

# Esercizio S9-L1

L'esercizio di oggi riguarda il verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno.

## Requisiti del laboratorio

IP delle macchine:

Windows XP: 192.168.240.150

Kali linux: 192.168.240.100

```
C:\Documents and Settings\Epicode_user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

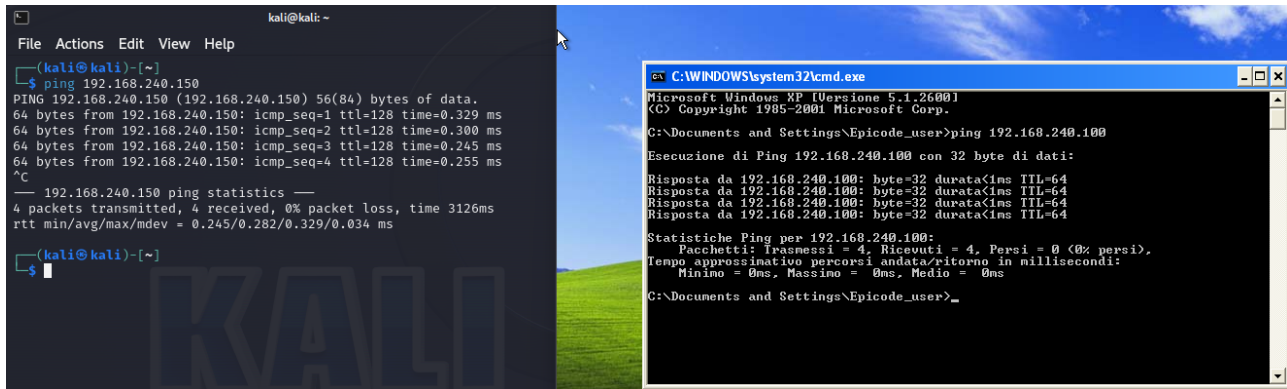
    Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.240.150
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.240.1

C:\Documents and Settings\Epicode_user>
```

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255
    inet6 fe80::a00:27ff:febe:2595 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:be:25:95 txqueuelen 1000 (Ethernet)
    RX packets 19 bytes 2157 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 4690 (4.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## Ping delle macchine



```
(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=0.329 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.300 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.245 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.255 ms
^C
--- 192.168.240.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3126ms
rtt min/avg/max/mdev = 0.245/0.282/0.329/0.034 ms

(kali@kali)-[~]
$
```

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ping 192.168.240.100

Esecuzione di Ping 192.168.240.100 con 32 byte di dati:

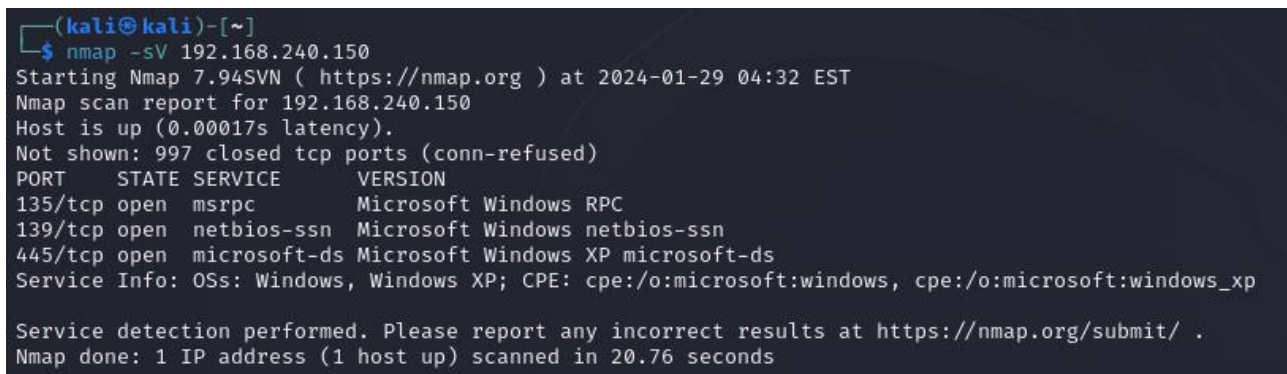
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.240.100:
Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\Documents and Settings\Epicode_user>
```

## Scansione con NMAP

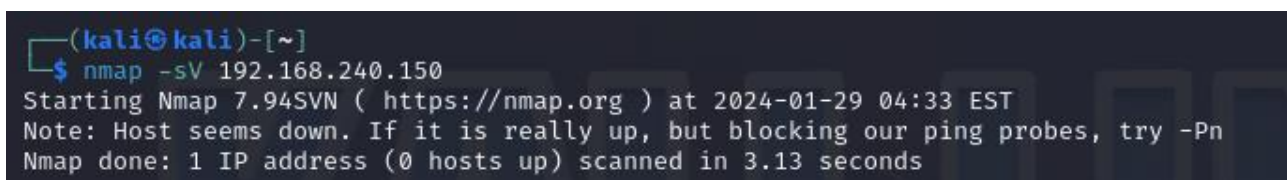
Firewall disattivato:



```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 04:32 EST
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 20.76 seconds
```

Firewall attivo:



```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 04:33 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 3.13 seconds
```

## Differenze e conclusioni finali

Le scansioni effettuate con Nmap evidenziano chiaramente l'effetto dei firewall sul sistema Windows XP. Con i firewall attivi, qualsiasi tentativo di ping viene bloccato, dimostrando l'efficacia delle misure di sicurezza implementate. Tuttavia, una volta disattivati i firewall, è stato possibile individuare le porte aperte e identificare potenziali vulnerabilità sulla macchina. Questo sottolinea l'importanza di un adeguato livello di protezione attraverso l'implementazione di firewall e altre misure di sicurezza per prevenire accessi non autorizzati e proteggere il sistema da possibili attacchi esterni.