

Esercizio S09-01

Per ridurre la possibilità di attacchi, abbiamo esaminato quelle relative alla rete. Possiamo quindi andare ad attivare e/o configurare un Firewall che permetta solo a determinati indirizzi IP di generare del traffico non desiderato nella nostra rete. Andiamo quindi ad effettuare una scansione con 'nmap' delle porte e dei relativi servizi attivi con lo switch '-sV' per la service detection sulla macchina Windows con e senza Firewall attivo.

Firewall attivo

```
alex@kali: ~  
File Actions Edit View Help  
(alex@kali)-[~]  
$ sudo nmap -sV 192.168.1.67  
[sudo] password for alex:  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 15:28 CET  
Nmap scan report for 192.168.1.67  
Host is up (0.00038s 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: 08:00:27:85:AC:9B (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 7.57 seconds  
(alex@kali)-[~]  
$
```

Firewall disattivato

```
(alex@kali)-[~]  
$ sudo nmap -sV 192.168.1.67  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 15:30 CET  
Nmap scan report for 192.168.1.67  
Host is up (0.00066s latency).  
All 1000 scanned ports on 192.168.1.67 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 08:00:27:85:AC:9B (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 23.09 seconds
```

Come possiamo notare, nella situazione con Firewall attivo 'nmap' non ci mostra in output alcuna informazione riguardo lo stato delle porte e i servizi attivi su di esse. Di contro ci comunica che tutte le porte scansionate su quell'IP sono in stato 'filtered': significa che per quelle porte è impossibile determinarne lo stato (aperto, chiuso, etc.) a causa di restrizioni dovute, in questo caso, al Firewall. Caso contrario per la situazione di Firewall disattivato, dove 'nmap' ci restituisce le porte aperte e la relativa versione dei servizi attivi in quanto non ci sono limiti o restrizioni sulla macchina vittima.

