Utilizzo di Wireshark per Osservare la Stretta di Mano TCP a 3 Vie

CyberOps Workstation [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Applications : Terminal - analyst@secOps:~ | ["Node: H1"] | "Node: H4" | 03:52 an

Terminal - analyst@secOps:~

File Edit View Terminal Tabs Help

```
        ------
        | 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> xterm h1
node 'h1' not in network
mininet> xterm H1
mininet> xterm H4
mininet>
```

"Node: H4"

```
[root@secOps analyst]# /home/analyst/lab.support.files/script/reg_server_start.
sh
bash: /home/analyst/lab.support.files/script/reg_server_start.sh: No such file o
r directory
[root@secOps analyst]# /home/analyst/lab.support.files/scripts/reg_server_start
.sh
[root@secOps analyst]# su analyst
[analyst@secOps ~]$ cyberops
bash: cyberops: command not found
[analyst@secOps ~]$ sudo -s
[sudo] password for analyst:
[root@secOps analyst]#
```

Mozilla Firefox

New Tab × +

Search or enter address

"Node: H1"

```
[root@secOps analyst]# su analyst
[analyst@secOps ~]$ firefox &
[1] 798
[analyst@secOps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.p
cap
[sudo] password for analyst:
tcpdump: listening on H1-eth0, link-type EN10MB (Ethernet), capture size 262144
bytes
Got 23
```

youtube   facebook   amazon

GETRICHSLOWLY   GETPOCKET   NYTIMES
How to retire early: Early   **Productivity Tips for People** **How to Reduce the Risk of**
retirement by the numbers   **Who Hate Productivity Tips**   **the Scary Thing You Want**
More and more, I'm meeting   "Traditional approaches to staying **to Do**
people who want to know how to   focused don't work for me." "I   You shouldn't start a restaurant
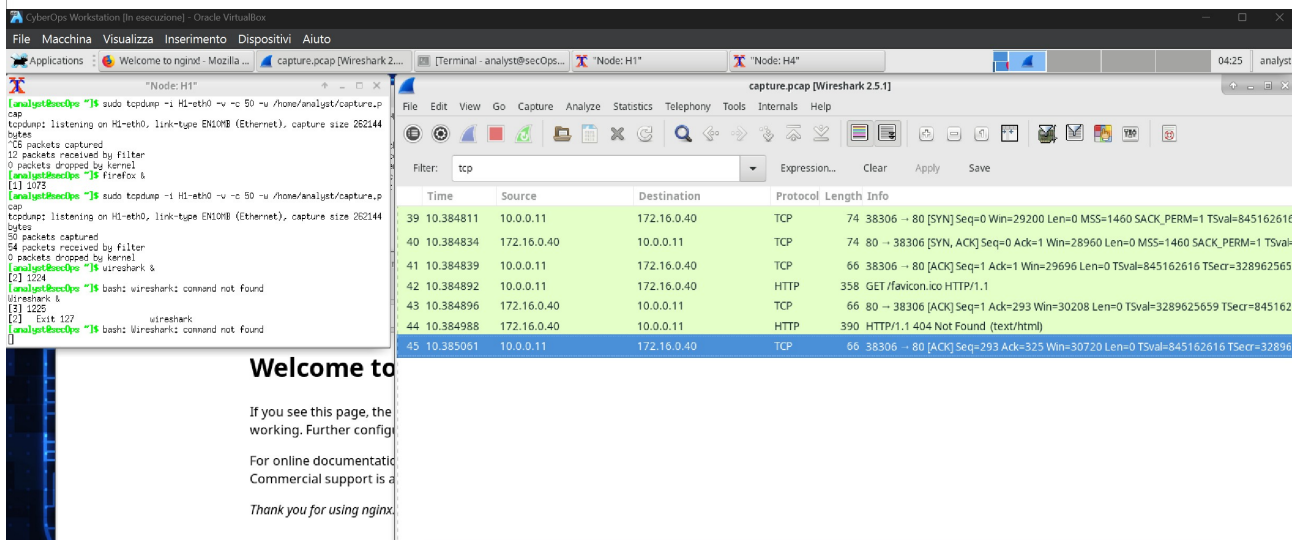
Welcome to nginx!

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.

172.16.0.40

Welcome to nginx! × +

CyberOps Workstation [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Applications | Welcome to nginx! - Mozilla ... | capture.pcap [Wireshark 2.... | [Terminal - analyst@secOps... | "Node: H1" | "Node: H4" | 04:25 analyst

"Node: H1"

```
[analyst@secOps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.p
cap
tcpdump: listening on H1-eth0, link-type EN10MB (Ethernet), capture size 262144
bytes
^C6 packets captured
12 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$ firefox &
[1] 1073
[analyst@secOps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.p
cap
tcpdump: listening on H1-eth0, link-type EN10MB (Ethernet), capture size 262144
bytes
50 packets captured
54 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$ wireshark &
[2] 1224
[analyst@secOps ~]$ bash: wireshark: command not found
wireshark &
[3] 1225
[2]   Exit 127              wireshark
[analyst@secOps ~]$ bash: Wireshark: command not found
[]
```

capture.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp   Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
39	10.384811	10.0.0.11	172.16.0.40	TCP	74	38306 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=845162616
40	10.384834	172.16.0.40	10.0.0.11	TCP	74	80 → 38306 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSva
41	10.384839	10.0.0.11	172.16.0.40	TCP	66	38306 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=845162616 TSecr=3289625655
42	10.384892	10.0.0.11	172.16.0.40	HTTP	358	GET /favicon.ico HTTP/1.1
43	10.384896	172.16.0.40	10.0.0.11	TCP	66	80 → 38306 [ACK] Seq=1 Ack=293 Win=30208 Len=0 TSval=3289625659 TSecr=845162
44	10.384988	172.16.0.40	10.0.0.11	HTTP	390	HTTP/1.1 404 Not Found (text/html)
45	10.385061	10.0.0.11	172.16.0.40	TCP	66	38306 → 80 [ACK] Seq=293 Ack=325 Win=30720 Len=0 TSval=845162616 TSecr=32896

Welcome to

If you see this page, the
working. Further config

For online documentatio
Commercial support is a

Thank you for using nginx.

39	10.384811	10.0.0.11	172.16.0.40	TCP	74	38306 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=84
40	10.384834	172.16.0.40	10.0.0.11	TCP	74	80 → 38306 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM
41	10.384839	10.0.0.11	172.16.0.40	TCP	66	38306 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=845162616 TSecr=32
42	10.384892	10.0.0.11	172.16.0.40	HTTP	358	GET /favicon.ico HTTP/1.1
43	10.384896	172.16.0.40	10.0.0.11	TCP	66	80 → 38306 [ACK] Seq=1 Ack=293 Win=30208 Len=0 TSval=3289625659 TSecr
44	10.384988	172.16.0.40	10.0.0.11	HTTP	390	HTTP/1.1 404 Not Found (text/html)
45	10.385061	10.0.0.11	172.16.0.40	TCP	66	38306 → 80 [ACK] Seq=293 Ack=325 Win=30720 Len=0 TSval=845162616 TSec

39 10.384811 10.0.0.11 172.16.0.40 TCP 74 38306 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=845162616 TSecr=0 WS=512

▼ Transmission Control Protocol, Src Port: 38306, Dst Port: 80, Seq: 0, Len: 0
      Source Port: 38306
      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

capture.pcap [Wireshark 2.5.1]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: | Expression... | Clear | Apply | Save

No.	Time	Source	Destination	Protocol	Length	Info
						80 → 38306 [SYN, ACK] Seq=0 Win=29200 Len=0 MSS=146 SACK_PE
40	10.384834	172.16.0.40	10.0.0.11	TCP	74	80 → 38306 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=146
41	10.384839	10.0.0.11	172.16.0.40	TCP	66	38306 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=845162
42	10.384892	10.0.0.11	172.16.0.40	HTTP	358	GET /favicon.ico HTTP/1.1
43	10.384896	172.16.0.40	10.0.0.11	TCP	66	80 → 38306 [ACK] Seq=1 Ack=293 Win=30208 Len=0 TSval=3289
44	10.384988	172.16.0.40	10.0.0.11	HTTP	390	HTTP/1.1 404 Not Found (text/html)
45	10.385061	10.0.0.11	172.16.0.40	TCP	66	38306 → 80 [ACK] Seq=293 Ack=325 Win=30720 Len=0 TSval=84
46	10.842497	10.0.0.11	209.165.200.235	DNS	87	Standard query 0xfc25 A safebrowsing.googleapis.com.

Terminal - analyst@secOps:~

File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$  tcpdump -r /home/analyst/capture.pcap tcp -c 3
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
04:22:54.745082 IP 10.0.0.11.38306 > 172.16.0.40.http: Flags [S], seq 3370723586, win 29200, options [mss 1460,sackOK,TS val 845162616 ecr 0,nop,wscale 9], length 0
04:22:54.745105 IP 172.16.0.40.http > 10.0.0.11.38306: Flags [S.], seq 3202242744, ack 3370723587, win 28960, options [mss 1460,sackOK,TS val 3289625659 ecr 845162616,nop,wscale 9], length 0
04:22:54.745110 IP 10.0.0.11.38306 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 845162616 ecr 3289625659], length 0
[analyst@secOps ~]$
```