Security Operation: azioni preventive

Pablo Andres Balbuena Rios

Esercizio 1
Settimana 9

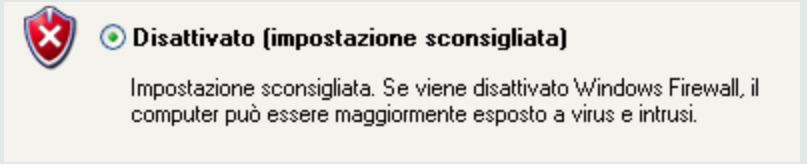
- Configurate l’indirizzo di Windows XP come di seguito: 192.168.240.150
- Configurate l’indirizzo della macchina Kalicome di seguito: 192.168.240.100
- Effettuate una scansione con nmap sulla macchina target , con il Firewall Disattivato e Attivato

Infine:

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

Scansione senza Firewall

Prima di procedere con la scansione delle vulnerabilità delle porte con l'aiuto di nmap, si deve configurare gli IP e provare se pingano fra di loro.
Successivamente si parte con la scansione

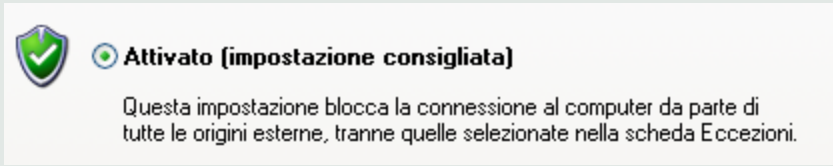



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.240.150 -o winxp
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 07:05 EST
Nmap scan report for 192.168.240.150
Host is up (0.88s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        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:windo
ws_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 20.34 seconds
```

Scansione con Firewall

Dopo aver scansionato con il Firewall spento, bisogna attivarlo in Windows XP. Successivamente si parte con la seconda scansione delle vulnerabilità delle porte.




```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.240.150 -o winxp2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 07:07 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 3.07 seconds
```

Differenza, con e senza Firewall

La principale differenza che notiamo è rilevare le porte aperte e chiuse in modo più accurato.

Questo è dovuto dalla configurazione e dalle regole di filtraggio implementate nel Firewall.