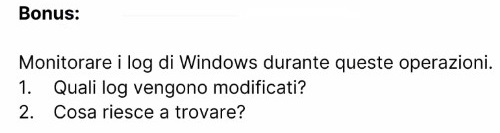
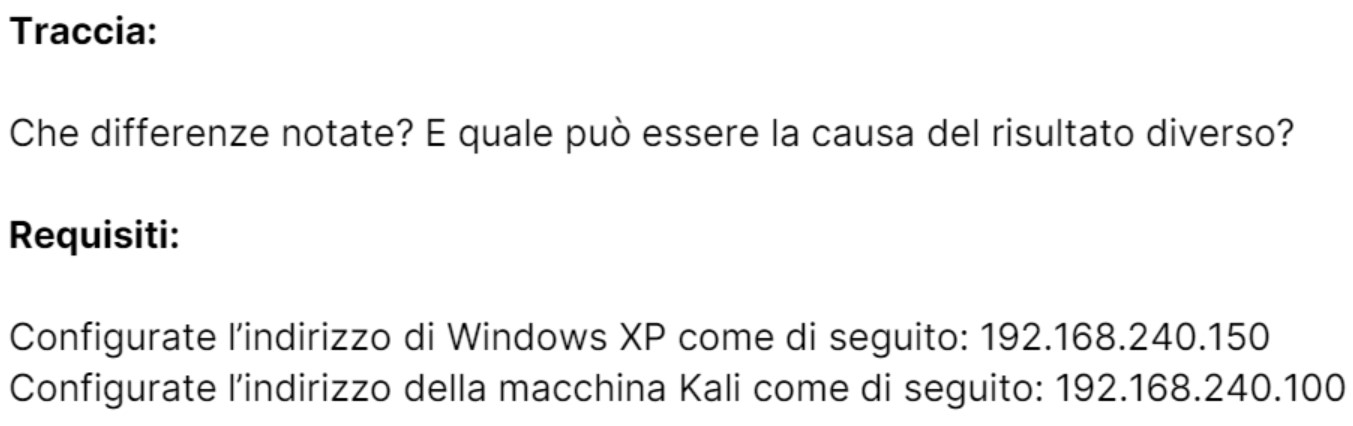
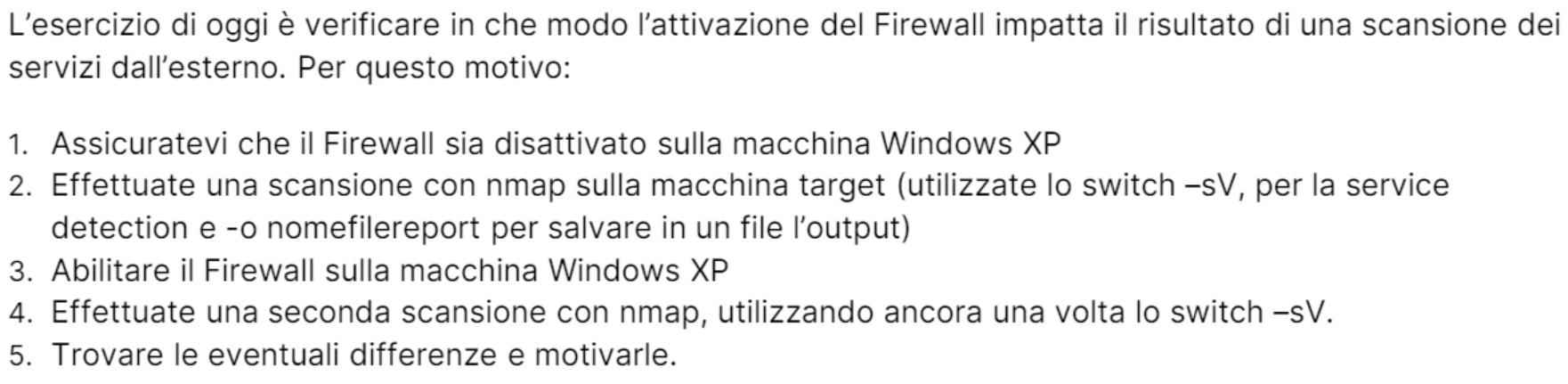
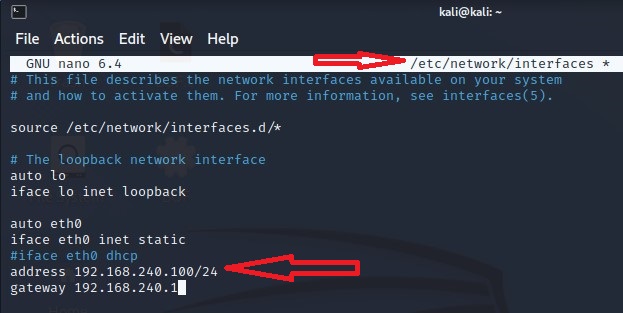
**SECURITY OPERATION: AZIONI PREVENTIVE**

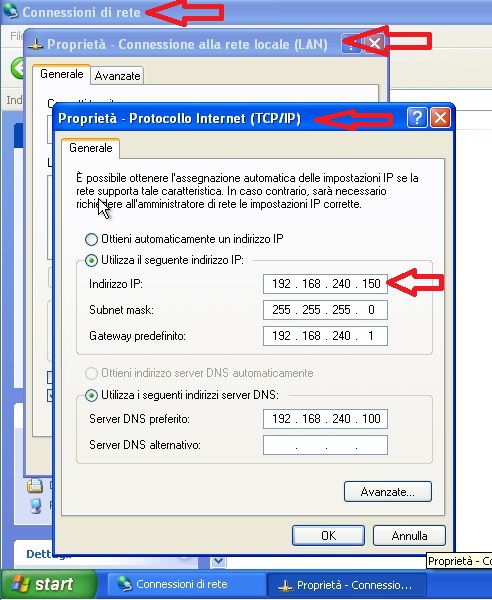


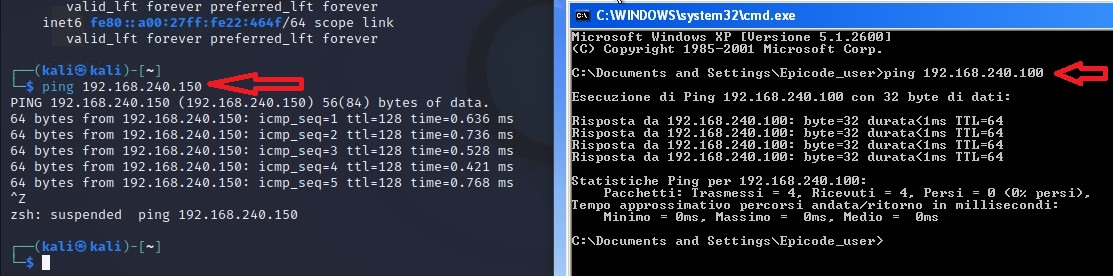
Come richiesto, siamo andati a modificare gli IP delle macchine; per la macchina attaccante Kali, abbiamo eseguito il comando “*sudo nano /etc/network/interfaces*”. 

Per poi riavviare il sistema con il comando “*sudo /etc/init.d/networking restart”* e controllato poi il cambio di IP tramite “*ip a”.* Immagine che contiene testo

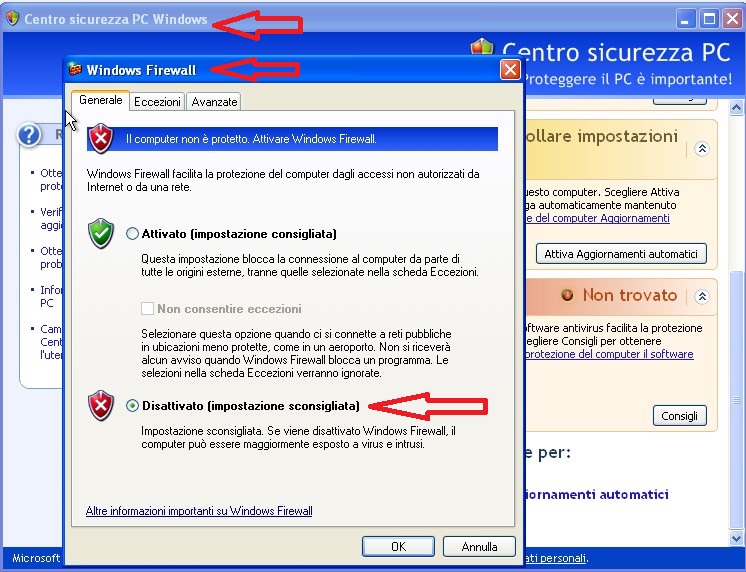
Descrizione generata automaticamente

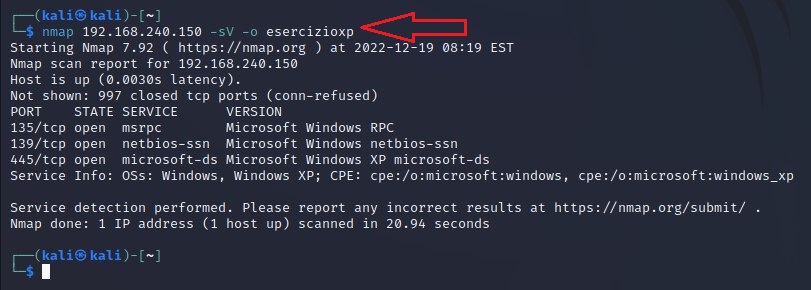
Siamo andati quindi a modificare l’indirizzo IP della macchina Windows XP tramite il percorso: *Start > Pannello di Controllo > Rete e connessioni Internet > Connessioni di Rete > Propietà – Connessione alla rete locale (LAN) > Proprietà – Protocollo Intenet (TCP/IP).*

**

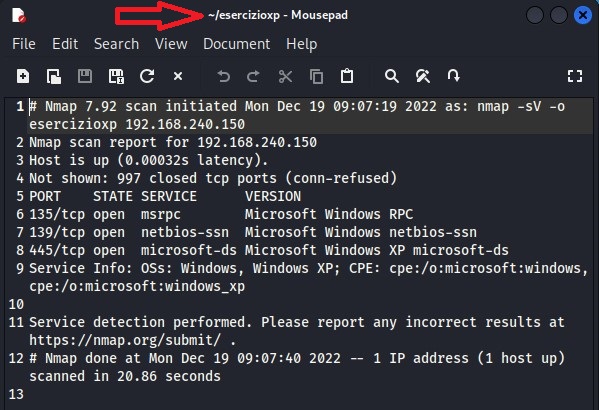
Abbiamo quindi controllato la giusta connessione tra le macchine con il comando di “*ping”.*

Abbiamo quindi controllato che su Windows XP il Firewall fosse disattivato come richiesto tramite il percorso *Start > Pannello di Controllo > Centro sicurezza PC > Windows Firewall.*

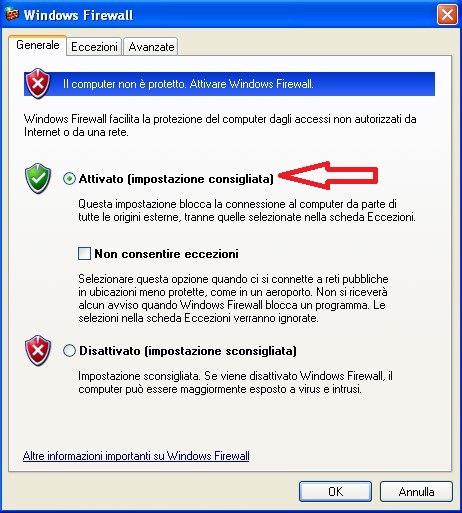


Abbiamo così avviato la nostra scansione nmap su Kali con il comando “*nmap 19.168.240.150 -sV -o esercizioxp”.*

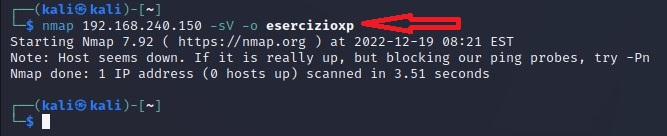
Abbiamo usato lo switch -*sV* per la service detection e visualizzare le versioni dei servizi attivi e lo switch -*o* per salvare in un file l’output.



Siamo andati ad attivare il Firewall sulla macchina Windows XP, seguendo il path precedente.

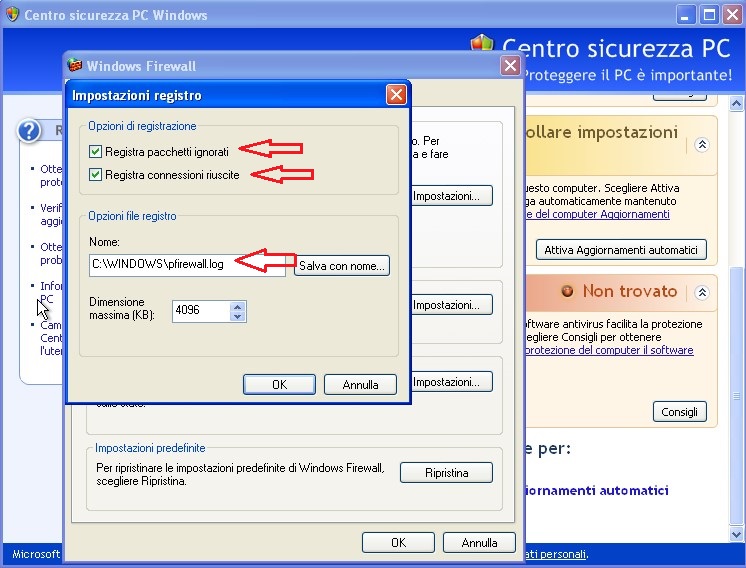


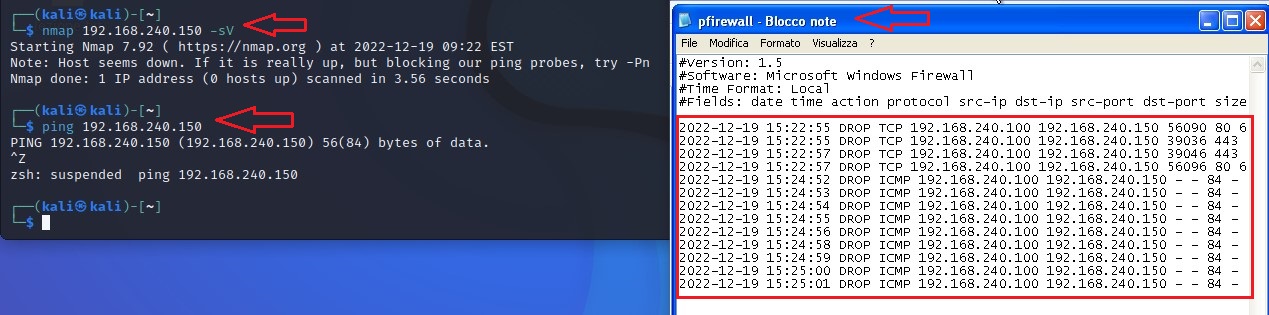
Abbiamo così riprovato la scansione con nmap.



Com’è possibile vedere la seconda scansione, con il Firewall attivo non darà alcun risultato, in quanto l’host target (Windows XP) ci risulterà non attivo o non raggiungibile.

Andremo a modificare le impostazioni avanzate del Firewall per permettere alla macchina di registrare i pacchetti di connessione ignorati/riuscite.



Andremo così a verificare sul file specificato le nostre prove di connessione con nmap e ping da Kali a Windows XP.

Com’è possibile vedere le connessioni in entrata (TCP per *nmap* e ICMP per il *ping*) appariranno nel log di Windows XP come scartate (DROP) in quanto il Firewall è attivo e bloccherà tutte le connessioni in entrata, mentre con il Firewall disattivato non avremo nessun tipo di log salvato sul file. Per permettere lo scambio di pacchetti tra le macchine e consentirne il salvataggio dei log si potrebbero creare delle Firewall Policy.