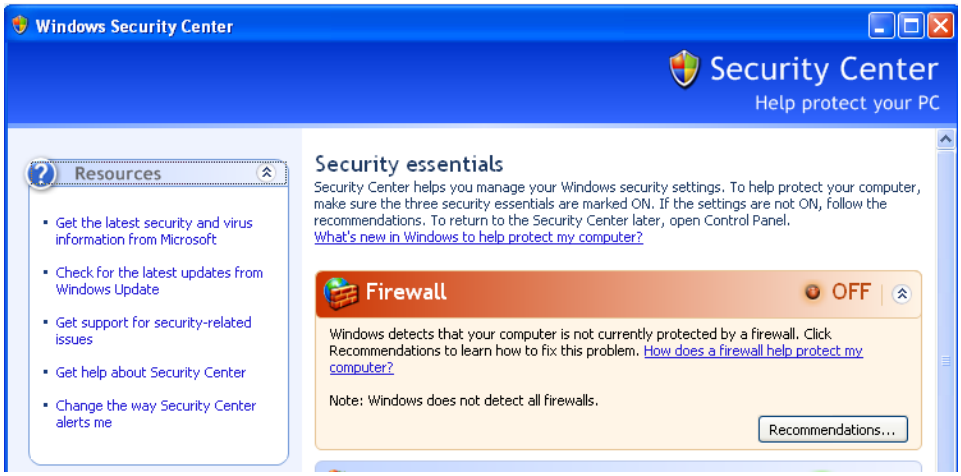
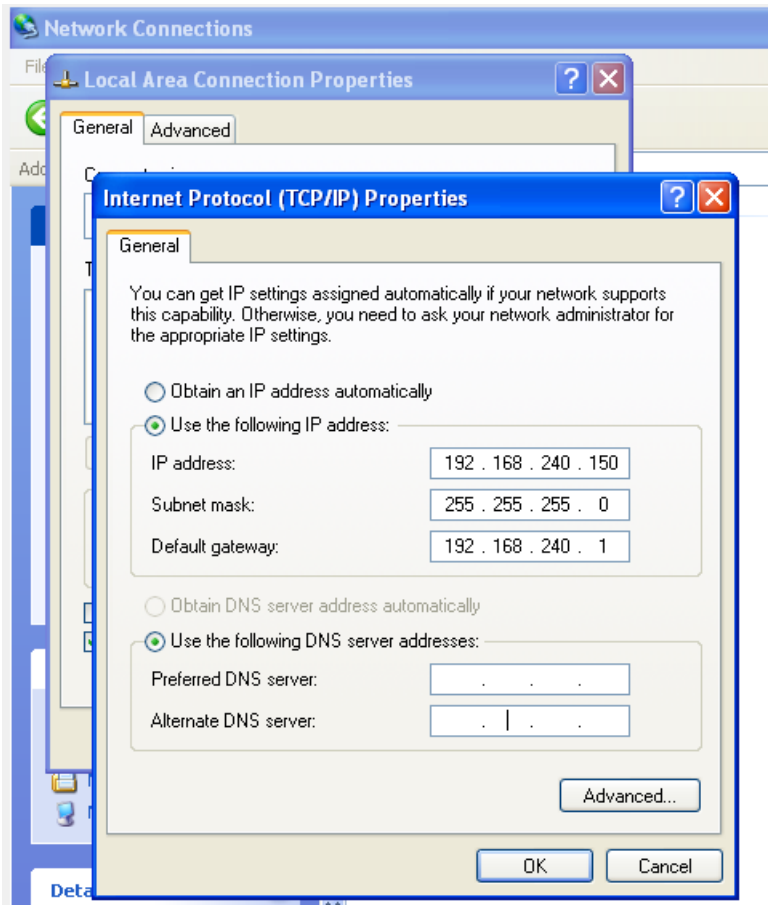
Security Operations

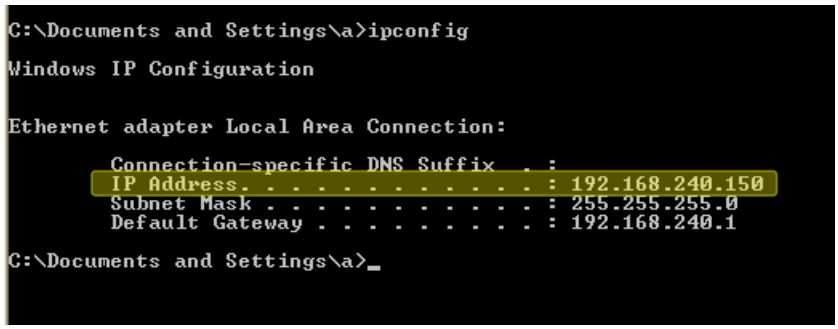
Verifica che la macchina virtuale Windows XP abbia il Firewall disabilitato:



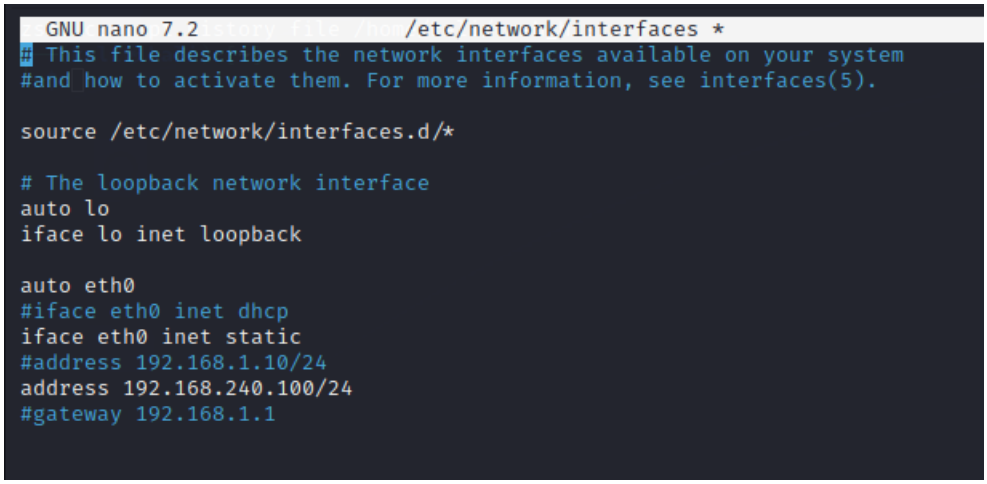
Configurazione indirizzo IP 192.168.240.150 su Windows XP:



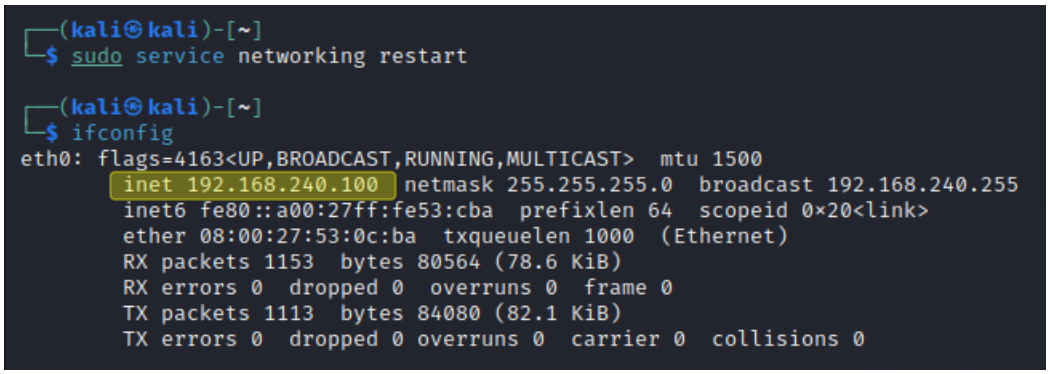
Verifica con `ipconfig`:



Configurazione indirizzo IP 192.168.240.100 su Kali Linux:



Restart dei servizi di rete e verifica con `ifconfig`:



Ping da Kali a XP

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(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=0.611 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.916 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.683 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=1.27 ms
^C
── 192.168.240.150 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.611/0.869/1.269/0.256 ms
```

Ping da XP a Kali

```
Pinging 192.168.240.100 with 32 bytes of data:

Reply from 192.168.240.100: bytes=32 time<1ms TTL=64
Reply from 192.168.240.100: bytes=32 time=1ms TTL=64
Reply from 192.168.240.100: bytes=32 time<1ms TTL=64
Reply from 192.168.240.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.240.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

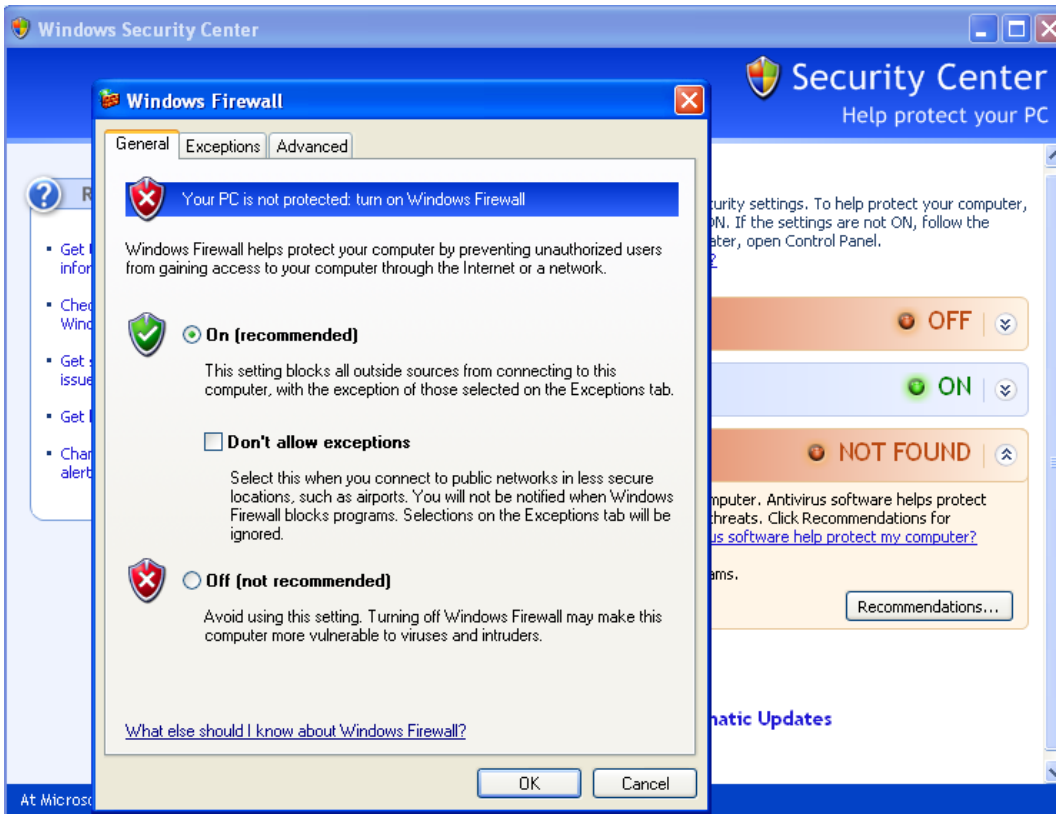
Scansione con `nmap -sV` della macchina Windows XP con output nel file `xpreportscan.txt`

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o xpreportscan.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-03 14:49 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00079s 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 20.64 seconds
```

Visualizzazione del report:

```
┌──(kali㉿kali)-[~]
└─$ cat xpreportscan.txt
# Nmap 7.93 scan initiated Tue Oct  3 14:49:36 2023 as: nmap -sV -o xpreportscan.txt 192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.00079s 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 at Tue Oct  3 14:49:56 2023 -- 1 IP address (1 host up) scanned in 20.64 seconds
```

Abilitazione del Firewall su Windows XP



Seconda cansione con `nmap -sV` della macchina Windows XP (con Firewall abilitato) con output nel file `xpreportscan2.txt`

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o xpreportscan2.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-03 14:54 EDT
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 3.36 seconds
```

Visualizzazione del report:

```
┌──(kali㉿kali)-[~]
└─$ cat xpreportscan2.txt
# Nmap 7.93 scan initiated Tue Oct  3 14:54:28 2023 as: nmap -sV -o xpreportscan2.txt 192.168.240.150
# Nmap done at Tue Oct  3 14:54:32 2023 -- 1 IP address (0 hosts up) scanned in 3.36 seconds
```

DIFFERENZE TRA SCANSIONE CON FIREWALL DISABILITATO E FIREWALL ABILITATO:

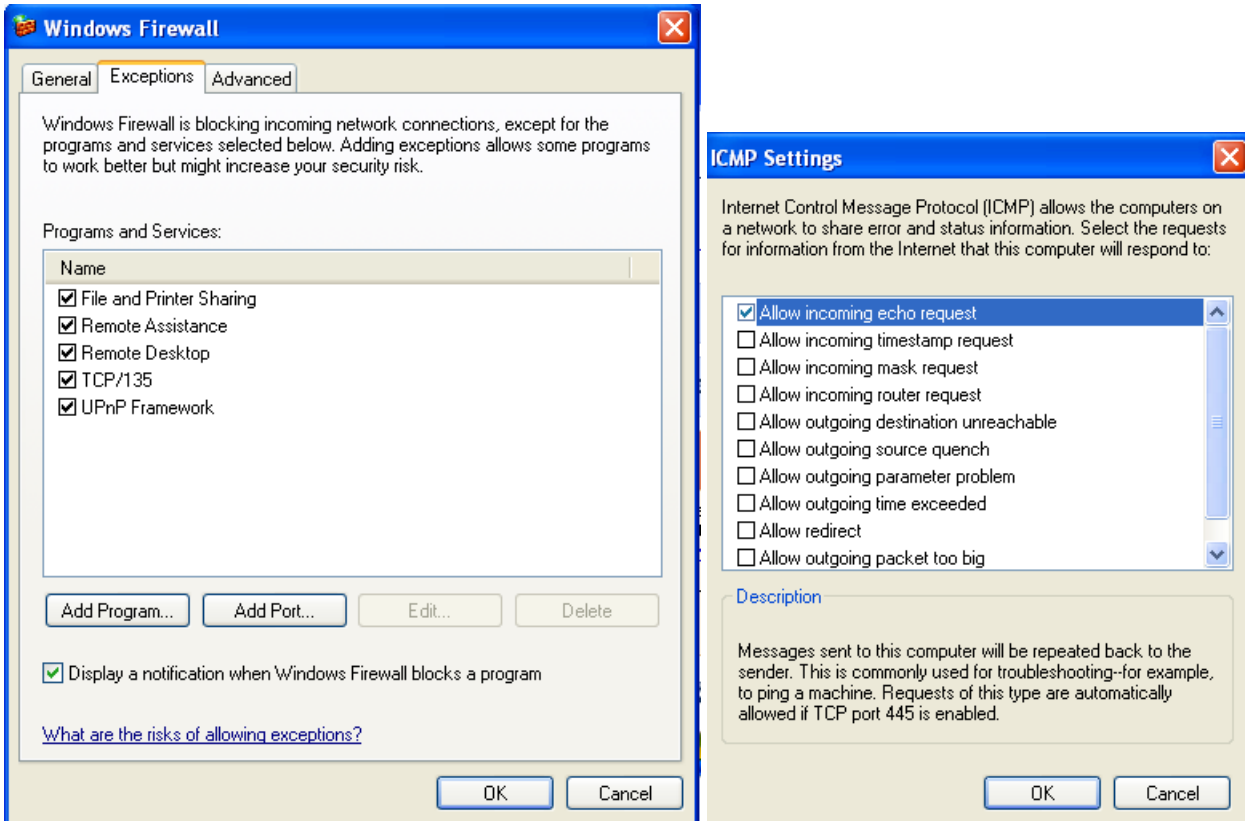
La scansione 1 ha rilevato le porte aperte e i relativi servizi in esecuzione. Vediamo il primo report:

```
└─$ cat xpreportscan.txt
# Nmap 7.93 scan initiated Tue Oct  3 14:49:36 2023 as: nmap -sV -o xpreportscan.txt 192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.00079s 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 at Tue Oct  3 14:49:56 2023 -- 1 IP address (1 host up) scanned in 20.64 seconds
```

La scansione 2 non è riuscita a rilevare l'host. Vediamo il secondo report:

```
└─$ cat xpreportscan2.txt
# Nmap 7.93 scan initiated Tue Oct  3 14:54:28 2023 as: nmap -sV -o xpreportscan2.txt
192.168.240.150
# Nmap done at Tue Oct  3 14:54:32 2023 -- 1 IP address (0 hosts up) scanned in 3.36 seconds
```

La differenza tra i due risultati è data dal Firewall Windows XP. Provando ad abilitare tutte le porte delle eccezioni, vediamo che in automatico si abilita anche il flag "Allow incoming echo request" del protocollo ICMP (utilizzato dal comando `ping`).



Con questa configurazione, eseguendo una scansione `nmap -Pn` che non esegue un ping prima di iniziare la scansione delle porte, riceviamo il risultato per le porte per le quali abbiamo abilitato l'eccezione. Notiamo che il messaggio "`Not shown: 995 filtered tcp ports (no-response)`" indica che le restanti 995 porte non abilitate nel Firewall (delle prime 1000 scansionate da nmap) sono filtrate, ovvero nmap non ha avuto risposta perché esistono regole d Firewall per quelle porte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-03 16:02 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0011s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
2869/tcp closed icslap
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 18.48 seconds
```

Mantenendo questa configurazione nel Firewall di Windows XP, la scansione continua a non rilevare l'host come attivo.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-03 16:08 EDT
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 3.18 seconds
```