CONSEGNA S9/L1

Security operation: azioni preventive

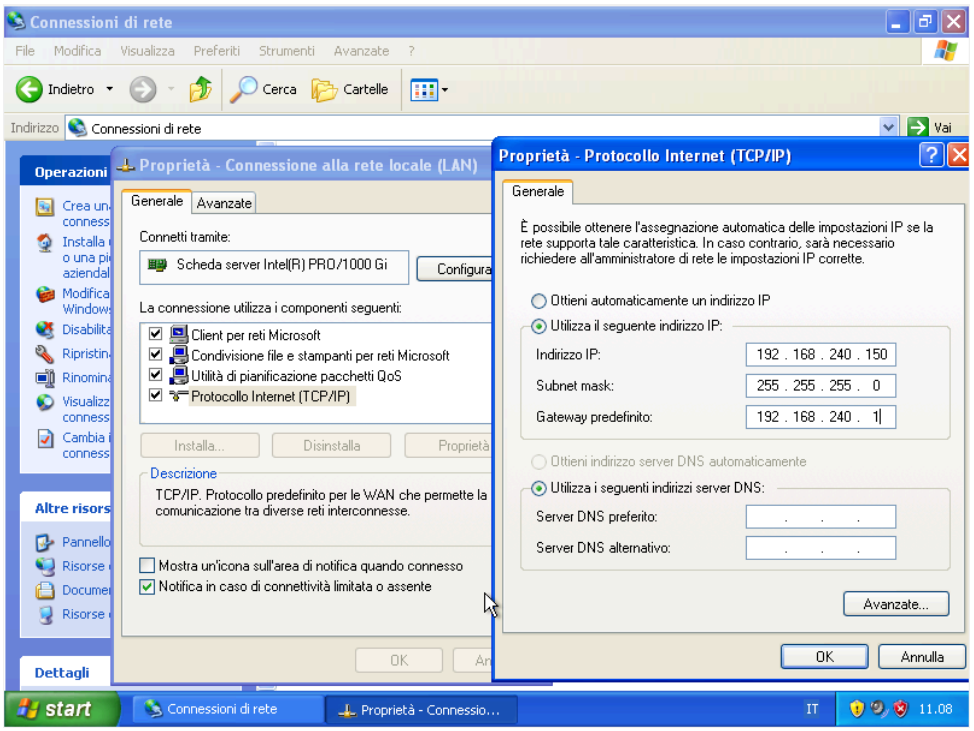
L’esercizio di oggi è verificare in che modo l’attivazione del Firewall impatta il risultato di una scansione dei servizi dall’esterno.
Per questo motivo effettueremo una scansione con Nmap della macchina virtuale Windows XP (con ip 192.168.240.150) prima dell’attivazione del firewall e dopo, per notare le differenze.

Cambio degli IP

Cambio IP Kali:

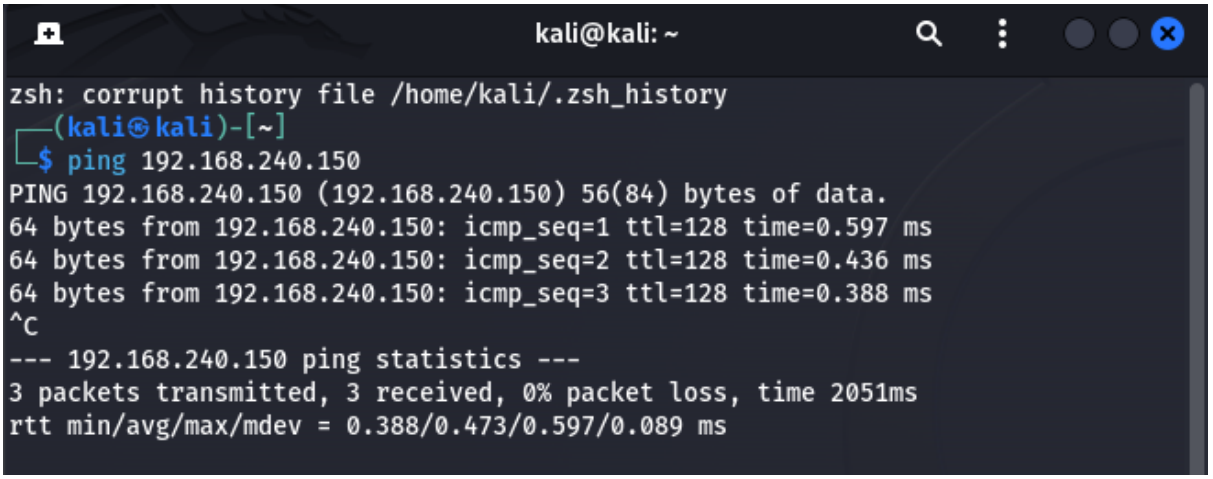
```
  GNU nano 7.2                  /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

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
gateway 192.168.240.1
netmask 255.255.255.0
```

Cambio IP Windows XP:

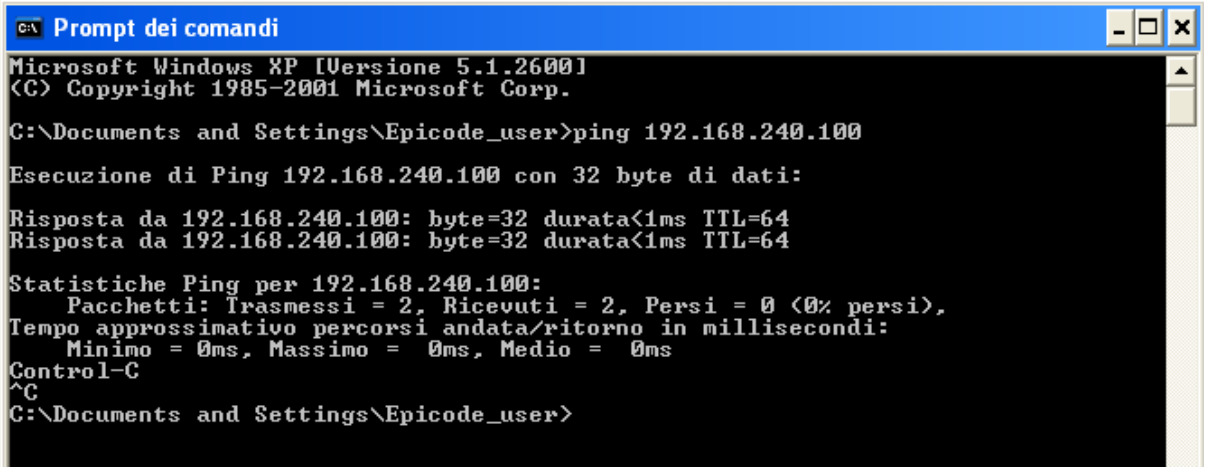


Ping delle macchine

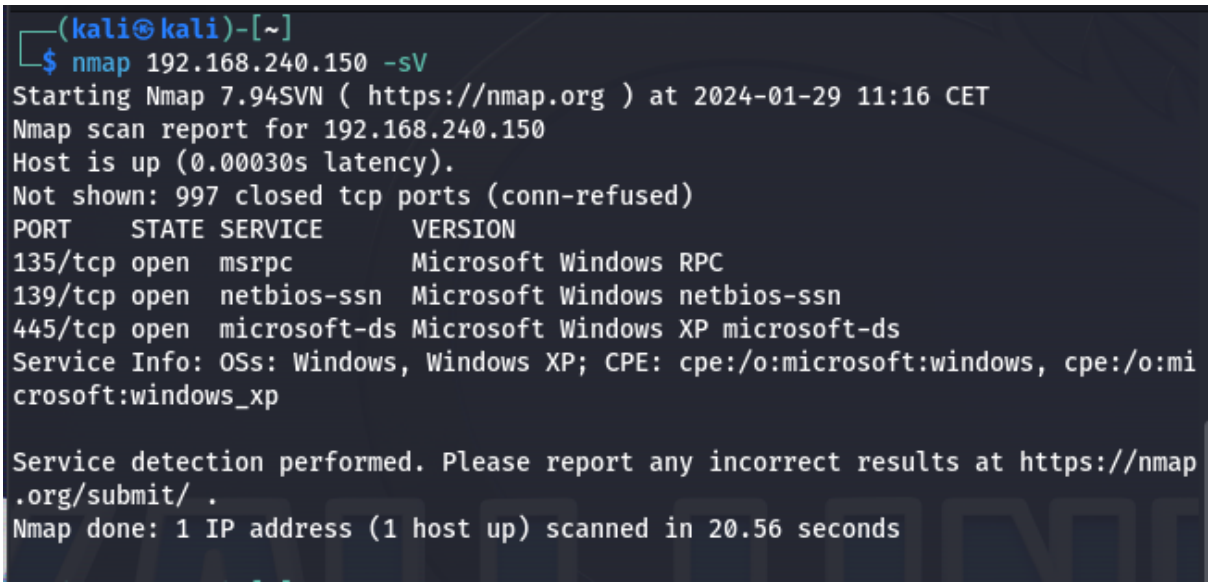
Da Kali a Windows:



Da windows a Kali:



Scansione Nmap pre attivazione firewall



In questo caso abbiamo visibili gli stati delle porte e gli annessi servizi in ascolto su ciascuna di esse, versione compresa.

Attivazione firewall

Scansione Nmap post attivazione firewall

Procediamo con lo stesso tipo di scansione effettuata in precedenza ma con il firewall di Windows XP ora attivo:

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.240.150 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 11:21 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 3.13 seconds
```

Non riceviamo informazioni sulle porte della macchina bersaglio. Nmap ci suggerisce di provare una scansione con lo switch -Pn che è utile per disabilitare la fase di discorvery dell'host, che di solito comporta l'invio di pacchetti di probing (come ping).

Di fatto se proviamo a lanciare il comando ping verso la macchina Windows questo è quello che otteniamo:

```
┌──(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 ---
8 packets transmitted, 0 received, 100% packet loss, time 7156ms
```

Scansione Nmap -Pn post attivazione firewall

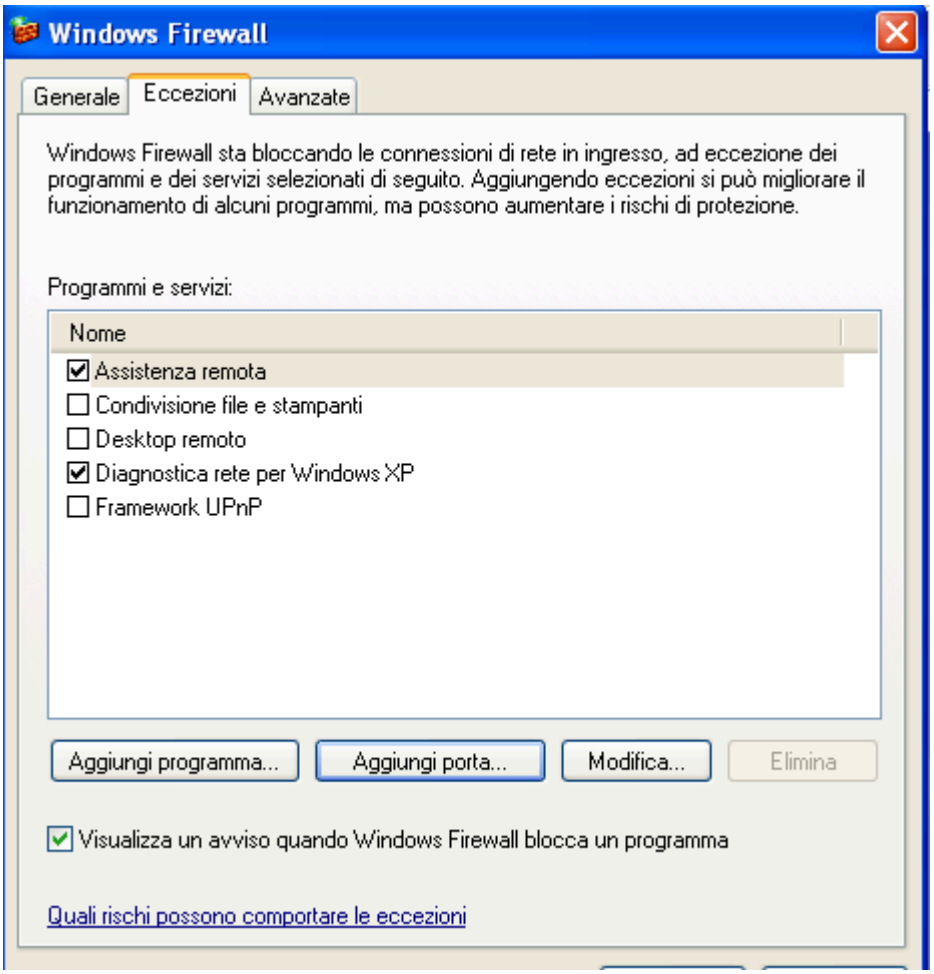
Lanciamo la scansione con lo switch -Pn:

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 11:24 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)

Nmap done: 1 IP address (1 host up) scanned in 216.09 seconds
```

In questo caso la risposta è diversa, Nmap identifica l'host come up ma ci notifica che tutte le 1000 porte analizzate ignorano le sue richieste essendo queste filtrate.

Considerazioni finali

Il firewall impedisce alle porte di comunicare con chiunque non sia inserito nella sua lista di eccezioni:



Questo ci impedisce di effettuare una scansione più dettagliata e di scoprire lo stato delle porte e servizi annessi.