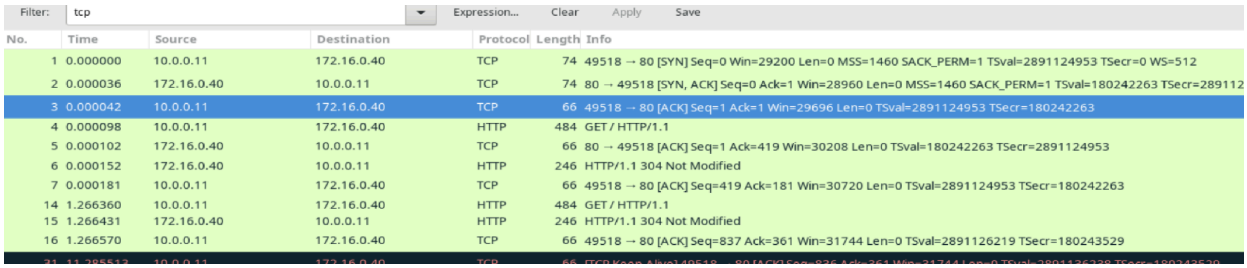
https://itexamanswers.net/9-2-6-lab-using-wireshark-to-observe-the-tcp-3-way-handshake-answers.htmlà

Esercizio personale Risultato:



Procedimento:

Parte 1: Preparare gli host per acquisire il traffico

un. Avviare la VM CyberOps. Accedi con il nome utente **dell'analista** e la password **cyberops**.

b. Avviare Mininet.

```
[analyst@secOps ~]$ sudo lab.support.files/scripts/cyberops_topo.py
```

c. Avviare l'host H1 e H4 in Mininet.

```
*** Starting CLI:
mininet> xterm H1

mininet> xterm H4
```

d. Avviare 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. Sull'host H1, utilizzare il comando switch user per passare dall'utente root all'account utente analista:

```
[root@secOps analyst]# su analyst
```

f. Avvia il browser web su H1. Ci vorranno alcuni istanti.

```
[analyst@secOps ~]$ firefox &
```

g. Dopo l'apertura della finestra di Firefox, avviare una sessione tcpdump nel **terminale Node: H1** e inviare l'output a un file chiamato **capture.pcap**. Con l'opzione -v, puoi guardare i progressi. Questa acquisizione si interromperà dopo l'acquisizione di 50 pacchetti, poiché è configurata con l'opzione -c 50.

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

h. Dopo l'avvio di tcpdump, passare rapidamente a 172.16.0.40 nel browser Web Firefox.

Parte 2: Analisi dei pacchetti con Wireshark

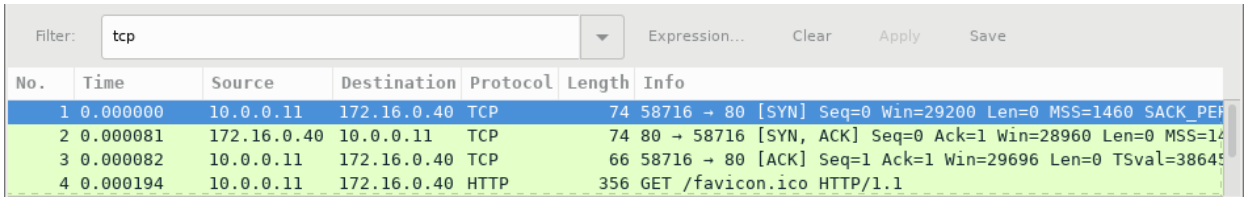
Passaggio 1: applica un filtro all'acquisizione salvata.

un. Premere INVIO per visualizzare il prompt. Avviare Wireshark sul **nodo: H1**. Fare clic su **OK** quando viene visualizzato l'avviso relativo all'esecuzione di Wireshark come utente avanzato.

```
[analyst@secOps ~]$ wireshark &
```

b. In Wireshark, fare clic **su File > Apri**. Selezionare il file pcap salvato che si trova in /home/analyst/capture.pcap.

c. Applicare un filtro tcp all'acquisizione. In questo esempio, i primi 3 frame sono il traffico interessato.



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

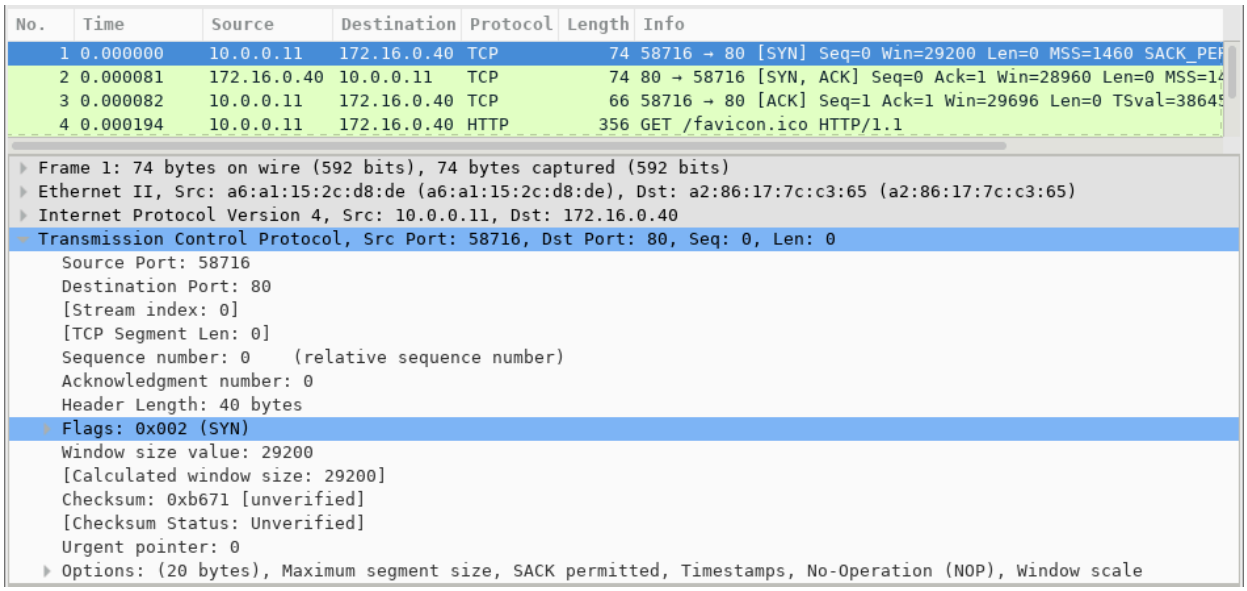
un. In questo esempio, il frame 1 è l'inizio dell'handshake a tre vie tra il PC e il server su H4. Nel riquadro dell'elenco dei pacchetti (sezione superiore della finestra principale), selezionare il primo pacchetto, se necessario.

b. Fare clic sulla **freccia** a sinistra del protocollo di controllo della trasmissione nel riquadro dei dettagli del pacchetto per espanderlo ed esaminare le

informazioni TCP. Individuare le informazioni sulla porta di origine e di destinazione.

c. Fare clic sulla **freccia** a sinistra delle bandiere. Il valore 1 indica che il flag è impostato. Individuare il flag impostato in questo pacchetto.

Nota: Potrebbe essere necessario regolare le dimensioni delle finestre superiore e centrale all'interno di Wireshark per visualizzare le informazioni necessarie.



Qual è il numero di porta di origine TCP?

Le risposte possono variare. Nell'esempio, la porta di origine è 58716.

Come classificheresti il porting di origine?

Dinamico o privato

Qual è il numero di porta di destinazione TCP?

Porta 80

Come classificheresti il porto di destinazione?

Noto, registrato (protocollo HTTP o web)

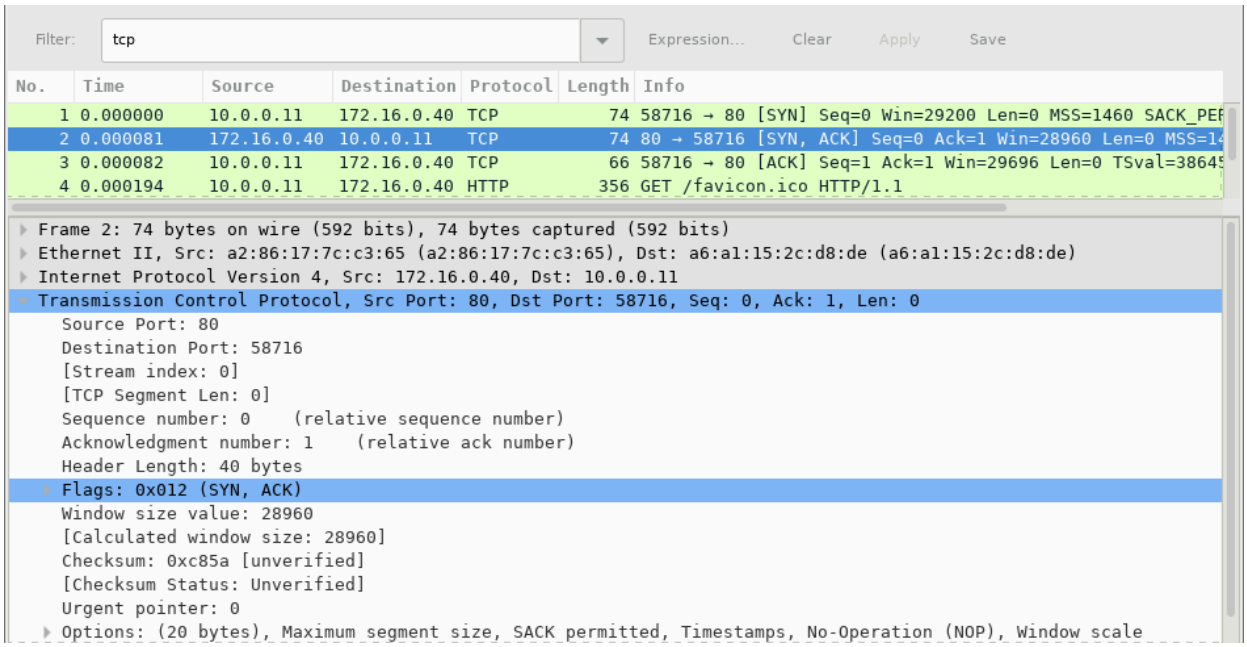
Quale flag (o bandiere) è impostato?

Flag SYN

Su cosa è impostato il numero di sequenza relativo?

0

d. Selezionare il pacchetto successivo nell'handshake a tre vie. Nell'esempio, si tratta del fotogramma 2. Questo è il server web che risponde alla richiesta iniziale di avviare una sessione.



Quali sono i valori delle porte di origine e di destinazione?

La porta di origine è ora 80 e la porta di destinazione è ora 58716

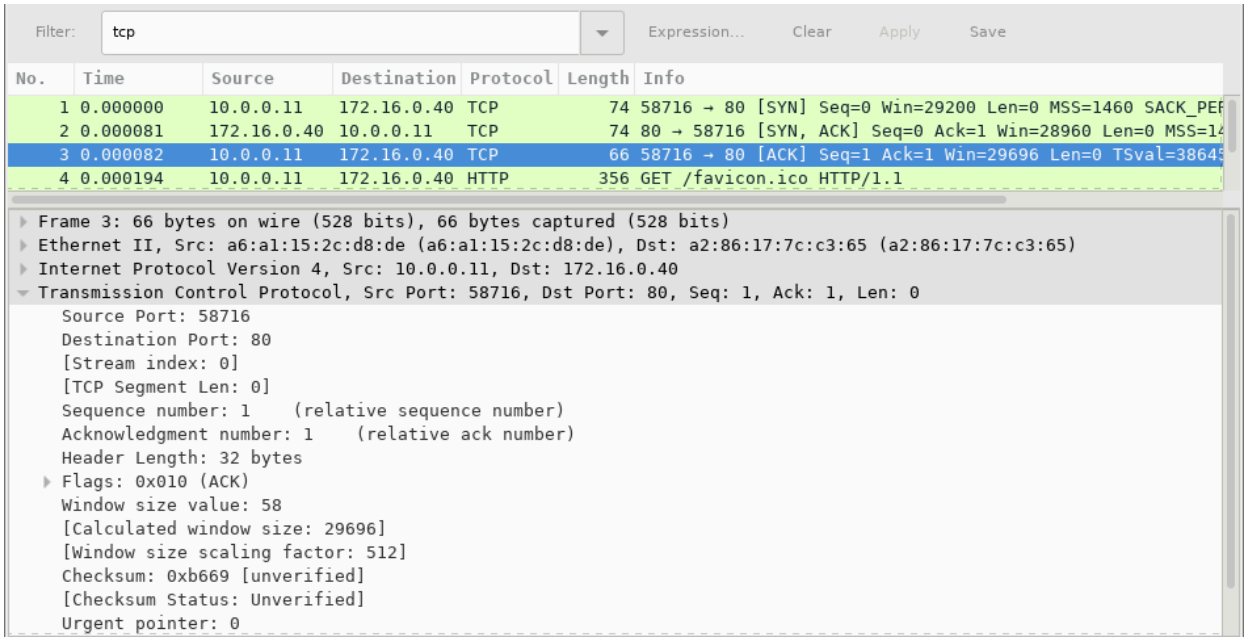
Quali flag sono impostati?

Il flag di riconoscimento (ACK) e il flag Syn (SYN)

Su cosa sono impostati i numeri di sequenza e di riconoscimento relativi?

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

e. Infine, selezionare il terzo pacchetto nell'handshake a tre vie.



Esamina il terzo e ultimo pacchetto della stretta di mano.

Quale flag (o bandiere) è impostato?

Flag di riconoscimento (ACK)

I numeri di sequenza e di riconoscimento relativi sono impostati su 1 come punto di partenza. Viene stabilita la connessione TCP e può iniziare la comunicazione tra il computer di origine e il server Web.

Parte 3: Visualizzare i pacchetti utilizzando tcpdump

È inoltre possibile visualizzare il file pcap e filtrare per le informazioni desiderate.

un. Apri una nuova finestra del terminale, inserisci . **Nota:** Potrebbe essere necessario premere INVIO per visualizzare il prompt.`man tcpdump`

Utilizzando le pagine di manuale disponibili con il sistema operativo Linux, è possibile leggere o cercare tra le pagine di manuale le opzioni per selezionare le informazioni desiderate dal file pcap.

```
[analyst@secOps ~]$ man tcpdump
TCPDUMP(1)                General Commands Manual                TCPDUMP(1)

NAME
       tcpdump - dump traffic on a network
```

```
SYNOPSIS
       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 ]
<some output omitted>
```

Per cercare tra le pagine man, si può usare / (cercando in avanti) o ? (cercando all'indietro) per trovare termini specifici, e n per andare avanti alla corrispondenza successiva e q per uscire. Ad esempio, cerca le informazioni sull'opzione -r, digita /-r. Digita n per passare alla corrispondenza successiva.

Cosa fa l'opzione -r?

L'opzione -r consente di leggere il pacchetto dal file che è stato salvato utilizzando l'opzione -w con tcpdump o altri strumenti che scrivono file pcap o pcap-ng, come Wireshark.

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

```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
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 l'handshake a 3 vie, potrebbe essere necessario aumentare il numero di righe dopo l'opzione -c.

c. Passare al terminale utilizzato per avviare Mininet. Termina il Mininet inserendo 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 chiuso Mininet, entra per ripulire i processi avviati da Mininet. Inserisci la password **cyberops** quando richiesto.`sudo mn -c`

[analyst@secOps ~]$ sudo mn -c

[sudo] password for analyst:

Opzionale:

https://itexamanswers.net/10-4-3-lab-using-wireshark-to-examine-tcp-and-udp-captures-answers.html