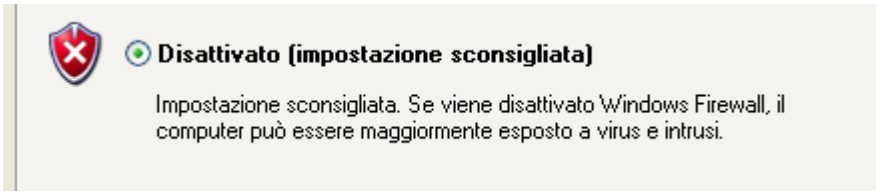
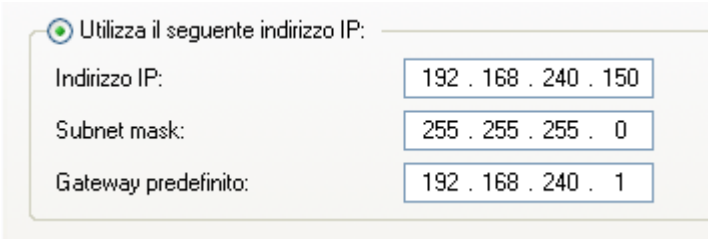
ESERCIZIO S9/L1

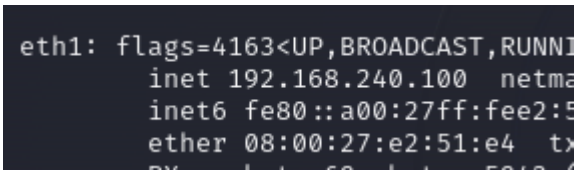
Per prima cosa andiamo su Windows XP e disattiviamo il firewall.



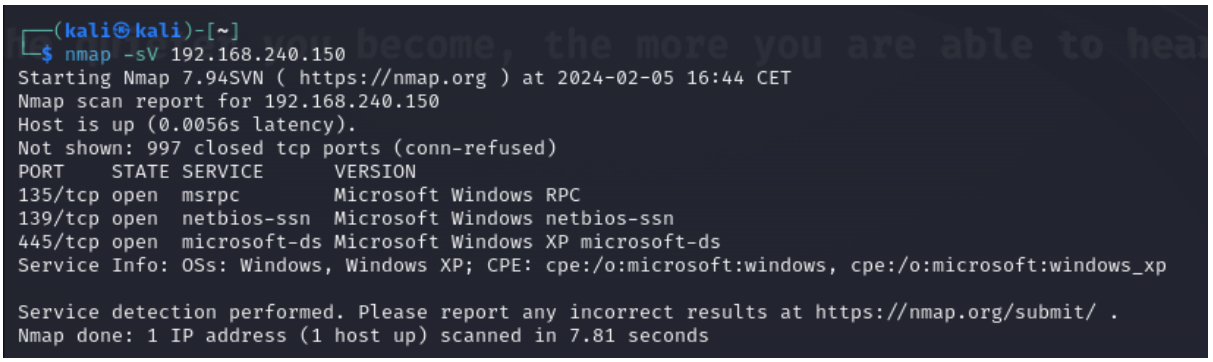
Poi cambiamo l'indirizzo IP:



Cambiamo anche l'indirizzo IP di Kali:



Facciamo una scansione della rete con nmap -sV, con questi risultati:



Se la porta TCP 135 è aperta su un sistema e non è protetta correttamente da un firewall o altre misure di sicurezza, ciò può rendere il sistema vulnerabile a vari tipi di attacchi informatici. Ecco alcuni dei rischi associati all'apertura non protetta della porta 135:

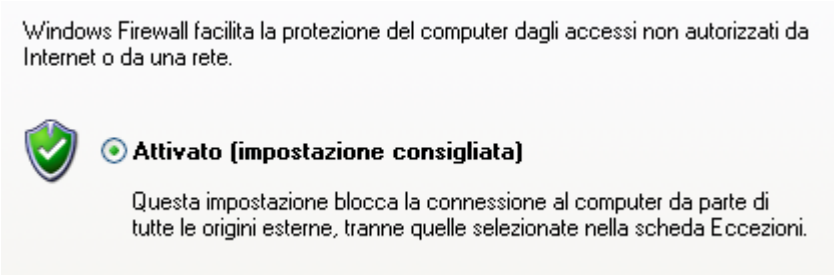
- Attacchi RPC: Un attaccante potrebbe sfruttare la porta 135 per avviare attacchi RPC (Remote Procedure Call) contro il sistema, come l'esecuzione di codice malevolo o la compromissione del sistema.
- Scansione di porte e rilevamento del sistema: Gli attaccanti potrebbero utilizzare strumenti di scansione delle porte per individuare sistemi con la porta 135 aperta. Questo potrebbe essere il primo passo verso un attacco più mirato.
- Distribuzione di malware: Una porta aperta potrebbe essere utilizzata per distribuire malware sul sistema, ad esempio attraverso exploit noti o attacchi di phishing.
- Denial of Service (DoS): Gli attaccanti potrebbero sfruttare la porta aperta per avviare attacchi DoS, sovraccaricando il sistema con un'elevata quantità di traffico di rete, rendendolo inaccessibile agli utenti legittimi.

- Esecuzione remota di comandi: In alcuni casi, una porta aperta potrebbe consentire a un attaccante di eseguire comandi arbitrari sul sistema vulnerabile, ottenendo così un controllo completo.

Se le porte TCP 139 e 445 sono aperte su un sistema senza protezione adeguata, ciò può esporre il sistema a vari rischi di sicurezza. Ecco alcuni dei potenziali rischi associati all'apertura non protetta delle porta 139 e 445:

- Vulnerabilità alle intrusioni: La porta 139 è comunemente associata al protocollo Server Message Block (SMB), che viene utilizzato per la condivisione di file e stampanti su una rete locale. Se la porta è aperta e non protetta, gli attaccanti potrebbero cercare di sfruttare vulnerabilità nel servizio SMB per ottenere accesso non autorizzato al sistema.
- Attacchi ransomware: Gli attaccanti potrebbero sfruttare la porta 139 per distribuire ransomware sui sistemi vulnerabili. Il ransomware può criptare i file del sistema e richiedere un riscatto per ripristinarli, causando gravi danni e perdite di dati.
- Accesso non autorizzato ai file condivisi: Se la porta 139 è aperta e configurata per consentire l'accesso non autorizzato ai file condivisi, gli attaccanti potrebbero ottenere accesso ai file sensibili o sensibili memorizzati sul sistema.
- Esecuzione di codice malevolo: Gli attaccanti potrebbero sfruttare vulnerabilità nel servizio SMB per eseguire codice malevolo sul sistema vulnerabile, consentendo loro di prendere il controllo del sistema o di eseguire altre azioni dannose.
- Scansione e rilevamento della rete: Gli attaccanti potrebbero utilizzare strumenti di scansione delle porte per individuare sistemi con la porta 139 aperta. Questo potrebbe essere il primo passo verso un attacco più mirato.

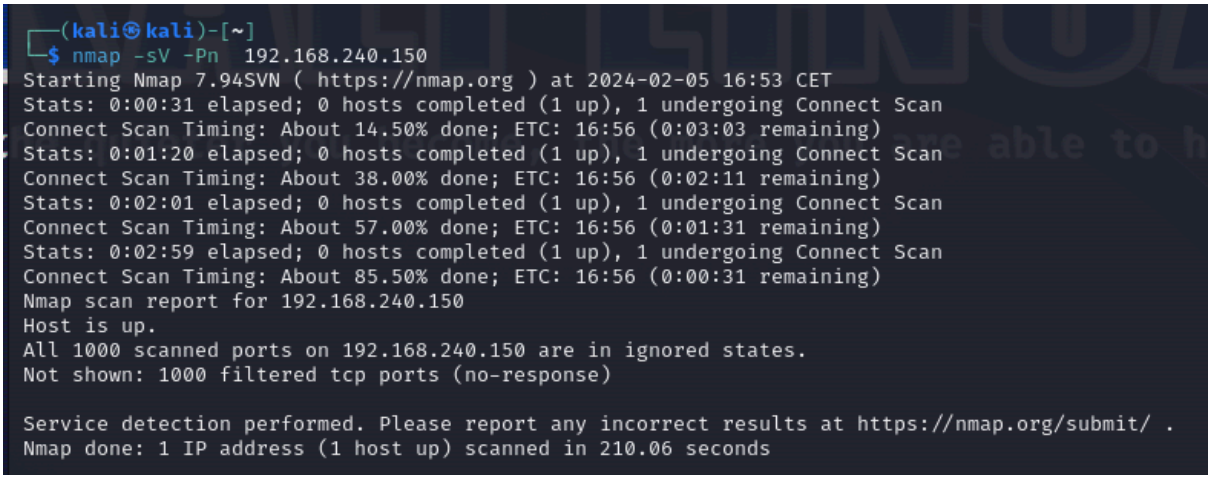
Ora riattiviamo il firewall di Windows XP:



E vediamo che la scansione con nmap riporta risultati diversi:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 16:52 CET
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 3.33 seconds
```

Per indagare più a fondo, proviamo ad aggiungere il comando -Pn:



L’attivazione del firewall ha rimosso la vulnerabilità delle porte aperte.