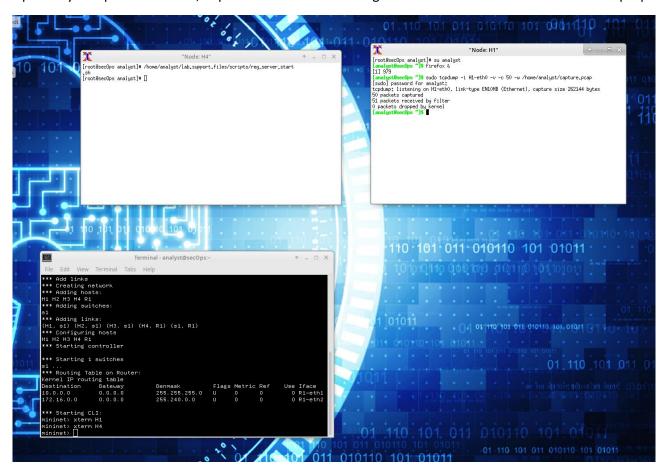
Pratica S11L3

Apro la CyberOps Workstation, imposto i terminali come da guida e catturo il traffico di rete in un file .pcap



Apro il file .pcap con wireshark ed imposto il filtro su TCP

File Ec	dit View Go	Capture Analyze Statistics	Telephony Tools		ure.pcap [Wireshark 2.5.1]
• 6			Q>	* ~ ×	
Filter:	tcp		•	Expression	Clear Apply Save
No.	Time	Source	Destination	Protocol	Length Info
	3 5.535866		172.16.0.40	TCP	74 54170 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3607270668 TSecr=0 WS=512
2	4 5.535905	172.16.0.40	10.0.0.11	TCP	74 80 → 54170 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2915393424 TSecr=36
2	5 5.535912	10.0.0.11	172.16.0.40	TCP	66 54170 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=3607270668 TSecr=2915393424
2	6 5.542158	10.0.0.11	172.16.0.40	HTTP	358 GET /favicon.ico HTTP/1.1
2	7 5.542182	172.16.0.40	10.0.0.11	TCP	66 80 → 54170 [ACK] Seq=1 Ack=293 Win=30208 Len=0 TSval=2915393430 TSecr=3607270674
2	8 5.542247	172.16.0.40	10.0.0.11	HTTP	390 HTTP/1.1 404 Not Found (text/html)
2	9 5.542356	10.0.0.11	172.16.0.40	TCP	66 54170 → 80 [ACK] Seq=293 Ack=325 Win=30720 Len=0 TSval=3607270674 TSecr=2915393430

Analizzo il primo pacchetto che corrisponde all'inizio del three-way handshake, vedo che la connessione parte dalla porta 54170 con destinazione porta 80, è attiva la flag SYN

```
Transmission Control Protocol, Src Port: 54170, Dst Port: 80, Seq: 0, Len: 0
      Source Port: 54170
      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)
         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
         .... 0 = Fin: Not set
         [TCP Flags: ······S·]
Analizzo il secondo pacchetto e vedo che c'è la risposta del server con un pacchetto SYN, ACK
 Frame 24: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 Ethernet II, Src: d6:87:37:72:1d:f8 (d6:87:37:72:1d:f8), Dst: da:bb:56:be:5b:1f (da:bb:56:be:5b:1f)
 ▶ Internet Protocol Version 4, Src: 172.16.0.40, Dst: 10.0.0.11
 ▼ Transmission Control Protocol, Src Port: 80, Dst Port: 54170, Seq: 0, Ack: 1, Len: 0
      Source Port: 80
      Destination Port: 54170
      [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 = Acknowledgment: Set 0... = Push: Not set 0... = Reset: Not set 1. = Syn: Set

Per chiudere il trhee-way handshake analizzo il terzo pacchetto e vedo la flag ACK attiva

```
Frame 25: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: da:bb:56:be:5b:1f (da:bb:56:be:5b:1f), Dst: d6:87:37:72:1d:f8 (d6:87:37:72:1d:f8)
Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
Transmission Control Protocol, Src Port: 54170, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
     Source Port: 54170
     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)

        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 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... .... .. 0. = Syn: Not set
        .... 0 = Fin: Not set
        ITCP Flags: ······A····1
```

Da terminale con tcpdump posso analizzare il file non avendo a disposizione wireshark

```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
10:04:02.185259 IP 10.0.0.11.54170 > 172.16.0.40.http: Flags [S], seq 1167130569, win 29200, options [mss 1460,sack OK,TS val 3607270668 ecr 0,nop,wscale 9], length 0
10:04:02.185298 IP 172.16.0.40.http > 10.0.0.11.54170: Flags [S.], seq 986220441, ack 1167130570, win 28960, option s [mss 1460,sackOK,TS val 2915393424 ecr 3607270668,nop,wscale 9], length 0
10:04:02.185305 IP 10.0.0.11.54170 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 3607270668 ecr 2915393424], length 0
[analyst@secOps ~]$ ■
```