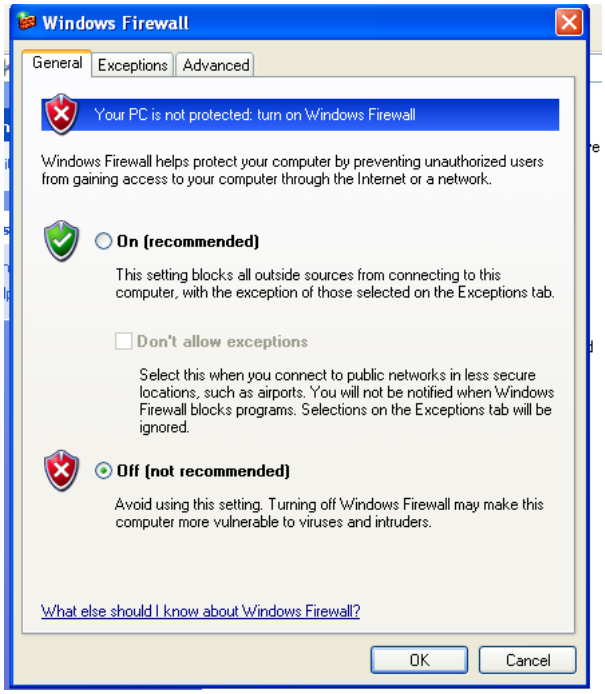
Come primo punto impostiamo gli IP delle due macchine come da traccia:

```
┌──(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:fec6:9a57  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c6:9a:57  txqueuelen 1000  (Ethernet)
        RX packets 442  bytes 122248 (119.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1012  bytes 998343 (974.9 KiB)
        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 108  bytes 12092 (11.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 108  bytes 12092 (11.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

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

C:\Documents and Settings\Davide>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.240.150
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Davide>
```



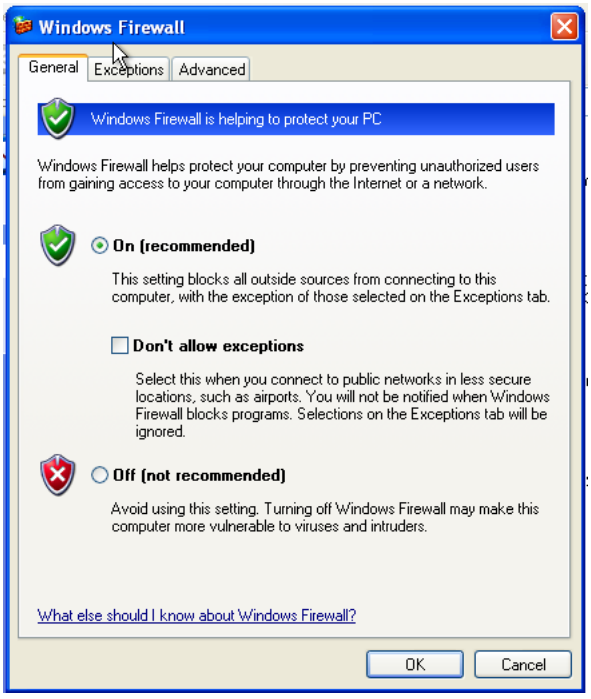
Dopo aver fatto ciò controlliamo che il firewall di windows sia spento.

A questo punto eseguiamo la prima scansione con nmap sia con lo switch -sV che con -o per salvare il risultato della scansione.

```
┌──(kali㉿kali)-[~]
└─$ nmap -oX filereport.xml 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-10 03:35 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0015s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds
```

Possiamo vedere che in questo caso nmap riesce ad individuare le porte aperte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-10 03:31 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0015s 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 20.95 seconds
```



Adesso settiamo invece il firewall su on ed andiamo ad eseguire una seconda scansione con nmap per valutare le eventuali differenze.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-10 03:39 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 50.00% done; ETC: 03:39 (0:00:01 remaining)
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 3.52 seconds
```

Vediamo infatti che in questo caso namp non riesce ad ottenere una scansione delle porte aperte perché il firewall blocca la connessione.

Quindi possiamo notare come la **Scansione con Firewall Attivo (On)** comporti un **Rilevamento Limitato:** Con un firewall attivo, il firewall può bloccare o filtrare alcune delle richieste di Nmap. Di conseguenza, Nmap potrebbe non essere in grado di rilevare tutti i servizi e le versioni dei servizi in esecuzione sulla macchina target. Inoltre per eventuali **Porte Chiuse o Filtrate i**l firewall può nascondere le porte chiuse o filtrate, quindi Nmap potrebbe non essere in grado di identificare la presenza di tali porte. Questo può portare a risultati incompleti nella scansione. Infatti come ci dice anche il risultato della seconda scansione il

firewall blocca il Ping Scan che invia pacchetti ICMP Echo Request (ping) all'indirizzo IP e attende le risposte per identificare se l'host è attivo e quali porte aperte ci sono.

Nella **Scansione con Firewall Disattivato (Off)** abbiamo un **Rilevamento Migliorato:** Senza un firewall attivo, Nmap ha maggiori possibilità di rilevare i servizi e le versioni dei servizi in esecuzione sulla macchina target; non ci sono ostacoli nella comunicazione con le porte aperte.
Tutte le porte aperte dovrebbero essere facilmente rilevate e identificate da Nmap senza essere ostacolate dal firewall.