Consegna S9-L1

Security Operation: azioni preventive

Traccia

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:

Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP

Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection)

Abilitare il Firewall sulla macchina Windows XP

Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

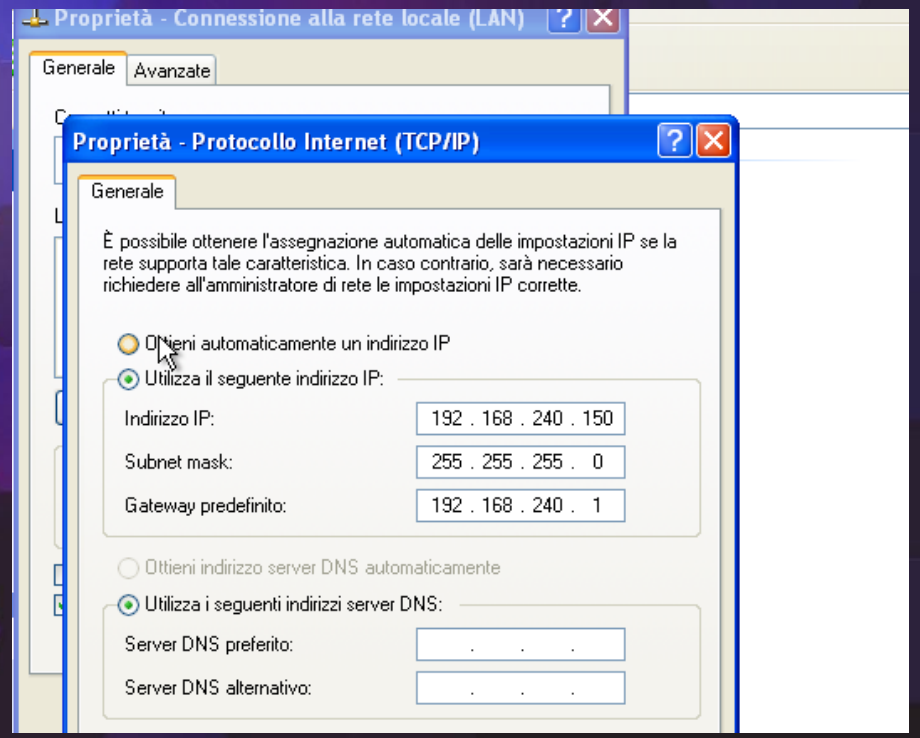
Che differenze notate? E quale può essere la causa del risultato diverso?

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

Configurazione macchine

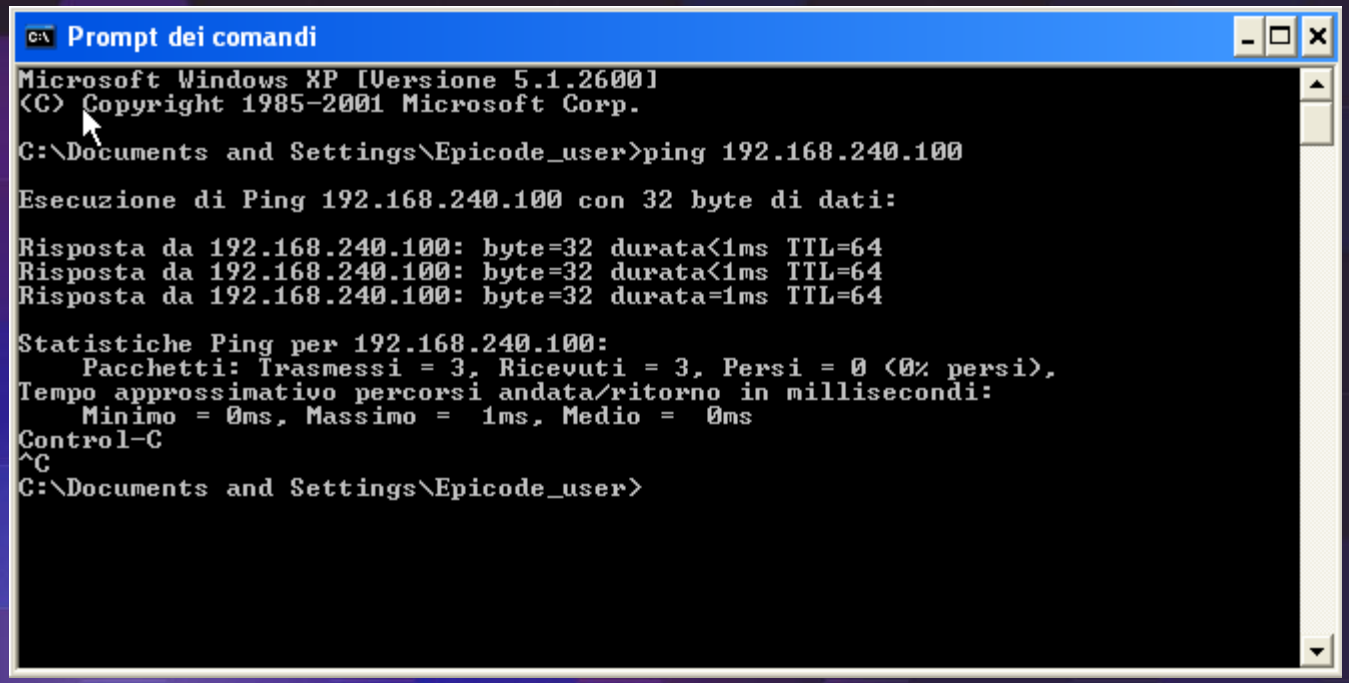
Per prima cosa è stato necessario configurare le macchine sulla stessa rete per metterle in comunicazione. Sono stati inseriti gli indirizzi IP richiesti dalla traccia

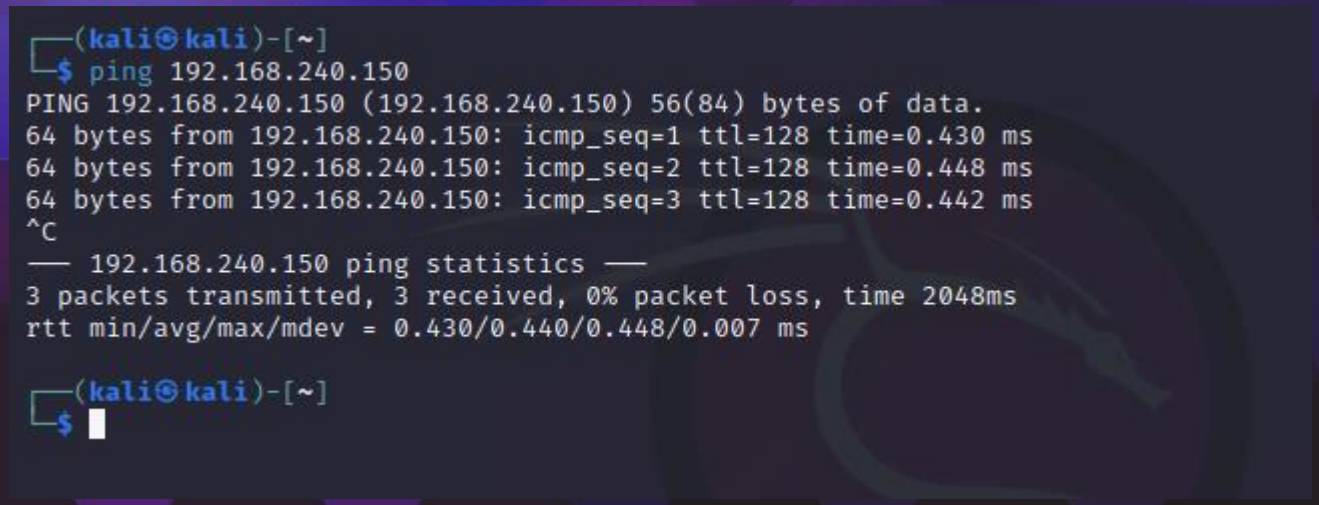
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

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
```



Comando Ping

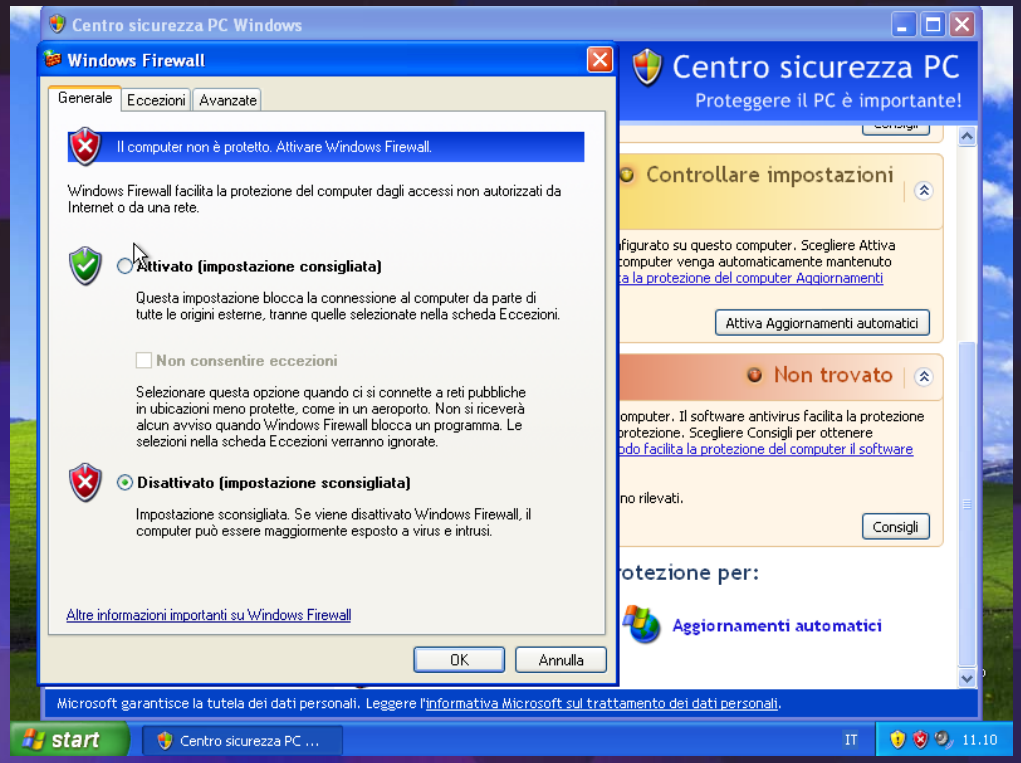
Con il comando ping, è stata confermata la corretta comunicazione tra le due macchine. Esse sono in grado di inviare e ricevere pacchetti ICMP tra loro.





Scansione con Firewall disattivato

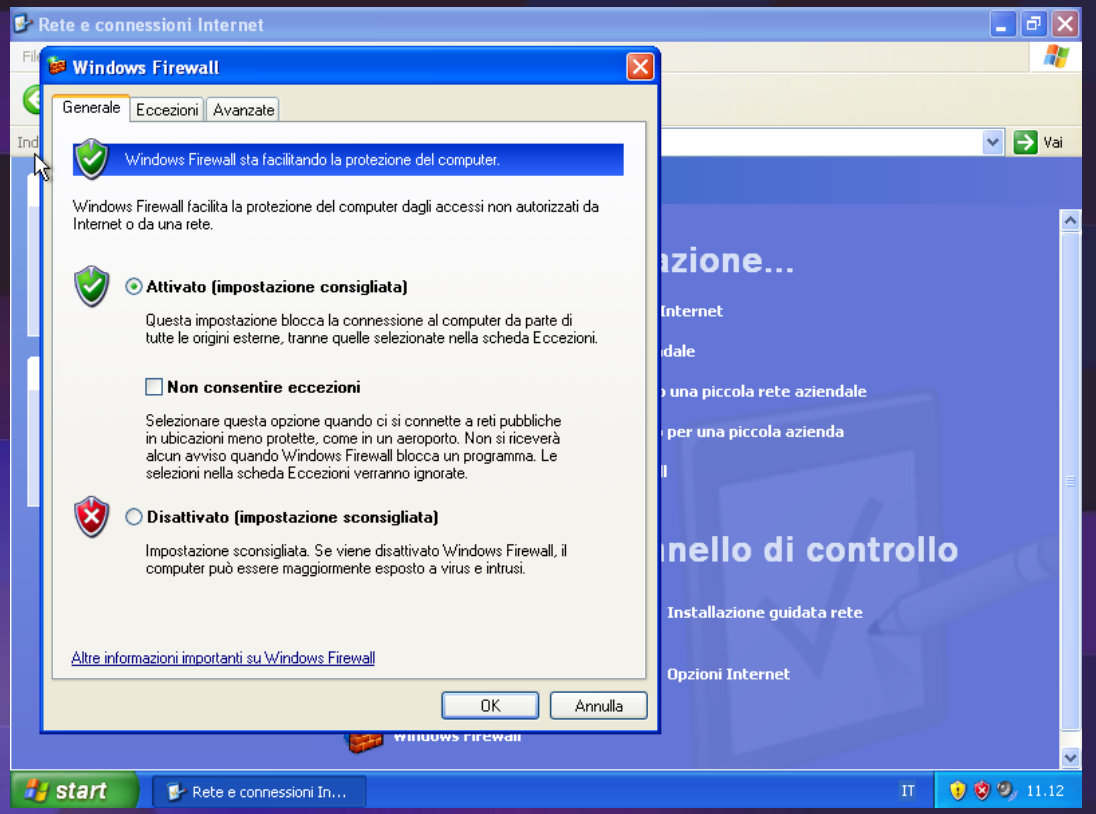
Inizialmente il firewall di Windows XP risultava disattivato. Una prima scansione da Kali verso la macchina Windows tramite il tool nmap ha riscontrato alcune porte aperte.




```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 12:11 CET
Nmap scan report for 192.168.240.150
Host is up (0.00017s 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 20.49 seconds

┌──(kali㉿kali)-[~]
└─$
```

Scnasione con Firwall attivato

A questo punto è stata ripetuta la scansione ma solo dopo aver attivato il Firwall di Windows. A differenza di prima, tutte le porte sono risultate filtrate. Il firewall ha svolto correttamente il suo ruolo.




```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 12:20 CET
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 3.21 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 12:26 CET
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 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 214.73 seconds

┌──(kali㉿kali)-[~]
└─$
```

Fine della presentazione

Amedeo Natalizi