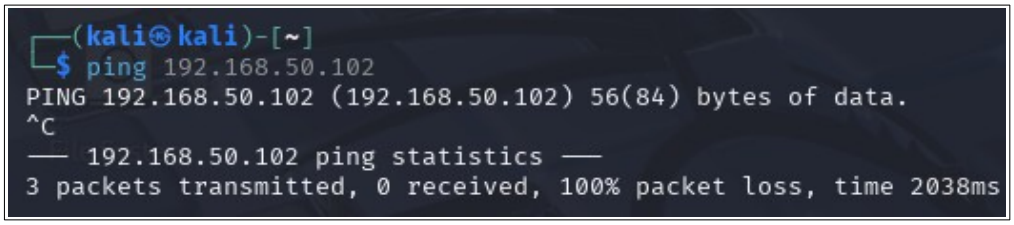
Esercitazione con macchine virtuali e Wireshark W3D4

In questa esercitazione vedremo come aggiungere una policy al Firewall di Windows 7, come utilizzare il servizio di InetSim su Kali Linux ed infine come catturare pacchetti su Wireshark.

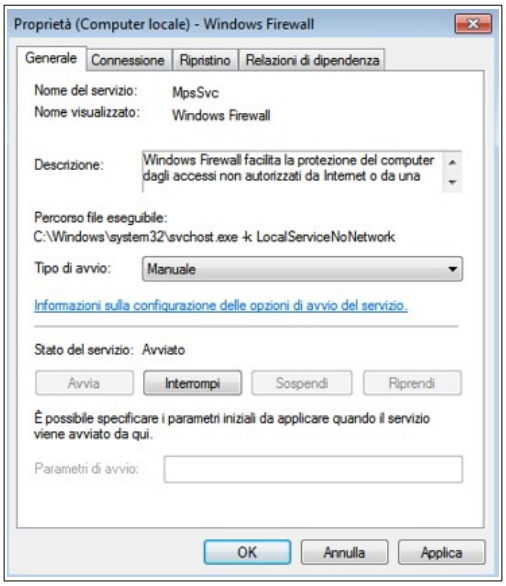
INDICE:

Instaurazione di una Policy sul Firewall di Windows

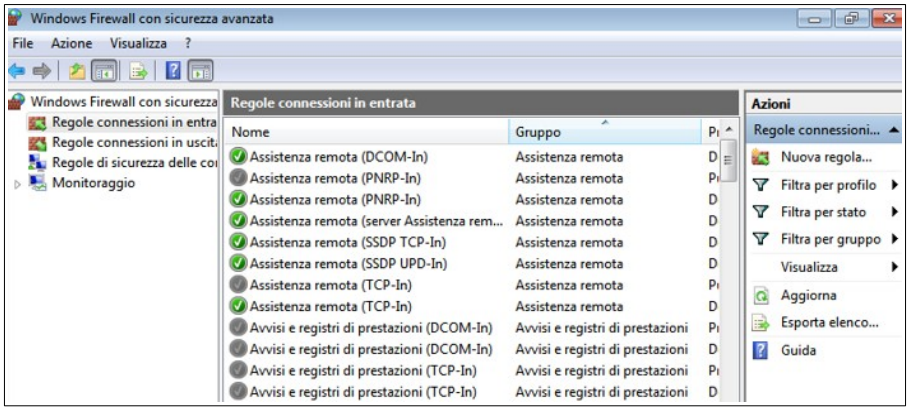
Come già visto in esercitazioni precedenti se proviamo a far partire il comando di ping da una macchina Linux a una Windows non riceveremo una risposta, questo perché il firewall di Windows impedisce la ricezione del ping da parte di Linux. Vedremo ora come ovviare al problema.



Step 1 Avviare la macchina di Windows 7, selezionare sevizi, Windows firewall e assicurarsi che il tipo di avvio selezionato sia “manuale”.



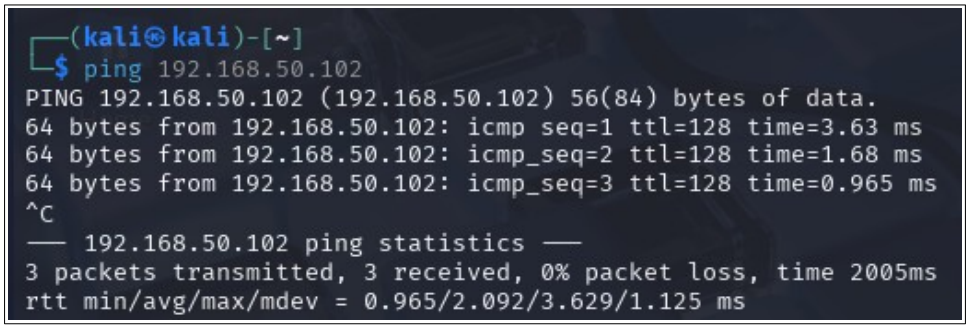
Step 2 Spostiamoci sulle impostazioni avanzate del firewall e, nel nostro caso, dovremo cliccare su “regole connessioni in entrata” in quanto vogliamo instaurare una policy che riguarda il traffico diretto verso la nostra macchina (ping).



Step 3 Ora andremo a definire la nuova policy, dandogli i parametri richiesti dall'esercitazione:

Tipo di regola	Personalizzata
Programma	Tutti i programmi
Protocollo e porte	ICMPv4
Ambito	Qualsiasi indirizzo IP (locali e remoti)
Operazione	Consenti la connessione
Profilo	Dominio, privato, pubblico
Nome	allow_ping

Step 4 Finalmente potremo tornare sulla macchina Kali, ritentare il ping e otterremo una risposta positiva.

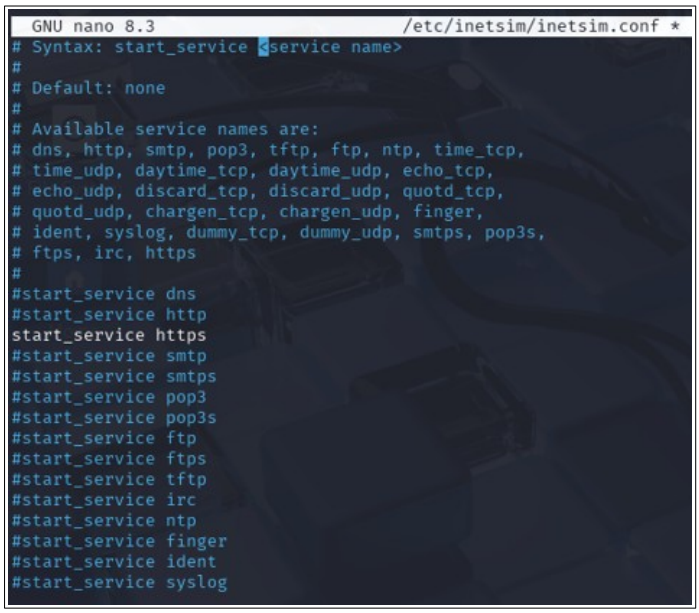


Utilizzo di InetSim su Kali Linux

InetSim è un utility presente su Kali Linux che ci permette di simulare diversi servizi, per lo scopo dell'esercizio andremo ad attivare il servizio HTTPS.

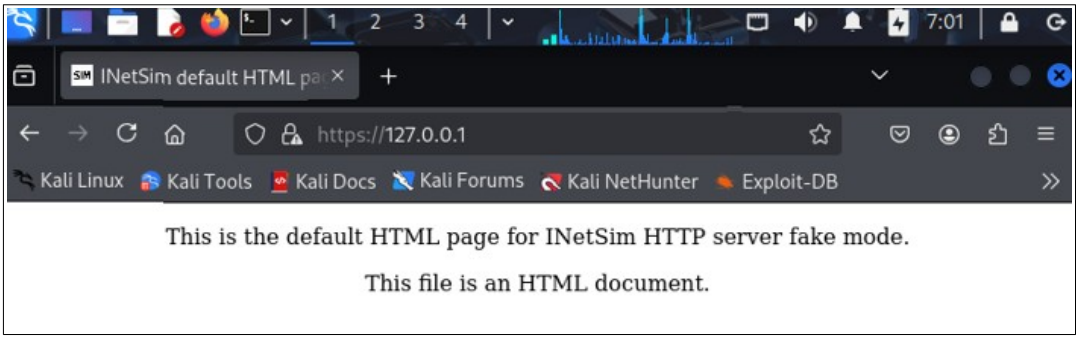
Step 1 Accendere la macchina Linux e da terminale eseguire il comando:
sudo nano /etc/inetsim/inetsim.conf

Step 2 Kali aprirà un file contente tutti i servizi offerti da InetSim, noi dovremo quindi aggiungere il carattere # davanti ad ogni riga di cui non ci interessa usare il servizio. Lasciando quindi solo la riga che riguarda HTTPS senza il cancelletto davanti.

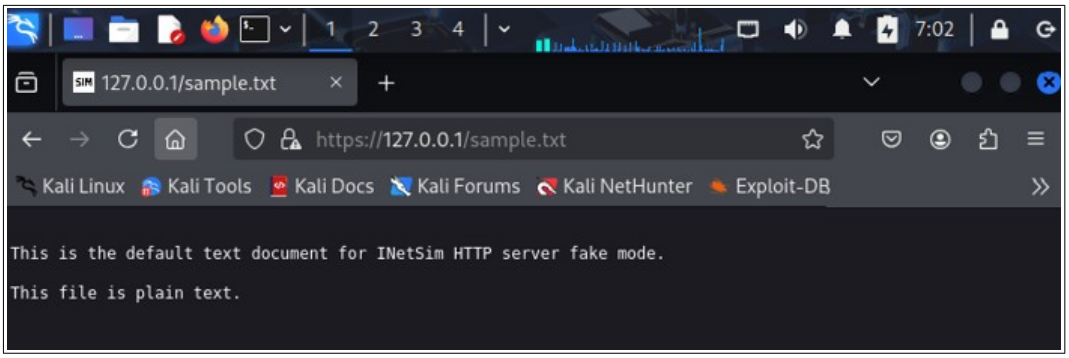


Step 3 Salviamo le modifiche apportate al file e proseguiamo impartendo il comando: *sudo inetsim.*
Questo avvierà la simulazione e ci fornirà dei dati sui parametri del servizio (ad esempio la porta su cui è in ascolto).

Step 4 Ricordandoci che si tratta di una simulazione, apriamo il browser web di Kali e inseriamo l'indirizzo del localhost: *https://127.0.0.1*. La pagina che si aprirà sarà la conferma che il servizio è attivo e raggiungibile dal localhost.



Step 5 Come ulteriore controllo possiamo richiedere al browser uno dei file fittizi forniti dal servizio HTTPS, per farlo dovremo scrivere *https://127.0.0.1/sample.txt* nella barra di ricerca del browser.



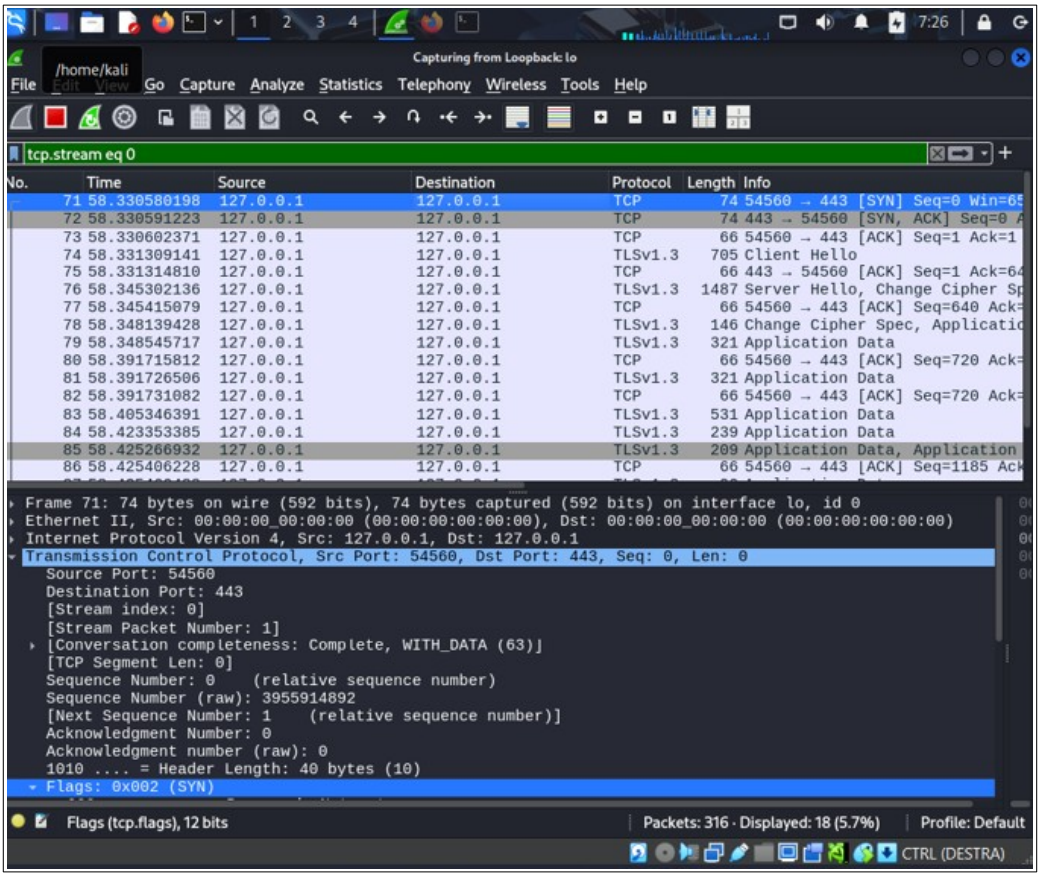
Cattura dei pacchetti con Wireshark

Come ultimo passaggio dell'esercizio dovremo catturare dei pacchetti mediante l'utilizzo di Wireshark.

Step 1 Avviare Wireshark sulla Macchina Kali e metterlo in ascolto sull' interfaccia di loopback.

Step 2 Connettiamoci al localhost e richiediamo il file fittizio come visto in precedenza.

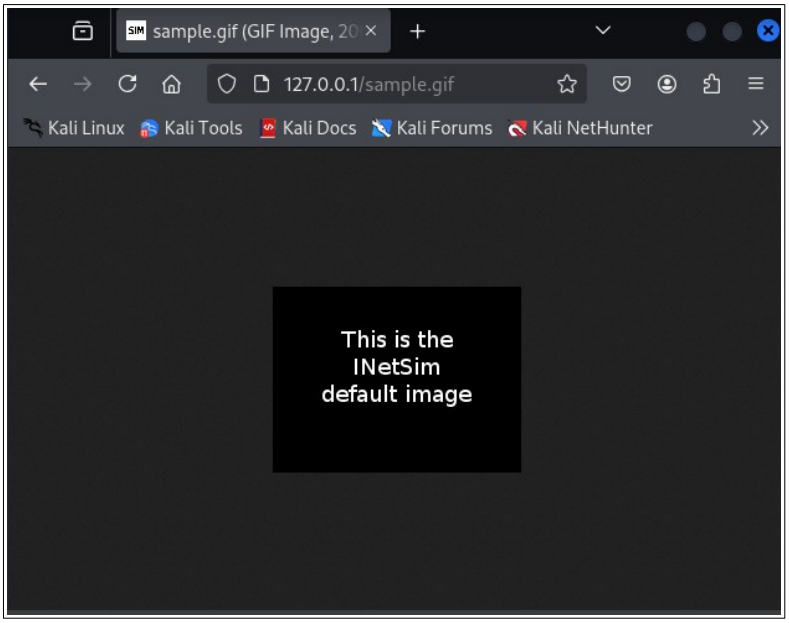
Step 3 Impostiamo il filtro *tcp.stream eq 0* ed analizziamo un pacchetto. Osserando i dati forniti da Wireshark possiamo vedere ad esempio: la connessione instaurata tramite TCP e la three-way-handshake (syn, syn+ack, ack), e la destination port del servizio HTTPS (443).



Esercizio facoltativo

Scegliamo un servizio diverso offerto da InetSim, catturiamo i pachetti con Wireshark e analizziamone il contenuto.

Per questo esercizio ho scelto il servizio HTTP, lo ho attivato con la stessa modalità prevista per il servizio HTTPS e avviato la simulazione
Ho aperto il browser, ho richiesto un file fittizio digitando *127.0.0.1/sample.gif* e tramite Wireshark ho analizzato i pacchetti.



Come possiamo notare nell'immagine sotto, dopo aver applicato il filtro HTTP, si può vedere il protocollo utilizzato (TCP) e la three-way-handshake, la porta di destinazione (80) e che sia il source IP che il destination IP corrispondono (localhost loopback).