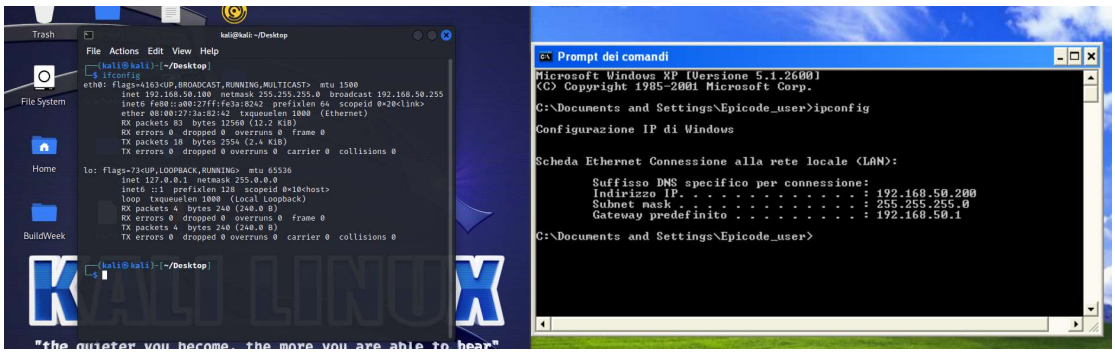
Security Operation: azioni preventive

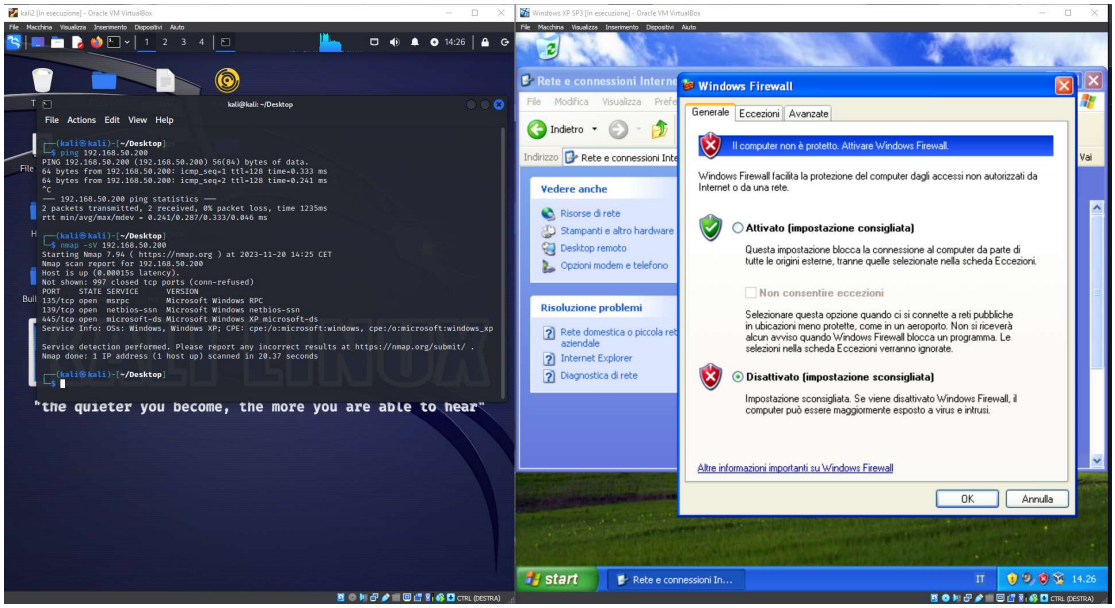
Durante l'esercizio di oggi andremmo a testare due scansioni da Kali verso la macchina Windows XP guardando come il firewall può mitigare la possibilità di attacchi provenienti dall'esterno.

Come prima cosa sono andato a cambiare gli indirizzi IP delle due macchine virtuali mettendole nella stessa rete così che riescano a comunicare.

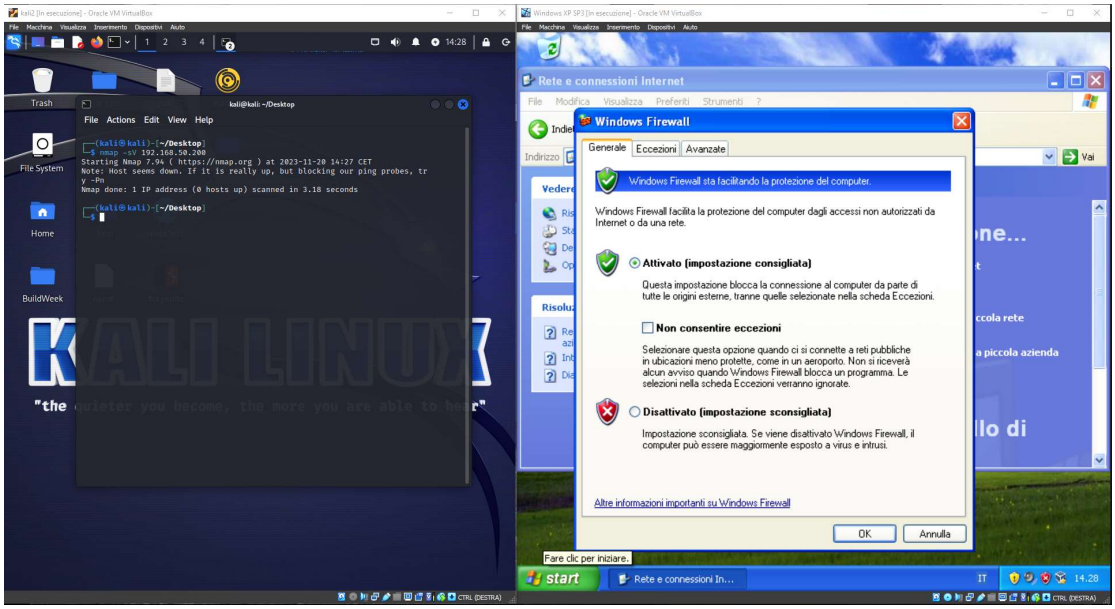


Sono andato ad effettuare due scansioni utilizzando il comando <nmap -sV [IP]> così da andare cercare i servizi con le versioni attive sulla macchina.

La prima scansione l'ho effetuata con il firewall spento e come possiamo vedere dallo screen successivo la scansione è andata a buon fine quindi sono riuscito a recuperare delle informazioni utili.



Mentre per la seconda scansione ho riattivato il firewall di Windows e possiamo vedere come non si riesca a vedere nessuna informazione.



Questo perchè nmap utilizza il ping per effettuare le scansioni e il firewall di windows ha una protezione che blocca i ping, quindi una volta attivato, tutti i ping che partivano da Kali per effettuare la scansione nmap venivano bloccati e non sono riuscito a vedere nessuna informazione, questo blocco è molto efficace per evitare le scansioni da utenti esterni.

Mentre, quando avevo il firewall disabilitato, questo blocco del ping non era presente quindi nmap ha potuto pingare la macchina Windows XP e di conseguenza recuperare le informazioni.

Con queste informazioni un malintenzionato può preparare un attacco ad hoc per bucare la macchina vittima.