

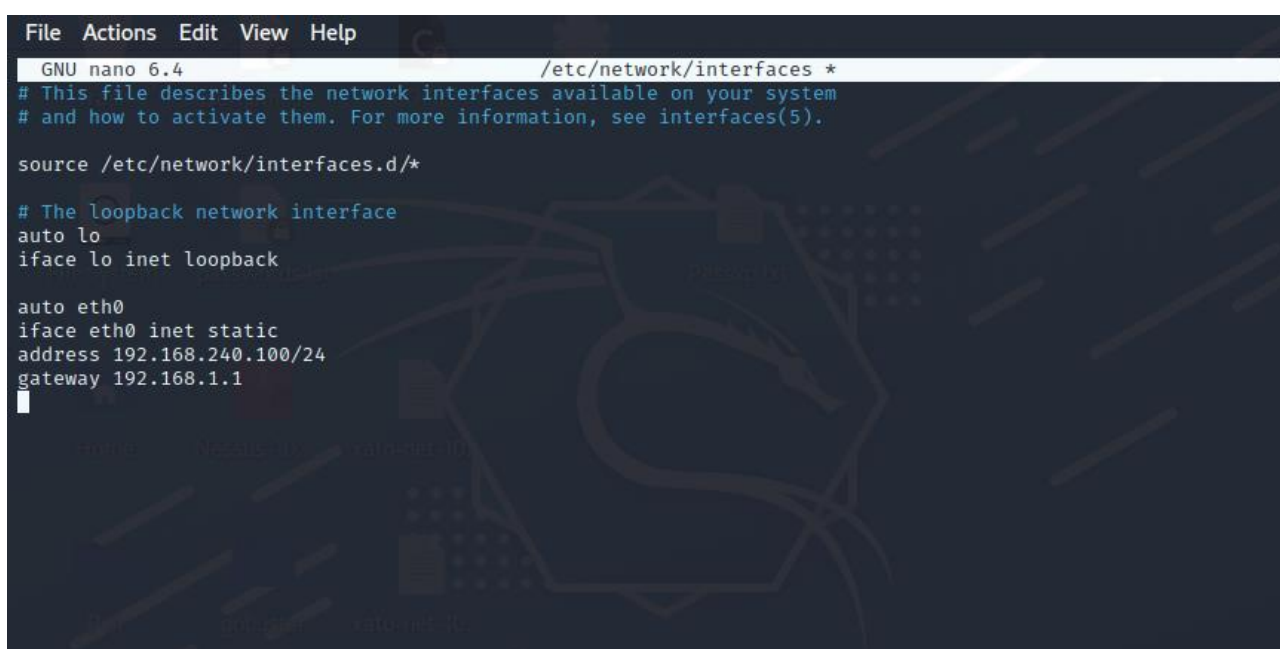
Security Operation: Azioni Preventive

Prerequisiti:

Kali Ip: 192.168.240.100

Windows Xp: 192.168.240.150

Impostiamo l'ip di Kali da terminale tramite il comando ***sudo nano /etc/interfaces/networking*** sostituendo quello presente con quello richiesto nei prerequisiti. Una volta fatto riavviamo il network con ***sudo /etc/init.d/networking restart***



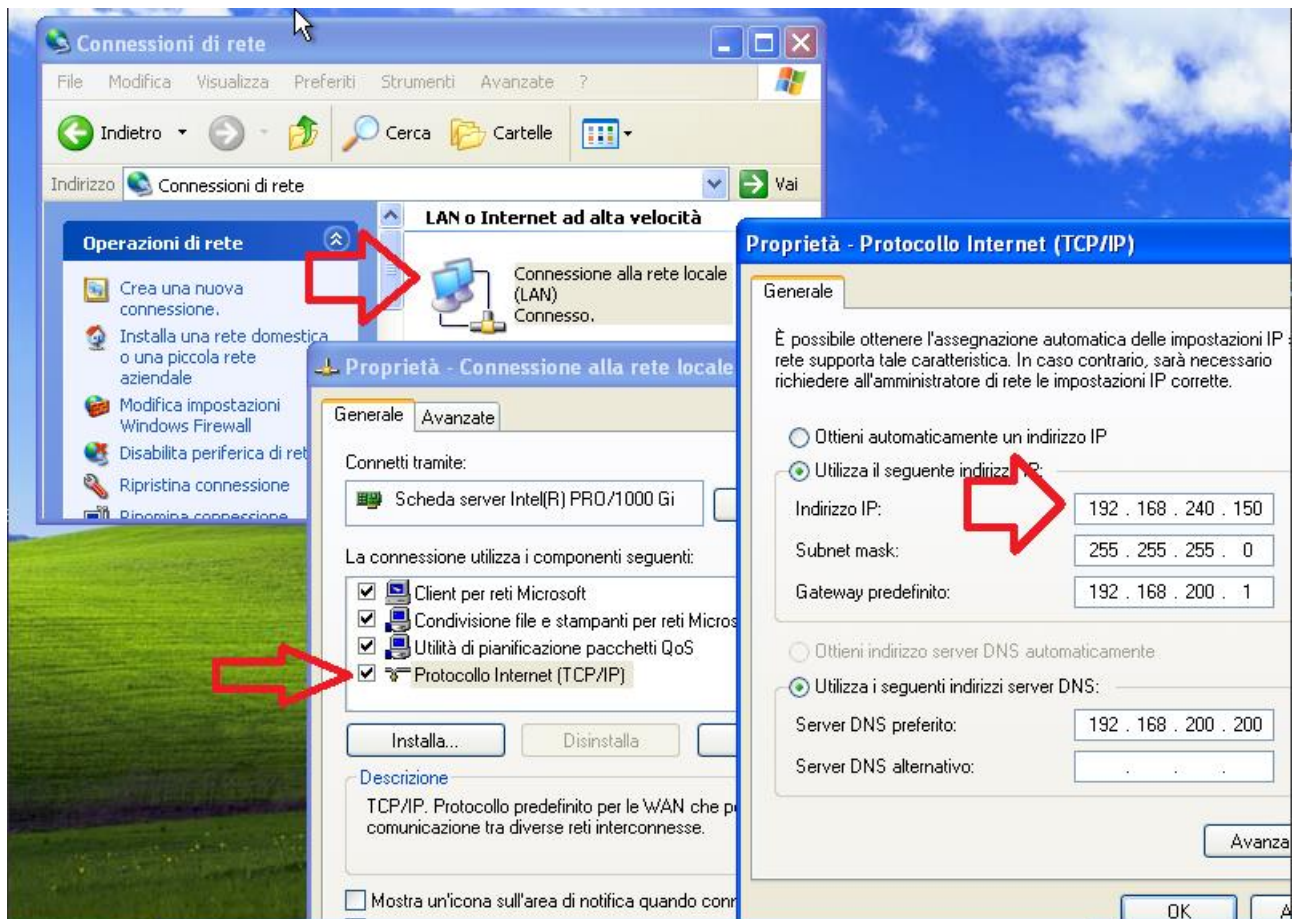
```
File Actions Edit View Help
GNU nano 6.4 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100/24
gateway 192.168.1.1
```

Potremmo poi controllare tramite ***Ifconfig*** che la procedura sia avvenuta correttamente. Mentre per quanto riguarda Xp dovremmo andare nel ***Pannello di Controllo -> Rete e connessioni Internet -> Connessioni di rete*** da qui, come visto nell'immagine, si proseguirà su ***Connessione alla rete Locale -> Protocollo Internet (TCP/IP)*** e qui modificheremo ***l'indirizzo ip*** come richiesto. Ora non ci resta che premere ***Ok***.



Effettuate le modifiche controlleremo se le due macchine siano connesse tra loro tramite il comando Ping

```

Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ping 192.168.240.100

Esecuzione di Ping 192.168.240.100 con 32 byte di dati:

Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.240.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 1ms, Medio = 0ms

C:\Documents and Settings\Epicode_user>

```

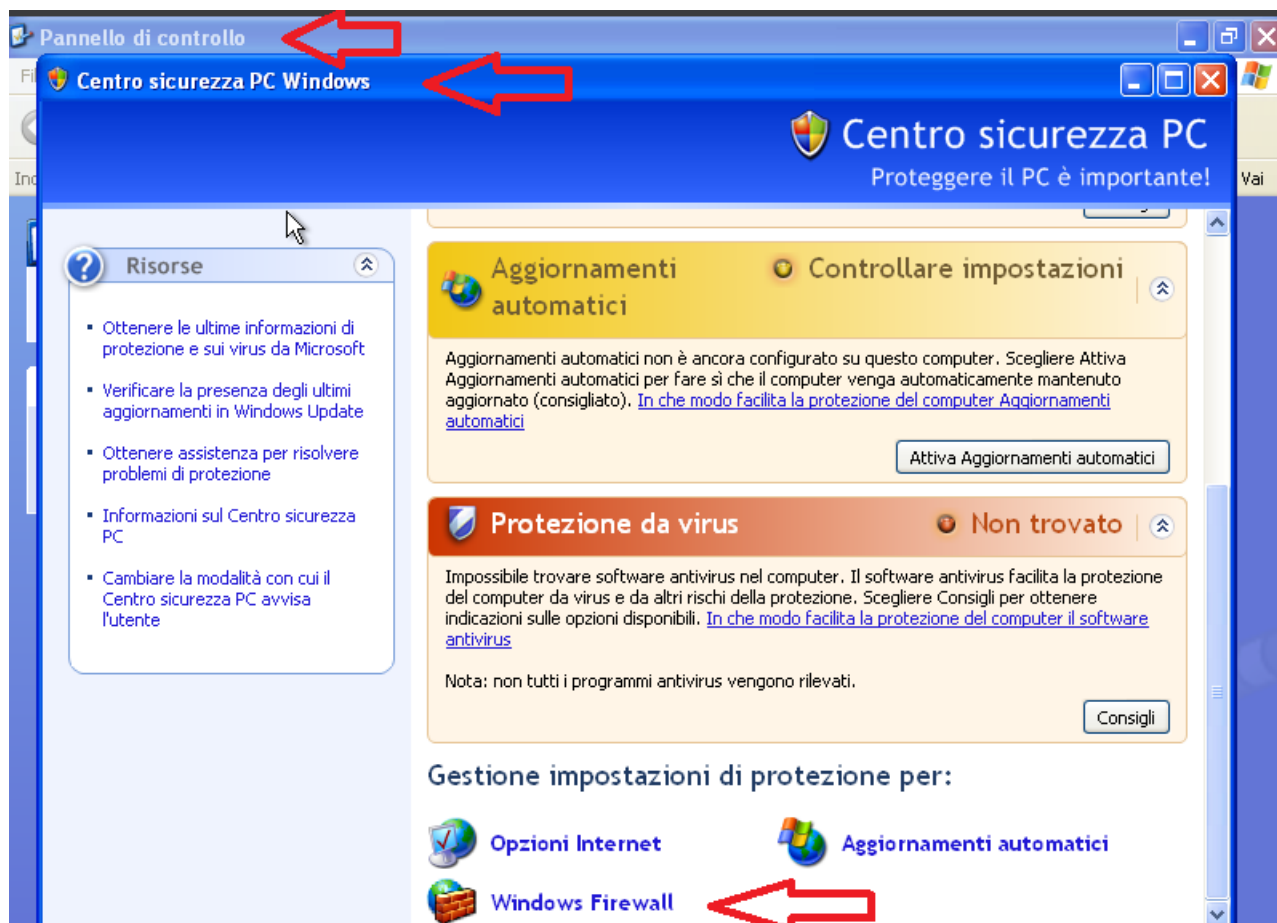
```

$ ping 192.168.240.100
PING 192.168.240.100 (192.168.240.100) 56(84) bytes of data.
64 bytes from 192.168.240.100: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 192.168.240.100: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 192.168.240.100: icmp_seq=3 ttl=64 time=0.029 ms
64 bytes from 192.168.240.100: icmp_seq=4 ttl=64 time=0.033 ms
64 bytes from 192.168.240.100: icmp_seq=5 ttl=64 time=0.023 ms
64 bytes from 192.168.240.100: icmp_seq=6 ttl=64 time=0.030 ms
^C
— 192.168.240.100 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5123ms
rtt min/avg/max/mdev = 0.018/0.027/0.033/0.005 ms

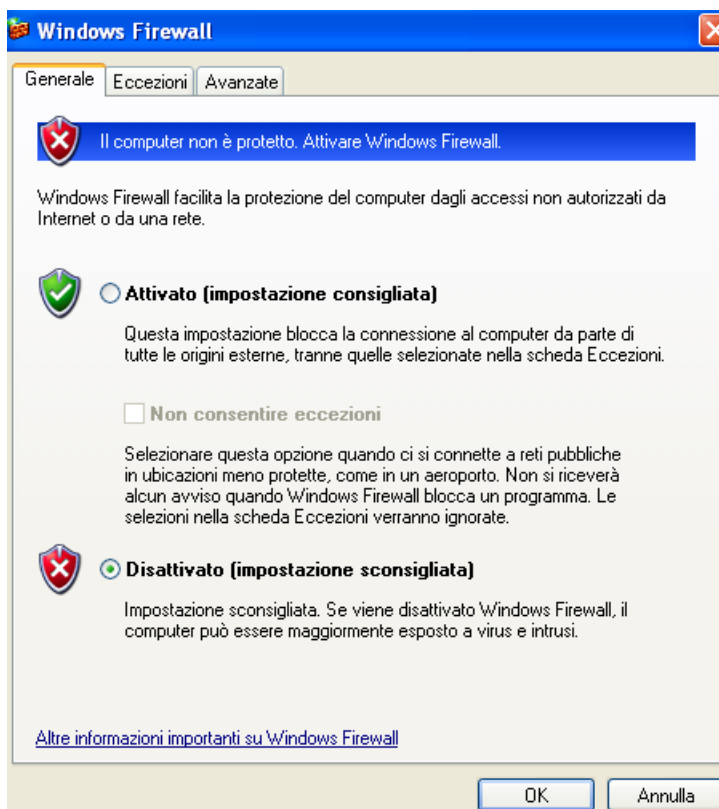
(kali@kali)-[~]
$

```

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

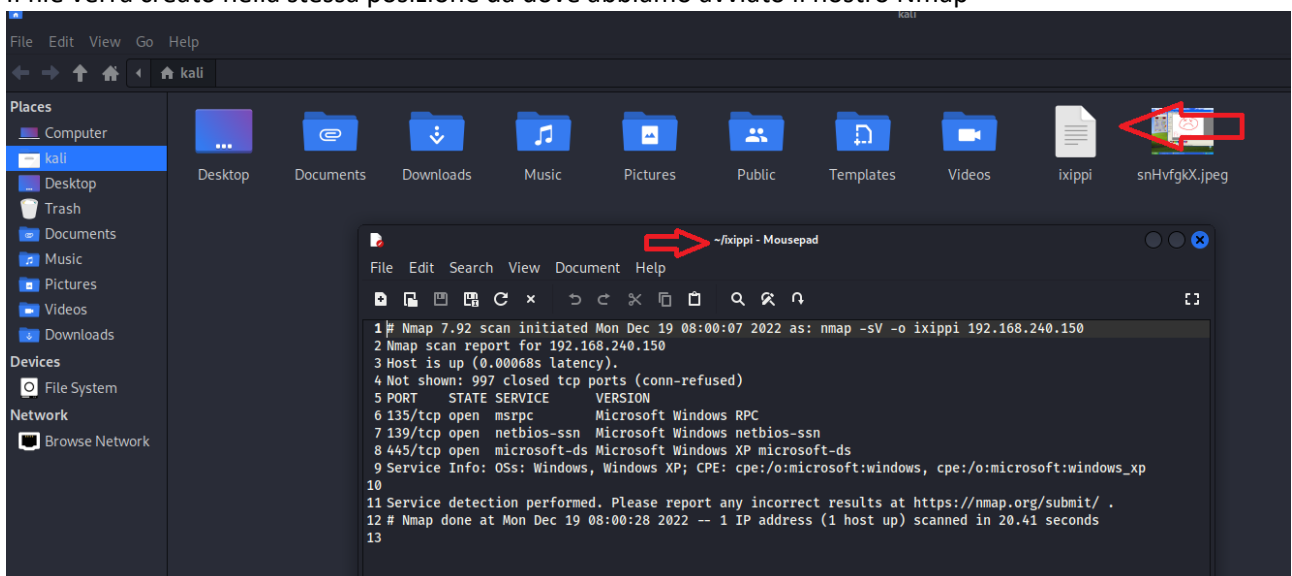


Ora non ci resta che effettuare il nostro **Nmap sV -o ixippi 192.168.240.150** dove -o ixippi sarà il nome del file log che Nmap creerà

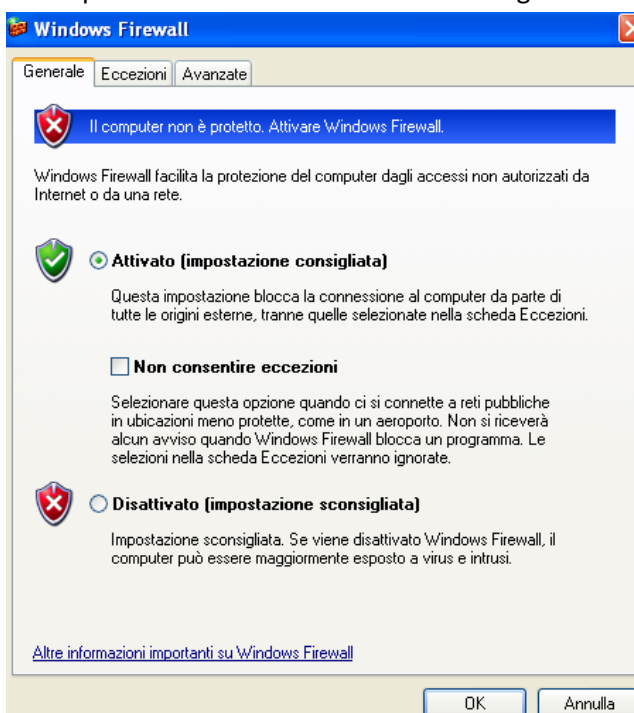
```
(kali㉿kali)-[~]
└─$ nmap -sV -o ixippi 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:00 EST
Nmap scan report for 192.168.240.150
Host is up (0.00068s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc 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

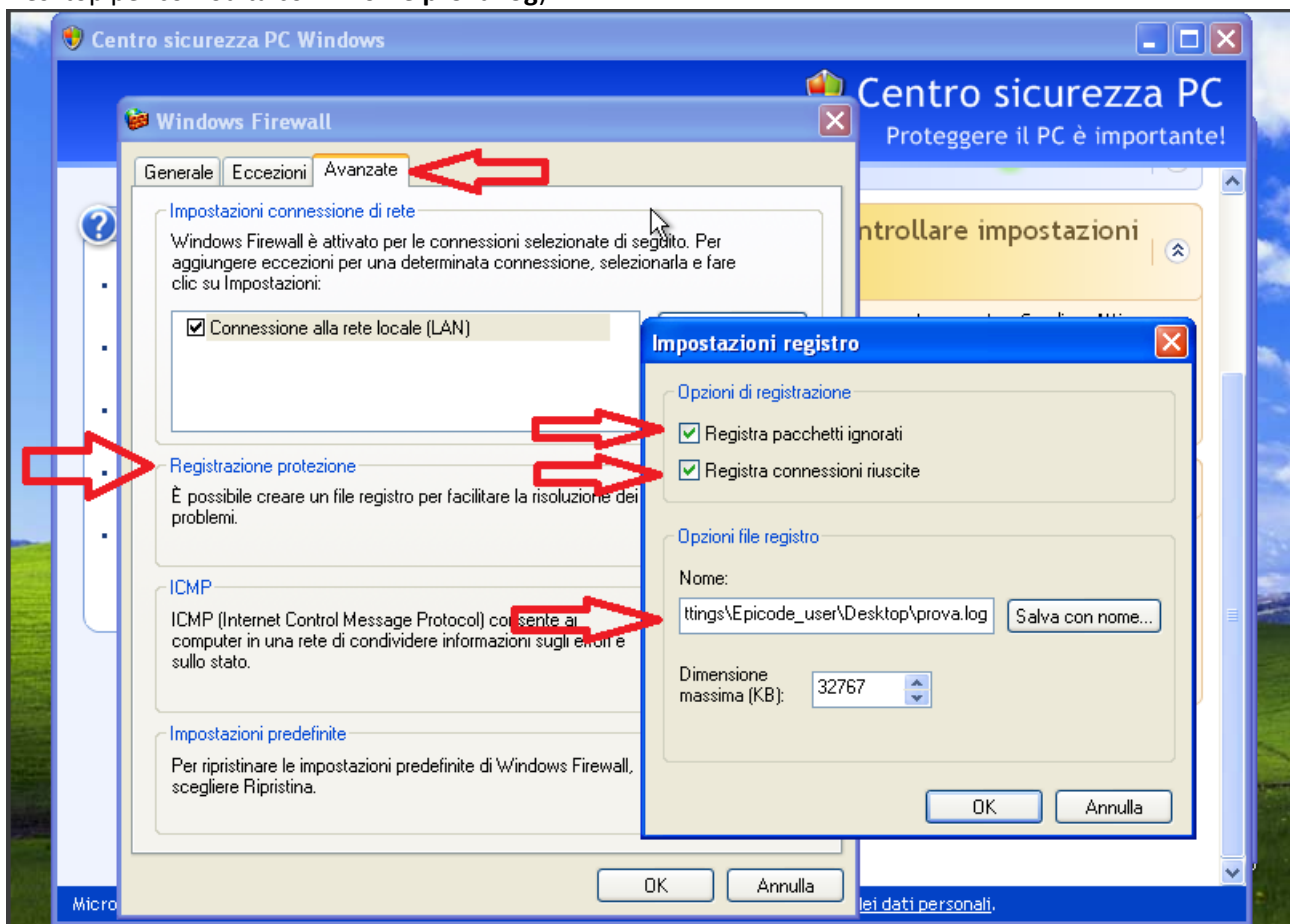


mentre se attiveremo il Firewall di Windows come abbiamo visto precedentemente

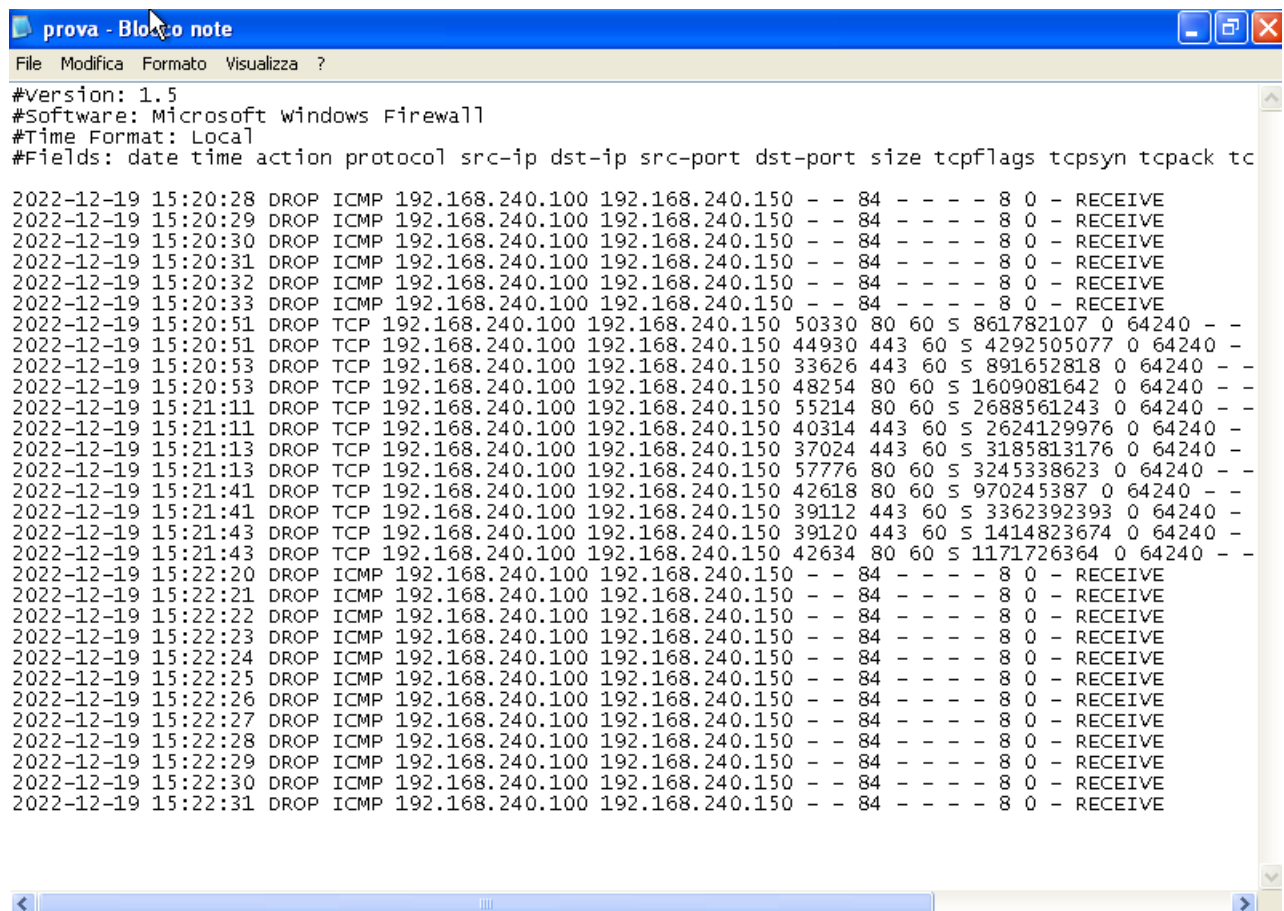
Potremmo notare come la nostra scansione verrà bloccata, impedendoci l'accesso alla scansione di Xp, non mostrando più alcuna informazione sulla macchina

```
(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
```