Security Operation: azioni preventive

L’esercizio di oggi è verificare in che modo l’attivazione del Firewall impatta il risultato di una scansione dei servizi dall’esterno.

FIREWALL DISATTIVATO

```
┌──(betta㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-20 14:35 CET
Nmap scan report for 192.168.240.150
Host is up (0.0078s 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: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 22.25 seconds
```

FIREWALL ATTIVO

```
┌──(betta㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-20 14:37 CET
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 3.34 seconds

┌──(betta㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-20 14:39 CET
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.44 seconds
```

La differenza evidente risiede nel fatto che, con il firewall attivo, il ping e la scansione di rete non hanno successo al contrario di quando è disattivato. Questo accade perché il firewall blocca i pacchetti ICMP utilizzati dal comando ping per testare la connettività.

Disattivare il firewall compromette la sicurezza della rete e dei dispositivi connessi, aumentando la vulnerabilità agli attacchi esterni e lasciando la rete più esposta a minacce dannose. È consigliabile mantenere il firewall attivo e configurarlo correttamente perchè:

- **Protegge da malware e intrusioni**, creando una barriera difensiva che filtra il traffico dannoso o non autorizzato.
- **Controlla il traffico di rete** consentendo solo il flusso di dati sicuri e autorizzati, in base alle regole predefinite.
- **Riduce le vulnerabilità della rete**, limitando l'esposizione a minacce esterne e potenziali attacchi.
- **Abilita il monitoraggio e il logging del traffico di rete**. Questa funzione permette di tenere traccia delle attività, rilevare comportamenti anomali e identificare potenziali

minacce.

- **Assicura la conformità alle normative di sicurezza** in vari settori. L'uso del firewall è spesso un requisito essenziale per garantire la sicurezza dei dati sensibili e rispettare gli standard di sicurezza richiesti.