

### Traccia:

Vedremo da vicino nmap e i suoi comandi.

Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla macchine metasploitable, come di seguito:

- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con switch «-A» sulle porte well-known

Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchina sorgente con Wireshark.

### • Scansione nmap TCP

```
(kali@kali) ~$ sudo nmap -sT -p 1-1024 192.168.30.130
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 19:20 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.30.130
Host is up (0.00093s latency).
Not shown: 1012 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
MAC Address: 08:00:27:96:59:DC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

The screenshot shows a Wireshark capture of a network scan. The packet list on the left shows several TCP segments from 192.168.30.130 to 192.168.30.130. The selected packet (No. 49) is a TCP segment with the following details:

- Source: 192.168.30.130
- Destination: 192.168.30.130
- Protocol: TCP
- Length: 60
- Sequence Number: 0 (relative sequence number)
- Next Sequence Number: 1 (relative sequence number)
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 757935300
- Header Length: 40 bytes (10)
- Flags: 0x012 (SYN, ACK)
- Window: 5792
- Checksum: 0x8d99 (unverified)

The packet bytes pane shows the raw data of the TCP segment, including the SYN and ACK flags.

- ❖ Il comando **nmap -sT <target>** esegue una scansione TCP utilizzando il metodo di connessione a tre vie (3-way handshake) per stabilire una connessione completa con il target.

- Scansione Syns

```
(kali@kali)-[~]
$ sudo nmap -sS -p 1-1024 192.168.30.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 19:30 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers=
Nmap scan report for 192.168.30.130
Host is up (0.00023s latency).
Not shown: 1012 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
MAC Address: 08:00:27:96:59:DC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

[illegible]

- ❖ Questo comando utilizza l'opzione **-sS** per specificare una scansione SYN, che è una delle tecniche più comuni per eseguire una scansione TCP.
- ❖ Come con Wireshark, vediamo chiaramente che sulla porta 80 non stabiliamo una connessione 3-way handshake ma una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il 3-way-handshake, ma appurato che la porta è aperta chiude la comunicazione.

- Scansione nmap -A

```
kali@kali:~$ sudo nmap -A -p 1-1024 192.168.30.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 20:17 EDT
Nmap scan report for 192.168.30.130
Host is up (0.00051s latency).
Not shown: 1022 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.30.125
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsftpd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh
|_OpenSSH 4.7p1 Debian Buntuntu (protocol 2.0)
|_ssh-hostkey:
|_1024 6018f6c1e1c05f6a7a4d690124fa6c1d586cdd (DSA)
|_2048 561561240f211d1de1a712b2ae01b12413d0e0f3 (RSA)
23/tcp    open  telnet?
25/tcp    open  smtp?
|_smtp-command: setsockoptable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain
|_ISC BIND 9.4.2
|_bind.version: 9.4.2
80/tcp    open  http
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-titler: Metasploitable2 - linux
111/tcp   open  rpcbind
|_RPC #100000
|_rpcinfo:
|_program version port/proto service
|_100000 2 111/tcp rpcbind
|_100000 2 111/udp rpcbind
|_100003 2,3,4 2049/tcp nfs
|_100003 2,3,4 2049/udp nfs
|_100005 1,2,3 37573/tcp mountd
|_100005 1,2,3 37573/udp mountd
|_100021 1,3,4 47671/tcp nlockmgr
|_100021 1,3,4 47671/udp nlockmgr
|_100024 1 30374/udp status
|_100024 1 45687/tcp status
139/tcp   open  netbios-ssn
|_Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn
|_Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
```

File Actions Edit View Help

111/tcp open rpcbind 2 (RPC #100000)

rpcinfo:

program version port/proto service

100000 2 111/tcp rpcbind

100000 2 111/udp rpcbind

100003 2,3,4 2049/tcp nfs

100003 2,3,4 2049/udp nfs

100005 1,2,3 37573/tcp mountd

100005 1,2,3 37573/udp mountd

100021 1,3,4 47671/tcp nlockmgr

100021 1,3,4 47671/udp nlockmgr

100024 1 30374/udp status

100024 1 45687/tcp status

139/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

512/tcp open exec?

513/tcp open login?

514/tcp open shell?

MAC Address: 08:00:27:96:59:DC (Oracle VM)

Device type: general purpose

Running: Linux 2.6.9

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: OS: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel:2.6

Host script results:

\_nbtstat: NetBIOS name: METASPOILTABLE, NetBIOS discovery:

\_OS: Unix (Samba 3.0.20-Debian)

\_Computer name: metasploitable

\_NetBIOS computer name:

\_Domain name: localdomain

\_FQDN: metasploitable.localdomain

\_System time: 2024-04-18T14:45:01-04:00

\_smb-time: Protocol negotiation failed (clock skew: mean: 1h59m0s, deviation: 2)

\_smb-security-mode:

\_account\_user: <None>

\_authentication\_level: user

\_challenge\_response: supported

\_message\_signing: disabled (dangerous, not recommended)

TRACEROUTE

HOP RTT ADDRESS

0 0.69 ms 192.168.30.130

OS and Service detection performed. Please see the Nmap project for help: https://nmap.org

OS and Service detection performed. Please see the Nmap project for help: https://nmap.org

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ...<Ctrl-F>

| No. | Time         | Source         | Destination    | Protocol | Length | Info   |
|-----|--------------|----------------|----------------|----------|--------|--|
| 46  | 20.872449546 | 192.168.30.125 | 192.168.30.130 | TCP      | 54     | 56075 - 139 [RST] Seq=1 Win=0 Len=0                        |
| 47  | 20.872473551 | 192.168.30.125 | 192.168.30.130 | TCP      | 54     | 56075 - 22 [RST] Seq=1 Win=0 Len=0                         |
| 48  | 20.872520383 | 192.168.30.125 | 192.168.30.130 | TCP      | 54     | 56075 - 21 [RST] Seq=1 Win=0 Len=0                         |
| 49  | 20.872541298 | 192.168.30.125 | 192.168.30.130 | TCP      | 54     | 56075 - 111 [RST] Seq=1 Win=0 Len=0                        |
| 50  | 20.872723822 | 192.168.30.125 | 192.168.30.130 | TCP      | 58     | 56075 - 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460            |
| 51  | 20.872754824 | 192.168.30.125 | 192.168.30.130 | TCP      | 58     | 56075 - 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460             |
| 52  | 20.872815599 | 192.168.30.125 | 192.168.30.130 | TCP      | 58     | 56075 - 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460             |
| 53  | 20.872873429 | 192.168.30.125 | 192.168.30.130 | TCP      | 58     | 56075 - 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460            |
| 54  | 20.872937718 | 192.168.30.125 | 192.168.30.130 | TCP      | 58     | 56075 - 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460             |
| 55  | 20.872950881 | 192.168.30.125 | 192.168.30.130 | TCP      | 58     | 56075 - 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460            |
| 56  | 20.873121023 | 192.168.30.130 | 192.168.30.125 | TCP      | 60     | 445 - 56075 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 57  | 20.873121287 | 192.168.30.130 | 192.168.30.125 | TCP      | 60     | 23 - 56075 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460  |
| 58  | 20.873164133 | 192.168.30.125 | 192.168.30.130 | TCP      | 54     | 56075 - 23 [RST] Seq=1 Win=0 Len=0                         |
| 59  | 20.873375625 | 192.168.30.130 | 192.168.30.125 | TCP      | 60     | 88 - 56075 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460  |
| 60  | 20.873375984 | 192.168.30.130 | 192.168.30.125 | TCP      | 60     | 993 - 56075 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 MSS=1460    |
| 61  | 20.873391037 | 192.168.30.130 | 192.168.30.125 | TCP      | 60     | 53 - 56075 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460  |
| 62  | 20.873376394 | 192.168.30.130 | 192.168.30.125 | TCP      | 60     | 443 - 56075 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 MSS=1460    |

Frame 60: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on eth0  
Ethernet II, Src: PCSysentec, 96:50:dc (08:00:27:96:59:dc), Dst: PCSysentec, 96:50:dc (08:00:27:96:59:dc)  
Internet Protocol Version 4, Src: 192.168.30.130, Dst: 192.168.30.125  
Transmission Control Protocol, Src Port: 80, Dst Port: 56075, Seq: 0, A  
Source Port: 80  
Destination Port: 56075  
[Stream index: 12]  
[Conversation completeness: Incomplete (35)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 150772895  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment Number (raw): 1367107850  
0110 .... = Header Length: 24 bytes (6)  
[RST] 0101111111 [SYN, ACK]  
Window: 5840  
[calculated window size: 5840]  
Checksum: 0x0000 (unverified)

❖ Il comando **nmap -A** esegue una scansione completa del target utilizzando diverse tecniche e opzioni avanzate di Nmap. Questa opzione è utile per ottenere una vasta gamma di informazioni sul target, inclusi dettagli sul sistema operativo, versioni dei servizi, tracciatura della rete e altro ancora.

• Differenze tra la connessione Tcp completa e connessione SyNs

- ❖ Nmap -St : con questo comando scansioniamo la rete completando il 3-way handshake e quindi faremo molto più rumore e aumentiamo il rischio di essere intercettati.
- ❖ Nmap -Ss : con questo comando invece scansioniamo la rete non completando il 3-way handshake. Quindi invieremo un pacchetto syNs e riceveremo un hack.

La differenza sostanziale tra i due comandi sta nel fatto che se completiamo il 3-way handshake il tipo di scann sarà più completo perché otteniamo più informazioni ma rischiamo di essere intercettati, nel secondo scann non completiamo il 3-way handshake perché l'unica cosa che ci interessa è sapere se la porta è aperta e passare avanti, quindi questo comando risulterebbe meno invasivo rispetto al primo.