Relazione sull'Attività Svolta: Osservazione three-way handshake TCP a Tre Vie con Wireshark

Obiettivo dell'Attività

Lo scopo di questo laboratorio era catturare e analizzare i pacchetti generati tra un browser web su un PC e un server web, utilizzando il protocollo HTTP. Questo processo includeva l'osservazione della stretta di mano TCP a tre vie (three-way handshake) e l'analisi dei pacchetti tramite Wireshark, un software di analisi del traffico di rete.

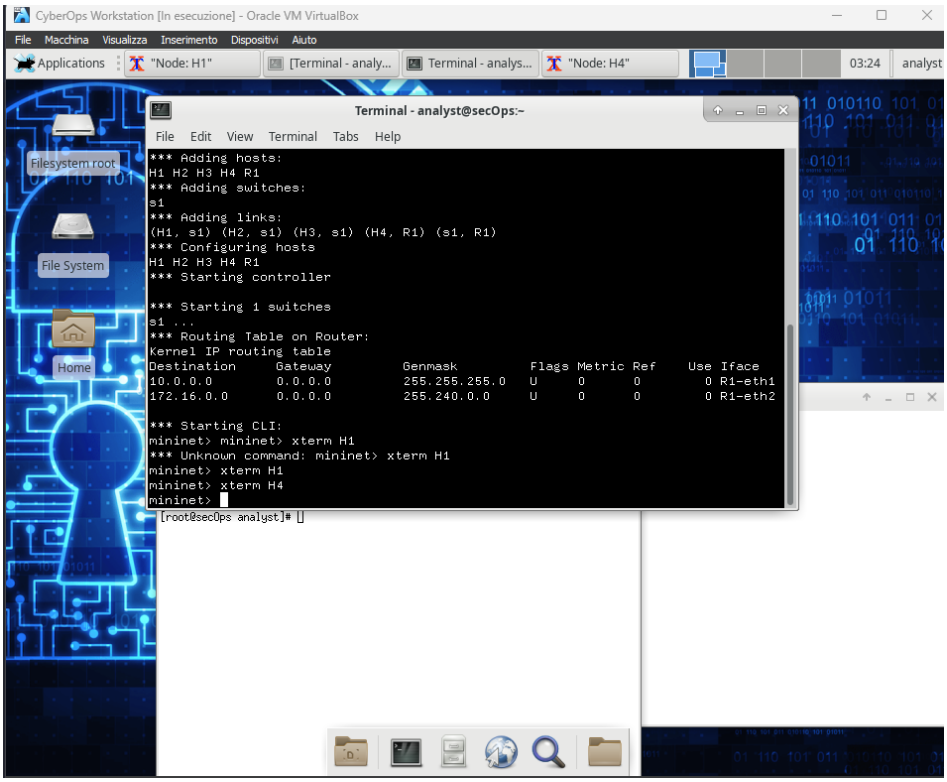
Risorse Utilizzate

- **CyberOps Workstation** (macchina virtuale)
- **Wireshark** per l'analisi dei pacchetti
- **Mininet** per simulare la topologia di rete
- **tcpdump** per la cattura dei pacchetti di rete

Procedura

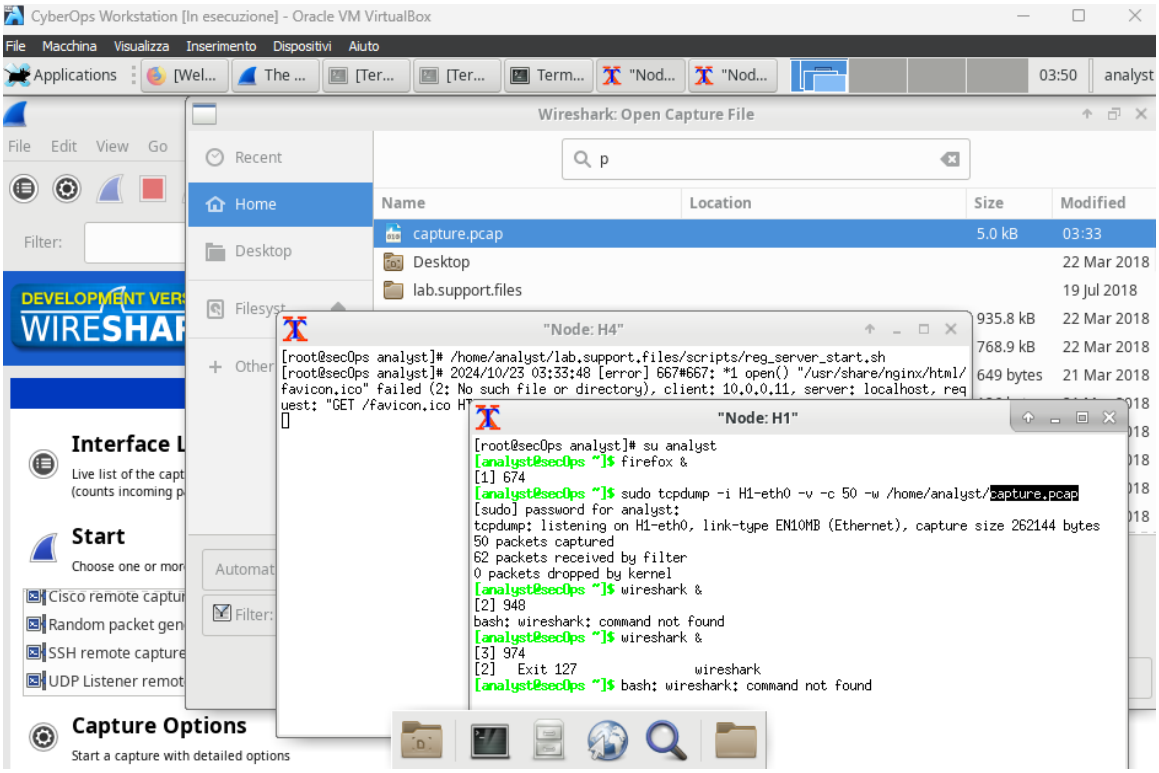
Parte 1: Preparazione degli Host per la Cattura del Traffico

1. **Avvio della VM CyberOps**: Dopo l'accesso con le credenziali di analista, è stato avviato **Mininet** con il comando `sudo lab.support.files/scripts/cyberops_topo.py`.



2. **Avvio degli Host**: Gli host H1 e H4 sono stati avviati e su H4 è stato lanciato il web server tramite lo script `reg_server_start.sh`
3. **Navigazione Web e Cattura dei Pacchetti**: Su H1, è stato aperto il browser Firefox e nel terminale è stata eseguita una sessione di tcpdump per catturare i pacchetti con il comando:

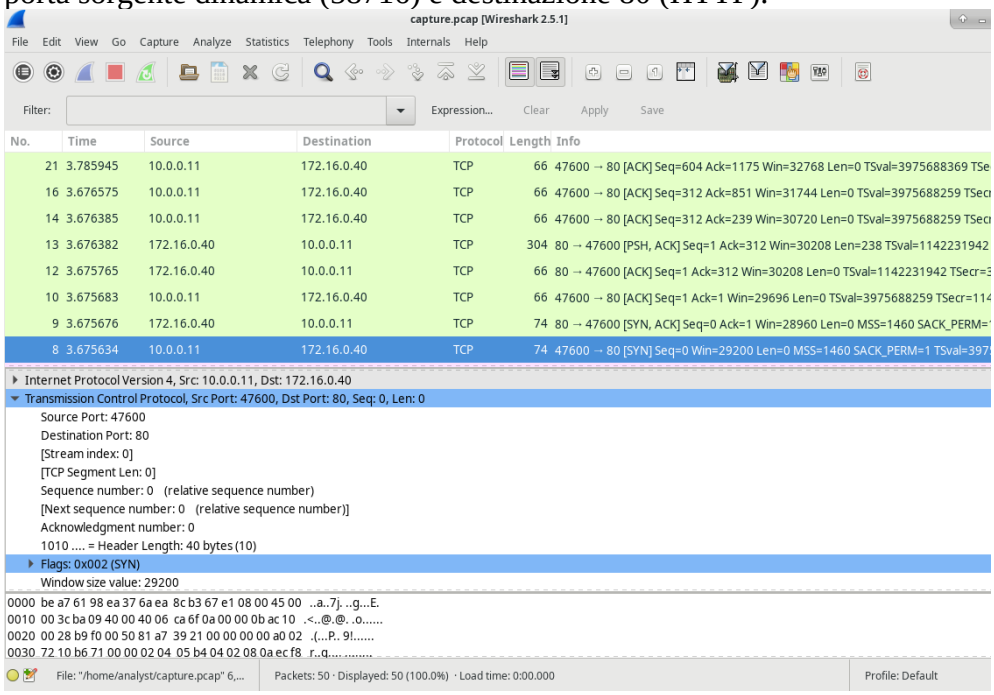
```
sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap
```



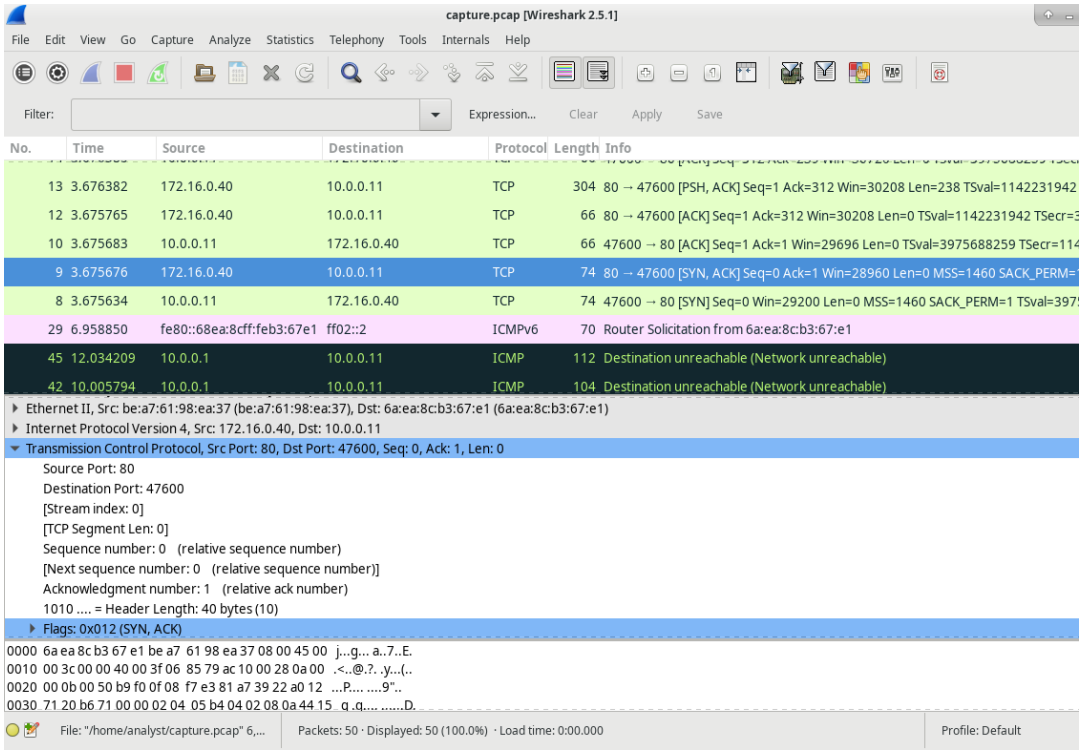
Questo comando ha catturato 50 pacchetti generati dalla navigazione verso l'indirizzo IP del server (172.16.0.40).

Parte 2: Analisi dei Pacchetti con Wireshark

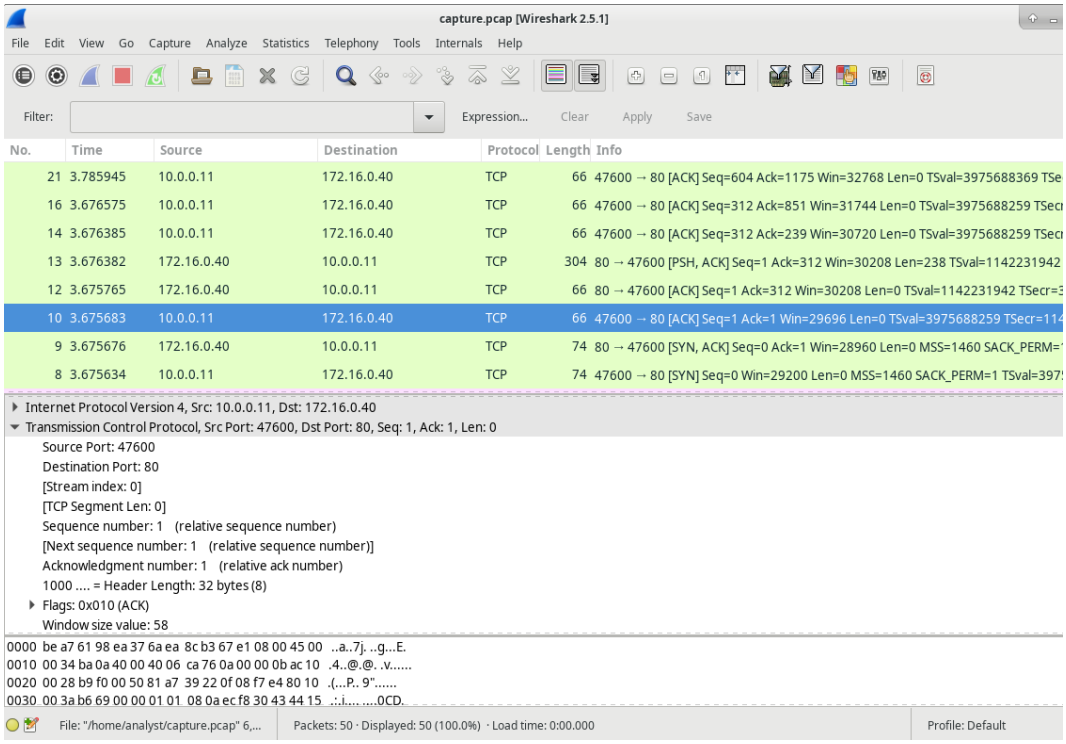
1. **Apertura di Wireshark**: Avviato Wireshark su H1 e aperto il file di cattura (`capture.pcap`).
2. **Applicazione di un filtro TCP**: È stato applicato un filtro TCP per isolare i pacchetti relativi alla stretta di mano TCP.
3. **Esame della Stretta di Mano a Tre Vie**: Sono stati analizzati i primi tre pacchetti catturati, corrispondenti alla stretta di mano tra il PC e il server web.
    - **Pacchetto 1 (SYN)**: Il PC ha inviato un pacchetto con il flag SYN impostato e una porta sorgente dinamica (58716) e destinazione 80 (HTTP).



    - **Pacchetto 2 (SYN-ACK)**: Il server ha risposto con un pacchetto SYN-ACK, confermando la richiesta di connessione.



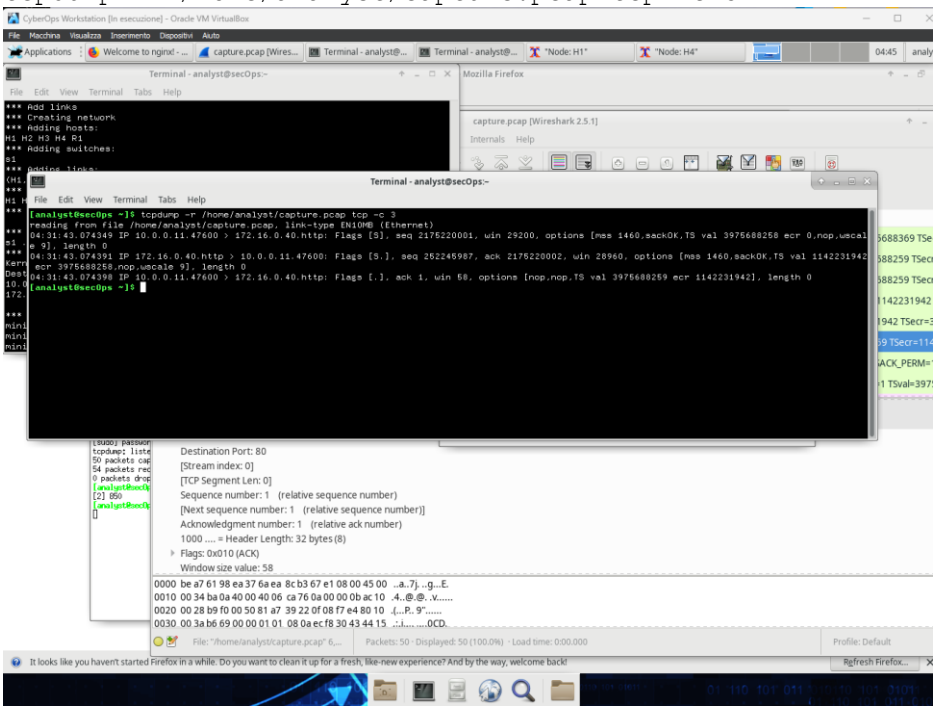
- **Pacchetto 3 (ACK)**: Il PC ha inviato un pacchetto ACK, completando la stretta di mano TCP.



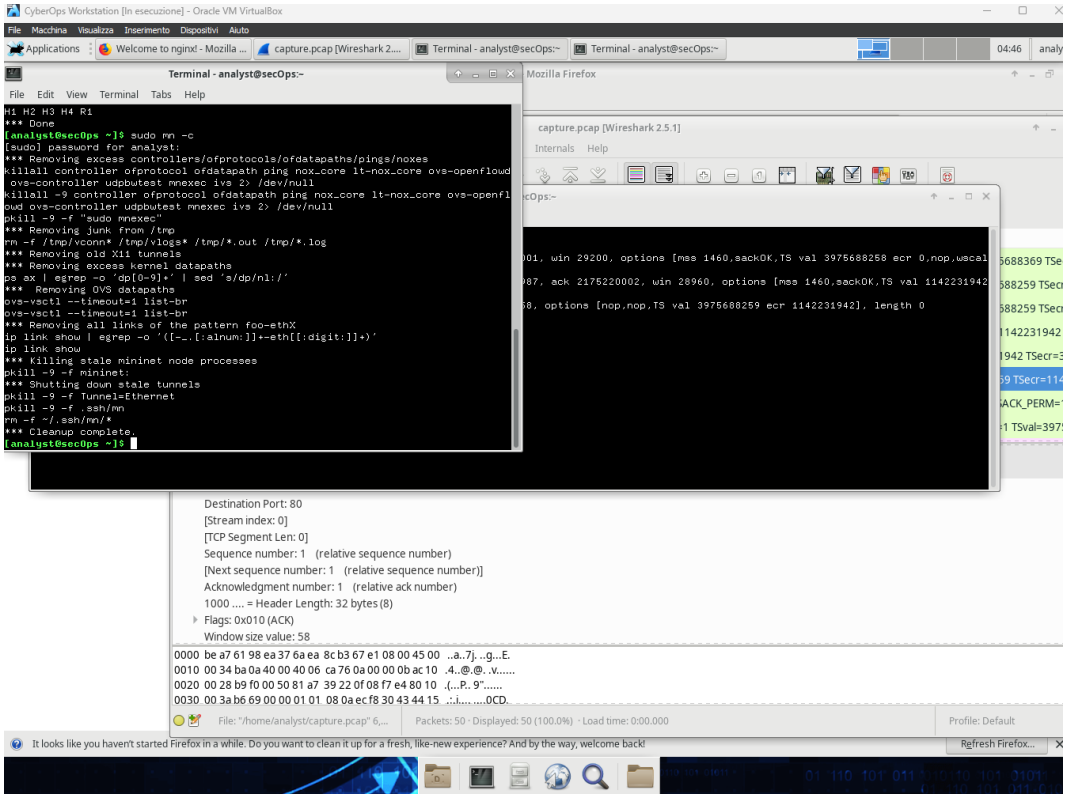
Parte 3: Visualizzazione dei Pacchetti con tcpdump

1. **Comando tcpdump per la visualizzazione**: Utilizzando tcpdump, è stata aperta la cattura per visualizzare i primi tre pacchetti TCP, verificando nuovamente la stretta di mano a tre vie:

```
tcpdump -r /home/analyst/capture.pcap tcp -c 3
```



2. **Pulizia della Topologia Mininet**: Al termine dell'analisi, Mininet è stato terminato con `quit`, e successivamente, sono stati puliti i processi residui con il comando `sudo mn -c`.



Conclusioni

Durante questo laboratorio, è stata acquisita una comprensione pratica della stretta di mano TCP a tre vie, fondamentale per stabilire una connessione affidabile tra due host in una rete. Inoltre, l'uso di strumenti come **Wireshark** e **tcpdump** ha permesso di approfondire le tecniche di cattura e analisi del traffico di rete, competenze essenziali per la gestione e la sicurezza delle reti.

Riflessioni e Risposte

1. **Filtri Utili in Wireshark per un Amministratore di Rete**:
    - **TCP**: Per monitorare le connessioni tra host.
    - **Indirizzi IP specifici**: Per tracciare il traffico da o verso host specifici.
    - **HTTP**: Per esaminare le richieste e risposte web.
2. **Altri Usi di Wireshark in una Rete Produttiva**:
    - Monitoraggio delle prestazioni di rete.
    - Identificazione di traffico sospetto durante attacchi di rete.
    - Analisi di nuovi protocolli per la verifica delle porte utilizzate.