*Traccia:*

La macchina Windows XP che abbiamo utilizzato ha di **default il Firewall disabilitato**.

L’esercizio di oggi è verificare in che modo l’attivazione del Firewall impatta il risultato di una scansione dei servizi dall’esterno. Per questo motivo:

1. Assicuratevi che il Firewall sia **disattivato** sulla macchina Windows XP

2.Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch–sV, per il service detection e -o nomefilereport per salvare in un file l’output)

3.**Abilitare il Firewall** sulla macchina Windows XP

4.Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch–sV.

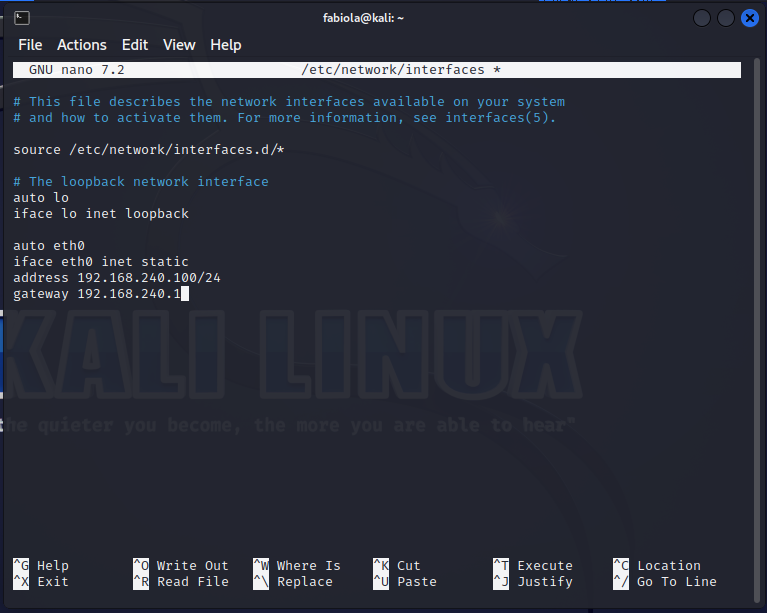
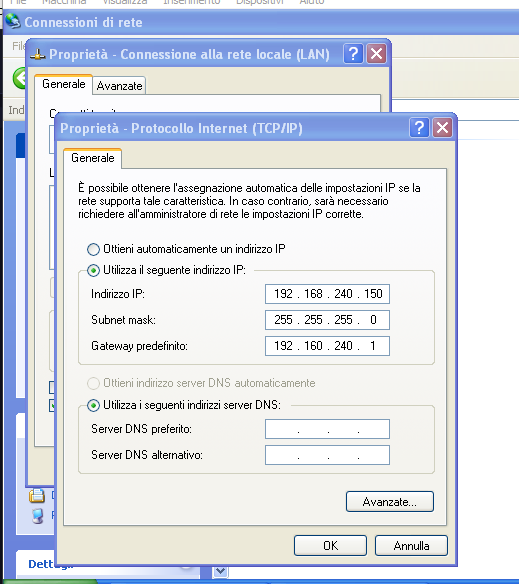
5.Trovare le eventuali differenze e motivarle.

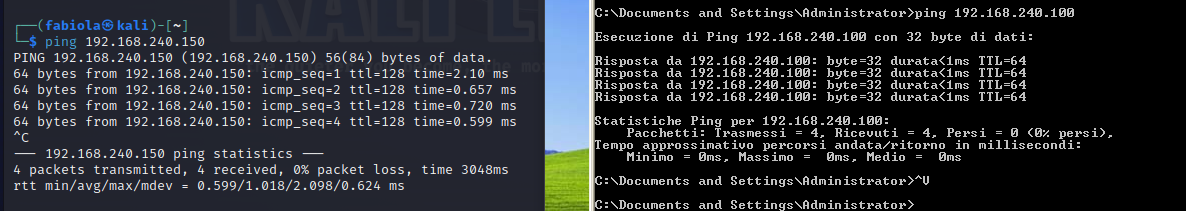
*Requisiti:*

Configurate l’indirizzo di Windows XP come di seguito: 192.168.240.150

Configurate l’indirizzo della macchina Kali come di seguito: 192.168.240.100

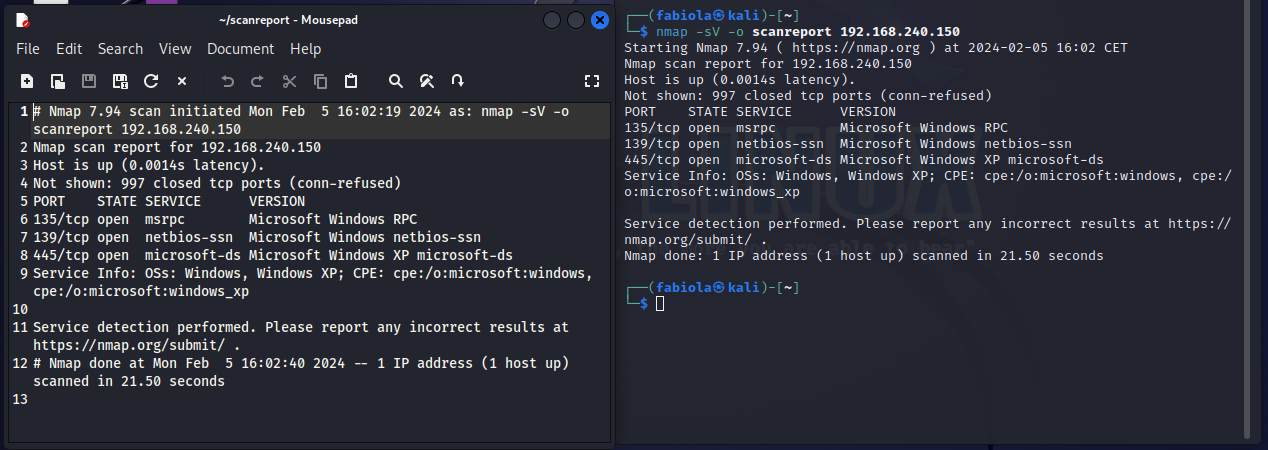
La prima cosa da fare, come richiesto dall’esercizio, è cambiare la configurazione di rete della macchina Kali e Windows XP ed assicurarsi che comunichino tra loro:



Una volta fatto questo fondamentale passaggio, andiamo sulla macchina target, e, attraverso il Centro Sicurezza PC assicuriamoci che il firewall sia disattivato, come dovrebbe di default; passiamo su Kali e creiamo un file di testo (che chiameremo scanreport, su cui si salverà l’output) prima di aprire un terminale su Kali su cui eseguire il seguente comando Nmap 🡪 **nmap -sV -o scanreport 192-168-240-150,** e vediamo cosa succede:

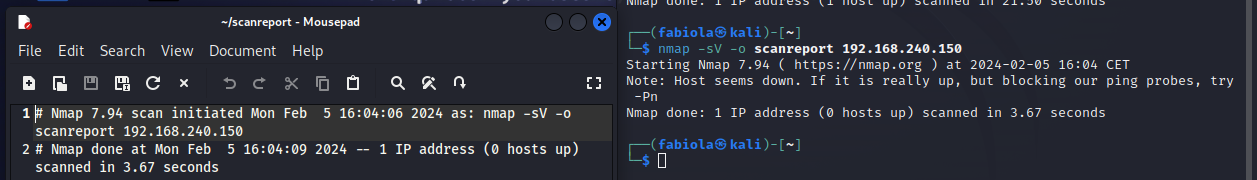




Come possiamo vedere, senza le restrizioni date dal filtraggio del Firewall, Nmap riesce ad ottenere un immagine completa delle porte aperte sul dispositivo target.

Se testiamo la scansione, riattivando il Firewall sul Windows XP, come possiamo vedere, essa non riesce.





Questo succede perché, come sappiamo, il Firewall ha il compito, fondamentale in un contesto di sicurezza informatica, di agire da barriera tra una rete interna e potenziali minacce esterne.

Quindi, quando si eseguono scansioni di rete con strumenti come Nmap, come abbiamo testato noi, il comportamento del firewall può influenzare i risultati della scansione. Un firewall configurato in modo rigoroso potrebbe bloccare i pacchetti di scansione in arrivo, rendendo difficile ottenere una visione completa della topologia e delle porte aperte sulla rete. Al contrario, se il firewall è configurato in modo più permissivo, la scansione potrebbe essere in grado di rilevare più informazioni sulla rete, il che lascia fin troppo campo libero a malintenzionati.