EPICODE

Esercizio
Nmap scan

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:

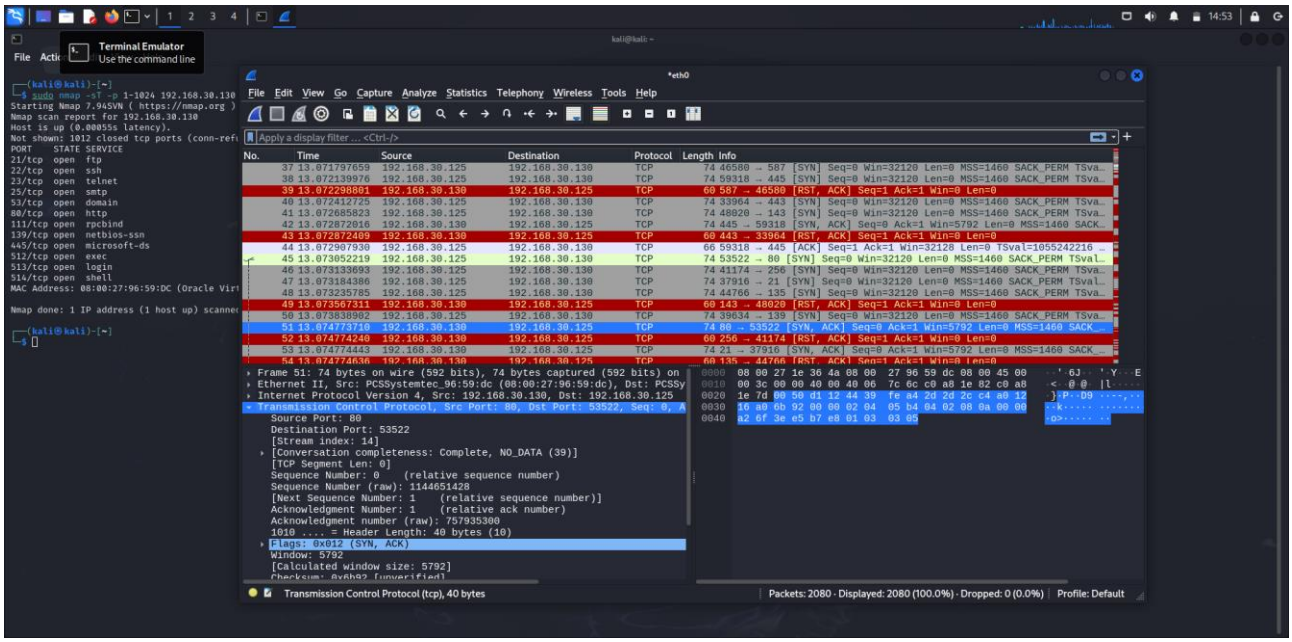
- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con switch «-A» sulle porte well-known

Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchine 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
```

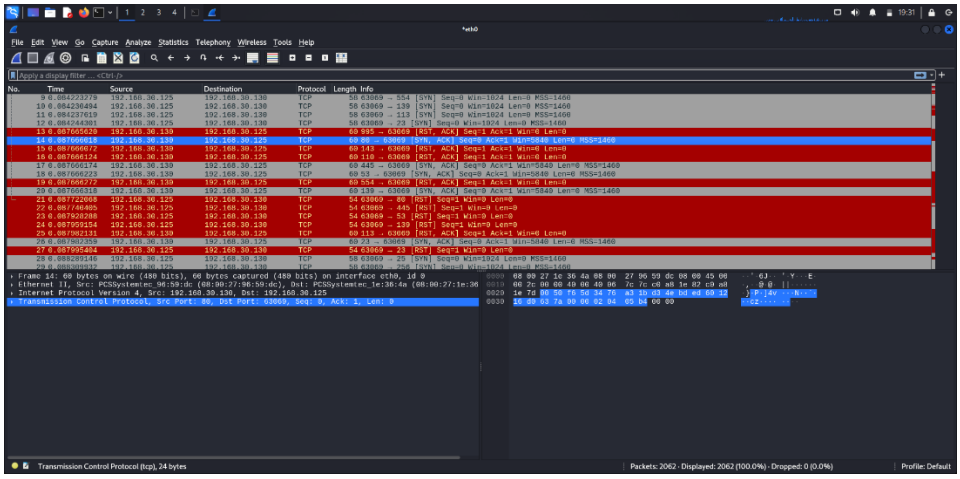


❖ Il comando **nmap -sT <target>** esegue una scansione TCP utilizzando il metodo di connessione a tre vie (3-way handshake) per stabilire una connessione completa con il target.

- Scansione Syns

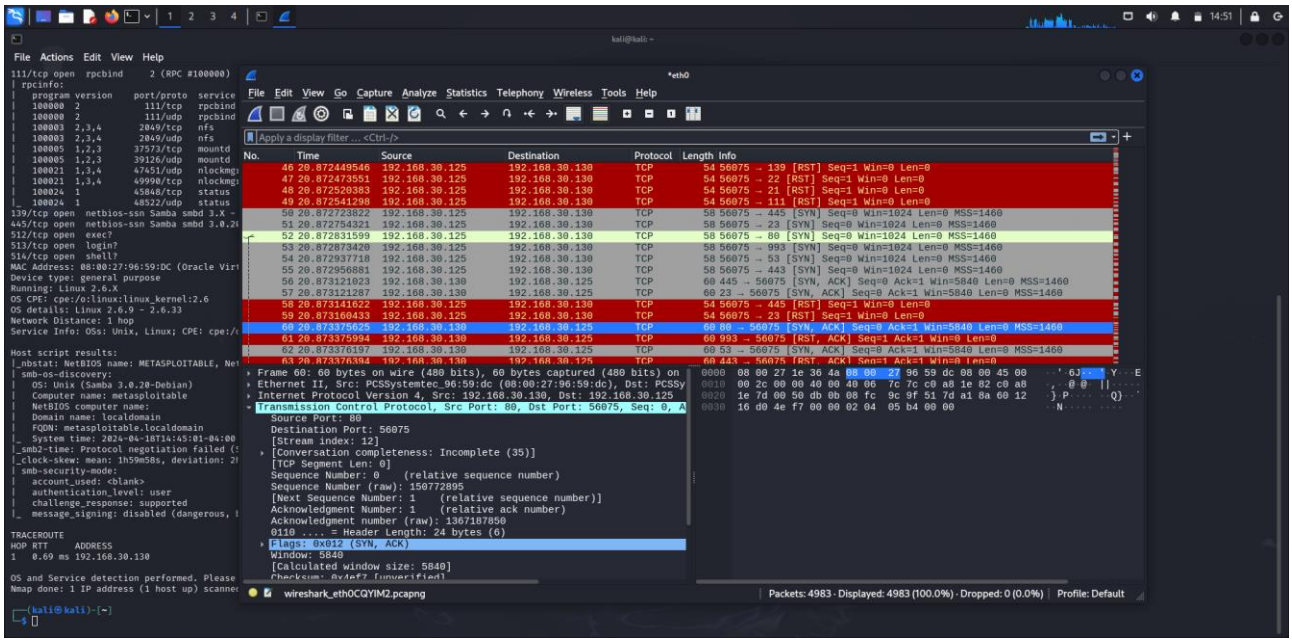
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 1-1024 192.168.30.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 19:30 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 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
```



- 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



- 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 ottieniamo più informazioni ma rischiamo di essere intercettati, nel secondo scann non completiamo il 3-way handshake perché l'unica cosa che ci interessa e sapere se la porta è aperta e passare avanti, quindi questo comando risulterebbe meno invasivo rispetto al primo.