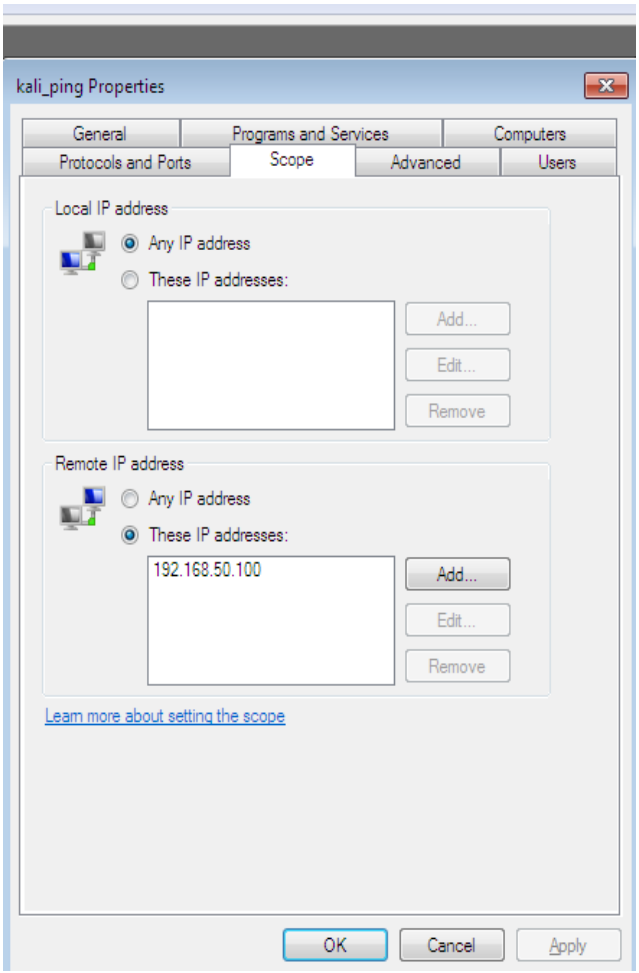
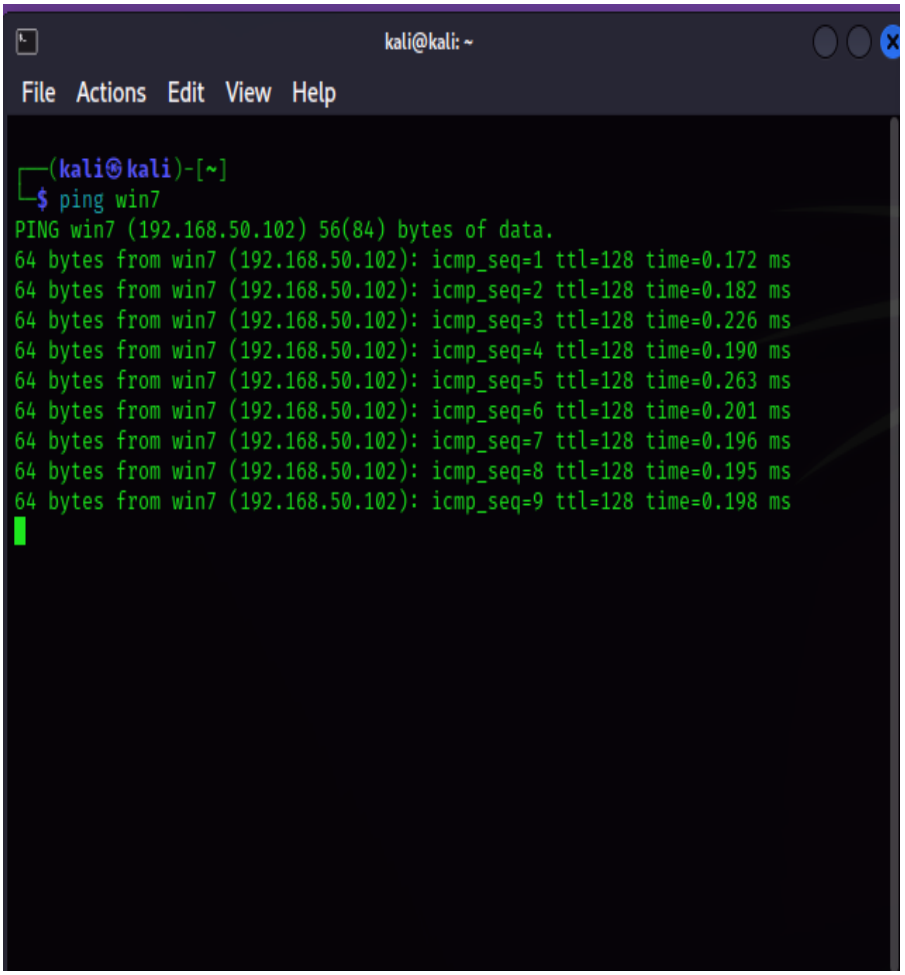
Esercizio 7 Wireshark e Firewall Win7

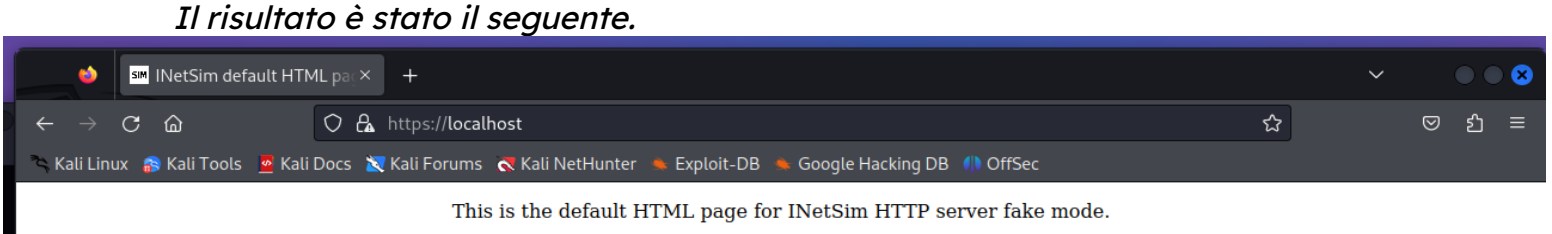
Gelosa Matteo

Abbiamo due macchine collegate tra loro tramite una rete interna. Provando con il comando ping per verificare la comunicazione, la risposta è stata negativa.
Ecco una versione corretta e più fluida del tuo testo:
Questo avviene perché la macchina con sistema operativo Windows7 (192.168.50.102) blocca le richieste in entrata grazie al suo firewall.
Ho proceduto con l'impostazione di una nuova regola sul firewall per permettere la comunicazione tra le due macchine.Ho impostato l'ip della macchina Kali(192.168.50.100) come "sicuro" ed il risultato è stato positivo, con il comando ping le due macchine comunicano tra loro.





Successivamente sulla macchina Kali ho usato un tool "Inetsim" che è in grado di emulare servizi http,https,dns ecc sulla propria rete locale.
Ho configurato il tool per far si che mi mostrasse una pagina web emulata quando cercavo l'indirizzo Localhost(127.0.0.1) nella barra di ricerca del browser.
Il risultato è stato il seguente.



Infine, ho utilizzato il tool 'Wireshark' per catturare i pacchetti scambiati durante la richiesta di visualizzazione della pagina web.
Come si può notare ad ogni richiesta che effettuo avviene uno scambio SYN/ACK.
La richiesta SYN viene mandata dal mittente, è come una richiesta di sincronizzazione per avviare la connessione.
Se il destinatario è disposto ad avviare la sincronizzazione risponderà positivamente con ACK. Questo fa sì che la connessiona possa avvenire correttamente.