

Cyber Security & Ethical Hacking

GIORNO 2 – CISCO CYBEROPS

Alejandro Cristino
S13-L2

TRACCIA

Lab - Using Wireshark to Observe the TCP 3-Way Handshake

In this lab, you will complete the following objectives:

- Part 1: Prepare the Hosts to Capture the Traffic
- Part 2: Analyze the Packets using Wireshark
- Part 3: View the Packets using tcpdump

<https://itexamanswers.net/9-2-6-lab-using-wireshark-to-observe-the-tcp-3-way-handshakeanswers.html>

Parte 1: Preparare gli host per catturare il traffico

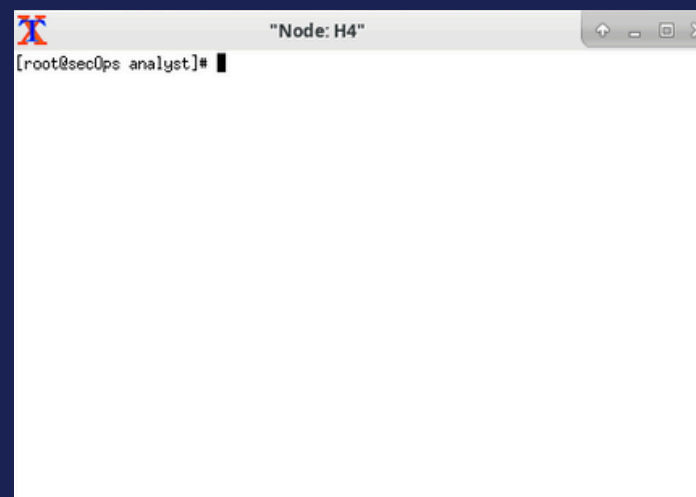
Avviare la VM CyberOps. Accedere con il nome utente analyst e la password cyberops .

1. Avvia Mininet.

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

2. Avviare gli host H1 e H4 in Mininet.

```
*** Starting CLI:  
mininet> xterm H1  
mininet> xterm H4
```

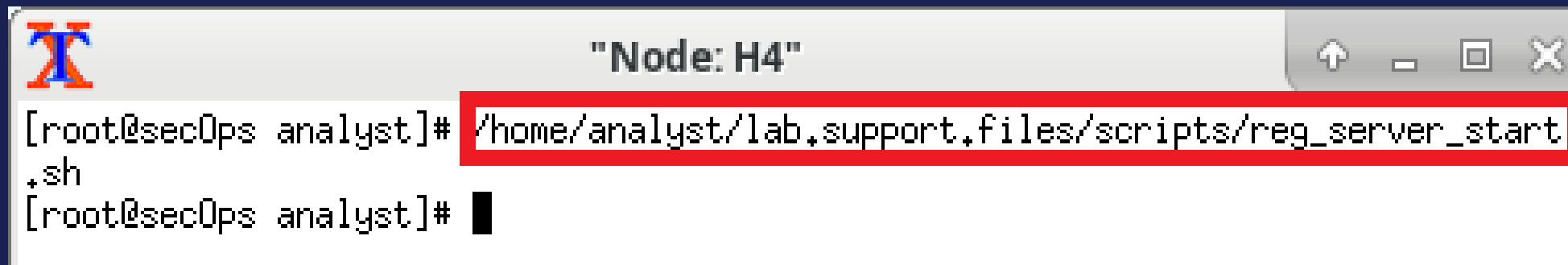


SEGUE



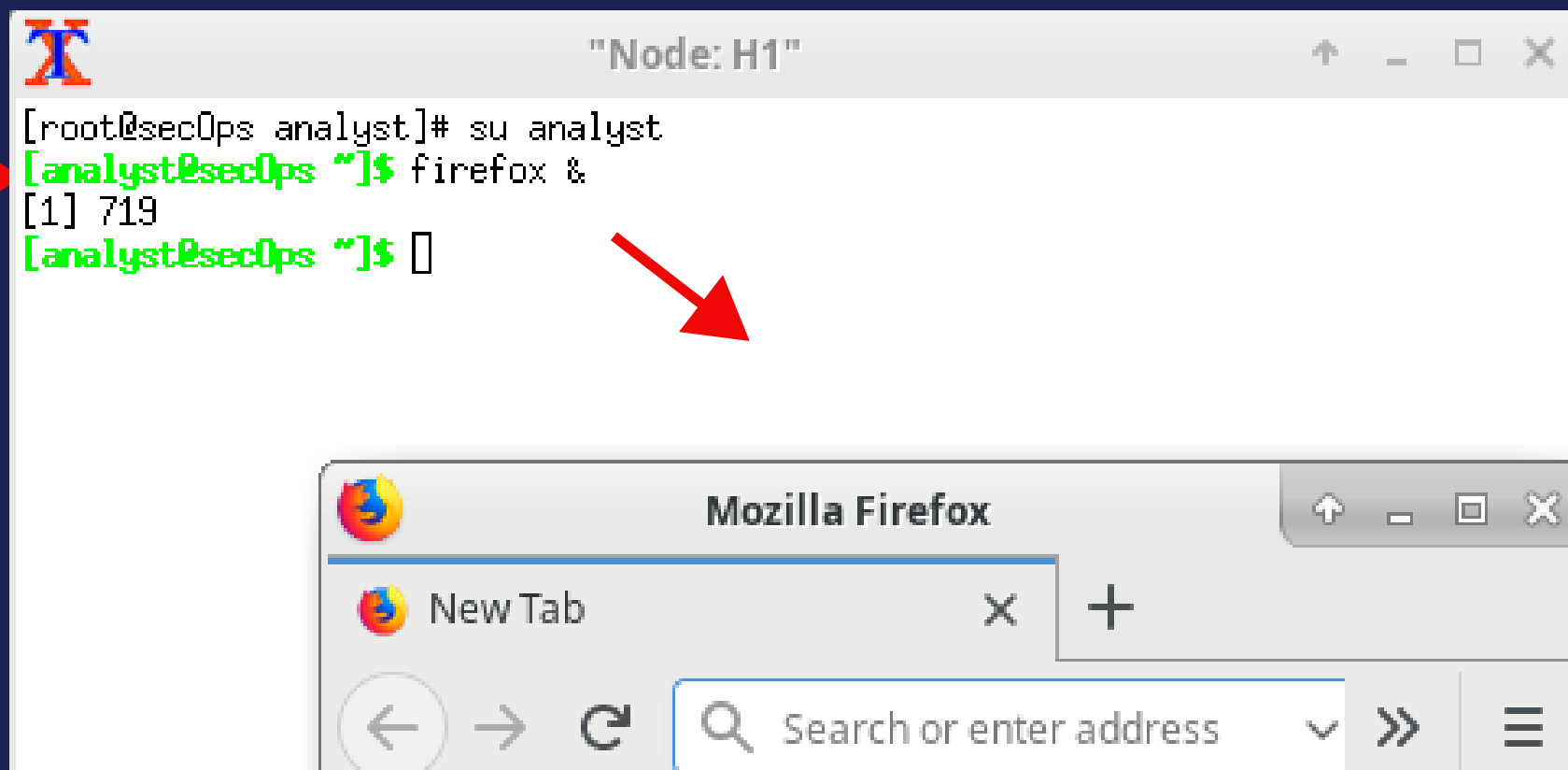
Parte 1: Preparare gli host per catturare il traffico

3. Avviare il server web su H4

A terminal window titled "Node: H4" with a blue and red icon. It shows a root user at secOps analyst prompt. The command `/home/analyst/lab.support.files/scripts/reg_server_start.sh` is entered and highlighted with a red box. The prompt returns to `[root@secOps analyst]#`.

```
[root@secOps analyst]# /home/analyst/lab.support.files/scripts/reg_server_start.sh
[root@secOps analyst]#
```

4. Sull'host H1 eseguire Firefox dall'account utente analyst

A terminal window titled "Node: H1" with a blue and red icon. It shows a root user at secOps analyst prompt. The command `su analyst` is entered. The prompt changes to `[analyst@secOps ~]$`. The command `firefox &` is entered, and the output `[1] 719` is shown. The prompt returns to `[analyst@secOps ~]$`. A red arrow points from the terminal to a Firefox browser window titled "Mozilla Firefox" which has a "New Tab" open. Another red arrow points from the terminal to the browser window.

```
[root@secOps analyst]# su analyst
[analyst@secOps ~]$ firefox &
[1] 719
[analyst@secOps ~]$
```

SEGUE

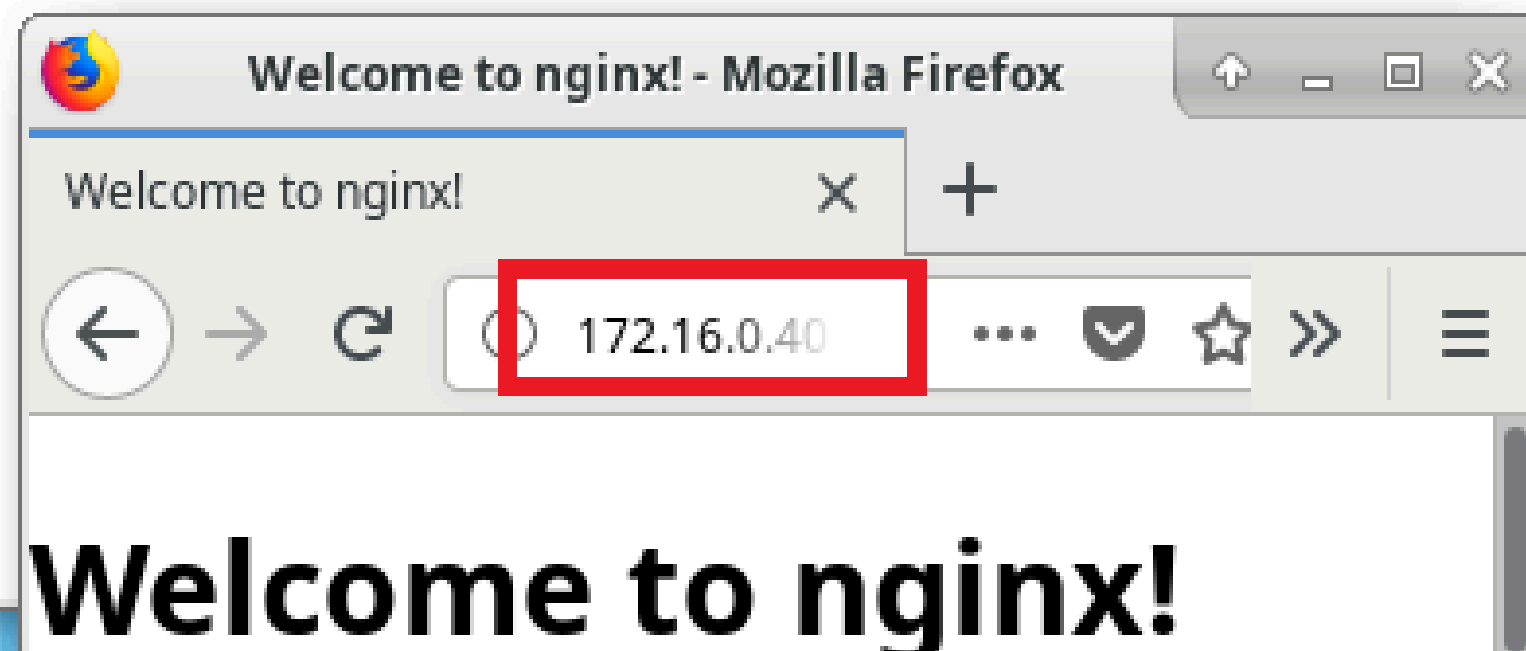


Parte 1: Preparare gli host per catturare il traffico

5. 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.

Dopo l'avvio di tcpdump, accedi rapidamente a 172.16.0.40 nel browser web Firefox.

```
[analyst@secOps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap
[sudo] password for analyst:
tcpdump: listening on H1-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
50 packets captured
51 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```



SEGUE



Parte 2: Analizzare i pacchetti utilizzando Wireshark

1. Avvia Wireshark sul nodo: H1 e fare clic su File > Apri, elezionare il file pcap salvato che si trova in /home/analyst/capture.pcap.



2. In questo esempio, il frame 9 è l'inizio dell'handshake a tre vie tra il PC e il server su H4. Fare clic sulla freccia a sinistra del Transmission Control Protocol nel riquadro dei dettagli del pacchetto per espanderlo ed esaminare le informazioni TCP.

Qual è il numero della porta sorgente TCP?

- 47480

Come classificheresti la porta sorgente?

- Dynamic or private

Qual è il numero della porta di destinazione TCP?

- 80

Come classificheresti il porto di destinazione?

- Porta ben nota, è comunemente utilizzata per HTTP

Quale Flags è impostata?

- SYN

A cosa è impostato il sequence number?

- 0

No.	Time	Source	Destination	Protocol	Length	Info
9	0.734597	10.0.0.11	172.16.0.40	TCP	74	47480 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=9759730
10	0.734696	172.16.0.40	10.0.0.11	TCP	74	80 → 47480 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSva

▶ Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

▶ Ethernet II, Src: fa:b6:a8:29:ce:f8 (fa:b6:a8:29:ce:f8), Dst: 8e:23:8a:0a:f7:90 (8e:23:8a:0a:f7:90)

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

▼ Transmission Control Protocol, Src Port: 47480, Dst Port: 80, Seq: 0, Len: 0

Source Port: 47480
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

▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

▶ [Timestamps]

Parte 2: Analizzare i pacchetti utilizzando Wireshark

3. Selezionando il pacchetto successivo nell'handshake a tre vie. In questo esempio, è il frame 10. Questo è il server web che risponde alla richiesta iniziale di avviare una sessione.

Qual è il numero della porta sorgente?

- 80

Qual è il numero della porta di destinazione?

- 47480

Come classificheresti il porto di destinazione?

- Porta ben nota, è comunemente utilizzata per HTTP

Quale Flags è impostata?

- SYN, ACK

A cosa è impostato il sequence number e relative ack number?

- 0 e 1

9	0.734597	10.0.0.11	172.16.0.40	TCP	74	47480 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSv
10	0.734696	172.16.0.40	10.0.0.11	TCP	74	80 → 47480 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_

- ▶ Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
- ▶ Ethernet II, Src: 8e:23:8a:0a:f7:90 (8e:23:8a:0a:f7:90), Dst: fa:b6:a8:29:ce:f8 (fa:b6:a8:29:ce:f8)
- ▶ Internet Protocol Version 4, Src: 172.16.0.40, Dst: 10.0.0.11
- ▼ Transmission Control Protocol, Src Port: 80, Dst Port: 47480, Seq: 0, Ack: 1, Len: 0
 - Source Port: 80
 - Destination Port: 47480
 - [Stream index: 0]
 - [TCP Segment Len: 0]
 - Sequence number: 0 (relative sequence number)
 - [Next sequence number: 0 (relative sequence number)]
 - Acknowledgment number: 1 (relative ack number)
 - 1010 = Header Length: 40 bytes (10)
 - ▶ Flags: 0x012 (SYN, ACK)
 - Window size value: 28960
 - [Calculated window size: 28960]
 - Checksum: 0xb671 [unverified]
 - [Checksum Status: Unverified]
 - Urgent pointer: 0
 - ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
 - ▶ [SEQ/ACK analysis]
 - ▶ [Timestamps]

Parte 2: Analizzare i pacchetti utilizzando Wireshark

4. selezionare il terzo pacchetto nell'handshake a tre vie. In questo esempio, è il frame 11.

Quale Flags è impostata?

- ACK

A cosa è impostato il sequence number e relative ack number?

- 1 e 1

9	0.734597	10.0.0.11	172.16.0.40	TCP	74	47480 → 80 [SYN] Seq=0 Win=29200 Len=0 M
10	0.734696	172.16.0.40	10.0.0.11	TCP	74	80 → 47480 [SYN, ACK] Seq=0 Ack=1 Win=289
11	0.734705	10.0.0.11	172.16.0.40	TCP	66	47480 → 80 [ACK] Seq=1 Ack=1 Win=29696 L

▶ Frame 11: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

▶ Ethernet II, Src: fa:b6:a8:29:ce:f8 (fa:b6:a8:29:ce:f8), Dst: 8e:23:8a:0a:f7:90 (8e:23:8a:0a:f7:90)

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

▶ Transmission Control Protocol, Src Port: 47480, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 47480

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

1000 = Header Length: 32 bytes (8)

▶ 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

Parte 3: Visualizza i pacchetti utilizzando tcpdump

1. Apri una nuova finestra del terminale e digita `man tcpdump`.

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 /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
09:23:52.892819 IP 10.0.0.11.47480 > 172.16.0.40.http: Flags [S], seq 1302549752, win 292
00, options [mss 1460,sackOK,TS val 975973023 ecr 0,nop,wscale 9], length 0
09:23:52.892918 IP 172.16.0.40.http > 10.0.0.11.47480: Flags [S.], seq 1178185151, ack 13
02549753, win 28960, options [mss 1460,sackOK,TS val 4277512059 ecr 975973023,nop,wscale
9], length 0
09:23:52.892927 IP 10.0.0.11.47480 > 172.16.0.40.http: Flags [.], ack 1, win 58, options
[nop,nop,TS val 975973024 ecr 4277512059], length 0
```

2. Dopo aver chiuso Mininet, `sudo mn -cper` per ripulire i processi avviati da Mininet. Inserisci la password `cyberops` quando richiesto.

```
*** Killing stale mininet node processes
pkill -9 -f mininet:
*** Shutting down stale tunnels
pkill -9 -f Tunnel=Ethernet
pkill -9 -f .ssh/mn
rm -f ~/.ssh/mn/*
*** Cleanup complete.
```

Cyber Security & Ethical Hacking

GRAZIE.