Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno.
Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.
La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato.

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno.
Per questo motivo:
1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2.Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch–sV, per la service detectione -o nomefile report per salvare in un file l'output)
3.Abilitare il Firewall sulla macchina Windows XP
4.Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch–sV.

Traccia:
Che differenze notate? E quale può essere la causa del risultato diverso?
Requisiti:
Configurate l'indirizzo di Windows XP come di seguito: **192.168.240.150**
Configurate l'indirizzo della macchina Kali come di seguito: **192.168.240.100**

Il **FIREWALL** è un filtro che controlla il traffico dei dati e blocca le trasmissioni pericolose ed indesiderate, basandosi su regole/policy precise. Esso si interpone tra la rete esterna e quella interna.
I Firewall possono essere:

- Packet Filtering Firewall (statico/stateless): si basano al solo controllo IP/Porte;
- Stateful Packet Inspection Firewall (SPI): oltre al controllo del pacchetto, mantengono le informazioni dello stato della connessione;
- Next Generation Firewall (NGFW): Evoluzione del Firewall che aggiunge l'analisi su tutti i livelli ISO/OSI.
- **Web Application Firewall (WAF)**: Dispositivi per la protezione di SQLi e XSS.

Dopo aver configurato le macchine è stato effettuato un **PING** per verificare che comunicassero

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.592 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.563 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.660 ms
^C
── 192.168.240.150 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2060ms
rtt min/avg/max/mdev = 0.563/0.605/0.660/0.040 ms
```

Eseguito «**nmap –sV 192.168.240.150 –o firewallXP.txt**» con firewall di XP disattivato

```
1 # Nmap 7.94SVN scan initiated Mon Feb  5 13:16:58 2024 as: nmap -sV -o
  firewallXP.txt 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00061s 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: 08:00:27:2E:07:58 (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 13:17:20 2024 -- 1 IP address (1 host up) scanned
  in 21.43 seconds
14
```

Eseguito nuovamente «**nmap –sV 192.168.240.150 –o firewallXP2.txt**» con firewall di XP attivato

```
1 # Nmap 7.94SVN scan initiated Mon Feb  5 13:19:22 2024 as: nmap -sV -o
  firewallXP2.txt 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00062s latency).
4 All 1000 scanned ports on 192.168.240.150 are in ignored states.
5 Not shown: 1000 filtered tcp ports (no-response)
6 MAC Address: 08:00:27:2E:07:58 (Oracle VirtualBox virtual NIC)
7
8 Service detection performed. Please report any incorrect results at https://
  nmap.org/submit/ .
9 # Nmap done at Mon Feb  5 13:19:59 2024 -- 1 IP address (1 host up) scanned
  in 37.06 seconds
10
```

La differenza tra le 2 scansione è:

- Firewall disattivato:
  - Quante porte sono chiuse (997) e non possono essere controllate;
  - Verifica quali porte sono aperte con relativi servizi e versioni;
  - Il sistema operativo installato;
- Firewall attivato:
  - Tutte le porte che sono state controllate (1000) sono state ignorate.

Con il Firewall disattivato è stato permesso di effettuare una scansione sulla macchina target permettendo di verificare quali servizi possono essere utilizzati per eventuali attacchi.
Con il Firewall attivato non è stato possibili verificare nessun controllo sulle porte o servizi e eseguire il PING, perché si basa su delle regole che vietano questi tipi di controlli.