

## Traccia

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

- OS fingerprint.
- SYN scan.
- TCP connect.
- Version detection.

E la seguente sul target Windows 7:

- OS fingerprint.

A valle delle scansioni è prevista la produzione di un report contenente le seguenti info:

- IP.
- Sistema operativo.
- Porte aperte.
- Servizi in ascolto con versione.

Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

## Svolgimento

Scansione di Metasploitable:

- OS fingerprint: comando 'nmap -O 192.168.40.101', il risultato è il seguente.

```
(root@francesco)-[/usr/share/nmap/scripts]
# nmap -O 192.168.40.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 14:06 CET
Nmap scan report for 192.168.40.101
Host is up (0.015s 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    filtered http
111/tcp   open  rpcbind
139/tcp   open  smb
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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.25 seconds
```

Con lo switch '-O' si può rilevare il sistema operativo e la versione dello stesso, del target che si sta scansionando. Come è evidenziato in figura, il sistema operativo target è Linux, versione che può essere dalla 2.6.15 alla 2.6.26.

- SYN scan: comando 'nmap -sS 192.168.40.101', il risultato è il seguente.

```
(root@francesco)-[/usr/share/nmap/scripts]
# nmap -sS 192.168.40.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:30 CET
Nmap scan report for 192.168.40.101 255.255.255.0 broadcast 192.
Host is up (0.039s latency). 192.168.40.101:4522 prefixlen 64 scopeid 0x20
Not shown: 977 closed tcp ports (reset) len 1000 (Ethernet)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain RUNNING> mtu 65536
80/tcp    filtered http netmask 255.0.0.0
111/tcp   open  rpcbind len 128 scopeid 0x10<host>
139/tcp   open  smb netbios-ssn (Local Loopback)
445/tcp   open  microsoft-ds (240.0 B)
512/tcp   open  exec dropped 0 overruns 0 frame 0
513/tcp   open  login bytes 240 (240.0 B)
514/tcp   open  shell dropped 0 overruns 0 carrier 0 collisions 0
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 1.81 seconds
```

Con lo switch '-sS', la connessione alla porta si ferma alla fase 'SYN' del three-way handshake. Nei log non sarà scritto che l'IP:porta della nostra macchina si è connesso con l'IP:porta del target. Inoltre, questo tipo di scansione genera un traffico di rete basso, quindi più difficile da individuare da un dispositivo IDS/IPS.

- TCP connect: comando 'nmap -sT 192.168.40.101', il risultato è il seguente.

```
(root@francesco)-[/usr/share/nmap/scripts]# nmap -sT 192.168.40.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:37 CET
Nmap scan report for 192.168.40.101
Host is up (0.041s 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    filtered 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 1.70 seconds
```

Con lo switch '-sT', la connessione alla porta esegue tutte le fasi del three-way handshake. Nei log sarà scritto che l'IP:porta della nostra macchina si è connesso con l'IP:porta del target.

Il risultato delle scansioni con gli switch 'sS' e 'sT', in questo caso, è sempre lo stesso.

- Version detection: comando 'nmap -sV 192.168.40.101', il risultato è il seguente.

```
(root@francesco)-[/usr/share/nmap/scripts]
# nmap -sV 192.168.40.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:37 CET
Nmap scan report for 192.168.40.101
Host is up (0.048s 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    filtered http
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  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
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 13.51 seconds
```

Con lo switch '-sV', si rileva anche la versione del protocollo attivo su una determinata porta. Si può poi andare a controllare la versione di un protocollo, in cerca di vulnerabilità note da poter sfruttare per ulteriori test.

#### Scansione di Windows 7:

- OS fingerprint: il risultato è il seguente.

```
(root@francesco)-[/usr/share/nmap/scripts]
# nmap -O 192.168.40.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 16:30 CET
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 3.44 seconds
```

Questo succede perché il firewall di Windows blocca le richieste di ping. Come suggerito da nmap, si può eseguire una scansione con lo switch '-Pn', che scandisce il target ignorando il ping. Il risultato è il seguente.

```
(root@francesco)-[/usr/share/nmap/scripts]
# nmap -Pn 192.168.40.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 16:30 CET
Nmap scan report for 192.168.40.102
Host is up.
All 1000 scanned ports on 192.168.40.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 206.37 seconds
```

Come si può vedere, nonostante la scansione sia stata eseguita ignorando il ping, non viene restituito nessun risultato utile, questo sempre perché il firewall blocca ogni richiesta.

Per continuare la scansione si può utilizzare lo switch '-Tn', dove n è un numero da 0 a 5, che indica il livello di 'intensità' con cui viene eseguita la scansione. Più n è basso, minore è la probabilità che la scansione venga bloccata dal firewall. Questa operazione è molto lenta.