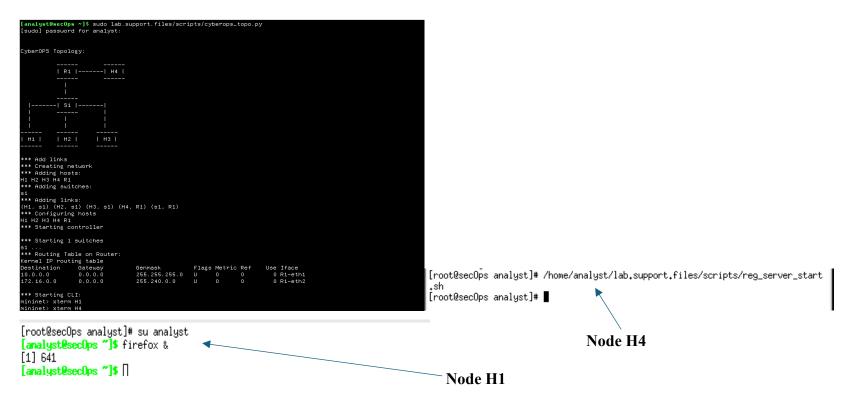
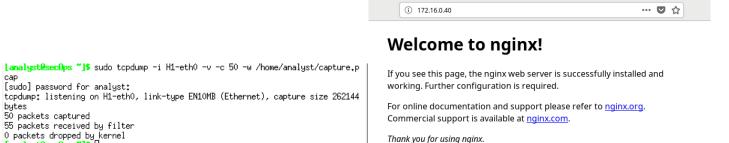
Esercitazione.

Preparazione per CyberOps.

Usare Wireshark per Osservare l'Handshake a 3 Vie TCP.

Qualche screen per il procedimento eseguito.





Parte 2: Analizzare i Pacchetti usando Wireshark.

[sudo] password for analyst:

55 packets received by filter O packets dropped by kernel

50 packets captured

Seguo la procedura fino ad ottenere questa schermata.

Filter:	tcp		•	Expression	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info	
1	5 4.492500	10.0.0.11	172.16.0.40	TCP	74	56438 → 80	[SYN] Seq=0 Win=29200 Len=0
1	6 4.492539	172.16.0.40	10.0.0.11	TCP	74	80 → 56438	[SYN, ACK] Seq=0 Ack=1 Win=2
1	7 4.492547	10.0.0.11	172.16.0.40	TCP	66	56438 → 80	[ACK] Seq=1 Ack=1 Win=29696
1	8 4.492717	10.0.0.11	172.16.0.40	HTTP	377	GET / HTTP/1	1.1
1	9 4.492730	172.16.0.40	10.0.0.11	TCP	66	80 → 56438	[ACK] Seq=1 Ack=312 Win=302
2	0 4.718404	172.16.0.40	10.0.0.11	TCP	304	80 → 56438	[PSH, ACK] Seq=1 Ack=312 Win

- 1) Qual è il numero di porta TCP di origine? Il numero di porta d'origine è 56438.
- Come classificheresti la porta di origine? La classificherei come porta dinamica/privata.
- Qual è il numero di porta TCP di destinazione? Il numero di porta di destinazione è 80. 3)
- Come classificheresti la porta di destinazione? La classificherei come porta nota dedicata ai servizi Web (al server Web nginx in questo caso).
- Quale flag è impostato? È impostato il flag 0x002 (SYN).
- A quale valore è impostato il numero di sequenza relativo? È impostato a 0.

Frame 2:

- 7) Quali sono i valori delle porte di origine e destinazione? La porta di origine è 80 e la porta di destinazione è la 56438.
- 8) Quali flag sono impostati? 0x012 (SYN, ACK).
- 9) A quali valori sono impostati i numeri relativi di sequenza e acknowledgment? Il numero relativo di sequenza è impostato su 0 mentre il numero di acknowledgement è impostato su 1.

```
Sequence number: 0 (relative sequence number)

[Next sequence number: 0 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)
```

10) Esaminare il terzo e ultimo pacchetto dell'handshake. Quale flag è impostato? Il flag impostato è 0x010 (ACK)

```
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)
```

Parte 3: Visualizzare i pacchetti usando tcpdump

11) Cosa fa l'opzione -r?

L'opzione -r permette di leggere i pacchetti da un file.

```
### 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 ``-''.

**Canalyst@secOps *|$ tcpdump -r /home/analyst/capture.pcap tcp -c 3

**reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)

08:27:31.663802 IP 10.0.0.11.56438 > 172.16.0.40.http: Flags [S], seq 591686644, win 29200, options [mss 1460,sackOK,TS val 1762803277 ecr 0,nop,wscale 9], length 0

08:27:31.663841 IP 172.16.0.40.http > 10.0.0.11.56438: Flags [S.], seq 3175599598, ack 591686645, win 28960, options [mss 1460,sackOK,TS val 1098819986] ecr 1762803277,nop,wscale 9], length 0

08:27:31.663849 IP 10.0.0.11.56438 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 1762803277 ecr 1098819986], length 0
```

Infine, navigo sul terminale dove ho attivato mininet e inserisco quit per terminare la sessione e sudo mn -c per pulire i processi avviati da mininet.

```
[analyst@secOps ~]$ sudo mn -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 udpbwtest mnexec
                                        killall –9 controller ofprotocol ofdatapath ping nox_core lt–nox_core ovs–openflowd ovs–controller udpbwtest mnex
                                        ec ivs 2> /dev/null
                                        pkill -9 -f "sudo mnexec"
                                        *** Removing junk from /tmp
                                        rm -f /tmp/vconn* /tmp/vlogs* /tmp/*.out /tmp/*.log
mininet> quit
                                        *** Removing old X11 tunnels
                                        *** Removing excess kernel datapaths
*** Stopping O controllers
                                       ps ax | egrep -o 'dp[0-9]+' | sed 's/dp/n1:/'
                                       *** Removing OVS datapaths
                                       ovs-vsctl --timeout=1 list-br
*** Stopping 2 terms
                                        ovs-vsctl --timeout=1 list-br
*** Stopping 5 links
                                        *** Removing all links of the pattern foo-ethX
                                        ip link show | egrep -o '([-_.[:alnum:]]+-eth[[:digit:]]+)'
*** Stopping 1 switches
                                        *** Killing stale mininet node processes
                                        pkill -9 -f mininet:
                                        *** Shutting down stale tunnels
*** Stopping 5 hosts
                                        pkill –9 –f Tunnel=Ether<u>net</u>
H1 H2 H3 H4 R1
                                        pkill –9 –f .ssh/mn
                                        rm -f ~/.ssh/mn/*
*** Done
```

Domande di riflessione.

- 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.
 - Su Wireshark si può filtrare attraverso i **protocolli** (per esempio: TCP, HTTP, DNS, ICMP), attraverso **indirizzo IP** sorgente e **IP destinatario** e attraverso **porte specifiche.**
- In quali altri modi Wireshark potrebbe essere utilizzato in una rete di produzione?
 - Wireshark può essere utilizzato per monitorare i tempi di risposta di applicazioni e servizi, per identificare problemi di connettività tra dispositivi e per l'analisi di incidenti di sicurezza.