Corso Epicode

SCANSIONE DEI SERVIZI CON NMAP

Report a cura di Valentino Pizzi
17 settembre, 2025

Obbiettivo:

- metasploitable 192.168.50.101

Contenuti:

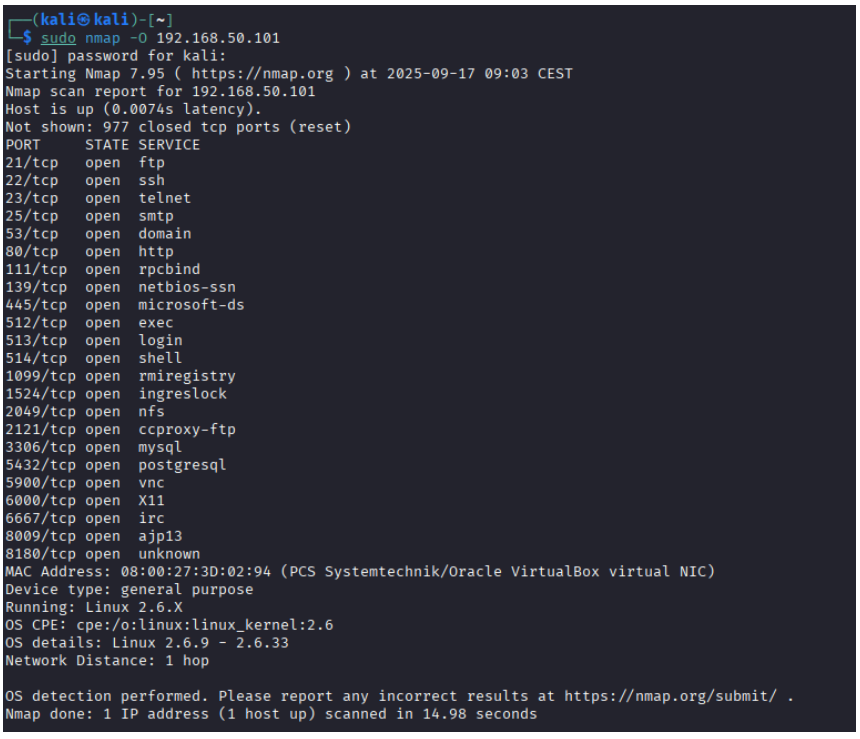
- Os fingerprint
- Syn Scan
- TCP connect
- Version Detection

Obbiettivo:

Utilizzare nmap per scansire la macchina metasploitable2 di “IP 192.168.50.101” per raccogliere informazioni e differenti flag di nmap.

Os fingerprint:

Utilizziamo il flag ***“-O”*** per identificare il sistema operativo e la sua versione analizzando i pacchetti di dati che trasmette alla rete



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 09:03 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0074s 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: 08:00:27:3D:02:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
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 14.98 seconds
```

SYN scan:

Utilizziamo il flag ***"-sS"*** per fare una scansione in cui l'attaccante inizia una conversazione TCP con la macchina target inviando solo il pacchetto ***"SYN"***.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 09:16 CEST
Nmap scan report for 192.168.50.101
Host is up (0.019s 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: 08:00:27:3D:02:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
```

TCP connect:

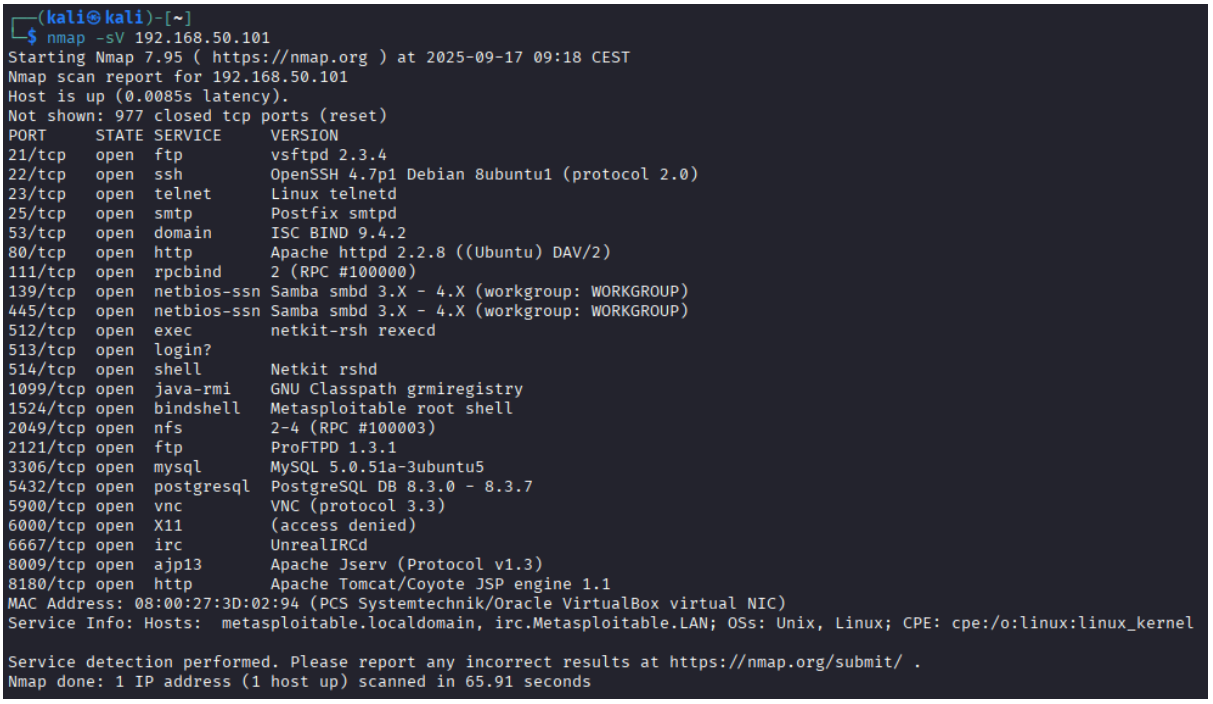
Usiamo il flag ***"-sT"*** per fare una scansione in cui l'attaccante porta a termine la connessione 3 way handshake.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 09:18 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0034s 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: 08:00:27:3D:02:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

Version Detection:

Utilizziamo il flag ***"-sV"*** per stabilire quali versioni dei servizi attivi sono disponibili nella nostra macchina target.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 09:18 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0085s 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      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
MAC Address: 08:00:27:3D:02:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 65.91 seconds
```

Conclusioni:

Le differenze fra le scansioni eseguite sono:

- Os fingerprint riesce ad individuare la versione ed il sistema operativo.
- Syn scan inizia una connessione TCP ma non la completa.
- TCP connect completa la connessione TCP ma individua le stesse informazioni della Syn scan.
- Version Detection è la più completa in quanto riesce a fornirci informazioni sulla versione dei servizi attivi sulle varie porte, inoltre trova anche il sistema operativo della macchina target.