

REPORT S11/L2

Cisco CyberOps 2

Traccia

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

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

Svolgimento

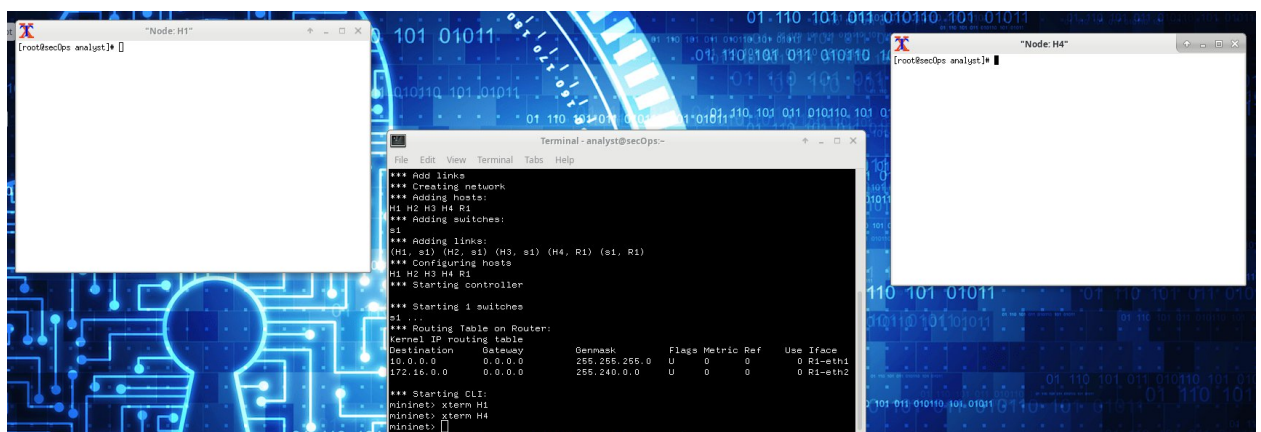
In questo laboratorio, utilizzerai Wireshark per acquisire ed esaminare i pacchetti generati tra il browser del PC e un server Web, utilizzando il protocollo HTTP (HyperText Transfer Protocol). Quando un'applicazione, che usa HTTP o FTP, comunica per la prima volta su un host, viene usata la stretta di mano a tre vie (3way handshake) per stabilire una sessione TCP affidabile tra i due host. Ad esempio, quando un PC utilizza un browser Web per navigare in Internet, viene avviata una stretta di mano a tre vie e viene stabilita una sessione tra l'host del PC e il server Web. Un PC può avere sessioni TCP multiple, simultanee e attive con vari siti Web.

Parte 1: Preparare gli host per catturare il traffico

Avviamo la CyberOps VM. Ci logghiamo con username **analyst** e password **cyberops**.

Avviamo Mininet tramite il comando **sudo lab.support.files/scripts/cyberops_topo.py**

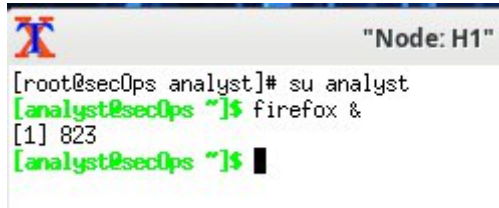
Avviamo gli host H1 e H4 in Mininet con i comandi **xterm H1** e **xterm H4**



Avviamo il web server sul nodo H4:

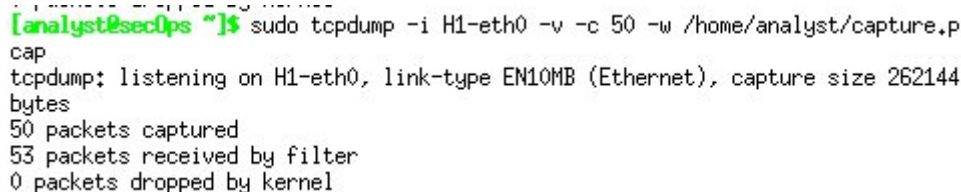
/home/analyst/lab.support.files/scripts/reg_server_start.sh

Per ragioni di sicurezza non possiamo avviare firefox con l'utente root, pertanto sul nodo H1 diamo il comando ***su analyst*** per switchare utente, poi avviamo il browser con il comando ***firefox &***



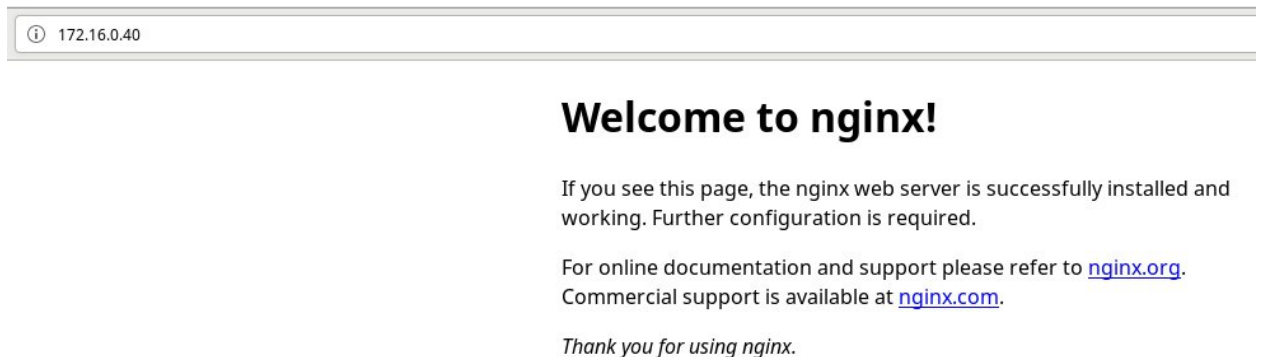
```
[root@secOps analyst]# su analyst
[analyst@secOps ~]$ firefox &
[1] 823
[analyst@secOps ~]$
```

Dopo l'apertura della finestra di Firefox, avviamo una sessione tcpdump nel terminale H1 e inviamo l'output a un file chiamato capture.pcap. Con l'opzione -v (verbose), possiamo guardare i progressi. Questa acquisizione si interromperà dopo aver acquisito 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
tcpdump: listening on H1-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
50 packets captured
53 packets received by filter
0 packets dropped by kernel
```

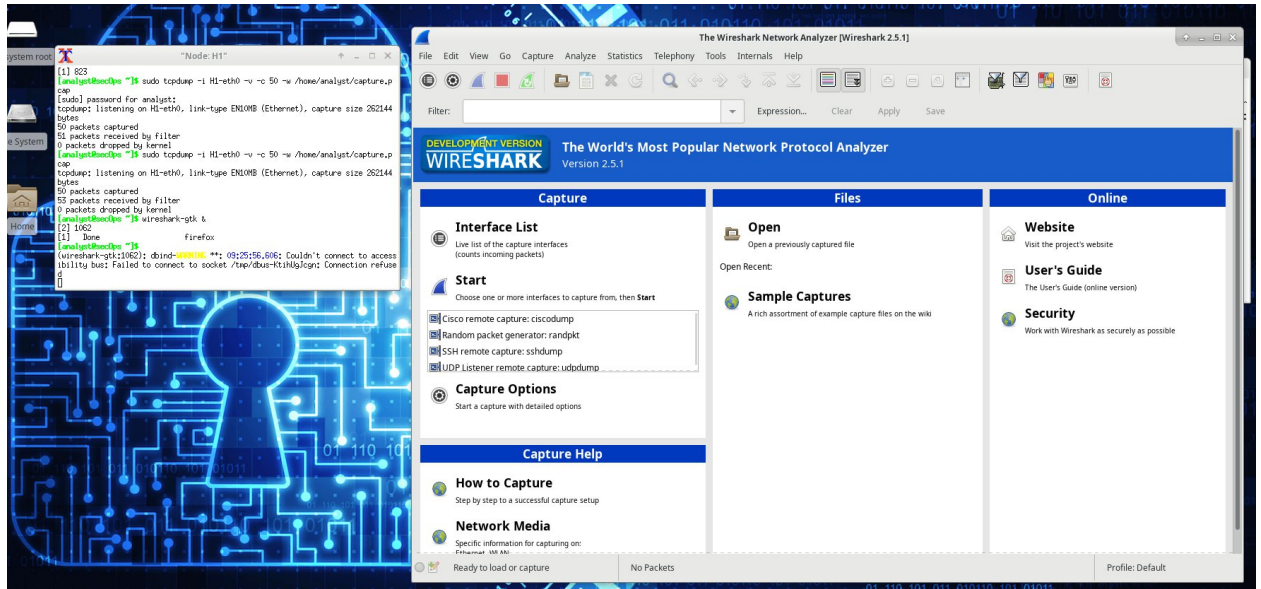
Dopo l'avvio di tcpdump, navighiamo rapidamente fino all'indirizzo 172.16.0.40 nel browser Web Firefox.



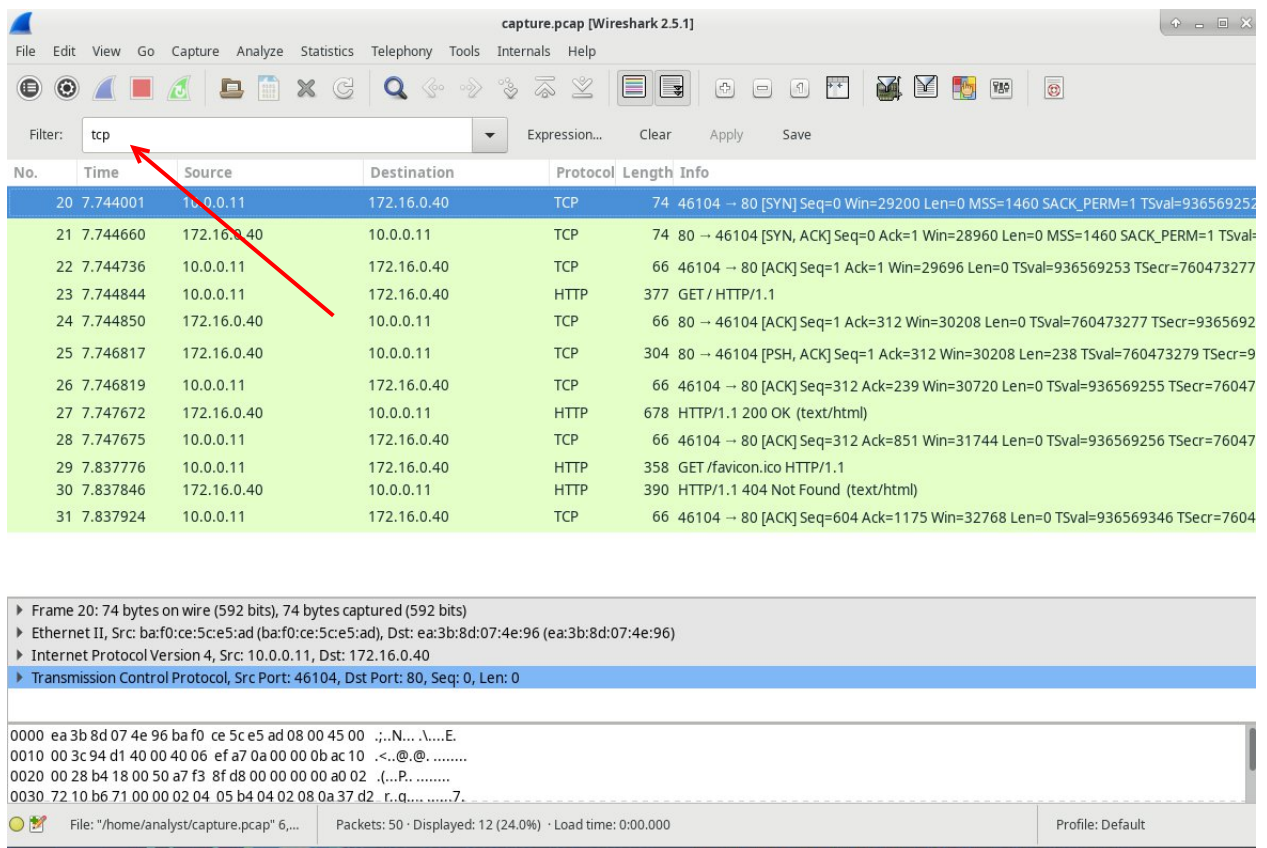
Parte 2: Analizzare i pacchetti utilizzando Wireshark

Passaggio 1: applicare un filtro all'acquisizione salvata.

Avviamo Wireshark sul nodo H1. Premiamo OK quando richiesto dall'avviso relativo all'esecuzione di Wireshark come superutente.



Apriamo ora il file che abbiamo salvato nella Parte 1 e applichiamo il filtro tcp per visualizzare solo i pacchetti scambiati con quel protocollo



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

In questo esempio, il pacchetto 1 è 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), selezionare il primo pacchetto, espandiamo la tendina del menu **Transmission Control Protocol**

20	7.744001	10.0.0.11	172.16.0.40	TCP	74 46104 → 80 [SYN] Seq
21	7.744660	172.16.0.40	10.0.0.11	TCP	74 80 → 46104 [SYN, ACK
22	7.744736	10.0.0.11	172.16.0.40	TCP	66 46104 → 80 [ACK] Seq
23	7.744844	10.0.0.11	172.16.0.40	HTTP	377 GET / HTTP/1.1
24	7.744850	172.16.0.40	10.0.0.11	TCP	66 80 → 46104 [ACK] Seq

▶ Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

▶ Ethernet II, Src: ba:f0:ce:5c:e5:ad (ba:f0:ce:5c:e5:ad), Dst: ea:3b:8d:07:4e:96 (ea:3b:8d:07:4e:96)

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

▼ Transmission Control Protocol, Src Port: 46104, Dst Port: 80, Seq: 0, Len: 0

Source Port: 46104
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1010 = Header Length: 40 bytes (10)

▶ Flags: 0x002 (SYN)
Window size value: 29200
[Calculated window size: 29200]
Checksum: 0xb671 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

Ora espandiamo anche il menu a tendina delle Flags e vediamo Un valore pari a 1. Questo indica che la bandiera è impostata in questo pacchetto.

▼ Flags: 0x002 (SYN)
000. = Reserved: Not set
...0 = Nonce: Not set
... 0... = Congestion Window Reduced (CWR): Not set
.... 0... = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... 0... = Push: Not set
....0.. = Reset: Not set
▶1. = Syn: Set

Riportiamo inoltre che la porta di origine è la 46104 e quella di destinazione ovviamente la 80, avendo usato il protocollo HTTP. La bandiera inoltre è impostata su **SYN**.

Ripetendo queste stesse operazioni per i successivi due pacchetti vediamo che il secondo riporta la bandiera **SYN, ACK** e il terzo è **ACK**.

Parte 3: Visualizza i pacchetti usando tcpdump

Ora analizziamo i pacchetti tramite tcpdump. Avviamolo da una nuova finestra del terminale, e diamo il comando ***tcpdump -r /home/analyst/capture.pcap -c 3***

```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap -c 3
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
09:19:24.247105 IP 10.0.0.11.55330 > 209-165-200-235.got.net.domain: 51146+ A? getpocket.cdn.mozilla.net. (43)
09:19:24.247154 IP 10.0.0.11.55330 > 209-165-200-235.got.net.domain: 42970+ AAAA? getpocket.cdn.mozilla.net. (43)
09:19:25.032366 IP 10.0.0.11.44916 > 209-165-200-235.got.net.domain: 23982+ A? www.google.com. (32)
[analyst@secOps ~]$
```

Vediamo quindi, nelle 3 righe risultanti i tre pacchetti corrispondenti al 3way handshake, che abbiamo sopra analizzato con wireshark.