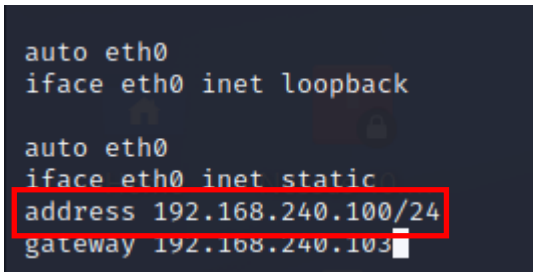
REPORT AZIONI PREVENTIVE

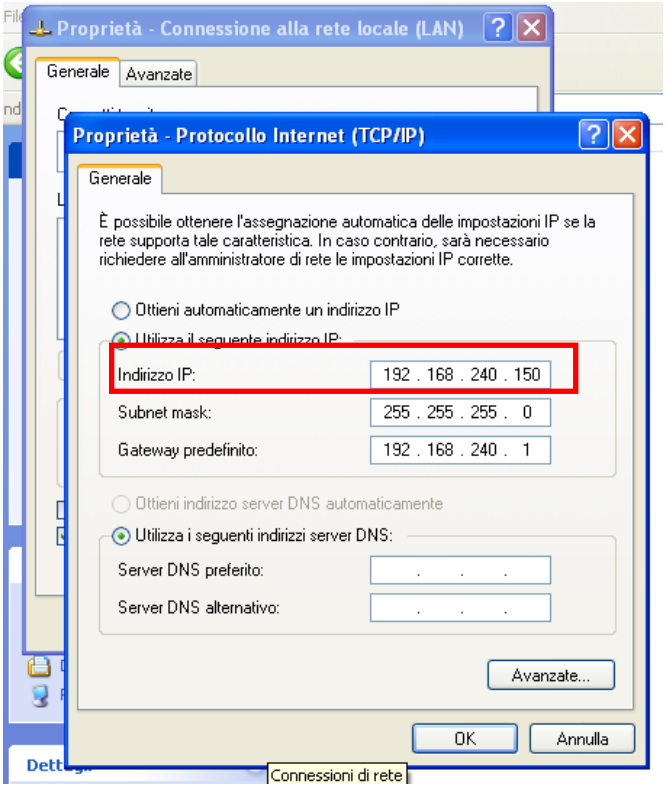
Task del giorno:

- Provare a scansionare Windows XP con e senza l'attivazione del firewall, e notare differenze

Per prima cosa come richiesto dai requisiti dell'esercizio vado a cambiare indirizzo IP di kali e XP



KALI



XP

Con il firewall spento (come lo è di default ogni volta che si accende la macchina) facciamo un "nmap" da kali per vedere cosa riesce a trovare

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -o report.txt  192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:23 EST
Nmap scan report for 192.168.240.150
Host is up (0.00072s 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 21.97 seconds
```

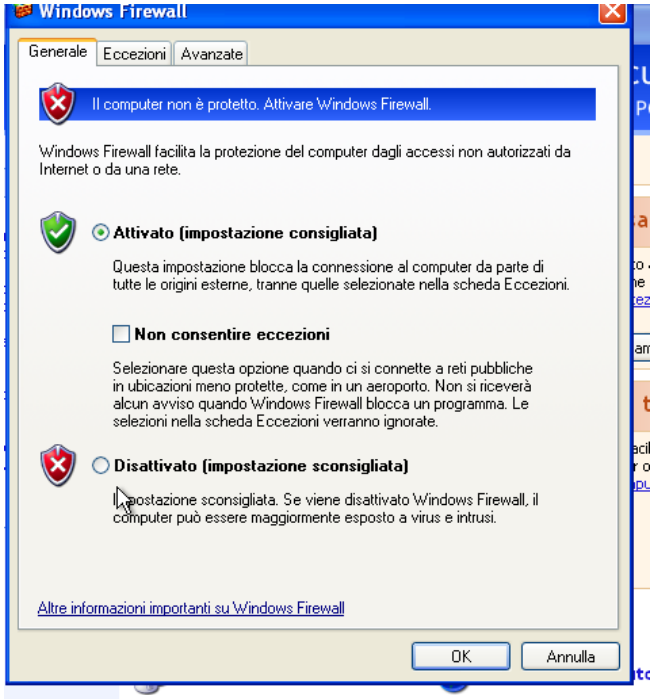
Con il rispettivo report

~/report.txt - Mousepad

File Edit Search View Document Help

```
1 # Nmap 7.92 scan initiated Mon Dec 19 08:23:07 2022 as: nmap -sV -o report.txt
  192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00072s latency).
4 Not shown: 997 closed tcp ports (conn-refused)
5 PORT    STATE SERVICE      VERSION
6 135/tcp open  msrpc        Microsoft Windows RPC
7 139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
9 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/
  o:microsoft:windows_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/
  submit/ .
12 # Nmap done at Mon Dec 19 08:23:28 2022 -- 1 IP address (1 host up) scanned in 21.97
  seconds
```

Ora attivo il firewall di XP e riprovo la scansione



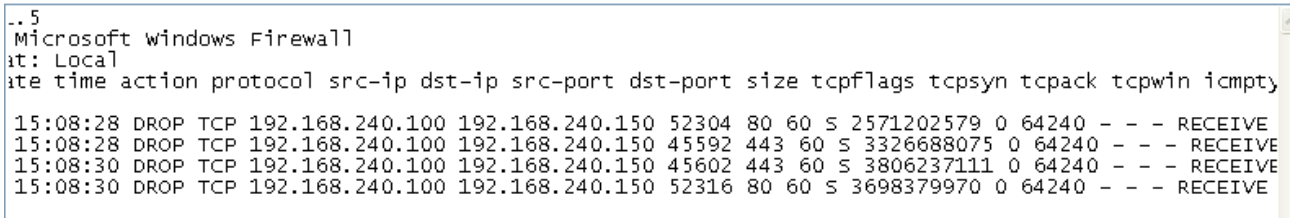

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -o report2.txt  192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:24 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.22 seconds
```

~/report2.txt - Mousepad

File Edit Search View Document Help

```
1 # Nmap 7.92 scan initiated Mon Dec 19 08:24:50 2022 as: nmap -sV -o report2.txt
  192.168.240.150
2 # Nmap done at Mon Dec 19 08:24:55 2022 -- 1 IP address (0 hosts up) scanned in 4.22
  seconds
3
```

La differenza principale tra le due scansioni è che la presenza del firewall accesso non fa comunicare le due macchine, non potendo quindi scansionare le porte della macchina target. Possiamo vederlo anche dai log di sessione salvati nel percorso “C:WINDOWS:pfirewall”



```
..5
 Microsoft Windows Firewall
at: Local
ate time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmpty

 15:08:28 DROP TCP 192.168.240.100 192.168.240.150 52304 80 60 S 2571202579 0 64240 - - - RECEIVE
 15:08:28 DROP TCP 192.168.240.100 192.168.240.150 45592 443 60 S 3326688075 0 64240 - - - RECEIVE
 15:08:30 DROP TCP 192.168.240.100 192.168.240.150 45602 443 60 S 3806237111 0 64240 - - - RECEIVE
 15:08:30 DROP TCP 192.168.240.100 192.168.240.150 52316 80 60 S 3698379970 0 64240 - - - RECEIVE
```