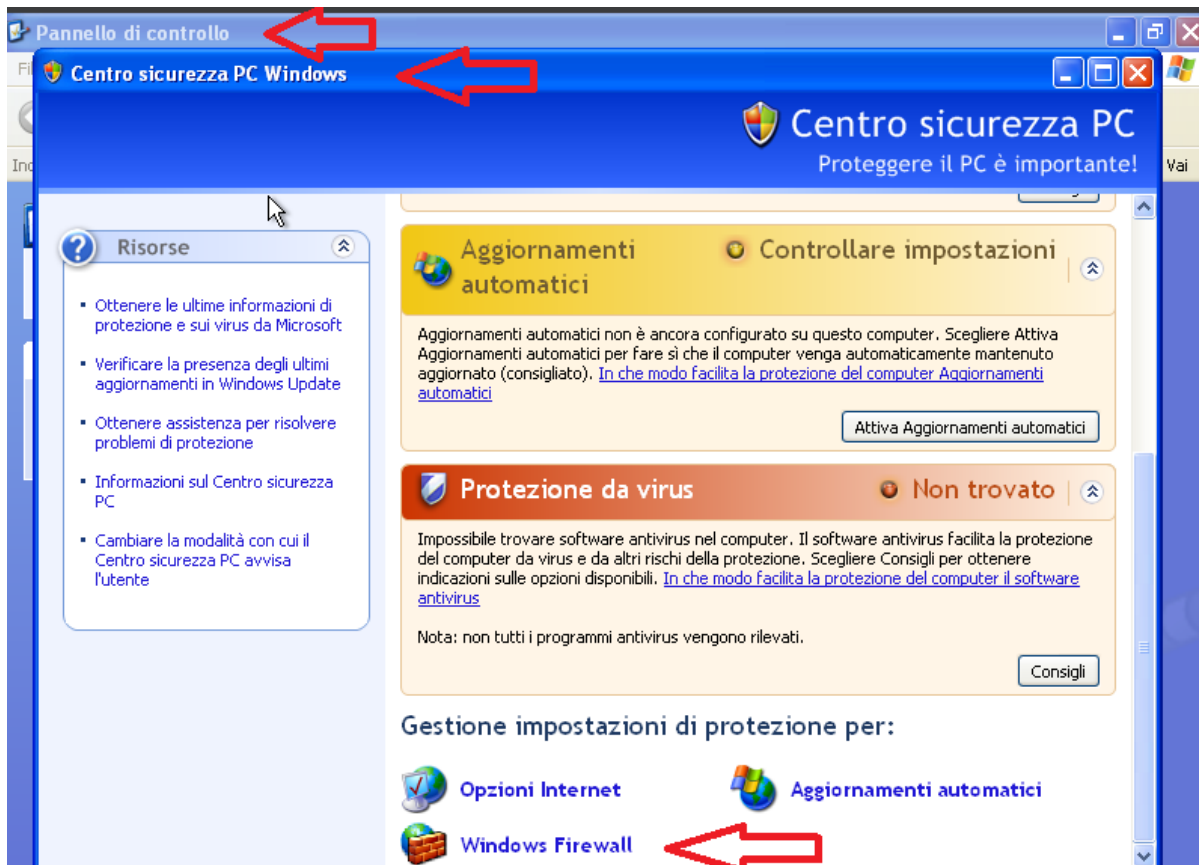
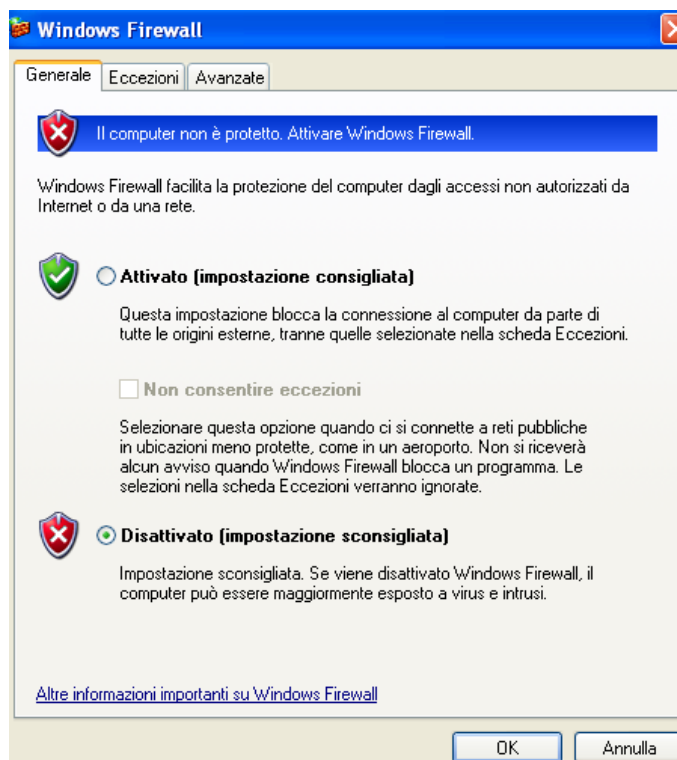


Ora passeremo all'esercizio, quindi dopo aver settato il Firewall da : **Pannello di Controllo -> Centro Sicurezza PC Windows -> Windows Firewall**



Ci apparirà la finestra del Firewall che noi andremo a disattivare

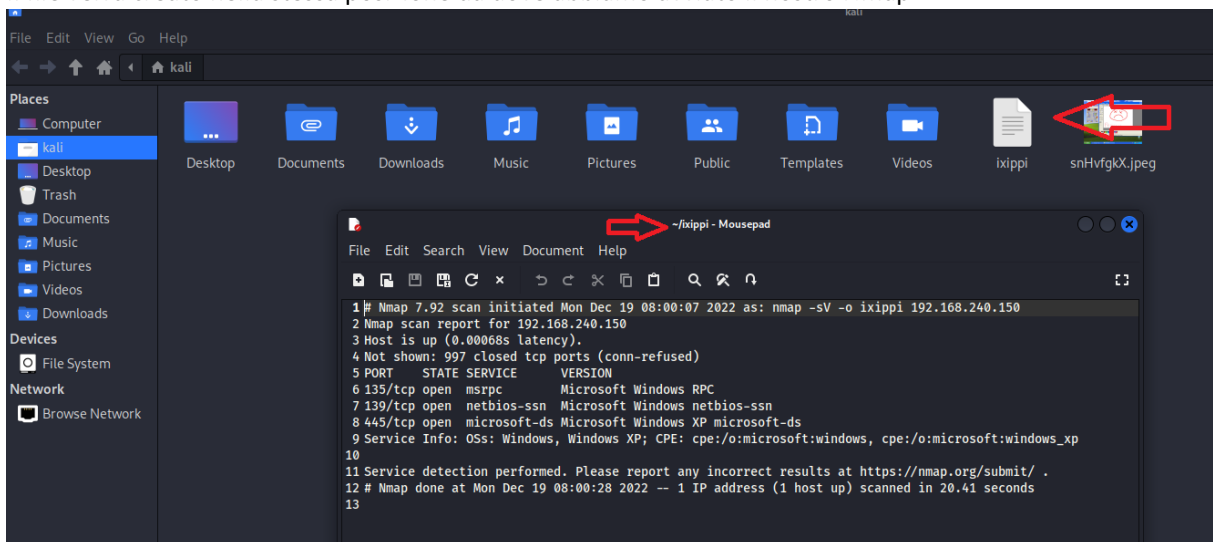


Ora non ci resta che effettuare il nostro **Nmap sV -o ixippi 192.168.240.150** dove -o ixippi sarà il nome del file log che Nmap creerà

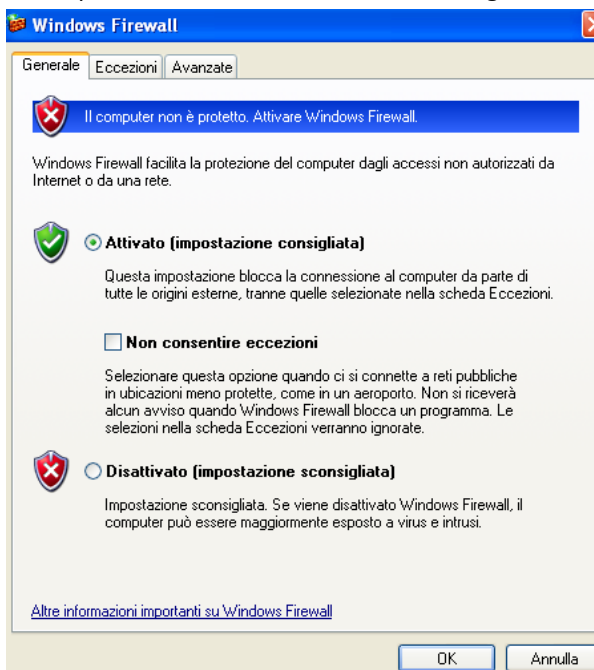
```
(kali㉿kali)-[~]
$ nmap -sV -o ixippi 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:00 EST
Nmap scan report for 192.168.240.150
Host is up (0.00068s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          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 20.41 seconds
```

Il file verrà creato nella stessa posizione da dove abbiamo avviato il nostro Nmap



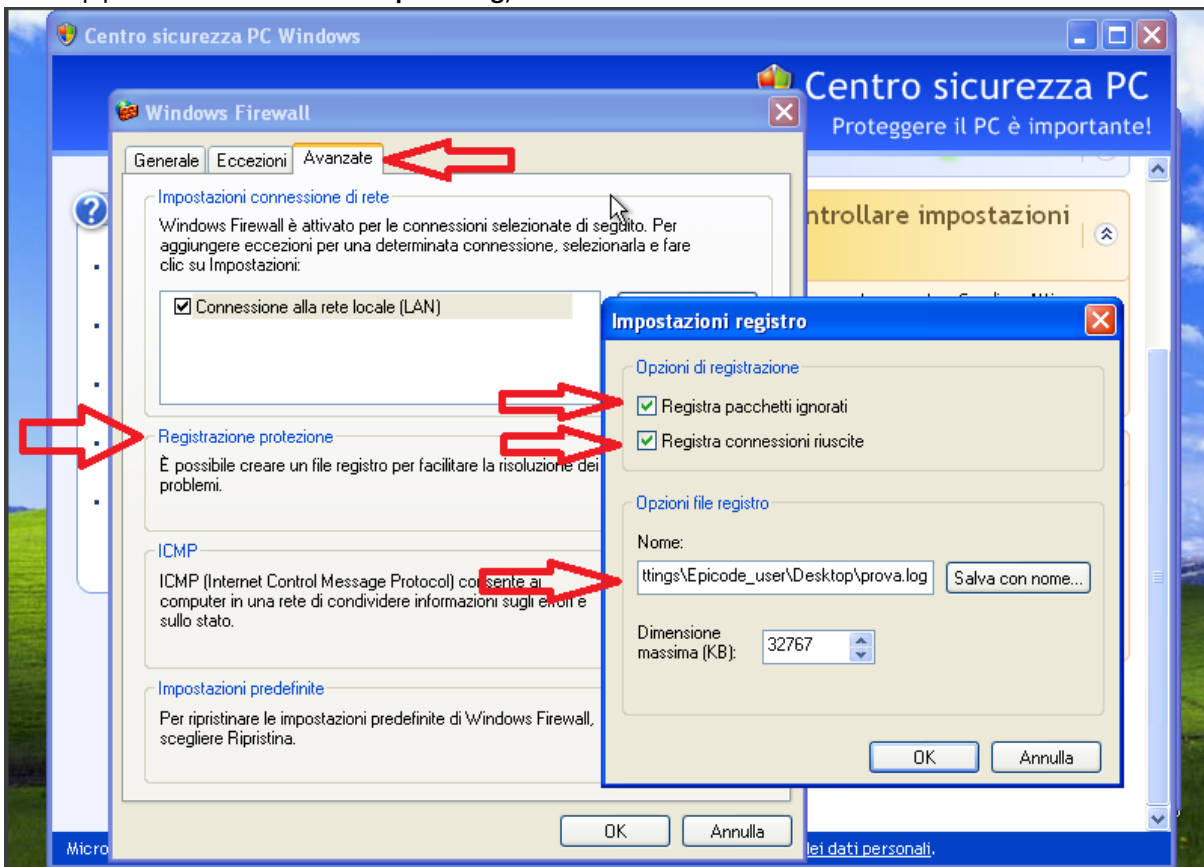
Come possiamo vedere ci verrà creato il Log della nostra scansione precedentemente fatta con Nmap, mentre se attiveremo il Firewall di Windows come abbiamo visto precedentemente



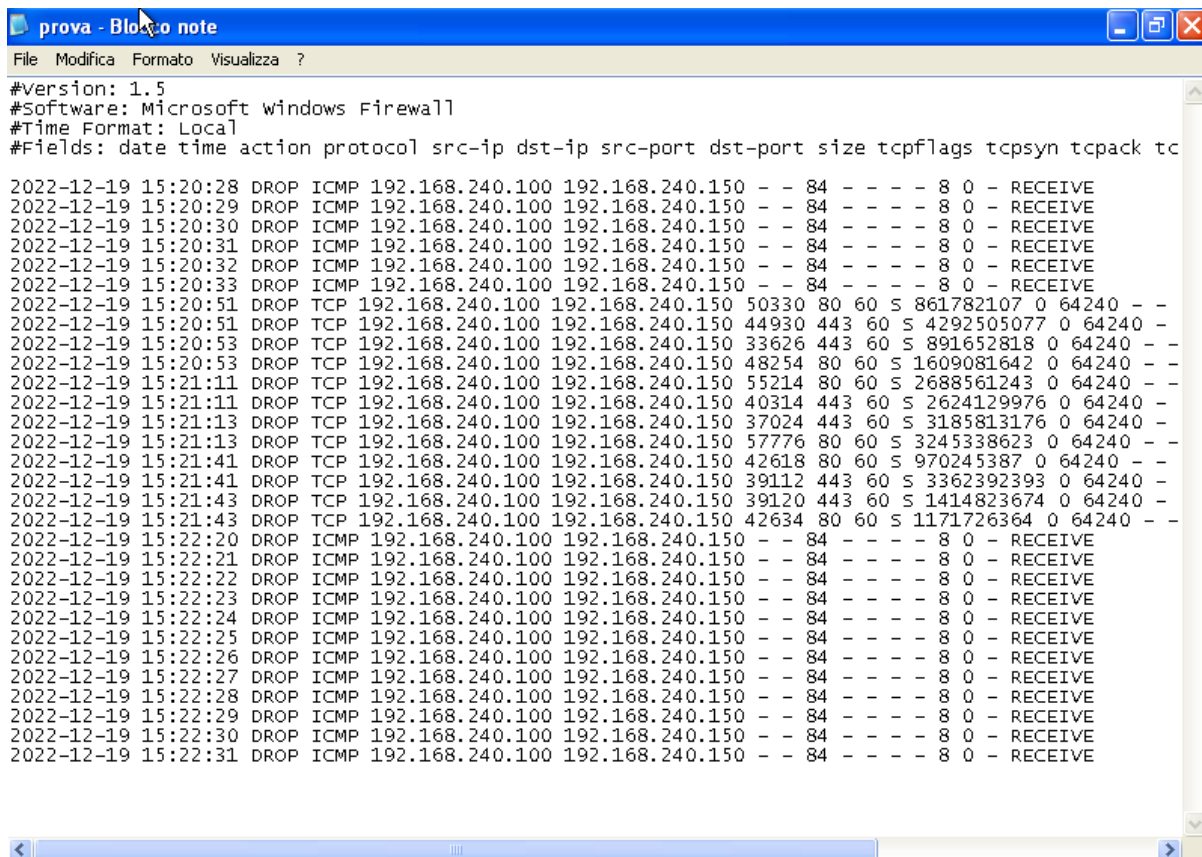
Potremmo notare come la nostra scansione verrà bloccata, impedendoci l'accesso alla scansione di Xp, non mostrando più alcuna informazione sulla macchina

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:05 EST  
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 3.23 seconds
```

Ma andando nelle impostazioni **Avanzate** del nostro Firewall, poi su **Registrazione Protezione** e sputando le due caselle che ci si presentano davanti ci verrà creato un file Log ( In questo caso è stata creato sul Desktop per comodità con il nome **prova.log**)



Il File viene creato automaticamente quando il Firewall è attivo, registrando tutto quello che avviene attraverso la nostra connessione



```
#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

2022-12-19 15:20:28 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:20:29 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:20:30 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:20:31 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:20:32 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:20:33 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:20:51 DROP TCP 192.168.240.100 192.168.240.150 50330 80 60 S 861782107 0 64240 - -
2022-12-19 15:20:51 DROP TCP 192.168.240.100 192.168.240.150 44930 443 60 S 4292505077 0 64240 - -
2022-12-19 15:20:53 DROP TCP 192.168.240.100 192.168.240.150 33626 443 60 S 891652818 0 64240 - -
2022-12-19 15:20:53 DROP TCP 192.168.240.100 192.168.240.150 48254 80 60 S 1609081642 0 64240 - -
2022-12-19 15:21:11 DROP TCP 192.168.240.100 192.168.240.150 55214 80 60 S 2688561243 0 64240 - -
2022-12-19 15:21:11 DROP TCP 192.168.240.100 192.168.240.150 40314 443 60 S 2624129976 0 64240 - -
2022-12-19 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 37024 443 60 S 3185813176 0 64240 - -
2022-12-19 15:21:13 DROP TCP 192.168.240.100 192.168.240.150 57776 80 60 S 3245338623 0 64240 - -
2022-12-19 15:21:41 DROP TCP 192.168.240.100 192.168.240.150 42618 80 60 S 970245387 0 64240 - -
2022-12-19 15:21:41 DROP TCP 192.168.240.100 192.168.240.150 39112 443 60 S 3362392393 0 64240 - -
2022-12-19 15:21:43 DROP TCP 192.168.240.100 192.168.240.150 39120 443 60 S 1414823674 0 64240 - -
2022-12-19 15:21:43 DROP TCP 192.168.240.100 192.168.240.150 42634 80 60 S 1171726364 0 64240 - -
2022-12-19 15:22:20 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:22:21 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:22:22 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:22:23 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:22:24 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:22:25 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:22:26 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:22:27 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:22:28 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:22:29 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:22:30 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
2022-12-19 15:22:31 DROP ICMP 192.168.240.100 192.168.240.150 - - 84 - - - - 8 0 - RECEIVE
```