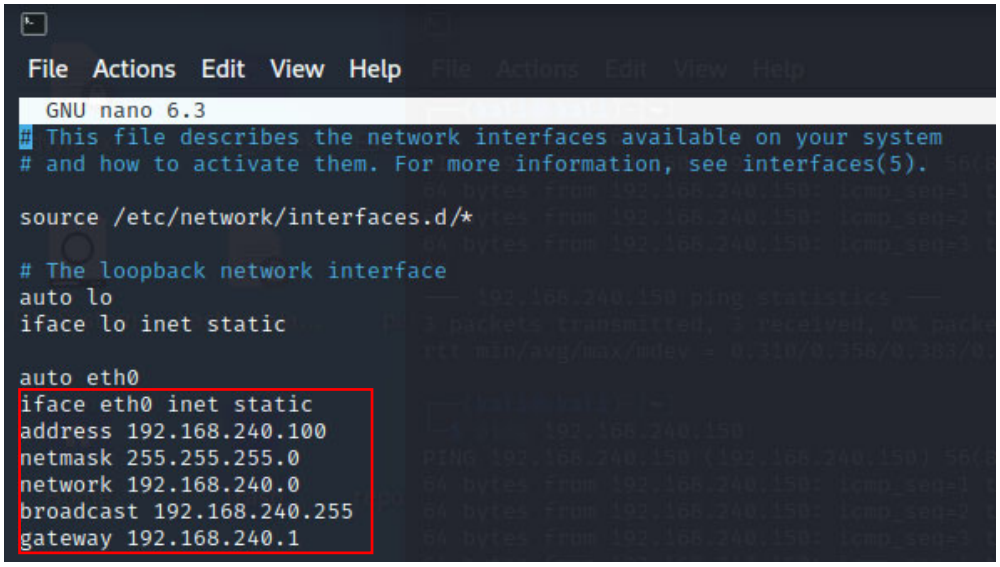
SECURITY OPERATION: Azioni Preventive

L'esericitazione di oggi è di verificare in che modo l'attivazione del firewall impatta sul risutato di una scansione dei servizi dall'esterno.

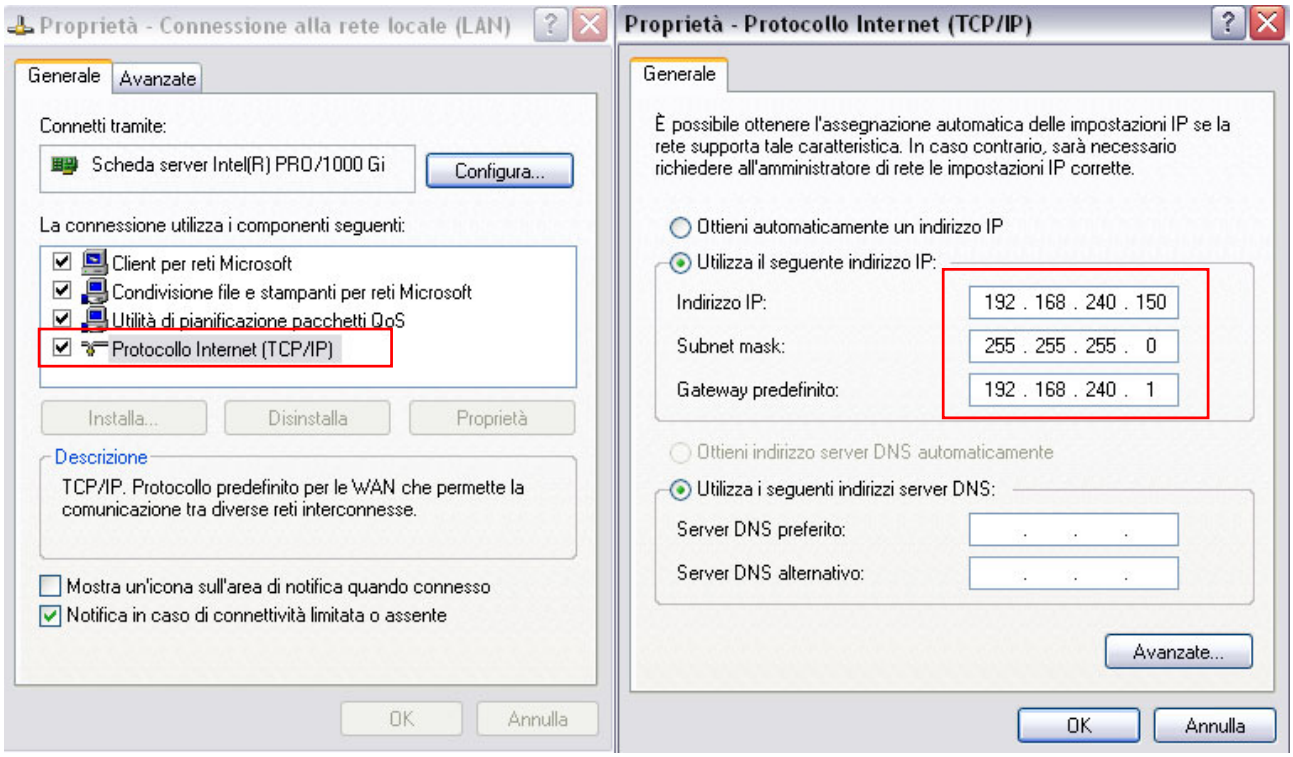
FASE 1

Per prima cosa abbiamo impostato i nostri ambienti di lavoro come rischiesto dalla traccia.

KALI: Tramite il comando **sudo nano /etc/network/interfaces** siamo andatiad impostare l'IP – **192.168.240.100**

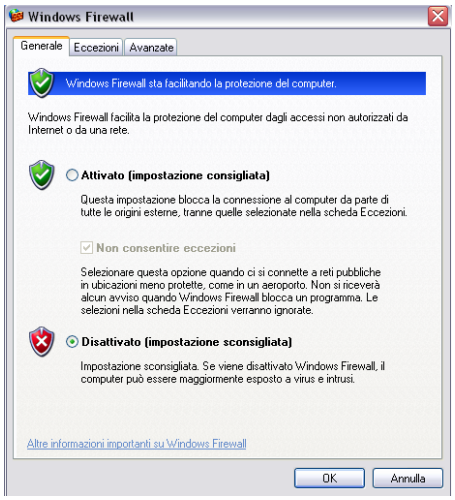


WIN XP: Tramite la schermata di opzioni avanzate nella scheda di rete, protocollo internet TCP/IP impostiamo l'IP – **192.168.240.150**



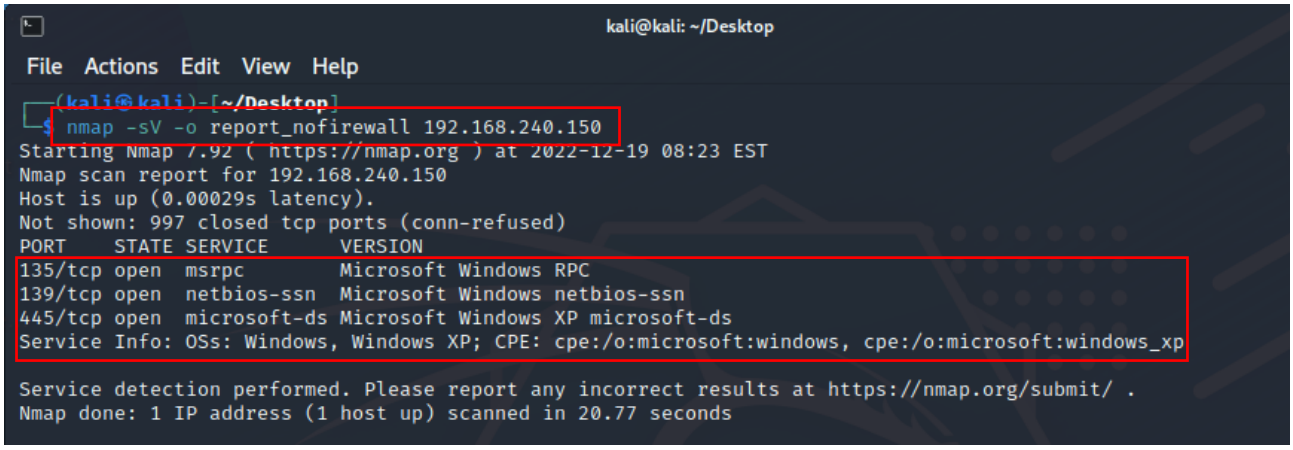
FASE 2

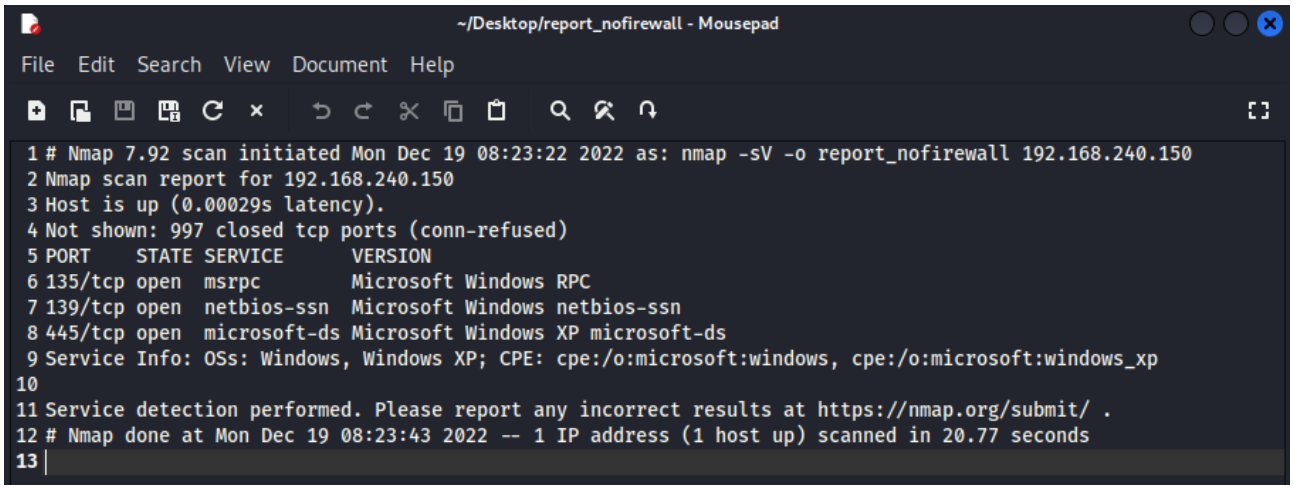
Nella seconda fase abbiamo effettuato una scansione tramite il tool nmap presente su Kali. Per prima cosa andiamo a disattivare il firewall su Windows XP presente come opzioni in Pannello di controllo >> **Windows Firewall**



Utilizzando il comando **nmap –sV –o "nomefile_report" IP BERSAGLIO** diamo inizio alla scansione.

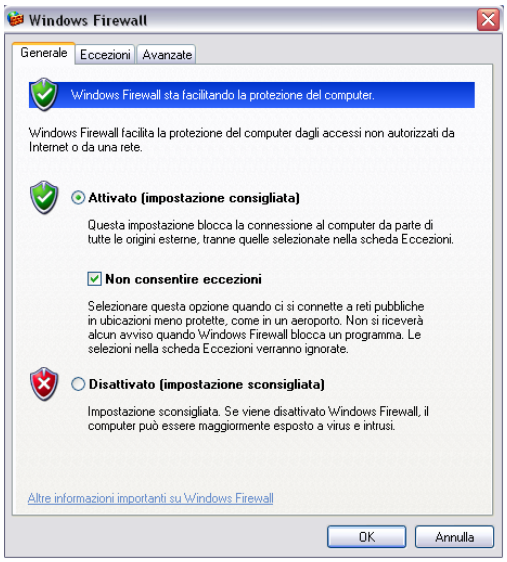
Gli switch inseriti permettono una scansione che come output ci restituisce la Versione dei servizi attivi (**-sV**) e la creazione di un file di log alla fine (**-o "nomefile_log"**).





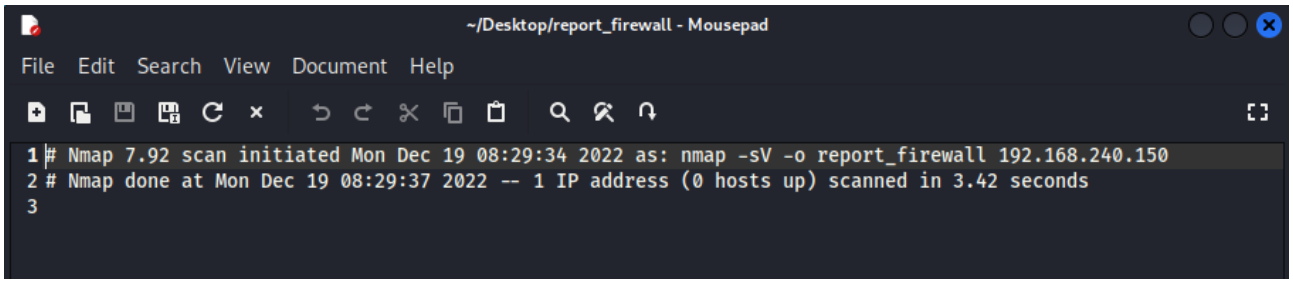
Qui possiamo vedere il risultato del file in output che nmap di crea

Stessa cosa anche per la seconda scansione. Attiviamo il Firewall di Windows XP e lanciamo di nuovo nmap, modificando solamente il nome in output del log che ci salverà




```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -o report_firewall 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:29 EST
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 3.42 seconds
```

Possiamo notare immediatamente che con il firewall attivo e nessuna policy che permetta alla macchina attaccante di “entrare” non ci verrà restituita alcuna informazione utile.

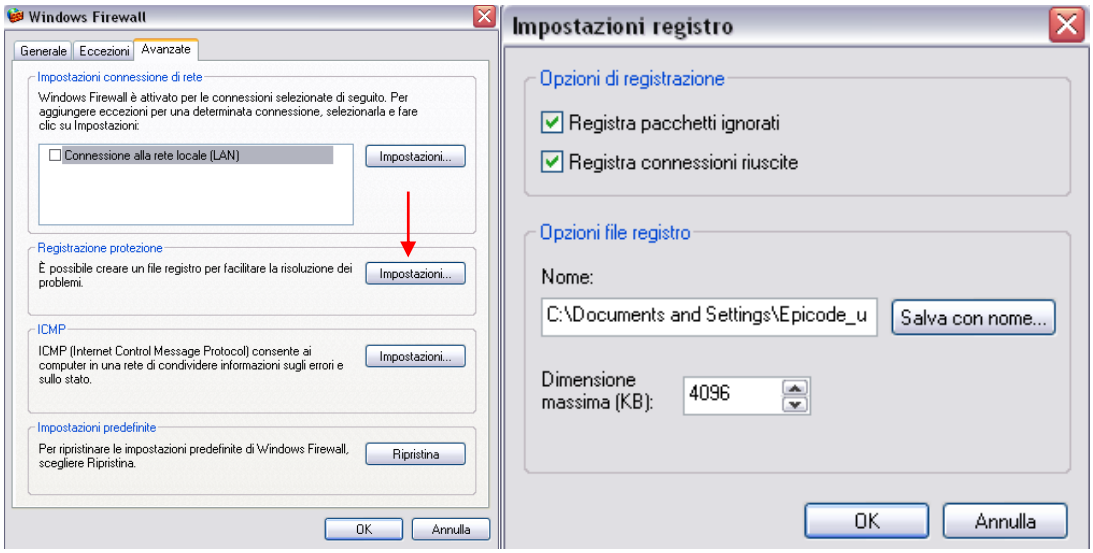


Bonus

Come bonus ci era stato chiesto di notare che differenze c'erano nel log presenti su Windows XP.

Prima di tutto entrano nelle impostazioni del Firewall >> Avanzate.

Da qui ci spostiamo su Registrazione Protezione >> impostazioni e diamo una direcotry al nostro file di log che verrà creato.



Con il firewall attivo possiamo avere un log delle "connessioni" in entrata che sono avvenute.

Possiamo notare al suo interno che la nostra macchina Kali (**src-ip**) ha tentato una connessione con Windows XP (**dst-ip**). L'azione **DROP** ci fa capire perché il log rilasciato nella seconda scansione di nmap era vuoto