

EPICODE S5-L3

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.

To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>

No mail.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:ec:b7:92
          inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feec:b792/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1867 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1145 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:120378 (117.5 KB) TX bytes:65985 (64.4 KB)
          Base address:0xd020 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:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:37101 (36.2 KB) TX bytes:37101 (36.2 KB)
```

(kali㉿kali)-[~]

Attraverso il comando **-O andiamo ad analizzare il sistema operativo dell'indirizzo IP target (in questo caso Metasploitable) e come si può vedere otteniamo una risposta corretta, l'OS della macchina target è Linux 2.6**

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 06:37 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0016s 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:EC:B7:92 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
```

```
(kali㉿kali)-[~]
$
```

```
(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 06:39 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0059s 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:EC:B7:92 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds
```

```
(kali㉿kali)-[~]
$
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:ec:b7:92
          inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feec:b792/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1867 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1145 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:120378 (117.5 KB) TX bytes:65985 (64.4 KB)
          Base address:0xd020 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:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:37101 (36.2 KB) TX bytes:37101 (36.2 KB)
```

```
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:155 errors:0 dropped:0 overruns:0 frame:0
TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:37101 (36.2 KB) TX bytes:37101 (36.2 KB)
```

```
Link encap:Ethernet HWaddr 08:00:27:ec:b7:92
inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:feec:b792/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1867 errors:0 dropped:0 overruns:0 frame:0
TX packets:1145 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:120378 (117.5 KB) TX bytes:65985 (64.4 KB)
Base address:0xd020 Memory:f0200000-f0220000
```

```
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:155 errors:0 dropped:0 overruns:0 frame:0
TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:37101 (36.2 KB) TX bytes:37101 (36.2 KB)
```

Se il comando *-sS* svolge una scansione attraverso l'invio di un pacchetto SYN di sincronizzazione (primo step di una three way handshake), il comando *-sT* effettua una connessione TCP completa, impiegando più tempo ma di solito ottenendo risultati più accurati.

Come è possibile vedere i comandi *-sS* e *-sT* producono lo stesso risultato. Questo avviene perché anche con l'invio del solo pacchetto SYN iniziale, senza quindi una 3WH completa otteniamo tutte le informazioni necessarie, e nel nostro caso non dobbiamo preoccuparci di congestionare reti o di eventuali sistemi di monitoraggio.

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Trash

kali@kali: ~

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 06:46 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0012s 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?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
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
MAC Address: 08:00:27:EC:B7:92 (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 193.97 seconds
```

(kali㉿kali)-[~]

msfadmin@metasploitable:~\$ ifconfig

eth0 Link encap:Ethernet HWaddr 08:00:27:ec:b7:92
inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:feec:b792/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:1867 errors:0 dropped:0 overruns:0 frame:0
 TX packets:1145 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:120378 (117.5 KB) TX bytes:65985 (64.4 KB)
 Base address:0xd020 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:155 errors:0 dropped:0 overruns:0 frame:0
 TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
 RX bytes:37101 (36.2 KB) TX bytes:37101 (36.2 KB)

Con il comando `-sV` andiamo ad eseguire una scansione della versione dei servizi attivi sulle porte aperte

```
-sS/S/T/SW/SM/ TCP SYN/Connect() /ACK/Window/Maimon scans
[kali㉿kali]-[~]
$ sudo nmap -O 192.168.50.102 Xmas scans
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 12:58 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:2E:06:6A (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop; --p 0:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>; Exclude the specified ports from scanning
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.17 seconds
--top-ports <number>; Scan <number> most common ports
[kali㉿kali]-[~] 1o>; Scan ports more common than <ratio>
$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 13:01 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00043s latency).  
st likely probes (intensity 2)
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response).ivity (for debugging)
MAC Address: 08:00:27:2E:06:6A (Oracle VirtualBox virtual NIC)
--sC; equivalent to --script=default
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.88 seconds
--script-args=script=vl [c2=v2 -l]; provide arguments to scripts
```

Dalla figura a sinistra possiamo notare che i due comandi nmap verso la macchina windows ottengono risultati incompleti, questo potrebbe essere causato dal firewall attivo sulla macchina

Con l'utilizzo del timing Template **T 1**, eseguiamo una scansione molto più discreta in modo da eludere il firewall e poter ottenere comunque informazioni riguardo la macchina target.

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 12:49 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00040s latency).

Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:2E:06:6A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:: - cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
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 33.32 seconds
```

Possiamo notare che avendo disattivato il firewall sulla macchina windows, riusciamo ad utilizzare liberamente i comandi di nmap e riceviamo le informazioni di cui abbiamo bisogno per un possibile attacco

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 12:52 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00047s latency).

Not shown: 990 closed tcp ports (reset)
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 (workgroup: WORKGROUP)
5357/tcp   open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc       Microsoft Windows RPC
49153/tcp  open  msrpc       Microsoft Windows RPC
49154/tcp  open  msrpc       Microsoft Windows RPC
49155/tcp  open  msrpc       Microsoft Windows RPC
49156/tcp  open  msrpc       Microsoft Windows RPC
49157/tcp  open  msrpc       Microsoft Windows RPC
MAC Address: 08:00:27:2E:06:6A (Oracle VirtualBox virtual NIC)
Service Info: Host: MZ-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 73.75 seconds
```

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 12:51 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00028s latency).

Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:2E:06:6A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.71 seconds
```

REALIZZATO DA

MICHAEL ANDREOLI
MICHAEL ANDREOLI

OTMAN HMICH
OTMAN HMICH

STEFANO CESARONI
STEFANO CESARONI