reset lasciando le nostre tracce e inoltre fa piu "rumore" per un firewall. Il SYN, al contrario, resetta e fa meno rumore.

Per quanto riguarda Windows 7 ho provato a utilizzare nmap sia lasciando attivo il suo firewall, sia disattivandolo. Il risultato è stato positivo perchè ho trovato una porta aperta nonostante il firewall:

```
┌──(kali㉿kali)-[~]
└─$ nmap -T5 -Pn -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:14 EST
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: 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 40.73 seconds
```

Questo mi darebbe la possibilità di mettermi in ascolto su quella porta e utilizzarla per l'ingresso, quindi possiamo considerarla una grossa vulnerabilità. Per continuare la scansione proporrei l'utilizzo di "-T1" cosi da fare meno rumore per il firewall (essendo in modalità stealth) e permetterci di individuare piu porte aperte, oppure proporrei di fare una scansione del firewall cosi da vedere cosa e chi puo far passare e magari modificare l'indirizzo IP fingendoci qualcuno che non siamo in modo da superare il firewall.

Disattivando il firewall queste sono le porte che ho trovato aperte utilizzando i comandi "-Pn, -sV e -O" :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O --osscan-guess 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:06 EST
Nmap scan report for 192.168.50.101
Host is up (0.00045s 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
49158/tcp open  unknown
MAC Address: 08:00:27:33:53:F5 (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 2.71 seconds
```