

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.

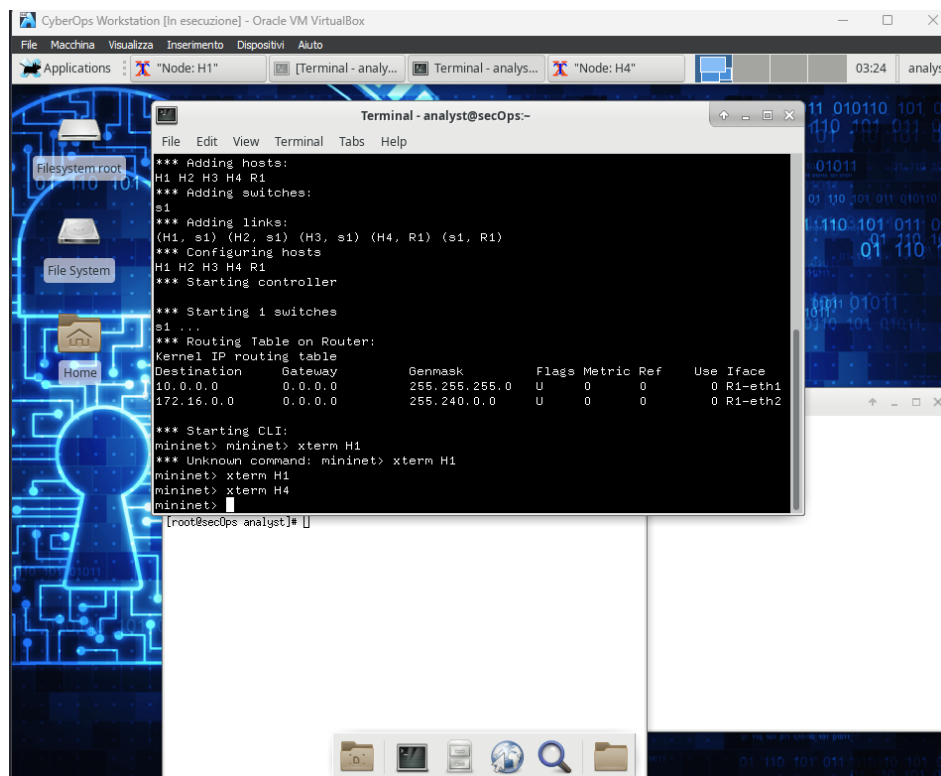
Risorse Utilizzate

- **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

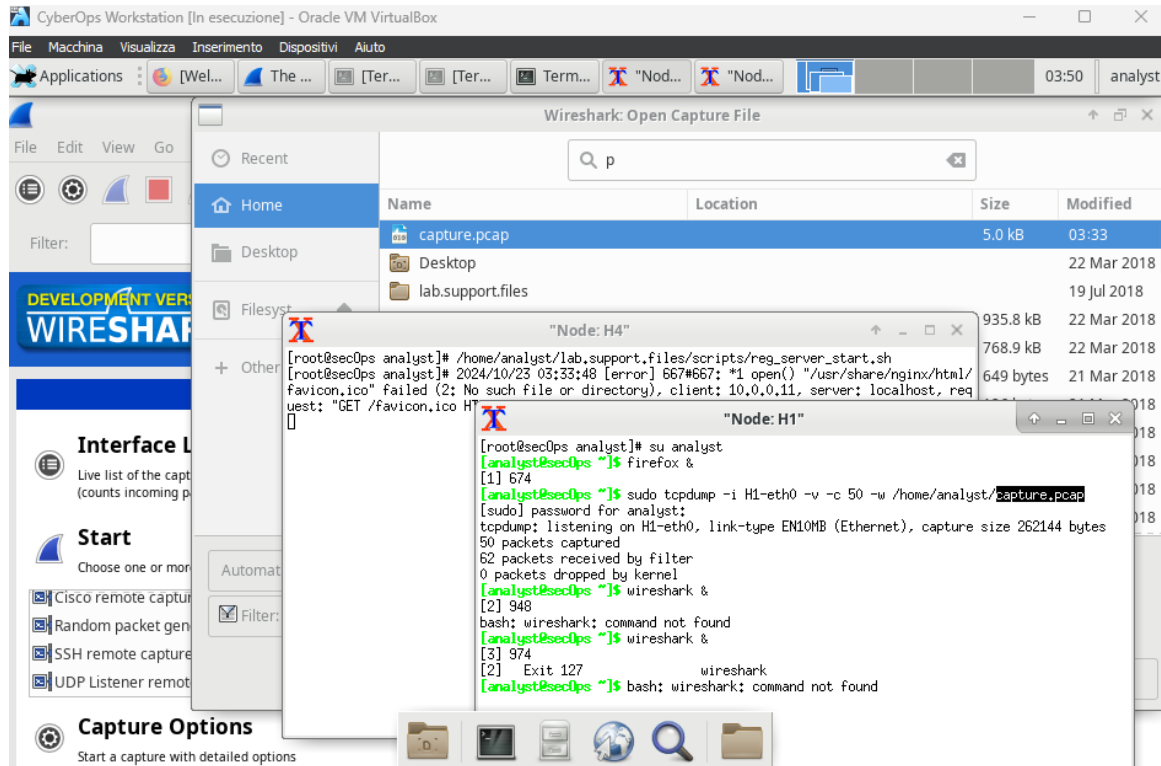
Parte 1: Preparazione degli Host per la Cattura del Traffico

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:

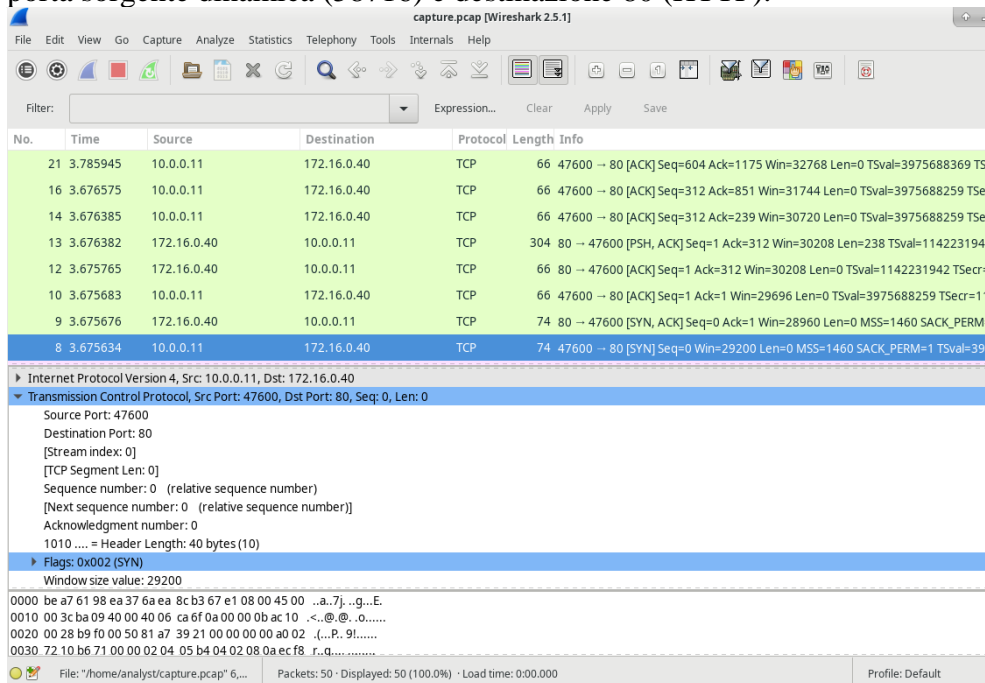
```
sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap
```



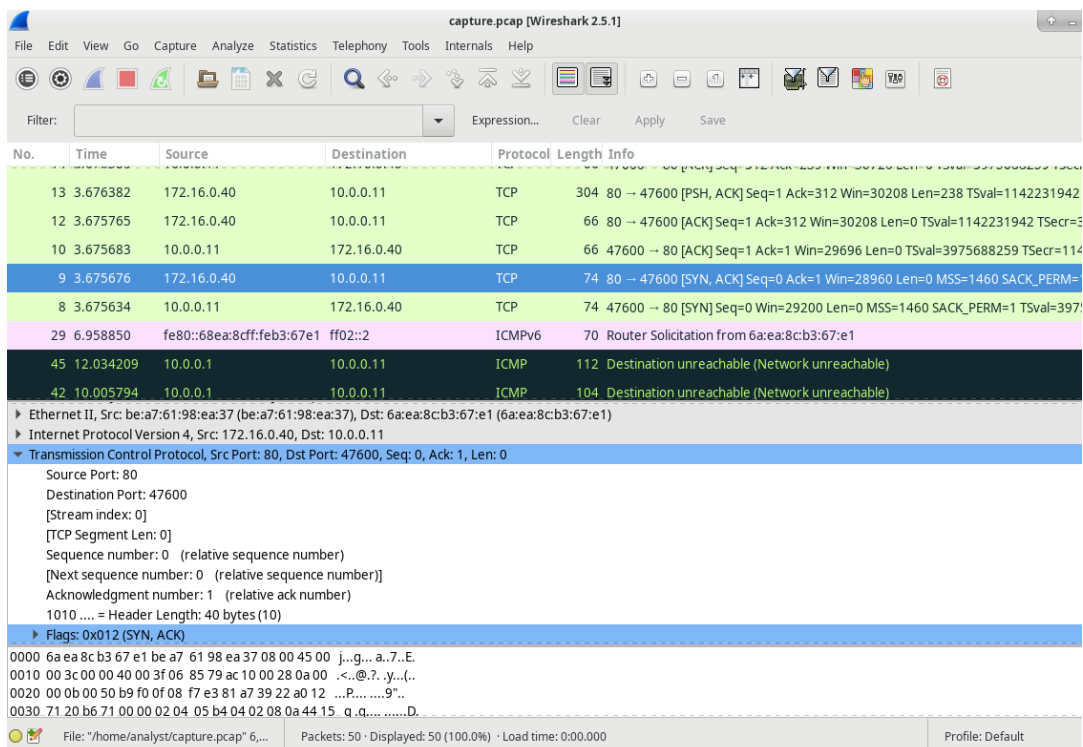
Questo comando ha catturato 50 pacchetti generati dalla navigazione verso l'indirizzo IP del server (172.16.0.40).

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.

capture.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
21	3.785945	10.0.0.11	172.16.0.40	TCP	66	47600 → 80 [ACK] Seq=604 Ack=1175 Win=32768 Len=0 TSval=3975688369 TSecr=1142231942
16	3.676575	10.0.0.11	172.16.0.40	TCP	66	47600 → 80 [ACK] Seq=312 Ack=851 Win=31744 Len=0 TSval=3975688259 TSecr=1142231942
14	3.676385	10.0.0.11	172.16.0.40	TCP	66	47600 → 80 [ACK] Seq=312 Ack=239 Win=30720 Len=0 TSval=3975688259 TSecr=1142231942
13	3.676382	172.16.0.40	10.0.0.11	TCP	304	80 → 47600 [PSH, ACK] Seq=1 Ack=312 Win=30208 Len=238 TSval=1142231942 TSecr=3975688259
12	3.675765	172.16.0.40	10.0.0.11	TCP	66	80 → 47600 [ACK] Seq=1 Ack=312 Win=30208 Len=0 TSval=1142231942 TSecr=3975688259
10	3.675683	10.0.0.11	172.16.0.40	TCP	66	47600 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=3975688259 TSecr=1142231942
9	3.675676	172.16.0.40	10.0.0.11	TCP	74	80 → 47600 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1142231942 TSecr=3975688259
8	3.675634	10.0.0.11	172.16.0.40	TCP	74	47600 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3975688259 TSecr=1142231942

► Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40

▼ Transmission Control Protocol, Src Port: 47600, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 47600
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1000 = Header Length: 32 bytes (8)
► Flags: 0x010 (ACK)
Window size value: 58

0000 be a7 61 98 ea 37 6a ea 8c b3 67 e1 08 00 45 00 ..a..7j...g...E.
0010 00 34 ba 0a 40 00 40 06 ca 76 0a 00 00 0b ac 10 .4..@..v.....
0020 00 28 b9 f0 00 50 81 a7 39 22 0f 08 f7 e4 80 10 {...P..9*.....
0030 00 3a b6 69 00 00 01 01 08 0a ec f8 30 43 44 15 ..!.....0CD..

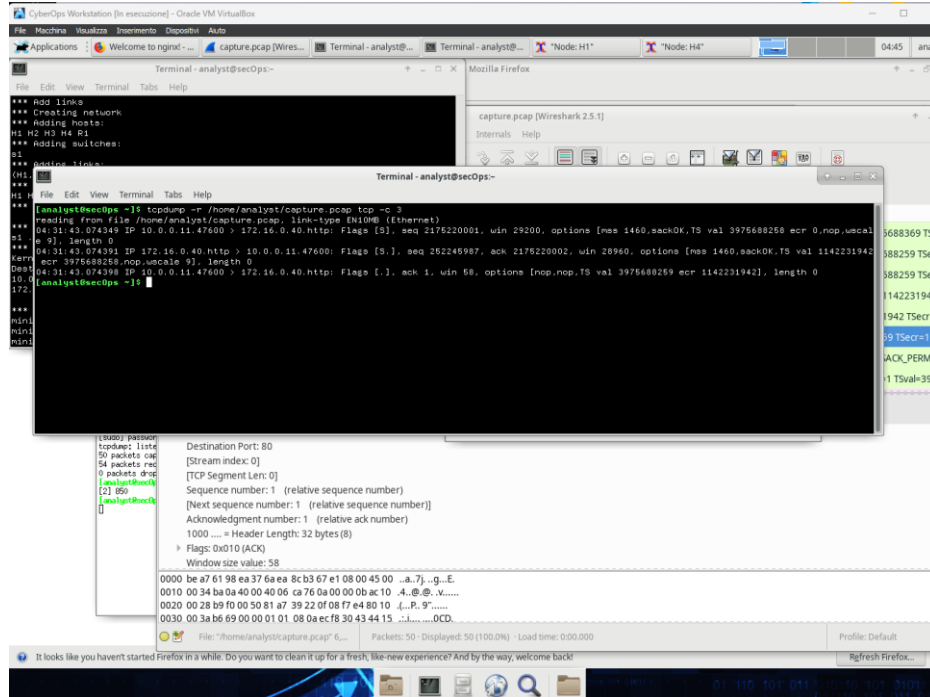
File: "/home/analyst/capture.pcap" 6,000 Bytes · Packets: 50 · Displayed: 50 (100.0%) · Load time: 0:00.000

Profile: Default

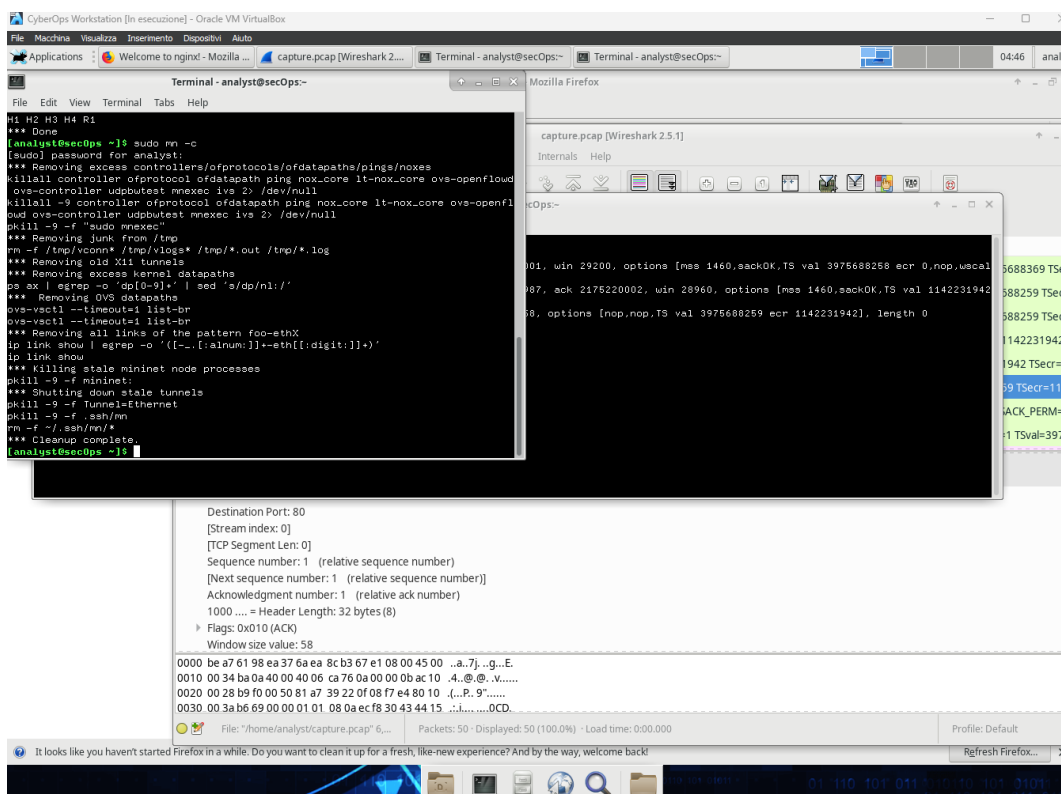
Parte 3: Visualizzazione dei Pacchetti con tcpdump

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.