SECURITY OPERATION: AZIONI PREVENTIVE

Eleonora Viola

INDICE

PREPARAZIONE

In primo luogo cambiamo gli Ip come da traccia e lanciamo un ping per verificare la connessione.
Per comodità ho impostato un alias per Windows XP.

CAMBIO IP KALI e ALIAS HOST

```
auto eth1
iface eth1 inet static
address 192.168.240.100/24
netmask 255.255.255.0
```

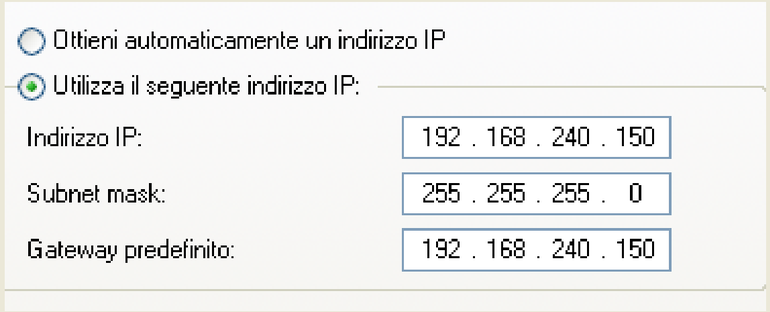
```
    valid_lft forever preferred_lft forever
: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_code
    link/ether 42:a9:7e:7e:68:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.240.100/24 brd 192.168.240.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::40a9:7eff:fe7e:6859/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

```
File  Actions  Edit  View  Help
 GNU nano 8.0                                    /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.240.150    xp
```

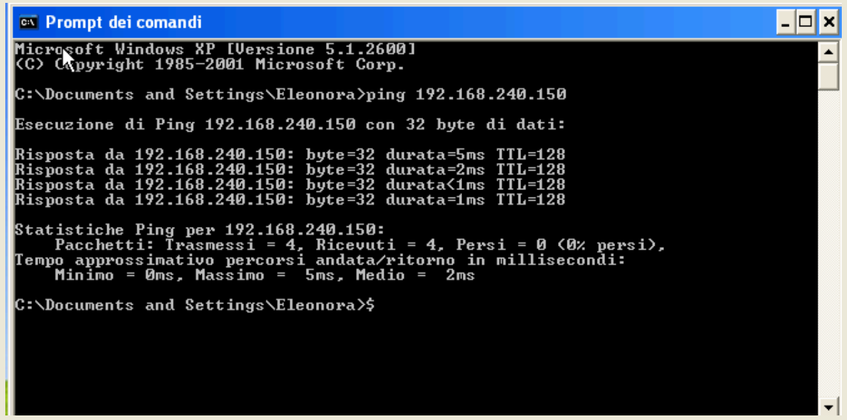
CAMBIO IP WINDOWS XP




```
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 . . . . . . . . . . : 192.168.240.150
```

PING



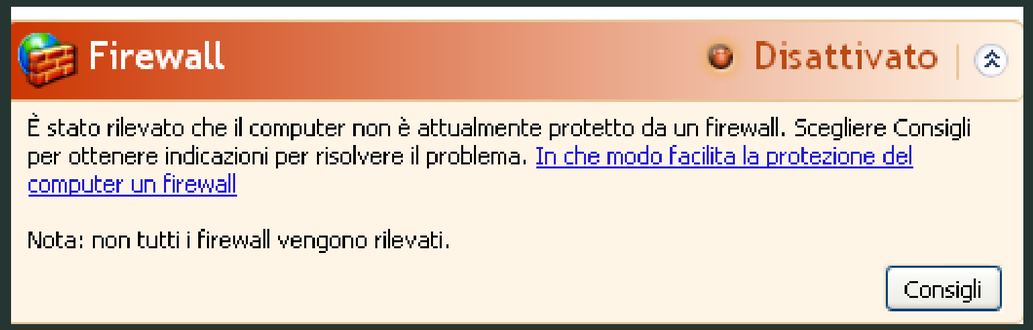

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping -c4 xp
PING xp (192.168.240.150) 56(84) bytes of data.
64 bytes from xp (192.168.240.150): icmp_seq=1 ttl=128 time=6.18 ms
64 bytes from xp (192.168.240.150): icmp_seq=2 ttl=128 time=1.74 ms
64 bytes from xp (192.168.240.150): icmp_seq=3 ttl=128 time=2.64 ms
64 bytes from xp (192.168.240.150): icmp_seq=4 ttl=128 time=1.26 ms

── xp ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.264/2.955/6.176/1.924 ms

┌──(kali㉿kali)-[~/Desktop]
```

FIREWALL DISATTIVO

In secondo luogo possiamo procedere con un Nmap verso windows XP, come impostazione di default ha il firewall disattivato.
Utilizziamo l'opzione -sV per stabilire le porte aperte, le informazioni e la versione dei servizi attivi, per poi salvare l'output su un file di testo.



Troviamo appunto 3 porte aperte:

1. **135/tcp open msrpc:**
- Utilizzata per le chiamate di procedura remota di Microsoft (RPC).
- È una porta critica per le funzionalità di rete di Windows e può essere un vettore di attacco se non adeguatamente protetta.

2. 139/tcp open netbios-ssn:
- Utilizzata dal servizio NetBIOS per sessioni di rete su TCP/IP.
- Tipicamente usata per condivisioni di file o stampanti.

3. 445/tcp open microsoft-ds:
- Utilizzata per la condivisione di file e stampanti tramite SMB (Server Message Block) su TCP/IP.
- Sostituisce la funzionalità del NetBIOS sulle reti più moderne.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -o scans9l1 xp
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 07:15 PDT
Nmap scan report for xp (192.168.240.150)
Host is up (0.0019s 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 7.39 seconds
```

FIREWALL ATTIVO

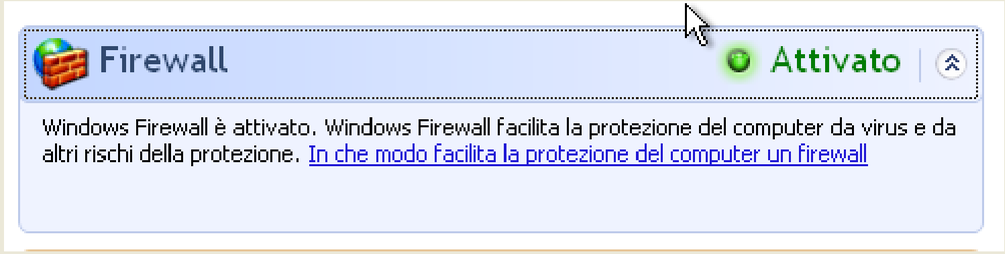
Per potere rimediare all'accesso di queste porte possiamo attivare le funzioni sul firewall su XP.

Notiamo che che il dispositivo sembra essere offline, questo perché il firewall ci impedisce di pingare la macchina.

Come da suggerimento di nmap si può utilizzare lo switch -Pn in modo da evitare il ping e occuparsi subito della service discovery.

Aggiungo anche il comando **nmap -sV -Pn -T4 xp >> scans9l1** per aggiungerlo al report creato prima.

Da questo scan si può vedere che con il firewall attivo non vediamo le porte aperte.




```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV xp
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 07:36 PDT
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 3.10 seconds
```

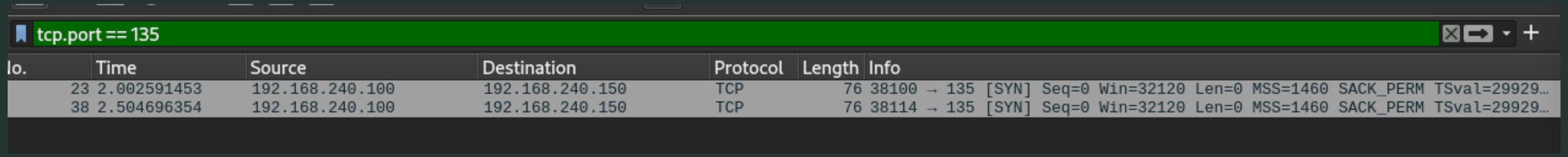
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -Pn -T4 xp >> scans9l1
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -Pn -T4 xp
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 07:38 PDT
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 3.00% done; ETC: 07:40 (0:02:09 remaining)
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 86.00% done; ETC: 07:40 (0:00:14 remaining)
Nmap scan report for xp (192.168.240.150)
Host is up.
All 1000 scanned ports on xp (192.168.240.150) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 101.51 seconds
```

WIRESHARK

Possiamo verificare la trasmissione dei pacchetti con il firewall attivato attraverso il tool Wireshark, come esempio mettiamo la porta 135 (che prima abbiamo trovato aperta) e possiamo confermare che il three-way handshake non va a buon fine perché manca l' ACK.



Mentre disattivando il firewall possiamo vedere come la situazione cambia e il three-way handshake va a buon fine.