

Es. S11-L3 Handshake a 3 vie



Tag:

#tcp

#handshake

#wireshark

#networking

#cybersecurity

Introduzione

L'handshake a tre vie è un processo fondamentale nel protocollo TCP (Transmission Control Protocol) che consente di stabilire una connessione affidabile tra due host. Questo meccanismo è cruciale per garantire che entrambe le parti siano pronte per la trasmissione dei dati.

Descrizione del Processo

L'handshake a tre vie si compone di tre fasi:

1. SYN (Synchronize)

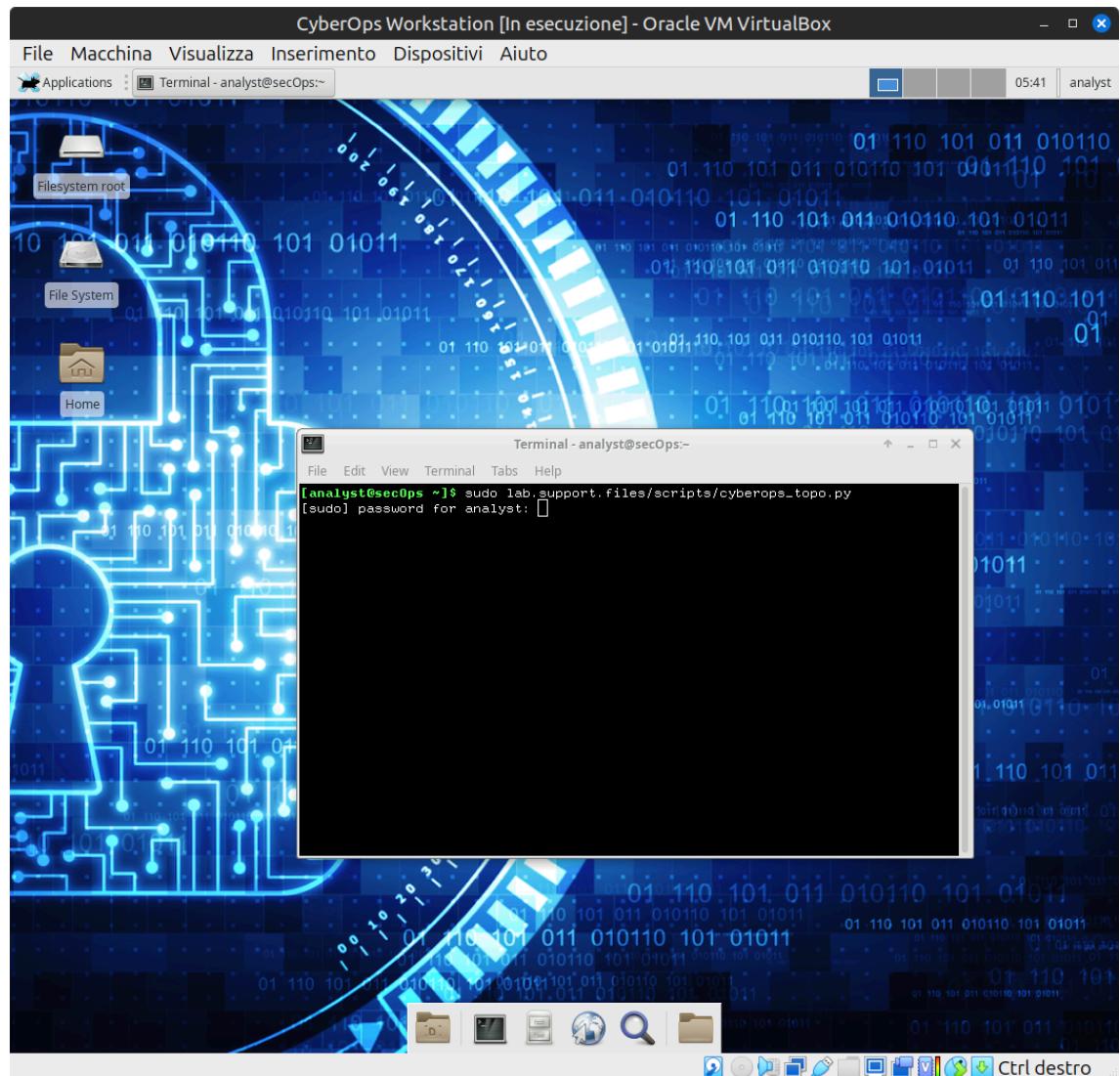
- Il client invia un pacchetto SYN al server per iniziare una nuova connessione.

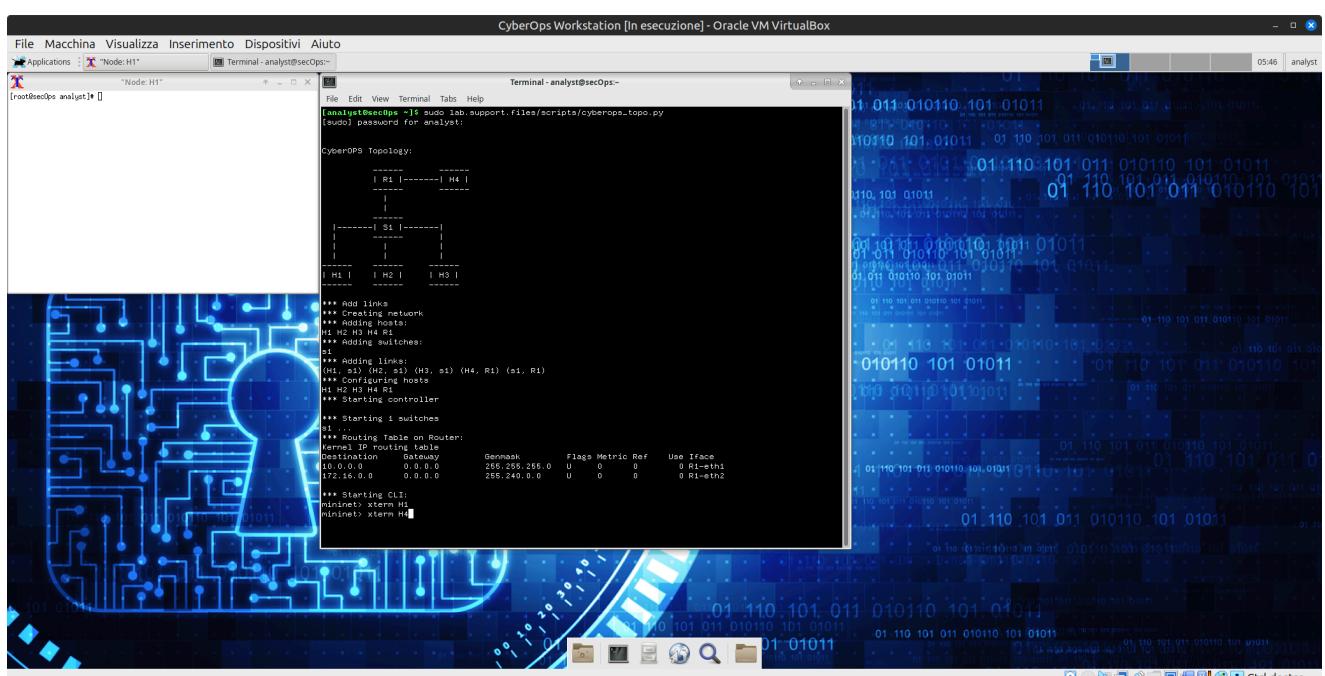
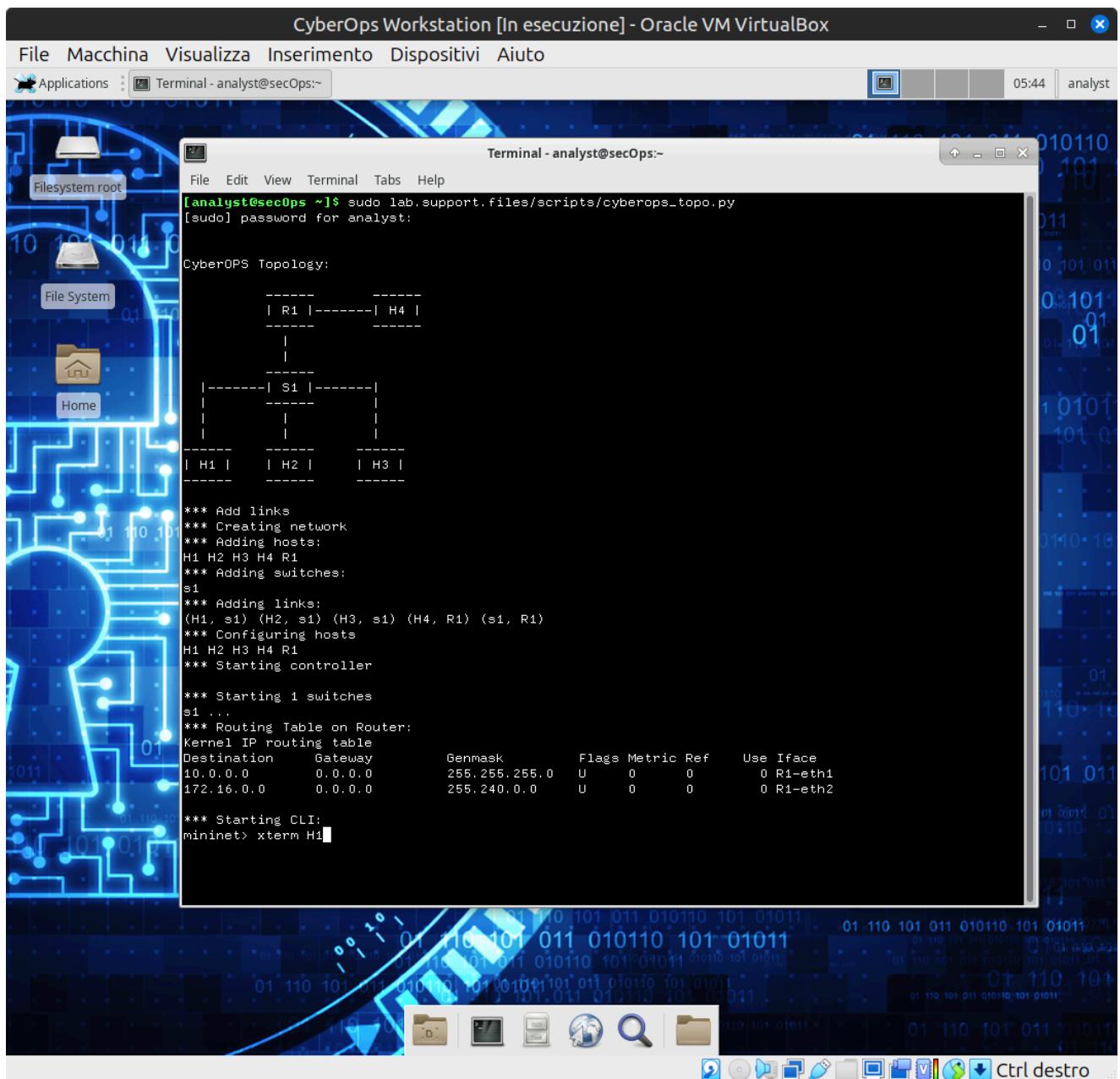
2. SYN-ACK (Synchronize-Acknowledge)

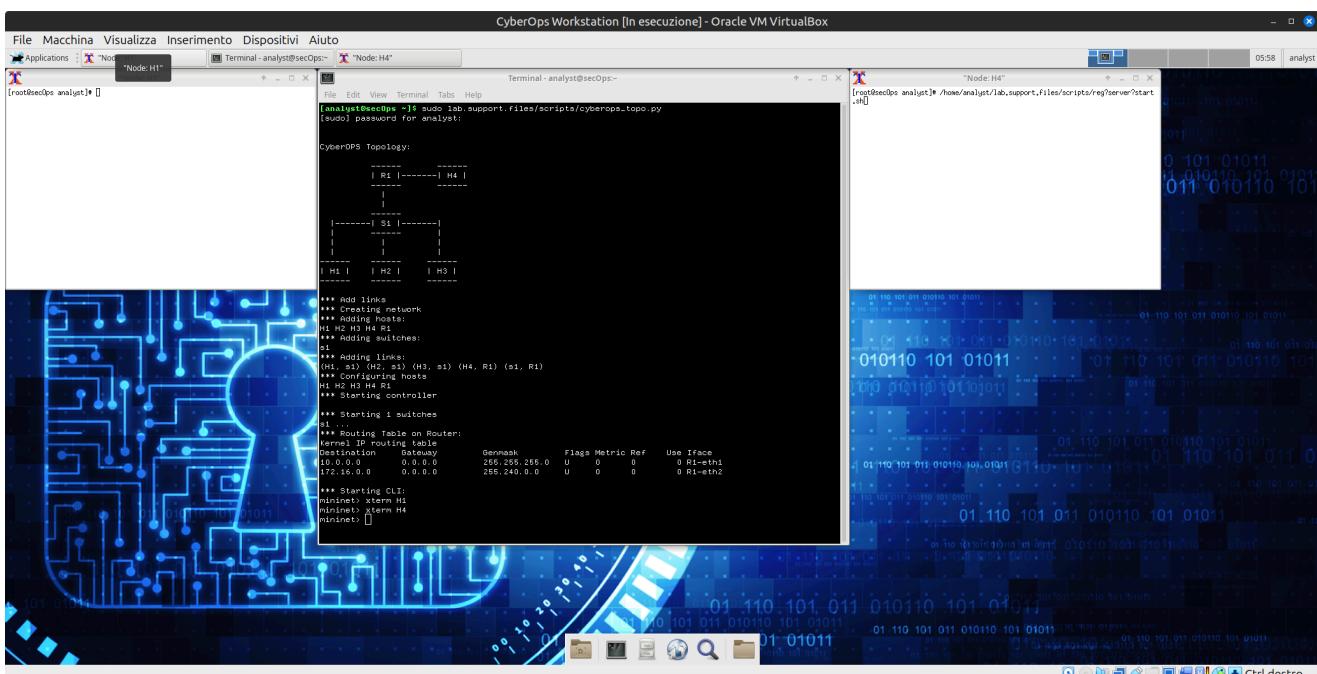
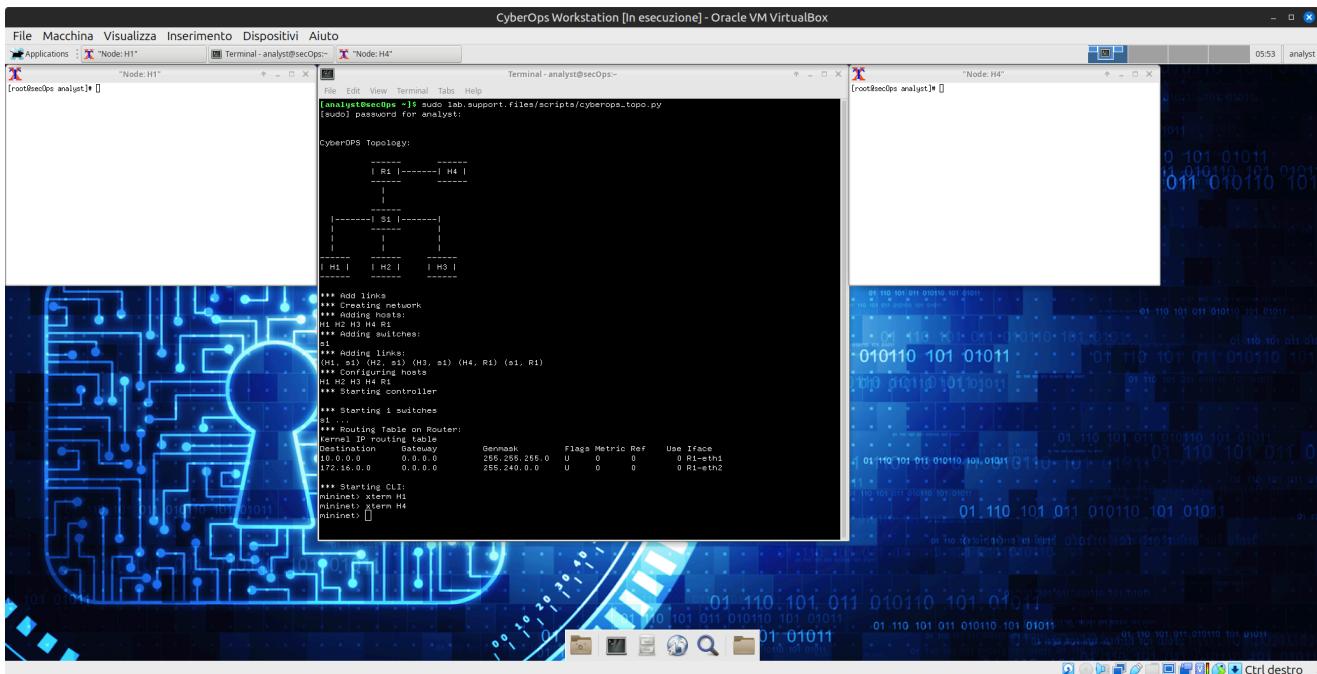
- Il server risponde con un pacchetto SYN-ACK, indicando di aver ricevuto la richiesta e di essere pronto a stabilire una connessione.

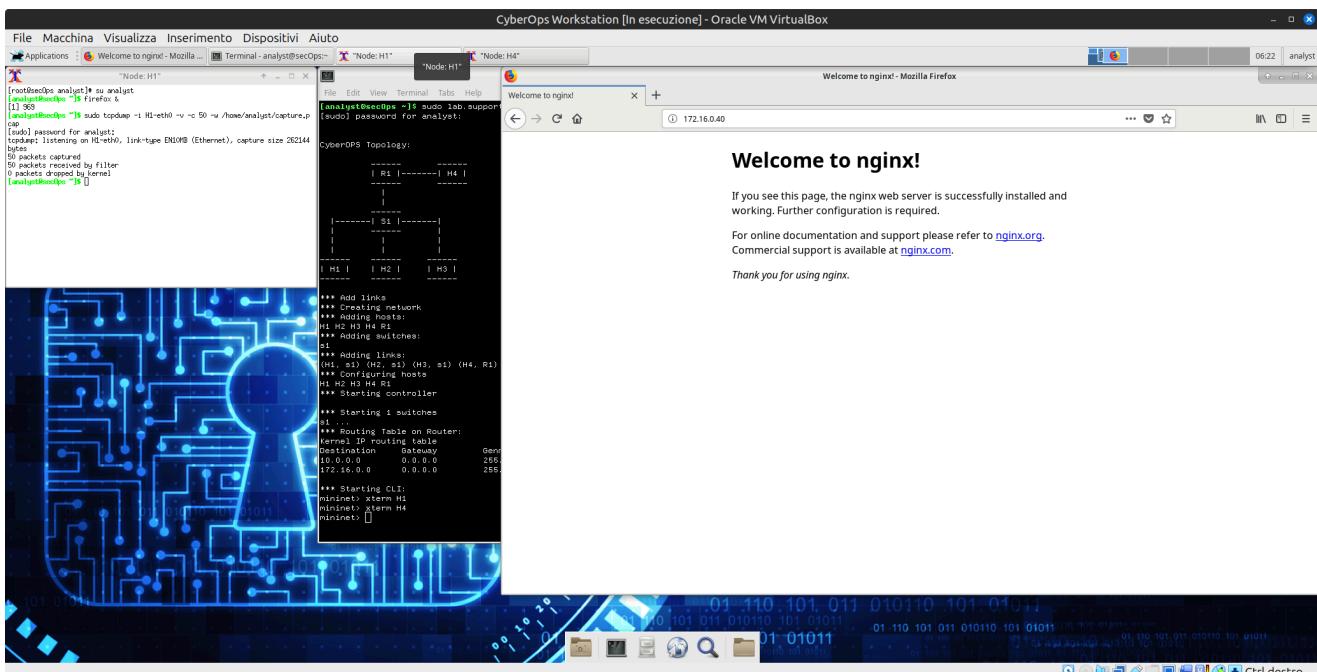
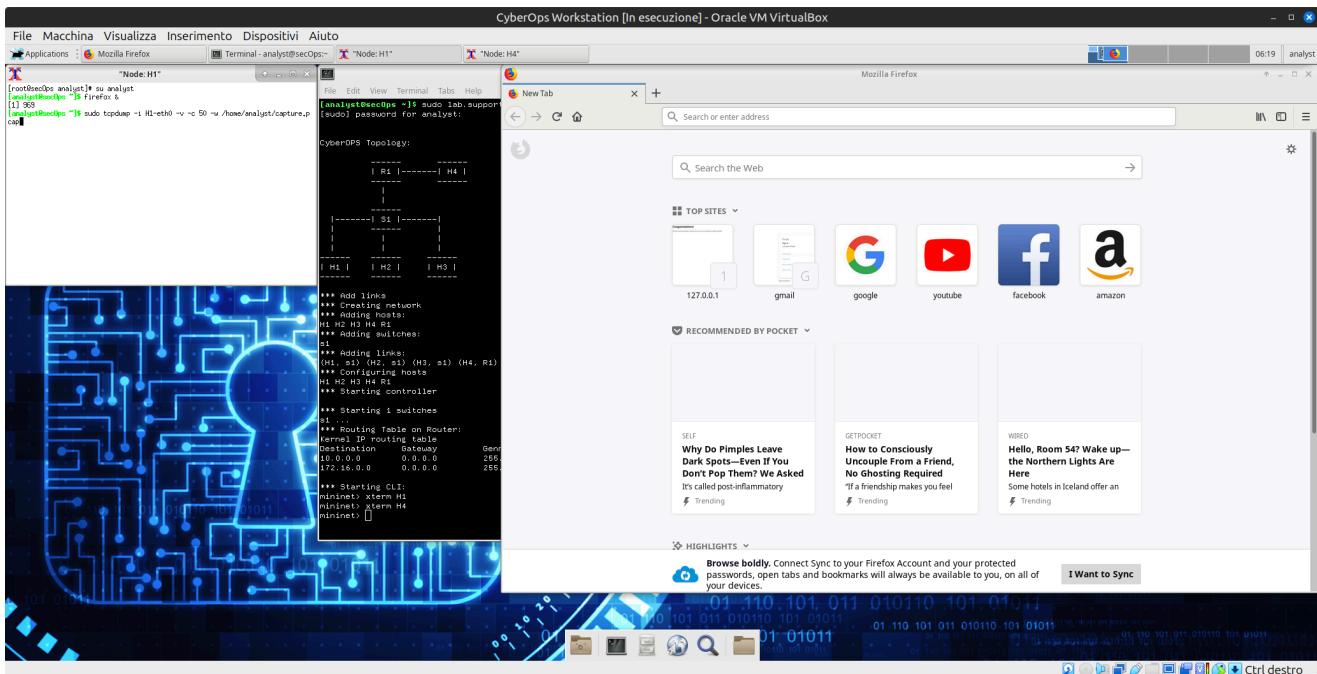
3. ACK (Acknowledge)

- Il client risponde con un pacchetto ACK, confermando che la connessione può essere stabilita.







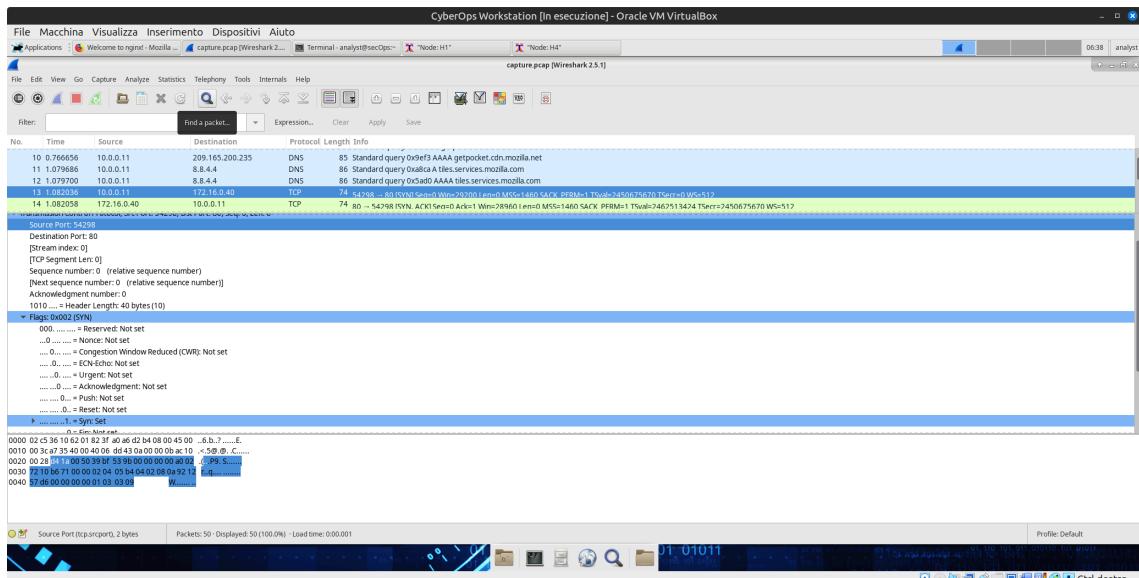


Analisi con Wireshark

Le immagini caricate mostrano l'acquisizione dei pacchetti tramite Wireshark durante l'handshake a tre vie.

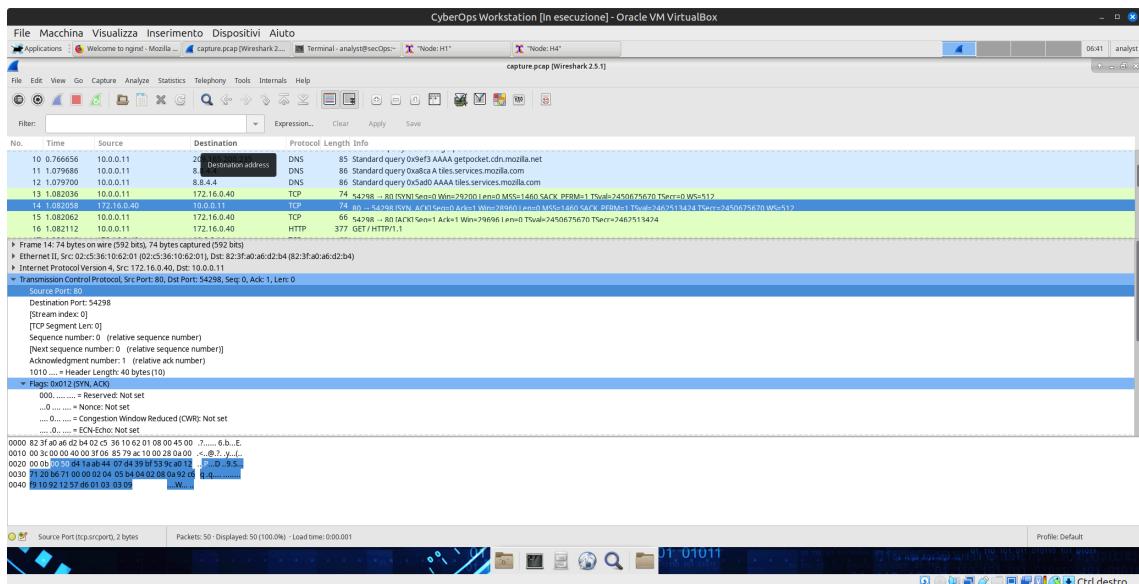
1. Pacchetto SYN

- Il primo pacchetto rappresenta la richiesta del client di stabilire una connessione (SYN).



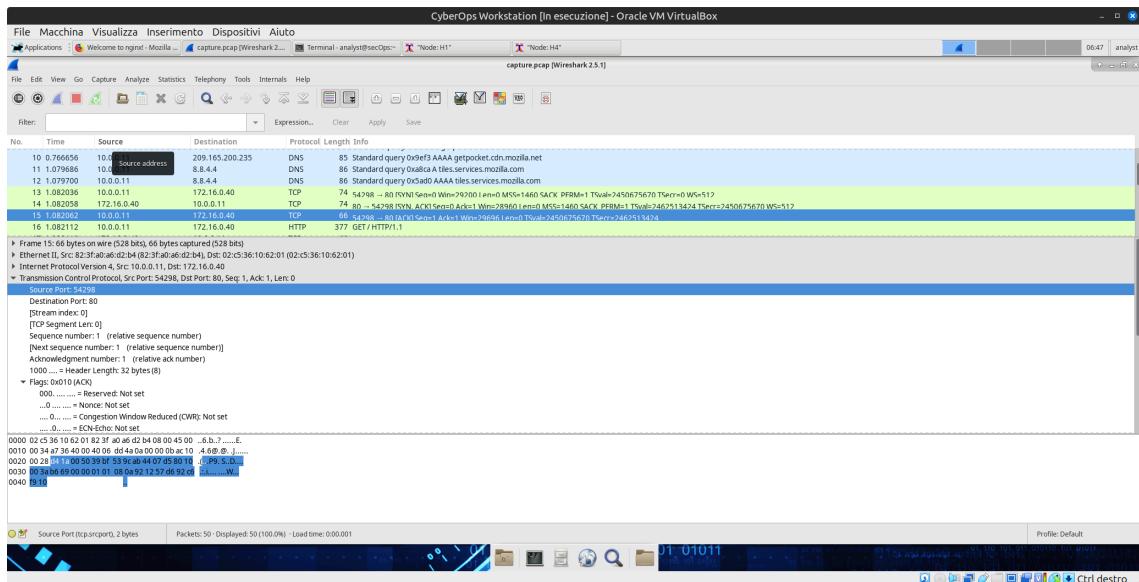
2. Pacchetto SYN-ACK

- Il server risponde con il pacchetto SYN-ACK, indicando di essere pronto.



3. Pacchetto ACK

- Il client risponde confermando la connessione con il pacchetto ACK.

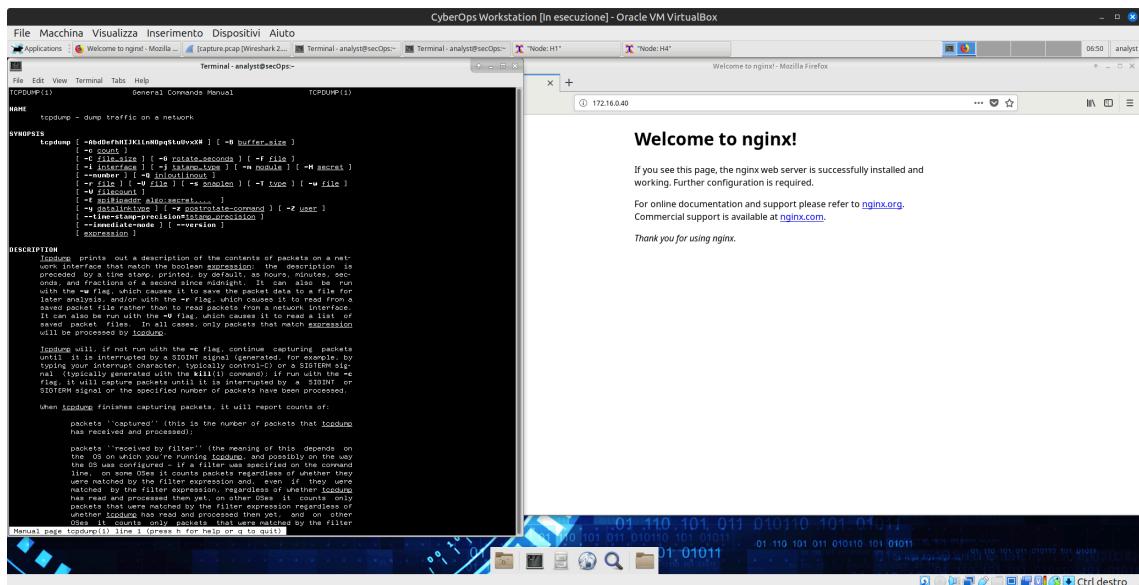


Utilizzo di Tcpdump e Mininet

Durante il test, sono stati utilizzati **tcpdump** e **Mininet** per catturare e analizzare il traffico di rete:

1. Manpage di tcpdump

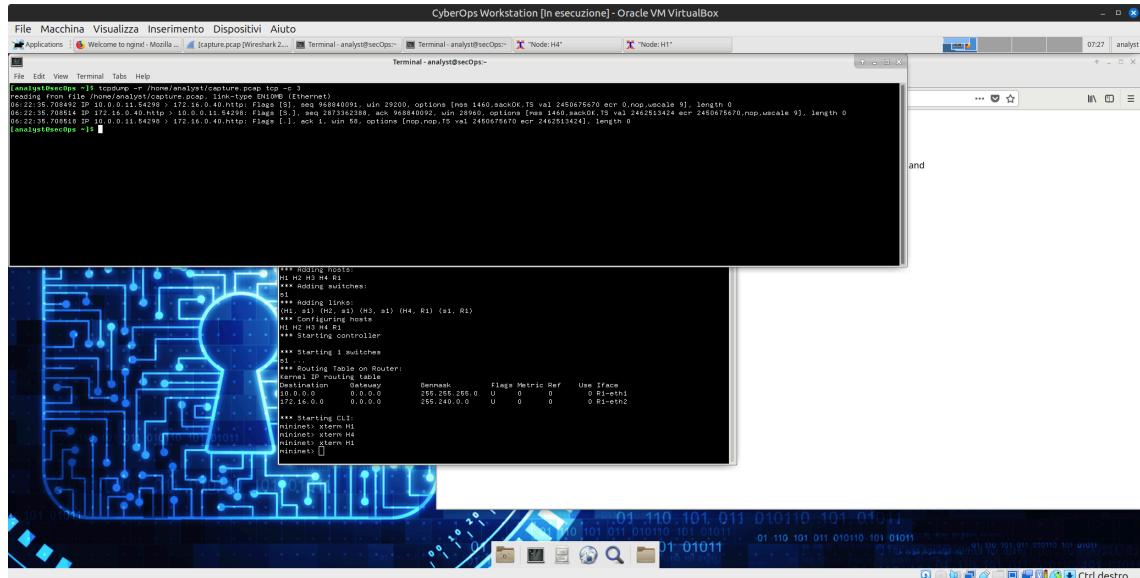
- È stata consultata la manpage di **tcpdump** per comprendere i parametri utilizzabili durante la cattura del traffico di rete.



2. Cattura dei pacchetti con tcpdump

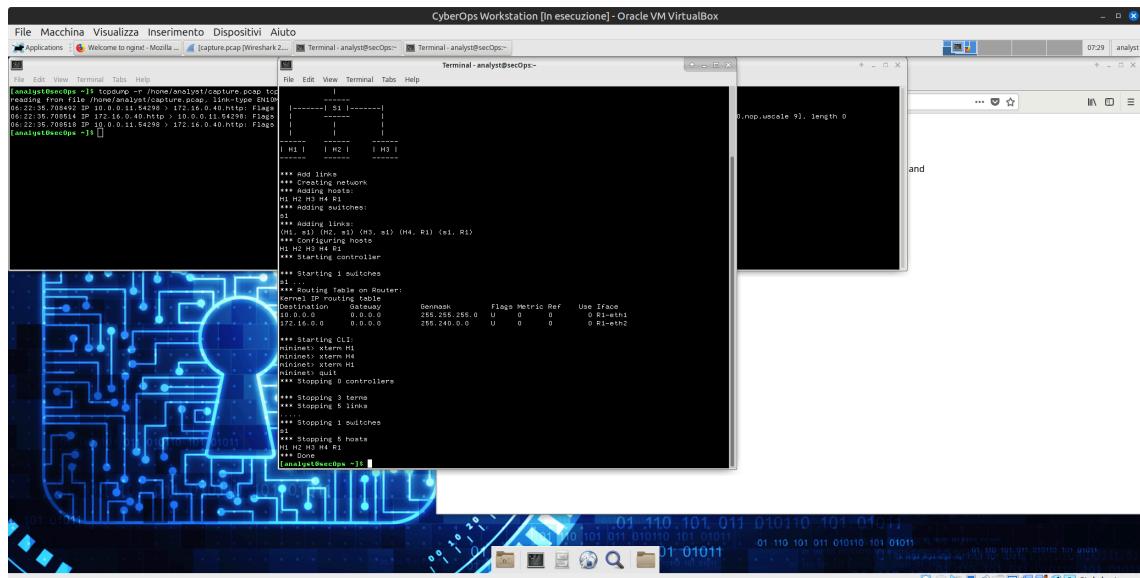
- Il comando `tcpdump -r /home/analyst/capture.pcap -c 3` è stato utilizzato per leggere il file di cattura dei pacchetti e

visualizzare i primi tre pacchetti acquisiti.



3. Mininet e terminazione della simulazione

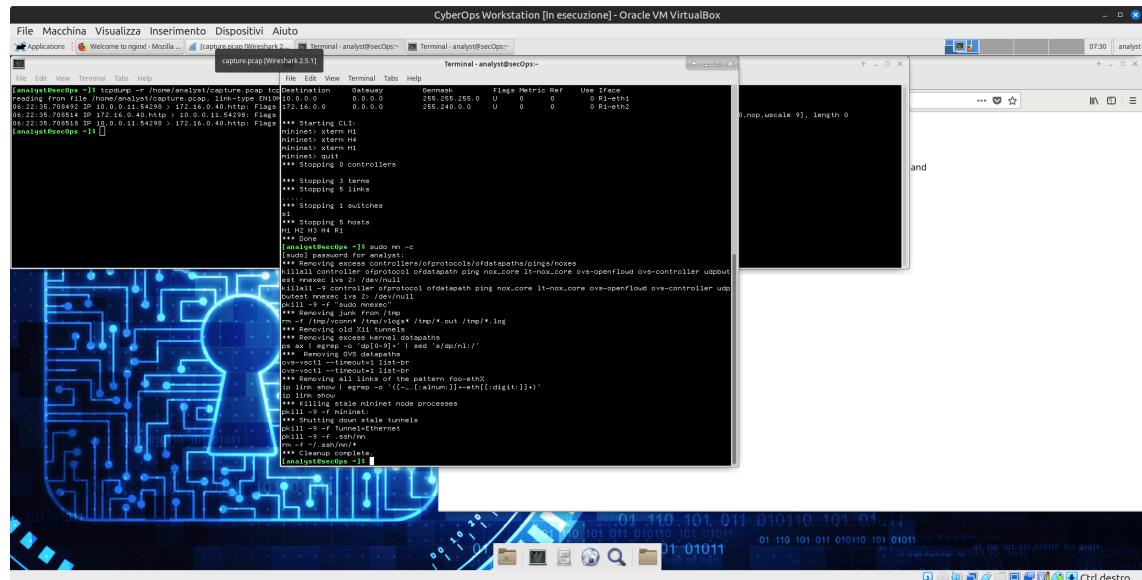
- Dopo aver eseguito la simulazione in Mininet, è stato utilizzato il comando `quit` per fermare la rete virtuale e terminare la sessione.



4. Pulizia dei processi avviati

- Un comando di pulizia (`sudo mn -c`) è stato eseguito per eliminare eventuali processi rimasti in esecuzione e garantire

che il sistema fosse pronto per ulteriori test.



🔑 Chiavi:

[tcp handshake, wireshark, rete]