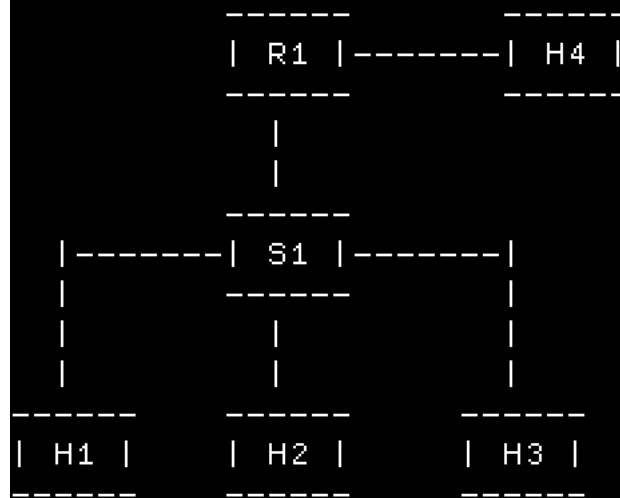


CyberOPS Topology:



```

*** Add links
*** Creating network
*** Adding hosts:
H1 H2 H3 H4 R1
  
```

Usare Wireshark per Osservare l'Handshake a 3 Vie TCP



PDF Embed API

- Qual è il numero di porta TCP di origine?
- Come classifichereesti la porta di origine?
- Qual è il numero di porta TCP di destinazione?
- Come classifichereesti 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?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	58716 → 80 [SYN] Seq=0 Win=
2	0.000081	172.16.0.40	10.0.0.11	TCP	74	80 → 58716 [SYN, ACK] Seq=6
3	0.000082	10.0.0.11	172.16.0.40	TCP	66	58716 → 80 [ACK] Seq=1 Ack=
4	0.000194	10.0.0.11	172.16.0.40	HTTP	356	GET /favicon.ico HTTP/1.1

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)	
Ethernet II, Src: a2:86:17:7c:c3:65 (a2:86:17:7c:c3:65), Dst: a6:a1:15:2c:d8:de (a6:a1:15:2c:d8:de)	
Internet Protocol Version 4, Src: 172.16.0.40, Dst: 10.0.0.11	
Transmission Control Protocol, Src Port: 80, Dst Port: 58716, Seq: 0, Ack: 1, Len: 0	
Source Port: 80	
Destination Port: 58716	
[Stream index: 0]	
[TCP Segment Len: 0]	
Sequence number: 0 (relative sequence number)	
Acknowledgment number: 1 (relative ack number)	
Header Length: 40 bytes	
Flags: 0x012 (SYN, ACK)	
Window size value: 28960	
[Calculated window size: 28960]	
Checksum: 0xc85a [unverified]	
[Checksum Status: Unverified]	

- 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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	58716 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERFECT
2	0.000081	172.16.0.40	10.0.0.11	TCP	74	80 → 58716 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
3	0.000082	10.0.0.11	172.16.0.40	TCP	66	58716 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=38645
4	0.000194	10.0.0.11	172.16.0.40	HTTP	356	GET /favicon.ico HTTP/1.1

Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: a6:a1:15:2c:d8:de (a6:a1:15:2c:d8:de), Dst: a2:86:17:7c:c3:65 (a2:86:17:7c:c3:65)

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

Transmission Control Protocol, Src Port: 58716, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 58716
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header Length: 32 bytes
Flags: 0x010 (ACK)
Window size value: 58
[Calculated window size: 29696]
[Window size scaling factor: 512]
Checksum: 0xb669 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

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 timestamp_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=timestamp_precision ]
    [ --immediate-mode ] [ --version ]
    [ expression ]

<output omissio>
```

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.

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



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

- Monitoraggio 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.