10/11/2023

Ilaria Pedrelli

Configurazione Policy su Firewall e Packet Capture con Wireshark

Esercizio:

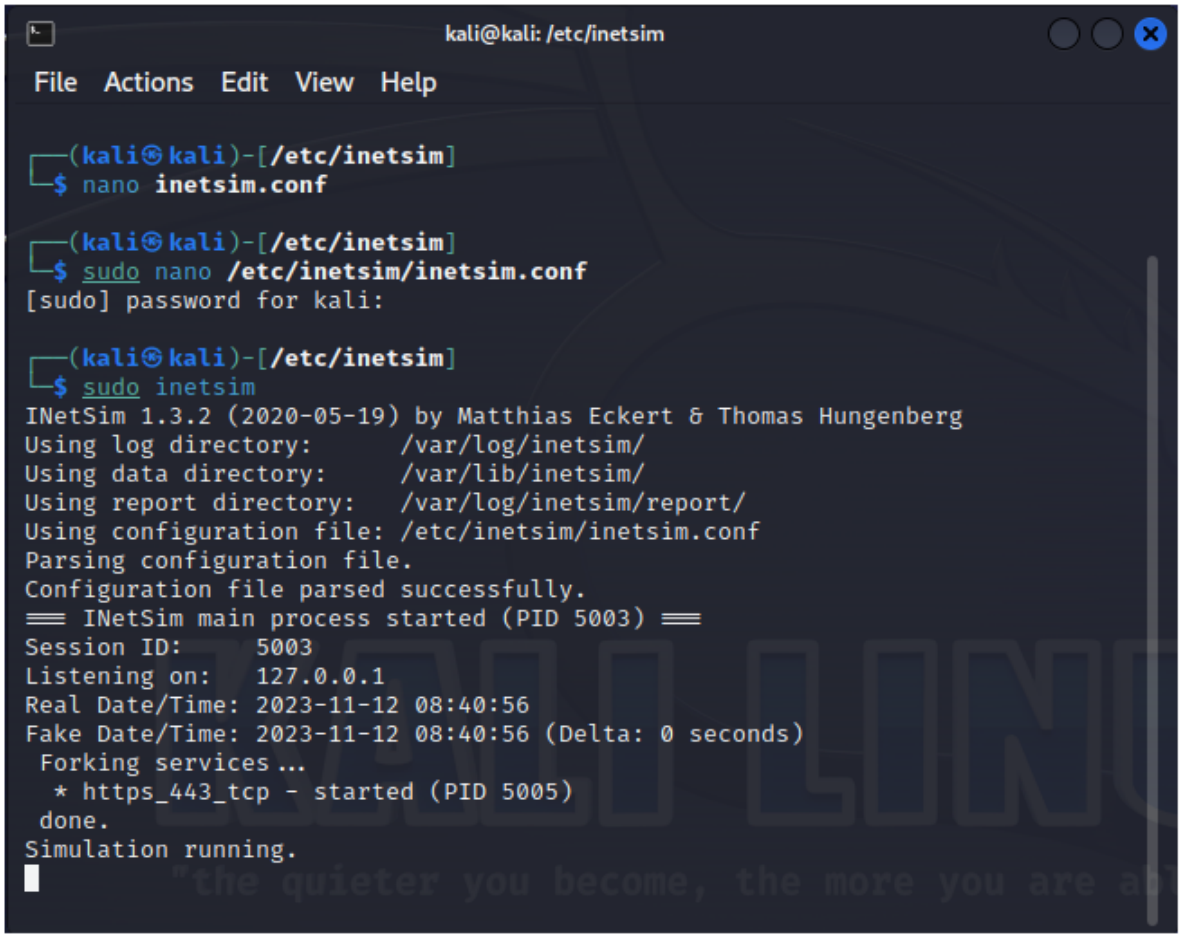
- Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio virtuale (windows firewall)
- Utilizzo dell'Utility InetSim per l'emulazione di servizi Internet
- Cattura di pacchetti con Wireshark

1. Utilizzo dell'Utility InetSim per l'emulazione di servizi Internet e Cattura di pacchetti con Wireshark

Per prima cosa, su laboratorio virtuale Kali Linux, configuro il software InetSim che mi permette di simulare una rete, per esempio, un web server.

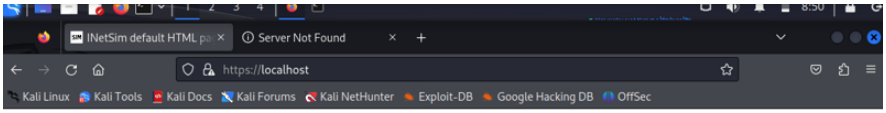
Inizio la configurazione dal prompt di Kali, con **nano /etc/inetsim** poi mi sposto nella directory con **cd /etc/inetsim** all'interno della directory lancio il comando **ls** per vedere i file all'interno, nel mio caso trovo inetsim.conf e lo apro con il comando nano. Nel file vado a disattivare tutti i servizi con esclusione del servizio HTTPS. Commento quindi gli altri per disattivarli.

Modifico anche l'indirizzo IP LocalHost con l'indirizzo 127.0.0.1.



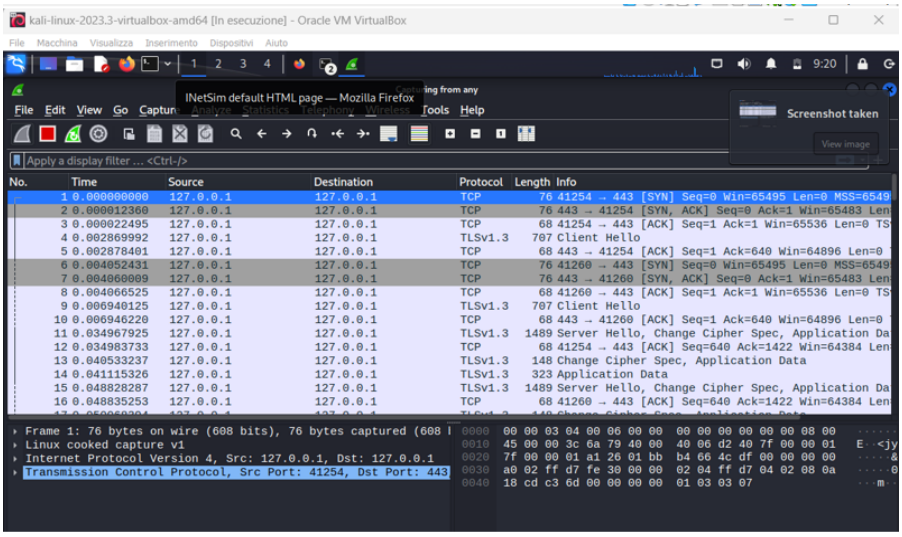
Successivamente testo la rete con l'indirizzo https://localhost/ e mi restituisce una pagina fake HTML. Verifico, poi, il traffico dei pacchetto su wireshark. Posso notare che vengono intercettati pacchetti con richiesta GET su porta 443.

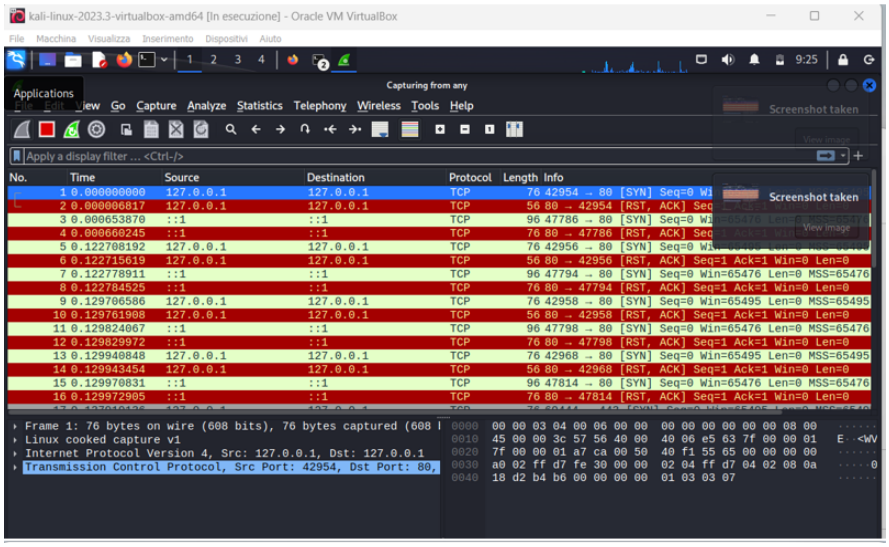
Su inetsim attivo anche il servizio HTTP per un ulteriore prova e posso vedere che vengono intercettati i pacchetti con richiesta GET su porta 80.



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

This file is an HTML document.

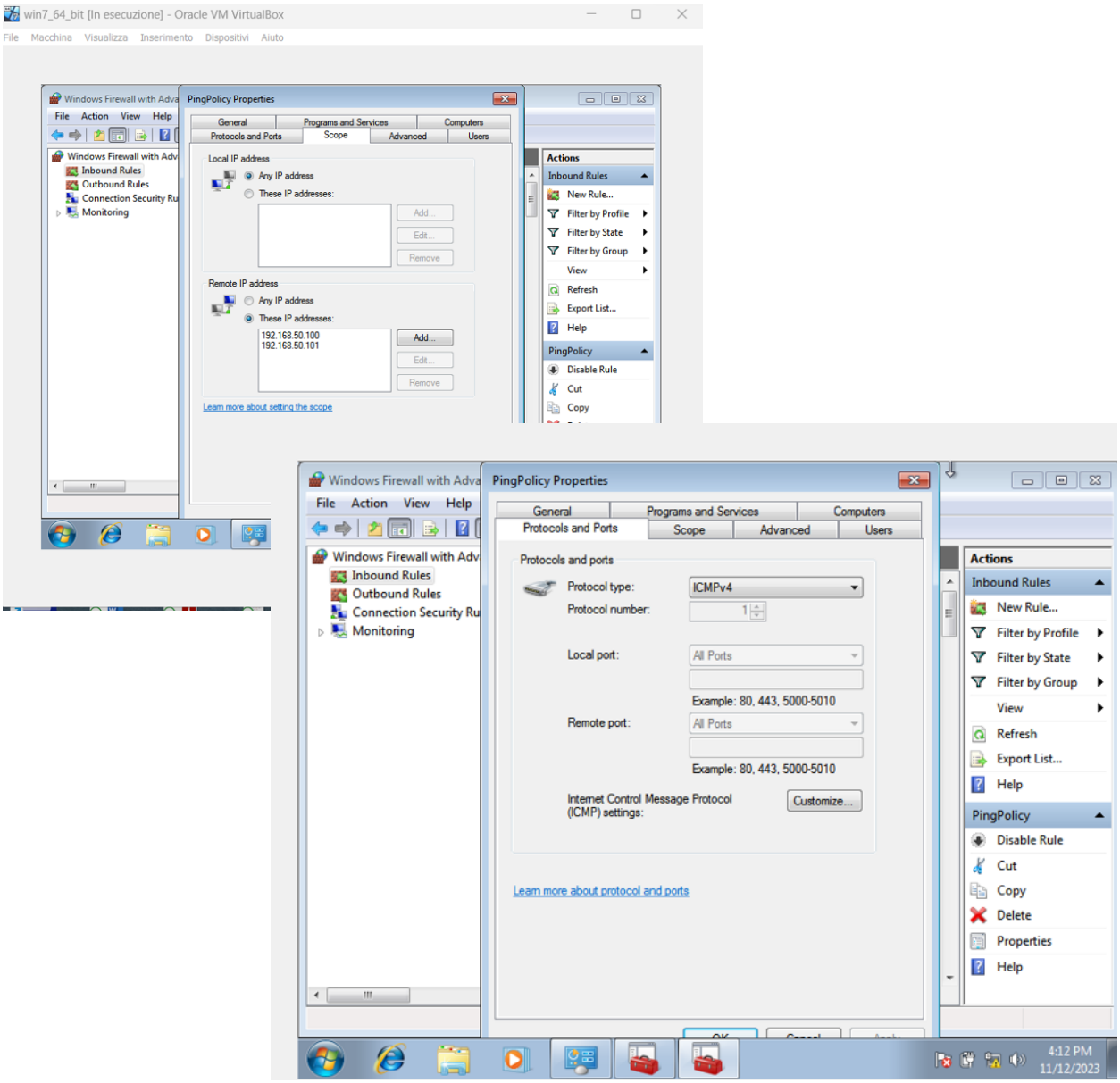




2. Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio virtuale (windows firewall)

Sul mio laboratorio virtuale avvio la macchina Window 7. Vado nelle configurazioni del Firewall e creo una nuova regola d'ingresso (INBOUND RULES). Imposto lo "scope": Local IP address (Win7) su any IP. Per remote IP address, imposto gli IP di Metasploitable e Kali.

In "protocols and ports" imposto il protocollo ICMPv4 per permettere il ping tra le macchine della nostra rete interna.



Verifico, infine, il ping dalla macchina Kali verso Win 7.