

Esercizio D1 W9

Firewall

Controllo che sia disabilitato su XP



Prova ping

```
(alessio@alessio-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=1.06 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.833 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.972 ms
^C
--- 192.168.240.150 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.833/0.954/1.058/0.092 ms
```

Scan Nmap

```
(alessio@alessio-kali)-[~/Desktop/Esercizi/Week9]
$ nmap -sV -T5 192.168.240.150 -o nmap.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 07:11 CDT
Nmap scan report for 192.168.240.150 (192.168.240.150)
Host is up (0.00083s 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 7.38 seconds
```

Riattivo il firewall su xp

contrassegnate con il valore Attivato. Se le impostazioni hanno un valore diverso da Attivato, seguire i consigli forniti. È possibile tornare al Centro sicurezza PC in qualsiasi momento, tramite il Pannello di controllo.

[Novità di Windows che facilitano la protezione del computer](#)



Rieseguo la scansione con Nmap

```
(alessio@kali)-[~/Desktop/Esercizi/Week9]
$ nmap -sV -T5 192.168.240.150 -o nmap2.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 07:11 CDT
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 1.64 seconds
```

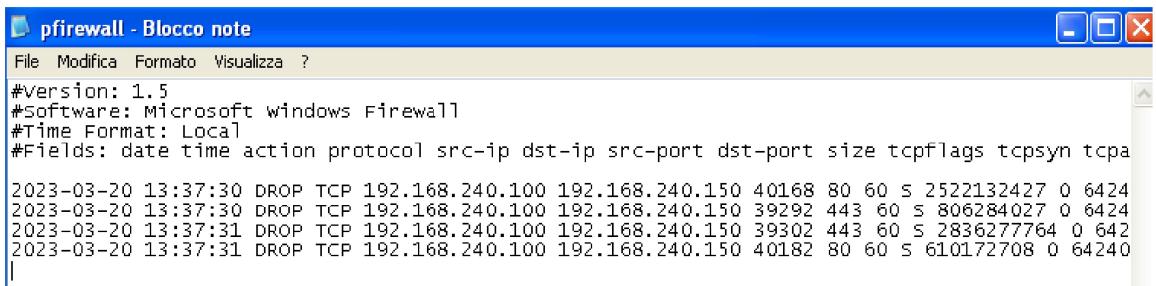
Abilito i log



Rieseguo la scansione

```
(alessio@kali)-[~/Desktop/Esercizi/Week9]
$ nmap -sV -T5 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 07:37 CDT
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 1.64 seconds
```

Si nota che il firewall blocca i ping di nmap, quindi non riesce a capire se l'host sia up



The screenshot shows a Windows Notepad window titled "pfirewall - Blocco note". The menu bar includes "File", "Modifica", "Formato", "Visualizza", and "?". The content of the window is a log of firewall events:

```
#Version: 1.5
#Software: Microsoft windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpa

2023-03-20 13:37:30 DROP TCP 192.168.240.100 192.168.240.150 40168 80 60 S 2522132427 0 6424
2023-03-20 13:37:30 DROP TCP 192.168.240.100 192.168.240.150 39292 443 60 S 806284027 0 6424
2023-03-20 13:37:31 DROP TCP 192.168.240.100 192.168.240.150 39302 443 60 S 2836277764 0 642
2023-03-20 13:37:31 DROP TCP 192.168.240.100 192.168.240.150 40182 80 60 S 610172708 0 64240
```

Come si può notare sono rimasti i log delle connessioni tentate dal esterno