

FIREWALL






COS'E'

Un firewall è un dispositivo o un software progettato per monitorare, filtrare e controllare il traffico di rete in base a regole di sicurezza predefinite.

L'obiettivo è proteggere una rete informatica o un sistema informatico da accessi non autorizzati, intrusioni o danni provocati da malware, e altre minacce informatiche.





TRACCIA

Fare scansione con nmap su macchina vittima Windows XP, con Firewall attivo e Firewall disattivo

Dopo essere andati sulle impostazioni di firewall ho disattivato il firewall e avviato la scansione con tanto di report

```
(root@kali)-[/home/kali/Desktop]
# nmap -sV -o scanreport 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 09:47 EST
Nmap scan report for 192.168.240.150
Host is up (0.0017s latency).
Not shown: 997 closed tcp ports (reset)
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
MAC Address: 08:00:27:F4:C3:C3 (Oracle VirtualBox virtual NIC)
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 20.72 seconds
```

```
1 # Nmap 7.94SVN scan initiated Mon Feb  5 09:47:46 2024 as: nmap -sV -o scanreport 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.0017s 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:F4:C3:C3 (Oracle VirtualBox virtual NIC)
10 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
11
12 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
13 # Nmap done at Mon Feb  5 09:48:06 2024 -- 1 IP address (1 host up) scanned in 20.72 seconds
14
```



Dopo essere andati sulle impostazioni di firewall ho disattivato il firewall e avviato la scansione con tanto di report

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 09:58 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 1.61 seconds
```



CONCLUSIONI

Con il firewall attivo, dopo la scansione, ci viene indicato che non vi è alcuna comunicazione in quanto il firewall può bloccare le richieste di connessione ai servizi su determinate porte di rete. (3 porte aperte con firewall disattivo).
Quindi se una porta è chiusa o bloccata dal firewall, la scansione non riuscirà a ottenere una risposta dal servizio in esecuzione su quella porta.

