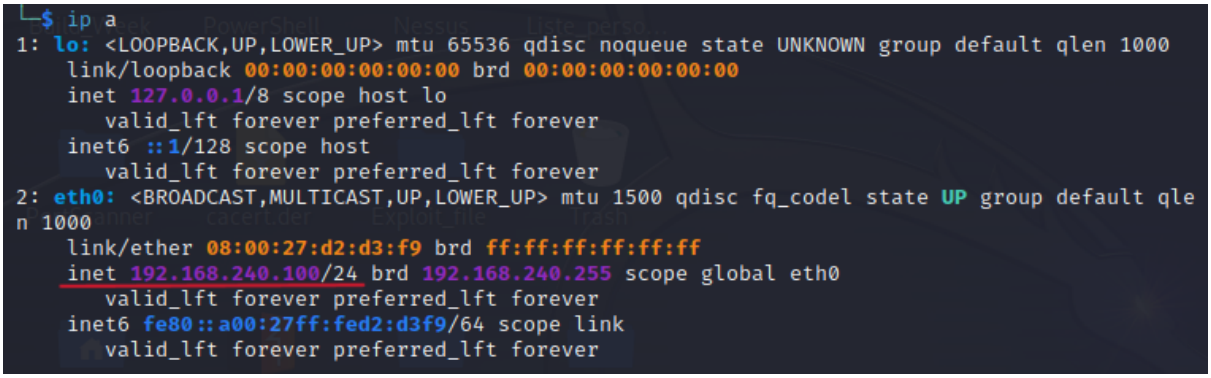
Esercizio 20-03

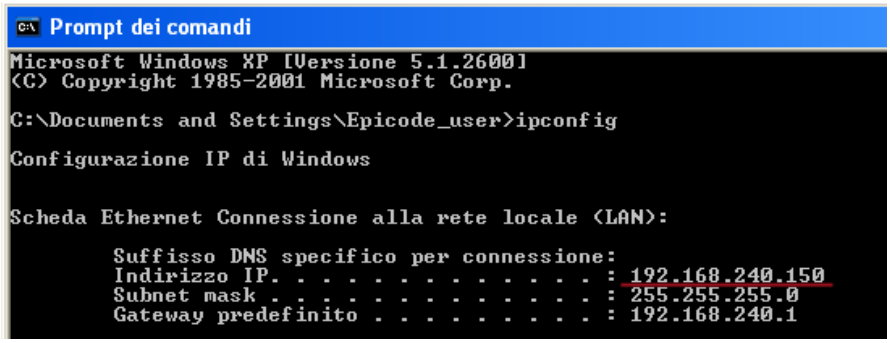
Traccia: eseguire delle scansioni nmap con Windows XP come target ed evidenziare le differenze nei log di Windows con Firewall spento a attivo.

Richiesta:

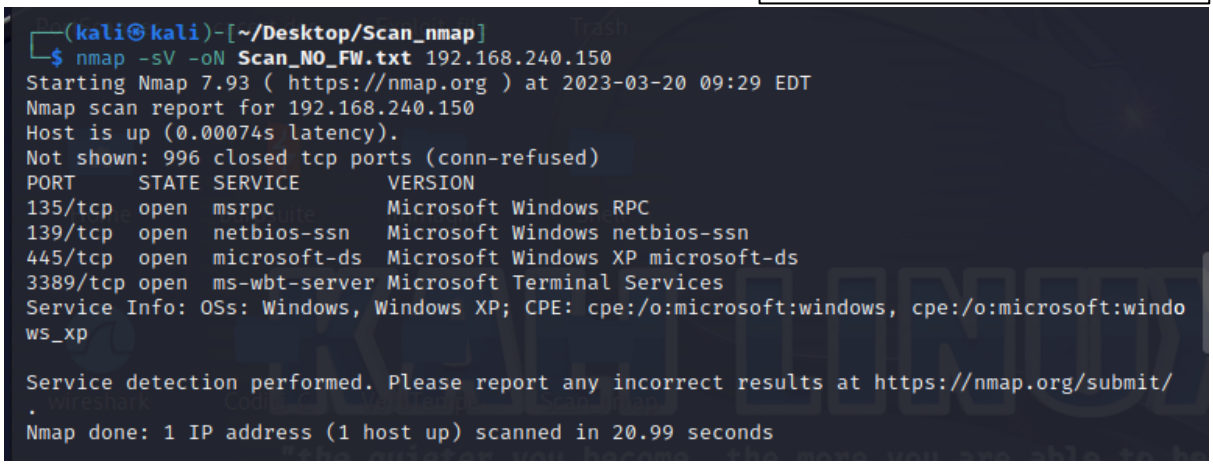
- IP Kali:192.168.240.100
- IP Windows XP:192.168.240.150

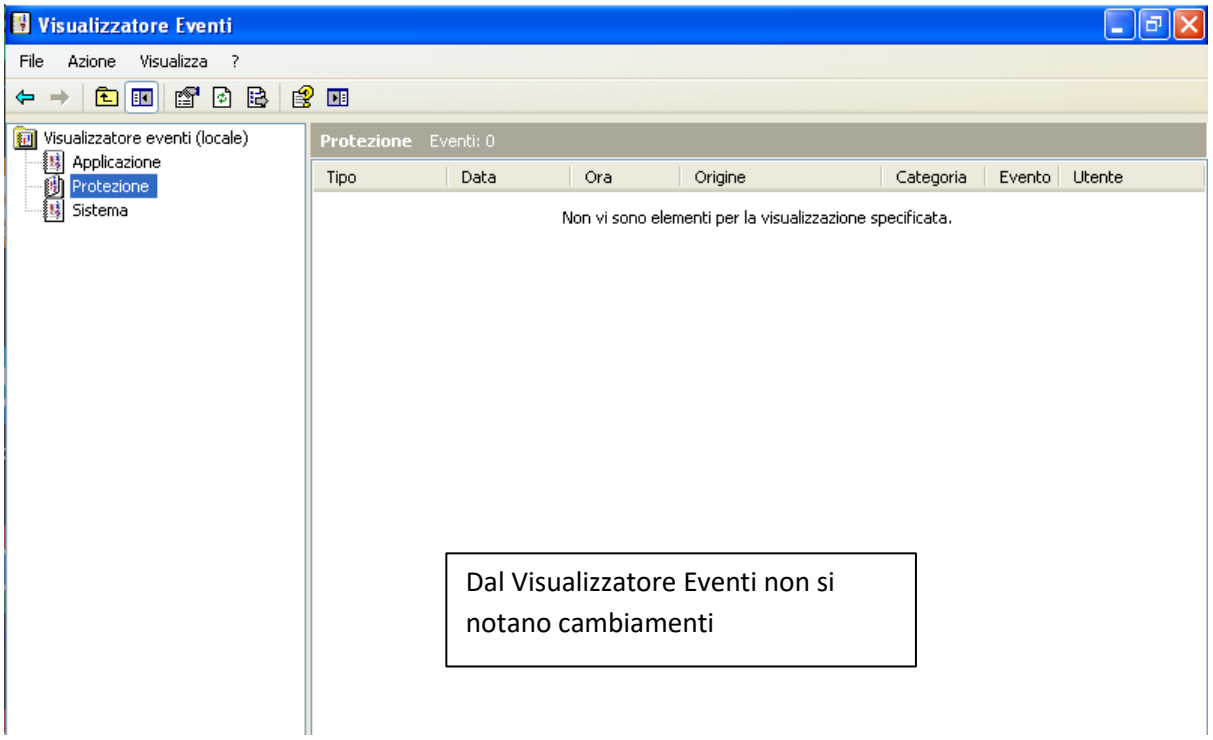
Configurazione degli IP di Kali e Windows XP





Lancio di una scansione nmap con Windows XP con il Firewall spento



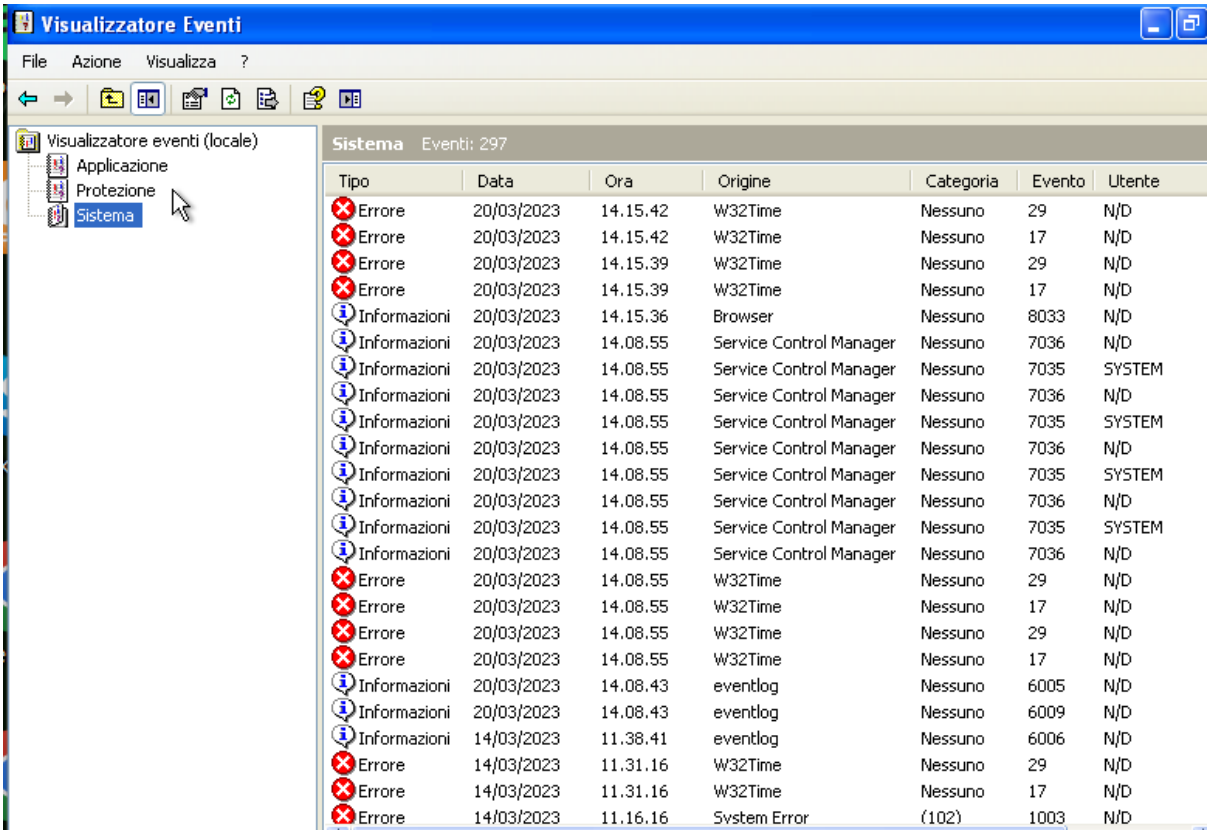


Protezione Eventi: 0

Tipo	Data	Ora	Origine	Categoria	Evento	Utente

Non vi sono elementi per la visualizzazione specificata.

Dal Visualizzatore Eventi non si notano cambiamenti

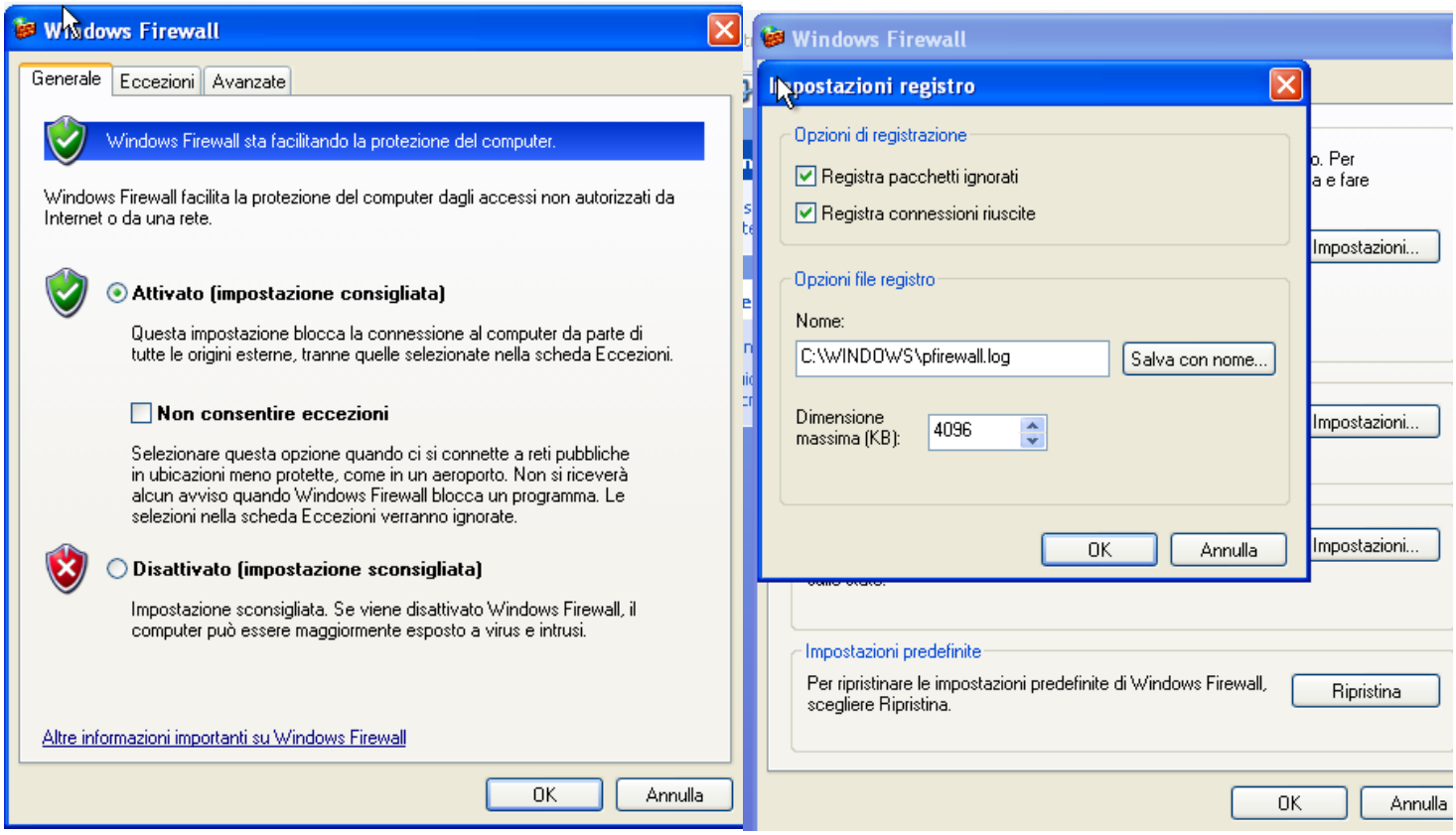


Sistema Eventi: 297

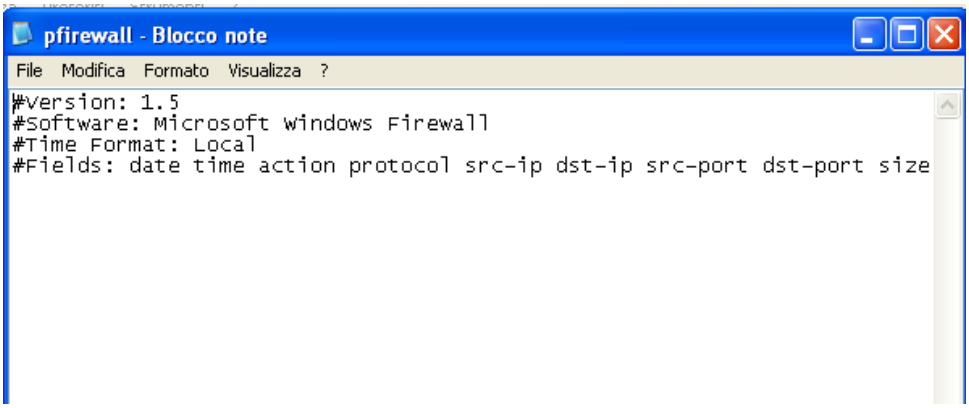
Tipo	Data	Ora	Origine	Categoria	Evento	Utente
Errore	20/03/2023	14.15.42	W32Time	Nessuno	29	N/D
Errore	20/03/2023	14.15.42	W32Time	Nessuno	17	N/D
Errore	20/03/2023	14.15.39	W32Time	Nessuno	29	N/D
Errore	20/03/2023	14.15.39	W32Time	Nessuno	17	N/D
Informazioni	20/03/2023	14.15.36	Browser	Nessuno	8033	N/D
Informazioni	20/03/2023	14.08.55	Service Control Manager	Nessuno	7036	N/D
Informazioni	20/03/2023	14.08.55	Service Control Manager	Nessuno	7035	SYSTEM
Informazioni	20/03/2023	14.08.55	Service Control Manager	Nessuno	7036	N/D
Informazioni	20/03/2023	14.08.55	Service Control Manager	Nessuno	7035	SYSTEM
Informazioni	20/03/2023	14.08.55	Service Control Manager	Nessuno	7036	N/D
Informazioni	20/03/2023	14.08.55	Service Control Manager	Nessuno	7035	SYSTEM
Informazioni	20/03/2023	14.08.55	Service Control Manager	Nessuno	7036	N/D
Informazioni	20/03/2023	14.08.55	Service Control Manager	Nessuno	7035	SYSTEM
Informazioni	20/03/2023	14.08.55	Service Control Manager	Nessuno	7036	N/D
Errore	20/03/2023	14.08.55	W32Time	Nessuno	29	N/D
Errore	20/03/2023	14.08.55	W32Time	Nessuno	17	N/D
Errore	20/03/2023	14.08.55	W32Time	Nessuno	29	N/D
Errore	20/03/2023	14.08.55	W32Time	Nessuno	17	N/D
Informazioni	20/03/2023	14.08.43	eventlog	Nessuno	6005	N/D
Informazioni	20/03/2023	14.08.43	eventlog	Nessuno	6009	N/D
Informazioni	14/03/2023	11.38.41	eventlog	Nessuno	6006	N/D
Errore	14/03/2023	11.31.16	W32Time	Nessuno	29	N/D
Errore	14/03/2023	11.31.16	W32Time	Nessuno	17	N/D
Errore	14/03/2023	11.16.16	System Error	(102)	1003	N/D

Accensione del Firewall si Windows XP

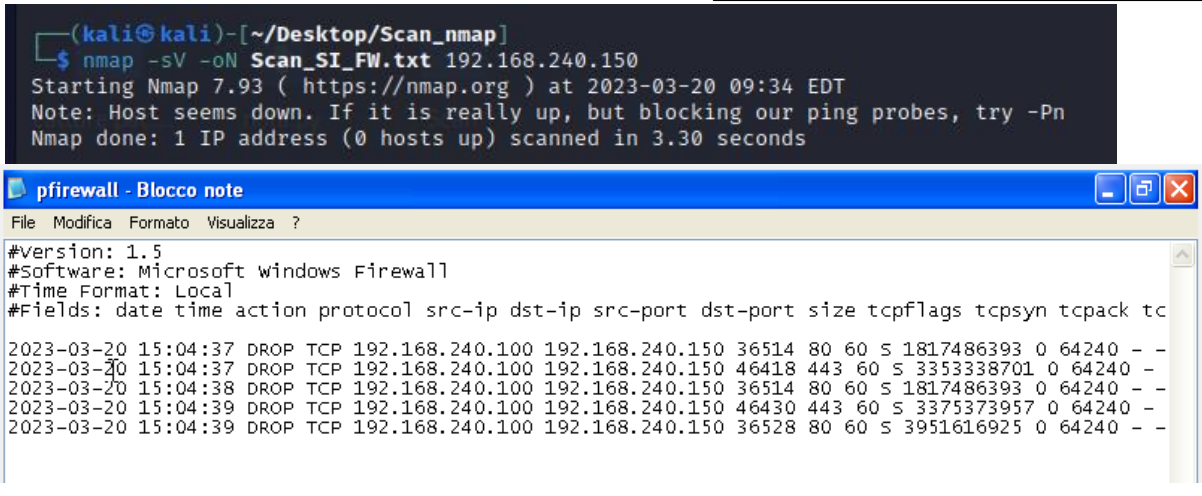
Abilitare la registrazione dei pacchetti in un file “pfirewall” nella cartella WINDOWS



Una volta aperto il file “pfirewall”, questo è il contenuto del log ancora “pulito”



Log post-scansione di nmap che non ha trovato l’host, reputandolo “down”



Scansione con utilizzo dello switch -Pn che permette di considerare tutti gli host come up, saltando la fase di host discovery

```
┌──(kali㉿kali)-[~/Desktop/Scan_nmap]
└─$ nmap -sV -Pn -oN Scan_SI_FW.txt 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:36 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0019s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows XP; CPE: 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 26.31 seconds
```

Log post-scansione con switch -Pn

pfirewall - Blocco note

File Modifica Formato Visualizza ?

```
#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 tcpack tc

2023-03-20 15:04:37 DROP TCP 192.168.240.100 192.168.240.150 36514 80 60 S 1814486393 0 64240 - -
2023-03-20 15:04:37 DROP TCP 192.168.240.100 192.168.240.150 46418 443 60 S 3333338701 0 64240 -
2023-03-20 15:04:38 DROP TCP 192.168.240.100 192.168.240.150 36514 80 60 S 1814486393 0 64240 - -
2023-03-20 15:04:39 DROP TCP 192.168.240.100 192.168.240.150 46430 443 60 S 3333373957 0 64240 -
2023-03-20 15:04:39 DROP TCP 192.168.240.100 192.168.240.150 36528 80 60 S 3951616925 0 64240 - -
2023-03-20 15:06:02 DROP TCP 192.168.240.100 192.168.240.150 41942 110 60 S 1736746497 0 64240 -
2023-03-20 15:06:02 DROP TCP 192.168.240.100 192.168.240.150 48770 445 60 S 2172723773 0 64240 -
2023-03-20 15:06:02 DROP TCP 192.168.240.100 192.168.240.150 54430 587 60 S 3294165865 0 64240 -
2023-03-20 15:06:02 OPEN-INBOUND TCP 192.168.240.100 192.168.240.150 49270 3389 - - - - - - - - -
2023-03-20 15:06:02 DROP TCP 192.168.240.100 192.168.240.150 33742 135 60 S 672218773 0 64240 - -
2023-03-20 15:06:02 DROP TCP 192.168.240.100 192.168.240.150 55626 3306 60 S 1334312181 0 64240 -
2023-03-20 15:06:02 DROP TCP 192.168.240.100 192.168.240.150 44522 139 60 S 1543038124 0 64240 -
2023-03-20 15:06:02 DROP TCP 192.168.240.100 192.168.240.150 54812 25 60 S 2918138869 0 64240 - -
2023-03-20 15:06:02 DROP TCP 192.168.240.100 192.168.240.150 55332 111 60 S 1818479874 0 64240 -
2023-03-20 15:06:02 DROP TCP 192.168.240.100 192.168.240.150 47168 993 60 S 1212100478 0 64240 -
2023-03-20 15:06:02 CLOSE TCP 192.168.240.150 192.168.240.100 3389 49270 - - - - - - - - -
2023-03-20 15:06:02 DROP TCP 192.168.240.100 192.168.240.150 45798 8080 60 S 705029637 0 64240 -
2023-03-20 15:06:02 DROP TCP 192.168.240.100 192.168.240.150 52386 554 60 S 614050843 0 64240 - -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 39464 554 60 S 199196522 0 64240 - -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 44028 8080 60 S 2520668233 0 64240 -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 42096 993 60 S 2819857380 0 64240 -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 60210 111 60 S 2713434494 0 64240 -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 52598 25 60 S 288601674 0 64240 - -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 44184 139 60 S 1276074200 0 64240 -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 39190 3306 60 S 840964459 0 64240 -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 51838 135 60 S 4032321916 0 64240 -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 57634 587 60 S 118264017 0 64240 - -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 37246 445 60 S 3537938248 0 64240 -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 35808 110 60 S 692736399 0 64240 - -
2023-03-20 15:06:04 OPEN-INBOUND TCP 192.168.240.100 192.168.240.150 56078 3389 - - - - - - - - -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 55272 1025 60 S 4148211928 0 64240 -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 40376 256 60 S 1490625412 0 64240 -
2023-03-20 15:06:04 DROP TCP 192.168.240.100 192.168.240.150 35404 1723 60 S 466553438 0 64240 -
```

La differenza tra Windows XP con Firewall ON e Firewall OFF è il comportamento a seguito di richieste fatte da un esterno: con Firewall OFF il sistema risponde alle richieste che arrivano (non filtrate) e non ne tiene traccia; con Firewall ON il sistema risponde (con risposte filtrate dal Firewall) a richieste (Filtrate dal Firewall) registrate in un file .log.