

## S9/L1

Eseguo, utilizzando Kali, una scansione Nmap su Windows XP con il firewall disabilitato.

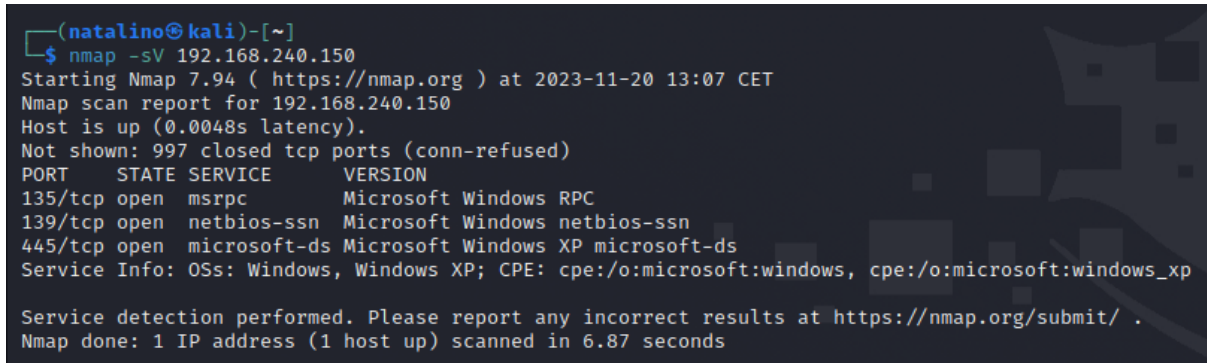
Nmap è un tool che può essere utilizzato per la scansione delle porte di rete, la ricerca di host attivi su una rete, la ricerca di servizi in esecuzione su un host attivo e la ricerca di eventuali vulnerabilità di sicurezza nei servizi in esecuzione su un host attivo.

Il firewall può essere un dispositivo o un software il cui scopo è proteggere una rete (firewall perimetrali) o anche solo un host (firewall host) da accessi non autorizzati. Funziona filtrando il traffico di rete in base a un insieme di regole, consentendo in tal modo solo il traffico autorizzato.

Eseguo la mia scansione eseguendo il comando

```
nmap -sV 192.168.240.150
```

e ottengo l'output seguente



```
(natalino@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 13:07 CET  
Nmap scan report for 192.168.240.150  
Host is up (0.0048s 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 6.87 seconds
```

La scansione, in questo caso, è stata eseguita utilizzando le opzioni -sV.

L'opzione -s indica a Nmap di eseguire una scansione TCP SYN stealth, ovvero una scansione in cui il client invia un pacchetto SYN a una porta specificata (TCP, ovvero un protocollo di comunicazione orientato alla connessione che fornisce un trasferimento affidabile dei dati tra due host di rete) e quindi attende una risposta. Se il target risponde con un pacchetto SYN/ACK, allora la porta è aperta. Se il server non risponde o risponde con un pacchetto RST (può essere utilizzato per interrompere una connessione TCP), allora la porta è chiusa.

L'opzione -V, invece, indica a Nmap di includere informazioni sulla versione del servizio in esecuzione su una specifica porta aperta.

Notiamo che l'host è attivo e ha 3 porte aperte. Il servizio *msrpc* è un protocollo di comunicazione utilizzato da Microsoft per fornire servizi di rete. Il servizio *netbios-ssn* è anch'esso un protocollo di comunicazione utilizzato da Microsoft per fornire servizi di rete. Il servizio *microsoft-ds* è spesso utilizzato

da aziende e organizzazioni per gestire i propri sistemi informatici. E' importante perché è anche utilizzato da malware per diffondersi da un sistema all'altro utilizzando una vulnerabilità presente nel servizio stesso.

Ho poi eseguito la stessa scansione abilitando il firewall, ottenendo quest'altro output

```
(natalino@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 13:13 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 3.12 seconds
```

attraverso il quale capisco che:

- l'host sembra essere giù;
- Nmap non è riuscito a stabilire una connessione con l'host, il che indica che potrebbe essere spento, scollegato dalla rete o che sta bloccando le richieste di Nmap;
- se l'host è effettivamente attivo, ma sta bloccando le richieste di Nmap, è possibile provare a eseguire la scansione con l'opzione *-Pn*, che indica a Nmap di eseguire una scansione ping senza inviare pacchetti TCP, e dovrebbe essere quindi in grado di stabilire una connessione con esso.

Infatti, con questa nuova scansione

```
(natalino@kali)-[~]  
$ nmap -Pn 192.168.240.150  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 14:39 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 201.84 seconds
```

capisco che:

- l'host è attivo;
- tutte le 1000 porte scansionate sull'host sono in uno stato ignorato;
- non sono state mostrate 1000 porte TCP filtrate poiché non ho ricevuto risposta da esse.

In base a queste informazioni, posso concludere che l'host potrebbe essere protetto da un firewall o da un altro dispositivo di sicurezza.