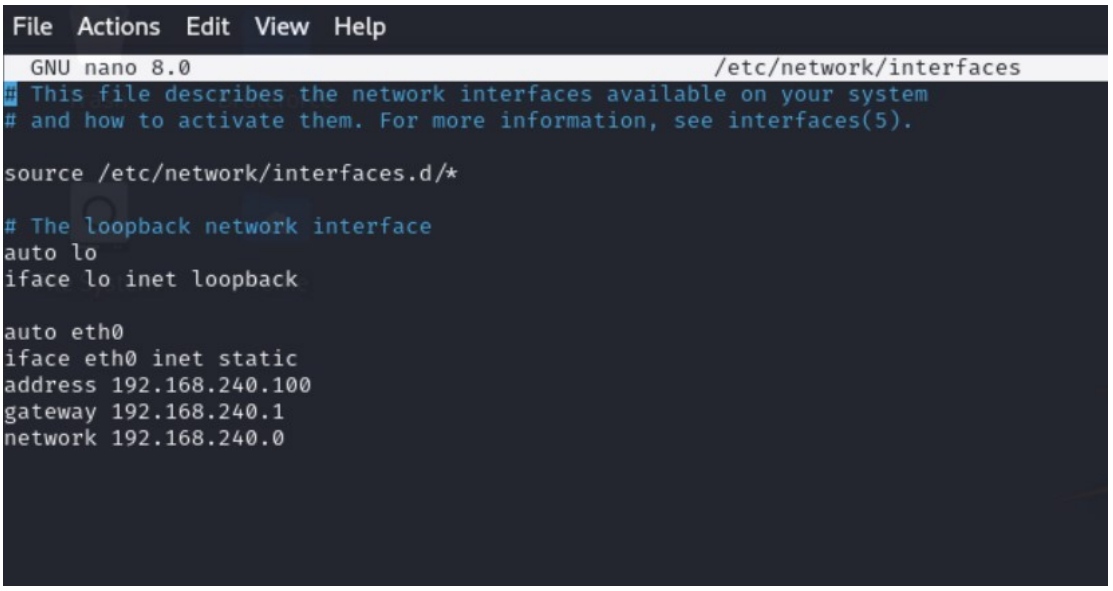
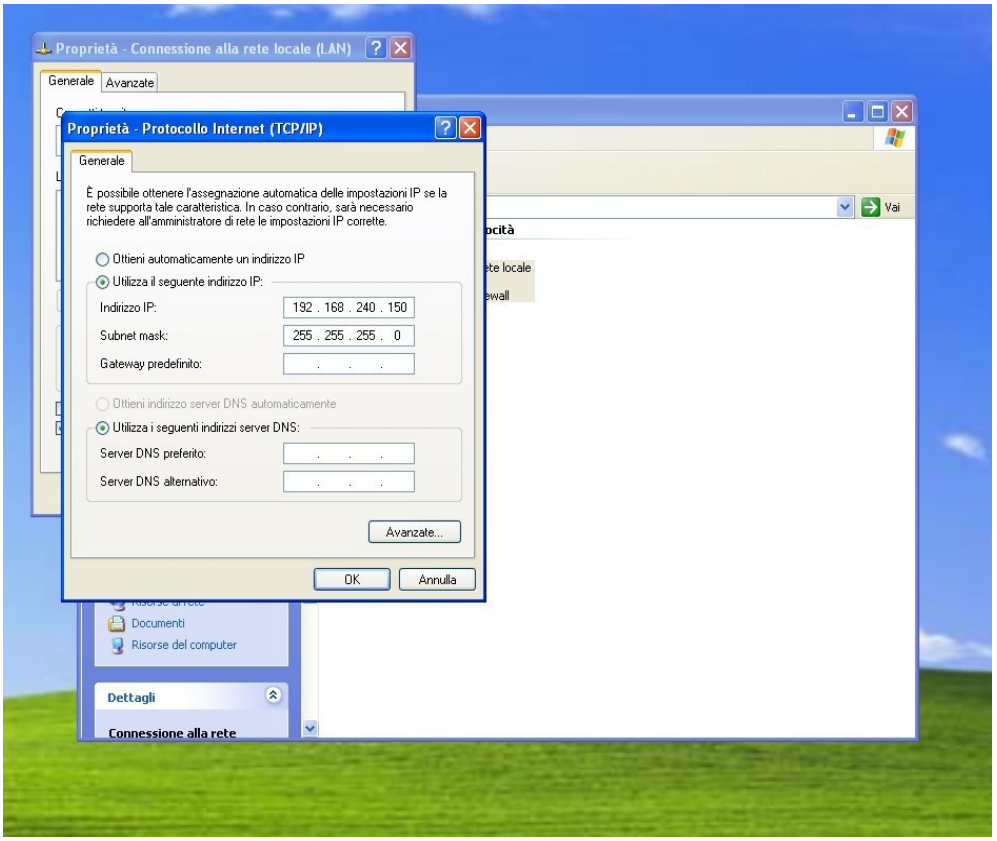
S9/L1
Configurazione Di Rete

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

Kali : **192.168.240.100**
Windows: **192.168.240.150**





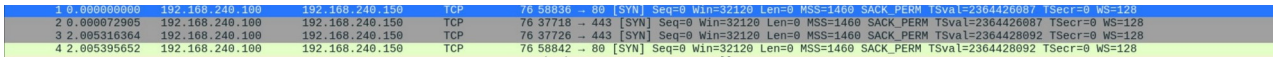
Firewall On

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.

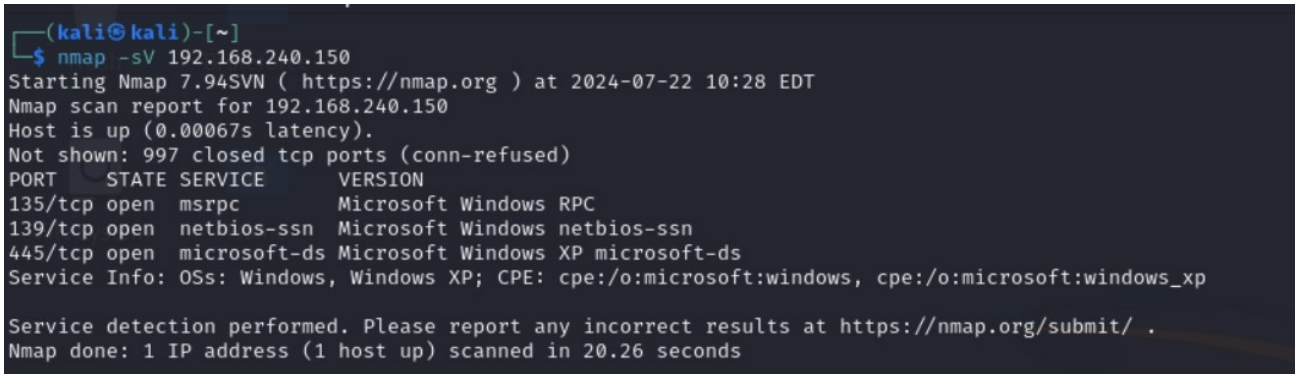


Alcuni firewall sono configurati per consentire il traffico su porte standard come 80 e 443, ma bloccare altre porte. nmap potrebbe provare a inviare pacchetti a queste porte per verificare se sono aperte, anche se il firewall è attivo.

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



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