CONSEGNA S9L1

L'obbiettivo di oggi è quello di verificare in che modo l'attivazione del firewall impatta sul risultato di una scansione dei servizi dall'esterno.
Effettuerò una scansione con Nmap da KALI sul target Windows XP.

La prima scansione l'ho effettuata con il firewall di Windows XP spento, e possiamo notare che ci sono tre servizi in ascolto rispettivamente sulle porte TCP 135, 139, 445. (Fig.1)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 10:36 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0022s 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
```

Fig.1

La seconda scansione l'ho effettuata con il firewall acceso e il risultato ci riporta che la macchina o non è accesa, o se è accesa sta bloccando l'host Discovery di Nmap. Possiamo dedurre che il firewall sta bloccando l'accesso alle porte con il protocollo ICPM. (Fig.2)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 10:41 EDT
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 3.33 seconds
```

Fig.2

Ho provato quindi ad inserire il parametro -Pn, che evita di piegare la macchina e passa direttamente alla scansione dei servizi. (Fig.3)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 10:41 EDT
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)
```

Fig.3

In questa scansione tutte le porte risultano filtrate, quindi lo scanner non ha ricevuto nessun segnale. Non possiamo quindi sapere se le porte sono aperte o chiuse, ma almeno sappiamo che il target è attivo, quindi possiamo dedurre che ci sia un firewall.

Posso concludere che il firewall, bloccando le scansione esterna dei servizi sul target, riduce preventivamente i rischi di attacco dall'esterno, rendendo in questo caso inaccessibili i servizi attivi.