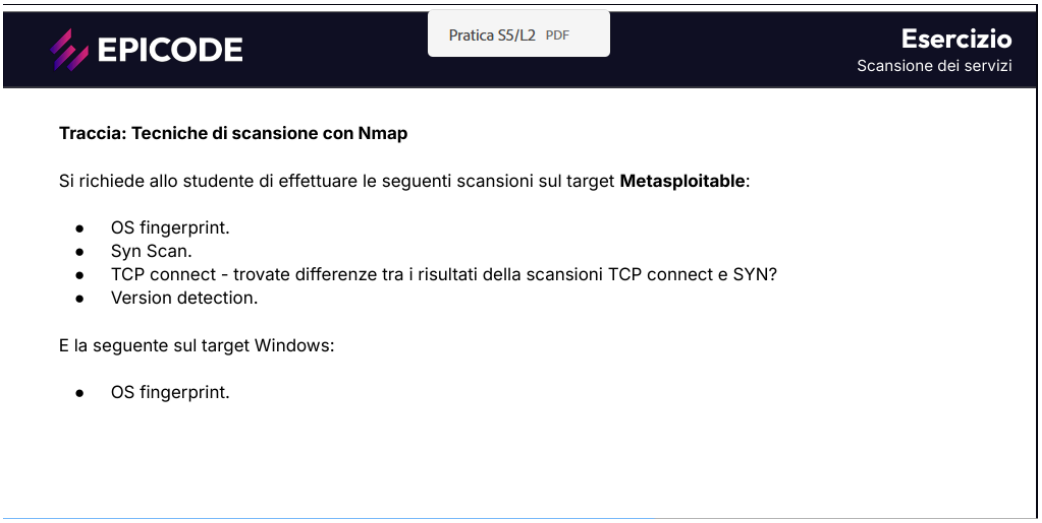
Obiettivo



EPICODE

Pratica S5/L2 PDF

Esercizio
Scansione dei servizi

Traccia: 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:

- OS fingerprint.

Os fingerprint

- Comando utilizzato : nmap -O <IP_metasploitable> (in questo caso 192.168.50.3)
- Spiegazione : L'opzione -O abilita la rilevazione del sistema operativo → invio di una serie di pacchetti TCP/IP ed analizzando le risposte e confrontandole con un database di firme note per identificare il sistema operativo target. Sotto troviamo la risposta relativa a nmap (⬇)

```
┌──(kali㉿kali)-[/]
└─$ nmap -O 192.168.50.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 08:49 EDT
Nmap scan report for 192.168.50.3
Host is up (0.00039s latency).
```

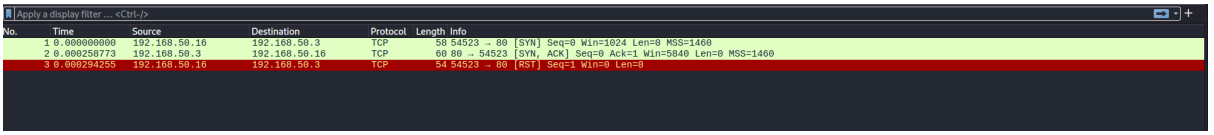
```
Host is up (0.00039s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  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:C3:01:73 (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
```

SYN scan

- Comando utilizzato : nmap -sS 192.168.50.3
- Spiegazione : L'opzione -sS invia un pacchetto SYN, se riceve un SYN/ACK, determina che la porta è aperta e invece di completare il 3-way handshake invia un pacchetto reset (come mostrato negli screen ⬇)

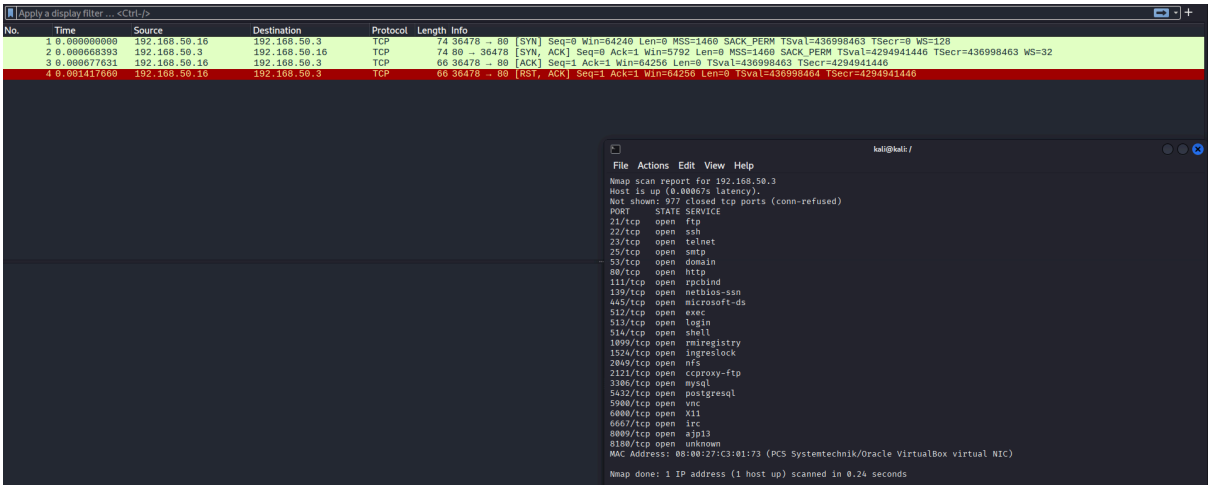
```
└─$ nmap -sS 192.168.50.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 08:58 EDT
Nmap scan report for 192.168.50.3
Host is up (0.000097s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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:C3:01:73 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Come possiamo vedere sotto da wireshark ad esempio per la porta 80 abbiamo una SYN, una SYN-ACK e un RST



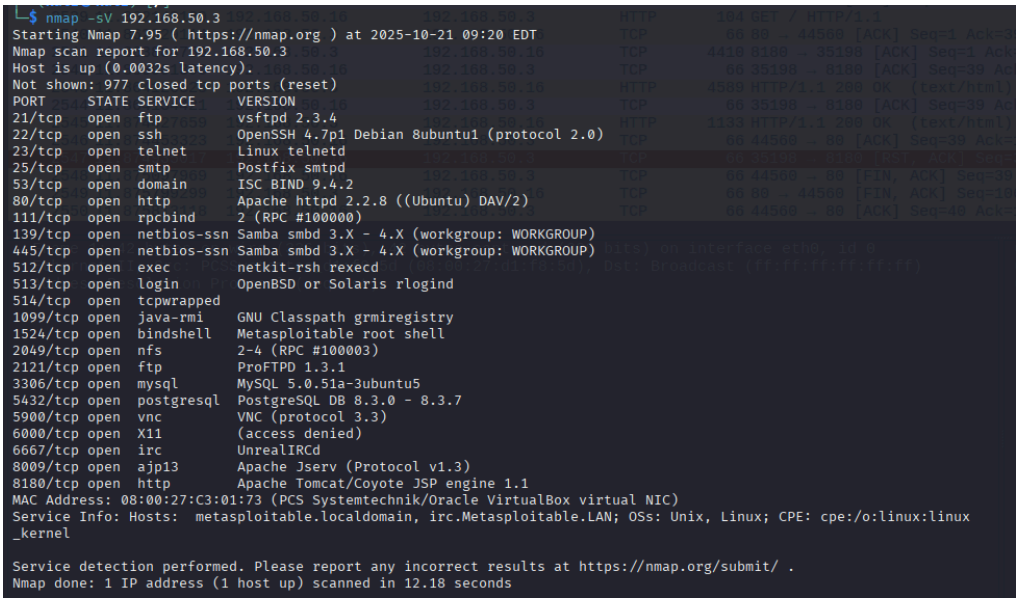
TCP Connect

- Comando utilizzato : nmap -sT 192.168.50.3
- Spiegazione : Con il comando -sT si esegue una scansione che stabilisce connessioni TCP complete , quindi si va a completare il processo di 3-way handshake.



Version Detection

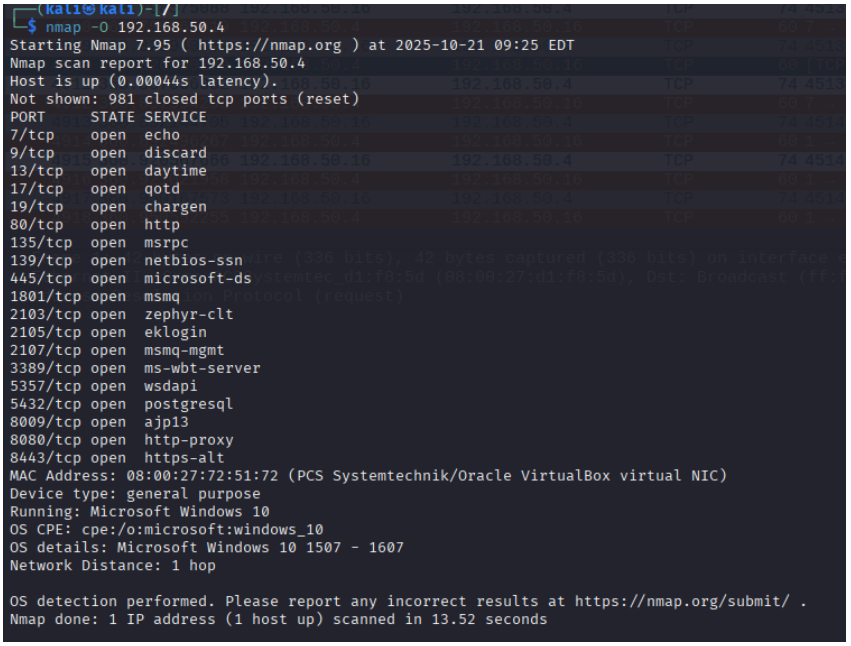
- Comando utilizzato : nmap -sV 192.168.50.3
- Spiegazione : Con il comando -sV (banner grabbing) il programma invia una serie di pacchetti di probe ai servizi sulle porte aperte e analizza le risposte. Nmap confronta le risposte con un database per identificare il servizio e la versione in esecuzione.(come possiamo vedere dalla figura sottostante in cui Nmap indica i servizi in esecuzione sulle porte)



```
└─$ nmap -sV 192.168.50.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 09:20 EDT
Nmap scan report for 192.168.50.3
Host is up (0.0032s 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       OpenBSD or Solaris rlogind
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:C3:01:73 (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 12.18 seconds
```

OS Fingerprint su Windows

- Comando utilizzato : nmap -O <IP_Windows>
- Spiegazione : Come per metasploitable il comando -O viene utilizzato per tentare di determinare quale sistema operativo e versione è in esecuzione sull'host Windows target.



```
┌──(kali㉿kali)-[/]
└─$ nmap -O 192.168.50.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 09:25 EDT
Nmap scan report for 192.168.50.4
Host is up (0.00044s 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: 08:00:27:72:51:72 (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 13.52 seconds
```

DIFFERENZE TRA TCP Connect e SYN Scan

Come evidenziato precedentemente all'interno del report, la differenza non risiede nei risultati finali dati da Nmap ma :

- -sT (TCP connect) : completa il 3-way handshake stabilendo una connessione completa (Come evidenziato da screen precedentemente inseriti).
  Inoltre è più invasiva andando a creare più "rumore" a livello di rete oltre che più facilmente identificabile.
- -sS (SYN Scan) : esegue una scansione "half-open" . Non completa il 3-way handshake ma invia un pacchetto RST ,prima di stabilire una connessione, dopo aver ricevuto il SYN-ACK ed aver appurato che la porta sia aperta. Ha il pregio inoltre di essere meno invasiva quindi generando meno "rumore" all'interno della rete.