

# **EPICODE**

**Progetto Alessandro Moscetti 07/11**



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.240.150
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.240.1

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

Sostituzione indirizzi IP macchine virtuali.

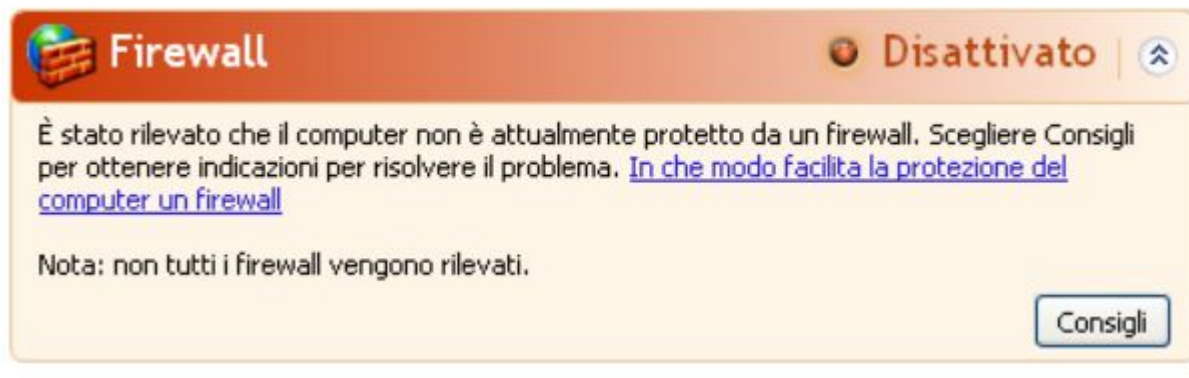
```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255
    inet6 2a0e:418:9c53:0:a00:27ff:fec4:61e9 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::a00:27ff:fec4:61e9 prefixlen 64 scopeid 0x20<link>
    inet6 fdd7:23:5c01:2030:a00:27ff:fec4:61e9 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:c4:61:e9 txqueuelen 1000 (Ethernet)
    RX packets 320 bytes 24688 (24.1 KiB)
    RX errors 0 dropped 202 overruns 0 frame 0
    TX packets 27 bytes 4572 (4.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

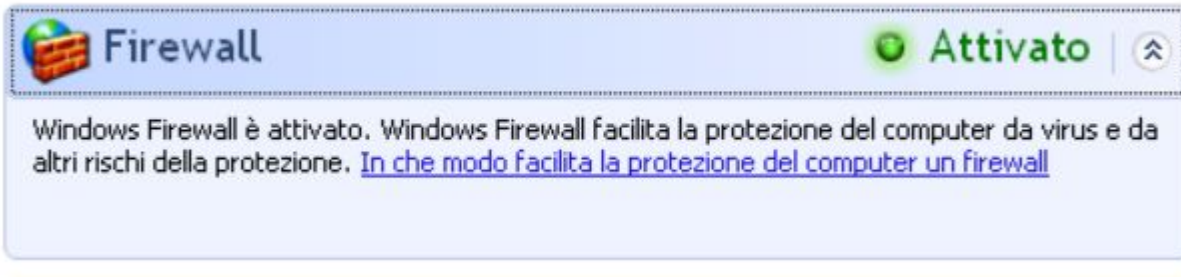
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(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 oggi. 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.**

