CS0424IT

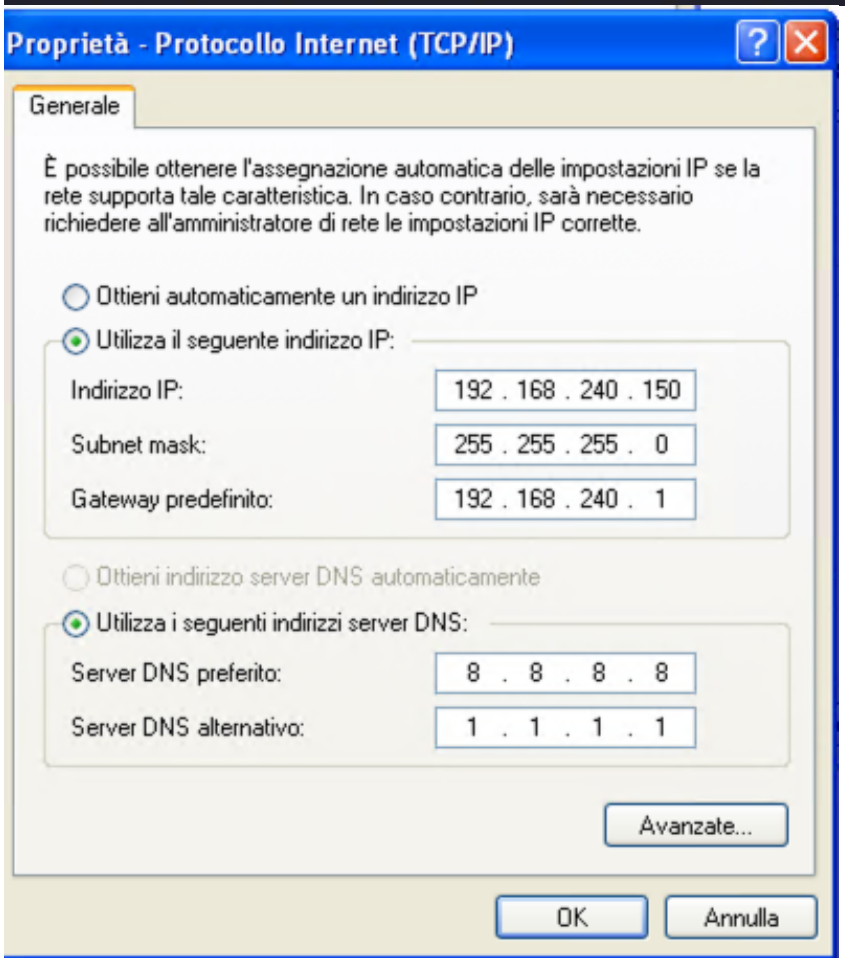
S9-L1

Ho iniziato configurando gli ip su kali e windows xp

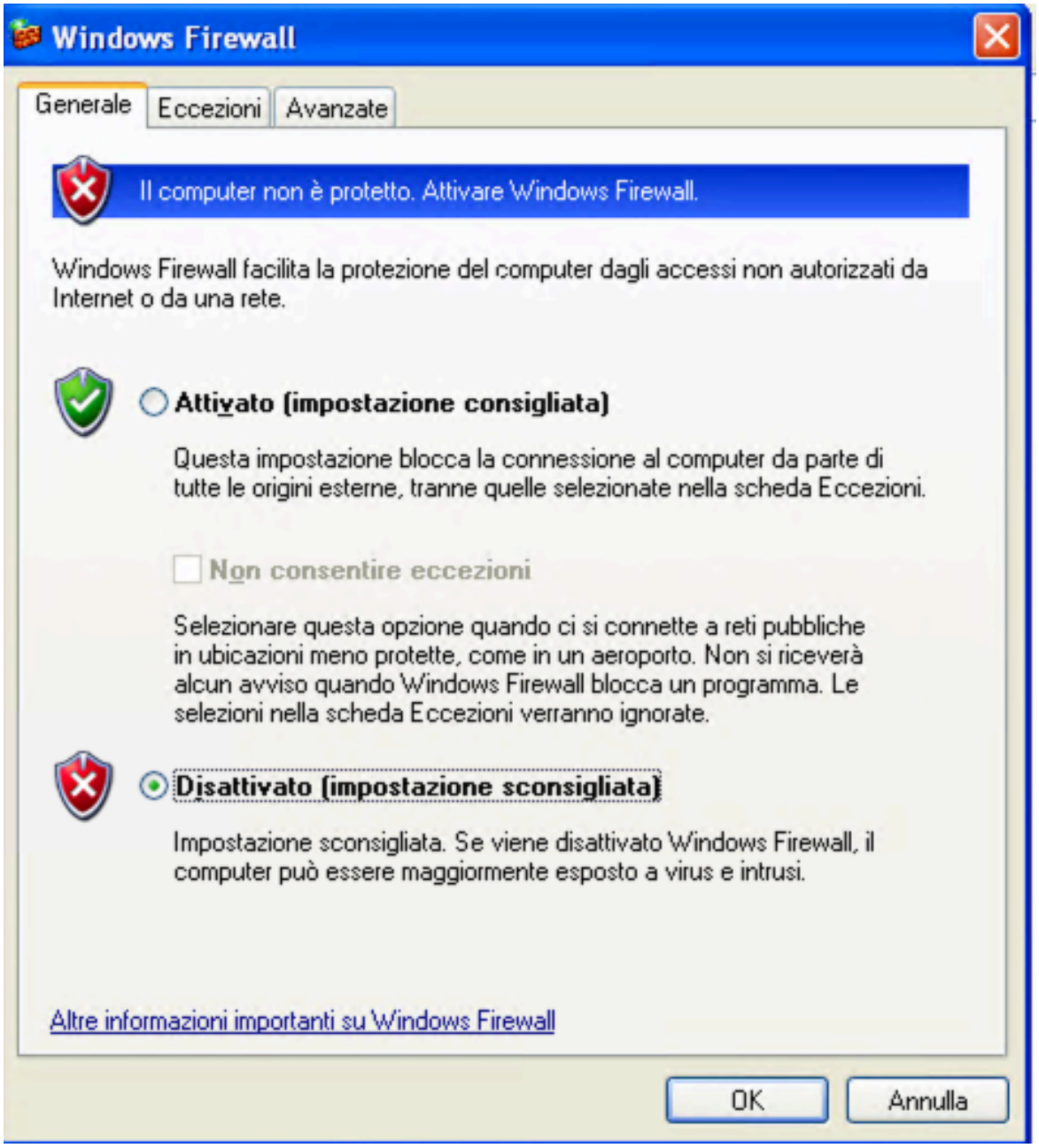
```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1b:0c:3a brd ff:ff:ff:ff:ff:ff
    inet 192.168.240.100/24 brd 192.168.240.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.708 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.351 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.374 ms
^C
── 192.168.240.150 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2051ms
rtt min/avg/max/mdev = 0.351/0.477/0.708/0.163 ms

┌──(kali㉿kali)-[~]
└─$ _
```



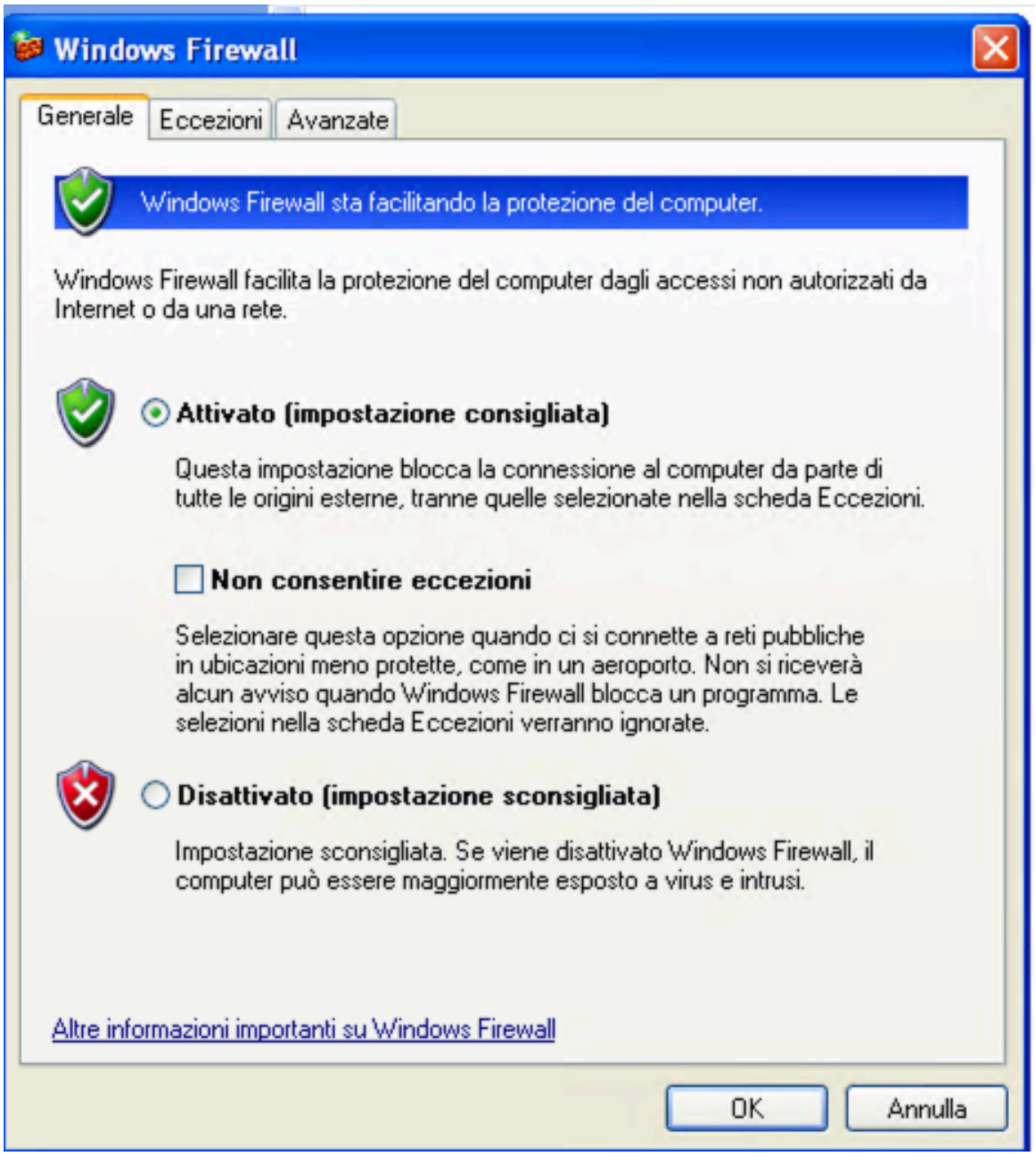
Ho disattivato il firewall su Windows xp



Ho eseguito una scansione con nmap con lo switch -sV e con un file di output

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -A 192.168.240.150 -o winxp_firewalloff
```

Poi ho attivato il firewall su windows xp e ho rieseguito la stessa scansione nmap, ovviamente cambiando il nome del file di output




```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.240.150 -o winxp_firewallon
```

Poi ho confrontato i due risultati

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat winxp_firewalloff
# Nmap 7.94SVN scan initiated Mon Jul 22 14:16:18 2024 as: nmap -sV -o winxp
_firewalloff 192.168.240.150
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disab
led. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.240.150
Host is up (0.00022s 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 at Mon Jul 22 14:16:25 2024 -- 1 IP address (1 host up) scanned
in 7.39 seconds
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat winxp_firewallon
# Nmap 7.94SVN scan initiated Mon Jul 22 14:18:13 2024 as: nmap -sV -o winxp
_firewallon 192.168.240.150
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disab
led. Try using --system-dns or specify valid servers with --dns-servers
# Nmap done at Mon Jul 22 14:18:16 2024 -- 1 IP address (0 hosts up) scanned
 in 3.15 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ _
```

Si può notare nel terminale a destra che con il firewall attivato non è stato possibile individuare le porte aperte/chiuse e i relativi servizi.
Per capire meglio si possono rieseguire le scansioni nei due casi e analizzarli con wireshark

Firewall disattivato:

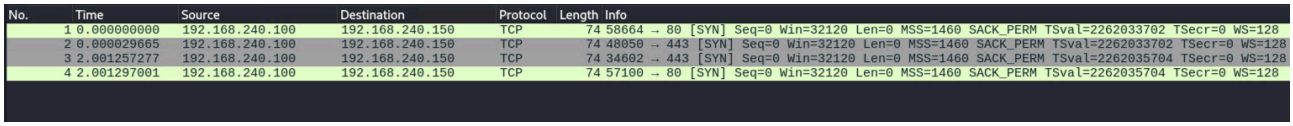
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_1b:0c:…	Broadcast	ARP	42	Who has 192.168.240.150? Tell 192.168.240.100
2	0.000368782	PCSSystemtec_5c:8d:…	PCSSystemtec_1b:0c:…	ARP	60	192.168.240.150 is at 08:00:27:5c:8d:1c
3	0.000372538	192.168.240.100	192.168.240.150	TCP	74	60918 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467078 TSecr=0 WS=128
4	0.000447990	192.168.240.100	192.168.240.150	TCP	74	44264 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467078 TSecr=0 WS=128
5	0.000666455	192.168.240.150	192.168.240.100	TCP	60	80 → 60918 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	0.000666519	192.168.240.150	192.168.240.100	TCP	60	443 → 44264 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.000828093	192.168.240.100	192.168.240.150	TCP	74	48430 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
8	0.000847283	192.168.240.100	192.168.240.150	TCP	74	46442 → 143 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
9	0.001013417	192.168.240.100	192.168.240.150	TCP	74	60216 → 111 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
10	0.001021555	192.168.240.100	192.168.240.150	TCP	74	42608 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
11	0.001022070	192.168.240.100	192.168.240.150	TCP	74	56540 → 53 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
12	0.001022380	192.168.240.100	192.168.240.150	TCP	74	41018 → 110 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
13	0.001095027	192.168.240.100	192.168.240.150	TCP	74	44270 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
14	0.001096543	192.168.240.100	192.168.240.150	TCP	74	54682 → 199 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
15	0.001096883	192.168.240.100	192.168.240.150	TCP	74	55210 → 5900 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
16	0.001097230	192.168.240.100	192.168.240.150	TCP	74	58214 → 995 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
17	0.001126782	192.168.240.150	192.168.240.100	TCP	78	445 → 48430 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
18	0.001126854	192.168.240.150	192.168.240.100	TCP	60	113 → 46442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	0.001137635	192.168.240.100	192.168.240.150	TCP	66	48430 → 445 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2260467079 TSecr=0
20	0.001188933	192.168.240.100	192.168.240.150	TCP	66	48430 → 445 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=2260467079 TSecr=0
21	0.001218225	192.168.240.100	192.168.240.150	TCP	74	50620 → 1025 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
22	0.001232574	192.168.240.100	192.168.240.150	TCP	74	60934 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
23	0.001244258	192.168.240.100	192.168.240.150	TCP	74	41456 → 3306 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
24	0.001255352	192.168.240.100	192.168.240.150	TCP	74	56612 → 8888 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2260467079 TSecr=0 WS=128
25	0.001281035	192.168.240.150	192.168.240.100	TCP	60	111 → 60216 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	0.001281166	192.168.240.150	192.168.240.100	TCP	78	135 → 42608 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
27	0.001281197	192.168.240.150	192.168.240.100	TCP	60	53 → 56540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	0.001281342	192.168.240.150	192.168.240.100	TCP	60	110 → 41018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	0.001281368	192.168.240.150	192.168.240.100	TCP	60	443 → 44270 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	0.001281394	192.168.240.150	192.168.240.100	TCP	60	199 → 54682 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Si può notare che la 192.168.240.100 (kali) effettua vari tentativi di connessione TCP SYN su varie porte (i pacchetti di colore grigio), mentre la macchina 192.168.240.150 (windows xp) risponde con pacchetti RST, ACK(i pacchetti di colore rosso).
Questo perchè che quelle porte sono chiuse ma senza un firewall che blocca attivamente questi tentativi.

Sulle porte aperte risponderà invece con SYN, ACK

192.168.240.100	192.168.240.150	TCP	74 41402 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PE
192.168.240.100	192.168.240.150	TCP	74 42332 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PE
192.168.240.100	192.168.240.150	TCP	74 34200 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PE
192.168.240.150	192.168.240.100	TCP	78 135 → 41402 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=14
192.168.240.150	192.168.240.100	TCP	78 139 → 42332 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=14
192.168.240.150	192.168.240.100	TCP	78 445 → 34200 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=14

Firewall attivato:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.240.100	192.168.240.150	TCP	74	58664 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2262033702 TSecr=0 WS=128
2	0.000029665	192.168.240.100	192.168.240.150	TCP	74	48050 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2262033702 TSecr=0 WS=128
3	2.001257277	192.168.240.100	192.168.240.150	TCP	74	34602 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2262035704 TSecr=0 WS=128
4	2.001297001	192.168.240.100	192.168.240.150	TCP	74	57100 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2262035704 TSecr=0 WS=128

In questo caso vengono catturate solo le richieste SYN da parte di 192.168.240.10 (kali) ma non ricevono alcuna risposta perchè il firewall le riconosce e le blocca attivamente impedendo alla macchina 192.168.240.150 di rispondere con pacchetti SYN, ACK o RST, ACK ai tentativi di connessione della macchina 192.168.240.100, in questo caso infatti nmap ha terminato subito la scansione non vedendo risposte.
Il firewall ha impedito alla macchina attaccante di poter conoscere lo stato delle porte e i servizi, questo è importante e porta alcuni vantaggi tra cui:

- La riduzione della superficie di attacco.
- Avere maggior tempo per individuare e rispondere ad un potenziale attacco.
- Difesa contro strumenti automatizzati