Security operation: Azioni preventive

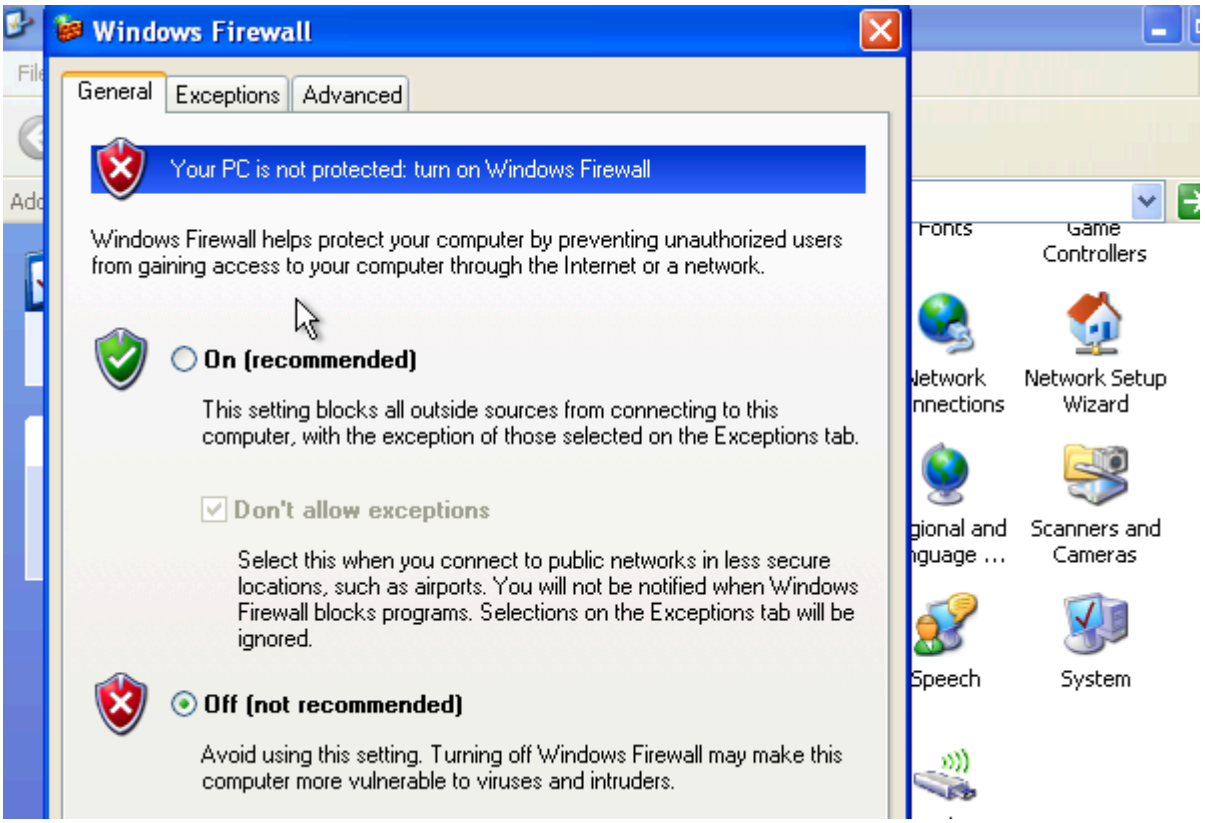
L’esercizio di oggi è verificare in che modo l’attivazione del Firewall impatta il risultato di una scansione dei servizi dall’esterno.

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 e -o nomefilereport 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?

Bonus: Monitorare i log di Windows durante queste operazioni.
1. Quali log vengono modificati? (se vengono modificati)
2. Cosa si riesce a trovare?

1. **Verifico che il firewall di windows xp sia disattivato.**



2. **Vado ad effettuare la scansione su XP con nmap -sV**

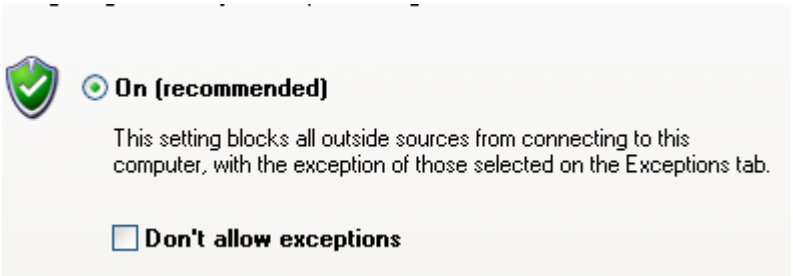
```
# Nmap 7.94 scan initiated Tue Mar  5 20:02:39 2024 as: nmap -sV -o scan_XP.txt 192.168.1.101
Nmap scan report for 192.168.1.101
Host is up (0.00098s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:B2:06:9F (Oracle VirtualBox virtual NIC)
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 at Tue Mar  5 20:03:01 2024 -- 1 IP address (1 host up) scanned in 21.54 seconds

```

La scansione ci riporta 3 servizi in ascolto rispettivamente sulle porte TCP 135,139,445.

3. Attiviamo il firewall



4. Effettuiamo di nuovo la scansione nmap - sV

```
└─$ sudo nmap -sV 192.168.1.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-09 11:52 CET
Nmap scan report for 192.168.1.101
Host is up (0.00047s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:B2:06:9F (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 39.83 seconds
```

Tutte le porte sembrano filtrate, ovvero non hanno risposto alle richieste dello scanner. Quindi possiamo dedurre che il Firewall sta bloccando l'accesso alle porte. Da questa scansione non si può dire con certezza se una porta filtrata sia aperta o chiusa (nella fattispecie sappiamo che sulle porte 135,139,445 sono in ascolto servizi).