

Obiettivo:

Configurazione del firewall su Windows per permettere il ping da Kali Linux.

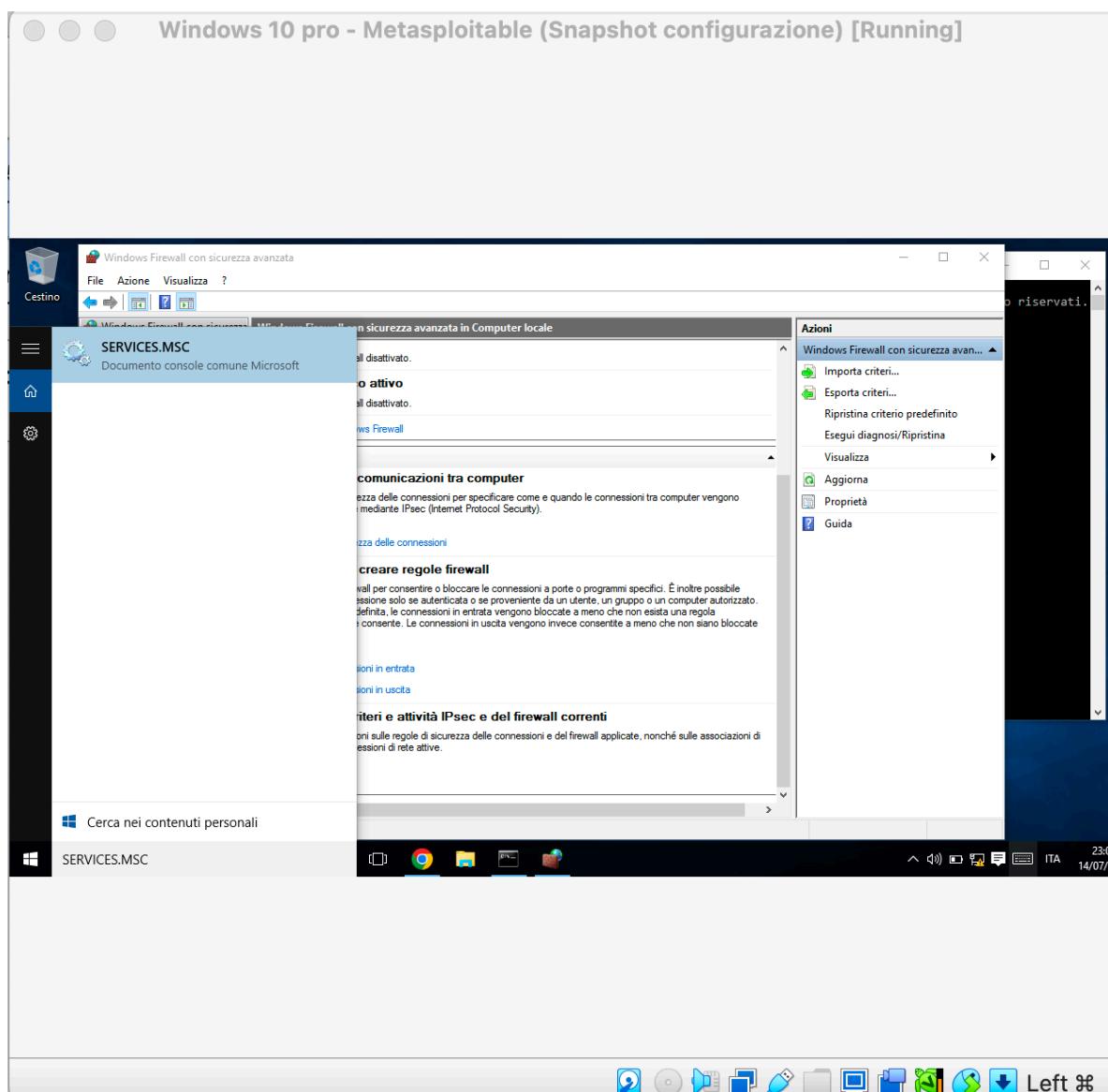
Avvio e configurazione di InetSim su Kali Linux per simulare servizi HTTPS.

Cattura e analisi dei pacchetti di rete con Wireshark.

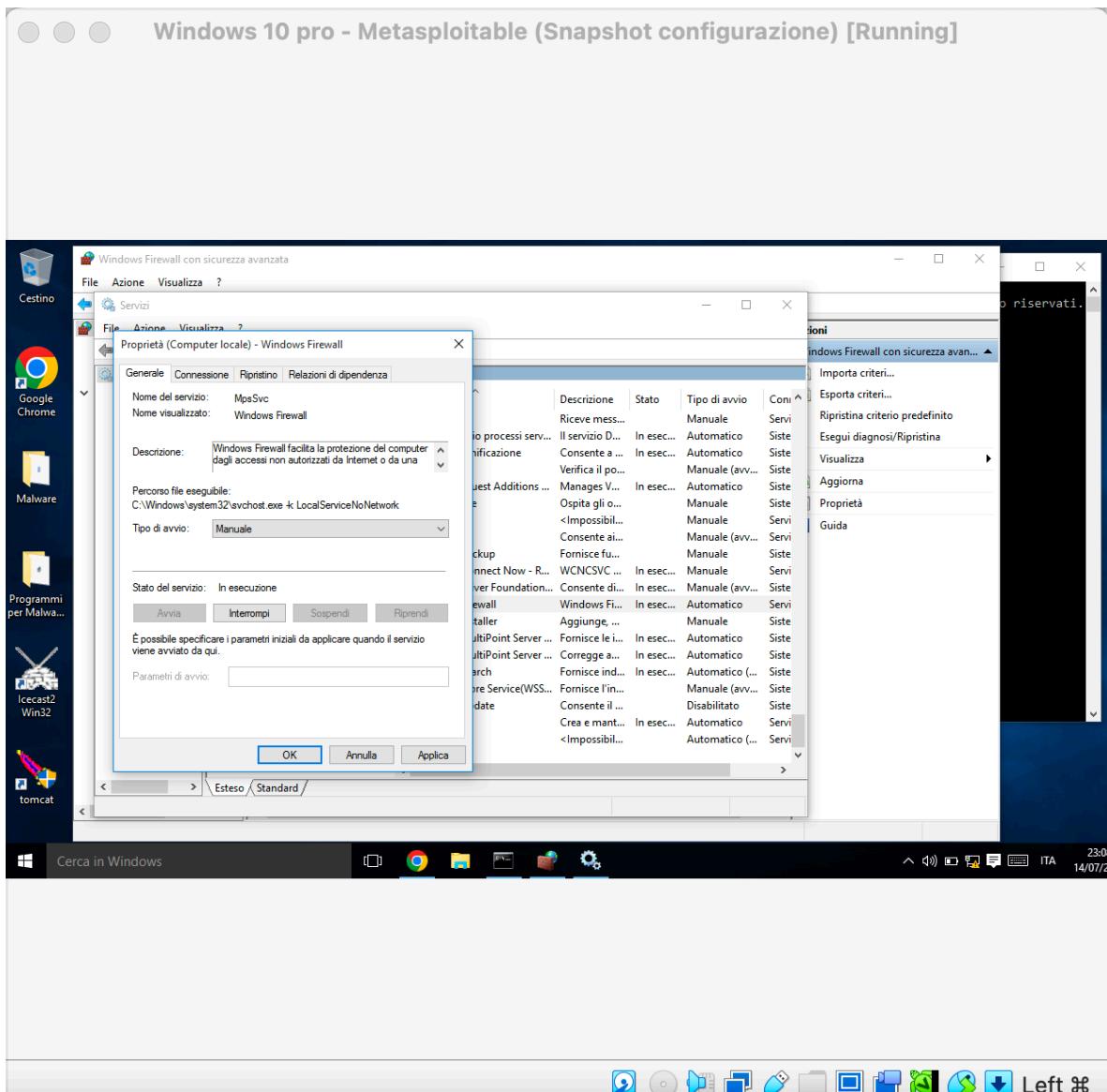
Configurazione del firewall su Windows

Per prima cosa ho verificato che le macchine virtuali fossero correttamente configurate in rete. Ho eseguito un ping dalla macchina Kali Linux verso l'indirizzo IP della macchina Windows (192.168.50.102). Come previsto, tutti i pacchetti risultavano persi, a causa del firewall Windows che blocca di default le richieste ICMP in ingresso.

Sono quindi passato sulla macchina Windows e ho aperto le impostazioni del firewall cercando "Windows Firewall" nel menu Start.



Ho impostato **Tipo di avvio: Manuale → Applica**.

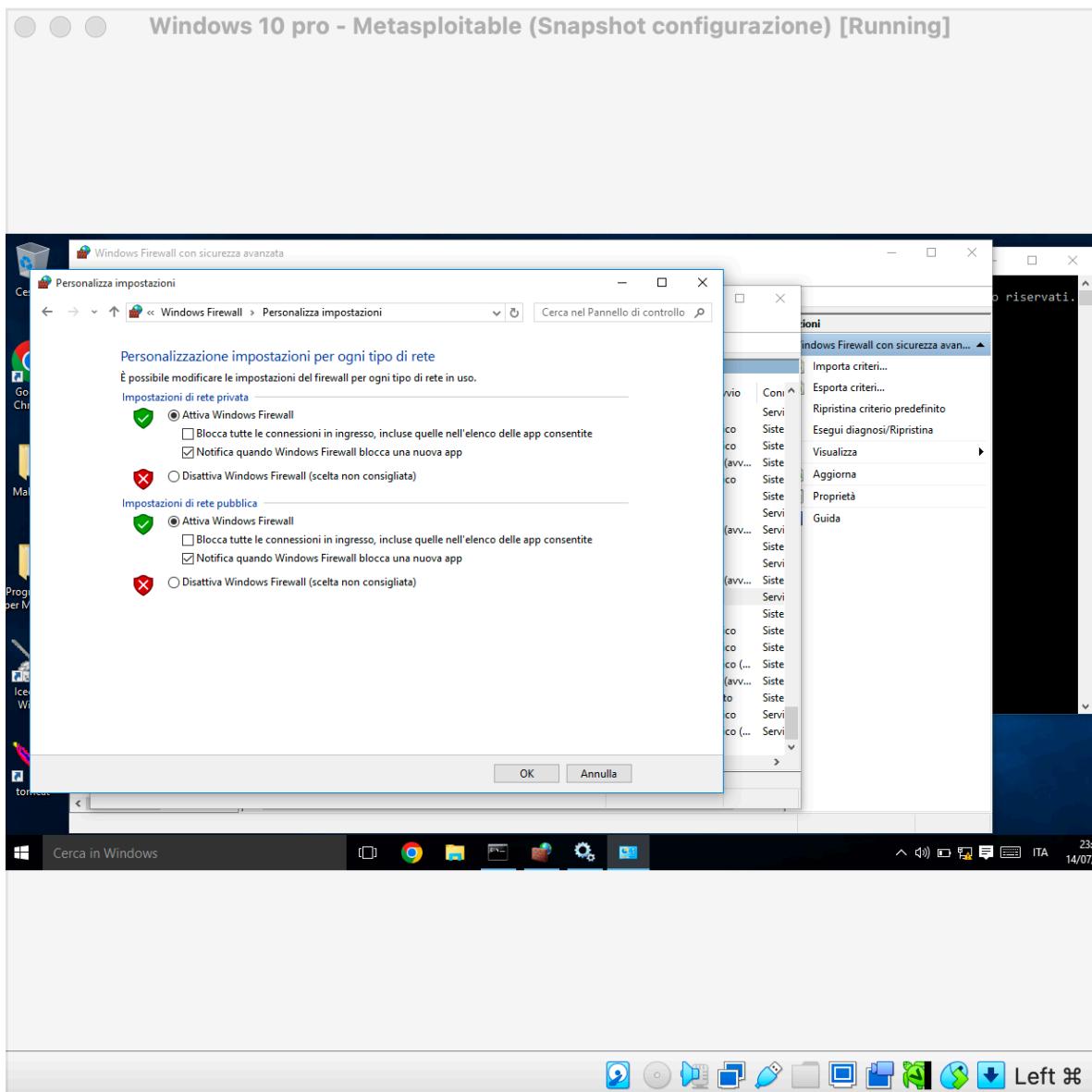


Ho, poi, avviato il servizio.

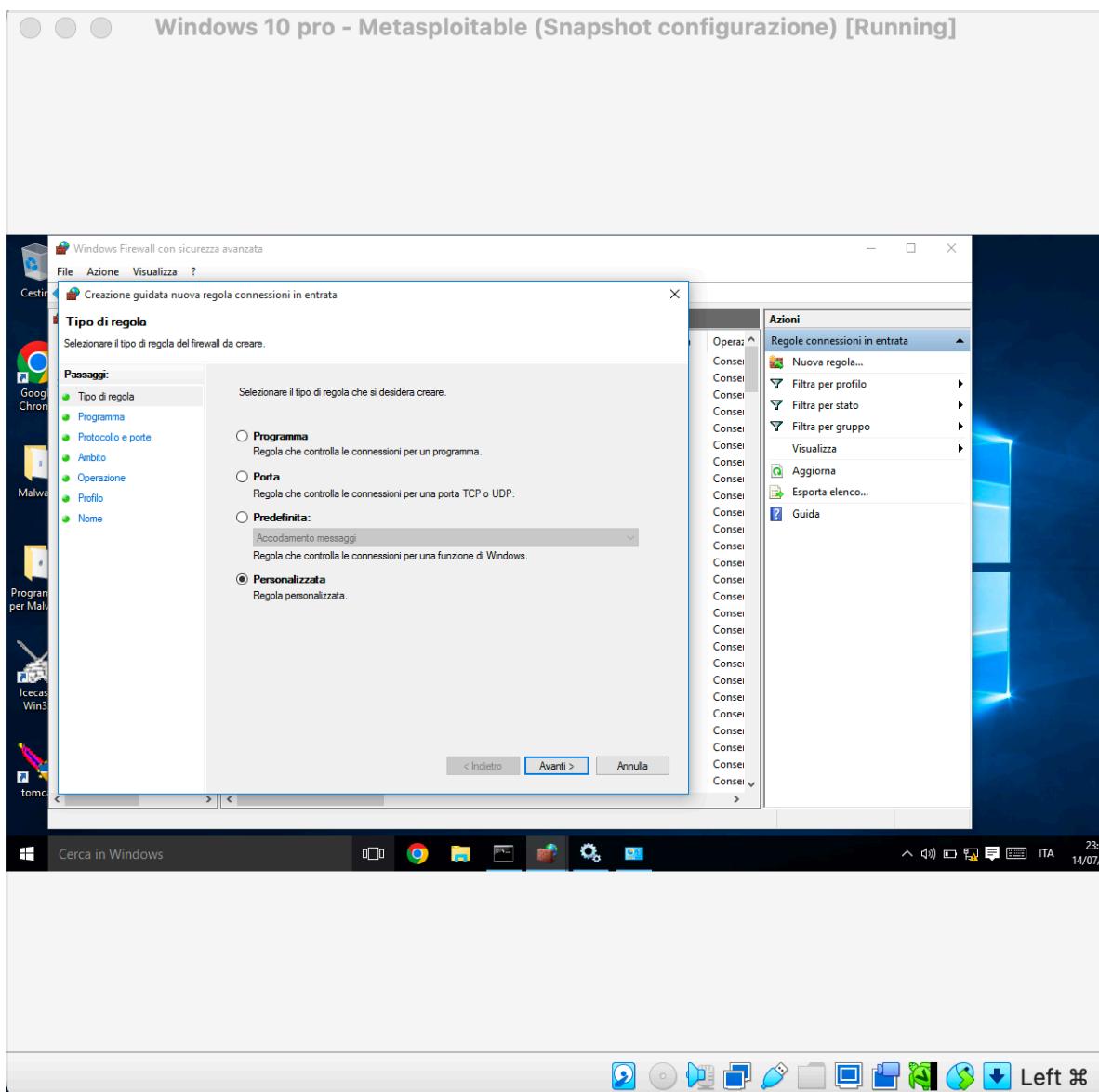
Come ultimo passo ho verificato che il firewall fosse abilitato anche da:

Pannello di controllo → Tutti gli elementi → Windows Firewall →

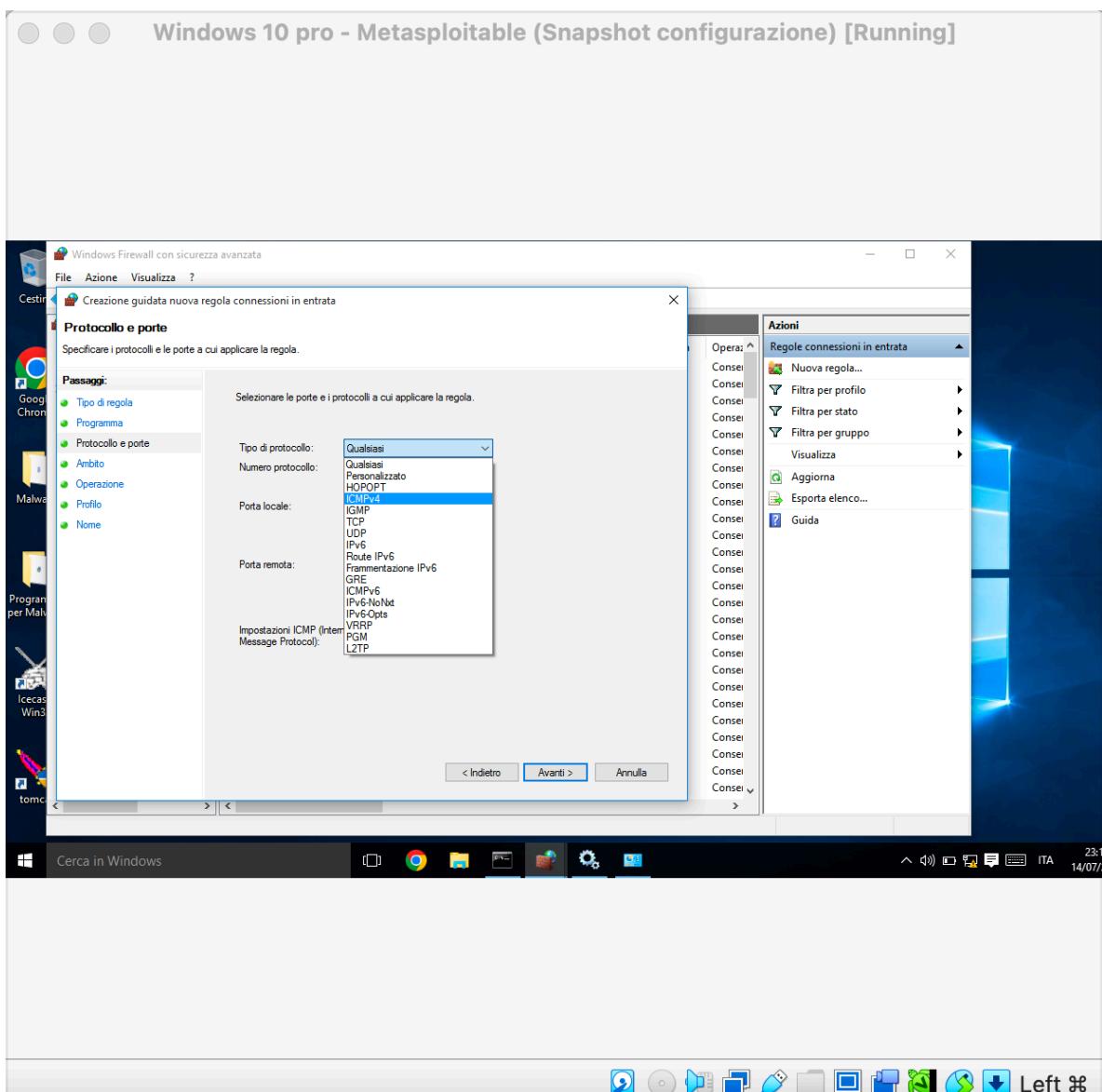
Personalizza impostazioni → Attiva.



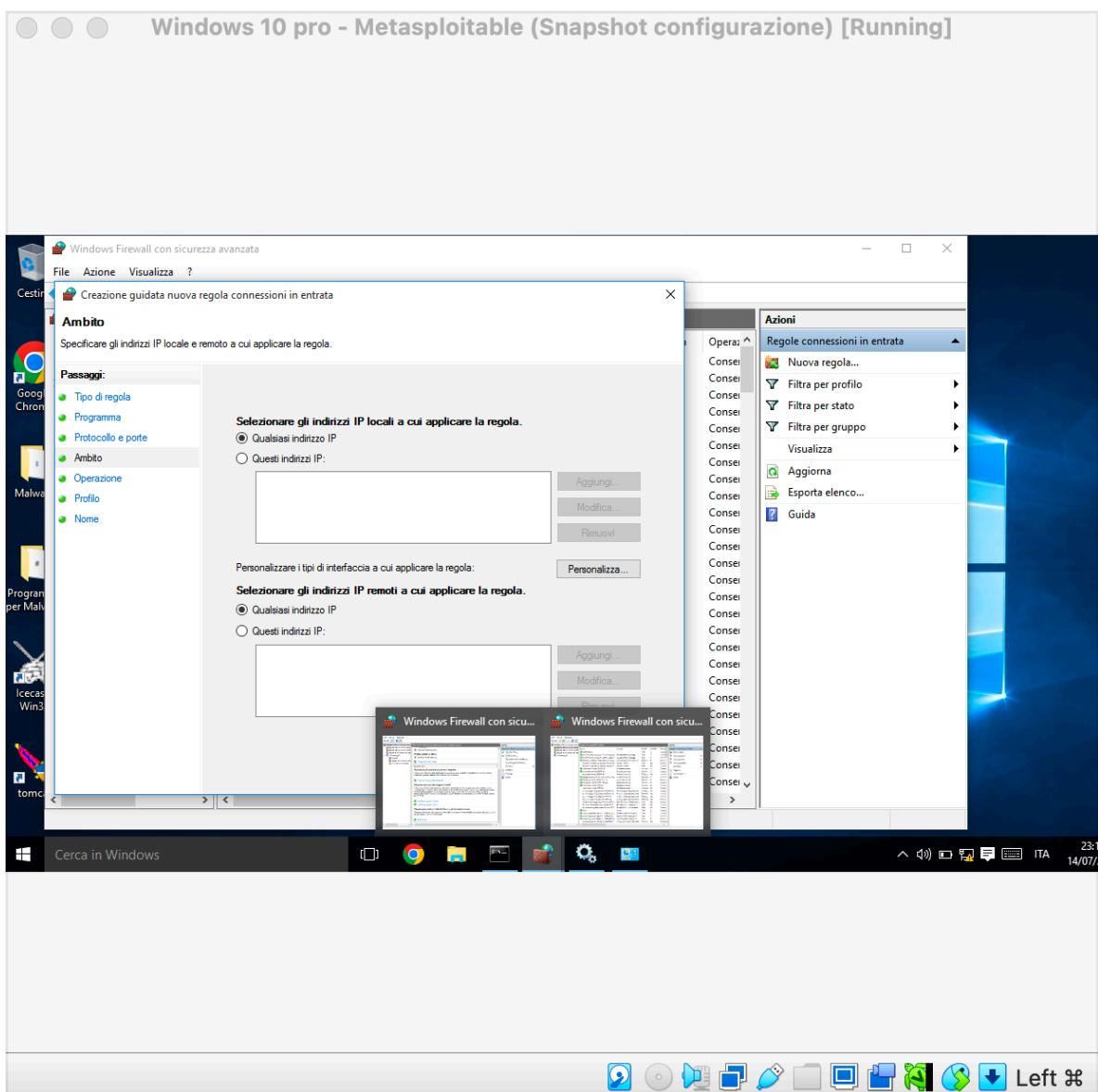
Dopo aver verificato che il servizio firewall fosse attivo e avviato (tramite la sezione Servizi), ho aperto la sezione "Inbound Rules" e creato una nuova regola personalizzata per abilitare il traffico ICMP (ping) proveniente da qualsiasi indirizzo IP.



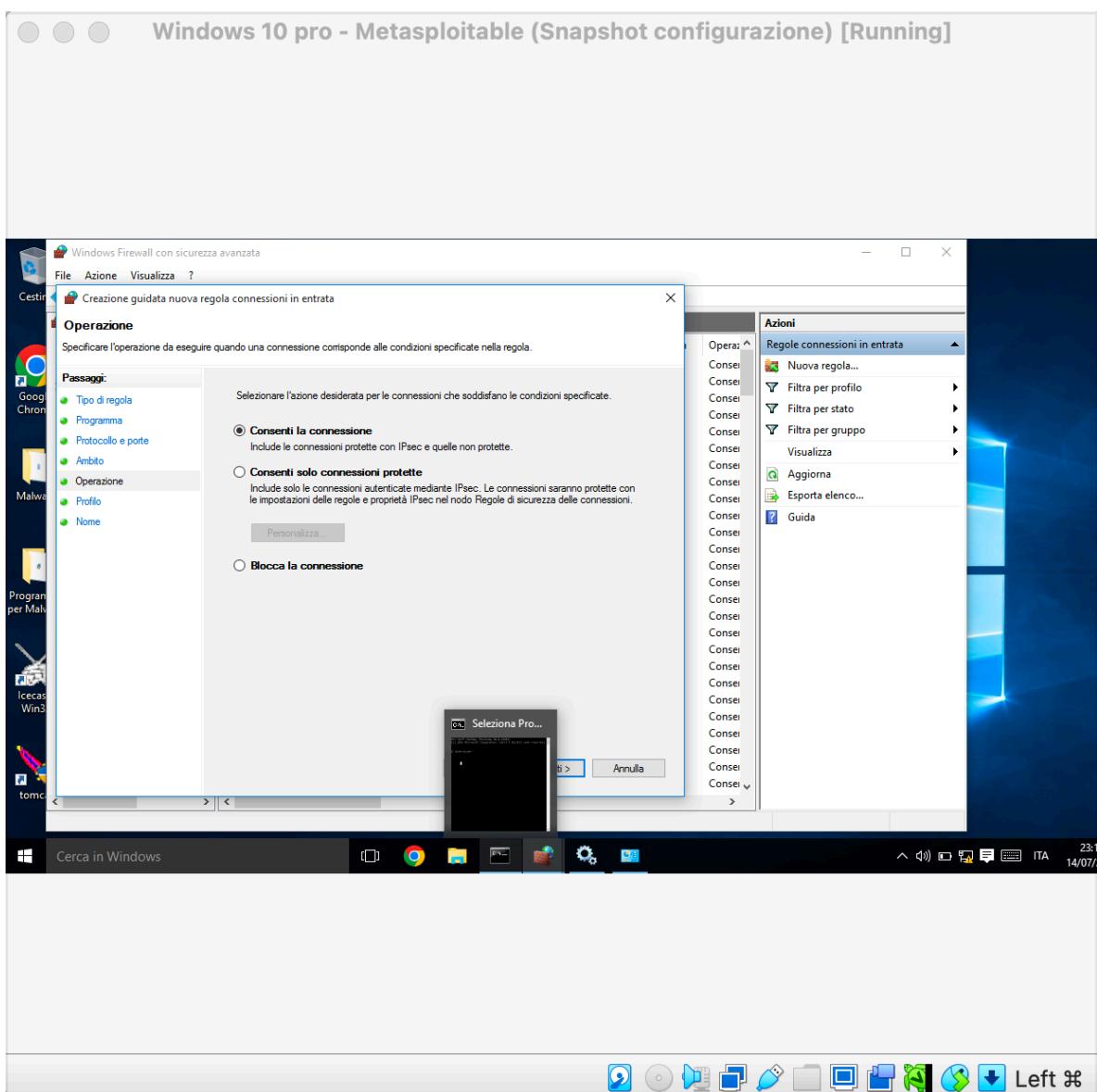
Protocollo: **ICMPv4** → Avanti



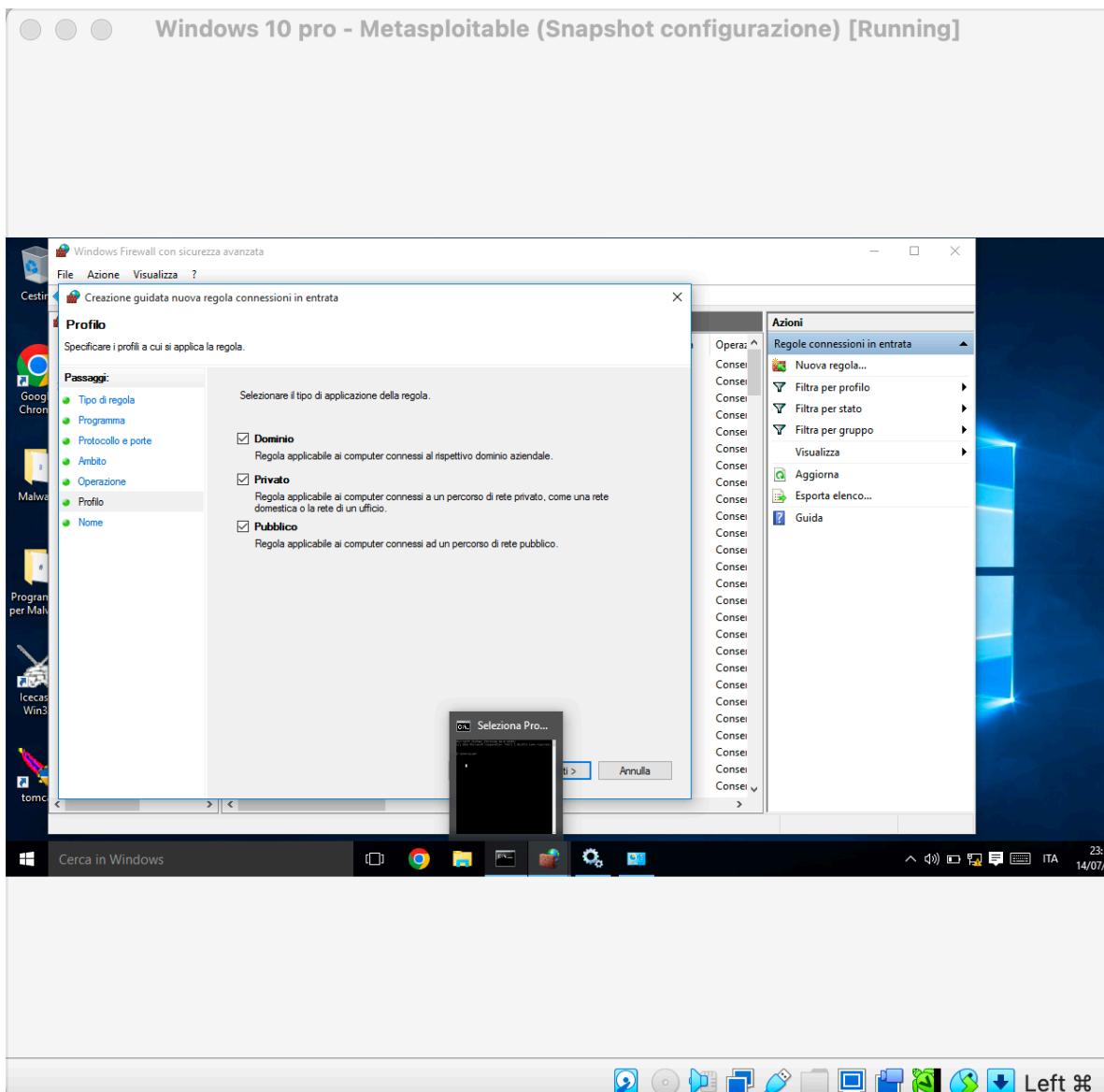
Ambito: **Qualsiasi indirizzo IP** → Avanti



Azione: **Consenti la connessione** → Avanti

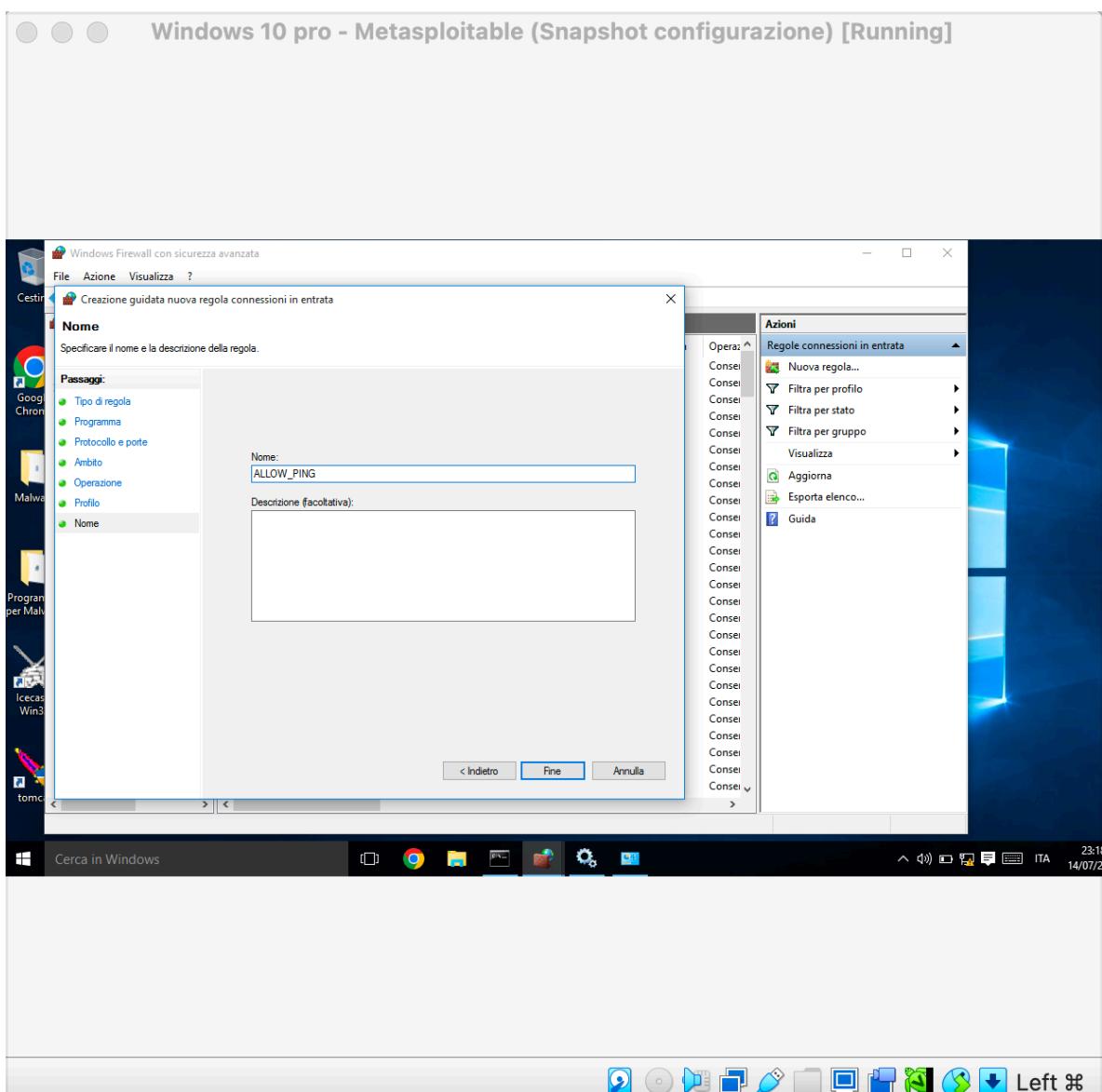


Profili: Dominio, Privato, Pubblico → Avanti

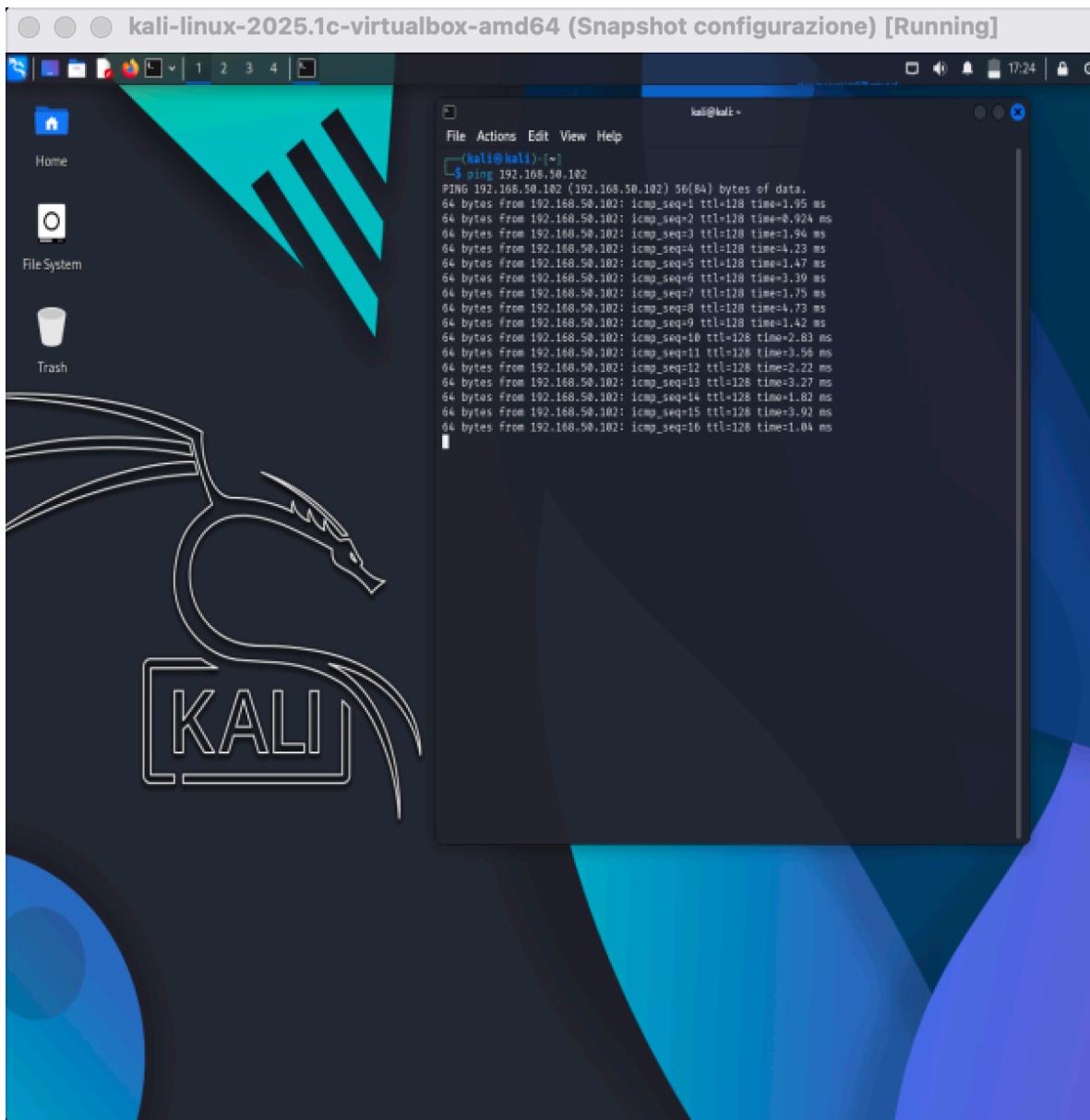


La regola è stata chiamata `allow_ping` ed è stata applicata a tutti i profili di rete (dominio, privato e pubblico).

Ho salvato la configurazione e verificato che la regola fosse attiva.

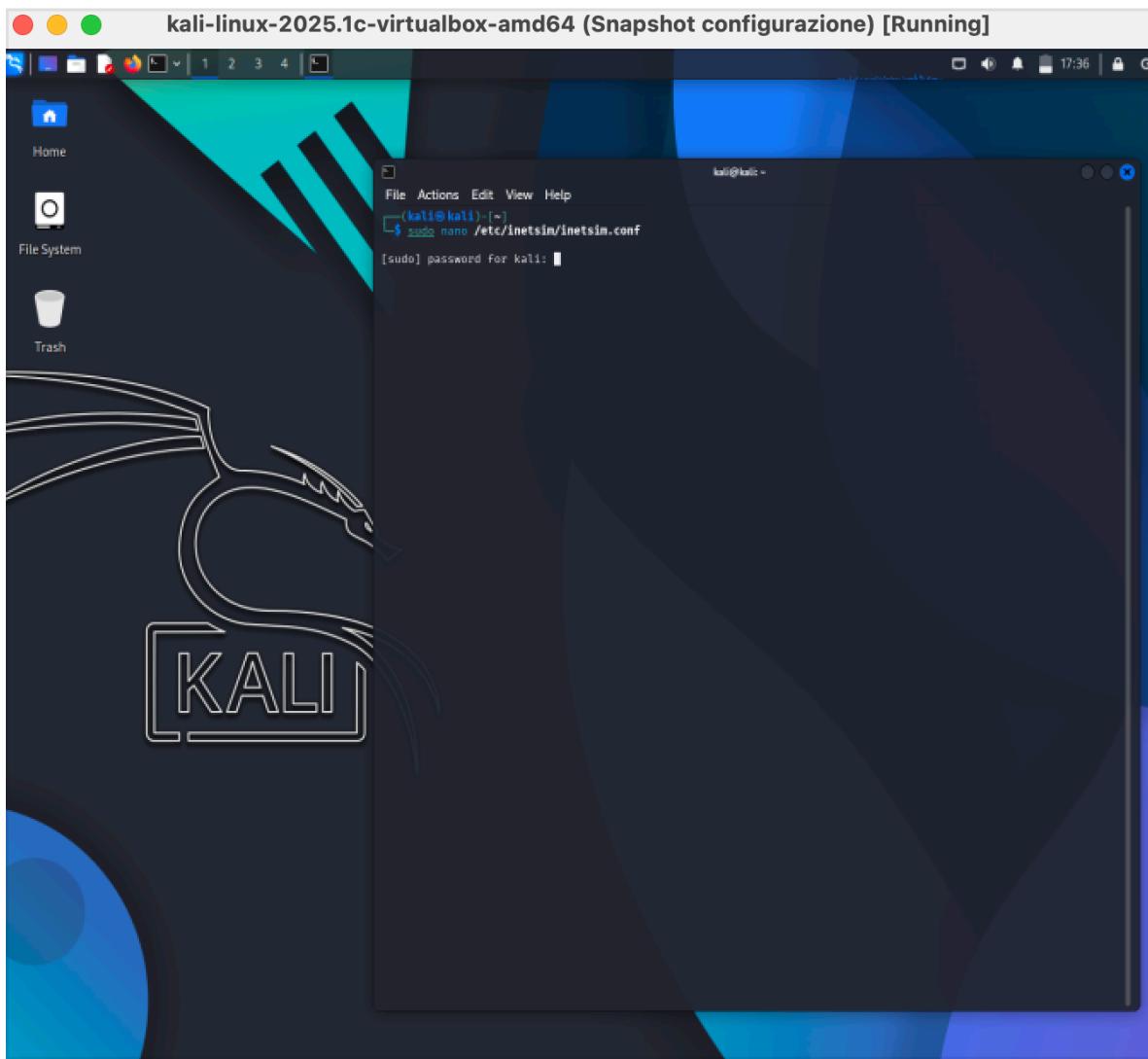


Infine, sono tornata sulla macchina Kali Linux ed eseguendo nuovamente il ping verso l'IP Windows, ho confermato che la comunicazione ora funzionava correttamente, ricevendo le risposte ICMP.

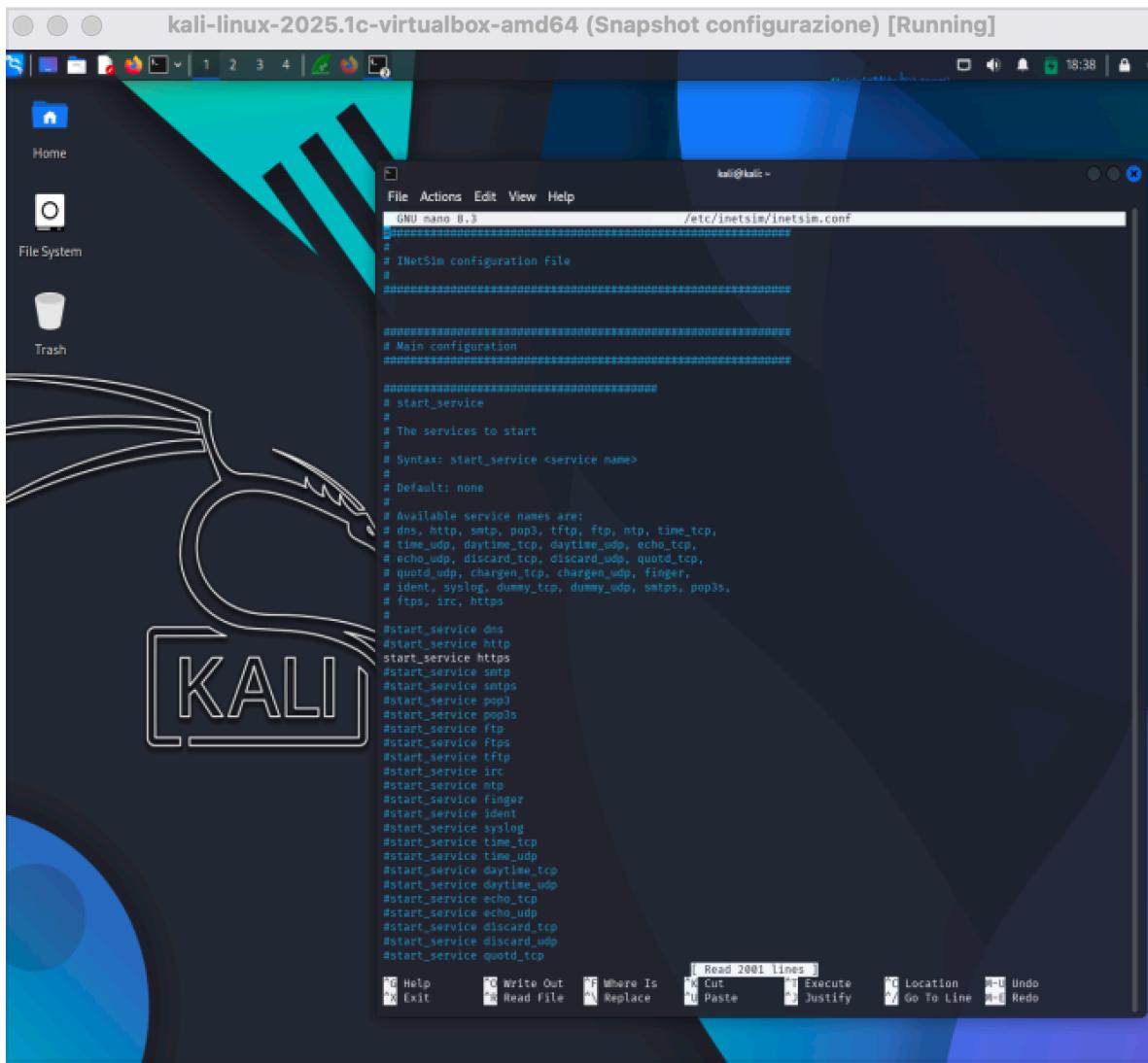


Seconda parte: simulazione dei servizi con InetSim

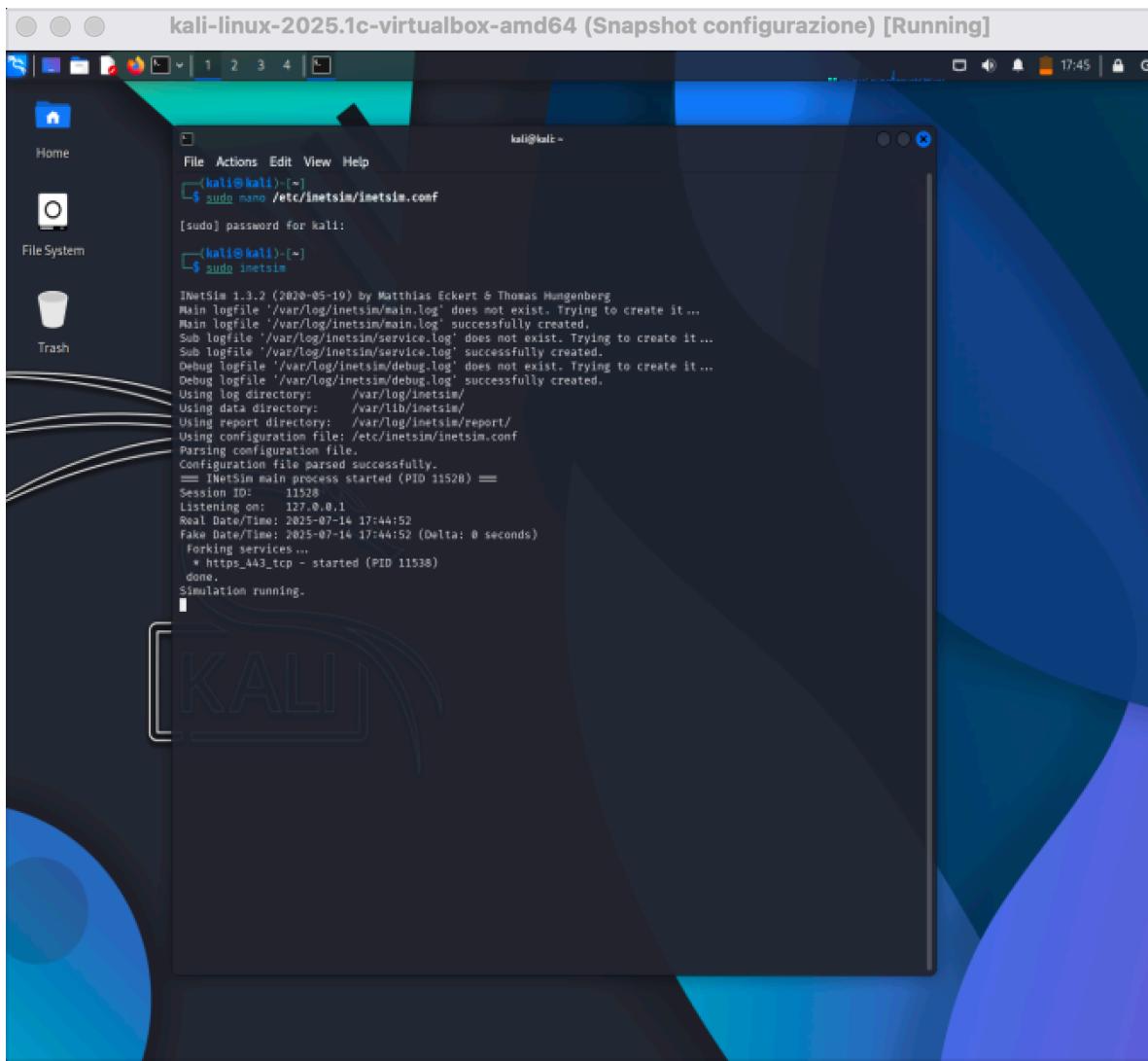
Successivamente, ho avviato un terminale su Kali Linux e aperto il file di configurazione di InetSim, situato in "sudo nano /etc/inetsim/inetsim.conf" , inserito la password di default kali e invio



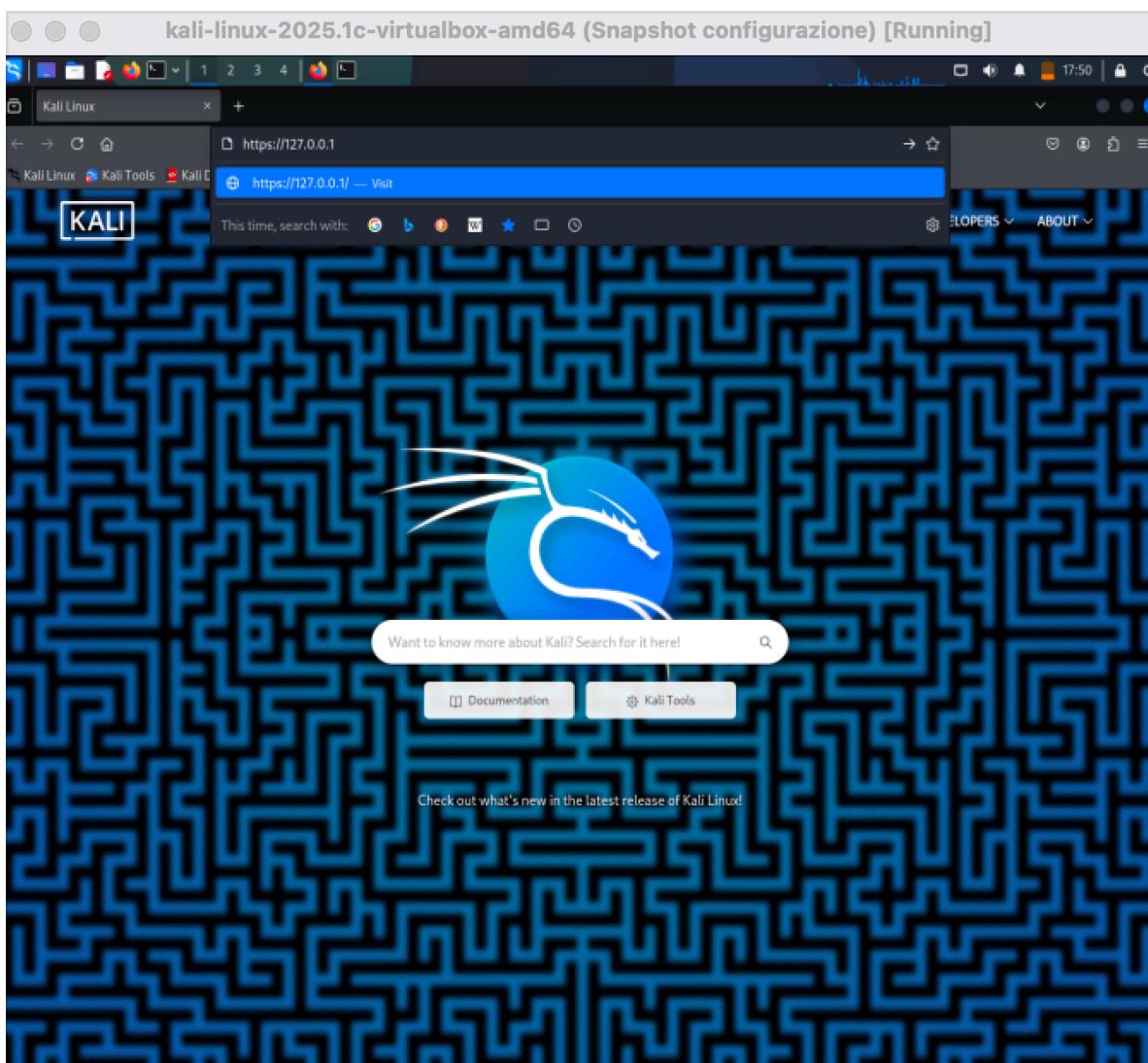
Ho modificato la configurazione commentando tutti i servizi predefiniti
(inserendo # davanti a ognuno) tranne HTTPS, lasciando questo come unico
servizio attivo.

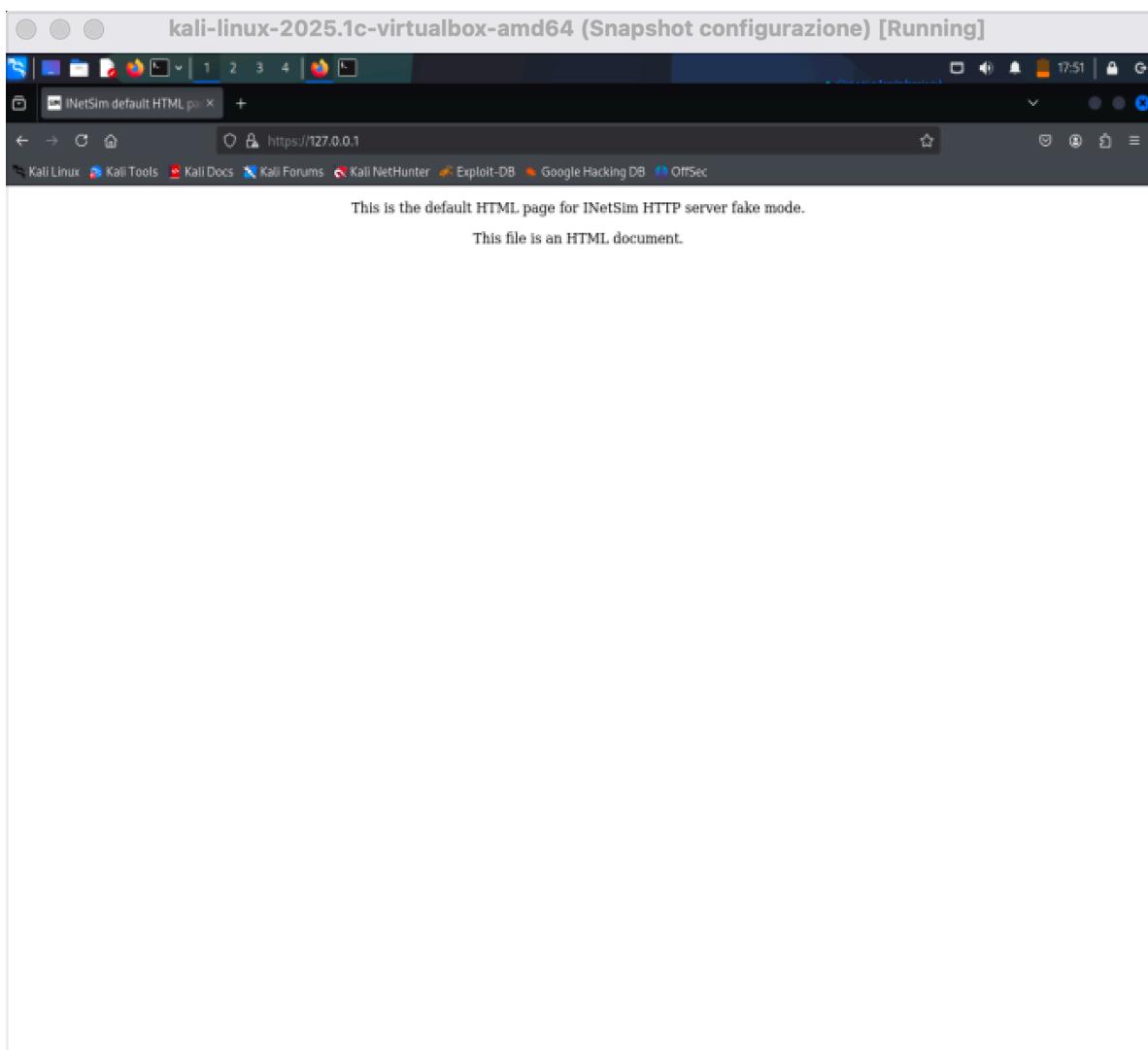


Ho salvato le modifiche e avviato InetSim con il comando "sudo inetsim"

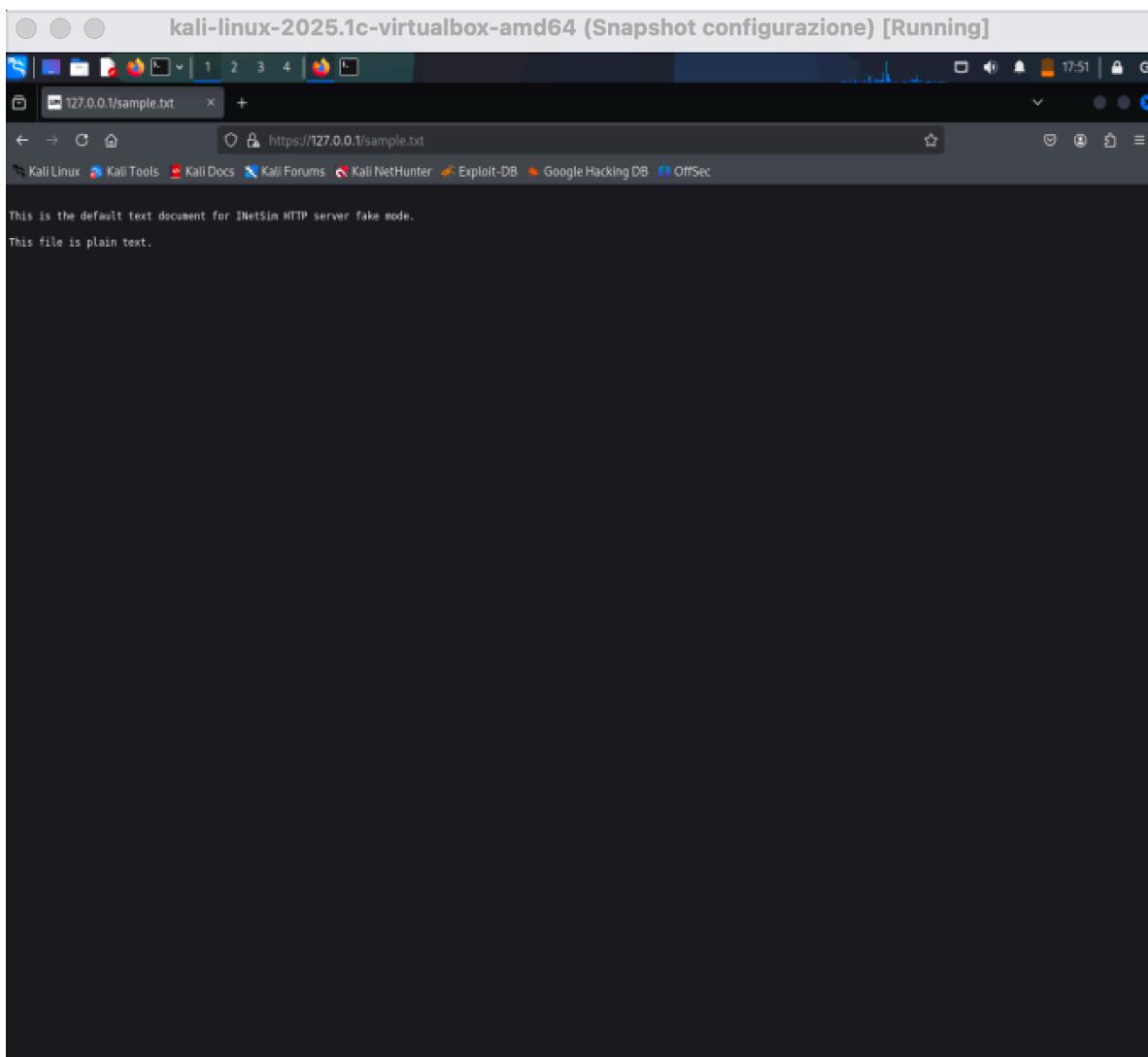


Dal browser della macchina Kali Linux mi sono connessa all'indirizzo "<https://127.0.0.1>" accettando il warning di sicurezza. Ho verificato la pagina iniziale fittizia fornita da InetSim.



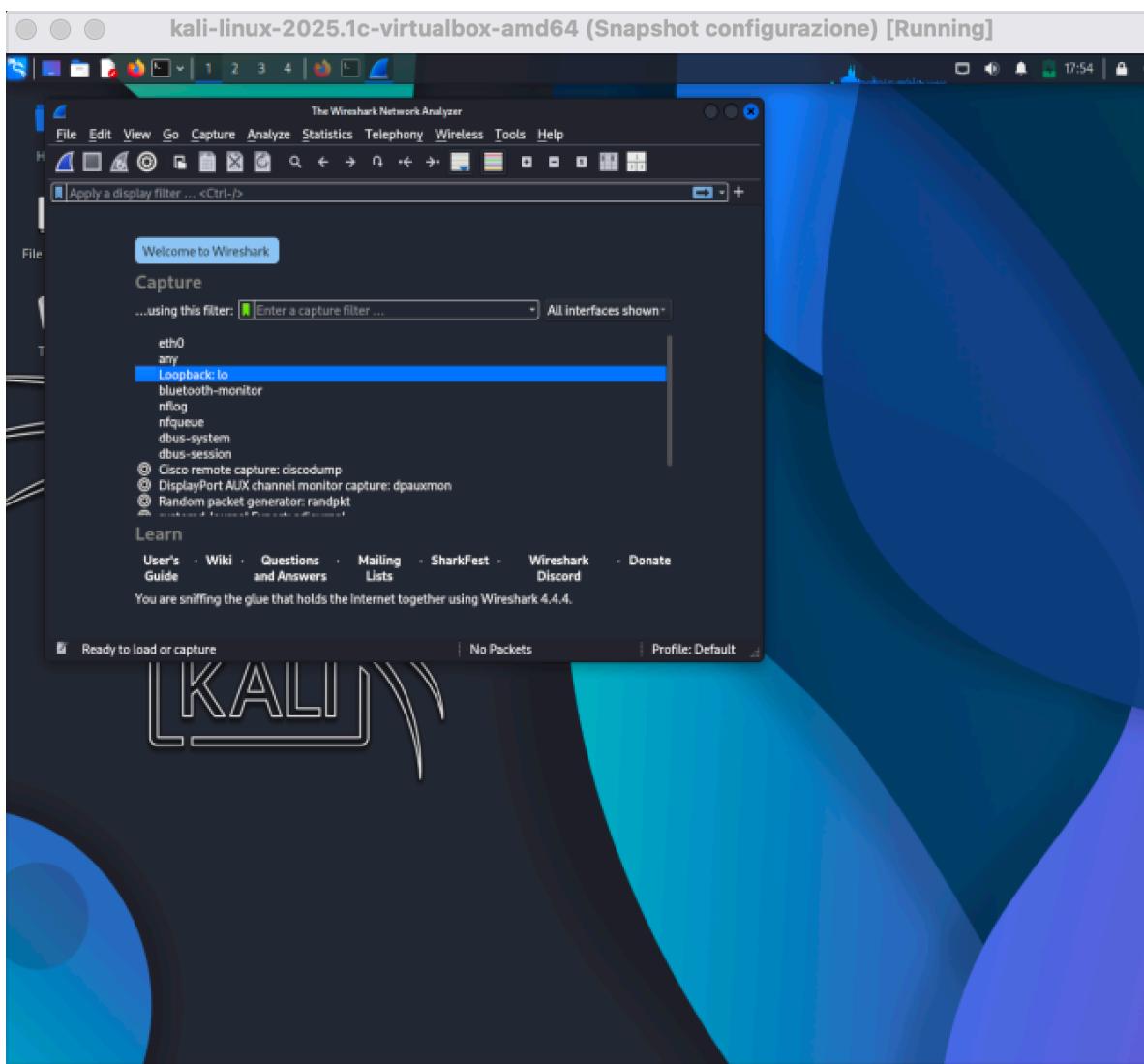


Inoltre, richiedendo "<https://127.0.0.1/sample.txt>" ho potuto scaricare un file fittizio, confermando che il servizio HTTPS simulato era attivo e funzionante.

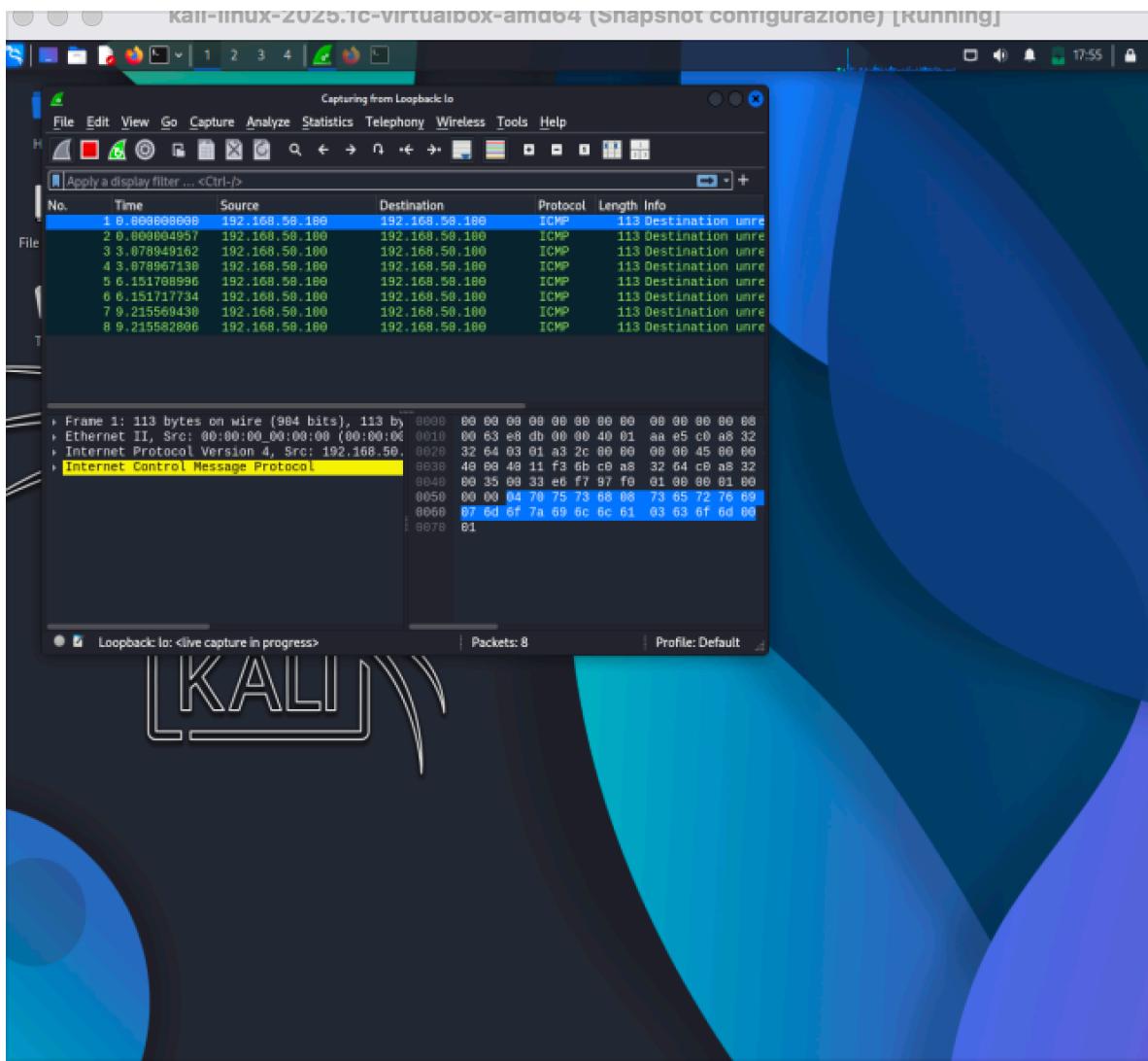


Terza parte: cattura e analisi dei pacchetti con Wireshark

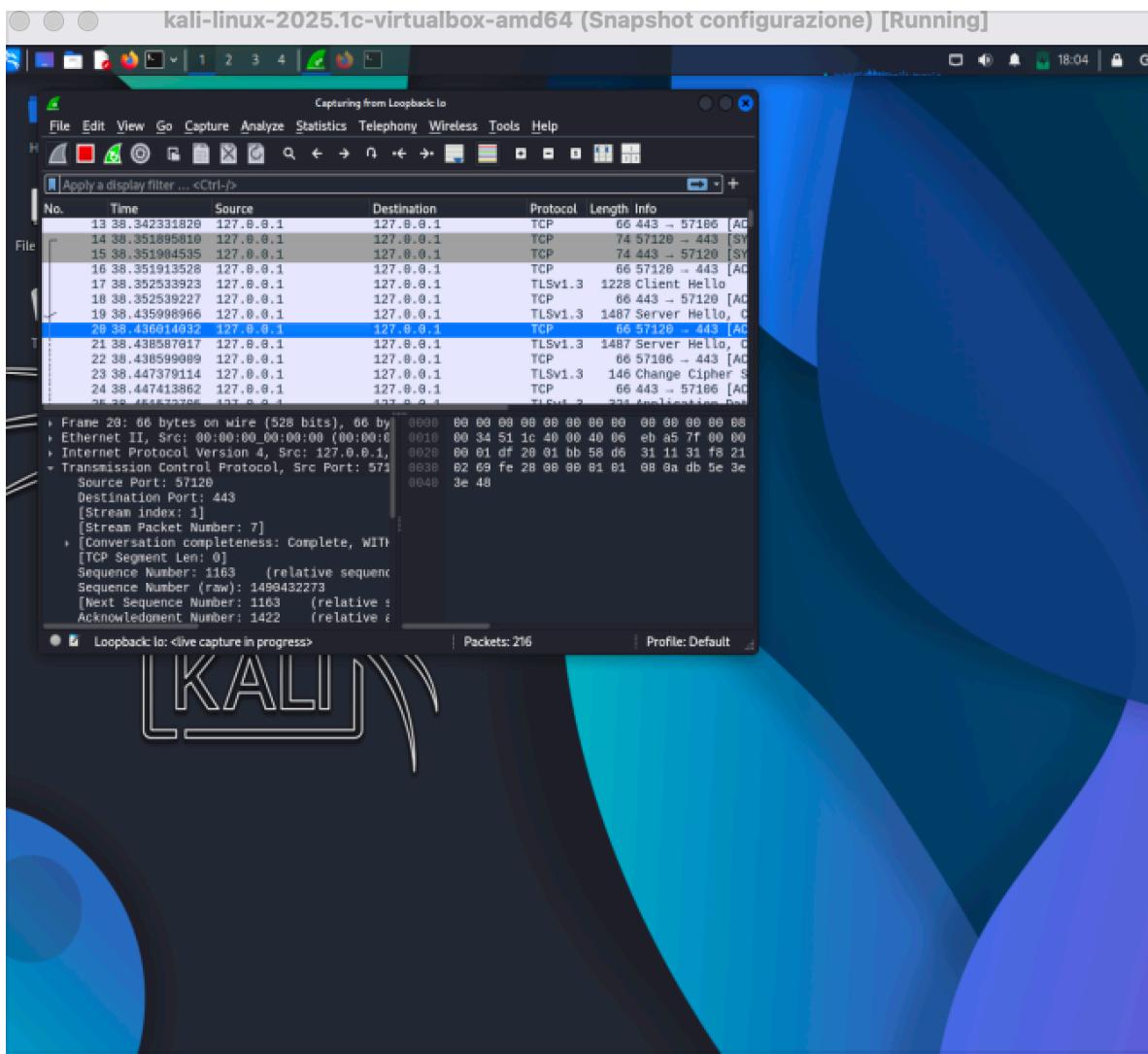
Infine, ho avviato Wireshark sulla macchina Kali Linux, impostandolo in ascolto sull'interfaccia di loopback.



Wireshark ha cominciato a catturare il traffico.



Analizzando i pacchetti, ho potuto osservare il corretto avvio della sessione TCP (3-way handshake con pacchetti SYN, SYN+ACK, ACK) e lo scambio dei dati HTTP/HTTPS tra client e server. Nel pannello di dettaglio di Wireshark, ho verificato le informazioni sui pacchetti ai vari livelli TCP/IP.



Parte Facoltativa