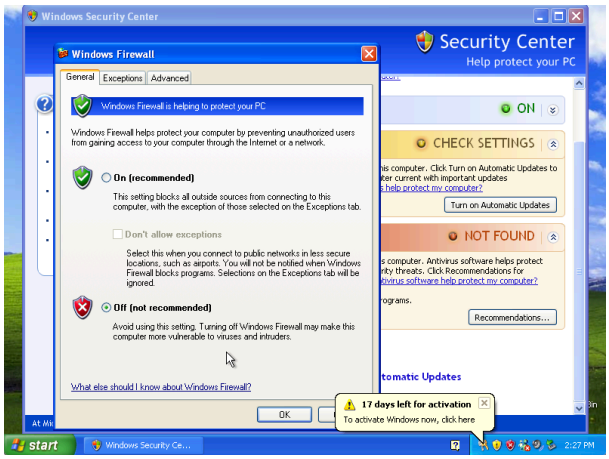
# 1.SOC Intro.

Modifica degli indirizzi ip di Kali Linux e Windows XP
Kali 192.168.240.100
XP 192.168.240.150

Prova di ping da Kali su XP

```
┌──(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=6.38 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=2.63 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=2.84 ms
^C
── 192.168.240.150 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 2.625/3.947/6.375/1.718 ms
```

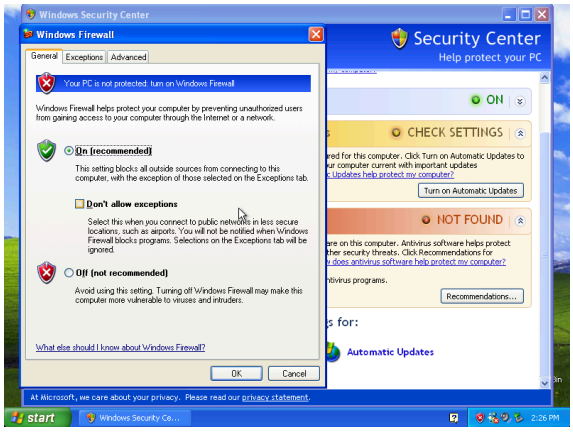
Disattivazione del firewall Windows




Successivamente utilizziamo nmap da Kali per effettuare una scansione di Windows

```
kali@kali: ~
File  Azioni  Modifica  Visualizza  Aiuto
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 14:28 CET
Nmap scan report for 192.168.240.150
Host is up (0.0022s 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 7.50 seconds
```

Attivazione del firewall Windows



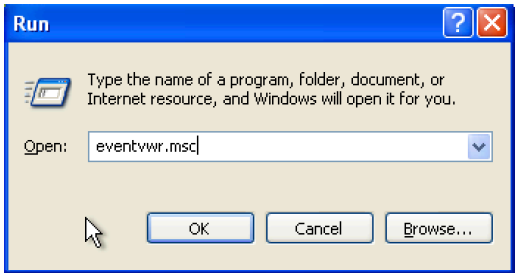

Scansione con nmap

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 14:29 CET
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 3.15 seconds
```

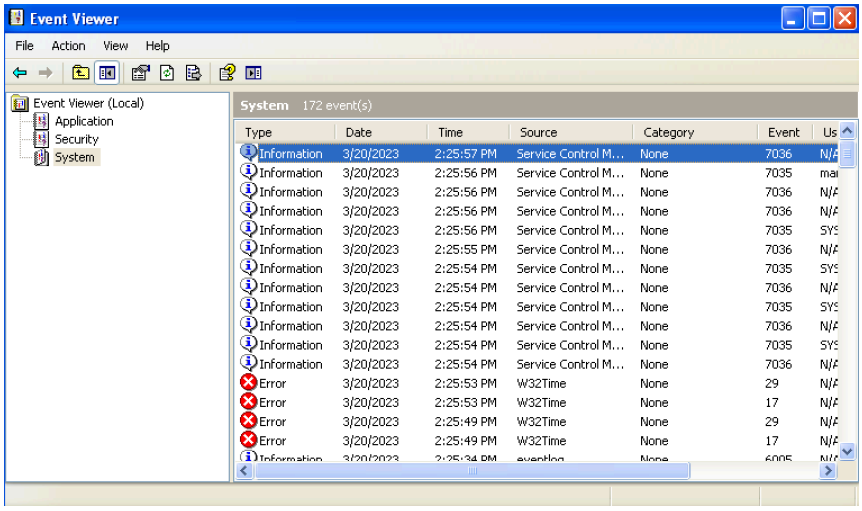
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 14:30 CET
Stats: 0:01:43 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 51.00% done; ETC: 14:33 (0:01:39 remaining)
Stats: 0:01:44 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 51.50% done; ETC: 14:33 (0:01:38 remaining)
Stats: 0:01:48 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 53.50% done; ETC: 14:33 (0:01:34 remaining)
Stats: 0:01:49 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 54.00% done; ETC: 14:33 (0:01:34 remaining)
Stats: 0:03:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 98.50% done; ETC: 14:33 (0:00:03 remaining)
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 201.83 seconds
```

Le differenze principali che troviamo nei due casi è il fatto che attraverso il firewall disattivato la scansione ha successo e possiamo riscontrare le porte ed i servizi attivi sulla macchina target a differenza del firewall attivo che indipendentemente dal scansione con o senza ping, non ci riporta nessun risultato utile se non l'informazione che l'host sia attivo.

Una volta completate le scansioni possiamo ora andare a controllare i log di Windows attraverso il seguente comando:




La schermata che ci viene riportata è la seguente.




In questo caso troviamo i log file che contengono le operazioni effettuate da un utente o macchina in ordine cronologico.