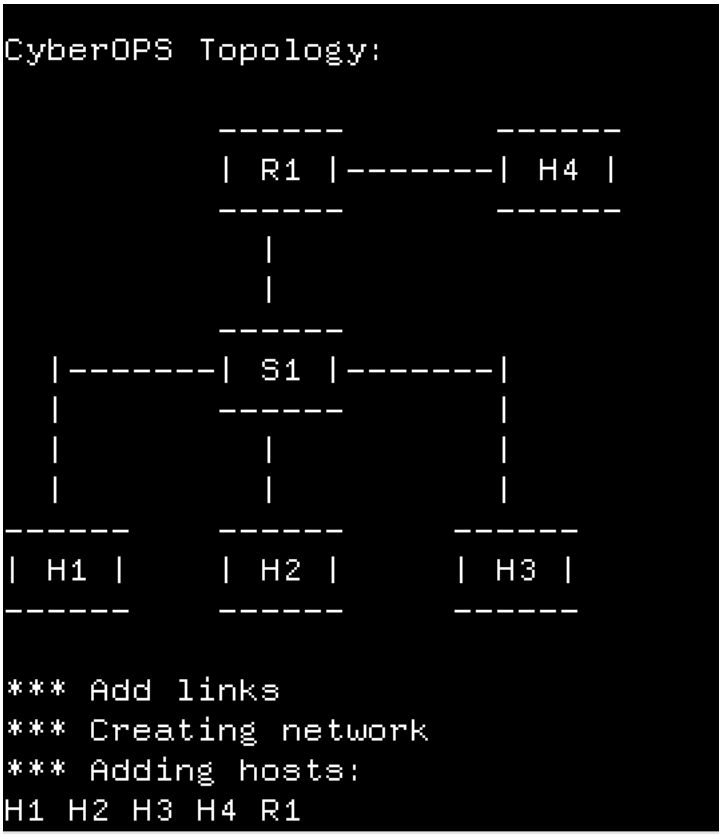
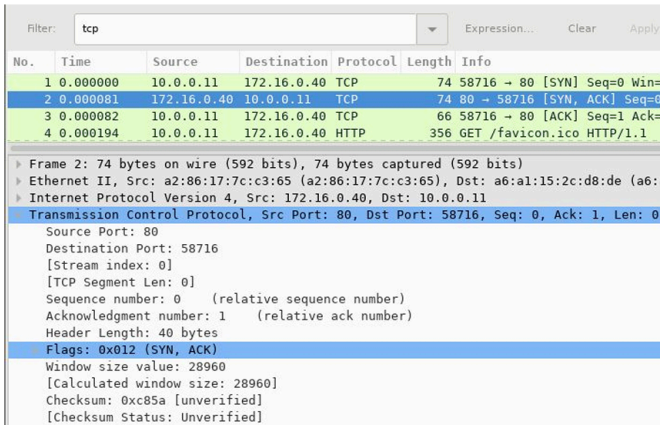


Usare Wireshark per Osservare l'Handshake a 3 Vie TCP

PDF Embed API

- **Qual è il numero di porta TCP di origine?**
- **Come classificheresti la porta di origine?**
- **Qual è il numero di porta TCP di destinazione?**
- **Come classificheresti la porta di destinazione?**
- **Quale flag è impostato?**
- **A quale valore è impostato il numero di sequenza relativo?**

d. Selezionare il pacchetto successivo nell'handshake a tre vie. In questo esempio, è il frame 2. Questa è la risposta del server web alla richiesta iniziale di avviare una sessione.



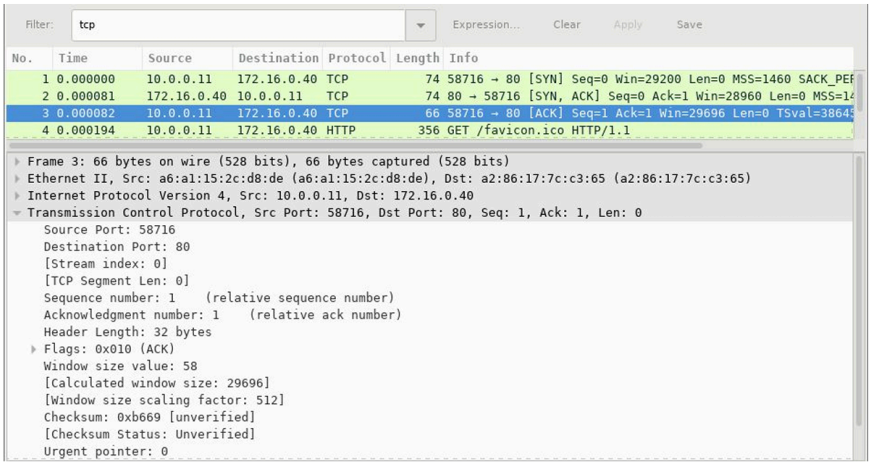
- **Quali sono i valori delle porte di origine e destinazione?**
- **Quali flag sono impostati?**
- **A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?**

1) 43914
2) Effimera perché generata dinamicamente per fare l'handshake, non è una porta (nota) standard come può essere la porta 80
3) 80
4) Porta nota
5) SYN
6) 0

7) 80 origine e destinazione 43914
8) SYN,ACK
9) 0 relative sequence number e acknowledgment 1

---

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



Esaminare il terzo e ultimo pacchetto dell'handshake.

Quale flag è impostato?

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

10) Sono entrambi impostati a 1

Parte 3: Visualizzare i pacchetti usando tcpdump

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

a. Aprire una nuova finestra di terminale, inserire `man tcpdump`. Nota: Potrebbe essere necessario premere INVIO per vedere il prompt.

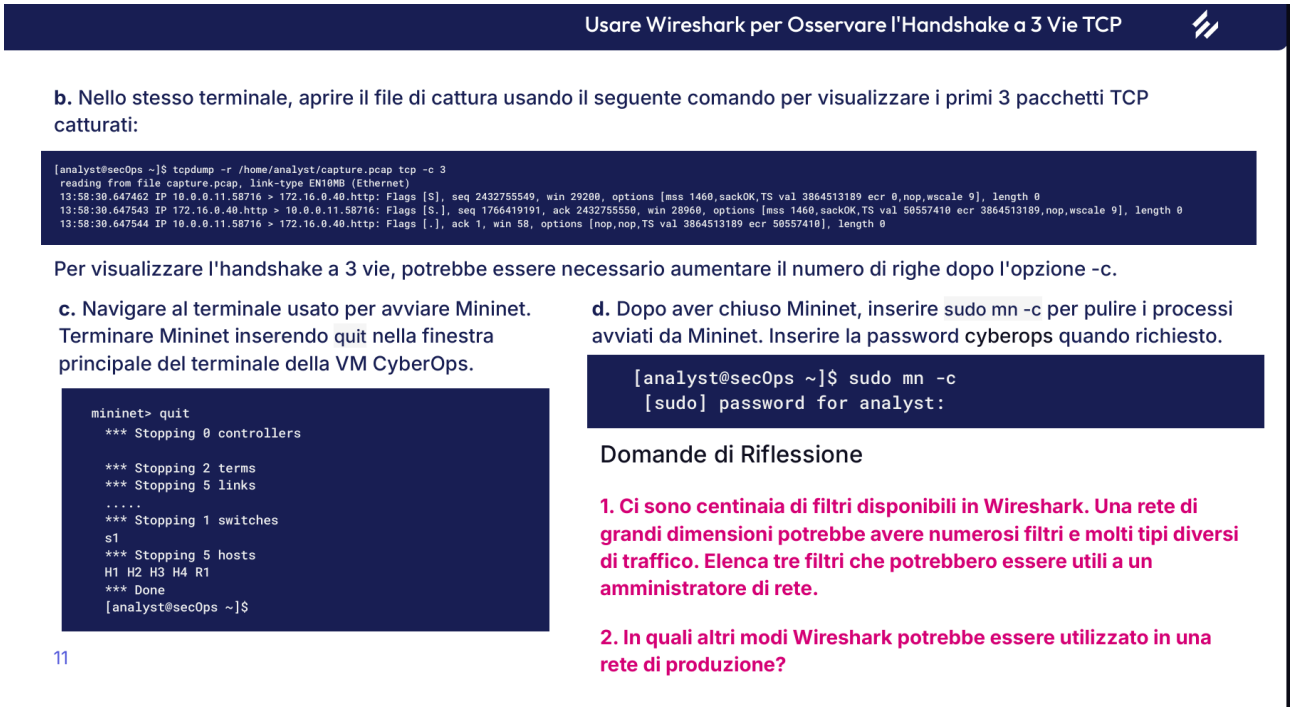
Utilizzando le pagine manuale (man pages) disponibili con il sistema operativo Linux, è possibile leggere o cercare tra le pagine manuale le opzioni per selezionare le informazioni desiderate dal file pcap.

```
[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 ]
  <output omesso>
```

Per cercare nelle pagine man, è possibile usare / (ricerca in avanti) o ? (ricerca indietro) per trovare termini specifici, n per passare alla corrispondenza successiva e q per uscire. Ad esempio, per cercare informazioni sull'opzione -r, digitare /-r. Digitare n per passare alla corrispondenza successiva.

Cosa fa l'opzione -r?

11) l’opzione -r permette di leggere i pacchetti da un file salvato e non da un’interfaccia online



Usare Wireshark per Osservare l'Handshake a 3 Vie TCP

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

```
[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. Navigare al terminale usato per avviare Mininet. Terminare Mininet inserendo quit nella finestra principale del terminale della VM CyberOps.

```
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 ~]$
```

11

d. Dopo aver chiuso Mininet, inserire sudo mn -c per pulire i processi avviati da Mininet. Inserire la password cyberops quando richiesto.

```
[analyst@secOps ~]$ sudo mn -c
 [sudo] password for analyst:
```

Domande di Riflessione

1. Ci sono centinaia di filtri disponibili in Wireshark. Una rete di grandi dimensioni potrebbe avere numerosi filtri e molti tipi diversi di traffico. Elenca tre filtri che potrebbero essere utili a un amministratore di rete.

2. In quali altri modi Wireshark potrebbe essere utilizzato in una rete di produzione?

12) HTTP per analizzare richieste e risposte web, diagnosticare problemi con server o client,
IP ADDR == per monitorare o risolvere problemi legati a un host specifico della rete,
TCP.PORT == per verificare la corretta comunicazione di servizi specifici (ad esempio server web sicuri, applicazioni aziendali).

13) **Risoluzione dei problemi**

- Identificare latenze o ritardi o pacchetti persi analizzando i tempi di risposta (es. handshake TCP lenti).
- Diagnosticare errori di configurazione (es. VLAN, routing, DHCP non funzionante).

Analisi delle performance

- Monitoraraggio di applicazioni o servizi.
- Controllare la qualità delle connessioni (ritardi in VoIP).

Sicurezza e monitoraggio

- Rilevare traffico sospetto o anomalo (es. scansioni di porte, tentativi di exploit).
- Analizzare connessioni non autorizzate o uso di protocolli non consentiti.
- Verificare se i dati sensibili viaggiano in chiaro invece che cifrati.

Documentazione

- Creare report sul traffico di rete per capire quali applicazioni consumano più banda.
- Fornire prove durante incidenti di sicurezza o dispute di rete.

Supporto alla configurazione e testing

- Verificare il corretto funzionamento dopo cambi di configurazione (firewall, NAT, VPN).
- Testare nuove applicazioni in ambiente di produzione.