Esercitazione WEEK 18 D1 (1)

Security Operation: Azioni preventive

Ettore Farris

Descrizione sintetica

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.
- 5. Trovare le eventuali differenze e motivarle.

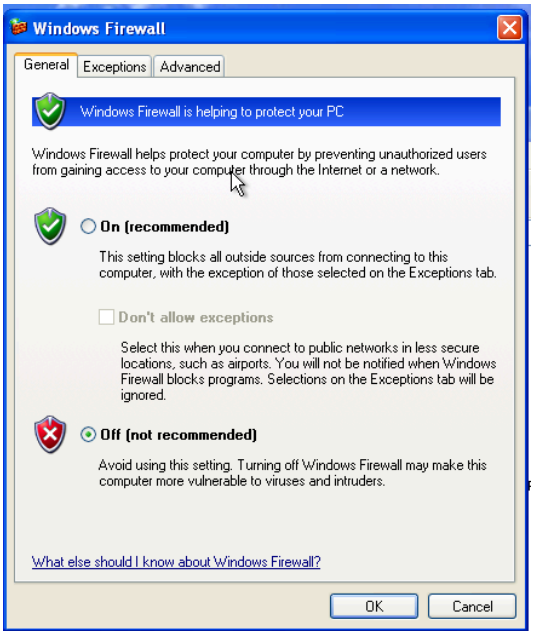
Bonus: Monitorare i log di Windows durante queste operazioni.

- 1. Quali log vengono modificati? (se vengono modificati)
- 2. Cosa si riesce a trovare?

Descrizione sintetica

- ***Scansione nmap con firewall disabilitato***

Per prima cosa, disabilitiamo il firewall dalle impostazioni della macchina Windows XP e cancelliamo il file *pfirewall.log* dalla cartella WINDOWS presente sull'unità C. Successivamente, effettuiamo una scansione nmap.



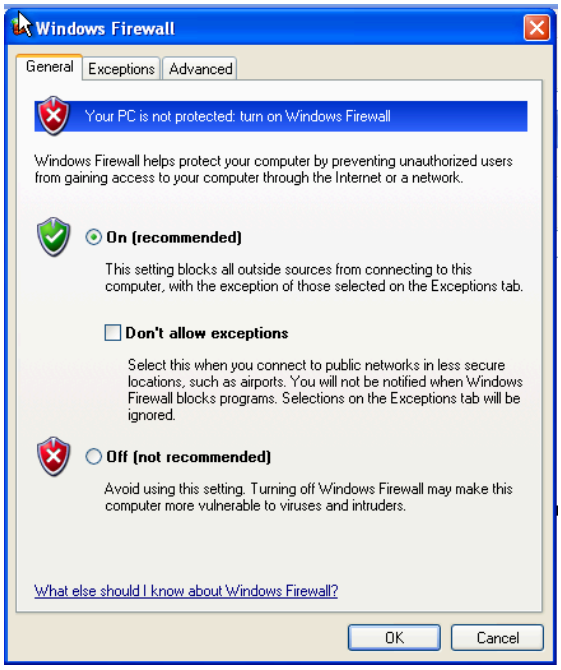

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.11.113
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-10 12:59 EDT
Nmap scan report for 192.168.11.113
Host is up (0.00070s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:2E:05:35 (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: 1 IP address (1 host up) scanned in 19.74 seconds
```

Notiamo che in assenza di firewall, le porte possono essere scansionate regolarmente. Possiamo quindi ottenere importanti informazioni per poter

performare un attacco. Nella cartella C:\Windows non è presente alcun file di log salvato dall'attività del firewall.

- ***Scansione nmap con firewall abilitato***

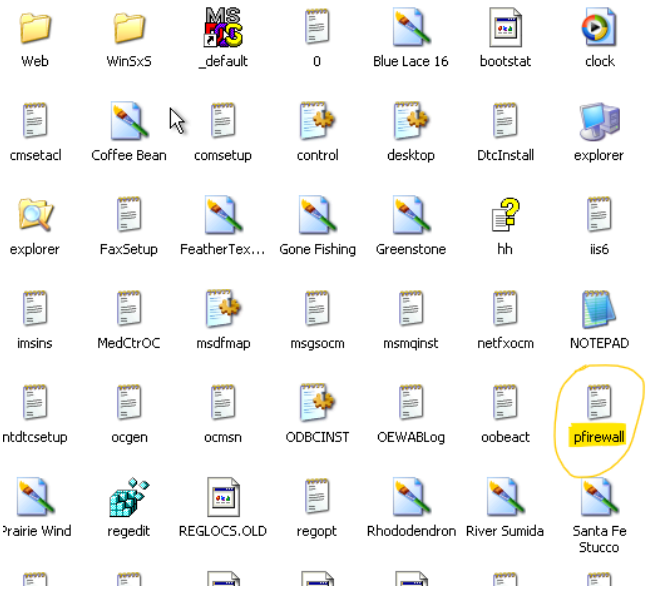
Abilitiamo il firewall ed effettuiamo la stessa scansione nmap.




```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.11.113
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-10 13:19 EDT
Nmap scan report for 192.168.11.113
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.11.113 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:2E:05:35 (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 34.58 seconds
```

Notiamo che il firewall sta proteggendo la macchina e ci sta impedendo di effettuare la scansione delle porte aperte trovate con la prima scansione.

Nella directory WINDOWS possiamo notare la presenza del file *pfirewall.log,* ovvero un file di log dell'attività del firewall generato dopo la nostra scansione.



Ispezionando il file, possiamo vedere l'azione della regola del firewall. Ad esempio nella prima riga, dopo la data e l'ora, vediamo che è stato *droppato* un pacchetto *TCP* dall'IP sorgente (Kali), ovvero 192.168.11.111 distinato alla macchina XP con IP 192.168.11.112. La porta sorgente è la 47281 mentre quella destinataria è la 5900.