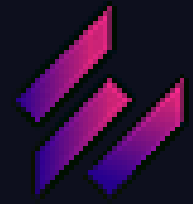


REPORT

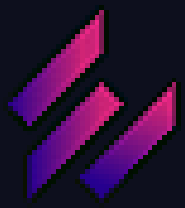
Scansione dei servizi con Nmap

By Xian Long Qiu



Indice

- Panoramica pag. 3
- Target Metasploitable pag.6
- Target Windows 10 pag.10
- Conclusione pag.12



Panoramica

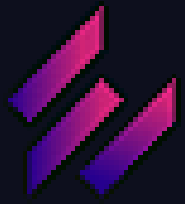
Effettuare le scansioni sul target [Metasploitable](#): OS fingerprint, SYN Scan, TCP connect(trovare differenze tra i risultati delle scansioni TCP connect e SYN) e Version detection.

Altro target e' [window 10](#), scansionare OS fingerprint.

Scopo

Trovare le seguenti info:

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

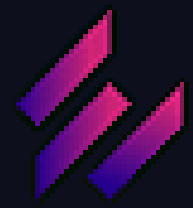


Origine traccia

Il presente report è relativo al Modulo 2 - Settimana 1 - lezione 2
del corso sulla piattaforma Epicode

Ambiente di lavoro OS

- Kali linux
- Metasploitable 2
- Windows 10 pro



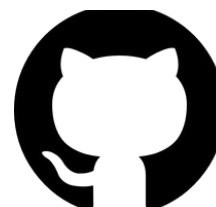
Strumenti

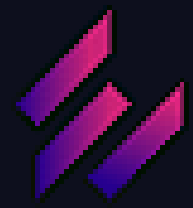
- terminale di Linux: interfaccia a riga di comando che consente l'esecuzione diretta dei comandi.
- Nmap: tool open source per la scansione delle reti e la raccolta di informazioni su host, porte e servizi.

Fonte

Repository

<https://github.com/XLQcyber/CS0225>



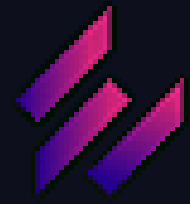


Scansione target: Metasploitable

IP: 192.168.178.16

```
(kali㉿kali)-[~]  
$ ping 192.168.178.16  
PING 192.168.178.16 (192.168.178.16) 56(84) bytes of data.  
64 bytes from 192.168.178.16: icmp_seq=1 ttl=64 time=1.30 ms  
64 bytes from 192.168.178.16: icmp_seq=2 ttl=64 time=5.61 ms  
64 bytes from 192.168.178.16: icmp_seq=3 ttl=64 time=0.921 ms  
64 bytes from 192.168.178.16: icmp_seq=4 ttl=64 time=0.745 ms  
^C  
— 192.168.178.16 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 0.745/2.145/5.614/2.012 ms
```

Verifico la connessione tra Kali e Meta attraverso il ping. La connessione tra di loro funziona.



```
(kali@kali)-[~]
$ nmap -O 192.168.178.16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:44 EDT
Nmap scan report for 192.168.178.16
Host is up (0.0058s 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:C3:08:16 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.21
OS details: Linux 2.6.21
Network Distance: 1 hop

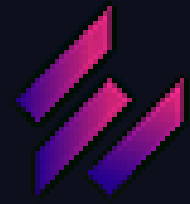
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
```

Uso la nmap -sS per
scannerizzare SYN.
Risultato: rilevamento delle porte
aperte.

Uso la nmap -O per
scannerizzare il sistema
operativo.
Risultato: linux 2.6.X.

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.178.16
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:48 EDT
Nmap scan report for 192.168.178.16
Host is up (0.0078s 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:C3:08:16 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
```

```
(kali@kali)~$ nmap -sT 192.168.178.16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:49 EDT
Nmap scan report for 192.168.178.16
Host is up (0.013s 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:C3:08:16 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

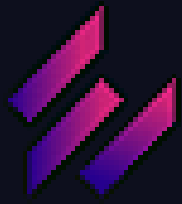
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Uso nmap -sT per scannerizzare
connessioni TCP.
Risultato: stesse porte aperte
rilevate dal SYN Scan.

Uso nmap -sV per scannerizzare le
versioni.
Risultato: rilevamento delle versioni
dei servizi attivi.

```
(kali@kali)~$ nmap -sV 192.168.178.16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:51 EDT
Nmap scan report for 192.168.178.16
Host is up (0.016s 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 Subuntu1 (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 rshd
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:C3:08:16 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

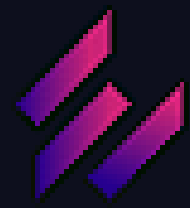
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.48 seconds
```

Differenze tra TCP Connect e SYN Scan

Entrambi hanno trovato le stesse porte. Questo è comune. Tuttavia, le differenze operative sono:

Aspetto	SYN Scan (-sS)	TCP Connect (-sT)
Connessione TCP	Incompleta (solo SYN)	Completa (connect())
Velocità	Più veloce	Più lenta
Stealth	Più stealth	Più visibile (registrato nei log)
Privilegi	Richiede root/sudo	Non richiede privilegi elevati

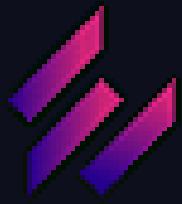


Scansione target: Windows 10 pro

IP : 192.168.178.78

```
(kali㉿kali)-[~]  
$ ping 192.168.178.78  
PING 192.168.178.78 (192.168.178.78) 56(84) bytes of data.  
64 bytes from 192.168.178.78: icmp_seq=1 ttl=128 time=1.98 ms  
64 bytes from 192.168.178.78: icmp_seq=2 ttl=128 time=0.743 ms  
64 bytes from 192.168.178.78: icmp_seq=3 ttl=128 time=0.810 ms  
64 bytes from 192.168.178.78: icmp_seq=4 ttl=128 time=0.792 ms  
64 bytes from 192.168.178.78: icmp_seq=5 ttl=128 time=0.678 ms  
^C  
— 192.168.178.78 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4029ms  
rtt min/avg/max/mdev = 0.678/1.001/1.982/0.492 ms
```

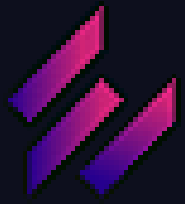
Verifico la connessione tra Kali e Windows attraverso il ping. La connessione tra di loro funziona.



```
(kali@kali)-[~]
$ nmap -O 192.168.178.78
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:02 EDT
Nmap scan report for 192.168.178.78
Host is up (0.00084s 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  wsapi
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:84:66:35 (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 2.64 seconds
```

Utilizzo nmap -O per verificare
il sistema operativo.
Risultato: Windows 10
correttamente identificato



Conclusione

La scansione è stata eseguita con successo su entrambi i target. Le funzionalità principali di Nmap sono state testate, e sono state confermate:

- L'affidabilità del rilevamento del sistema operativo tramite -O
- La corrispondenza dei risultati tra SYN e TCP Connect (sebbene tecnicamente differenti)
- La possibilità di ottenere dettagli sui servizi attivi tramite -sV