Esercitazione W18D1 - Pratica 1

Security Operation - Azioni Preventive

Fabio Benevento - 05/03/2024

Traccia

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.

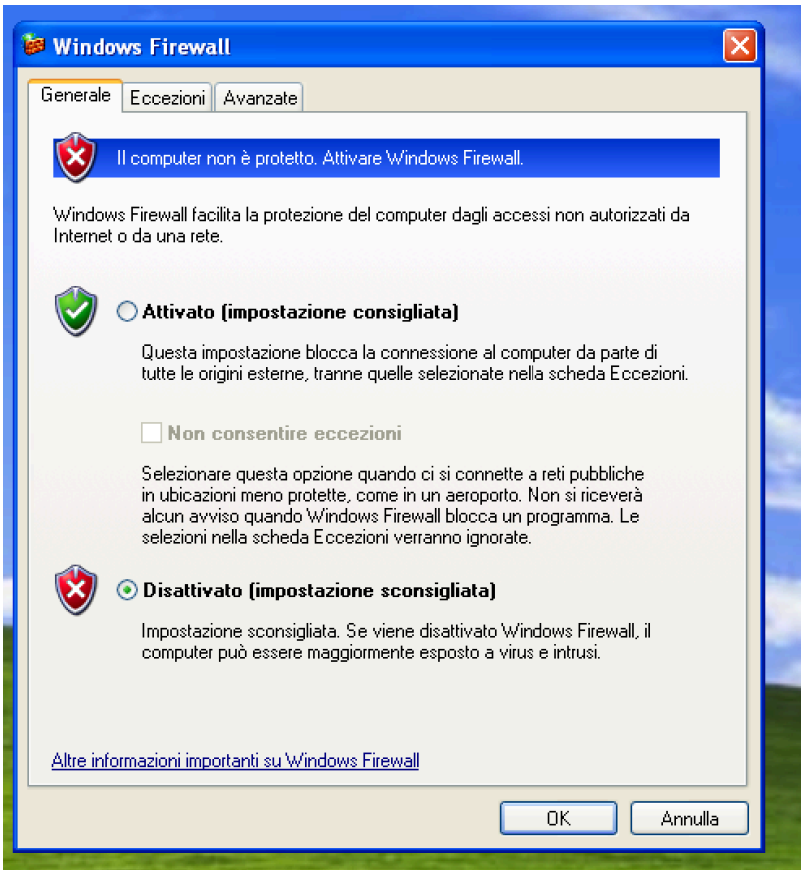
Che differenze notate? E quale può essere la causa del risultato diverso?

Bonus:

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

Implementazione

Ho provveduto in primo luogo a disabilitare il firewall sulla macchina Windows XP.
Successivamente ho avviato la scansione nmap dei servizi con il comando sudo nmap -sV 192.168.11.113 dove 192.168.11.113 è l'indirizzo assegnato alla macchina Windows XP.

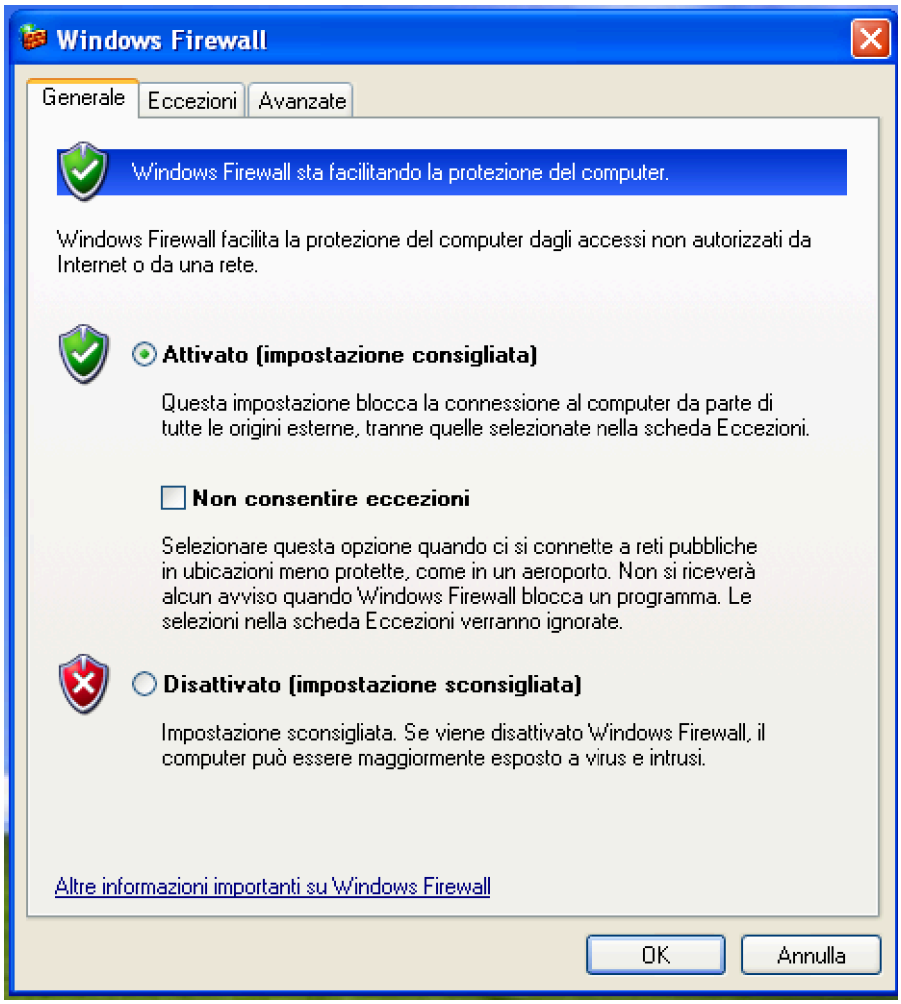


La scansione rileva la presenza di 3 servizi accessibili sulle porte 135, 139 e 445 come mostrato in figura.

```
└─$ sudo nmap -sV 192.168.11.113
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-12 04:13 EDT
Nmap scan report for 192.168.11.113
Host is up (0.0014s 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: 08:00:27:83:C0:1F (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 19.92 seconds
```

Ho quindi ripetuto la scansione dopo aver riabilitato il firewall su Windows XP.



In questo secondo caso la scansione nmap non rileva i servizi precedentemente individuati.

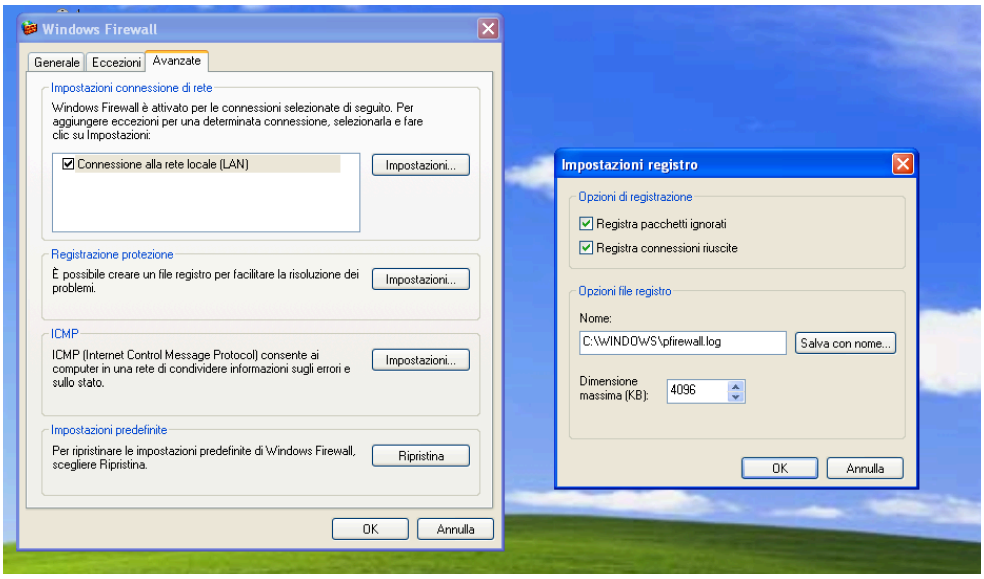
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.11.113
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-12 04:21 EDT
Nmap scan report for 192.168.11.113
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.11.113 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:83:C0:1F (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 35.62 seconds
```

Ciò sta a significare che il firewall sta agendo bloccando il discovery delle porte.

Bonus

Per monitorare i log durante queste operazioni sono acceduto alla sezione Avanzate di Windows FIrewall e ho aperto le Impostazioni di registro (Registrazione protezione - Impostazioni...), quindi ho abilitato la registrazione su file (denominato pfirewall.log) dei pacchetti ignorati e delle connessioni riuscite.



Ripetendo quindi la scansione svolta in precedenza con il firewall attivo e aprendo il file di log pfirewall.log con un file di monitor log come BareTail è possibile vedere i tentativi di connessione che vengono stoppati (DROP TCP) da parte del firewall