## 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
                                                                       5900 44
           14:41:49
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                               S
                                                                38608
                                                                                 328635703
                                                                                              1024
2023-11-20
           14:41:49
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                38608 8080 44
                                                                                              1024
2023-11-20
           14:41:49
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                                 328635703
                     DROP
                                                                38608
                                                                      1720 44
                                                                               ς
                                                                                              1024
                                                                               328635703
                                                                       53 44 S
2023-11-20
           14:41:49
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                38608
                                                                                            1024
2023-11-20
                              192.168.240.100
                                               192.168.240.150
                                                                      3389 44
                                                                                            0 1024
           14:41:49
                     DROP
                          TCP
                                                                38608
                                                                               5 328635703
                                                                38608 22 44 5
                                                                               328635703
2023-11-20
                     DROP
           14:41:49
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                                          0
                                                                                            1024
2023-11-20
           14:41:49
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                38608
                                                                       445 44
                                                                                328635703
                                                                                             1024
                              192.168.240.100
2023-11-20
           14:41:49
                     DROP
                          TCP
                                               192.168.240.150
                                                                38608
                                                                      111 44
                                                                                328635703
                                                                                           0 1024
                                                                      23 44 5 328635703
                              192.168.240.100
2023-11-20
           14:41:49
                     DROP
                          TCP
                                               192.168.240.150
                                                                38608
                                                                                          0 1024
2023-11-20
                              192.168.240.100
                                               192.168.240.150
                                                                       23 44
                                                                               328504629
           14:41:50
                     DROP
                          TCP
                                                                38610
                                                                                          0 1024
                                               192.168.240.150
2023-11-20
           14:41:50
                     DROP
                          TCP
                              192.168.240.100
                                                                38610
                                                                      111 44
                                                                                328504629
                                                                                             1024
2023-11-20
           14:41:50
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                38610 445 44
                                                                                328504629
                                                                                           0 1024
2023-11-20
           14:41:50
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                38610
                                                                      22 44 5
                                                                               328504629
                                                                                          0
                                                                                            1024
2023-11-20
                                                                       3389 44
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
           14:41:50
                                                                38610
                                                                               S
                                                                                 328504629
                                                                                            0 1024
                     DROP
2023-11-20
           14:41:50
                              192.168.240.100
                                               192.168.240.150
                                                                38610
                                                                       53 44
                                                                               328504629 0
                          TCP
2023-11-20
                                                                                              1024
           14:41:50
                     DROP
                          TCP
                                                                      1720 44
                              192.168.240.100
                                               192.168.240.150
                                                                38610
                                                                               S
                                                                                 328504629
2023-11-20
                                                                                 328504629
           14:41:50
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                38610
                                                                       8080
                                                                           44
                                                                                              1024
2023-11-20
           14:41:50
                              192.168.240.100
                                               192.168.240.150
                                                                                 328504629
                     DROP
                          TCP
                                                                38610
                                                                       5900
                                                                                           0 1024
                                                                                328504629 0 1024
2023-11-20
                                                                      139 44 5
           14:41:50
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                38610
2023-11-20
           14:41:50
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                38608
                                                                       993 44
                                                                              S
                                                                                328635703
                                                                                             1024
                                                                      135
2023-11-20
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                              S
                                                                                328635703
           14:41:50
                                                                38608
                                                                          44
                                                                                             1024
2023-11-20
           14:41:50
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                38608
                                                                      3306 44 5 328635703
                                                                                            0
                                                                                              1024
                                                                                328635703
328635703
2023-11-20
           14:41:50
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                38608
                                                                      143 44
                                                                              S
                                                                                           0 1024
2023-11-20
                              192.168.240.100
                                                                       113 44
                                                                                             1024
           14:41:50
                     DROP
                          TCP
                                               192.168.240.150
                                                                38608
                                                                             s 328635703
2023-11-20
           14:41:50
                     DROP
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                       21 44
                                                                38608
2023-11-20
                                                                       25 44
           14:41:50
                              192.168.240.100
                                               192.168.240.150
                                                                             S
                                                                               328635703
                     DROP
                          TCP
                                                                38608
                                                                                          0 1024
2023-11-20
                              192.168.240.100
                                               192.168.240.150
                                                                       995 44
                                                                              S
           14:41:50
                     DROP
                          TCP
                                                                38608
                                                                                328635703
                                                                                           0 1024
2023-11-20
           14:41:50
                              192.168.240.100
                                               192.168.240.150
                                                                       1723 44
                                                                               S
                                                                                 328635703
                     DROP
                          TCP
                                                                38608
                                                                                              1024
2023-11-20
                    DROP
           14:41:50
                          TCP
                              192.168.240.100
                                               192.168.240.150
                                                                38608
                                                                       8888 44
                                                                                 328635703
                                                                                              1024
                          TCP
2023-11-20
           14:41:51
                     DROP
                              192.168.240.100
                                               192.168.240.150
                                                                38610
                                                                       8888
                                                                            44
                                                                               S
                                                                                 328504629
                                                                                              1024
                    DROP
                          TCP
                                                                       1723
                                                                                 328504629 0 1024
2023-11-20
           14:41:51
                              192.168.240.100
                                               192.168.240.150
                                                                38610
                                                                           44
                                                                               S
                              192.168.240.100 192.168.240.150 38610 995 44 5 328504629 0 1024
2023-11-20 14:41:51 DROP TCP
```

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