**S11-L3 Obiettivi**

Parte 1: Preparare gli Host per Catturare il Traffico

Parte 2: Analizzare i Pacchetti utilizzando Wireshark

Parte 3: Visualizzare i Pacchetti utilizzando tcpdump

**Background / Scenario**

In questo laboratorio, utilizzerai Wireshark per catturare ed esaminare i pacchetti generati tra il browser del PC utilizzando il Protocollo di Trasferimento Ipertestuale (HTTP) e un server web, come www.google.com. Quando un'applicazione, come HTTP o il Protocollo di Trasferimento File (FTP), inizia per la prima volta su un host, TCP utilizza la stretta di mano a tre vie per stabilire una sessione TCP affidabile tra i due host. Ad esempio, quando un PC utilizza un browser web per navigare su internet, viene avviata una stretta di mano a tre vie, e si stabilisce una sessione tra l'host PC e il server web. Un PC può avere sessioni TCP multiple, simultanee e attive con vari siti web.

Nota per l'Istruttore: L'uso di un analizzatore di pacchetti, come Wireshark, può essere considerato una violazione della politica di sicurezza della scuola. Si raccomanda di ottenere il permesso prima di utilizzare Wireshark per questo laboratorio. Se l'uso di un analizzatore di pacchetti è un problema, l'istruttore potrebbe voler assegnare il laboratorio come compito a casa o eseguire una dimostrazione guidata.

Risorse Richieste

Macchina virtuale CyberOps Workstation

Istruzioni

Ecco la traduzione mantenendo il formato:

**Parte 1: Preparare gli Host per Catturare il Traffico**

a. Avvia la VM CyberOps. Accedi con il nome utente \*\*analyst\*\* e la password \*\*cyberops\*\*.

b. Avvia Mininet.

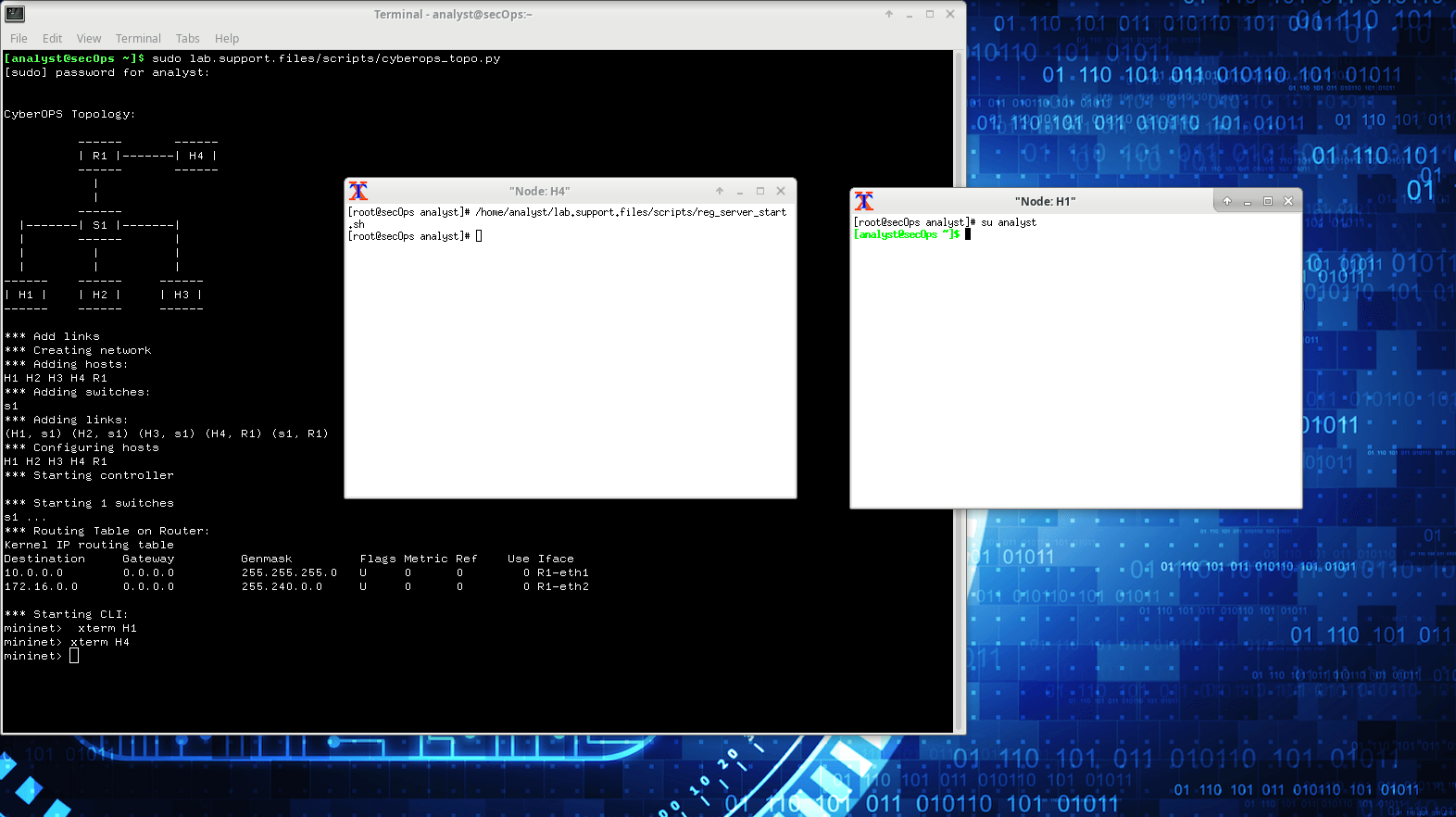
[analyst@secOps ~]$ sudo lab.support.files/scripts/cyberops\_topo.py

c. Avvia gli host H1 e H4 in Mininet.

Starting CLI:

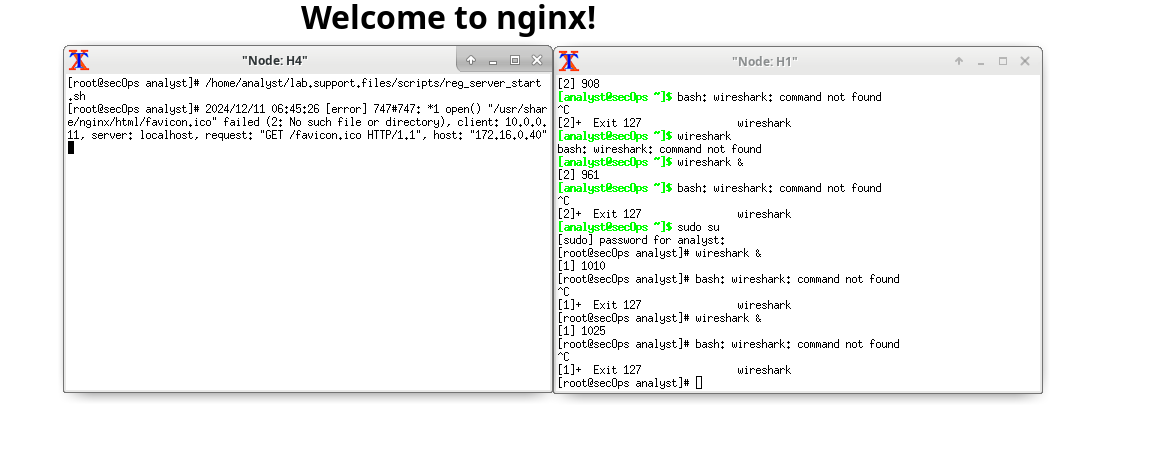
mininet> xterm H1

mininet> xterm H4



d. Avvia il server web su H4.

[root@secOps analyst]# /home/analyst/lab.support.files/scripts/reg\_server\_start.sh

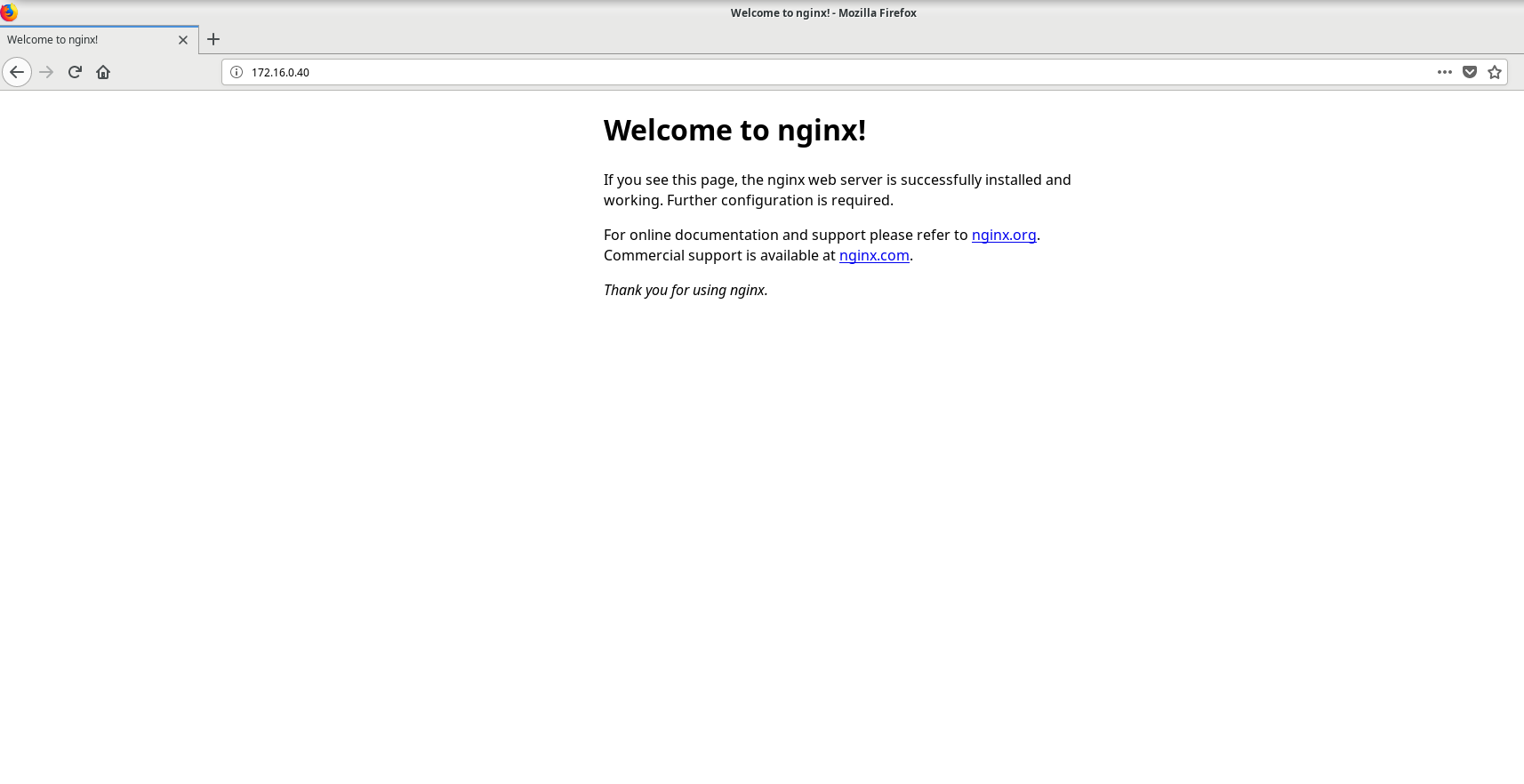


e. Per motivi di sicurezza, non è possibile eseguire Firefox dall'account utente root. Su H1, usa il comando \*\*switch user\*\* per passare dall'utente root all'utente analyst:

[root@secOps analyst]# su analyst

f. Avvia il browser web su H1. Questo richiederà alcuni momenti.

[analyst@secOps ~]$ firefox &

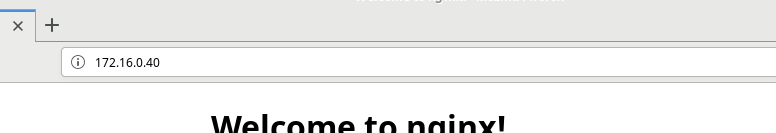


g. Dopo che la finestra di Firefox si apre, avvia una sessione \*\*tcpdump\*\* nel terminale del nodo H1 e invia l'output a un file chiamato \*\*capture.pcap\*\*. Con l'opzione \*\*-v\*\*, puoi osservare i progressi. Questa cattura si fermerà automaticamente dopo aver catturato 50 pacchetti, grazie all'opzione \*\*-c 50\*\*.

[analyst@secOps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap

```

h. Dopo aver avviato \*\*tcpdump\*\*, naviga rapidamente a \*\*172.16.0.40\*\* nel browser web Firefox.



**Parte 2: Analizzare i Pacchetti utilizzando Wireshark**

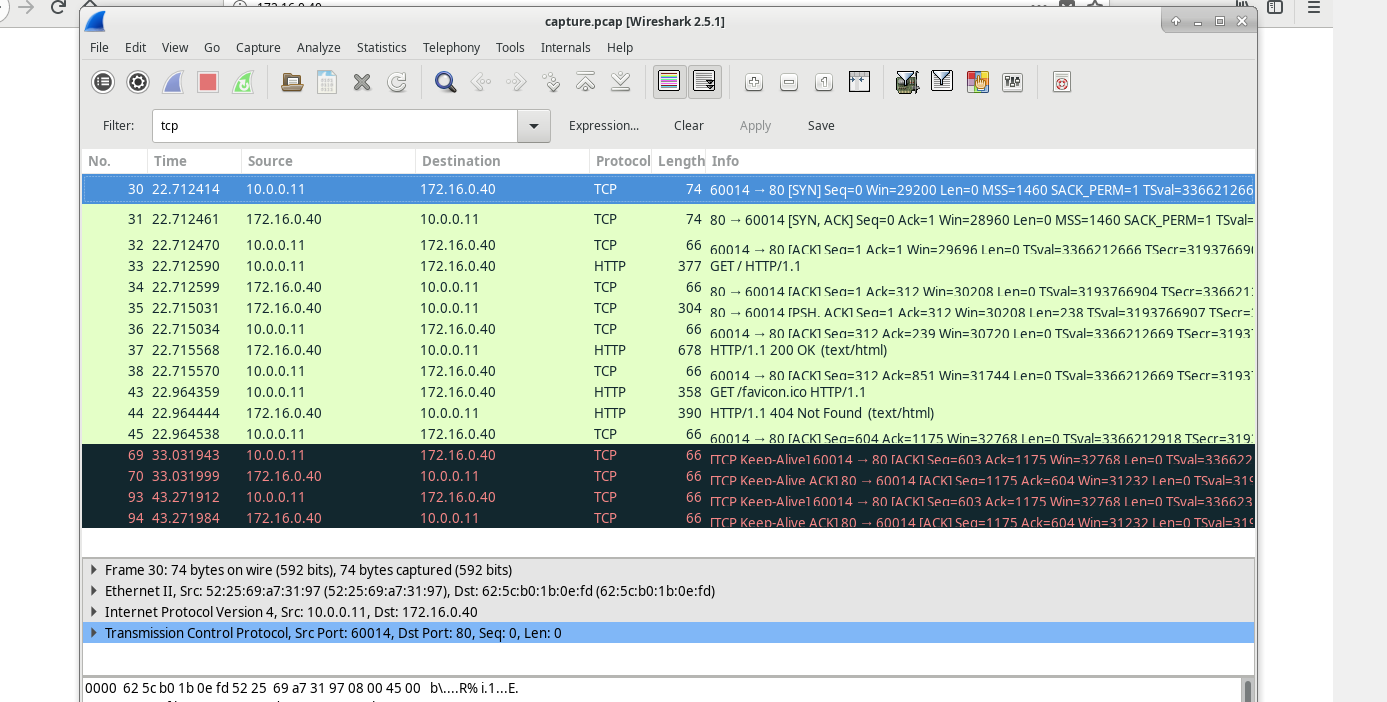
Passaggio 1: Applicare un filtro alla cattura salvata.

a. Premi \*\*INVIO\*\* per visualizzare il prompt. Avvia Wireshark sul nodo H1. Fai clic su \*\*OK\*\* quando viene visualizzato l'avviso relativo all'esecuzione di Wireshark come superutente.

[analyst@secOps ~]$ wireshark &

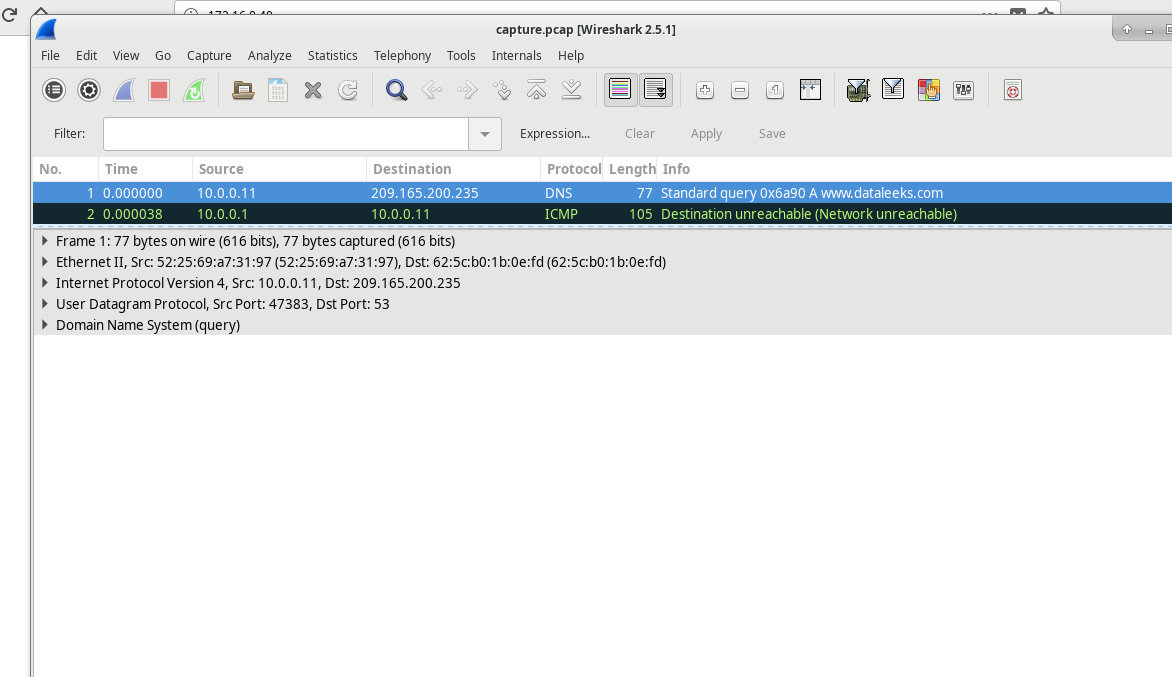
b. In Wireshark, fai clic su \*\*File > Open\*\*. Seleziona il file pcap salvato situato in \*\*/home/analyst/capture.pcap\*\*.

c. Applica un filtro \*\*tcp\*\* alla cattura. In questo esempio, i primi 3 frame rappresentano il traffico di interesse.



Passaggio 2: Esaminare le informazioni all'interno dei pacchetti, inclusi indirizzi IP, numeri di porta TCP e flag di controllo TCP.

a. In questo esempio, il \*\*frame 1\*\* rappresenta l'inizio della stretta di mano a tre vie tra il PC e il server su H4. Nel riquadro dell'elenco dei pacchetti (sezione superiore della finestra principale), seleziona il primo pacchetto, se necessario.



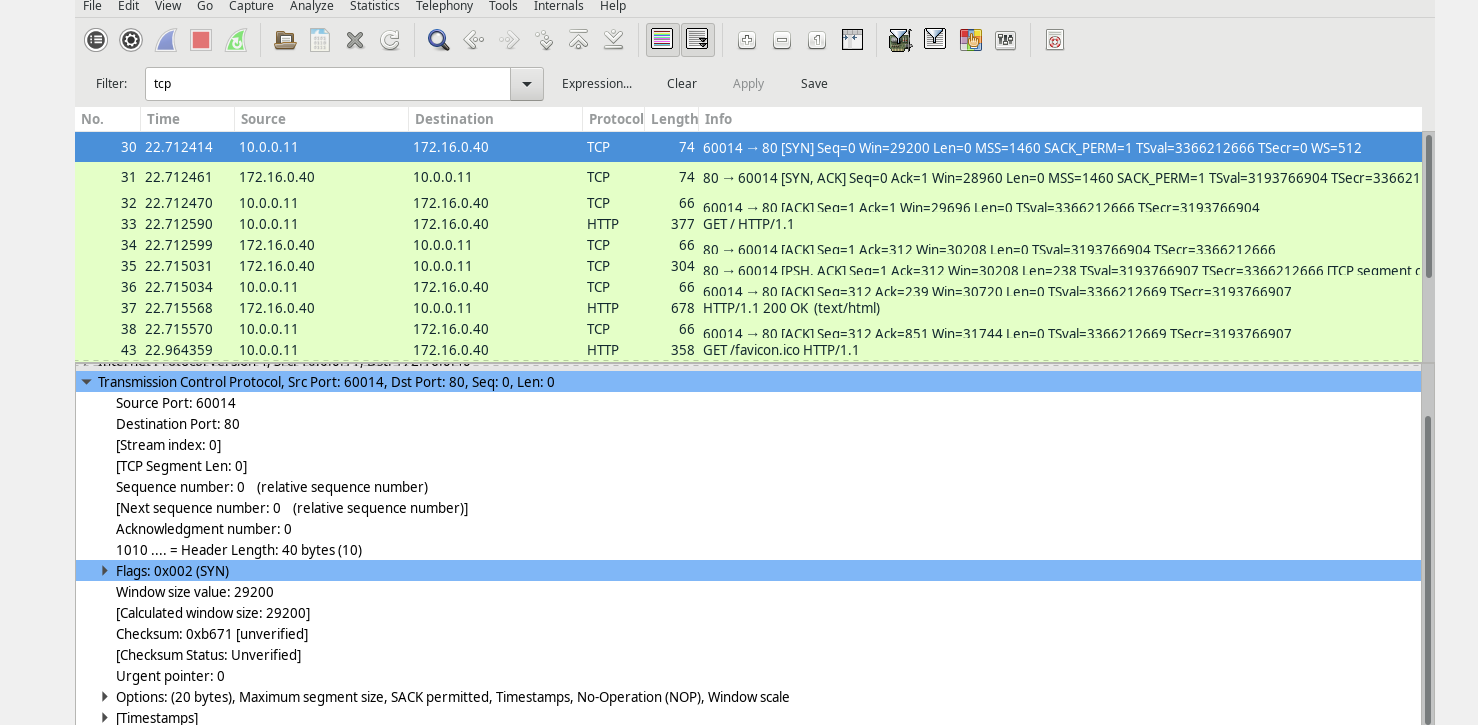
b. Clicca sulla freccia a sinistra del \*\*Transmission Control Protocol\*\* nel riquadro dei dettagli del pacchetto per espanderlo ed esaminare le informazioni TCP. Individua le informazioni sulla porta sorgente e di destinazione.

c. Clicca sulla freccia a sinistra dei \*\*Flags\*\*. Un valore pari a \*\*1\*\* indica che il flag è impostato. Individua il flag impostato in questo pacchetto.

\*\*Nota\*\*: Potrebbe essere necessario regolare le dimensioni delle finestre superiore e centrale in Wireshark per visualizzare le informazioni necessarie.

### Qual è il numero di porta sorgente TCP?

Le risposte possono variare. In questo esempio, la porta sorgente è \*\*58716\*\*.



Come classificheresti la porta sorgente?

\*\*Dinamica\*\* o \*\*Privata\*\*

Qual è il numero di porta di destinazione TCP?

\*\*Porta 80\*\*

Come classificheresti la porta di destinazione?

\*\*Ben nota\*\*, registrata (\*\*HTTP\*\* o protocollo web)

Quale flag (o quali flag) è impostato?

\*\*Flag SYN\*\*

A quale valore è impostato il numero di sequenza relativo?

\*\*0\*\*

d. Seleziona il pacchetto successivo nella stretta di mano a tre vie.

In questo esempio, si tratta del \*\*frame 2\*\*. Questo è il server web che risponde alla richiesta iniziale per avviare una sessione.

Quali sono i valori delle porte sorgente e di destinazione?

La porta sorgente è ora \*\*80\*\*, e la porta di destinazione è ora \*\*58716\*\*.

Quali flag sono impostati?

Il \*\*flag di riconoscimento (ACK)\*\* e il \*\*flag SYN\*\*.

A quali valori sono impostati i numeri relativi di sequenza e riconoscimento?

Il numero relativo di sequenza è \*\*0\*\*, e il numero relativo di riconoscimento è \*\*1\*\*.

e. Infine, seleziona il terzo pacchetto della stretta di mano a tre vie.

Esamina il terzo e ultimo pacchetto della stretta di mano.

Quale flag (o quali flag) è impostato?

\*\*Flag di riconoscimento (ACK)\*\*

I numeri relativi di sequenza e riconoscimento sono impostati a \*\*1\*\* come punto di partenza. La connessione TCP è stabilita e la comunicazione tra il computer sorgente e il server web può iniziare.

Ecco la traduzione del testo:

**Parte 3: Visualizzare i pacchetti utilizzando tcpdump**

Puoi anche visualizzare il file pcap e filtrare per ottenere le informazioni desiderate.

a. Aprire una nuova finestra del terminale e digitare \*\*man tcpdump\*\*.

\*\*Nota\*\*: Potrebbe essere necessario premere \*\*INVIO\*\* per visualizzare il prompt.

Usando le pagine del manuale disponibili nel sistema operativo Linux, puoi leggere o cercare attraverso le opzioni per selezionare le informazioni desiderate dal file pcap.

[analyst@secOps ~]$ man tcpdump

\*\*TCPDUMP(1)\*\*

Manuale dei comandi generali \*\*TCPDUMP(1)\*\*

\*\*NOME\*\*

tcpdump - cattura il traffico su una rete

\*\*SINOSSI\*\*

tcpdump [ -AbdDefhHIJKlLnNOpqStuUvxX# ] [ -B buffer\_size ]

[ -c count ]

[ -C file\_size ] [ -G rotate\_seconds ] [ -F file ]

[ -i interface ] [ -j tstamp\_type ] [ -m module ] [ -M secret ]

[ --number ] [ -Q in|out|inout ]

[ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]

[ -W filecount ]

[ -E spi@ipaddr algo:secret,... ]

[ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]

[ --time-stamp-precision=tstamp\_precision ]

[ --immediate-mode ] [ --version ]

[ expression ]

Per cercare nelle pagine del manuale, puoi usare \*\*/\*\* (cerca in avanti) o \*\*?\*\* (cerca all’indietro) per trovare termini specifici, e \*\*n\*\* per passare al prossimo risultato o \*\*q\*\* per uscire.

Ad esempio, cerca informazioni sull’opzione \*\*-r\*\*, digitando \*\*/-r\*\*. Digita \*\*n\*\* per spostarti al prossimo risultato.

Cosa fa l’opzione -r?\*\*

L’opzione \*\*-r\*\* consente di leggere i pacchetti da un file salvato utilizzando l’opzione \*\*-w\*\* di tcpdump o altri strumenti che generano file pcap o pcap-ng, come Wireshark.

b. Nello stesso terminale, apri il file di cattura utilizzando il seguente comando per visualizzare i primi 3 pacchetti TCP catturati:

[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3

\*\*Output\*\*:

reading from file capture.pcap, link-type EN10MB (Ethernet)

13:58:30.647462 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [S], seq 2432755549, win 29200, options [mss 1460,sackOK,TS val 3864513189 ecr 0,nop,wscale 9], length 0

13:58:30.647543 IP 172.16.0.40.http > 10.0.0.11.58716: Flags [S.], seq 1766419191, ack 2432755550, win 28960, options [mss 1460,sackOK,TS val 50557410 ecr 3864513189,nop,wscale 9], length 0

13:58:30.647544 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 3864513189 ecr 50557410], length 0

Per visualizzare la stretta di mano a tre vie, potrebbe essere necessario aumentare il numero di linee dopo l'opzione \*\*-c\*\*.

c. Navigare nel terminale usato per avviare Mininet. Termina Mininet digitando \*\*quit\*\* nella finestra principale del terminale CyberOps VM.

mininet> quit

Stopping 0 controllers

Stopping 2 terms

Stopping 5 links

.....

\*\*\* Stopping 1 switches

s1

\*\*\* Stopping 5 hosts

H1 H2 H3 H4 R1

\*\*\* Done

[analyst@secOps ~]$

d. Dopo aver terminato Mininet, inserisci \*\*sudo mn -c\*\* per pulire i processi avviati da Mininet. Inserisci la password \*\*cyberops\*\* quando richiesto.

[analyst@secOps ~]$ sudo mn -c

[sudo] password for analyst: