Report Esercizio

W18-D2

Redatto da Andrea Sciattella

21/06/2024

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 e -o nomefilereport per salvare in un file l'output)

3. Abilitare il Firewall sulla macchina Windows XP

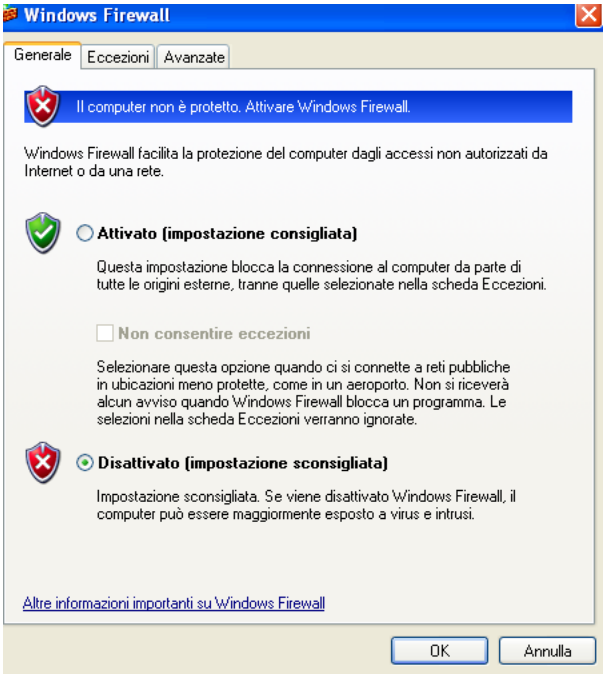
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

5. Trovare le eventuali differenze e motivarle.

Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.

SVOLGIMENTO ESERCIZIO

- Settiamo prima il laboratorio come indicato dalla traccia con l'indirizzo di Windows XP come di seguito: 192.168.240.150 e l'indirizzo della macchina Kali come di seguito: 192.168.240.100
- Proviamo il ping tra le macchina, ed eseguiamo le istruzioni.
- Controlliamo che il firewall di Win XP si disattivato come di seguito



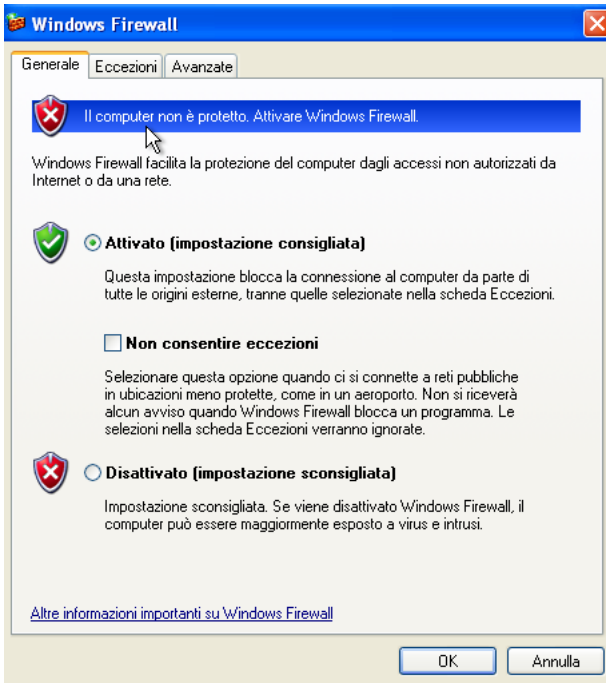
- Eseguiamo la scansione nmap da Kali tramite il comando "sudo nmap -sV 192.168.240.150 -o scansione_senza_firewall" dove lo switch sV indica una scansione dei servizi e lo switch -o indica la trascrizione in un file di dato nome.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV 192.168.240.150 -o scansione_senza_firewall
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-21 09:13 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0018s 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: 08:00:27:38:39:6F (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 21.40 seconds
```

- La scansione è andata a buon fine, ed ha rivelato le seguenti porte e servizi disponibili.

- Ora andiamo ad attivare il firewall windows seguendo lo stesso identico percorso di prima.



- Eseguiamo la medesima scansione cambiando solo il nome dell'output del file in "scansione_con_firewall".

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV 192.168.240.150 -o scansione_con_firewall
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-21 09:18 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00093s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:38:39:6F (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 36.63 seconds
```

- Come possiamo vedere dallo screenshot, la scansione non ha rilevato nessuna porta o servizio aperto.

CONCLUSIONI

Possiamo evincere dalla esercitazione che, il firewall di windows effettivamente lavora per proteggere i dispositivi, bloccando quindi ogni connessione non autorizzata dall'host.

Vediamo infatti nel secondo screeshot che la scansione del tool Nmap non rileva le stesse porte aperte della scansione con il firewall down, indicando quindi che il dispositivo viene protetto da azioni di reconnaissance avversaria.