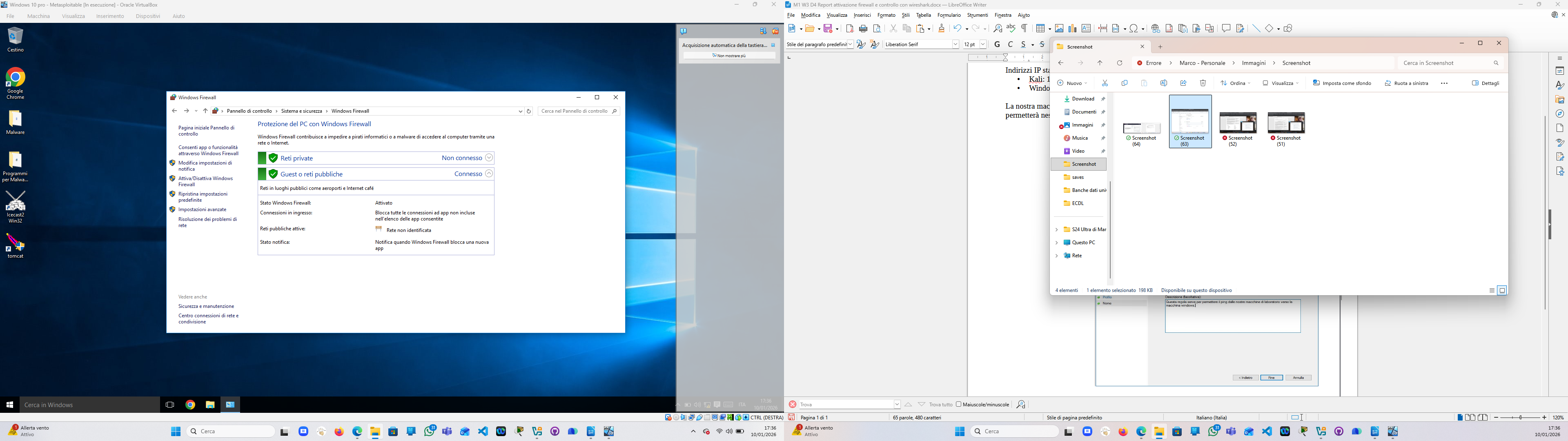
**ATTIVAZIONE FIREWALL SULLA MACCHINA VIRTUALE WINDOWS E RISULTATI**

Con questa attività sulla macchina virtuale windows andremo ad attivare il \*firewall e vedremo come farlo funzionare correttamente per ricevere o inviareun \*ping dalla macchina virtuale kali.

Indirizzi IP statici:

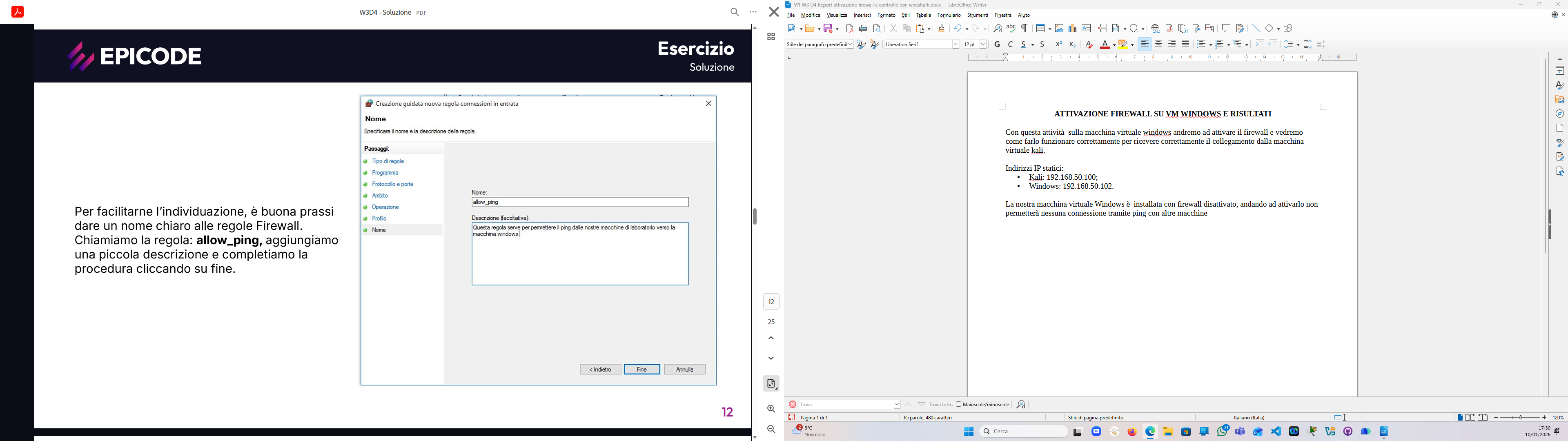
* Kali: 192.168.50.100;
* Windows: 192.168.50.102.

La nostra macchina virtuale Windows è installata con il firewall disattivato, andando ad attivarlo non permetterà nessuna connessione tramite ping con altre macchine.



**Nella Fig 1 vediamo che è stato attivato il firewall.**

Per permettere al firewall della \*VM di windows di gestire il flusso di dati, e nel nostro caso specifico il ping che riceverà dalla VM kali, andremo a creare una “Nuova regola” sul firewall.



**Nella Fig 2, dopo aver inserito i dati che servono al programma per gestire il flusso di dati secondo la nostra esigenza possiamo vedere il procedimento finale e la descrizione, in sintesi, della regola che abbiamo creato.**

Fig 2

Fig 1

Per controllare che tutto funzioni in modo corretto dalla Kali abbiamo inviato un ping e controllato il buon esito come descritto in Fig 3.

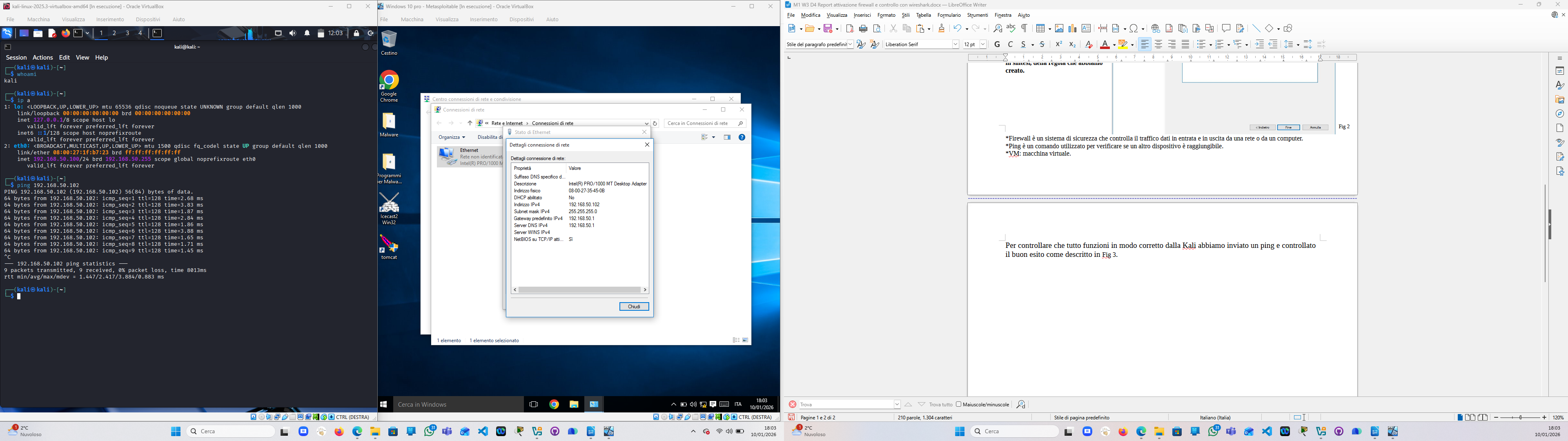
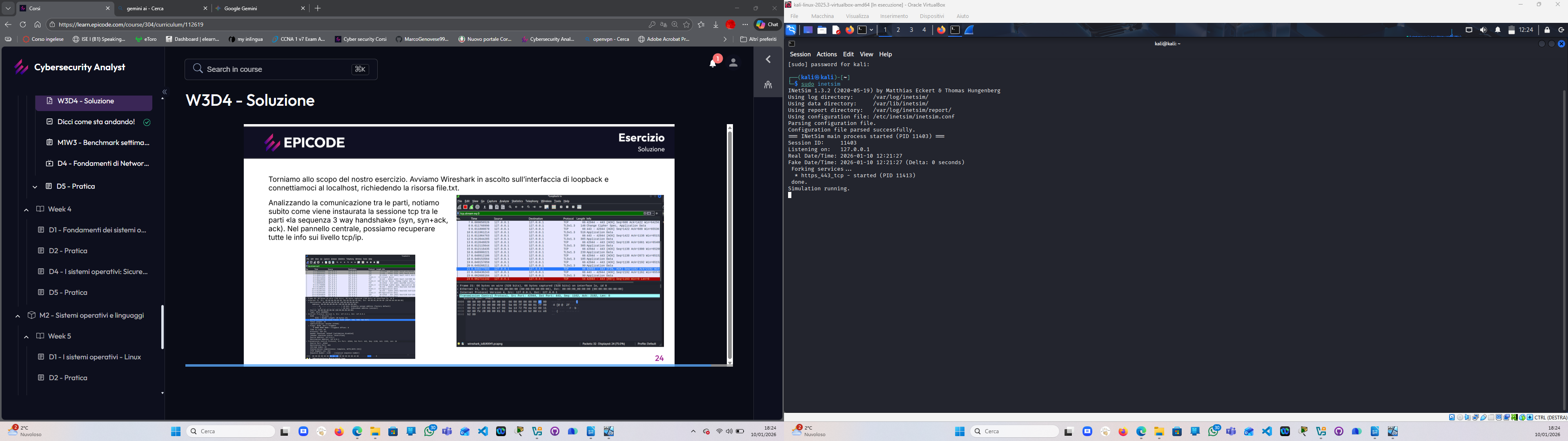
**In Fig 3 possiamo vedere che sulla VM di Kali sono stati chiesti i propri dati con il comando “ip a” che ci conferma il suo indirizzo IP, e successivamente con il comando “ping 192.168.50.102” abbiamo creato il collegamento con la macchina accanto Windows e che tutto funziona corettamente.**

Fig 3

**SIMULAZIONE DI UNA RETE REALE CON TOOL INETSIM E CATTURA DEI PACCHETTI**

Per questa attività utilizzeremo il tool pre-installato sulla Kali “inetsim” che è un simulatore di servizi internet come DNS, HTTP, HTTPs e altri.



**In Fig 4 vediamo l’inserimento del comando “sudo inetsim” che ci permette di avviare il tool specificato in precedenze (la configurazione del tool l’ abbiamo modificata prima di attivarlo per farlo funzionare solo sul protocollo HTTPs utilizzando il comando “sudo nano /etc/inetsim/inetsim.conf”).**

Fig 4

**Possiamo leggere in fondo “Simulation Running” ovvero il tool è partito correttamente.**

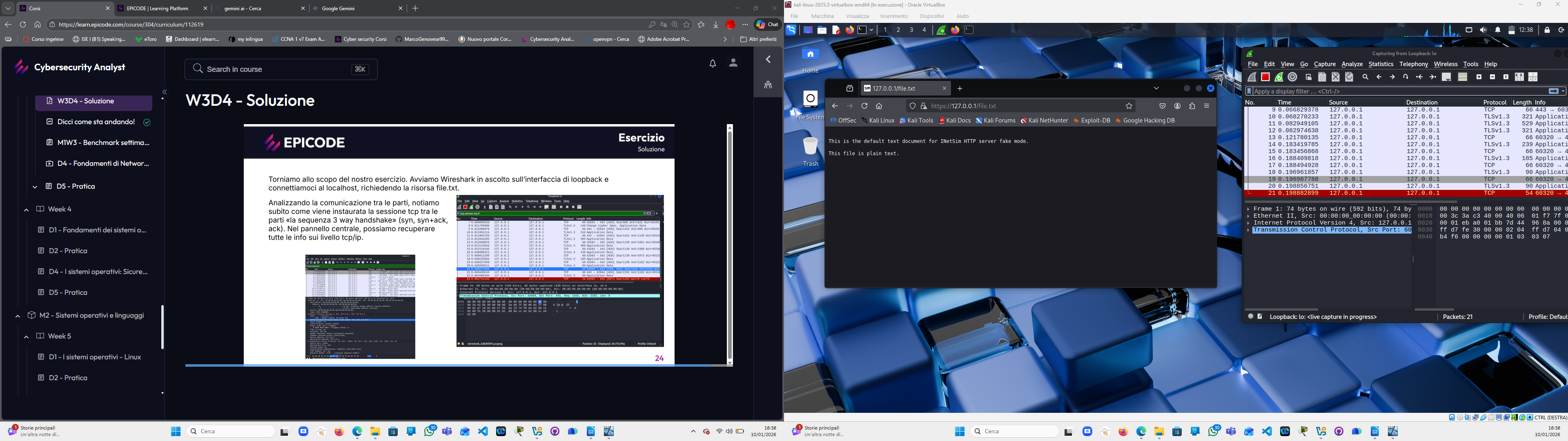
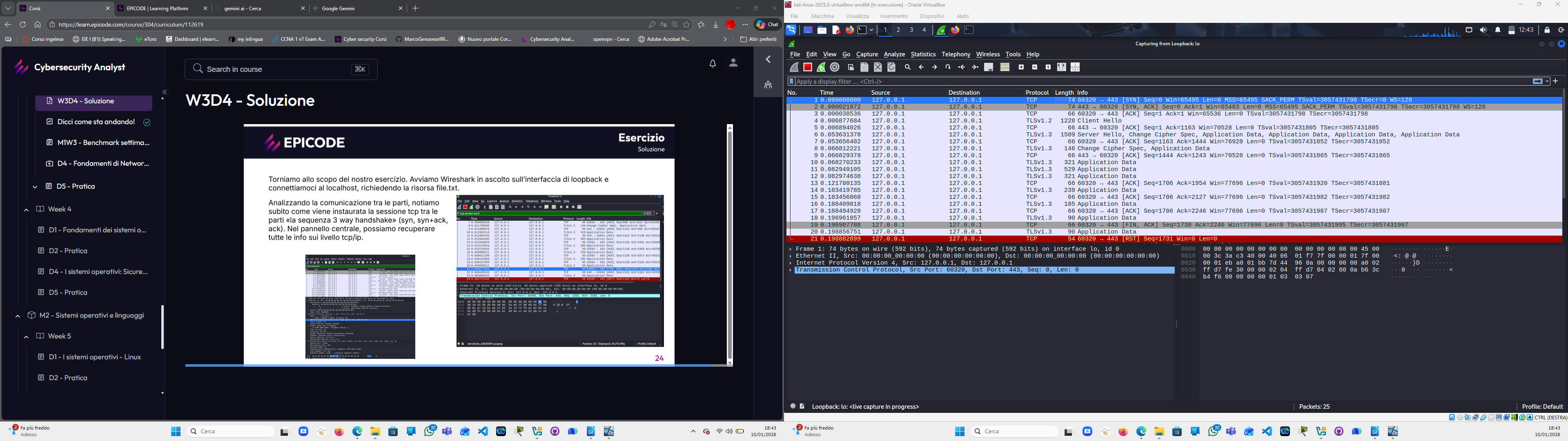
Un ulteriore controllo del funzionamento di inetsim lo abbiamo fatto collegandoci all’indirizzo web “[https://127.0.0.1](https://127.0.0.1/)”. Il browser ha dato in risposta la pagina corretta, quindi ora andiamo ad attivare wireshark per monitorare il flusso di pacchetti che avviene collegandoci alla pagina “<https://127.0.0.1/file.txt>”.

Fig 5

In **Fig 5 possiamo vedere che la table di wireshark all’attivazione della pagina web si è popolata.**

****

Possiamo notare dalla Fig 6 che la prima procedura del protocollo TCP alla richiesta della pagina web è il 3-way hanshake, ovvero la procedura per stabilire una connessione affidabile tra il client ed il server o, più in generale, tra due dispositivi che cercano di comunicare tra loro.

La procedura del 3-way handshake in breve:

* Il primo dispositivo invia un pacchetto “SYN” che richiede la connessione;
* Il secondo dispositivo risponde, se esiste realmente, con un pacchetto “SYN,ACK” per dare conferma della sua esistenza;
* Infine il primo dispositivo alla ricezione del pacchetto “SYN,ACK” invia un ultimo pacchetto per comunicare la ricezione della risposta e che da quel momento sono in una connessione sicura.

In conclusione abbiamo potuto vedere l’utilizzo corretto del firewall con la prima procedura. Con la seconda attività abbiamo potuto simulare una rete reale con l’utilizzo del tool inetsim e analizzato i pacchetti che viaggiano sulla rete con l’ausilio del programma wireshark.