

SCANSIONE DEI SERVIZI CON NMAP

ENUMERAZIONE SERVIZI E SCANSIONE (2)

TRACCIA: Tecniche di scansione con Nmap

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

- OS fingerprint
- Syn Scan
- TCP connect
- Version detection

OS FINGERPRINT

```
$ sudo nmap -O «ip address»
```

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-24 17:37 CEST
Nmap scan report for 192.168.50.103
Host is up (0.0039s latency).
Not shown: 977 filtered tcp ports (no-response)
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (91%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (91%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.70 seconds
```

```
$ sudo nmap -PN -O «ip address»
```

```
(kali㉿kali)-[~]
$ sudo nmap -PN -O 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-24 17:38 CEST
Nmap scan report for 192.168.50.103
Host is up (0.0060s latency).
Not shown: 977 filtered tcp ports (no-response)
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (92%), Bay Networks embedded (85%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (92%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.52 seconds
```

SYN SCAN

```
$ sudo nmap -sS «ip address»
```

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-24 17:39 CEST
Nmap scan report for 192.168.50.103
Host is up (0.0040s latency).
Not shown: 977 filtered tcp ports (no-response)
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 4.61 seconds
```

TCP CONNECT

```
$ sudo nmap -sT -p 1-53,100 <192.168.*.10>
```

Gli ip 192.168.x.10, dove x assume tutti i risultati ammessi [0;255]
con lo switch -p, nmap effettuerà la scansione sulle porte [1;53] e sulla porta 100.

```
(kali㉿kali)-[~]  
$ nmap -sT -p 1-53, 100 192.168.*.10  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-24 17:43 CEST  
Nmap done: 257 IP addresses (0 hosts up) scanned in 7.87 seconds
```

VERSION DETECTION

```
$ sudo nmap -sV <ip address>
```

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.50.103  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-24 17:41 CEST  
Nmap scan report for 192.168.50.103  
Host is up (0.024s latency).  
Not shown: 977 filtered tcp ports (no-response)  
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  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 17.02 seconds
```

REPORT

OS fingerprint = L'utilizzo del flag -O sul comando Nmap rivelerà ulteriori informazioni sul sistema operativo degli host mappati.

SYN scan = (-sS) Questo è di gran lunga il tipo di scansione più popolare perché è il modo più veloce per scansionare le porte del protocollo più popolare (TCP). È più furtivo della scansione connect e funziona contro tutti gli stack TCP funzionali (a differenza di alcune scansioni speciali come la scansione FIN).

TCP connect = (-sT) Connect Scan utilizza la chiamata di sistema con lo stesso nome per eseguire la scansione delle macchine, anziché fare affidamento su pacchetti non elaborati come fa la maggior parte degli altri metodi.

Version Detection = a volte, potrebbe essere necessario rilevare informazioni sul servizio e sulla versione da porte aperte. Ciò è utile per la risoluzione dei problemi, la scansione delle vulnerabilità o l'individuazione dei servizi che devono essere aggiornati.