

Esercizio S9 L1

Nell'esercizio di oggi compariamo due scansioni di Nmap su un sistema target prima e dopo aver abilitato il firewall su quel sistema.

Abbiamo usato una scansione *version detection*, con cui andiamo ad implementare il *banner grabbing*, ovvero Nmap scansiona il sistema target in cerca della versione dei servizi attivi sul sistema.

Con questo tipo di scansione, che usa sia il ping che la stretta di mano a tre vie, abbiamo potuto recuperare tutte le informazioni che ci aspettavamo: porte aperte, servizi attivi su queste porte e la loro versione. Abbiamo anche informazioni sul sistema operativo presente sulla macchina vittima.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.50.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-20 07:07 EST
Nmap scan report for 192.168.50.200
Host is up (0.0015s 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 21.07 seconds
```

Dopo aver attivato il firewall su Windows XP andiamo a ripetere la stessa scansione, ma questa volta non otteniamo alcuna informazione. Nmap riporta solo che il sistema target potrebbe non essere attivo e suggerisce di usare una nuova scansione senza ping, nel caso siamo sicuri che il sistema sia invece attivo.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.50.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-20 07:17 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
```

Riproviamo la scansione, questa volta senza usare il ping, e vediamo che ora Nmap riconosce il sistema come attivo, ma tutte le porte scansionate sono filtrate (succede quando è attivo un firewall).

```
(kali㉿kali)-[~]
$ nmap -sV -Pn 192.168.50.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-20 07:24 EST
Nmap scan report for 192.168.50.200
Host is up.
All 1000 scanned ports on 192.168.50.200 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 223.45 seconds
```

Facendo una contro prova, abbiamo provato a lanciare un semplice ping verso Windows XP, ma nessun pacchetto ha potuto raggiungere l'host target.

```
(kali㉿kali)-[~]  
$ ping 192.168.50.200  
PING 192.168.50.200 (192.168.50.200) 56(84) bytes of data.  
^C  
— 192.168.50.200 ping statistics —  
14 packets transmitted, 0 received, 100% packet loss, time 13357ms
```