Report S5L2

Traccia: Tecniche di scansione con nmap

Utilizzare il tool nmap per effettuare le seguenti scansioni sul target Metasploitable2:

- OS fingerprint.
- Syn Scan.
- TCP connect, trovare se ci sono differenze tra i risultati della scansioni TCP connect e SYN
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

Obiettivo:

- IP.
- Sistema Operativo.
- Porte Aperte.
- Servizi in ascolto con versione.

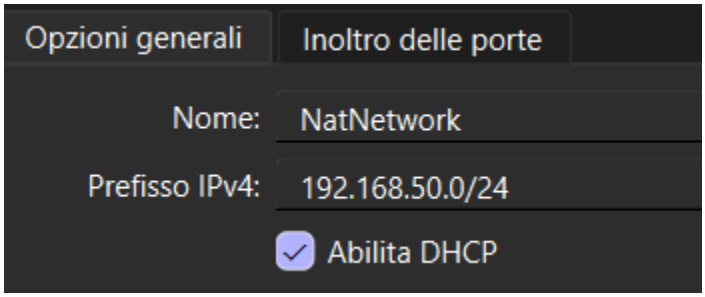
Configurazione indirizzi IP:

Gli indirizzi IP sono configurati nella rete con NAT: **192.168.50.0/24** e DHCP abilitato

Kali: 192.168.50.10

Metasploitable: 192.168.50.3

Windows: 192.168.50.4



Eseguiamo l'OS fingerprint sulla Metasploitable:

Tenta di determinare quale tipo di sistema operativo è in esecuzione su un host remoto basandosi su un database di firme di sistemi operativi noti per identificare il sistema operativo del target, in questo caso **Linux 2.6** (2.6.9-2.6.33).

```
┌──(kali㉿kali)-[~]
└─$ nmap -O  192.168.50.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 09:59 EDT
Nmap scan report for 192.168.50.3
Host is up (0.0020s 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: 08:00:27:04:3F:E1 (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 1.75 seconds
```

Eseguiamo il TCP SYN scan su Metasploitable:

Invia pacchetti **SYN** e attende una risposta **SYN/ACK** (porta aperta) o **RST** (porta chiusa), quando riceve un **SYN/ACK** invia un pacchetto RST per terminare la connessione senza completare la stretta di mano **TCP**, non stabilendo una connessione completa è meno probabile che venga registrata nei log e che venga rilevata dai sistemi di intrusion detection.

Il comando **-p-** è utilizzato per la scansione di tutte le porte per trovare tutte le porte aperte.

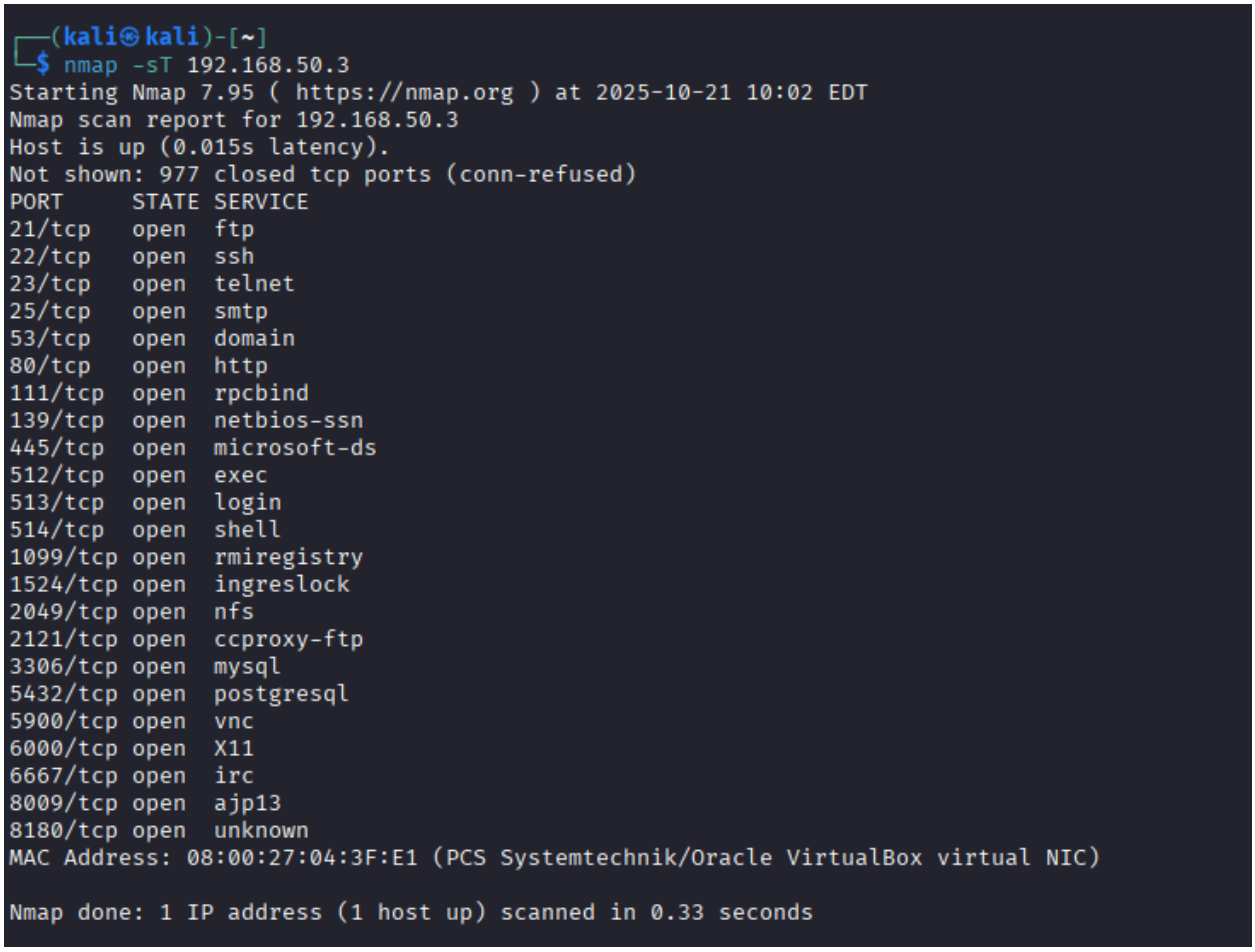
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- 192.168.50.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 10:01 EDT
Nmap scan report for 192.168.50.3
Host is up (0.0042s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
34765/tcp open  unknown
49990/tcp open  unknown
52317/tcp open  unknown
56432/tcp open  unknown
MAC Address: 08:00:27:04:3F:E1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.92 seconds
```

Eseguiamo il TCP connect scan su Metasploitable:

È la scansione **TCP** più semplice e affidabile disponibile, dato che esegue una scansione **TCP** completa per ciascuna porta di destinazione.

Si usa in ambienti dove non è importante non essere rilevati.



Differenze tra TCP e SYN:

Come si può vedere il tempo è minore nella scansione **SYN** (parziale), su **Wireshark** non completa le richieste al contrario della **TCP**.

Eseguiamo il version detected su metasploitable:

-sV esegue la rilevazione della versione dei servizi in esecuzione sulle porte aperte, invia una serie di pacchetti di prova ai servizi sulle porte aperte e analizza le risposte.

Si usa per determinare esattamente quali servizi e versioni sono in esecuzione su un host remoto, aiutando ad identificare potenziali vulnerabilità note.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 10:03 EDT
Nmap scan report for 192.168.50.3
Host is up (0.0034s 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?
513/tcp  open  login
514/tcp  open  tcpwrapped
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: 08:00:27:04:3F:E1 (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 63.75 seconds
```

Come si può vedere elenca tutte le versioni in esecuzione per ogni porta aperta.

Eseguiamo l'OS fingerprint su Windows:

Come per la Metasploitable anche in questo caso tenta di determinare quale tipo di sistema operativo è in esecuzione su un host remoto basandosi su un database di firme di sistemi operativi noti per identificare il sistema operativo del target, il sistema operativo rilevato è **Windows 10**.

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 10:06 EDT
Nmap scan report for 192.168.50.4
Host is up (0.0018s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
5432/tcp open  postgresql
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:68:01:A1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 2.59 seconds
```