S9L1

SCRITTO DA: SARAH ORTIZ

TRACCIA

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato. L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

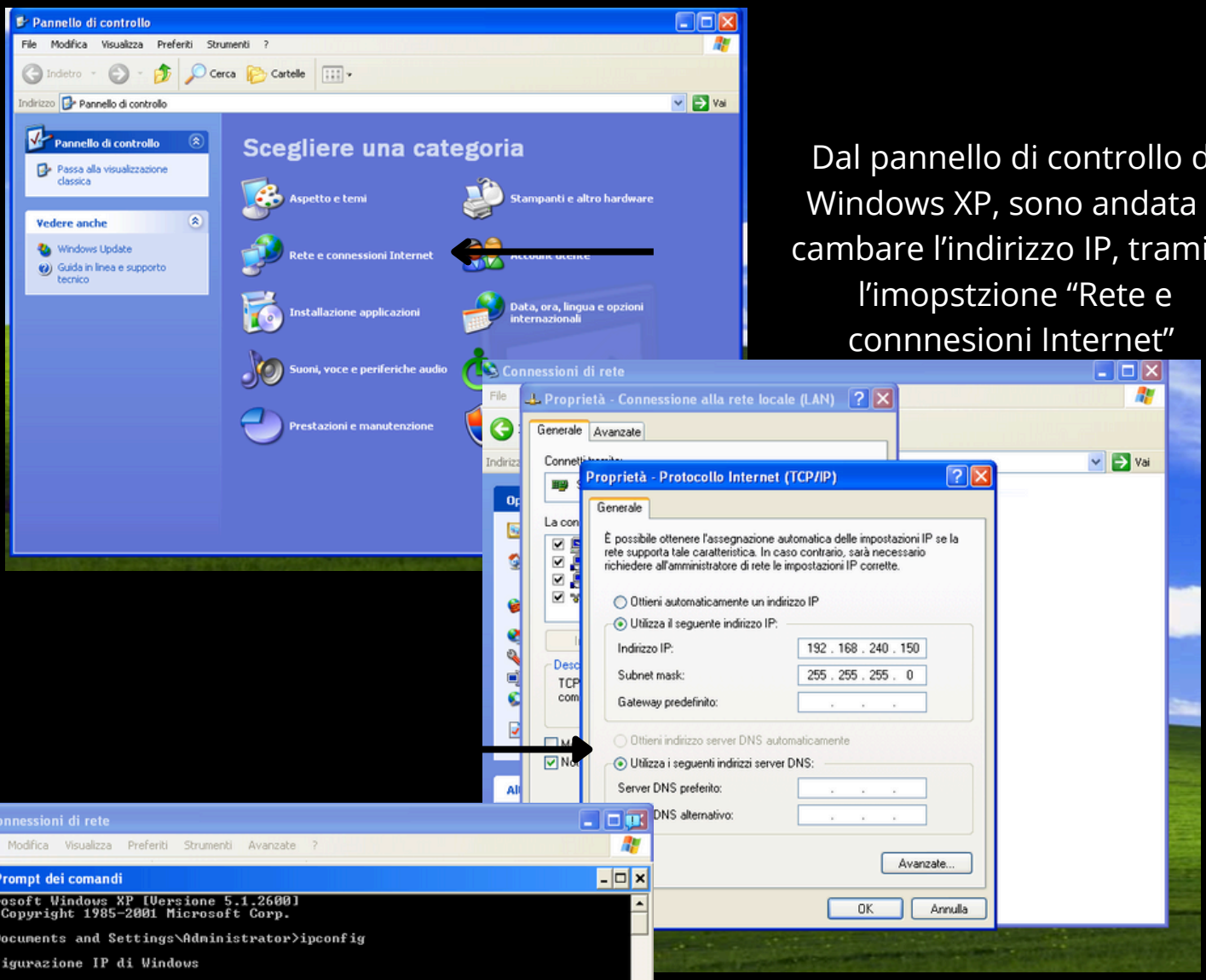
1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch–sV, per la service detection e -o nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch–sV.
5. Trovare le eventuali differenze e motivarle

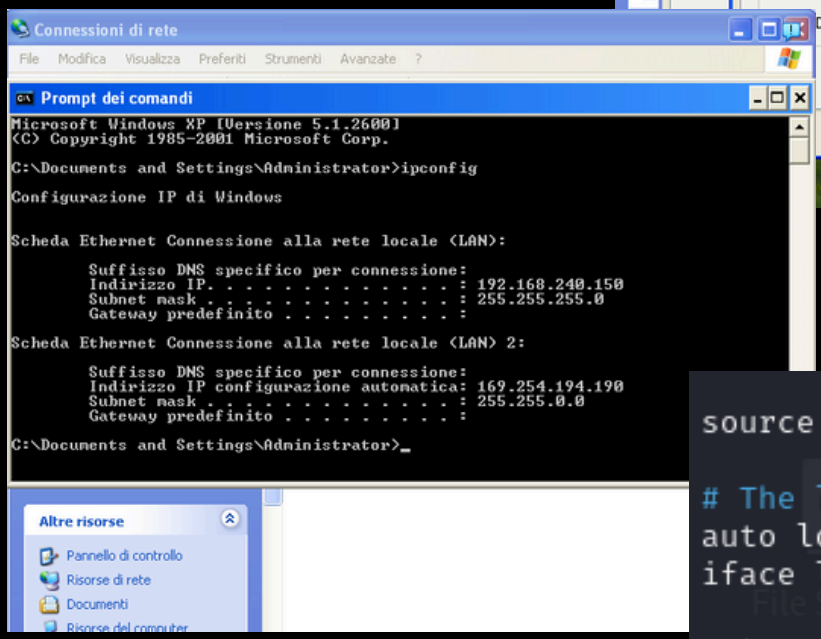
Traccia: Che differenze notate? E quale può essere la causa del risultato diverso?

REQUISITI

Configurate l'indirizzo di Windows XP come di seguito:
192.168.240.150
Configurate l'indirizzo della macchina Kali come di seguito:
192.168.240.100

Dal pannello di controllo di Windows XP, sono andata a cambare l’indirizzo IP, tramite l’imopstzione “Rete e connnesioni Internet”



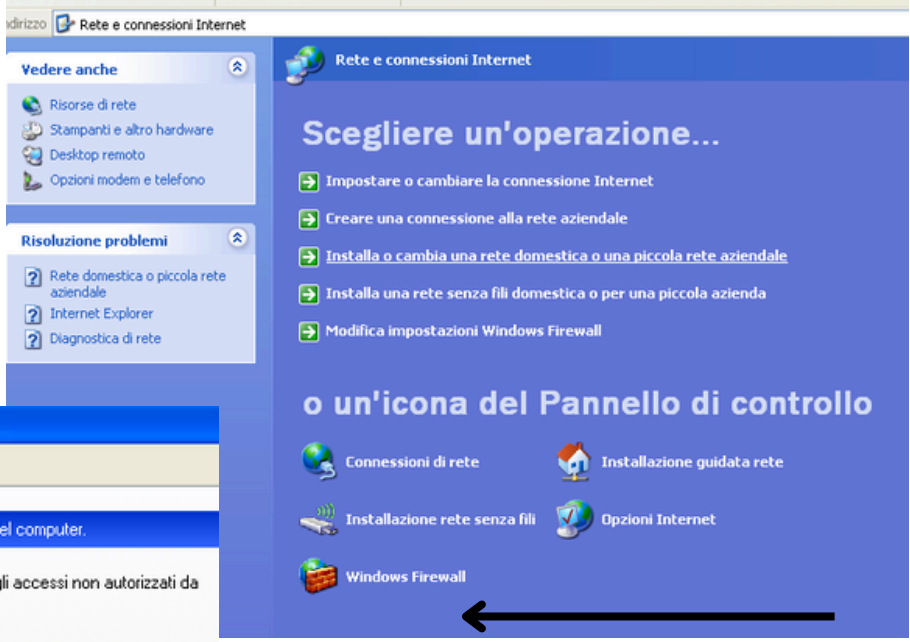


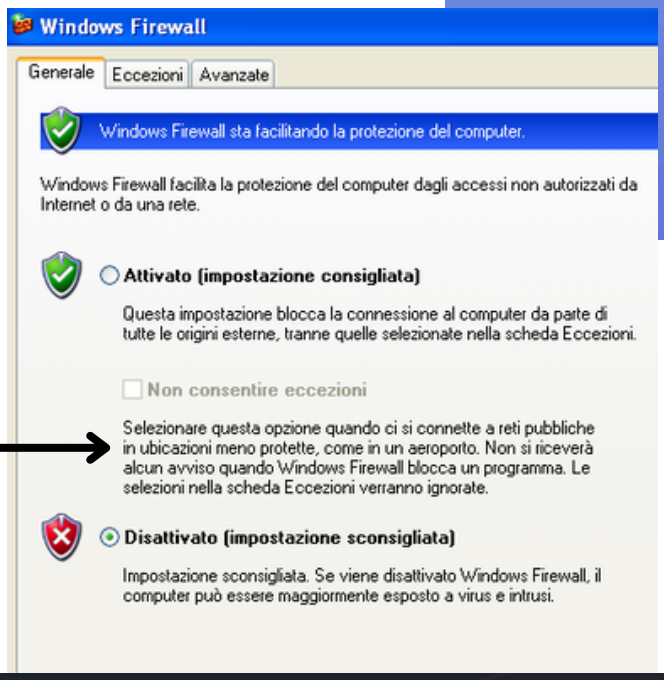
come ho cambiato l’indirizzo anche alla macchina di Kali, poi ho fatto in modo che pingassero insieme, per vedere se comunicavano

```
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
gateway 192.168.240.1
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.240.150

PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=2061 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1022 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=7.43 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=3.05 ms
^C
— 192.168.240.150 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
rtt min/avg/max/mdev = 3.054/773.339/2061.061/851.457 ms, pipe 3

┌──(kali㉿kali)-[~]
└─$
```

Pe poter visualizzare le porte che sono in esecuzione, andremo a disattivar eil firewall da Windows XP

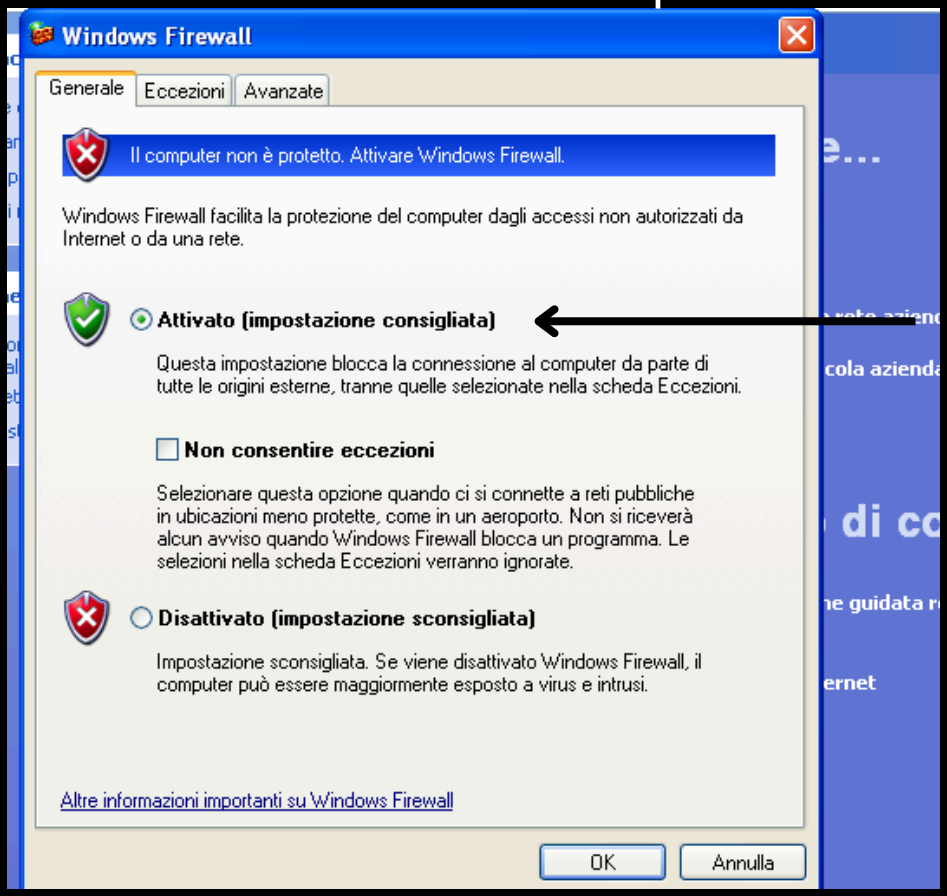





```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 07:15 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0013s 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: 08:00:27:5C:8D:1C (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 21.72 seconds
```

con il comando “sudo nmap -sV 192.168.240.150” identificherà le porte aperte e i servizi in esecuzione.

Successivamente andremo ad attivare il firewall, per poter vedere, se effettivamente c'è stato un cambiamento con le porte



Riutilizziamo il comando "sudo nmap -sV 192.168.240.150" per scoprire i servizi in esecuzione sulla macchina Windows XP e per mantenere coerenza nei risultati.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 07:16 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (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 25.38 seconds
```

CONSIDERAZIONI FINALI

- Il firewall è progettato per bloccare il traffico su porte specifiche e migliorare la sicurezza della rete.
- Il confronto tra i risultati della scansione con il firewall abilitato e disabilitato ti aiuta a capire come il firewall protegge la macchina Windows XP e quali servizi sono esposti al rischio.
- La porta 135 con il firewall attivato notiamo che non è aperto, indicando che il firewall la blocca.