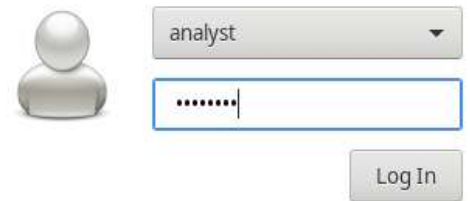


USARE WIRESHARK PER OSSERVARE L'HANDSHAKE A 3 VIE TCP

S11L2

SEGUO UN PASSO ALLA VOLTA QUELLO CHE CI DICE LA TRACCIA, INIZIAMO!!
AVVIO LA VM CYBEROPS, METTENDO LOGIN E PASSWORD.



A login interface for a user named 'analyst'. It features a user icon, a dropdown menu with 'analyst' selected, a password field with masked characters, and a 'Log In' button.

HO AVVIATO GLI HOST H1 E H4 IN MININET.

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

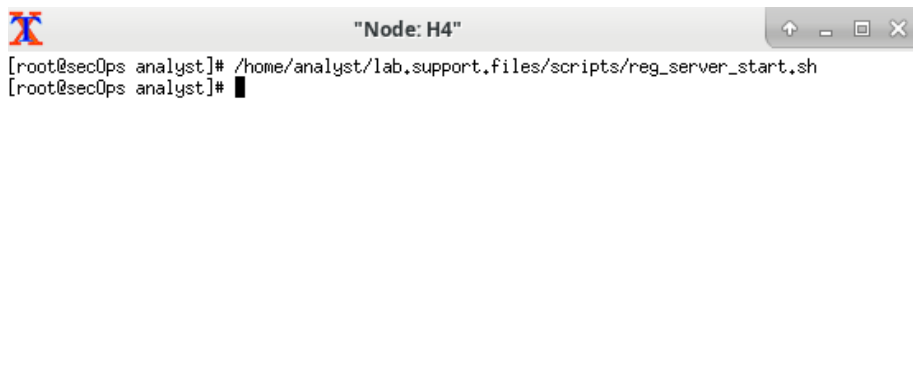
CyberOPS Topology:

  +-----+
  | R1 |-----| H4 |
  +-----+
  |
  |
  +-----+
  | S1 |-----+
  |
  |
  +-----+
  | H1 | | H2 | | H3 |
  +-----+

*** Add links
*** Creating network
*** Add the hosts
```

```
mininet> xterm H1
mininet> xterm H4
```

HO AVVIATO PRIMA IL SERVER WEB SU H4.



A terminal window titled "Node: H4" showing the execution of a script to start a web server. The prompt is [root@secOps analyst]#.

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

SU H1 HO ESEGUITO QUESTI COMANDI, DA QUI PER PASSARE DALL'UTENTE ROOT ALL'ACCOUNT UTENTE ANALYST. CON IL COMANDO FIREFOX & LO AVVIAMO.

```
"Node: H1"
[root@sec0ps analyst]# su analyst
[analyst@sec0ps ~]$ firefox &
```

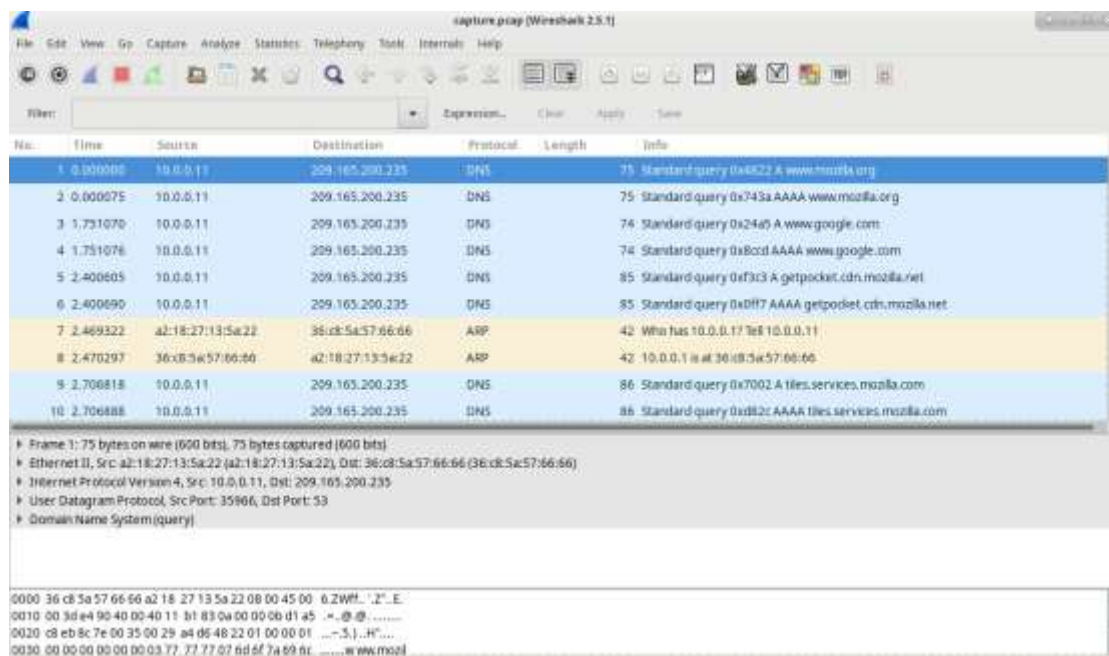
DOPO AVER AVVIATO FIREFOX & HO AVVIATO UNA SESSIONE TCPDUMP

```
[analyst@sec0ps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap
[sudo] password for analyst:
```

DOPO L'AVVIO DI TCPDUMP, HO DIGITATO IMMEDIATAMENTE L'IP 172.16.0.40 NEL BROWSER WEB FIREFOX.



DOPODICHÈ HO QUINDI APERTO WIRESHARK, CON IL COMANDO WIRESHARK-GTK &, E SELEZIONO IL FILE .PCAP



DA QUI APPLICO IL FILTRO TCP

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------|-------------|----------|--------|---|
| 15 | 3.407993 | 10.0.0.11 | 172.16.0.40 | TCP | 74 | 56064 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=60571251 TSecr=53662 |
| 16 | 3.408049 | 172.16.0.40 | 10.0.0.11 | TCP | 74 | 80 → 56064 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=53662 TSecr=60571251 |
| 17 | 3.408058 | 10.0.0.11 | 172.16.0.40 | TCP | 66 | 56064 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=60571251 TSecr=53662 |
| 18 | 3.408262 | 10.0.0.11 | 172.16.0.40 | HTTP | 358 | GET /favicon.ico HTTP/1.1 |
| 19 | 3.408271 | 172.16.0.40 | 10.0.0.11 | TCP | 66 | 80 → 56064 [ACK] Seq=1 Ack=293 Win=30208 Len=0 TSval=536628903 TSecr=60571251 |
| 20 | 3.408576 | 172.16.0.40 | 10.0.0.11 | HTTP | 390 | HTTP/1.1 404 Not Found (text/html) |
| 21 | 3.409524 | 10.0.0.11 | 172.16.0.40 | TCP | 66 | 56064 → 80 [ACK] Seq=293 Ack=325 Win=30720 Len=0 TSval=60571252 TSecr=53662 |

● QUAL È IL NUMERO DI PORTA TCP DI ORIGINE?

56064

● COME CLASSIFICHERESTI LA PORTA DI ORIGINE?

56064

● QUAL È IL NUMERO DI PORTA TCP DI DESTINAZIONE?

IL NUMERO DI PORTA TCP È 80

● COME CLASSIFICHERESTI LA PORTA DI DESTINAZIONE?

CONNETTENDOMI DAL SERVER QUINDI IN QUESTO CASO DALLA PORTA 80 (HTTP)

● QUALE FLAG È IMPOSTATO?

È IMPOSTATO IN SYN

● A QUALE VALORE È IMPOSTATO IL NUMERO DI SEQUENZA RELATIVO?

Sequence number: 0 (relative sequence number)

● QUALI SONO I VALORI DELLE PORTE DI ORIGINE E DESTINAZIONE?

SONO PRATICAMENTE INVERSE, QUELLA DI DESTINAZIONE È 56064, LA PORTA DI ORIGINE È 80

● QUALI FLAG SONO IMPOSTATI?

SYN E ACK

● A QUALI VALORI SONO IMPOSTATI I NUMERI RELATIVI DI SEQUENZA E ACKNOWLEDGMENT?

SYN 0, ACKNOWLEDGMENT 1

● QUALE FLAG È IMPOSTATO? (2)

ACK

| | | | | | | |
|----|----------|-----------|-------------|-----|----|--------------------------|
| 21 | 3.409524 | 10.0.0.11 | 172.16.0.40 | TCP | 66 | 56064 → 80 [ACK] Seq=293 |
|----|----------|-----------|-------------|-----|----|--------------------------|

[Next sequence number: 293 (relative sequence number)]

Acknowledgment number: 325 (relative ack number)

1000 = Header Length: 32 bytes (8)

▼ Flags: 0x010 (ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

VADO SU TCDUMP

● COSA FA L'OPZIONE -R?

-R SERVE PER LEGGERE E ANALIZZARE PACCHETTI DA UN FILE

```
-r file
Read packets from file (which was created with the -w option or by other tools that write pcap or pcap-ng files). Standard input is used if file is '-'.
```

DA QUI VEDIAMO I LOG ANALIZZATI DA WIRESHARK

```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
reading from file /home/analyst/capture.pcap, link-type: ETH10MB (Ethernet)
10.49:00.987997 IP 10.0.0.11.56044 > 172.16.0.40.http: Flags [S], seq 1564657103, win 29200, options [mss 1460, sackOK, TS val 60571251 ecr 0,nop,wscale 9], length 0
10.49:00.987963 IP 172.16.0.40.http > 10.0.0.11.56044: Flags [S], seq 361866330, ack 1564657104, win 28960, options [mss 1460, sackOK, TS val 536628993 ecr 60571251,nop,wscale 9], length 0
10.49:00.987962 IP 10.0.0.11.56044 > 172.16.0.40.http: Flags [A], ack 1, win 68, options [nop,nop,TS val 60571251 ecr 536628993], length 0
[analyst@secOps ~]$
```

PULISCO I PROCESSI AVVIATI COME È STATO DETTO

```
[analyst@secOps ~]$ sudo rm -c
[sudo] password for analyst:
*** Removing excess controllers/ofprotocols/ofdatapaths/pings/noxes
killall controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udbbtest mnexec ivs 2> /dev/null
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udbbtest mnexec ivs 2> /dev/null
pkill -9 -f "sudo mnexec"
*** Removing junk from /tmp
rm -f /tmp/vconn* /tmp/vlogs* /tmp/*.out /tmp/*.log
*** Removing old X11 tunnels
*** Removing excess kernel datapaths
ps ax | egrep -o 'dp[0-9]+' | sed 's/dp/nl:/'
*** Removing OVS datapaths
ovs-vsctl --timeout=1 list-br
ovs-vsctl --timeout=1 list-br
*** Removing all links of the pattern foo-ethX
ip link show | egrep -o '([[:alnum:]]+-eth[[:digit:]]+)'
ip link show
*** Killing stale mininet node processes
pkill -9 -f mininet:
*** Shutting down stale tunnels
pkill -9 -f Tunnel=Ethernet
pkill -9 -f .ssh/rm
rm -f ~/.ssh/rm/*
*** Cleanup complete.
[analyst@secOps ~]$
```

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?

Attività di Riflessione

1 MI CONCENTREREI PIU' SU:

- IP.ADDR == (UN INDIRIZZO IP): PER VEDERE SOLO QUELLO CHE FA UN COMPUTER SPECIFICO.
- TCP.PORT == 80 O ALTRA PORTA: PER GUARDARE IL TRAFFICO DI UN SERVIZIO PARTICOLARE, AD ESEMPIO UNA NAVIGAZIONE WEB.
- DNS O HTTP: PER VEDERE SOLO LE RICHIESTE DNS O IL TRAFFICO WEB.

2 WIRESHARK È MOLTO UTILE PROPRIO PER VEDERE SE C'È QUALCOSA DI STRANO, PER CAPIRE QUANTO TRAFFICO C'È. ANCHE PER VERIFICARE CONFIGURAZIONI, QUINDI, CONTROLLANDO SE TUTTO COMUNICA COME DOVREBBE DOPO AVER FATTO DEI CAMBIAMENTI.