Tecniche scansione Nmap

Richiesta OS fingerprint, target Windows 7.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 10:29 EST
Nmap scan report for 192.168.50.7
Host is up (0.00088s latency).
Not shown: 996 filtered tcp ports (no-response)
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 (workgrou
p: WORKGROUP)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:F4:5F:74 (Oracle VirtualBox virtual NIC)
Service Info: Host: CRIS-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 37.67 seconds
```

Attraverso il comando “nmap -sV <<ip host>> ottengo le seguenti informazioni:
-Si tratta di windows, il range della versione varia dal 7 al 10 (porta 445 mi da queste informazioni)
-Nome host: CRIS-PC

```
root@kali: /home/kali
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sT -T4 -O 192.168.50.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 11:05 EST
Nmap scan report for 192.168.50.7
Host is up (0.0014s latency).
Not shown: 996 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  wsdapi
MAC Address: 08:00:27:F4:5F:74 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at leas
t 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (98%), Microsoft
Windows Embedded Standard 7 (98%), Microsoft Windows 7 Professional or Wind
ows 8 (97%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, o
r Windows 7 (97%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows S
erver 2008 (96%), Microsoft Windows Server 2008 R2 or Windows 8.1 (95%), Mi
crosoft Windows 7 (94%), Microsoft Windows Server 2008 SP1 (93%), Microsoft
 Windows 8.1 R1 (92%), Microsoft Windows 7 SP1 (92%)
No exact OS matches for host (test conditions non-ideal).
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 23.60 seconds
```

Utilizzando il comando “nmap -Pn -sT -T4 -0 <<ip host>>” riesco a capire attraverso le probabiltà che si tratta di windows 7, anche aiutandomi con la ricorrenza delle ipotesi della versione 7, e dei server riconducibili al 2008.

Metasploitable

Informazioni: OS fingerprint, Syn scan, tcp connect, version detection.

OS fingerprint

```
MAC Address: 08:00:27:EF:A8:F1 (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
```

Attraverso il comando “nmap -O <<ip host>>” riesco ad avere questi risultati:
Il sistema operativo, il suo range di versione., la versione del kernel.

Syn scan

```
root@kali: /home/kali
File  Actions  Edit  View  Help
Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -p 1-1024 192.168.50.6
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 11:36 EST
Nmap scan report for 192.168.50.6
Host is up (0.00013s latency).
Not shown: 1012 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
MAC Address: 08:00:27:EF:A8:F1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.67 seconds
```

Qui effettuiamo uno scan sulle prime 1024 porte utilizzando solamente la prima stretta di mano (syn).

TCP scan

```
root@kali: /home/kali
File  Actions  Edit  View  Help

Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sT -p 1-1024 192.168.50.6
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 13:23 EST
Nmap scan report for 192.168.50.6
Host is up (0.0019s latency).
Not shown: 1012 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
MAC Address: 08:00:27:EF:A8:F1 (Oracle VirtualBox virtual NIC)

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

Qui invece effettuiamo una scansione che stabilisce una connessione TCP con ciascuna delle porte in range.
A differenza della scansione precedente esegue una scansione più completa, utilizza un metodo più invasivo e di conseguenza maggiormente rintracciabile.

Version Detection

```
root@kali: /home/kali
File  Actions  Edit  View  Help
Nmap done: 1 IP address (1 host up) scanned in 26.90 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p 1-1024 192.168.50.6
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 14:01 EST
Nmap scan report for 192.168.50.6
Host is up (0.00049s latency).
Not shown: 1012 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       OpenBSD or Solaris rlogind
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:EF:A8:F1 (Oracle VirtualBox virtual NIC)
Service Info: Host:  metasploitable.localdomain; 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 24.80 seconds
```

Con questo comando otteniamo una scansione più dettagliata delle porte, riuscendo a visualizzare anche la versione di esse.