ESERCIZIO 1 SETTIMANA 9

Quest'oggi andremo ad effettuare una scansione con nmap verso windows XP, prima andiamo ad impostare gli indirizzi come da esercizio. Eseguiamo come prima la scansione con il firewall disattivato e notiamo che riusciamo a trovare dei servizi aperti alcuni pericolosi.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -o ReportXP 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 07:57 EST
Nmap scan report for 192.168.240.150
Host is up (0.00085s 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 20.32 seconds
```

Ora andiamo ad eseguire la stessa scansione ma con il firewall attivo, notiamo che la scansione non riesce, infatti nmap ci consiglia di riprovare senza il ping, ma di fatto la scansione effettuata nello stesso modo non ci riscontra risultati poiché il firewall blocca la scansione.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -o ReportXP 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 07:58 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 3.07 seconds
```

Quindi possiamo la netta differenza tra il firewall attivo e disattivo, ovvero che blocca completamente la scansione, sappiamo che ci sono scansioni più intelligenti da poter fare che magari ci danno risultati diversi, ma con questa scansione in particolare notiamo che il firewall la blocca.