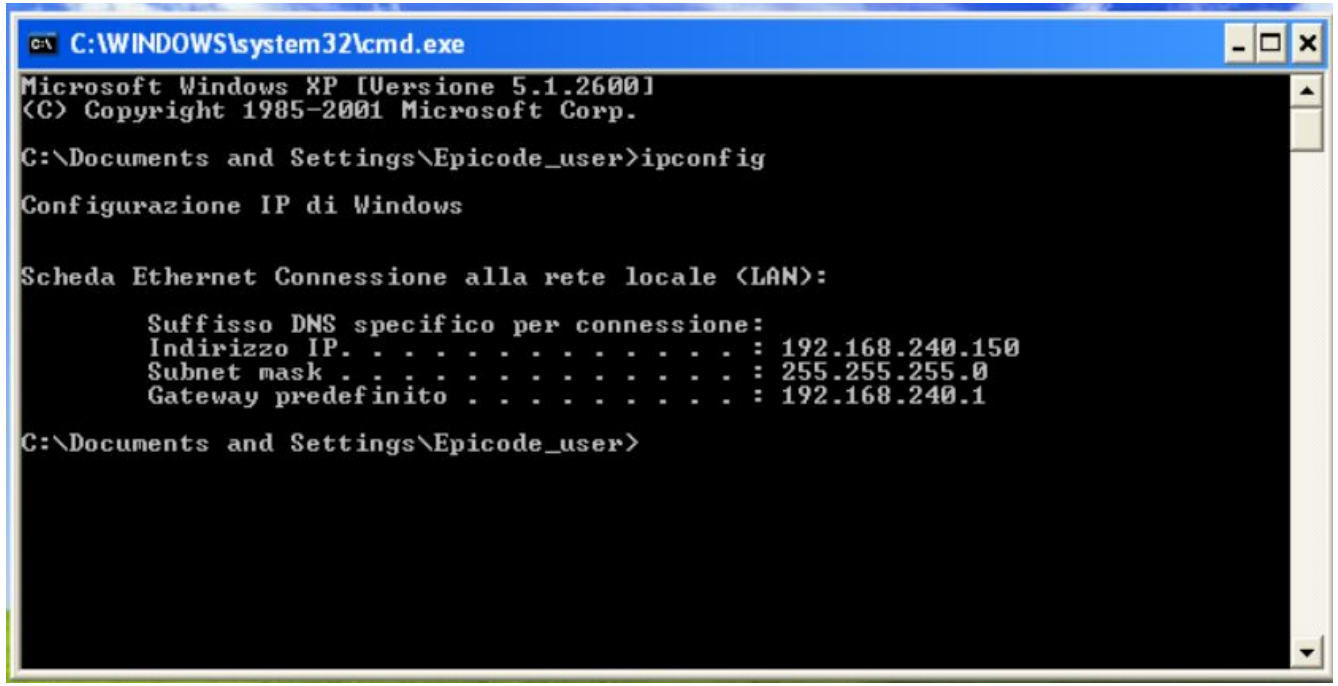
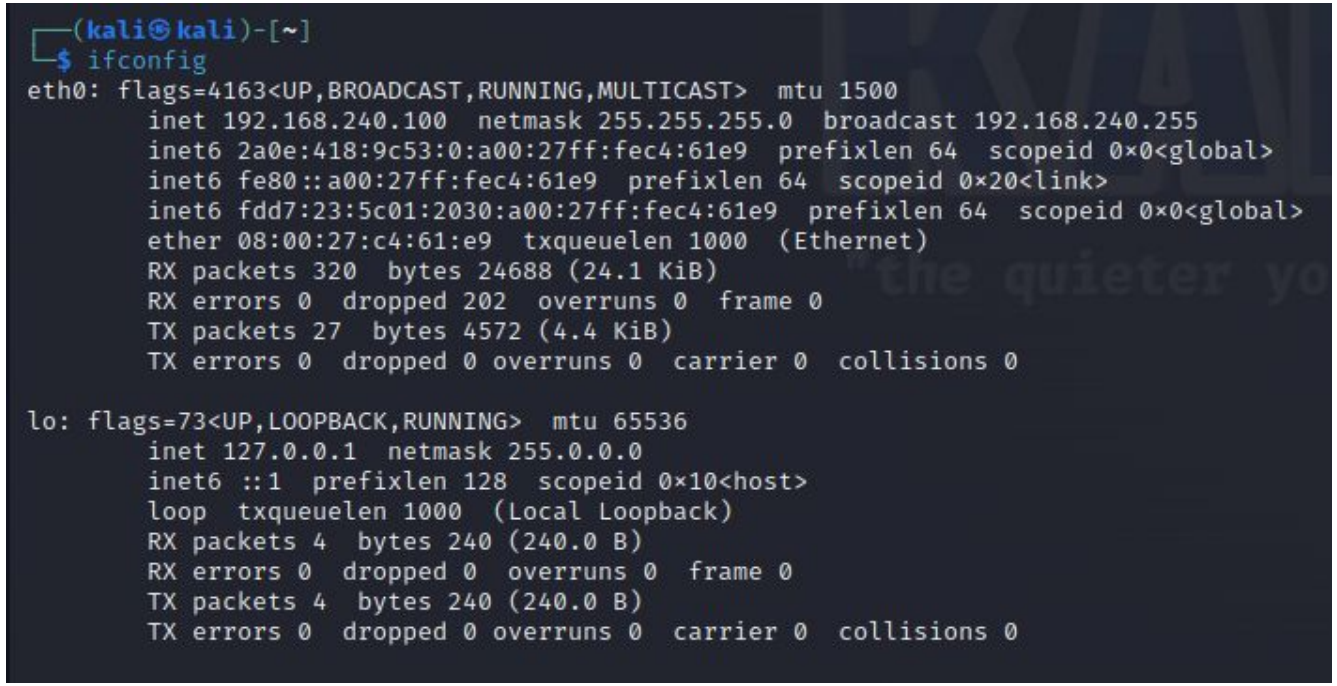
EPICODE

Progetto Alessandro Moscetti 07/11

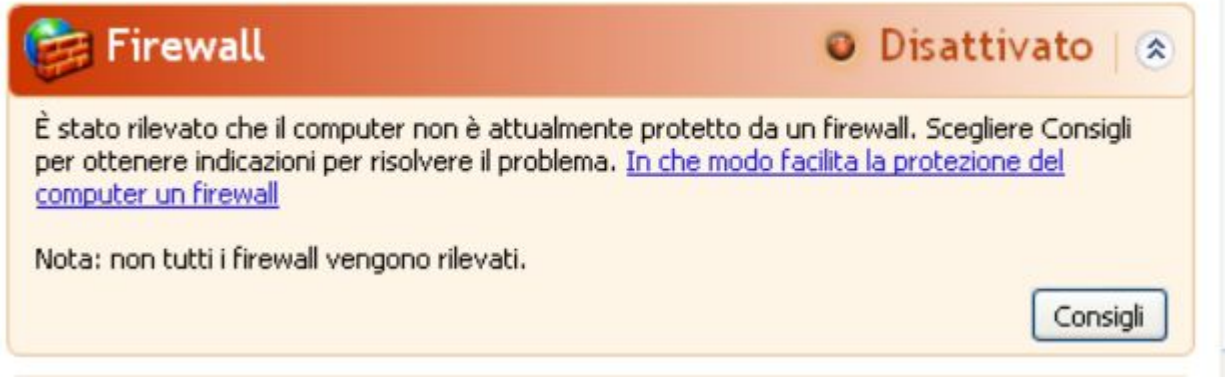




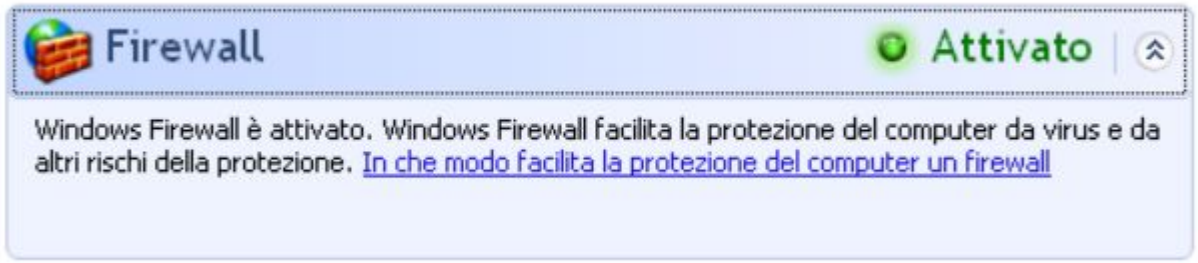
Sostituzione indirizzi IP macchine virtuali.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 13:07 CET
Nmap scan report for 192.168.240.150
Host is up (0.00055s latency).
Not shown: 997 closed tcp ports (reset)
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
MAC Address: 08:00:27:BA:9D:D9 (Oracle VirtualBox virtual NIC)
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 19.55 seconds
```



Prima scansione verso la macchina Windows XP con Firewall disattivato.
Possiamo notare come il tool nmap riesca a stabilire tutti i servizi attivi con le relative versioni, il MAC address e il sistema operativo utilizzato dalla macchina.




```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 13:10 CET
Nmap scan report for 192.168.240.150
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:BA:9D:D9 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.56 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
^C
── 192.168.240.150 ping statistics ──
5 packets transmitted, 0 received, 100% packet loss, time 4088ms
```

Seconda scansione verso la macchina Windows XP con Firewall attivato.
Possiamo notare come il tool nmap non ci dia nessuna informazione sulla macchina e dalla fig. 3 notiamo anche che non riceviamo risposta neanche da un ping.
Questo accade perchè il firewall abilitato è a filtraggio dinamico come la stragrande maggioranza dei firewall in circolazione oggigiorno.
Un Firewall a filtraggio dinamico andrà a bloccare tutte le connessioni in entrata verso il dispositivo che non siano prima partite dal dispositivo stesso.

Conclusione

Con questo semplice esercizio notiamo come anche la semplice disattivazione del firewall ci possa esporre a dei rischi notevoli in termini di sicurezza informatica.

Grazie per l’attenzione.