

Ilaria Pedrelli

Security Operation: Azioni Preventive

```
(kali@kali)-[~]
$ nmap -sV 192.168.11.104
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-05 14:34 EST
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 14:35 (0:00:05 remaining)
Nmap scan report for 192.168.11.104
Host is up (0.0030s latency).
Not shown: 996 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 Vista Embedded microsoft-ds (workgroup: WORKGROUP)
1026/tcp   open  msrpc           Microsoft Windows RPC
Service Info: Host: WINDOWSXP; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.20 seconds

(kali@kali)-[~]
$ nmap -sV 192.168.11.104
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-05 14:38 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 3.10 seconds

(kali@kali)-[~]
$
```

Seguendo la traccia dell'esercitazione, eseguo prima una scansione con nmap -sV da macchina Kali a Windows XP mantenendo il firewall attivo. Posso subito notare che la scansione, a Firewall non attivo, mi restituisce come risultato le porte aperte, i servizi in esecuzione, la versione e le info sull'Host.

Nel caso della scansione con firewall attivo invece, ricevo il risultato "host seems down"

Un firewall è un componente di sicurezza che filtra il traffico di rete tra un computer o una rete e internet. La sua funzione principale è quella di regolare e controllare il flusso di dati in entrata e uscita, decidendo quali comunicazioni permettere o bloccare in base a regole predefinite. In questo caso, il firewall su XP potrebbe bloccare le richieste di Nmap perché vengono interpretate come attività sospette o dannose.