
S5-L3

SOMMARIO

Inizio usando il target Metasploitable.

IP: 192.168.56.11

OS FINGERPRINT

SYN SCAN

TCP CONNECT

VERSION DETECTION

Tempistica del progetto

```
┌──(kali1㉿kali)-[~]
└─$ sudo nmap -sS 192.168.56.11
[sudo] password for kali1:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:54 CET
Nmap scan report for 192.168.56.11
Host is up (0.00011s 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:B3:F1:94 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

```
┌──(kali1㉿kali)-[~]
└─$ nmap -sT 192.168.56.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:53 CET
Nmap scan report for 192.168.56.11
Host is up (0.00068s 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 13.16 seconds
```

```
┌──(kali1㉿kali)-[~]
└─$ nmap -sV 192.168.56.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 11:55 CET
Nmap scan report for 192.168.56.11
Host is up (0.00058s 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  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  unknown
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 185.80 seconds
```

Differenze:

Nello scan SYN noto che nmap risponde al SYN/ACK del destinatario con un comando RST, pertanto non conclude il 3-way-handshake.

Invece, nello scan Full TCP nmap chiude il 3-way-handshake e crea un canale di comunicazione. Tuttavia il firewall di meta lo impedisce (conn-refused).

```
┌──(kali1㉿kali)-[~]
└─$ nmap -sV 192.168.56.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 12:06 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 3.14 seconds
```

```
┌──(kali1㉿kali)-[~]
└─$ sudo nmap -Pn 192.168.56.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 12:09 CET
Nmap scan report for 192.168.56.13
Host is up (0.00046s latency).
All 1000 scanned ports on 192.168.56.13 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:04:CE:C5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.34 seconds
```

```
┌──(kali1㉿kali)-[~]
└─$ sudo nmap -sS 192.168.56.13
[sudo] password for kali1:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 12:32 CET
Nmap scan report for 192.168.56.13
Host is up (0.0027s latency).
Not shown: 991 filtered tcp ports (no-response)
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
MAC Address: 08:00:27:04:CE:C5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.64 seconds
```

```
┌──(kali1㉿kali)-[~]
└─$ sudo nmap -sT 192.168.56.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 12:34 CET
Nmap scan report for 192.168.56.13
Host is up (0.0015s latency).
Not shown: 991 filtered tcp ports (no-response)
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
MAC Address: 08:00:27:04:CE:C5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.76 seconds
```

```
┌──(kali1㉿kali)-[~]
└─$ sudo nmap -sV 192.168.56.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 12:33 CET
Nmap scan report for 192.168.56.13
Host is up (0.00080s latency).
Not shown: 991 filtered tcp ports (no-response)
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
MAC Address: 08:00:27:04:CE:C5 (Oracle VirtualBox virtual NIC)
Service Info: Host: MALILA-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 76.44 seconds
```