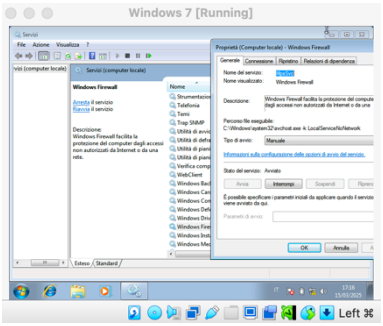
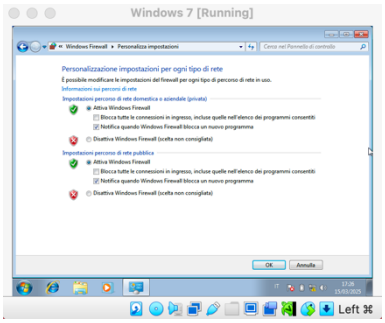
POLICY & PACKET CAPTURE W3D4

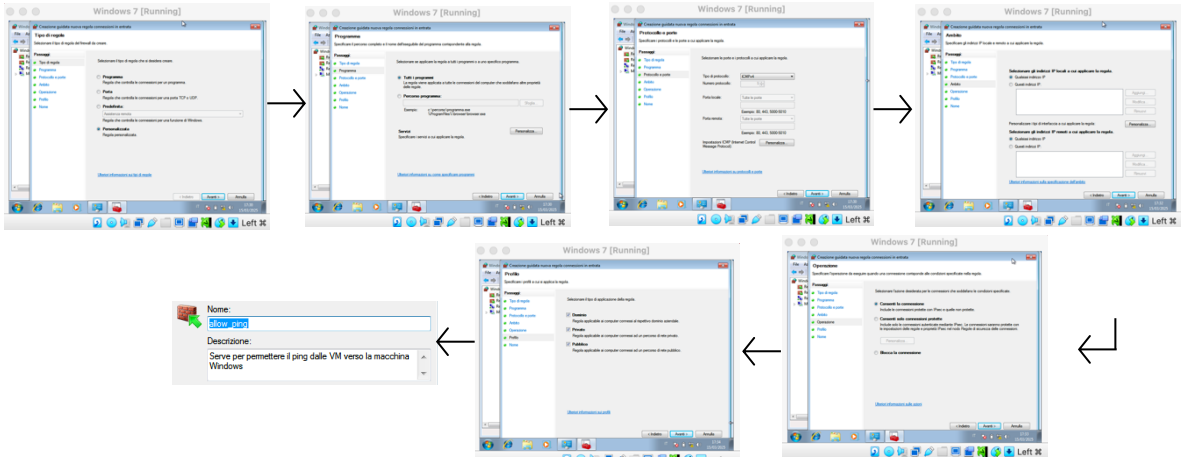
1. Configuro una policy sul Firewall Windows, per permettere il ping dalla VM Kali Linux alla VM Windows:
   Accendo la macchina virtuale Windows → cerco Servizi → cerco Windows Firewall → lo imposto Manuale → Applica → Avvia



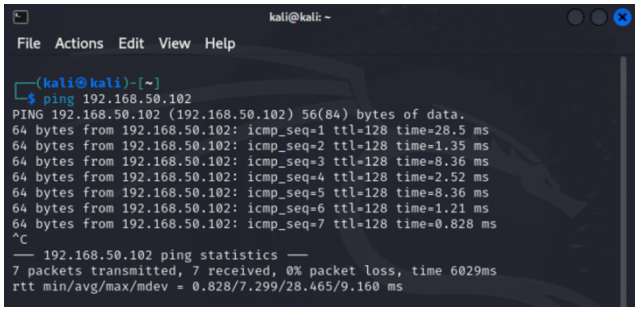
   Vado su Pannello di controllo → Tutti gli elementi del Pannello di controllo → Windows Firewall → modifica impostazioni di notifica



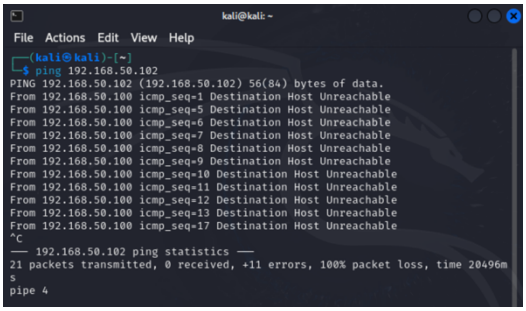
   Torno su Windows Firewall → impostazioni avanzate → regole connessioni in entrata → nuova regola → Personalizzata → Avanti → tutti i programmi → Avanti → tipo di protocollo: ICMPv4 → Avanti → qualsiasi indirizzo IP (ad entrambe le selezioni) → Avanti → consenti la connessione → Avanti → seleziono tutti i profili → Avanti → inserisco un nome e una descrizione (come in figura) → Fine



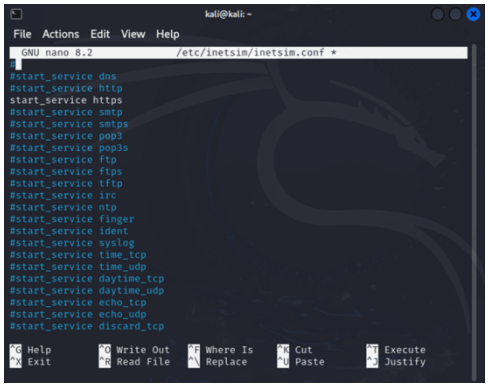
   Mando la richiesta di ping dalla macchina virtuale Kali:



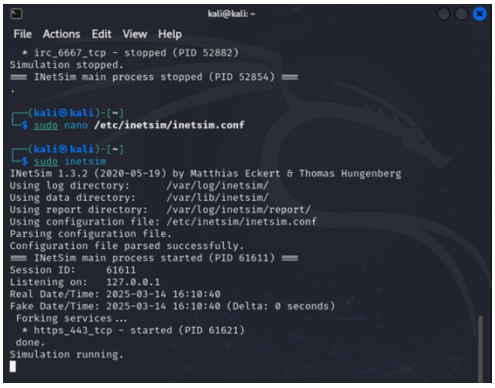
Senza questa configurazione il ping non funzionerebbe:



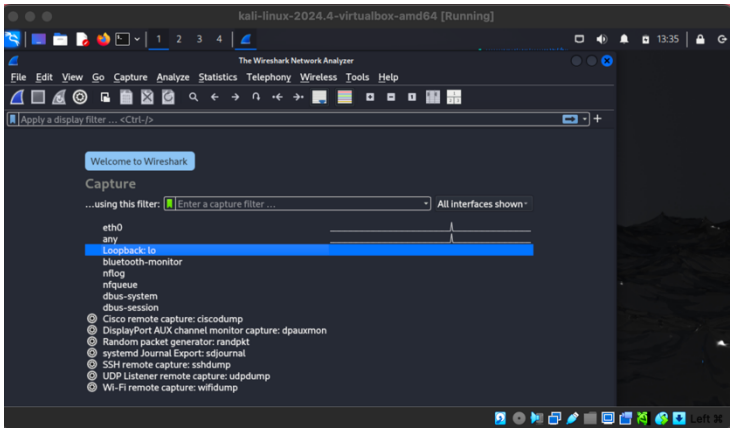
2. Configuro InetSim tramite la VM Kali:
   Apro il terminale → do il comando “sudo nano /etc/inetsim/inetsim.conf” → metto “#” davanti a tutti i servizi, tranne https → salvo ed esco



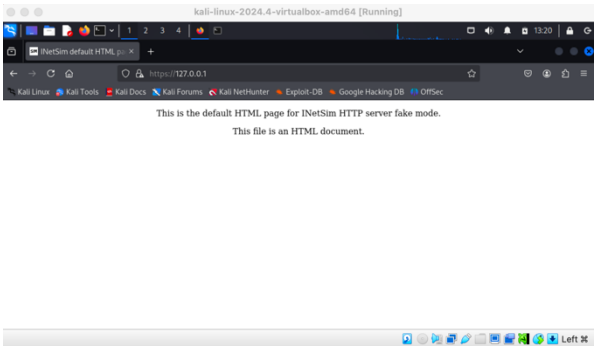
Do il comando “sudo inetsim”



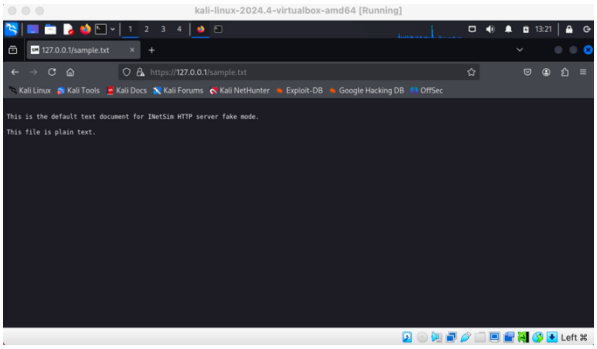
3. Configuro una packet capture con Wireshark:
   Apro l’app Wiresherk sulla VM Kali → clicco su Loopback



Apro Firefox e cerco “https://127.0.0.1”



Cerco anche “https://127.0.0.1/sample.txt”



Su Wireshark monitoro il traffico di rete per verificare i pacchetti inviati e ricevuti