

S9/L1

Nell'esercizio di oggi andremo ad eseguire due tipi di scansione della macchina WindowsXP, in una i firewall saranno disattivati mentre nell'altra attiveremo i firewall di Windows.

PRIMA SCANSIONE (FIREWALL DISATTIVATI)

```
(kali㉿kali)-[~]  
$ sudo nmap -sV 192.168.240.150  
[sudo] password for kali:  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 13:49 CET  
Nmap scan report for 192.168.240.150  
Host is up (0.0021s 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: 08:00:27:0F:1A:9E (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 20.68 seconds
```

SECONDA SCANSIONE (FIREWALL ATTIVI)

```
(kali㉿kali)-[~]  
$ sudo nmap -sV 192.168.240.150  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 13:51 CET  
Nmap scan report for 192.168.240.150  
Host is up (0.00031s latency).  
All 1000 scanned ports on 192.168.240.150 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 08:00:27:0F:1A:9E (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 42.92 seconds
```

Come possiamo notare nella prima scansione riusciamo ad individuare le porte attive sulla macchina WindowsXP mentre con i firewall attivi la scansione delle porte risultano filtrate.

Questo è dovuto dal fatto che il firewall sta bloccando la risposta alla scansione della porta al punto che Nmap non riesce a distinguere tra aperta o chiusa.

2023-11-20	14:41:49	DROP	TCP	192.168.240.100	192.168.240.150	38608	139	44	S	328635703	0	1024	-	-
2023-11-20	14:41:49	DROP	TCP	192.168.240.100	192.168.240.150	38608	5900	44	S	328635703	0	1024	-	-
2023-11-20	14:41:49	DROP	TCP	192.168.240.100	192.168.240.150	38608	8080	44	S	328635703	0	1024	-	-
2023-11-20	14:41:49	DROP	TCP	192.168.240.100	192.168.240.150	38608	1720	44	S	328635703	0	1024	-	-
2023-11-20	14:41:49	DROP	TCP	192.168.240.100	192.168.240.150	38608	53	44	S	328635703	0	1024	-	-
2023-11-20	14:41:49	DROP	TCP	192.168.240.100	192.168.240.150	38608	3389	44	S	328635703	0	1024	-	-
2023-11-20	14:41:49	DROP	TCP	192.168.240.100	192.168.240.150	38608	22	44	S	328635703	0	1024	-	-
2023-11-20	14:41:49	DROP	TCP	192.168.240.100	192.168.240.150	38608	445	44	S	328635703	0	1024	-	-
2023-11-20	14:41:49	DROP	TCP	192.168.240.100	192.168.240.150	38608	111	44	S	328635703	0	1024	-	-
2023-11-20	14:41:49	DROP	TCP	192.168.240.100	192.168.240.150	38608	23	44	S	328635703	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38610	23	44	S	328504629	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38610	111	44	S	328504629	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38610	445	44	S	328504629	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38610	22	44	S	328504629	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38610	3389	44	S	328504629	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38610	53	44	S	328504629	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38610	1720	44	S	328504629	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38610	8080	44	S	328504629	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38610	5900	44	S	328504629	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38610	139	44	S	328504629	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38608	993	44	S	328635703	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38608	135	44	S	328635703	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38608	3306	44	S	328635703	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38608	143	44	S	328635703	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38608	113	44	S	328635703	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38608	21	44	S	328635703	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38608	25	44	S	328635703	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38608	995	44	S	328635703	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38608	1723	44	S	328635703	0	1024	-	-
2023-11-20	14:41:50	DROP	TCP	192.168.240.100	192.168.240.150	38608	8888	44	S	328635703	0	1024	-	-
2023-11-20	14:41:51	DROP	TCP	192.168.240.100	192.168.240.150	38610	8888	44	S	328504629	0	1024	-	-
2023-11-20	14:41:51	DROP	TCP	192.168.240.100	192.168.240.150	38610	1723	44	S	328504629	0	1024	-	-
2023-11-20	14:41:51	DROP	TCP	192.168.240.100	192.168.240.150	38610	995	44	S	328504629	0	1024	-	-

Come possiamo notare dai file di log del firewall di WindowsXP, viene bloccata la connessione sulle porte porte del sistema.