

ESERCIZIO S9-L1

Lo scopo dell'esercizio di oggi è quello di verificare in che modo l'attivazione del firewall impatta il risultato di una scansione dei servizi dall'esterno.

SCANSIONE NMAP CON FIREWALL DISATTIVATO SULLA MACCHINA WINDOWS XP.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 08:35 EST
Nmap scan report for 192.168.240.150
Host is up (0.0022s 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 20.96 seconds
```

SCANSIONE CON IL FIREWALL ABILITATO

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 08:49 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 3.22 seconds
```

```
(kali㉿kali)-[~]
$ nmap -sV -Pn 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 08:58 EST
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 218.53 seconds
```

La differenza tra le due scansioni è che la prima ci dà un risultato normale con le porte aperte e le versioni, nella seconda invece la scansione non ha successo perché una volta attivato il firewall, quest'ultimo blocca i pacchetti ICMP utilizzati dal comando ping.

Il ping è un modo per testare se il dispositivo target è raggiungibile inviando dei pacchetti di dati e ricevendo una risposta. Se il firewall è configurato per bloccare il ping, quest'ultimo non avviene con successo. Lo stesso per la scansione di rete. Tuttavia disattivare il firewall non è un buon metodo perché si va a compromettere la sicurezza aumentando i rischi di potenziali attacchi provenienti dall'esterno.