S11-L3

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

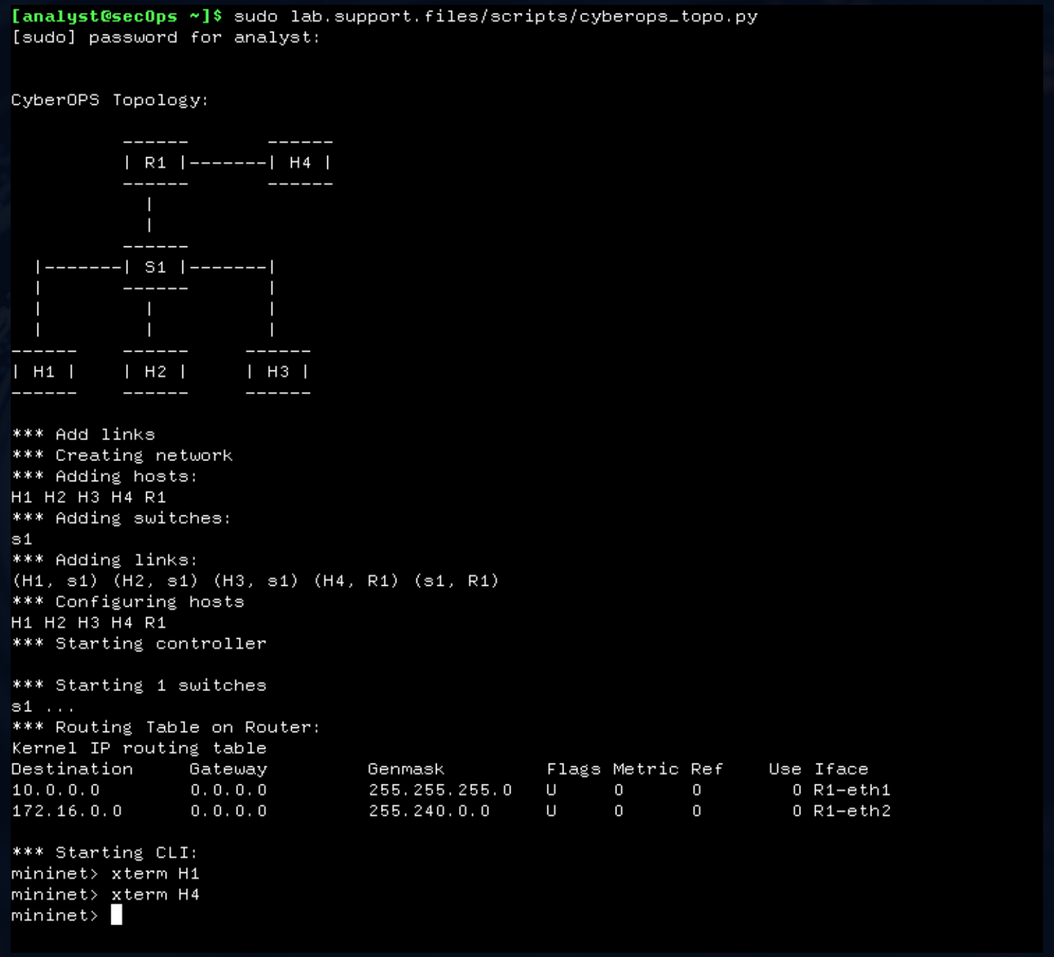
TRACCIA

In questo laboratorio, completeremo i seguenti obiettivi:

- Parte 1: Preparare gli host per catturare il traffico
- Parte 2: Analizzare i pacchetti utilizzando Wireshark
- Parte 3: Visualizzare i pacchetti utilizzando tcpdump

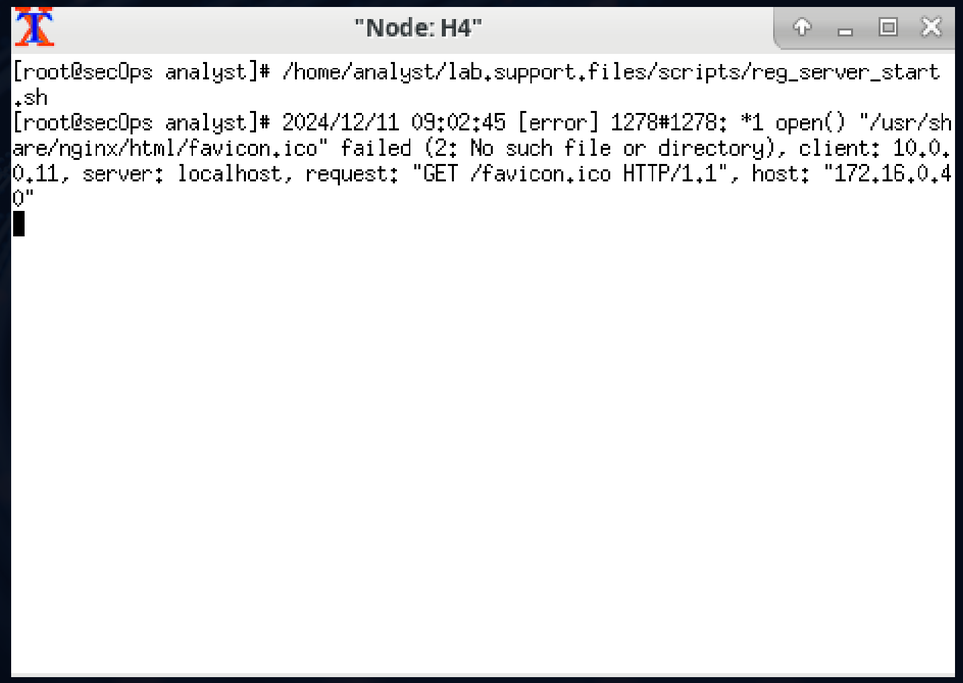
PREPARAZIONE HOST PER CATTURA

Come prima cosa apriamo il nostro terminale e inseriamo il comando “sudo lab.support.files/scripts/cyberops_topo.py “. Questo script viene utilizzato all’interno della VM di cyberops per configurare una topologia di rete simulata. Dopodichè creiamo i nostri host attraverso il comando “xterm H1” per l’host H1 e “xterm H4” per l’host H4.



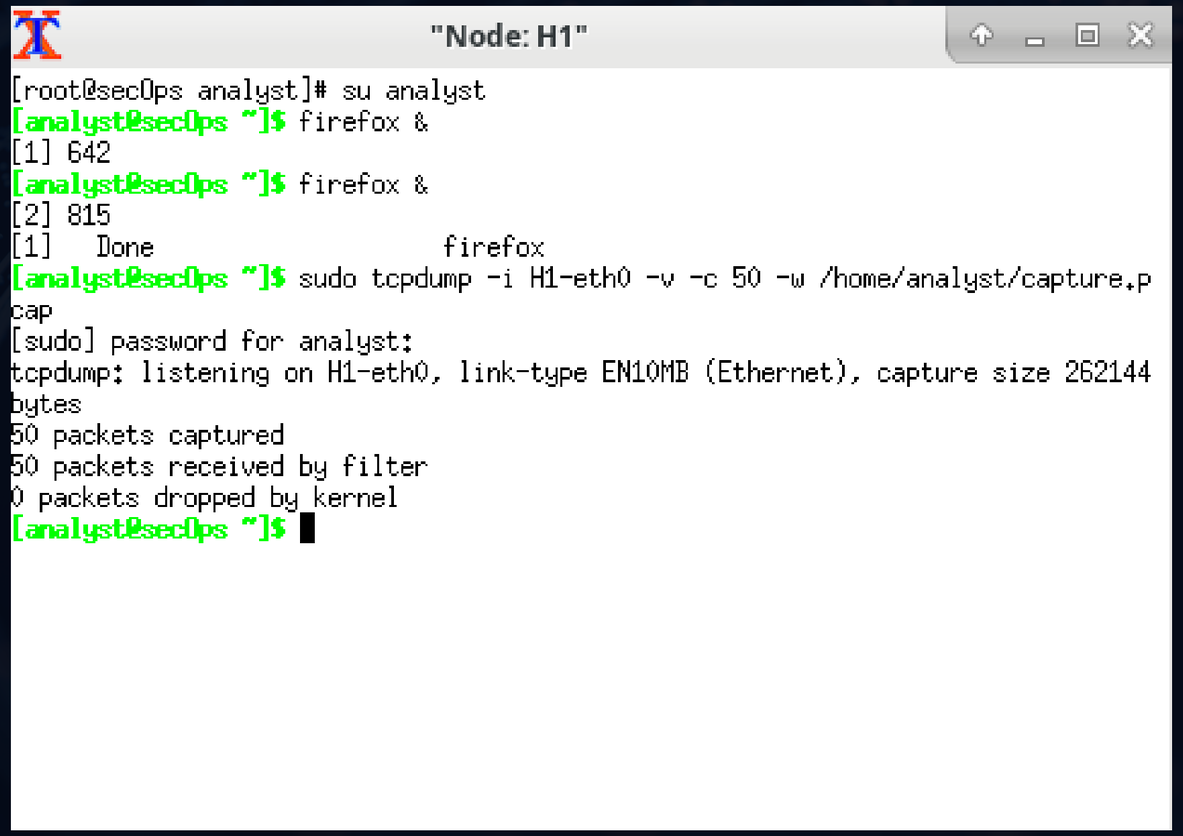
AVVIO SERVER H4

Procediamo poi con l’avvio di un server web che ci servirà al fine di registrare eventi di rete con wireshark

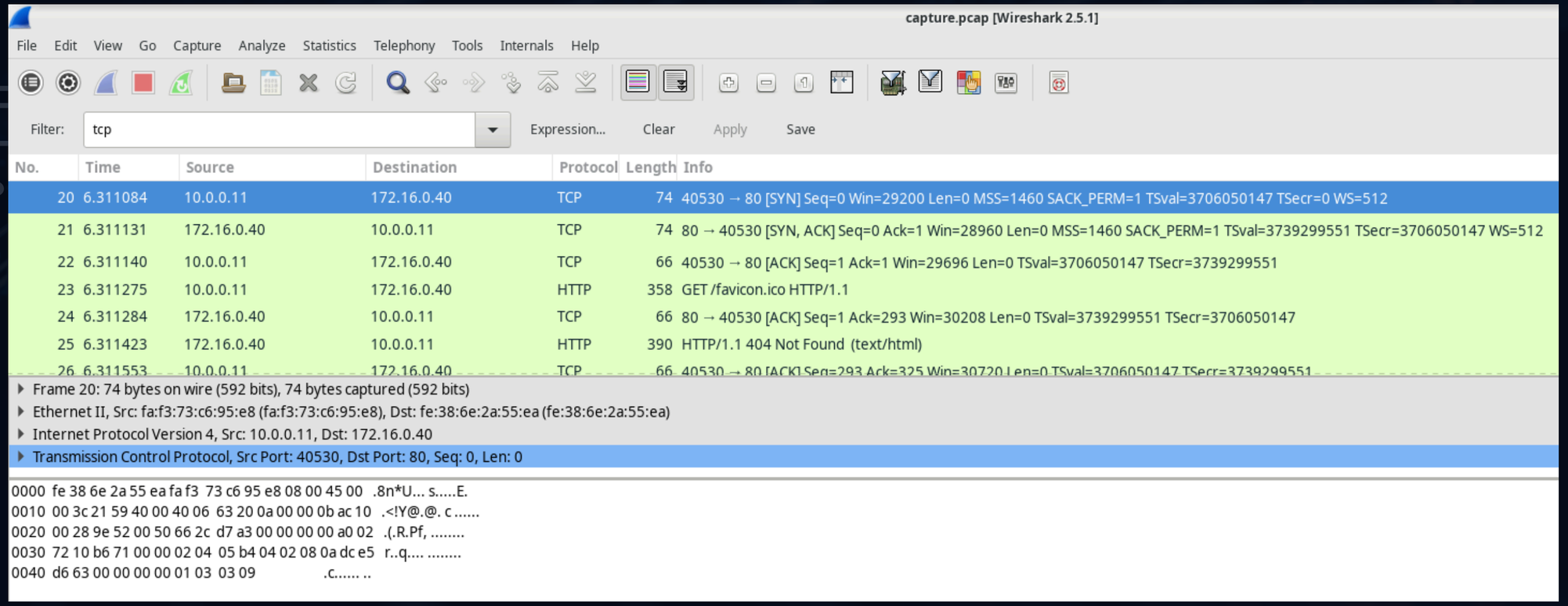


CATTURA PACCHETTI TCPDUMP

Avviamo poi il nostro browser web firefox attraverso l’apposito comando e mettiamoci a catturare i pacchetti. Ne verranno catturati 50 in quanto nel comando abbiamo stabilito un massimo di 50 pacchetti. il pacchetto che verrà salvato sarà .pcap il quale è un formato leggibile da strumenti come wireshark e tcpdump



HANDSHAKE 3 WAYS SU WIRESHARK



HANDSHAKE 3 WAYS SU WIRESHARK

Come si può vedere dall’immagine precedente, abbiamo catturato l’handshake 3ways tra il pc client e il server creato su H4.

- SYN: un pacchetto syn viene inviato dall’IP 10.0.0.11 alla porta 80 dell’indirizzo 172.16.0.40 per iniziare la connessione TCP.
- SYN-ACK: Viene risposto con un syn-ack da 172.16.0.40 che conferma la ricezione del Syn.
- ACK: conferma il completamento dell’handshake da parte del client 10.0.0.11

L'handshake TCP è completato con successo, dimostrando che la connessione tra il client e il server è stata stabilita senza problemi.

HANDSHAKE 3 WAYS SU TCPDUMP

Si può, inoltre, verificare la cattura tramite tcpdump specificando il numero di righe che si vuole vedere e i pacchetti TCP. Ci mostrerà le stesse cose di wireshark ma direttamente in CLI.

```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 6
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
09:02:45.020319 IP 10.0.0.11.40530 > 172.16.0.40.http: Flags [S], seq 1714214819, win 29200, options [mss 1460,sackOK,TS val 3706050147 ecr 0,nop,wscale
09:02:45.020366 IP 172.16.0.40.http > 10.0.0.11.40530: Flags [S.], seq 1717130966, ack 1714214820, win 28960, options [mss 1460,sackOK,TS val 373929955
09:02:45.020375 IP 10.0.0.11.40530 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 3706050147 ecr 3739299551], length 0
09:02:45.020510 IP 10.0.0.11.40530 > 172.16.0.40.http: Flags [P.], seq 1:293, ack 1, win 58, options [nop,nop,TS val 3706050147 ecr 3739299551], length
09:02:45.020519 IP 172.16.0.40.http > 10.0.0.11.40530: Flags [.], ack 293, win 59, options [nop,nop,TS val 3739299551 ecr 3706050147], length 0
09:02:45.020658 IP 172.16.0.40.http > 10.0.0.11.40530: Flags [P.], seq 1:325, ack 293, win 59, options [nop,nop,TS val 3739299551 ecr 3706050147], leng
[analyst@secOps ~]$
```

THANKS FOR THE ATTENTION

MATTIA DI DONATO