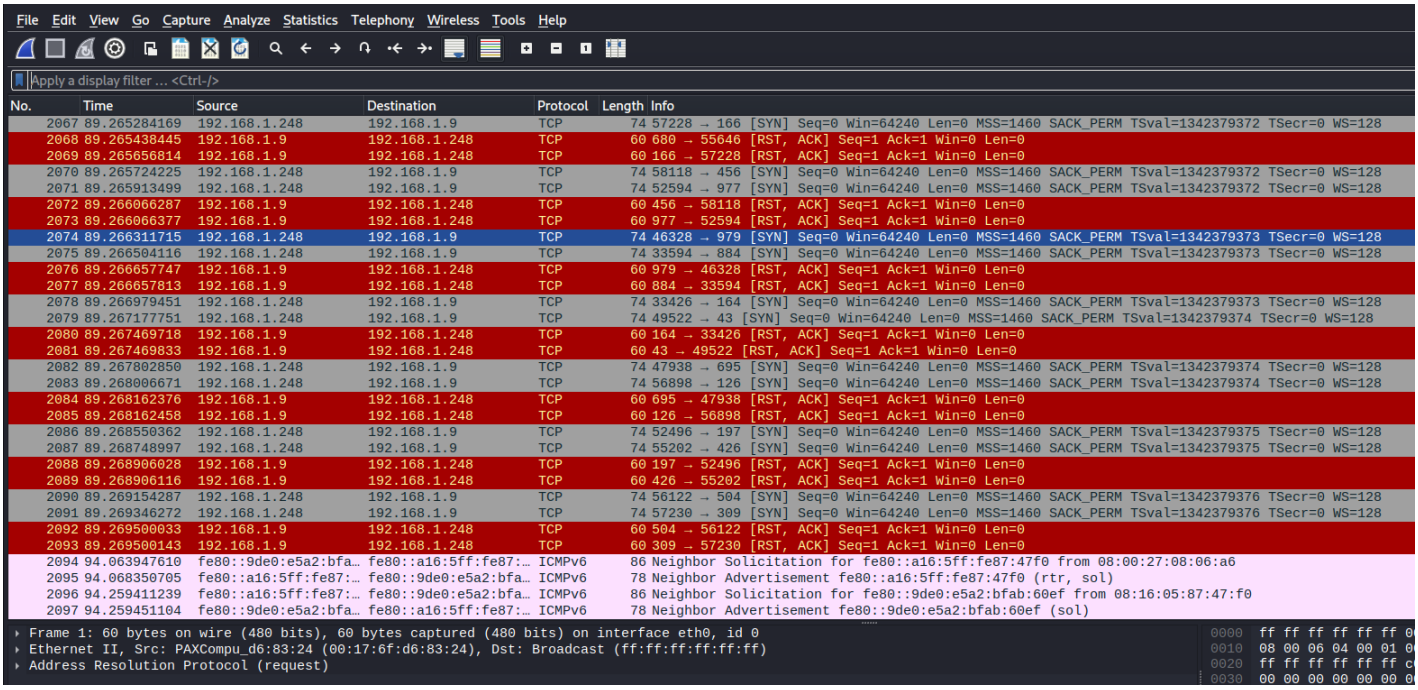
Nella scansione TCP delle porte well-known  dalla macchina kali (192.168.1.248) verso la macchina metasploitable (192.168.1.9) notiamo come la maggior parte delle richieste di connessione si interrompono (RST, ACK) perché le porte sono chiuse; mentre le porte aperte rispondono con pacchetto SYN portando a termine la connessione




```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-1024 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 12:51 EDT
Nmap scan report for kali.station (192.168.1.9)
Host is up (0.0017s 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

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

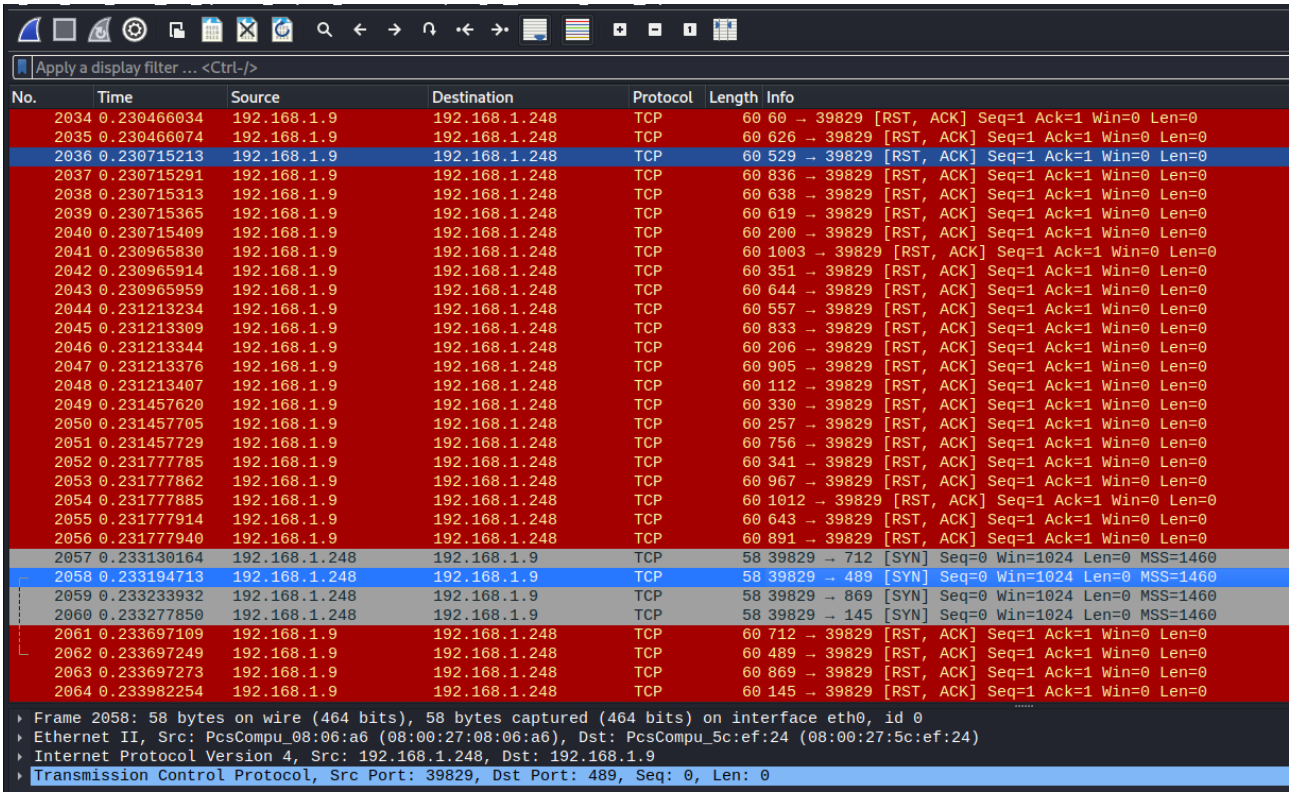
Nella scansione SYN delle porte well-known con switch -sS  le porte chiuse rispondono con il pacchetto RSK ACK e quindi la richiesta di connssione non viene conclusa, invece quelle aperte rispondo con il pacchetto SYN

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p 1-1024 192.168.1.9
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -p 1-1024 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 12:53 EDT
Nmap scan report for kali.station (192.168.1.9)
Host is up (0.0011s 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: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

┌──(root㉿kali)-[/home/kali]
└─# _
```




La differenza fra la scansione SYN e TCP è che la TCP stabilisce delle connessioni complete, mentre la SYN inizia l'handshake a 3 vie senza completare la connessione infatti anche nelle porte aperte la connessione MISS viene interrotta, è quindi migliore poiché viene rilevata più difficilmente dalla macchina attaccata.

Lo switch -A fornisce una scansione più approfondita che include la versione dei servizi, il sistema operativo, ci da quindi più informazioni.