



Emanuele Di Stefano

# S9-L1



Il primo passaggio è stato quello di settare gli IP sulla rete interna sulla stessa rete.

```
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (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 24.82 seconds

(lelo@lelo)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b9:30:af brd ff:ff:ff:ff:ff:ff
    inet 192.168.240.100/24 brd 192.168.240.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feb9:30af/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

(lelo@lelo)-[~]
```

rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.

☐ Ottieni automaticamente un indirizzo IP

☒ Utilizza il seguente indirizzo IP:

Indirizzo IP:

Subnet mask:

Gateway predefinito:

☐ Ottieni indirizzo server DNS automaticamente

☒ Utilizza i seguenti indirizzi server DNS:

Server DNS preferito:

Server DNS alternativo:

Il secondo passaggio consiste nel fare un “nmap -sV 192.168.240.150” e vediamo che la risposta è “host seems down”.

```
nmap -sV
(lelo@lelo)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 16:29 CEST
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 3.14 seconds
```

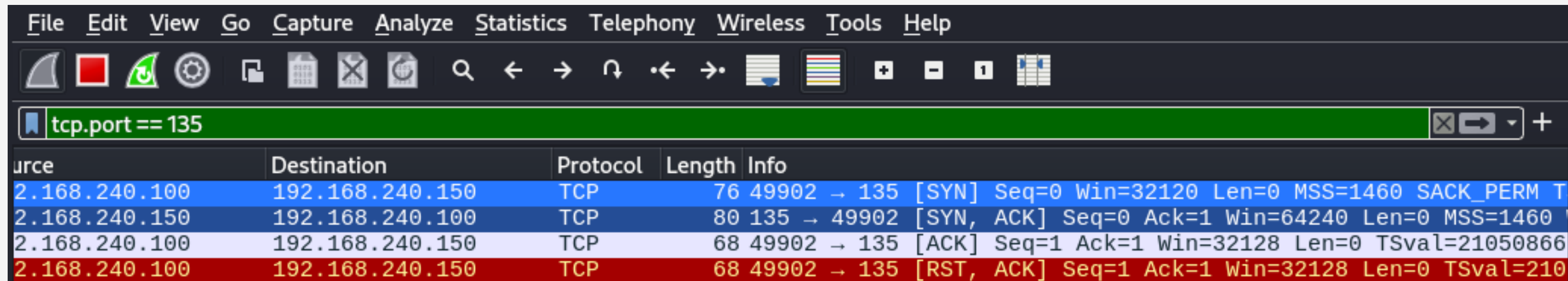
Il terzo passaggio consiste sempre nel fare un “nmap -sV 192.168.240.150” e vediamo che la risposta ci dice che trova delle porte aperte, la 135, 139 e 445. Con il firewall di XP spento abbiamo accesso a queste porte.

```
(lelo@lelo)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 16:30 CEST
Nmap scan report for 192.168.240.150
Host is up (0.0032s 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 20.52 seconds

(lelo@lelo)-[~]
$ █
```

Nel quarto passaggio analizziamo il comando nmap, con il firewall spento, mentre wireshark è in ascolto e vediamo che al quarto passaggio si crea la connessione seq=1 ack=1 e quindi viene stabilita. Lo capiamo analizzando i passaggi prima.



The image shows a Wireshark interface with a filter 'tcp.port == 135'. The packet list shows four packets:

Source	Destination	Protocol	Length	Info
2.168.240.100	192.168.240.150	TCP	76	49902 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T
2.168.240.150	192.168.240.100	TCP	80	135 → 49902 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
2.168.240.100	192.168.240.150	TCP	68	49902 → 135 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=21050866
2.168.240.100	192.168.240.150	TCP	68	49902 → 135 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=210

nel quinto ed ultimo passaggio vediamo sempre con il lancio di un nmap, che wireshark in ascolto non riceve traffico da analizzare in entrata, poiché il firewall è spento.

