

Firewall Windows XP

Firewall

Di default la macchina Xp ha il firewall disattivato, in questo esercizio ci viene chiesto di evidenziare le differenze con firewall attivo e poi disattivo

Firewall Disattivo

Una volta messe le macchine in comunicazione tramite IP e confermato il collegamento tramite comando ping; eseguo comando scansione nmap per vedere i servizi disponibili

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.200.200  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 11:04 CET  
Nmap scan report for 192.168.200.200  
Host is up (0.00070s 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 20.65 seconds
```

Firewall Attivo

```
(kali㉿kali)-[~]  
└─$ ping 192.168.200.200  
PING 192.168.200.200 (192.168.200.200) 56(84) bytes of data.  
^C  
--- 192.168.200.200 ping statistics ---  
13 packets transmitted, 0 received, 100% packet loss, time 12263ms
```

La prima differenza che si nota attivando il firewall da XP è che viene bloccata la comunicazione del comando ping.

Firewall Attivo

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.200.200  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 11:08 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 3.36 seconds
```

```
(kali㉿kali)-[~]  
$ nmap -Pn -sV 192.168.200.200  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 11:09 CET  
Nmap scan report for 192.168.200.200  
Host is up.  
All 1000 scanned ports on 192.168.200.200 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 214.76 seconds
```

Anche eseguendo la scansione nmap ci viene detto che l'host sembra spento e che se siamo sia acceso dobbiamo eseguire di nuovo il comando aggiungendo -Pn

Firewall Attivo

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.200.200  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 11:08 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 3.36 seconds
```

```
(kali㉿kali)-[~]  
$ nmap -Pn -sV 192.168.200.200  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 11:09 CET  
Nmap scan report for 192.168.200.200  
Host is up.  
All 1000 scanned ports on 192.168.200.200 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 214.76 seconds
```

Purtroppo anche con -Pn tutte le porte sono state filtrate rendendo così di fatto impossibile la comunicazione