

Pratica S5L2

Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target **Metasploitable**:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

Configuriamo la metasploitable2 con IP statico “192.168.50.101”

```
Metasploitable2 1 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:71:2f:a3
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe71:2fa3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:424783 errors:0 dropped:0 overruns:0 frame:0
          TX packets:370861 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29278392 (27.9 MB)  TX bytes:44805544 (42.7 MB)
          Base address:0x4020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1863 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1863 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:859049 (838.9 KB)  TX bytes:859049 (838.9 KB)

msfadmin@metasploitable:~$
```

OS fingerprint lo troviamo con il comando “nmap -O 192.168.50.101”

```
(kali㉿kali)-[~]
$ nmap -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:20 CET
Nmap scan report for 192.168.50.101
Host is up (0.00069s 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: 08:00:27:71:2F:A3 (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 1.61 seconds
```

Il SynScan viene effettuato con il comando “nmap -sS 192.168.50.101”

```
(kali@kali)-[~]
$ nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:23 CET
Nmap scan report for 192.168.50.101
Host is up (0.0046s 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: 08:00:27:71:2F:A3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Lo scan TCP viene eseguito con “nmap -sT 192.168.50.101”

```
(kali@kali)-[~]
$ nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:23 CET
Nmap scan report for 192.168.50.101
Host is up (0.0039s 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: 08:00:27:71:2F:A3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

A livello visivo le due scansioni risultano uguali, cambia il modo di operare, mentre lo scan TPC stabilisce una connessione piena scambiando l'intero pacchetto dati, lo scan Syn non completa il 3-way-handshake non restituendo l'ultimo ACK ma restituisce un pacchetto RST per chiudere la comunicazione, questo gli permette di recuperare informazioni sullo stato della porta creando meno rumore all'interno della rete.

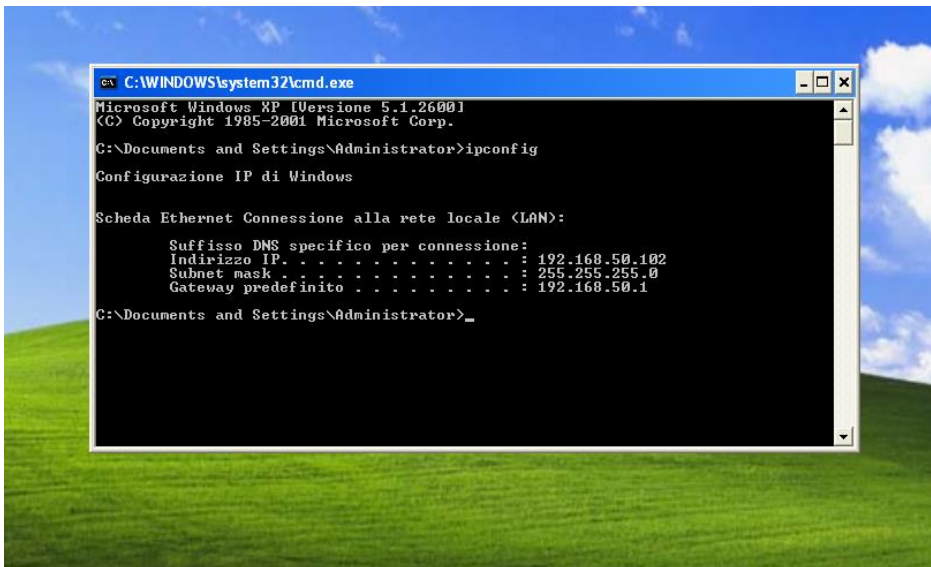
La version detection si effettua con il comando “nmap -sV 192.168.50.101”

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:24 CET
Nmap scan report for 192.168.50.101
Host is up (0.00033s 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 rshd
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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: 08:00:27:71:2F:A3 (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 11.64 seconds
```

Restituisce uno scan delle porte con le versioni dei software in uso sulle rispettive porte

Configuriamo WinXP con un IP statico “192.168.50.102”



Usiamo il comando “nmap -O 192.168.50.102” per verificare la versione

```
(kali@kali)~$ nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:22 CET
Nmap scan report for 192.168.50.102
Host is up (0.0013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (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|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2008|2000 (97%), General Dynamics embedded (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_2000::sp4
Aggressive OS guesses: Microsoft Windows XP SP3 (97%), Microsoft Windows Server 2003 SP1 or SP2 (95%), Microsoft Windows Server 2008 Enterprise SP2 (95%), Microsoft Windows Server 2003 SP2 (94%), Microsoft Windows XP SP2 or Windows Server 2003 (93%), Microsoft Windows XP SP2 or SP3 (93%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (92%), Microsoft Windows XP SP2 (91%)
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 8.73 seconds
```