

Security Operation: azioni preventive

Davide Diglio

Traccia

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:

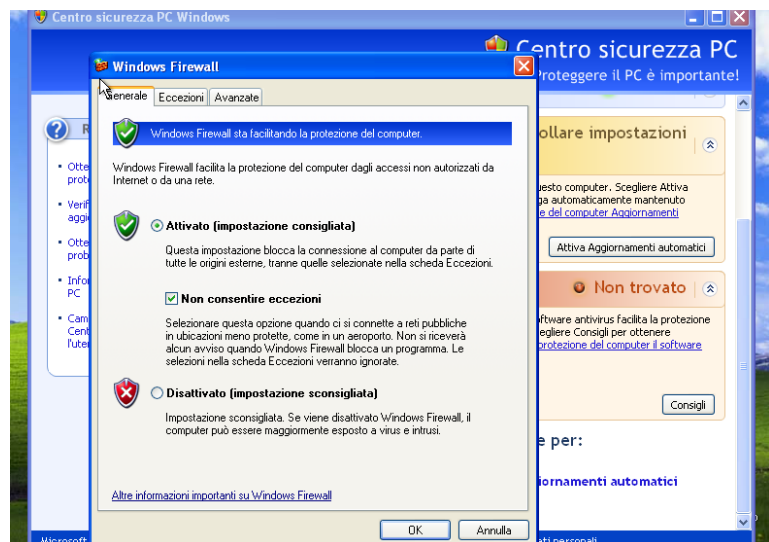
- Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP.
- Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch -sV).
- Abilitare il Firewall sulla macchina Windows XP.
- Effettuate una seconda scansione con nmap (utilizzando ancora una volta lo switch -sV).

Svolgimento

Parte I

In questo esercizio dobbiamo capire come impatta il Firewall sulla scansione dei servizi dall'esterno. Utilizziamo le due macchine virtuali, che sono: Windows XP e Kali.

Sulla macchina Windows XP si deve disattivare il Firewall prima di fare la scansione, andando su Windows Firewall.



Dopo aver disattivato il Firewall sulla macchina Windows XP, nella macchina Kali andiamo a scansionare con il comando "nmap -sV 192.168.1.200" la macchina target.

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.1.200  
  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 09:07 EST  
Nmap scan report for DESKTOP-77CHCEC.station (192.168.1.200)  
Host is up (0.00093s latency).  
Not shown: 814 closed tcp ports (conn-refused), 183 filtered tcp ports (no-response)  
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 11.72 seconds
```

Subito dopo abbiamo attivato il Firewall e rifatto la scansione sulla macchina.

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.1.200  
  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 09:08 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 3.24 seconds
```

Notiamo in questo esercizio se il Firewall è disattivato la scansione nmap può far vedere le porte aperte e i servizi attivi, questo comporta di avere più possibilità di attacchi. Abilitando il Firewall si può non rilevare queste informazioni, perché il Firewall filtra e blocca il traffico di rete.