Convezione o normalita’ la presenza dei firewall?

Traccia:

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall’esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato.

L’esercizio di oggi è verificare in che modo l’attivazione del Firewall impatta il risultato di una scansione dei servizi dall’esterno.

Per questo motivo:

1. Assicuratevi che il Firewall sia **disattivato** sulla macchina Windows XP / 7

2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch**–sV**, per la service detection e **-o** nomefilereport per salvare in un file l’output)

3. Abilitare il Firewall sulla macchina Windows XP / 7

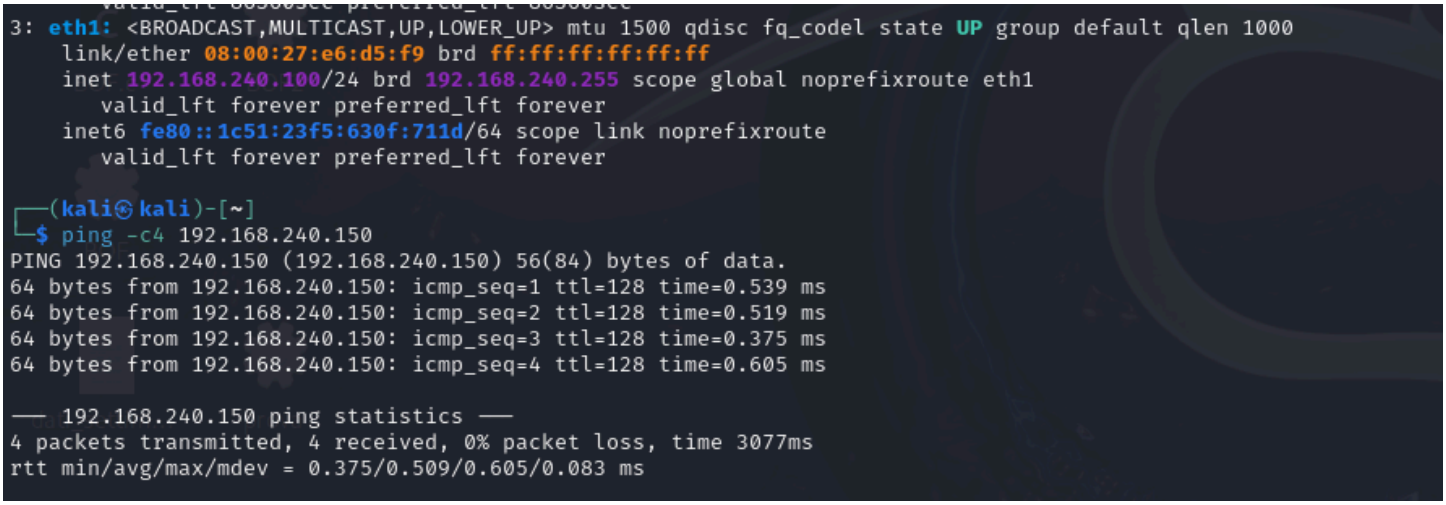
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch**–sV**.

5. Provare eventuale ulteriore **scansione differente** sempre con firewall attivato.

6.Trovare le eventuali differenze e motivarle

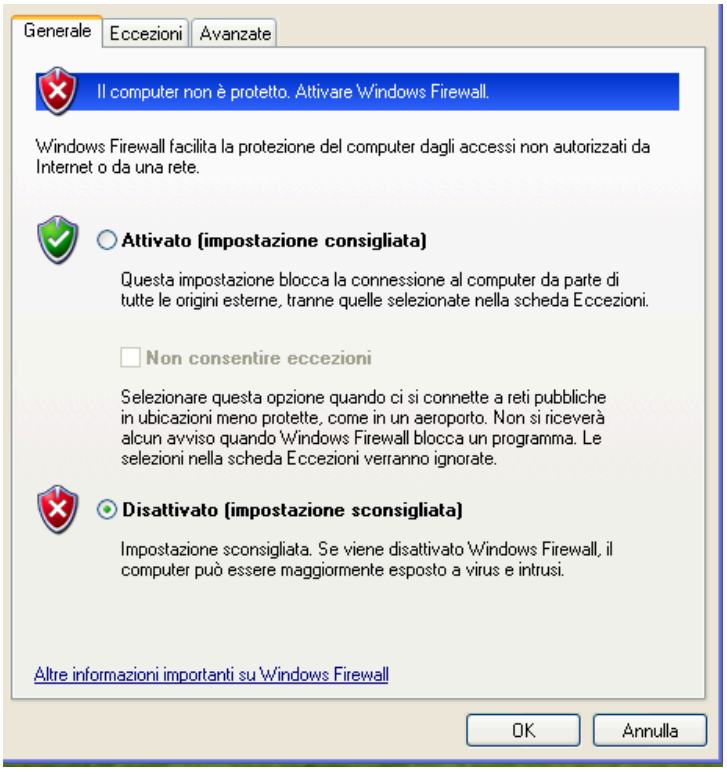
Configurazione delle macchine

Come primo passaggio, configuriamo le macchine con l’ip scelto e verifichiamo che il ping vada a buon fine:



```
Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . : 192.168.240.150
        Subnet mask . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . : 192.168.240.1

C:\Documents and Settings\Administrator>ping 192.168.240.100

Esecuzione di Ping 192.168.240.100 con 32 byte di dati:

Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64

Statistiche Ping per 192.168.240.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo =  1ms, Medio =  0ms
```

Come seconda cosa verifichiamo che sia disattivo il firewall della macchina vittima, in questo caso windows XP:



Scansione senza firewall

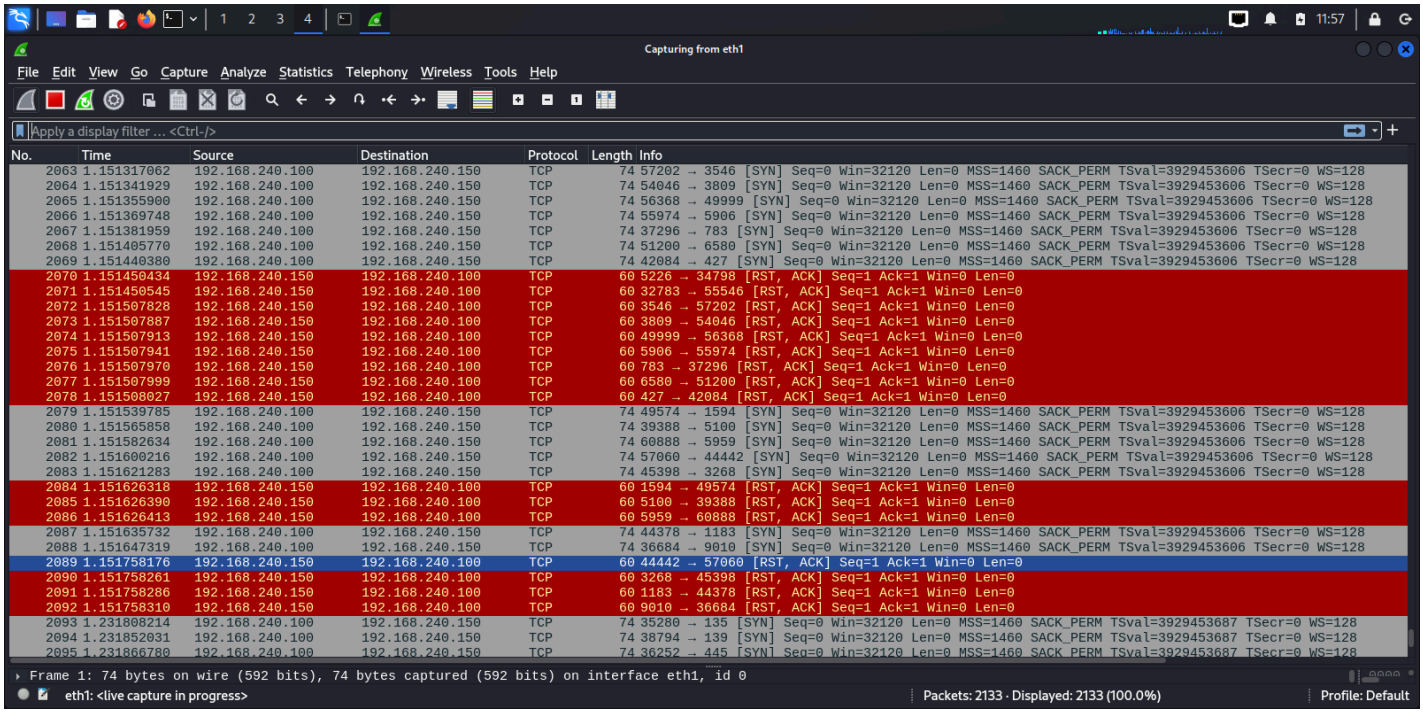
Adesso possiamo mandare una scansione tramite **nmap** per ottenere informazioni:

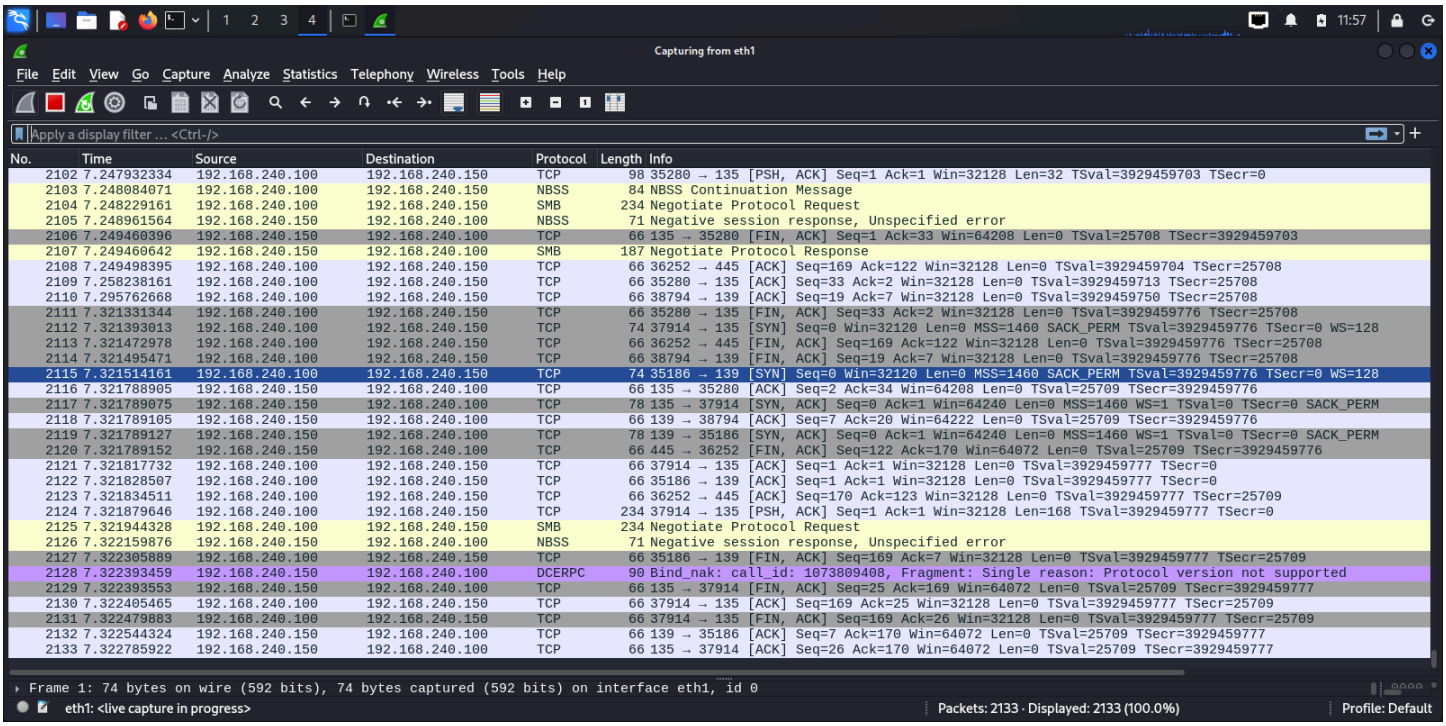
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -o dati.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 11:52 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00036s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.49 seconds
```

ove **-sV** sta per **service detection** che permette una scansione piu' approfondita, permette di ottenere dati sul tipo di servizio attivo e **-o** che sta per **output** per salvare tutto in un file output.

Possiamo notare che in assenza di firewall, nmap ha notato 3 porte aperte e buone informazioni sull'**OS.**

In contemporanea ho lasciato **Wireshark** attivo a sniffare il traffico:



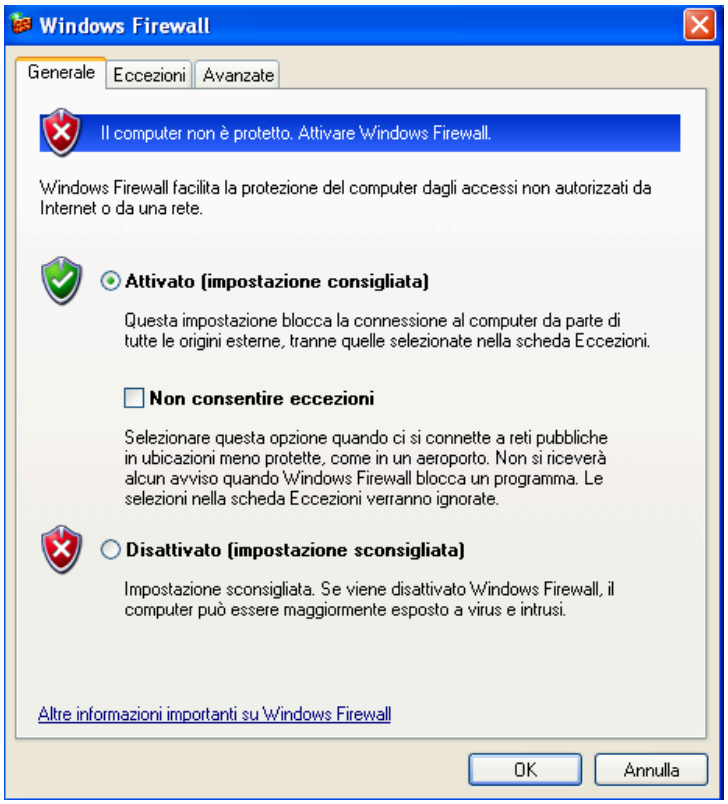


Possiamo notare che ci sono principalmente 3 tipi risposte alle domande **TCP [SYN]** (Synchronize):

1. **Risposta vuota;** la mancata risposta puo' avvenire per vari motivi, per la perdita del pacchetto, per la chiusura della porta, per un errore di connessione, oppure i sistemi possono essere configurati in modo tale da non destare segnali.
2. **Risposta rifiutata [RST, ACK];** questo implica che la macchina vittima ha ricevuto il pacchetto di richiesta ma non essendoci un servizio attivo in ascolto sulla determinata porta, rifiuta la connessione (rammentiamo che **[RST, ACK]** sta per Reset Acknowledgment).
3. **Risposta accettata [ACK]; i**n questo caso se la richiesta viene accettata, allora significa che abbiamo ricevuto un pacchetto **[ACK]** dal servizio attivo, questo implica che la porta e aperta.

Scansione in presenza del firewall

Attiviamo il firewall di WindowsXP:



Mandiamo nuovamente la scansione tramite **nmap**:

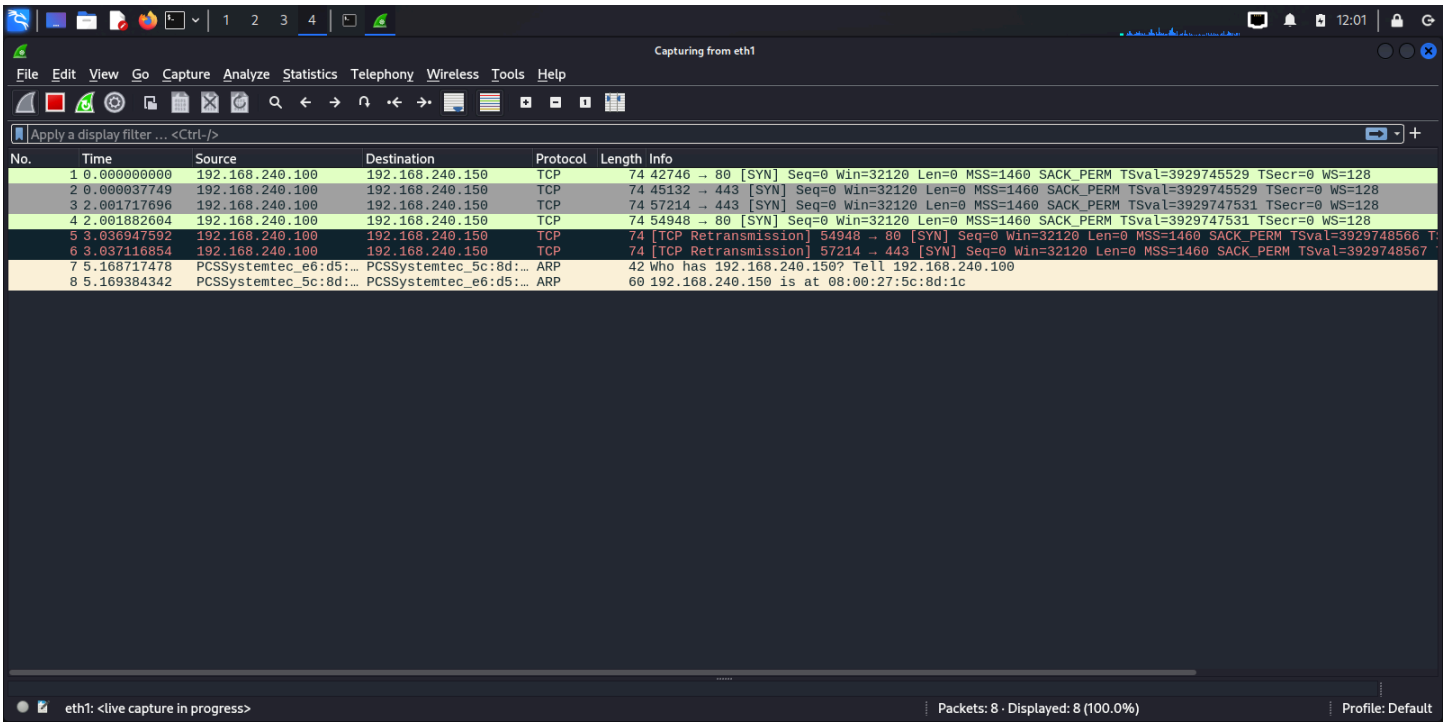
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -o dati.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:01 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.14 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sV -o dati.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:02 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds
```

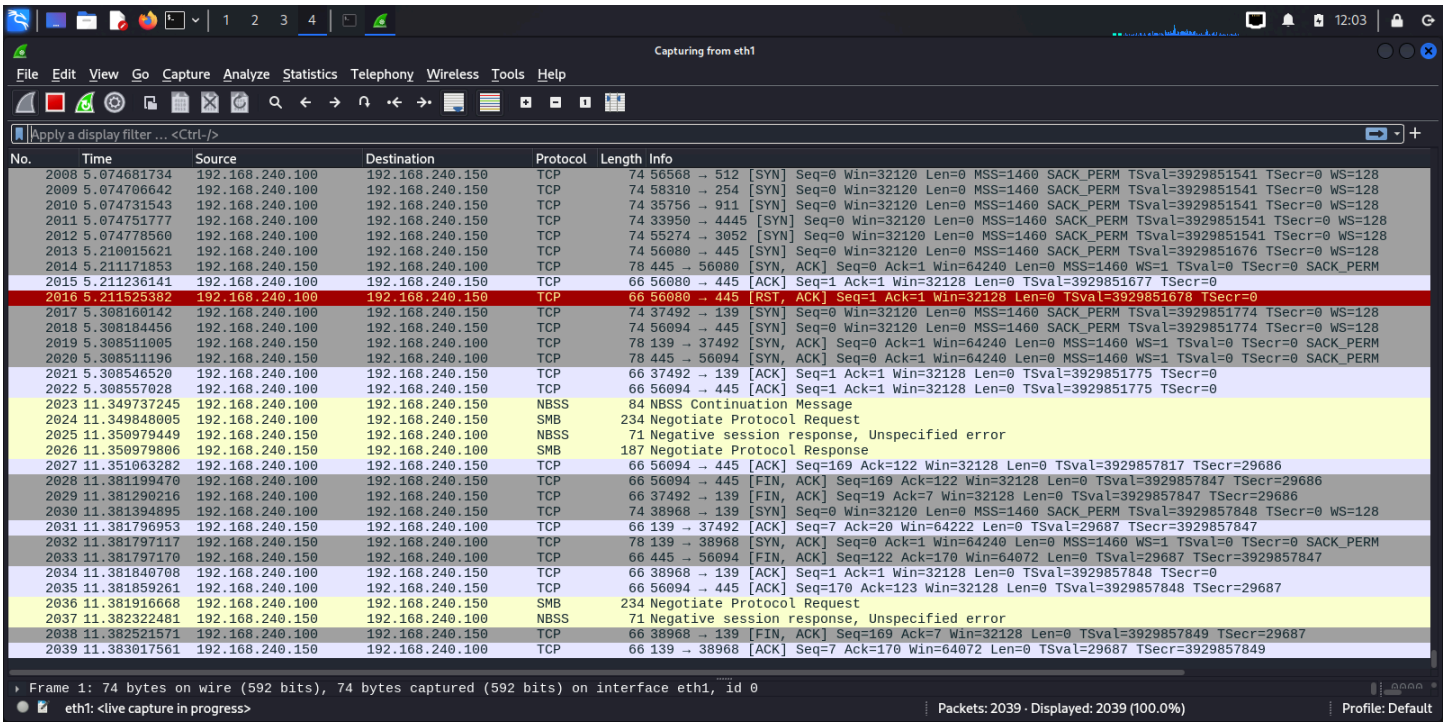
Possiamo notare che con la stessa scansione, **nmap** non trova nessun host.
Questo perche' la strutturazione di **nmap** e' fatta in modo tale da mandare una scansione solo dopo avere ottenuto dei pacchetti **ICMP** (Internet Control Message Protocol) o chiamata anche richiesta ping, ma dato che il firewall di Windows e' configurato per ignorare le richieste **ICMP**, giustamente **nmap** non manda la scansione.

Per risolvere questo problema, bisogna aggiungere un sotto comando di **nmap**, il **-Pn** che permette di avviare la scansione senza controllare i pacchetti **ICMP**.

Infatti possiamo notare che in questo modo ha trovato l'host, seppur con servizi in meno.

Osserviamo ora i due casi con **Wireshark**:





Notiamo nel primo caso che **wireshark** riceve pochissimi pacchetti proprio dovuto al fatto che **nmap** non ha trovato l'host, mentre nel secondo caso, possiamo notare invece la quantita' di pacchetti e quasi tutti contenenti richieste ignorate.

In particolare abbiamo ottenuto poche risposte **[ACK]**, pochissime **[RST, ACK]**, e tante 'non risposte', cioe' lasciate richieste **[SYN]**.

Questo in realta' ha senso, perche' dimostra che il firewall ha il compito di ignorare quante piu' possibili risposte per lasciare il dubbio all'attaccante.

Conclusione:

Questo breve esercizio dimostra che la presenza di un firewall, puo' fare la differenza in ambito sicurezza.

Lasciare sistemi in balia di possibili attacchi, non ha alcun senso a meno che non lo si fa per uso didattico, percio' consiglio di mantenere sempre attivi i firewall di sistema e mantenerli aggiornati.