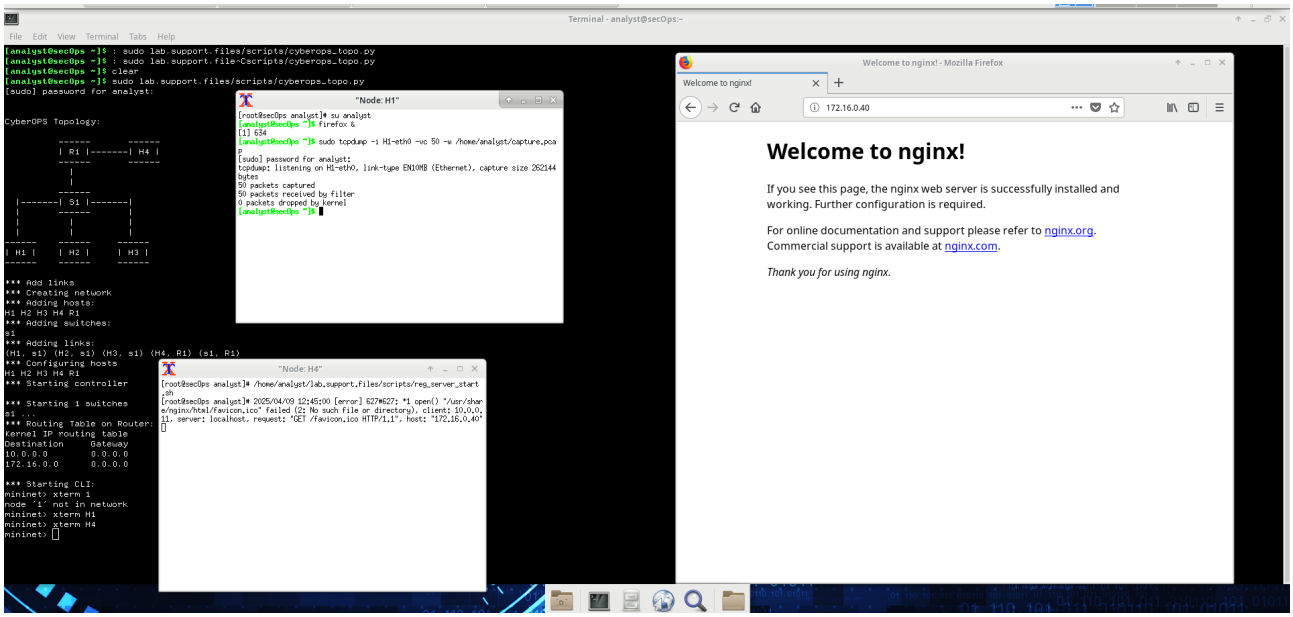
Laboratorio: Utilizzo di Wireshark per Osservare la Stretta di Mano TCP a 3 Vie.

Preparare gli host per catturare il traffico

Dopo essere entrati nella VM CyberOps Workstation prepariamo gli host per catturare il traffico. Per fare ciò apriamo un terminale e avviamo Mininet con il comando “sudo lab.support.files/scripts/cyberops_topo.py” . Poi avviamo gli host H1 e H4 con i comandi “xterm H1” e “xterm H4”. Sulla nuova schermata che si è aperta per H4 avviamo il server web con il comando “/home/analyst/lab.support.files/scripts/reg_server_start.sh”.
Dopo di che passiamo alla schermata relativa all'H1, passiamo all'utente analyst con il comando “su analyst” ed avviamo Firefox con il comando “firefox &”
Avviamo tcpdump e eseguiamo il comando per catturare e sarlvare 50 pacchetti di traffico nel file capture.pcap (formato Wireshark) con il comando “sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap”. Subito dopo sulla pagina Firefox aperta ci colleghiamo subito all'indirizzo 172.16.0.40



Avviamo Wireshark e apriamo il file capture.pcap salvato nel percorso /home/analyst/ e analizziamo i pacchetti dei primi 3 frame tcp

1° FRAME

CAMPO	VALORE	DESCRIZIONE
PORTA SORGENTE TCP	57850	PORTA DINAMICA O PRIVATA
PORTA DESTINAZIONE TCP	80	HTTP
FLAG IMPOSTATO	SYN	RICHIESTA DI SINCRONIZZAZIONE
NUMERO DI SEQUENZA RELATIVO	0	VALORE INIZIALE

2° FRAME

CAMPO	VALORE	DESCRIZIONE
PORTA SORGENTE	80	HTTP
PORTA DESTINAZIONE	57850	CLIENT
FLAG IMPOSTATO	ACK, SYN	ACKNOWLEDGMENT E SYNCHRONIZATION
NUMERO DI SEQUENZA RELATIVO	0	VALORE INIZIALE DEL SERVER
NUMERO DI AACKNOWLEDGMENT RELATIVO	1	CONFERMA RICEZIONE SYN

3° FRAME

Flag Impostato: Acknowledgment flag (ACK)
Numeri di Sequenza e Acknowledgment: entrambi impostati a 1 come punto di partenza
Stato della connessione TCP stabilita e la comunicazione può iniziare