Esercizio 1 settimana 9

Oggi andremo ad effettuare due scansioni nmap -sV da una macchina Kali ad una windows xp. Nella prima scansione terremo il firewall di windows disattivato, mentre nella seconda lo attiveremo.

Ricordiamo che è nmap è uno strumento usato per eseguire scansioni di rete e che darà informazioni delle porte attive e, nel caso dell'opzione -sV, delle versioni dei servizi che operano sulle porte aperte.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 09:56 CET
Nmap scan report for 192.168.240.150
Host is up (0.0015s 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:m
icrosoft:windows_xp

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.54 seconds
```

Questo è il risultato della scansione con il firewall disattivato.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 09:58 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -P
n
Nmap done: 1 IP address (0 hosts up) scanned in 3.08 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Questo, invece, il risultato della scansione con il firewall attivo.

Possiamo notare un'evidente differenza tra le due scansioni. Mentre nella prima nmap riesce ad identificare le porte ed i servizi su di esse attivi, nella scansione con il firewall attivo nmap non riesce nemmeno a mettersi in contatto con l'host. Questo perché, probabilmente, il firewall è configurato in modo tale da bloccare il protocollo ICMP (quello del ping) che nmap usa per controllare se l'host e attivo o meno. In questo caso, l'host è attivo ma non potendo ricevere risposte ICMP nmap pensa che sia offline.