

S9/L1

Configurazione Di Rete

Effettuiamo la configurazioni della macchina Kali e Windows Xp come richiesto dalla traccia:

Kali : **192.168.240.100**

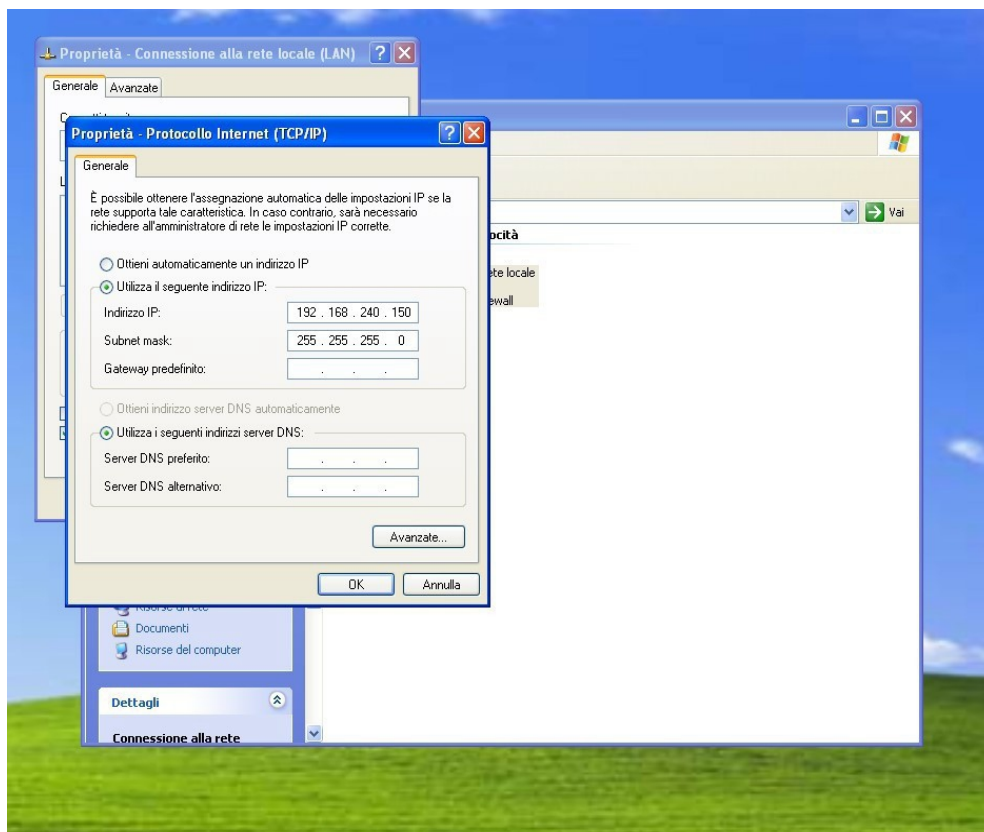
Windows: **192.168.240.150**

```
File Actions Edit View Help
GNU nano 8.0 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100
gateway 192.168.240.1
network 192.168.240.0
```



Firewall On

Effettuiamo un nmap -sV per determinare le porte open ed i servizi che girano su di esse:

nmap -sV 192.168.240.150

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 10:29 EDT  
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 3.06 seconds
```

Come possiamo vedere le porte risultano filtered. Questo ci fa appunto capire che c'è un firewall in funzione che blocca il probing.

Apriamo Wireshark per analizzare cosa sta accadendo ai pacchetti.

Come possiamo notare dallo screen , il Three Way Handshake del protocollo TCP non avviene in maniera corretta. Parte il probing dalla macchina scan (kali), per poi terminare solamente al Syn iniziale. La macchina target non risponde con l'Ack.

1 0.0000000000	192.168.240.100	192.168.240.150	TCP	76 58842 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2364428092 TSecr=0 WS=128
2 0.000072905	192.168.240.100	192.168.240.150	TCP	76 37718 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2364428087 TSecr=0 WS=128
3 2.005316364	192.168.240.100	192.168.240.150	TCP	76 37726 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2364428092 TSecr=0 WS=128
4 2.005395652	192.168.240.100	192.168.240.150	TCP	76 58842 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2364428092 TSecr=0 WS=128

Alcuni firewall sono configurati per consentire il traffico su porte standard come 80 e 443, ma bloccare altre porte. nmap potrebbe provare a inviare pacchetti a queste porte per verificare se sono aperte, anche se il firewall è attivo.

Firewall Off

Effettuiamo un nmap -sV per determinare le porte open ed i servizi che girano su di esse:

nmap -sV 192.168.240.150

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 10:28 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00067s 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 20.26 seconds
```

Come possiamo notare le alcune porte risultano aperte dal probing . Questo ci fa presupporre che nessun firewall sia a difesa della macchina target.

Procediamo a controllare i pacchetti con Wireshark. Come possiamo notare in questo caso il Three Way Handshake è avvenuto correttamente. Dallo screen possiamo notare come ci sia risposta nei 3 step del Syn , Syn/Ack, Ack

47	13.010254477	192.168.240.100	192.168.240.150	TCP	76 35578 → 135 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM TSval=4065579825 TSecr=0 WS=128
68	13.010842312	192.168.240.150	192.168.240.100	TCP	80 135 → 35578 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
74	13.010853031	192.168.240.100	192.168.240.150	TCP	68 35578 → 135 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=4065579826 TSecr=0