



# **Security Operation: azioni preventive**

Cyber Security & Ethical Hacking



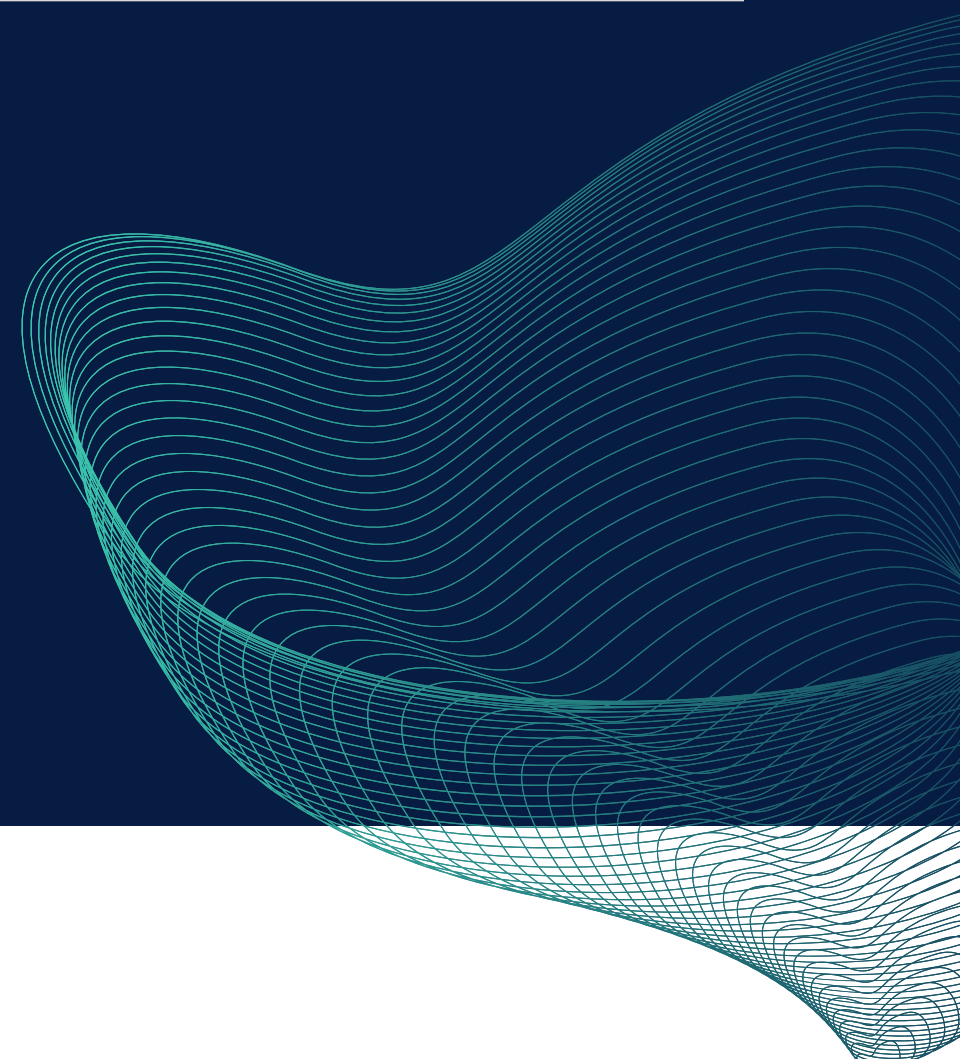
```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 09:32 EST
Nmap scan report for 192.168.240.150 (192.168.240.150)
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  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 7.68 seconds
```

Se si esegue Nmap su un sistema Windows XP senza firewall attivo, potremmo ottenere molte informazioni sulle porte aperte e sui servizi in esecuzione su quel sistema. Nmap è uno strumento di scansione di rete che viene utilizzato per rilevare host e servizi su una rete, identificare le porte aperte e ottenere informazioni dettagliate sui servizi in esecuzione su tali porte.

```
1 # Nmap 7.94SVN scan initiated Mon Feb  5 09:50:15 2024 as: nmap -sV -o report1 192.168.240.150
2 Nmap scan report for 192.168.240.150 (192.168.240.150)
3 Host is up (0.00040s latency).
4 Not shown: 997 closed tcp ports (conn-refused)
5 PORT      STATE SERVICE      VERSION
6 135/tcp    open  msrpc        Microsoft Windows RPC
7 139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
9 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
12 # Nmap done at Mon Feb  5 09:50:23 2024 -- 1 IP address (1 host up) scanned in 7.55 seconds
13
```

Senza un firewall attivo, Nmap potrebbe identificare aperte molte porte e servizi, fornendo informazioni sulle vulnerabilità potenziali presenti nel sistema. Questo è particolarmente rischioso su un sistema operativo obsoleto come Windows XP, che non riceve più aggiornamenti di sicurezza da diversi anni e può essere vulnerabile a svariate minacce.



```
(kali@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 09:33 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 3.26 seconds
```

Se si esegue Nmap su un sistema Windows XP con il firewall attivo, il firewall potrebbe impedire o limitare la visibilità di alcune porte e servizi durante la scansione. Il firewall è progettato per proteggere il sistema impedendo l'accesso non autorizzato alle porte e ai servizi. Pertanto, il risultato della scansione potrebbe essere influenzato dalla configurazione e dalle regole del firewall.

1. Porte filtrate o chiuse: Se il firewall blocca le porte durante la scansione, potresti vedere un numero limitato di porte aperte o nessuna porta aperta, a seconda di come sono configurate le regole del firewall.
2. Porte aperte: Se le regole del firewall consentono il traffico sulla porta che stai esaminando, Nmap potrebbe comunque rilevare le porte aperte e i servizi in esecuzione su di esse.
3. Limitazioni nella scoperta dei servizi: Il firewall potrebbe influire sulla capacità di Nmap di identificare accuratamente i servizi in esecuzione su alcune porte.