

## S9 LEZIONE 1

### Traccia:

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 in formato OVA che abbiamo utilizzato nella Unit 2 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 detection)
  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?

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.104.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 05:07 EST
Nmap scan report for 192.168.104.200
Host is up (0.00s 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 20.41 seconds
```

La scansione è stata eseguita con le opzioni `-sV`:

`-s` indica a Nmap di eseguire una scansione TCP SYN stealth, ovvero una scansione in cui il client invia un pacchetto SYN ad una porta. Se il target risponde con un pacchetto SYN/ACK, allora quella porta è aperta. Se il server non risponde allora quella porta è chiusa.

L'opzione `-V`, indica a Nmap di includere informazioni sulla versione del servizio.

Come si può notare l'host è attivo ed ha 3 porte aperte.

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV 192.168.104.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 07:19 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 3.36 seconds

(kali㉿kali)-[~]
$ nmap -Pn 192.168.104.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 07:20 EST
Nmap scan report for 192.168.104.200
Host is up.
All 1000 scanned ports on 192.168.104.200 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 229.00 seconds

(kali㉿kali)-[~]
$
```

Attivando il firewall su windows XP ed eseguendo di nuovo la scansione l'host sembra essere down, nmap non riesce a stabilire una connessione il che potrebbe indicare che che l'host sia offline. Con il comando -Pn si riesce che l'host è effettivamente attivo, 1000 porte sono state scansionate ma non è stata ricevuta nessuna risposta da esse.

In base a queste info, posso concludere che il firewall ha fatto il suo lavoro, bloccando ogni tipo di connessione