


Security Operation: azioni preventive

La traccia di oggi ci chiedeva di studiare il comportamento del nmap verso Windows XP prima con il firewall attivato poi senza questo attivato.

1) La prima richiesta era quella di cambiare le configurazioni di rete di KALI e XP:

Kali : 192.168.240.100



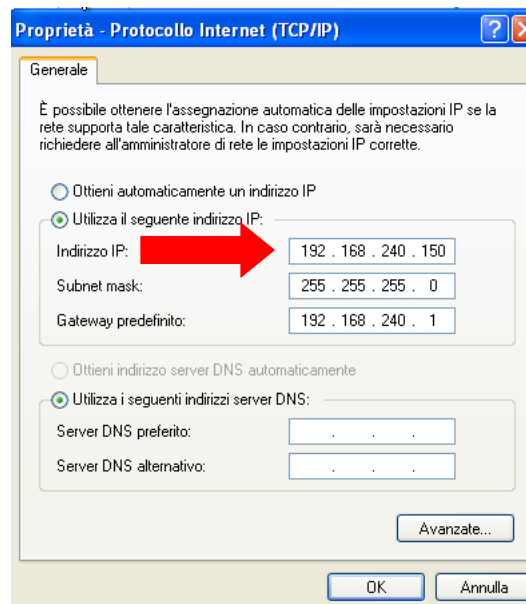
```
GNU nano 6.3
# This file describes the network i
# and how to activate them. For mor

source /etc/network/interfaces.d/*

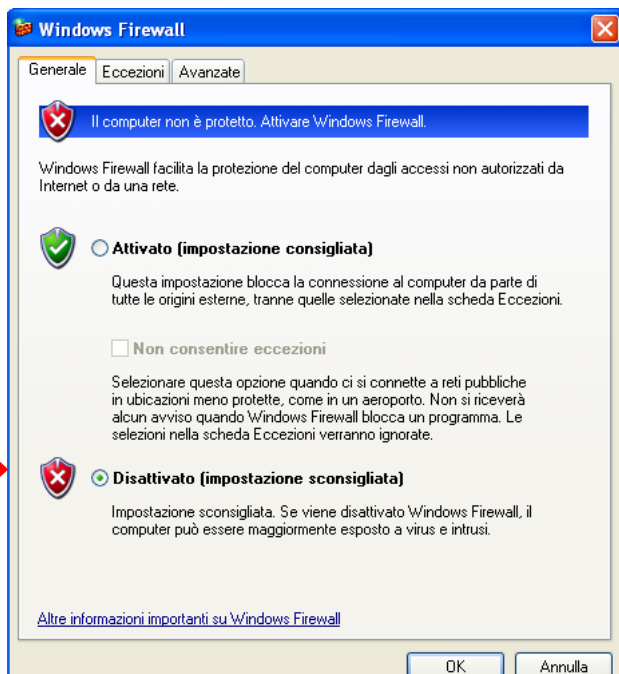
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100
netmask 255.255.255.0
#network 192.168.240.0
#broadcast 192.168.240.255
gateway 192.168.240.1
```

XP : 192.168.240.150

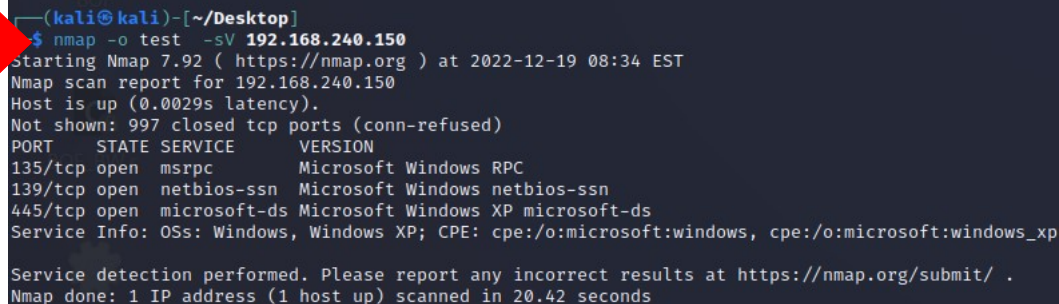


2) Ci veniva poi richiesto di disattivare il firewall:



Una volta fatto ciò bisognava poi fare un nmap da kali verso xp, con i seguenti parametri:
nmap -o test -sV 192.168.240.150

-o: per avere un file report nel attuale directory
-sV: version detection

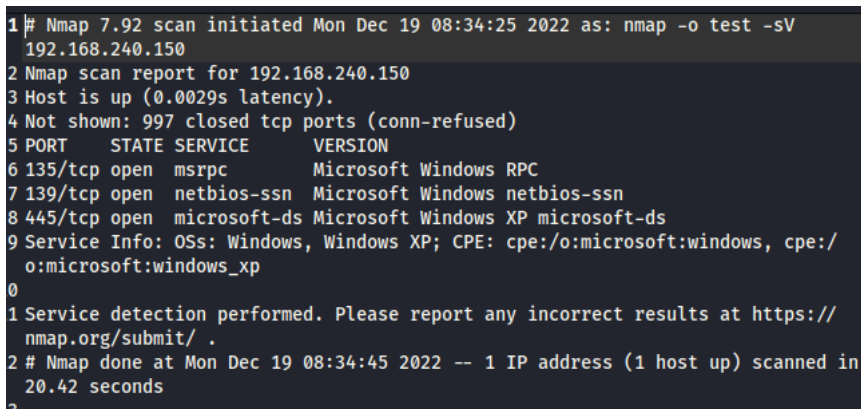


A terminal window on Kali Linux showing the execution of the command `nmap -o test -sV 192.168.240.150`. A red arrow points to the command line. The output shows the scan results for 192.168.240.150, indicating it is up and listing three open ports: 135/tcp (msrpc), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds). The service info indicates Windows XP.

```
(kali@kali)-[~/Desktop]
$ nmap -o test -sV 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:34 EST
Nmap scan report for 192.168.240.150
Host is up (0.0029s 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 20.42 seconds
```

Questo è il risultato del report dello switch -o :
Come si può vedere senza firewall l' nmap ci mostra le tre porte aperte con i rispettivi servizi.

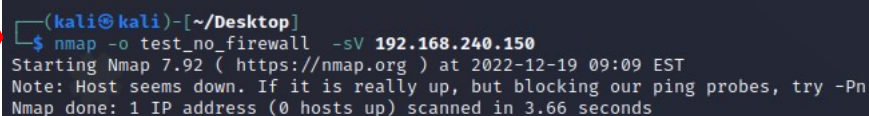


A terminal window showing the same nmap scan as above, but with line numbers 1 through 9 added to the left of each line. A red arrow points to line 5, which is the header of the open ports table.

```
1 # Nmap 7.92 scan initiated Mon Dec 19 08:34:25 2022 as: nmap -o test -sV
2 192.168.240.150
3 Nmap scan report for 192.168.240.150
4 Host is up (0.0029s latency).
5 Not shown: 997 closed tcp ports (conn-refused)
6 PORT      STATE SERVICE      VERSION
7 135/tcp    open  msrpc        Microsoft Windows RPC
8 139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
9 445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
10 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/
11 o:microsoft:windows_xp
12
13 Service detection performed. Please report any incorrect results at https://
14 nmap.org/submit/ .
15
16 # Nmap done at Mon Dec 19 08:34:45 2022 -- 1 IP address (1 host up) scanned in
17 20.42 seconds
18
19
```

3) In seguito ho poi attivato il firewall di XP e questo è stato il risultato con lo stesso nmap:

nmap -o test_firewall -sV 192.168.240.150

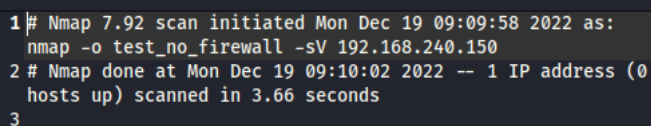


A terminal window showing the execution of the command `nmap -o test_firewall -sV 192.168.240.150`. A red arrow points to the command line. The output shows that the host seems down because the firewall is blocking the ping probes.

```
(kali@kali)-[~/Desktop]
$ nmap -o test_no_firewall -sV 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 09:09 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 3.66 seconds
```

Questo è il risultato del report dello switch -o :

Come si può vedere una volta acceso il firewall non si può più vedere i servizi e le porte in ascolto.



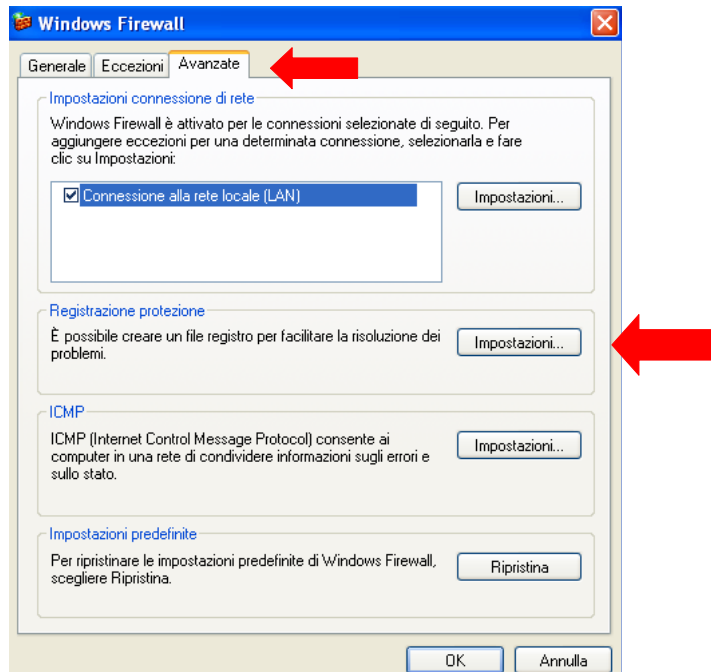
A terminal window showing the same nmap scan as above, but with line numbers 1 through 3 added to the left of each line. A red arrow points to line 2, which indicates that no hosts were up.

```
1 # Nmap 7.92 scan initiated Mon Dec 19 09:09:58 2022 as:
2 nmap -o test_no_firewall -sV 192.168.240.150
3 # Nmap done at Mon Dec 19 09:10:02 2022 -- 1 IP address (0
4 hosts up) scanned in 3.66 seconds
5
```

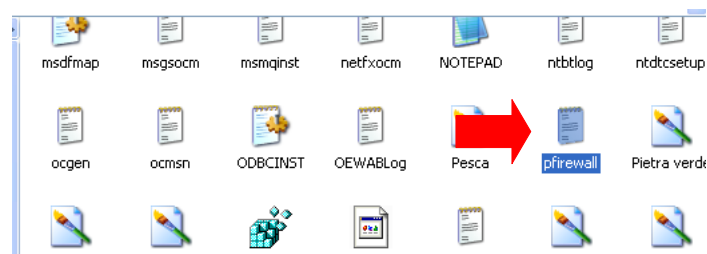
BONUS:

La richiesta bonus era quella di monitorare i file di log durante queste operazioni.

Come prima cosa con il firewall attivo sono andato nella sezione windows firewall poi in avanzate, nella sezione Registrazione protezione:



Creiamo quindi il file che si chiamerà pfirewall, andiamo poi a cercarlo nella cartella WINDOWS:



Quindi aprendolo possiamo notare la scansione che abbiamo fatto con nmap venire bloccata.

```
pfirewall - Blocco note
File Modifica Formato Visualizza ?
#Version: 1.5
#Software: Microsoft windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tc
2022-12-19 15:12:17 OPEN TCP 192.168.240.150 192.168.240.100 1037 4444 - - - - -
2022-12-19 15:12:18 CLOSE TCP 192.168.240.150 192.168.240.100 1037 4444 - - - - -
2022-12-19 15:12:28 OPEN TCP 192.168.240.150 192.168.240.100 1037 4444 - - - - -
2022-12-19 15:12:29 CLOSE TCP 192.168.240.150 192.168.240.100 1037 4444 - - - - -
```

Disattivando il firewall questo file non ci sarà possiamo quindi dedurre che il nostro client non sia protetto in alcuno modo.