

Usare Wireshark per Osservare l'Handshake a 3 Vie TCP

Avvio di mininet:

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

CyberOPS Topology:

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

*** Add links
*** Creating network
*** Adding hosts:
H1 H2 H3 H4 R1
*** Adding switches:
s1
*** Adding links:
(H1, s1) (H2, s1) (H3, s1) (H4, R1) (s1, R1)
*** Configuring hosts
H1 H2 H3 H4 R1
*** Starting controller

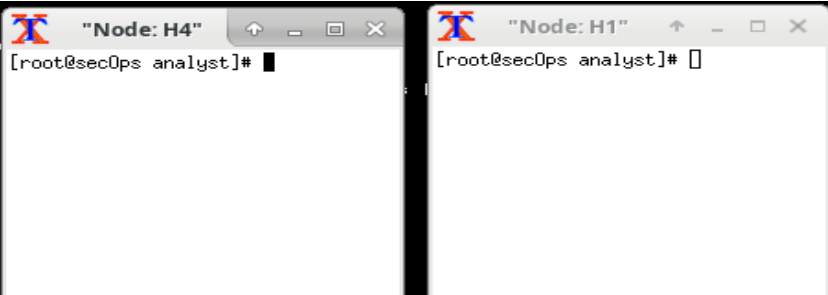
*** Starting 1 switches
s1 ...
*** Routing Table on Router:
Kernel IP routing table
Destination        Gateway            Genmask           Flags Metric Ref    Use Iface
10.0.0.0            0.0.0.0            255.255.255.0     U        0      0        0 R1-eth1
172.16.0.0          0.0.0.0            255.240.0.0       U        0      0        0 R1-eth2

*** Starting CLI:
mininet> 
```

Avvio di H1 e H4:

```
*** Starting 1 switches
s1 ...
*** Routing Table on Router:
Kernel IP routing table
Destination        Gateway            Genmask           Flags Metric Ref    Use Iface
10.0.0.0            0.0.0.0            255.255.255.0     U        0      0        0 R1-eth1
172.16.0.0          0.0.0.0            255.240.0.0       U        0      0        0 R1-eth2

*** Starting CLI:
mininet> xterm h1
node 'h1' not in network
mininet> xterm H1
mininet> xterm H4
mininet> 
```



Avvio del server web su H4:

```
"Node: H4"
[root@secOps analyst]# /home/analyst/lab.support.files/scripts/reg_server_start.sh
[root@secOps analyst]#
```

Apertura browser su H1:

```
"Node: H1"
[analyst@secOps ~]$ firefox $
```

Avvio cattura:

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

```
"Node: H1"
[analyst@secOps ~]$ firefox &
[1] 1187
[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 ~]$
```

Apertura della cattura con wireshark:

```
[analyst@secOps ~]$ wireshark-gtk &
[2] 1400
[analyst@secOps ~]$
(wireshark-gtk:1400): dbind-WARNING **: 10:49:56.989: Couldn't connect to accessibility bus: Failed to connect to socket /tmp/dbus-zddUIbXcCK: Connection refused
(wireshark-gtk:1400): Gtk-CRITICAL **: 10:51:01.523: gtk_box_gadget_distribute: assertion 'size >= 0' failed in GtkScrollbar
[analyst@secOps ~]$
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	48244 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=
2	0.000068	172.16.0.40	10.0.0.11	TCP	74	80 → 48244 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_Pe
3	0.000077	10.0.0.11	172.16.0.40	TCP	66	48244 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=817781294 TSer=

Analisi dei pacchetti:

Come possiamo notare il primo frame ha come porta sorgente una porta casuale scelta dal client e la porta 80 del web-server

1	0.000000	10.0.0.11	172.16.0.40	TCP	74	48244 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=817781294 TSecr=0 WS=512
2	0.000058	172.16.0.40	10.0.0.11	TCP	74	80 → 48244 [ACK] Seq=0 Ack=1 Win=38060 Len=0 MSS=1460 SACK_PERM=1 TSval=1018025262 TSecr=817781294
▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)						
▶ Ethernet II, Src: 1a:95:6f:7b:df:5f (1a:95:6f:7b:df:5f), Dst: 36:95:e7:cf:06:ac (36:95:e7:cf:06:ac)						
▶ Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40						
▼ Transmission Control Protocol, Src Port: 48244, Dst Port: 80, Seq: 0, Len: 0						
Source Port: 48244						
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]						

Analizzando i flags del frame, notiamo che l'unico impostato e' il SYN

▼ 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

1. Qual è il numero di porta TCP di origine?
2. Come classificheresti la porta di origine?
3. Qual è il numero di porta TCP di destinazione?
4. Come classificheresti la porta di destinazione?
5. Quale flag è impostato?
6. A quale valore è impostato il numero di sequenza relativo?

1. 48244
2. E' una porta non registrata e utilizzabile liberamente.
3. 80 HTTP
4. la porta 80 appartiene alle well-known ports, gia' prese dai servizi piu' comuni.
5. Syn (Synchronize)
6. valore = 0

Secondo pacchetto:

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 48244, Seq: 0, Ack: 1, Len: 0

Source Port: 80
Destination Port: 48244
[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)

000. = Reserved: Not set
...0 = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set

1. Quali sono i valori delle porte di origine e destinazione?
2. Quali flag sono impostati?
3. A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?

1. stavolta la porta di origine e' 80, e destinazione: 48244
2. SYN e ACK
3. seq=0, ack=1

Nel terzo pacchetto e' presente solo il flag di ACK,

Parte 3 Visualizzare i pacchetti usando tcpdump

```
[analyst@sec0ps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
10:44:10.417710 IP 10.0.0.11.48244 > 172.16.0.40.http: Flags [S], seq 407506876, win 29200, options [mes 1460,sackOK,TS val 817781294 ecr 0,nop,wscale 9], length 0
10:44:10.417778 IP 172.16.0.40.http > 10.0.0.11.48244: Flags [S.], seq 4136320402, ack 407506877, win 28960, options [mes 1460,sackOK,TS val 1018935262 ecr 817781294,nop,wscale 9], length 0
10:44:10.417787 IP 10.0.0.11.48244 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 817781294 ecr 1018935262], length 0
[analyst@sec0ps ~]$
```

L'opzione -r permette di specificare il percorso del file.

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.

1. Filtro porte: Filtrare le porte e selezionare solo quelle di interesse puo' far risparmiare tempo ad un amministratore di rete, soprattutto se vuole capire cosa e' stato attaccato per primo, se il servizio web sulla porta 80, o un servizio ssh sulla porta 22...

2. Filtro ip: Dopo aver rilevato azioni sospette da parte di un certo ip, si puo' filtrare per vedere solo le comunicazioni in cui e' presente.

3. Espressioni: wireshark permette di costruire delle espressioni in app, così facendo un amministratore di rete può essere più flessibile nel filtrare le comunicazioni.

2. In quali altri modi Wireshark potrebbe essere utilizzato in una rete di produzione?

1. Wireshark può essere usato per fare reverse engineering del traffico di un software che non ha una buona documentazione, oppure non ne ha affatto.
2. Inoltre può essere usato per Auditing e per la valutazione delle performance di rete.

Wireshark può essere impostato per catturare solo il traffico di interesse riducendo la latenza in ambienti carichi di traffico.

E' inoltre importante proteggere i file .pcap poiché possono contenere informazioni riservate.