

In questo laboratorio, completa i seguenti obiettivi:

- Parte 1: Preparare gli host per catturare il traffico
- Parte 2: Analizzare i pacchetti utilizzando Wireshark
- Parte 3: Visualizzare i pacchetti utilizzando tcpdump

```
[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
*** Adding hosts:
H1 H2 H3 H4 R1
```

```
FILE EDIT VIEW TERMINAL STATUS HELP
*** 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-eth
172.16.0.0      0.0.0.0         255.240.0.0   U     0      0      0 R1-eth

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

Apriamo Wireshark e importiamo il file di cattura, seguendo i passaggi mostrati nelle schermate seguenti:

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Open... Ctrl+O

Open Recent

Merge...

Import from Hex Dump...

Close Ctrl+W

Save Ctrl+S

Save As... Shift+Ctrl+S

File Set

Export Specified Packets...

Export Packet Dissections

Export Selected Packet Bytes... Ctrl+H

Export PDUs to File...

Export SSL Session Keys...

Export Objects

Print... Ctrl+P

Quit Ctrl+Q

The Wireshark Network Analyzer

Wireshark: Open Capture File

Recent

Home

Desktop

Filesystem

+ Other Locations

Name

Size

Modified

.idlerc 51 bytes 2 Apr 20

.lessht 22 Mar 21

.local .mozilla 24 Mar 21

.ssh 2 Apr 20

.vim 20 Mar 21

.viminfo 13.9 kB 19 Jul 20

Xauthority 51 bytes 02:16

xinitrc 16 bytes 22 Mar 21

Xinitrc 16 bytes 22 Mar 21

xsession-errors 557 bytes 02:32

xsession-errors.old 307 bytes Yesterday

capture.pcap 5.1 kB 02:29

Desktop 22 Mar 21

Downloads 22 Mar 21

lab.support.files 19 Jul 20

second_drive 21 Mar 21

Format: Wireshark/tcpdump/... - pcap

Size: 5117 bytes

Packets: 50

Start / elapsed: 2025-02-19 02:28:33 / 00:00:28

Automatically detect file type

Filter:

Cancel Open

capture.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

tcp

No. Time Source Destination Protocol Length Info

43 25.731437 10.0.0.11 172.16.0.40 TCP 74 49682 → 80

44 25.732117 172.16.0.40 10.0.0.11 TCP 54 80 → 49682

▶ Frame 43: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

▶ Ethernet II, Src: 0:0:ad:81:0:d (0:a:0:ad:81:0:d), Dst: 0:0:0:0:0:0 (0:0:0:0:0:0)

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

▶ Transmission Control Protocol, Src Port: 49682, Dst Port: 80, Seq: 0, Len: 0

0000 0a 00 ad 81 0d e9 22 fe 7d 86 88 35 08 00 45 00:5.E.

0010 00 3c fa 40 00 40 06 d4 ae 0a 00 00 0b ac 10 .<@.@.

capture.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

tcp

No. Time Source Destination Protocol Length Info

43 25.731437 10.0.0.11 172.16.0.40 TCP 74 49682 → 80

44 25.732117 172.16.0.40 10.0.0.11 TCP 54 80 → 49682

▶ Frame 44: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

▶ Ethernet II, Src: 0:0:ad:81:0:d (0:a:0:ad:81:0:d), Dst: 22:fe:7d:86:8b:35 (22:fe:7d:86:8b:35)

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

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49682, Seq: 1, Ack: 1, Len: 0

Source Port: 80

Destination Port: 49682

[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)

0101 = Header Length: 20 bytes(5)

Flags: 0x014 (RST, ACK)

000. = Reserved: Not set

.... = Nonce: Not set

.... = Congestion Window Reduced (CWR): Not set

.... = ECN-Echo: Not set

0010 00 72 77 40 00 3f 06 13 16 10 00 28 0a 00 .rw@.?.

0020 00 0b 00 50 c2 12 00 00 00 00 c9 f7 2c 71 50 14 ..P.....qP.

0030 00 40 c2 00 00 00 ..@...

"Node: H1"

TCPDUMPGeneral Commands ManTCPDUMP(1)

NAME

tcpdump - dump traffic on a network

SYNOPSIS

```
tcpdump [ -AbdDefHHIJKQS
          LlNMPqStuvxz ] [ -B buffer_size ]
          [ -c count ]
          [ -C file_size ] [ -G rotate_seconds ]
          [ -F file ] [ -i interface ] [ -j timestamp_type ]
          [ -m module ] [ -M secret ]
          [ -n number ] [ -q
          inout | inout ]
          [ -r file ] [ -v file ]
          [ -s snaplen ] [ -T type ]
          [ -w file ]
          [ -u filecount ]
          [ -E spip@ipaddr ]
```

Manual page tcpdump(1) line 1 (press h for help or q to quit)

"Node: H1"

units of file_size are millions of bytes (1,000,000 bytes, not 1,048,576 bytes).

-d Dump the compiled packet-matching code in a human readable form to standard output and stop.

-dd Dump packet-matching code as a C program

[analyst@secops ~]\$ tcpdump -r /home/analyst/capture.pcap tcp /c 3
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
tcpdump: syntax error in filter expression: syntax error
[analyst@secops ~]\$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
02:28:59.474502 IP secOps.49682 > 172.16.0.40.http: Flags [S], seq 3388419184, win 29200, options [mss 1460,sackOK,TS val 2113852960 ecr 0,nop,wscale 9], length 0
02:28:59.475182 IP 172.16.0.40.http > secOps.49682: Flags [R], seq 0, ack 3388419184, length 0
[analyst@secops ~]\$

```
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 Ifac.
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 R1-e
172.16.0.0       0.0.0.0         255.240.0.0    U     0      0        0 R1-e
```

Terminal - analyst@secOps:~

File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ sudo mn -c
*** Removing excess controllers/ofprotocols/ofdatapaths/pings/noxes
killall controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflow
ovs-controller udpbwtest mnexec ivs 2> /dev/null
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflow
ovs-controller udpbwtest 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 del s1-eth3;ip link del s1-eth4;ip link del s1-eth1 ) 2> /dev/null
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/mn
```