Marzo 2024

CYBER SECURITY SPECIALIST

S9L1

Jacopo Trovato

Security Operation: azioni preventive

La macchina di Windows XP di default è protetta da un firewall, ovvero una funzionalità di sicurezza che consente di proteggere il dispositivo filtrando il traffico di rete che entra e esce dal dispositivo. Per vedere cosa protegge il firewall è possibile fare una scansione con Nmap, prima con i firewall disattivato e poi con il firewall attivato.

Per prima cosa aprire cambiare gli indirizzi IP delle macchine per metterli sulla stessa rete, disattivare il firewall di windows e aprire il terminale di Kali e usare il comando: "nmap -sV (IP Windows XP)"

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:13 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0012s 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:F4:00:59 (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 20.73 seconds
```

Scansione con firewall disattivato

Questa scansione mostra 4 porte aperte, e le informazioni relative alla macchina Windows, come l'indirizzo MAC.

Attivando il firewall invece la scansione non restituisce nulla se non il ping che avviene in automatico dato che entrambe le macchine si trovano sulla stessa rete.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:15 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0012s 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:F4:00:59 (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 41.57 seconds
```

Come è visibile non è stata trovata nessuna porta aperta, proprio a causa del firewall che protegge Windows XP.