

S5L3

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 7:

- OS fingerprint.

OS fingerprinting: È un processo utilizzato per conoscere il sistema operativo in esecuzione su un host di destinazione sulla base delle caratteristiche delle risposte ricevute durante una scansione di rete.

```
└─$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 04:04 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00078s 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

OS detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds
```

L'OS fingerprinting può essere utile per scopi di sicurezza, ad esempio per individuare dispositivi non autorizzati sulla rete, o per scopi di amministrazione di rete, ad esempio per

tenere traccia dei sistemi operativi utilizzati all'interno di una rete aziendale. Tuttavia, è importante notare che alcuni sistemi possono essere configurati per mascherare la loro identità, rendendo più difficile l'OS fingerprinting.

SYN scan e TCP connect:

```
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 03:44 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00066s 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 0.22 seconds
```

```
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 03:48 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0013s 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 0.30 seconds
```

La differenza principale tra una scansione TCP Connect e una scansione SYN (Syn Scan) riguarda il modo in cui viene stabilita la connessione con le porte di destinazione.

Scansione TCP Connect:

In una scansione TCP Connect, Nmap tenta di stabilire una connessione TCP completa con l'host di destinazione sulla porta specificata.

Questo tipo di scansione richiede l'apertura di una connessione completa per determinare lo stato della porta (aperta, chiusa o filtrata).

È più silenziosa rispetto alla scansione SYN perché completa il handshake TCP.

Scansione SYN (Syn Scan):

In una scansione SYN, Nmap invia pacchetti SYN al host di destinazione senza completare il handshake TCP.

Se il porto è aperto, l'host di destinazione risponderà con un pacchetto SYN-ACK.

Se il porto è chiuso, l'host di destinazione risponderà con un pacchetto RST (reset).

Se il porto è filtrato, non viene ricevuta alcuna risposta.

La scansione SYN è più veloce e discreta poiché non completa la connessione TCP.

In breve, la scansione TCP Connect è più accurata ma meno discreta e più lenta rispetto alla scansione SYN, che è più veloce e discreta ma può essere meno accurata in determinate situazioni di filtraggio del firewall.

Version detection: È utile per comprendere meglio il panorama dei servizi in esecuzione su un host di destinazione e per individuare potenziali vulnerabilità legate a versioni obsolete o note di software.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 03:57 EDT
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 03:59 (0:00:07 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (conn-refused)
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?
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/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 174.93 seconds
```

OS fingerprint su Windows:

Protezione contro la scansione: Alcuni sistemi possono essere configurati per rilevare e bloccare attivamente le scansioni di rete, rendendo difficile per Nmap ottenere una risposta.

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 04:34 EDT
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 3.13 seconds
```

Se facciamo una fingerprint su Windows con il firewall attivo ci bloccherà senza poter fare la scansione.

Ma come nell'esempio avendo fatta una scansione è possibile visionare in questi casi con il block disattivato. Ulteriormente si può fare anche un fingerprint parallelo, implementando così anche il comando -T, che varierà dalla potenza minima, ovvero, 0 alla massima, cioè, 5. Oppure un'altra tecnica di evasione del blocco IPS/IDS può essere quella di puntare alla porta sorgente, e attaccheremo la porta 80/443 dato che generalmente non bloccano i pacchetti provenienti da porte http/https.

```
└─$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 04:30 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00074s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
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 2.86 seconds
```