



S9-L1

## Overview

---

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.



Dopo aver modificato i file di configurazione di rete e avviato la scansione di nmap, come indicato nella traccia, possiamo notare che risultano presenti alcuni servizi attivi ( sulle porte: 135, 139, 445).

Proviamo ora a effettuare una nuova scansione con nmap ma abilitando il firewall.

```
*~/Desktop/Utili/esercizi/reportxp.txt [Read Only] - Mousepad
File Edit Search View Document Help
[Icons] [Navigation] [Zoom] [Full Screen]

1 # Nmap 7.94 scan initiated Mon Feb  5 15:29:15 2024 as: nmap -sV -o reportxp.txt -O 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00055s latency).
4 Not shown: 997 closed tcp ports (reset)
5 PORT      STATE SERVICE      VERSION
6 135/tcp    open  msrpc        Microsoft Windows RPC
7 139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
9 MAC Address: 08:00:27:B3:D9:26 (Oracle VirtualBox virtual NIC)
10 Device type: general purpose
11 Running: Microsoft Windows XP|2003
12 OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
13 OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
14 Network Distance: 1 hop
15 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
16
17 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
18 # Nmap done at Mon Feb  5 15:29:38 2024 -- 1 IP address (1 host up) scanned in 23.02 seconds
19
20 |
```



Come possiamo notare una volta attivato il firewall non saremo più in grado di rintracciare i servizi precedentemente ottenuti, infatti tutte le porte risulteranno chiuse. I firewall possono prevenire le scansioni di software come nmap in diversi modi, tra cui:

- Alcuni firewall sono in grado di rilevare pattern di traffico sospetti o comportamenti anomali associati a Nmap e possono bloccare le sue attività di scansione.
- Il firewall può limitare il numero di richieste o di pacchetti inviati da un singolo indirizzo IP in un determinato periodo di tempo.
- Alcuni firewall possono ispezionare i pacchetti di dati in transito e rilevare firme o modelli di traffico associati a Nmap, bloccando quindi le sue attività.

```
~/Desktop/Utili/esercizi/reportxp2.txt [Read Only] - Mousepad
File Edit Search View Document Help
1 # Nmap 7.94 scan initiated Mon Feb  5 16:08:12 2024 as: nmap -A -sV -o reportxp2.txt 192.168.
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00033s latency).
4 All 1000 scanned ports on 192.168.240.150 are in ignored states.
5 Not shown: 1000 filtered tcp ports (no-response)
6 MAC Address: 08:00:27:B3:D9:26 (Oracle VirtualBox virtual NIC)
7 Device type: specialized|general purpose
8 Running: AKCP embedded, General Dynamics embedded, Microsoft Windows 2000|2003|XP
9 OS CPE: cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_server_2003 cpe:/o:micros
10 Too many fingerprints match this host to give specific OS details
11 Network Distance: 1 hop
12
13 TRACEROUTE
14 HOP RTT      ADDRESS
15 1    0.33 ms 192.168.240.150
16
17 OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
18 # Nmap done at Mon Feb  5 16:08:55 2024 -- 1 IP address (1 host up) scanned in 43.34 seconds
19
```