

```
TX errors 0 dropped 0 overruns 0 frame 0
TX packets 3430 bytes 345245 (337.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ sudo nano /etc/network/interfaces

(kali@kali)-[~]
$ sudo /etc/init.d/networking restart
Restarting networking (via systemctl): networking.service.

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255
    inet6 fe80::a00:27ff:fe34:f4be prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:34:f4:be txqueuelen 1000 (Ethernet)
    RX packets 2725 bytes 594823 (580.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6526 bytes 1516207 (1.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (local loopback)
    RX packets 3430 bytes 345245 (337.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3430 bytes 345245 (337.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$
```

Cambiare l'indirizzo ip con il comando: “sudo nano /etc/network/interfaces

Una volta aperto il file di interfaccia di rete configurare cambiare l'indirizzo address e l'indirizzo di gateway con l'ip desiderato, nel nostro caso metteremo 192.168.240.100 sulla macchina kali.

Una volta fatto ciò digitiamo sulla tastiera ctrl+o e poi premiamo invio ,

```
GNU nano 2.9.4 /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

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.240.100
netmask 255.255.255.0
gateway 192.168.240.1
```

Questo dovrebbe essere il risultato

Successivamente premere ctrl+x per chiudere il file di interfaccia di rete.

Digitiamo poi il comando sudo /etc/init.d/networking restart per restartare il file in questione

Se digitato correttamente vi dara il risultato riportato nella figura sotto

```
(kali@kali)-[~]
$ sudo /etc/init.d/networking restart
Restarting networking (via systemctl): networking.service.
```

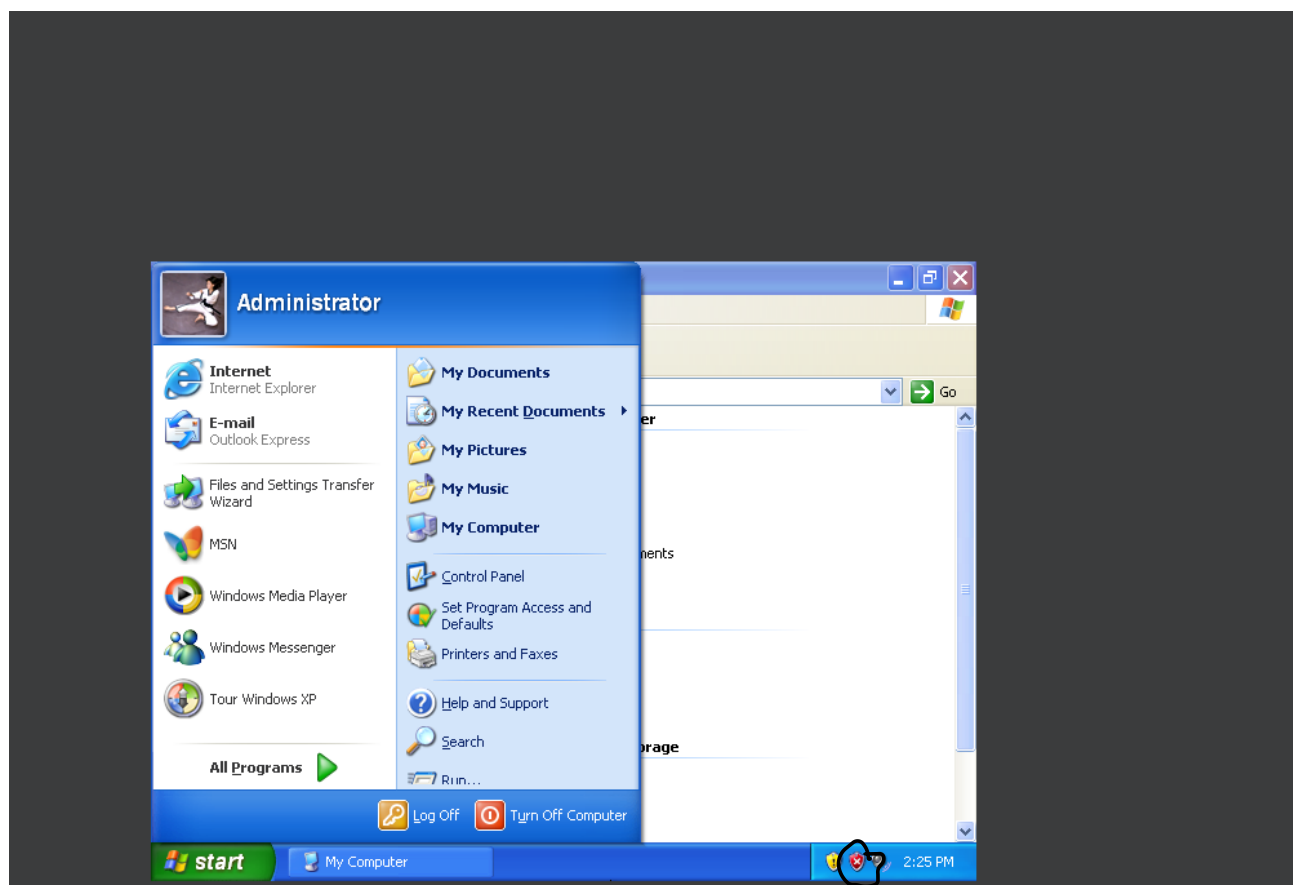
Digitare poi il comando `ifconfig` per visualizzare l'attuale settaggio di interfaccia di rete , grazie a cio si potra vedere se le modifiche applicatre sono andate a buon fine (vedi la figura sotto)

```
Restarting networking (via systemctl): networking.service.

(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255
    inet6 fe80::a00:27ff:fe34:f4be prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:34:f4:be txqueuelen 1000 (Ethernet)
    RX packets 2725 bytes 594823 (580.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6526 bytes 1516207 (1.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3430 bytes 345245 (337.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3430 bytes 345245 (337.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Recarsi poi sulla macchina con windows xp e procedere con la disattivazione del firewall.



Per poter fare questo premere start e cliccare con il cursore del mouse sul simbolo cerchiato in figura (quello del firewall)

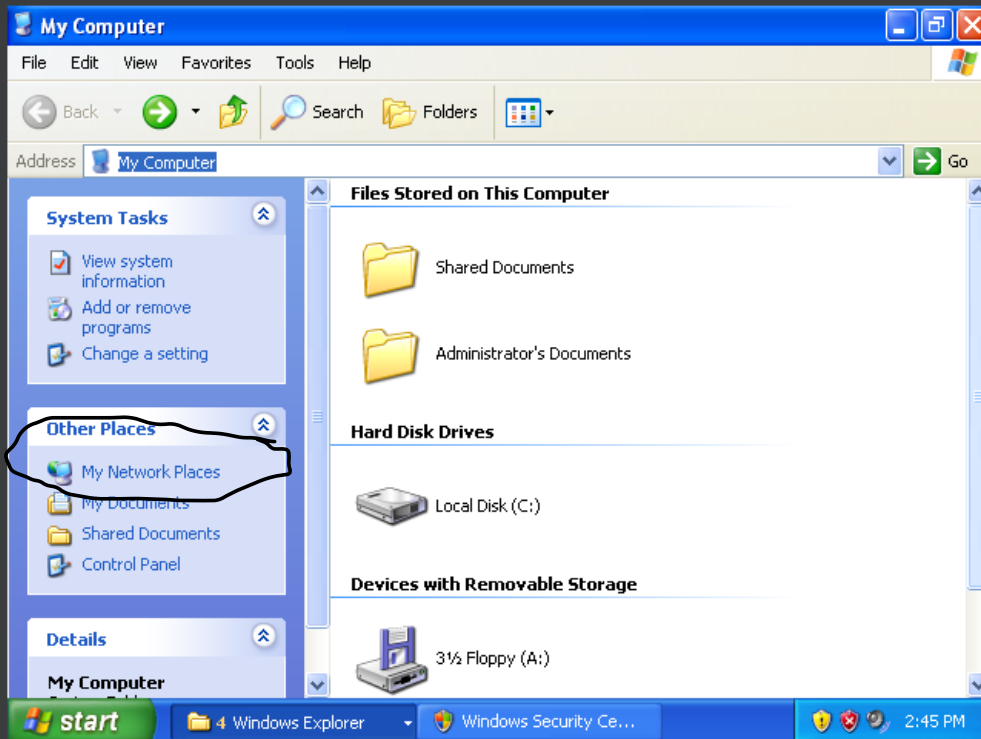
Si aprirà quindi una finestra (sotto riportata) con una sezione apposita legata al firewall controllare che l'icona sia rossa e abbia una scritta con scritto off.



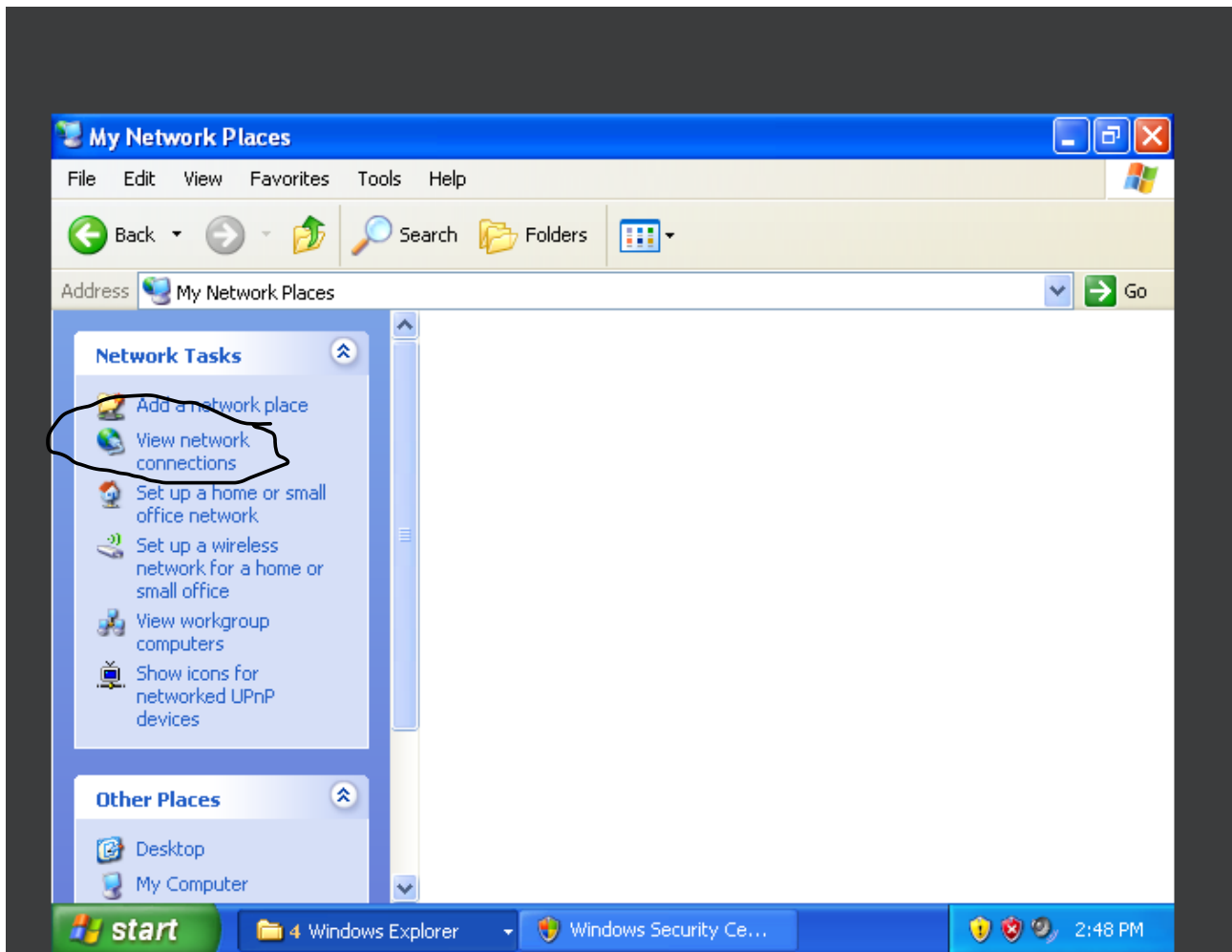
Qualora fosse abilitato apparirà blu e la scritta on (vedi immagine)



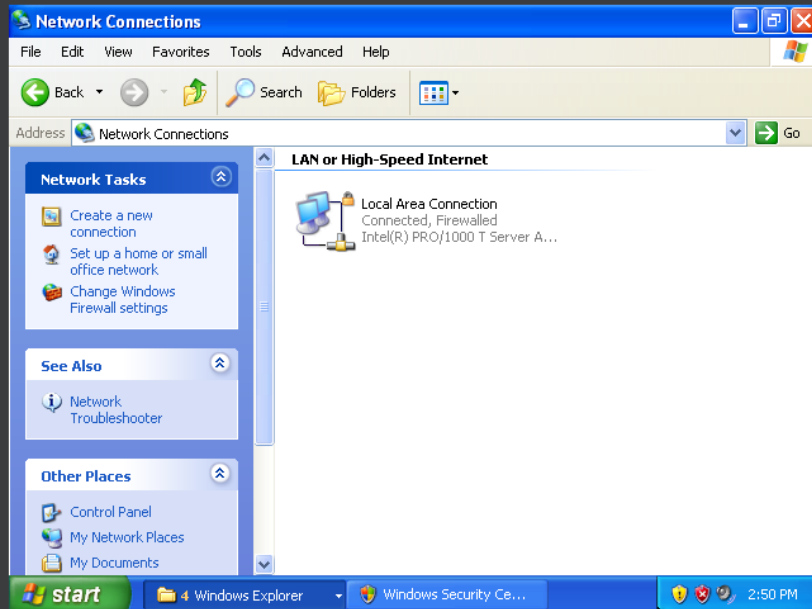
Per disabilitare il firewall spostare il cursore sulla parte evidenziata ovvero: “my network places”



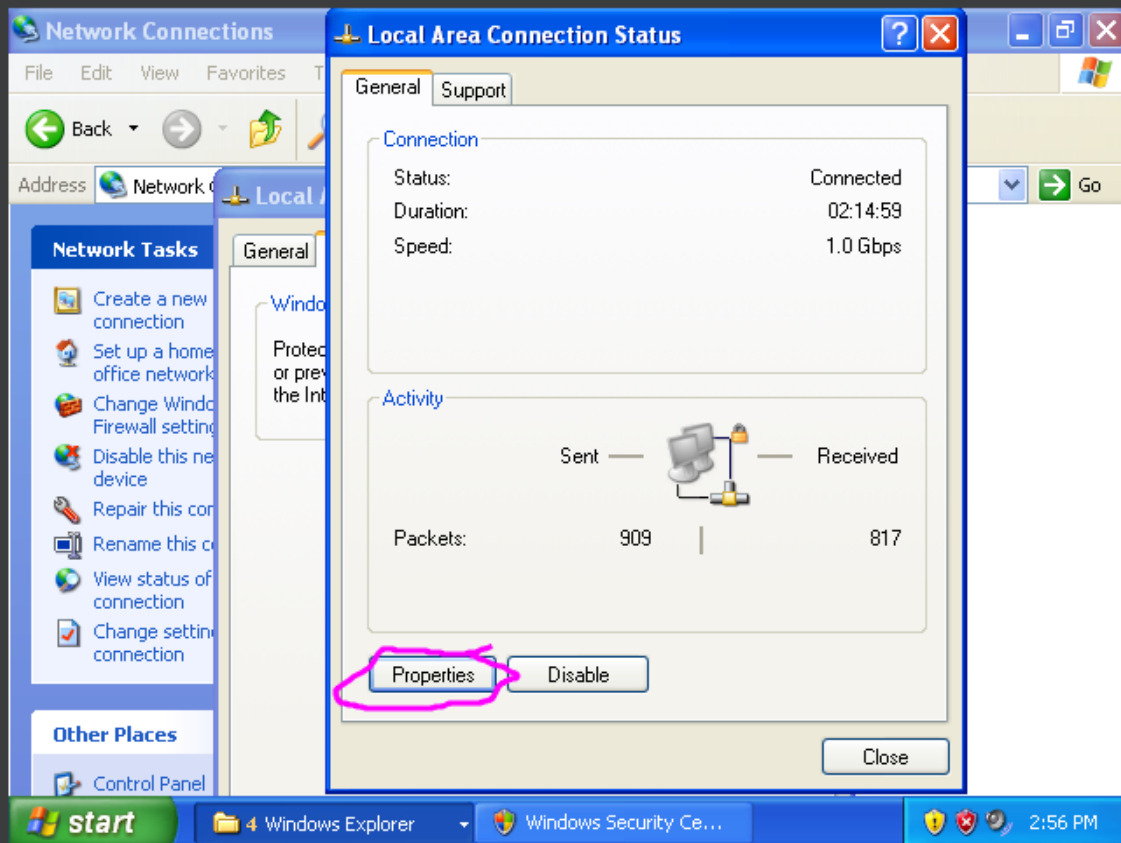
Digitare la sezione view network connections



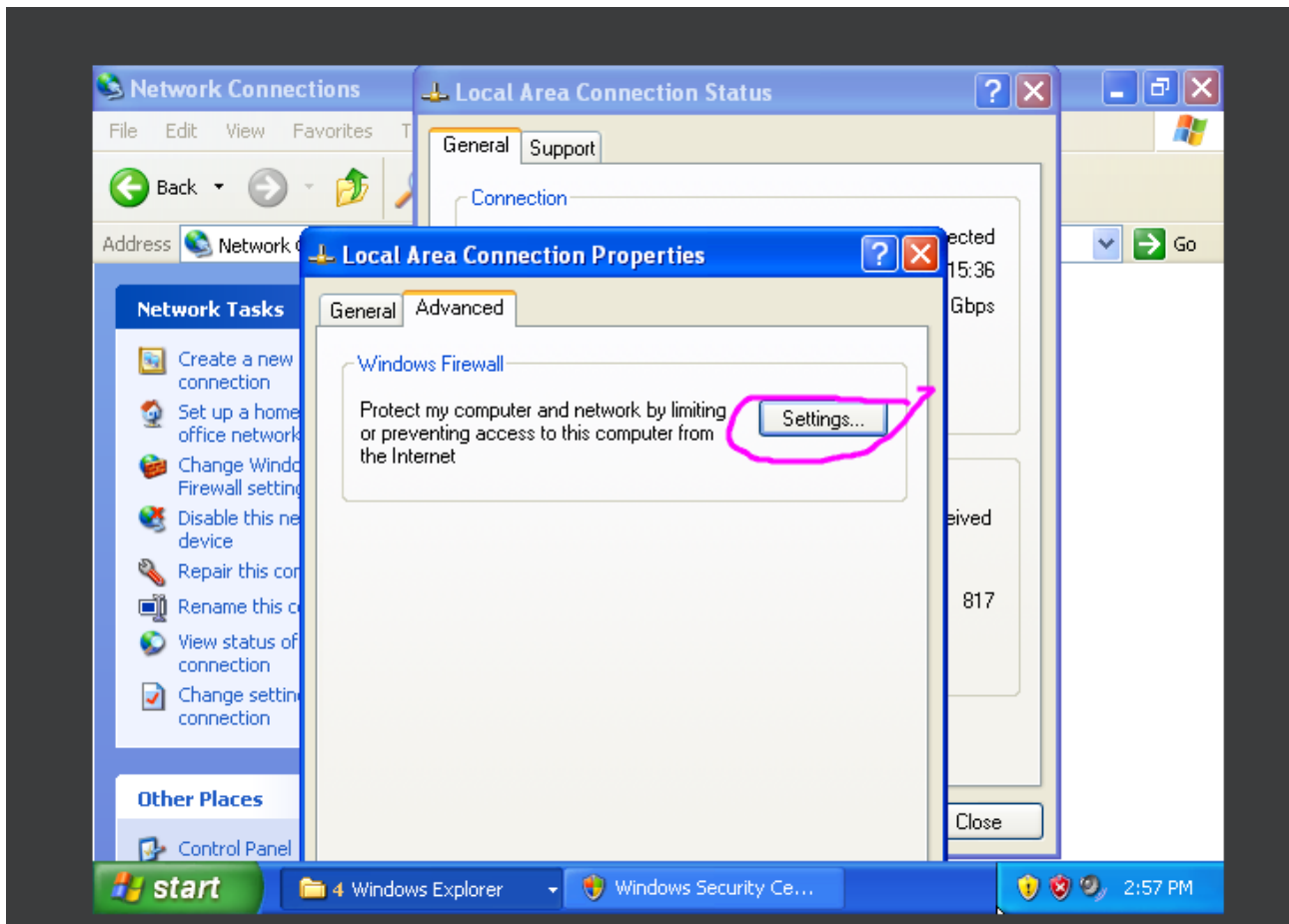
Selezionare con il cursore local area connection



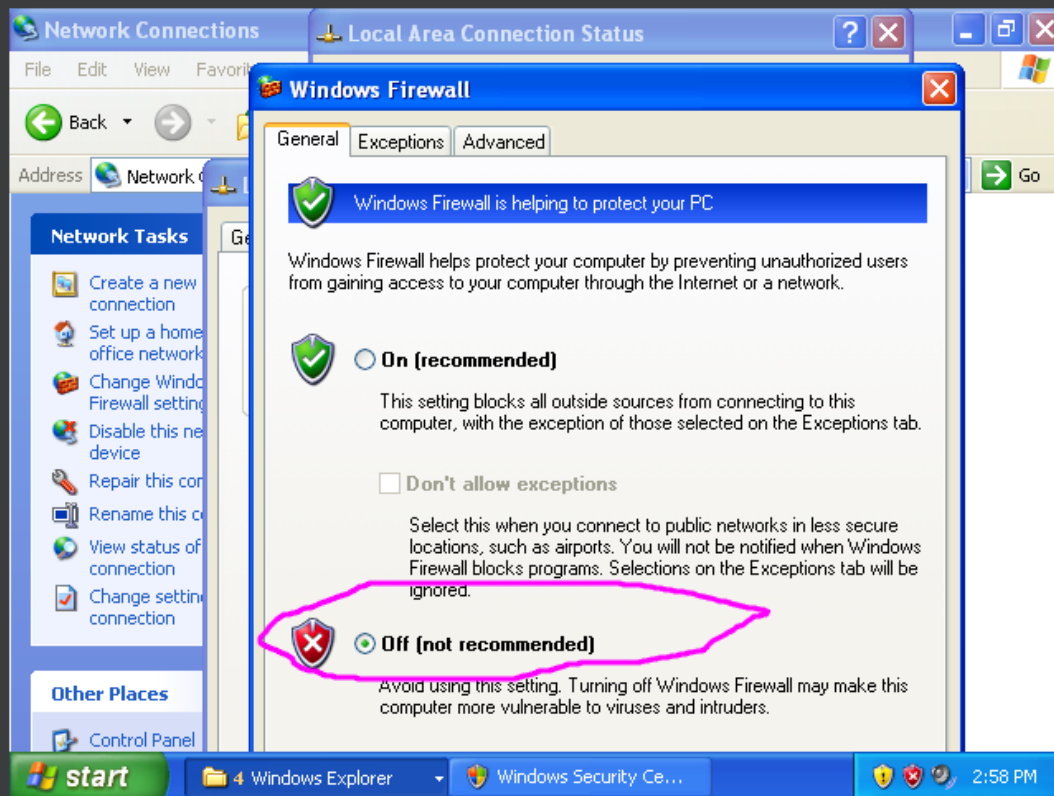
Selezionare con il cursore l'opzione proprieties (vedi figura)



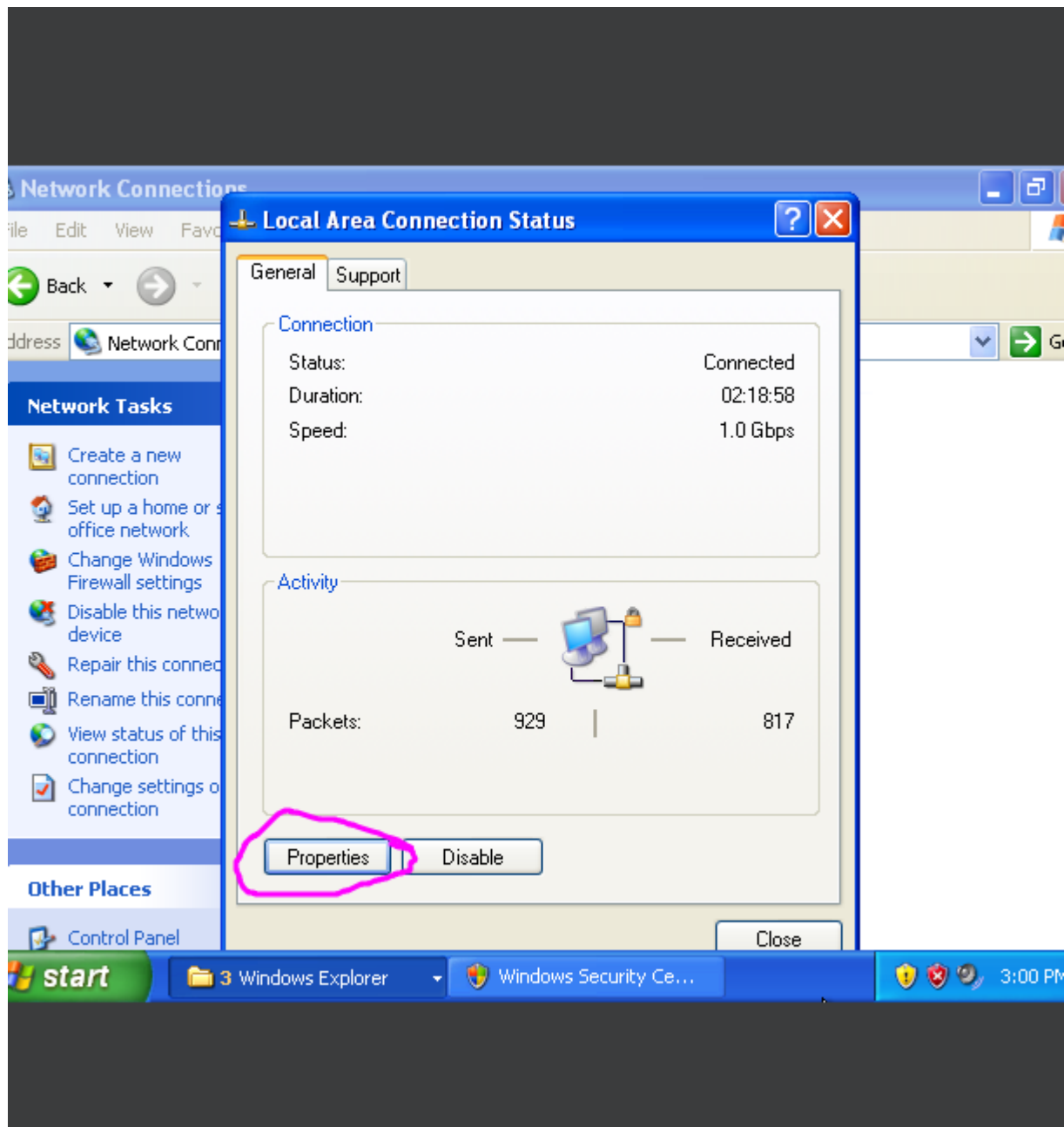
Andare sull' opzione advanced e apparira windows firewall, selezionare con il cursore il tasto settings



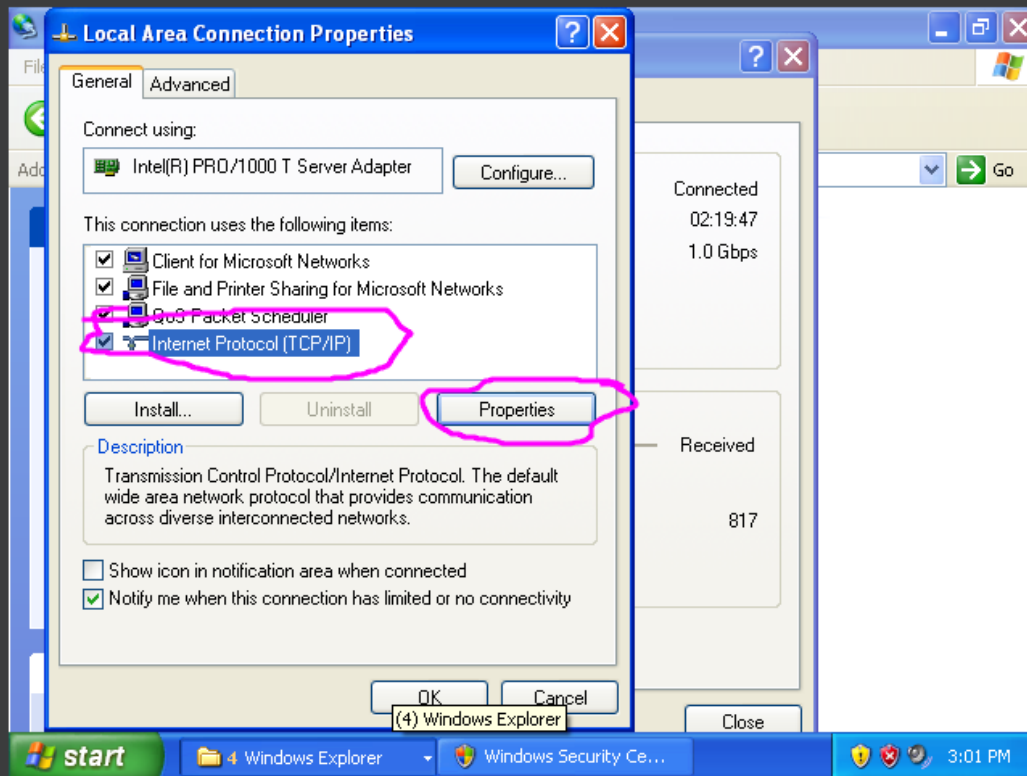
A questo punto selezionare l'opzione off , in questo modo disattiveremo il firewall per riattivarlo bastera rieseguire il medesimo procedimento, con l'unica differenza che bisognerà cliccare su on.



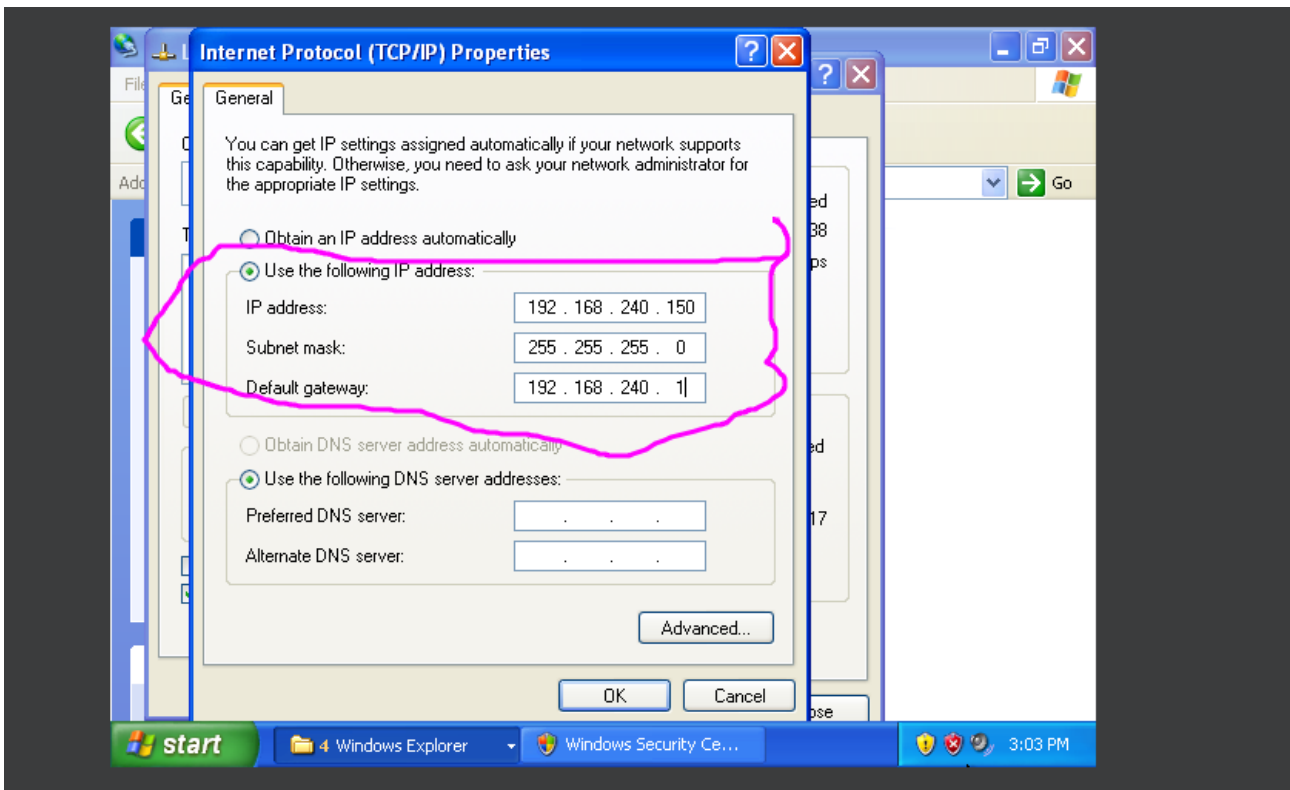
Passiamo dunque al procedimento di settaggio dell'ip su windows andare nella sezione network connections local area connections sezione general e cliccare su properties



spostare il cursore sulla sezione evidenziata in blu e anche cerchiata ovvero internet Protocol (Tcp/ip) poi spostare il cursore e cliccare il tasto properties cerchiato in viola

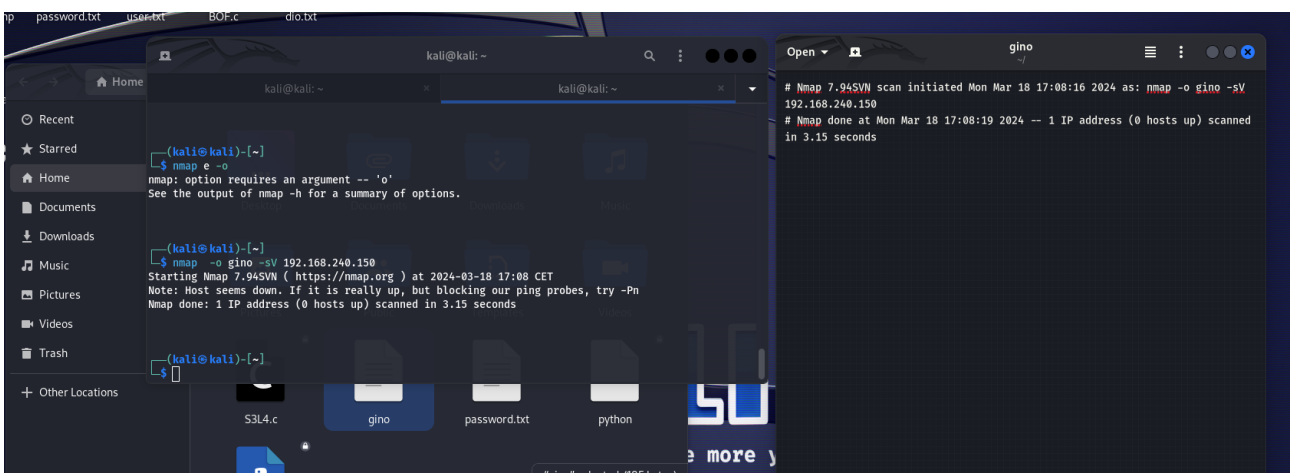


A questo punto si aprirà una finestra qui sotto riportata settare ip address la subnet mask e il default gateway come da immagine .



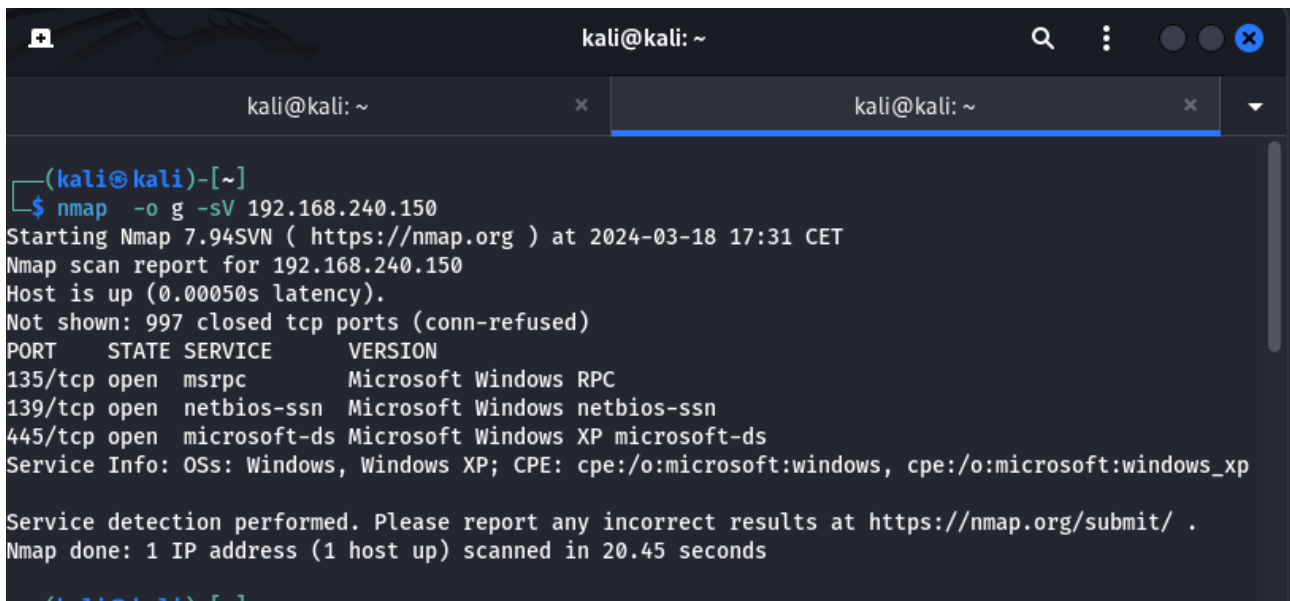
A questo punto avremo soddisfatto tutti i prerequisiti.

Tornare sulla macchina kali e aprire la console e digitare il seguente comando



Una volta che abbiamo effettuato la scansione con nmap e grazie al comando anche creato nella sezione chiamata con il nome che abbiamo scritto dopo -o

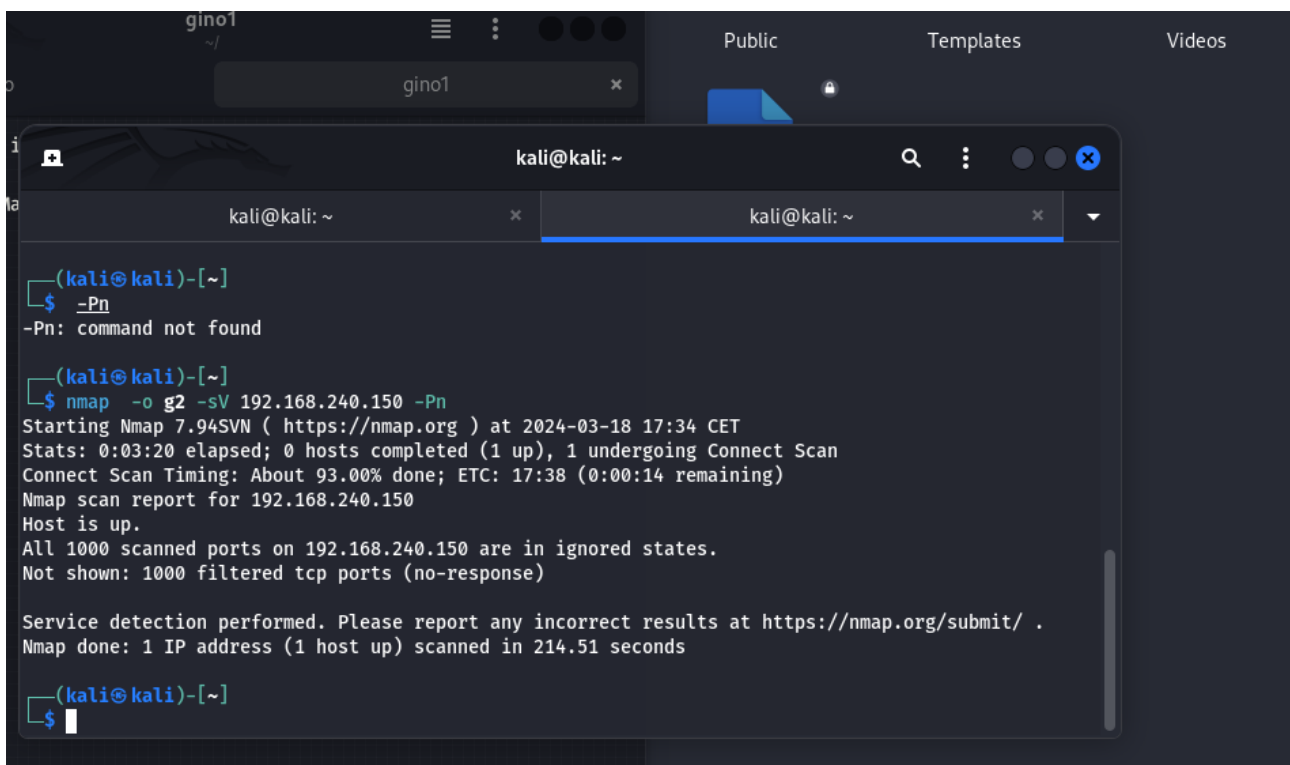
Una volta effettuata la scansione con il firewall di windows xp disattivato andiamo ad disattivare il firewall su windows xp e rieffettuiamo la scansione con nmap il comando precedentemente usato (vedi immagine sotto)



```
(kali@kali)-[~]
$ nmap -o g -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 17:31 CET
Nmap scan report for 192.168.240.150
Host is up (0.00050s 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 20.45 seconds
```

Una volta attivato il firewall apparirà il risultato sotto riportato da qui quindi si può dedurre che il firewall fa da filtro e rende invisibili le porte dell'ip della macchina target.



```
gino1
~ /
Public Templates Videos

(kali@kali)-[~]
$ nmap -o g2 -sV 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 17:34 CET
Stats: 0:03:20 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 93.00% done; ETC: 17:38 (0:00:14 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 214.51 seconds
```