

Esercizio 7 Wireshark e Firewall Win7

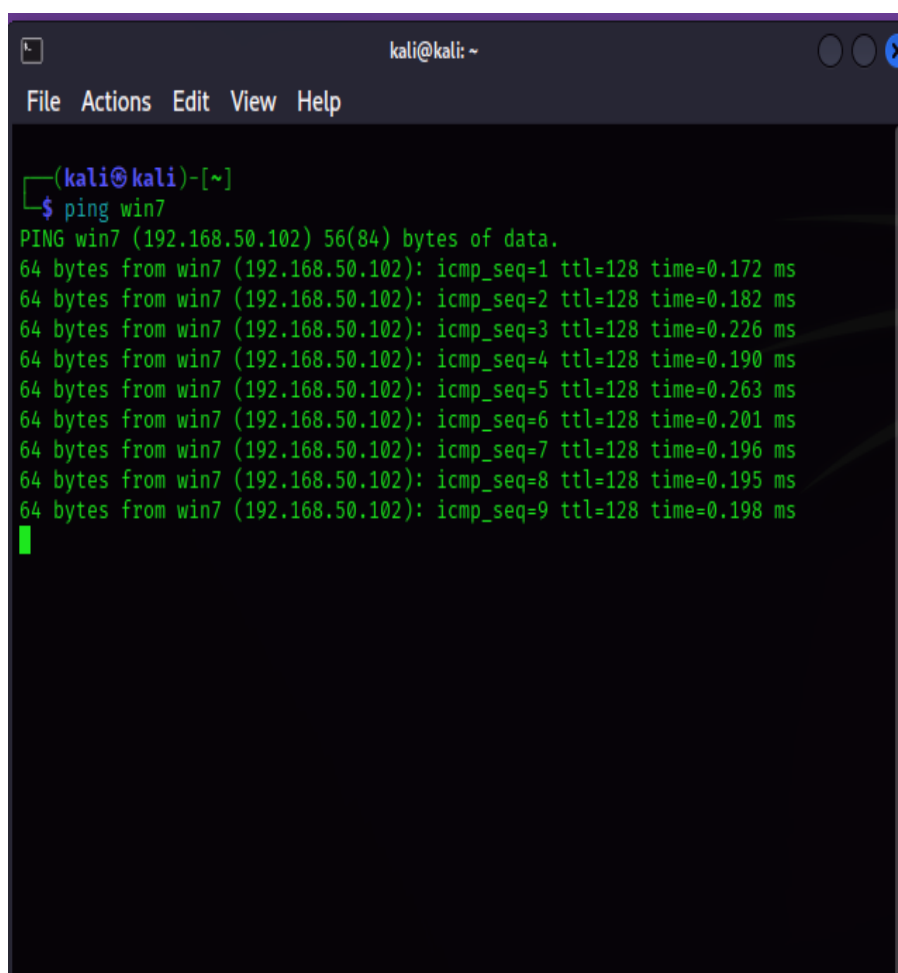
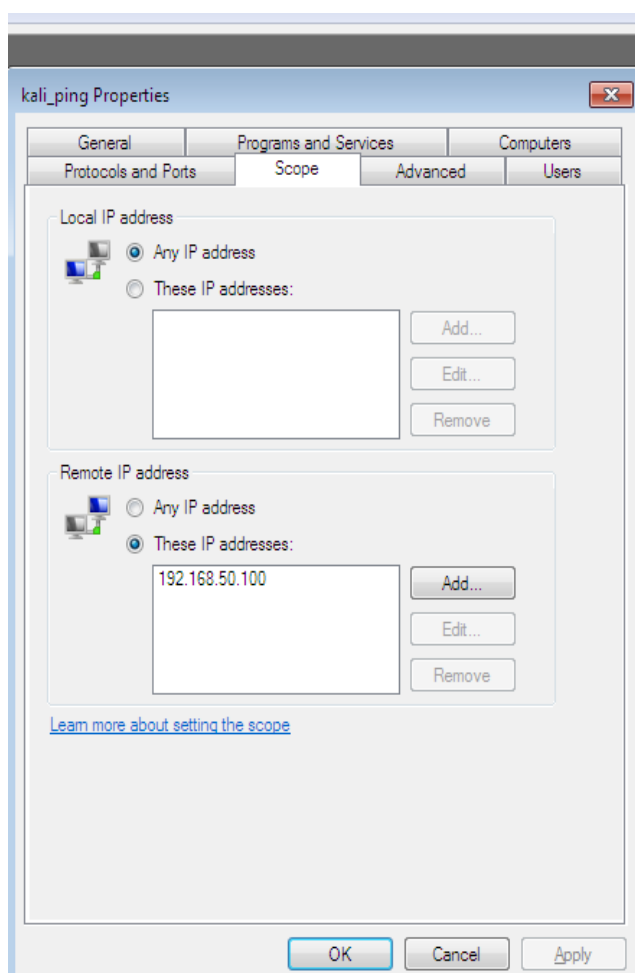
Gelosa Matteo

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.

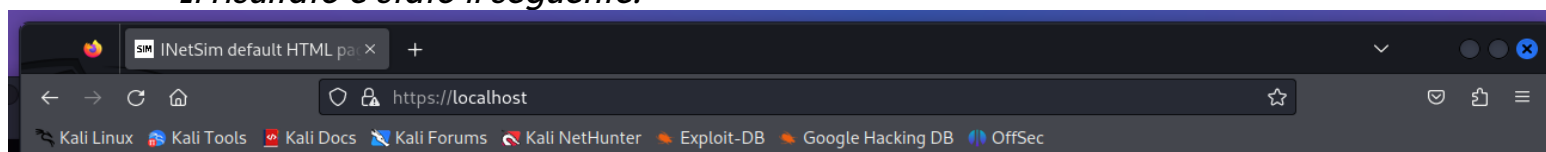
Ho proceduto con l'impostazione di una nuova regola sul firewall per permettere la comunicazione tra le due macchine. Ho impostato l'ip della macchina Kali(192.168.50.100) come "sicuro" ed il risultato è stato positivo, con il comando ping le due macchine comunicano tra loro.



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 sì 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.



This is the default HTML page for INetSim HTTP server fake mode.

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 connessione possa avvenire correttamente.

TCP	66 443 → 59794	[ACK]	Seq=1 Ack=622 Win=64896 Len=0 TSval=1768052564 TSecr=1768052564
TCP	74 59796 → 443	[SYN]	Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=1768052572 TSecr=0 WS=128
TCP	74 443 → 59796	[SYN, ACK]	Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=1768052572 TSecr=1768052572 WS=128
TCP	66 59796 → 443	[ACK]	Seq=1 Ack=1 Win=65536 Len=0 TSval=1768052572 TSecr=1768052572
TLSv1.3	687	Client Hello	
TCP	66 443 → 59796	[ACK]	Seq=1 Ack=622 Win=64896 Len=0 TSval=1768052573 TSecr=1768052573
TLSv1.3	1487	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data	
TCP	66 59794 → 443	[ACK]	Seq=622 Ack=1422 Win=64384 Len=0 TSval=1768052605 TSecr=1768052605
TLSv1.3	146	Change Cipher Spec, Application Data	
TCP	66 443 → 59794	[ACK]	Seq=1422 Ack=702 Win=65536 Len=0 TSval=1768052606 TSecr=1768052606