
S5 - L2

Scansione dei servizi

Emanuele Benedetti | 8 gennaio 2025

Consegna

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

Svolgimento

Ho eseguito l'esercizio tramite l'utilizzo di macchine virtuali, configurate in VirtualBox. In particolare ho utilizzato una macchina Kali Linux per eseguire le scansioni e due macchine target, la prima Metasploitable2 e la seconda Windows 7. Come mostrato dalle immagini che seguono, le macchine sono configurate in "rete interna", su due network diverse e comunicano tramite una terza macchina virtuale pfSense.

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:6d:4b:19 brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.2/29 brd 192.168.20.7 scope global eth0
    inet6 fe80::a00:27ff:fe6d:4b19/64 scope link
        valid_lft forever preferred_lft forever
```

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:0a:c2:32 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.2/27 brd 192.168.10.31 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe0a:c232/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
```

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet0         -> v4: 192.168.10.1/27
LAN2 (opt1)    -> vtnet1         -> v4: 192.168.20.1/29
```

Per prima cosa ho eseguito un ping sweep per verificare quali dispositivi fossero connessi alla rete target. Tramite il comando **fping -a -g 192.168.20.0/29** ho ottenuto tutta la lista dei dispositivi connessi nella rete di interesse e sono solamente il gateway pfSense e la macchina Metasploitable2 target.

Lo switch **-a** del comando permette di elencare gli host attivi, mentre **-g** è usato per specificare il range di indirizzi da scansionare. In questo caso, tramite la notazione CIDR, eseguiamo una scansione nella rete 192.168.20.0/29.

```
(kali㉿kali)-[~]
$ fping -a -g 192.168.20.0/29
192.168.20.1
192.168.20.2
```

OS fingerprint

Come da prima richiesta, ho usato Nmap per ottenere il fingerprint del sistema operativo target, tramite il comando **nmap -O 192.168.20.2**

```
(kali㉿kali)-[~]  
$ nmap -O 192.168.20.2  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 12:31 CET  
Nmap scan report for 192.168.20.2  
Host is up (0.0039s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
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), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)  
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 3.14 seconds
```

Dopo pochi secondi il programma ha individuato il sistema operativo della macchina all'indirizzo specificato, in questo caso nmap ci fornisce l'informazione che Metasploitable gira su Linux 2.6 e più di preciso tra le versioni 2.6.15 e 2.6.26.

SYN scan

Tramite il comando **nmap -sS 192.168.20.2** ho effettuato una scansione TCP SYN scan che non stabilisce una connessione TCP completa, ma dopo aver ricevuto il pacchetto SYN/ACK, invia un pacchetto RST per terminare la connessione.

L'immagine che segue mostra il risultato della scansione TCP SYN scan evidenziando tutte le porte aperte sulla macchina target:

```
(kali㉿kali)-[~]
$ nmap -sS 192.168.20.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 12:35 CET
Nmap scan report for 192.168.20.2
Host is up (0.042s 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 0.72 seconds
```

TCP Connect Scan

La TCP connect scan è una scansione che mostra le porte aperte ma a differenza della scansione precedente, stabilisce una connessione TCP completa con ciascuna porta del target.

Ho utilizzato il comando **nmap -sT 192.168.20.2** per eseguire questo tipo di scansione ed ho ottenuto il seguente risultato:

```
(kali㉿kali)-[~]  
$ nmap -sT 192.168.20.2  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 12:35 CET  
Nmap scan report for 192.168.20.2  
Host is up (0.014s 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 1.73 seconds
```

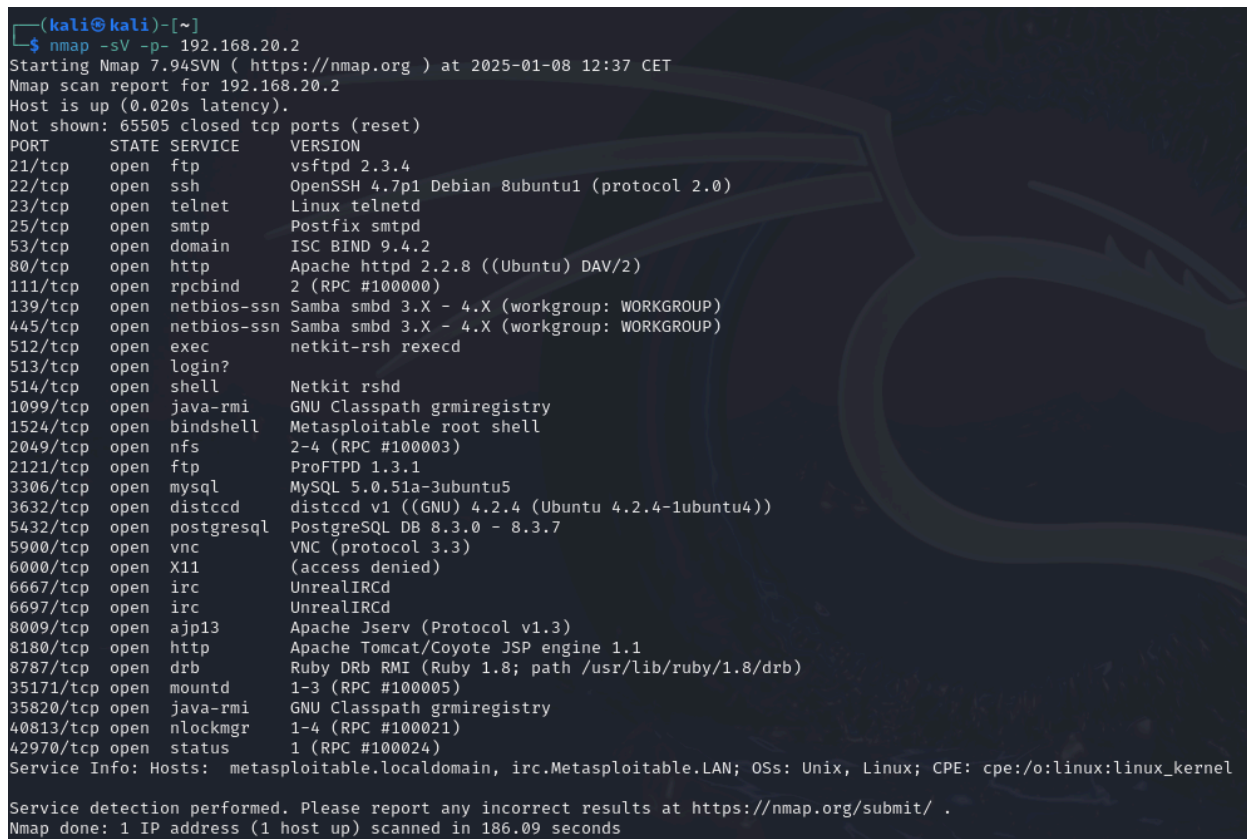
Come mostrato dalle immagini, i risultati prodotti dalle due scansioni è il medesimo, ciò che differisce tuttavia è il tempo impiegato per arrivare a fornire l'output da parte di nmap. Infatti, non stabilendo una connessione TCP completa, la SYN scan è molto più rapida rispetto alla TCP connect scan.

Nel mio caso è possibile notare che la prima scansione impiega meno della metà del tempo della seconda.

Version detection

Nmap mette a disposizione dei comandi che permettono di ottenere non solo le porte aperte ma anche la versione dei protocolli utilizzati dalla macchina target (tramite banner grabbing), in modo tale da individuare “facilmente” possibili vulnerabilità del sistema.

Ho eseguito il comando **nmap -sV -p- 192.168.20.2** per ottenere le versioni dei protocolli in uso su metasploitable2, come mostrato nell'immagine.



```
(kali@kali)-[~]
└─$ nmap -sV -p- 192.168.20.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 12:37 CET
Nmap scan report for 192.168.20.2
Host is up (0.020s latency).
Not shown: 65505 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 rshcd
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
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbc)
35171/tcp open  mountd       1-3 (RPC #100005)
35820/tcp open  java-rmi     GNU Classpath grmiregistry
40813/tcp open  nlockmgr     1-4 (RPC #100021)
42970/tcp open  status       1 (RPC #100024)
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 186.09 seconds
```

Come da aspettative, la macchina Metasploitable2 ha in esecuzione dei protocolli non aggiornati all'ultima versione e quindi potenzialmente vulnerabili (MySQL 5.0, Apache 2.2 ecc.).

Windows OS fingerprint

Come ultimo passaggio, ho connesso una macchina virtuale Windows 7 alla stessa rete della macchina Kali Linux.

```
C:\Users\User>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::6921:d452:29a3:47d1
    11
    Indirizzo IPv4. . . . . : 192.168.10.3
    Subnet mask . . . . . : 255.255.255.224
    Gateway predefinito . . . . . : 192.168.10.1
```

Ho eseguito nuovamente il comando nmap per visualizzare le informazioni sul sistema operativo **nmap -O 192.168.10.3**.

```
(kali@kali)-[~]
$ nmap -O 192.168.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 10:31 EST
Nmap scan report for 192.168.10.3
Host is up (0.00043s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
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: 08:00:27:3E:96:A8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
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 3.27 seconds
```

Tramite le informazioni ricevute da nmap, siamo in grado di visualizzare che il sistema operativo target è Windows. L'ambiguità sulla versione è data dalla similarità del fingerprint dei sistemi operativi Windows 7, Windows 8, Vista SP2 e Windows Server 2008 e pertanto non è possibile stabilire con certezza di quale versione si tratti.