S11L3

Relazione Tecnica sull'Osservazione del Three-Way Handshake TCP tramite Wireshark

L'obiettivo di questo laboratorio era catturare, analizzare e comprendere il processo di connessione TCP noto come *three-way handshake*. Questo studio è stato eseguito in un ambiente virtuale configurato con Mininet, utilizzando strumenti quali Wireshark e tcpdump per monitorare il traffico generato tra un client e un server.

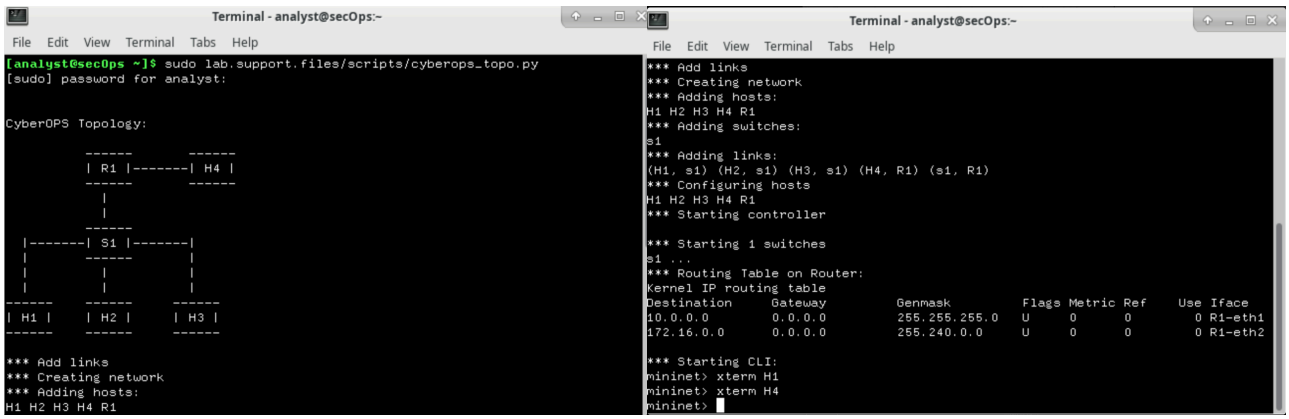
Scenario Operativo e Preparazione degli Host

Il laboratorio si è svolto su una macchina virtuale CyberOps configurata come ambiente di simulazione. Mininet è stato utilizzato per creare una topologia di rete emulata, comprendente due nodi principali:

- **H1:** configurato come client.
- **H4:** configurato come server web.

Passaggi di Configurazione

1. **Avvio dell'ambiente virtuale:**
   - Si è avviata la macchina virtuale CyberOps e si è effettuato l'accesso utilizzando le credenziali fornite (*username*: `analyst`, *password*: `cyberops`).
   - Mininet è stato avviato dalla riga di comando tramite il comando appropriato (`sudo mn`), consentendo la simulazione di una topologia di rete virtuale.
2. **Inizializzazione degli host:**
   - Gli host H1 e H4 sono stati attivati con i comandi di Mininet specifici (`xterm H1` e `xterm H4`), aprendo terminali dedicati per ciascun host.
   - H4 è stato configurato come server web eseguendo uno script fornito (`/home/analyst/lab.support.files/scripts/reg_server_start.sh`). Questo script ha avviato un server HTTP locale all'indirizzo IP 172.16.0.40.

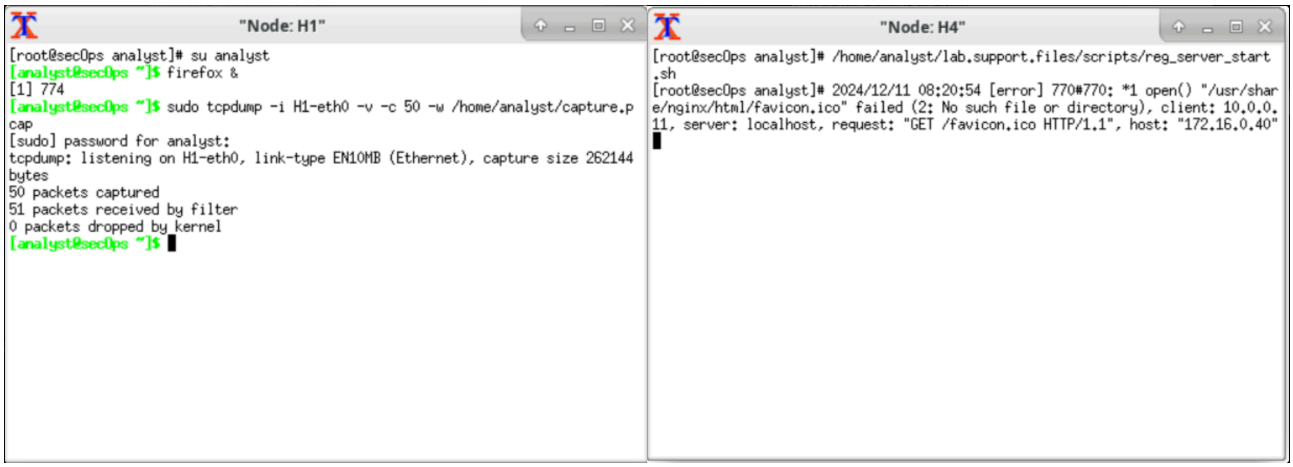


3. **Configurazione del client H1:**
   - Su H1, si è eseguito un cambio utente dal superutente (root) all'utente analyst per motivi di sicurezza (`su analyst`).
   - È stato avviato il browser Firefox per simulare il comportamento del client web. Questo passaggio richiedeva un'attesa di qualche secondo per l'inizializzazione completa.

4. **Cattura del traffico su H1:**
   - Prima di inviare richieste al server, si è avviata una sessione di tcpdump per catturare il traffico di rete. Il comando eseguito è stato: `sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap`
   - Questo comando ha configurato tcpdump per monitorare l'interfaccia di rete di H1 (H1-eth0), catturando un massimo di 50 pacchetti e salvandoli in un file PCAP denominato capture.pcap.

5. **Generazione del traffico:**
   - Una volta avviata la cattura, si è utilizzato il browser su H1 per accedere all'indirizzo IP del server web (172.16.0.40). Questa azione ha generato traffico HTTP, includendo l'handshake TCP tra il client e il server.

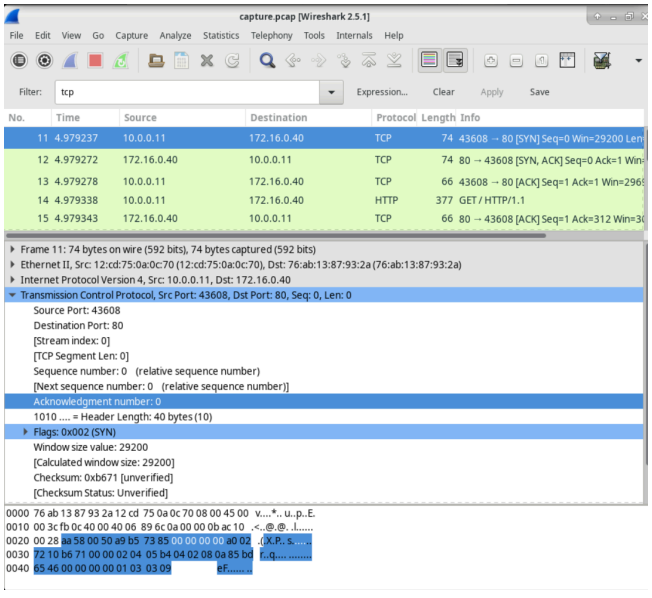
Schermata che mostra la giusta configurazione di H1 e H4



Analisi dei Pacchetti con Wireshark

Dopo aver completato la cattura del traffico, il file PCAP è stato analizzato utilizzando Wireshark:

- Il file è stato caricato in Wireshark tramite il menu `File > Open`.
- È stato applicato un filtro `tcp` per isolare i pacchetti rilevanti per l'handshake a tre vie.
- L'analisi ha evidenziato tre pacchetti fondamentali:
  1. **Primo pacchetto:** Il client (H1) invia un pacchetto SYN al server (H4), indicando l'intenzione di avviare una connessione. Il numero di sequenza relativo è impostato a 0.
  2. **Secondo pacchetto:** Il server risponde con un pacchetto contenente i flag SYN e ACK, confermando la ricezione e indicando il proprio numero di sequenza relativo (0). L'acknowledgment è impostato a 1.
  3. **Terzo pacchetto:** Il client invia un ACK finale per completare l'handshake. A questo punto, la connessione TCP è stabilita.



Esplorazione tramite tcpdump
Per confermare i risultati ottenuti con Wireshark, tcpdump è stato utilizzato per leggere il file PCAP:

- Il comando eseguito è stato: tcpdump -r /home/analyst/capture.pcap tcp -c 3
- Questo ha permesso di visualizzare i primi tre pacchetti TCP, corrispondenti all'handshake.

Considerazioni e Applicazioni

Il laboratorio ha dimostrato l'importanza degli strumenti di analisi del traffico come Wireshark e tcpdump nella comprensione e nel monitoraggio delle comunicazioni TCP.

- **Applicazioni pratiche:** Questi strumenti possono essere utilizzati per analisi di sicurezza, debugging di rete e individuazione di anomalie.
- **Utilità in ambienti di produzione:** Wireshark è particolarmente utile per diagnosticare problemi di rete e investigare attacchi informatici, mentre tcpdump offre un'alternativa più leggera per scenari che richiedono scripting o automazione.