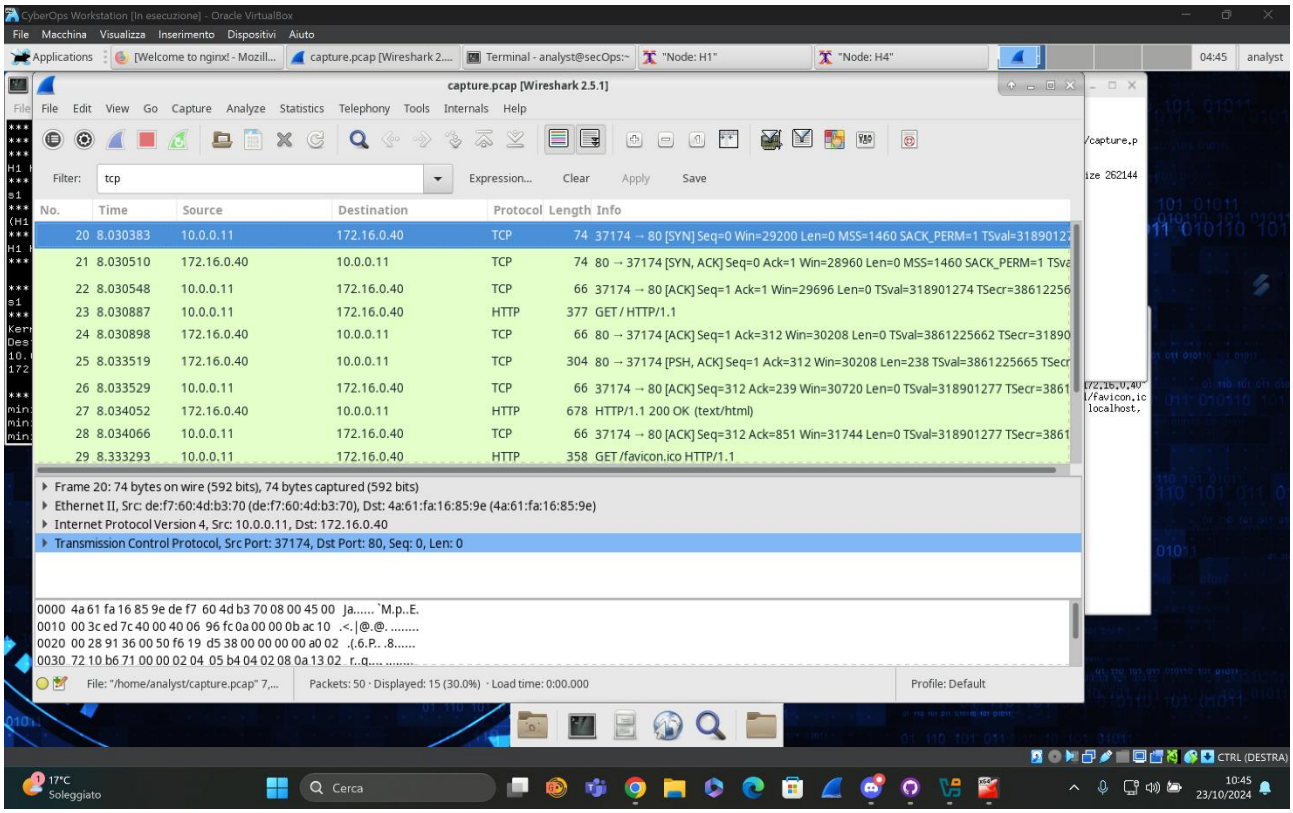
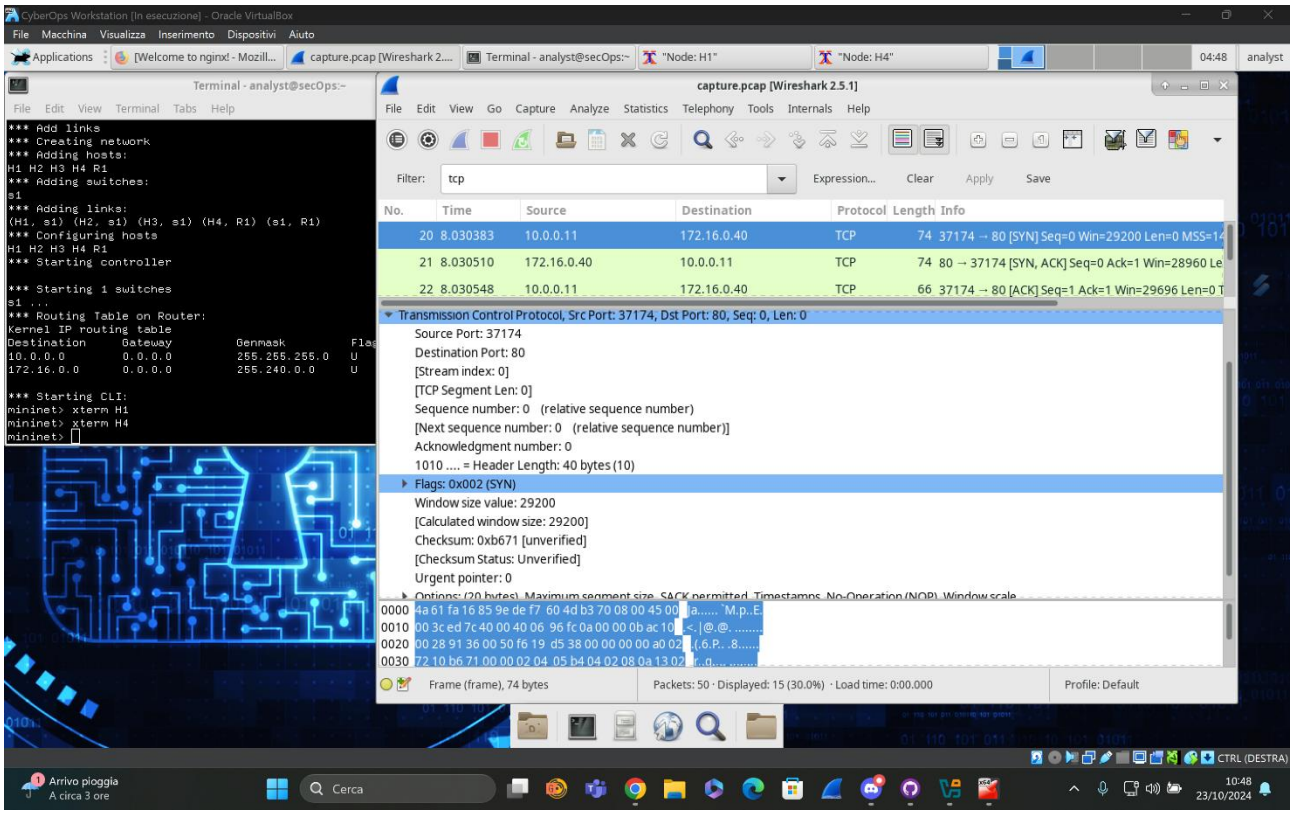
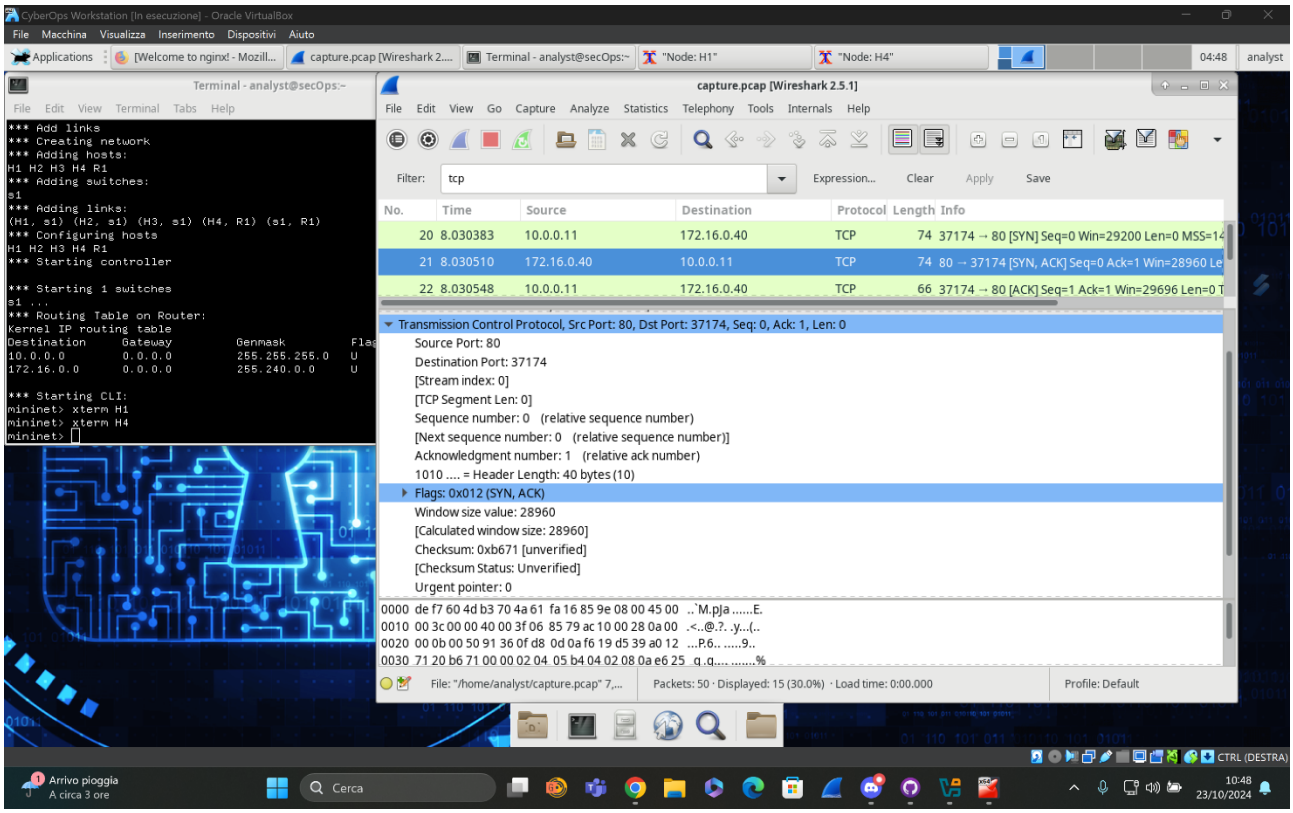
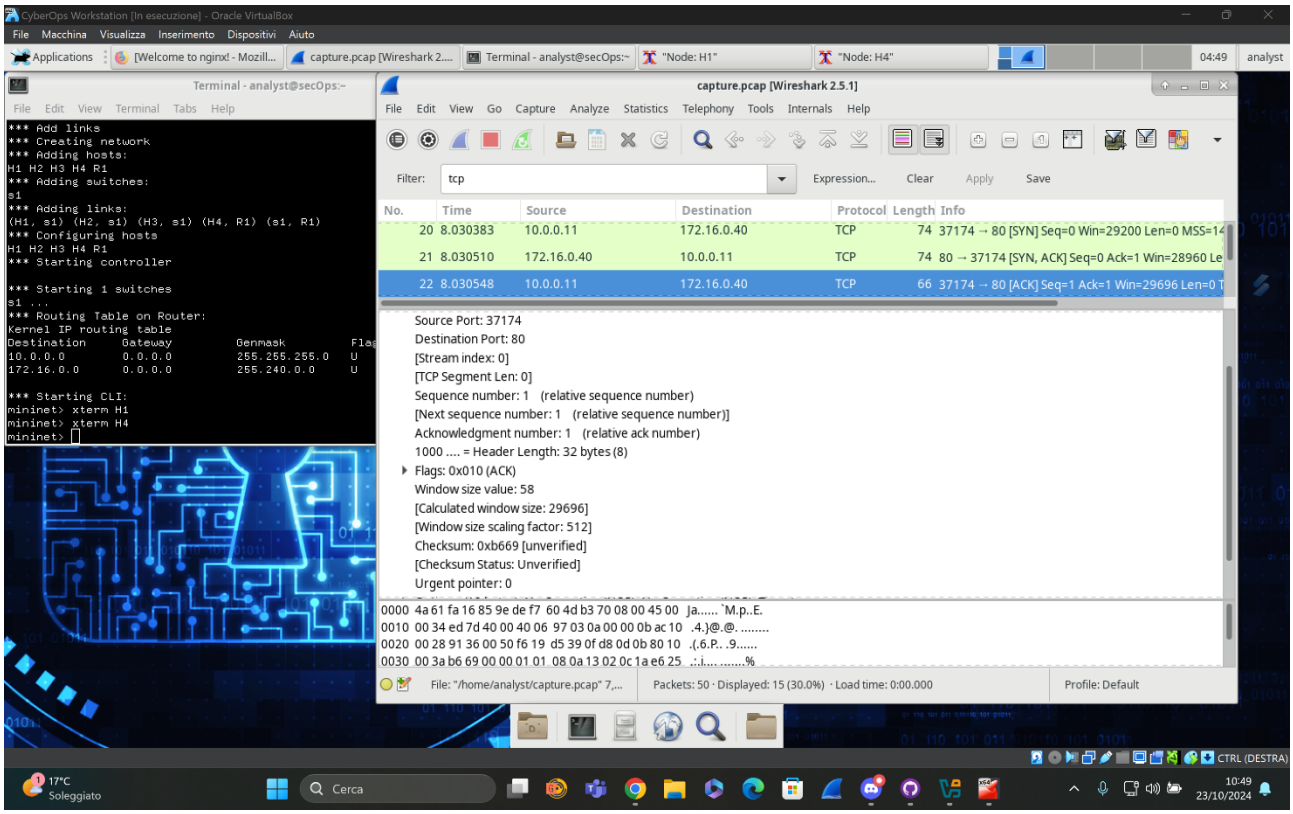
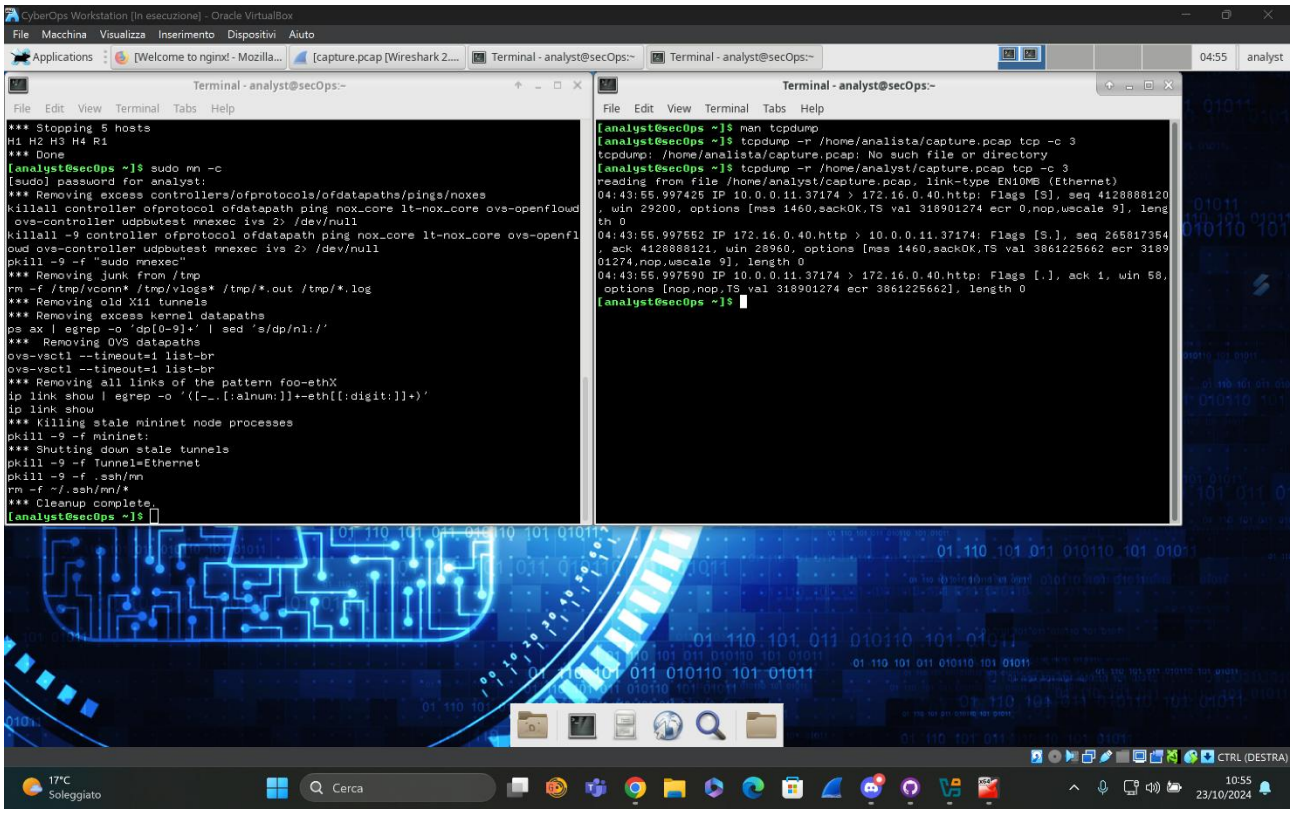

CyberOps Workstation [In esecuzione] - Oracle VirtualBox
capture.pcap [Wireshark 2.5.1]
Filter: tcp
No. Time Source Destination Protocol Length Info
20 8.030383 10.0.0.11 172.16.0.40 TCP 74 37174 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=318901274
21 8.030510 172.16.0.40 10.0.0.11 TCP 74 80 → 37174 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3861225662
22 8.030548 10.0.0.11 172.16.0.40 TCP 66 37174 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=318901274 TSecr=3861225662
23 8.030887 10.0.0.11 172.16.0.40 HTTP 377 GET / HTTP/1.1
24 8.030898 172.16.0.40 10.0.0.11 TCP 66 80 → 37174 [ACK] Seq=1 Ack=312 Win=30208 Len=0 TSval=3861225662 TSecr=318901274
25 8.033519 172.16.0.40 10.0.0.11 TCP 304 80 → 37174 [PSH, ACK] Seq=1 Ack=312 Win=30208 Len=238 TSval=3861225665 TSecr=318901277
26 8.033529 10.0.0.11 172.16.0.40 TCP 66 37174 → 80 [ACK] Seq=312 Ack=239 Win=30720 Len=0 TSval=318901277 TSecr=3861225665
27 8.034052 172.16.0.40 10.0.0.11 HTTP 678 HTTP/1.1 200 OK (text/html)
28 8.034066 10.0.0.11 172.16.0.40 TCP 66 37174 → 80 [ACK] Seq=312 Ack=851 Win=31744 Len=0 TSval=318901277 TSecr=3861225665
29 8.333293 10.0.0.11 172.16.0.40 HTTP 358 GET /favicon.ico HTTP/1.1
Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: de:f7:60:4d:b3:70 (de:f7:60:4d:b3:70), Dst: 4a:61:fa:16:85:9e (4a:61:fa:16:85:9e)
Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
Transmission Control Protocol, Src Port: 37174, Dst Port: 80, Seq: 0, Len: 0
0000 4a 61 fa 16 85 9e de f7 60 4d b3 70 08 00 45 00 Ja..... `M.p..E.
0010 00 3c ed 7c 40 00 40 06 96 fc 0a 00 00 0b ac 10 .<.|@.@. ....
0020 00 28 91 36 00 50 f6 19 d5 38 00 00 00 00 a0 02 .(.6.P.. .8......
0030 72 10 b6 71 00 00 02 04 05 b4 04 02 08 0a 13 02 r..q.... ....
File: "/home/analyst/capture.pcap" 7,...
Packets: 50 · Displayed: 15 (30.0%) · Load time: 0:00.000
Profile: Default
17°C Soleggiato
Cerca
10:45 23/10/2024


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
Terminal - analyst@secOps:~
*** 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
10.0.0.0 0.0.0.0 255.255.255.0 U
172.16.0.0 0.0.0.0 255.240.0.0 U
*** Starting CLI:
mininet> xterm H1
mininet> xterm H4
mininet>
capture.pcap [Wireshark 2.5.1]
Filter: tcp
No. Time Source Destination Protocol Length Info
20 8.030383 10.0.0.11 172.16.0.40 TCP 74 37174 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=14
21 8.030510 172.16.0.40 10.0.0.11 TCP 74 80 → 37174 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le
22 8.030548 10.0.0.11 172.16.0.40 TCP 66 37174 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 T
Transmission Control Protocol, Src Port: 37174, Dst Port: 80, Seq: 0, Len: 0
Source Port: 37174
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
0000 4a 61 fa 16 85 9e de f7 60 4d b3 70 08 00 45 00 Ja..... `M.p..E.
0010 00 3c ed 7c 40 00 40 06 96 fc 0a 00 00 0b ac 10 .<.|@.@. ....
0020 00 28 91 36 00 50 f6 19 d5 38 00 00 00 00 a0 02 .(.6.P.. .8......
0030 72 10 b6 71 00 00 02 04 05 b4 04 02 08 0a 13 02 r..q.... ....
Frame (frame), 74 bytes
Packets: 50 · Displayed: 15 (30.0%) · Load time: 0:00.000
Profile: Default
Arrivo pioggia A circa 3 ore
Cerca
10:48 23/10/2024


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Terminal - analyst@secOps:~
*** 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
10.0.0.0 0.0.0.0 255.255.255.0 U
172.16.0.0 0.0.0.0 255.240.0.0 U
*** Starting CLI:
mininet> xterm H1
mininet> xterm H4
mininet>
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
20 8.030383 10.0.0.11 172.16.0.40 TCP 74 37174 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=14
21 8.030510 172.16.0.40 10.0.0.11 TCP 74 80 → 37174 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le
22 8.030548 10.0.0.11 172.16.0.40 TCP 66 37174 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 T
Transmission Control Protocol, Src Port: 80, Dst Port: 37174, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 37174
[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)
Window size value: 28960
[Calculated window size: 28960]
Checksum: 0xb671 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
0000 de f7 60 4d b3 70 4a 61 fa 16 85 9e 08 00 45 00 ..`M.pJa ......E.
0010 00 3c 00 00 40 00 3f 06 85 79 ac 10 00 28 0a 00 .<..@.?. .y...(..
0020 00 0b 00 50 91 36 0f d8 0d 0a f6 19 d5 39 a0 12 ...P.6.. .....9..
0030 71 20 b6 71 00 00 02 04 05 b4 04 02 08 0a e6 25 q .q.... ....%
File: "/home/analyst/capture.pcap" 7,... Packets: 50 · Displayed: 15 (30.0%) · Load time: 0:00.000 Profile: Default
Arrivo pioggia
A circa 3 ore
Cerca
10:48
23/10/2024


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Terminal - analyst@secOps:~
*** 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
10.0.0.0 0.0.0.0 255.255.255.0 U
172.16.0.0 0.0.0.0 255.240.0.0 U
*** Starting CLI:
mininet> xterm H1
mininet> xterm H4
mininet>
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
20 8.030383 10.0.0.11 172.16.0.40 TCP 74 37174 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=14
21 8.030510 172.16.0.40 10.0.0.11 TCP 74 80 → 37174 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le
22 8.030548 10.0.0.11 172.16.0.40 TCP 66 37174 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 T
Source Port: 37174
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)
Window size value: 58
[Calculated window size: 29696]
[Window size scaling factor: 512]
Checksum: 0xb669 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
0000 4a 61 fa 16 85 9e de f7 60 4d b3 70 08 00 45 00 Ja..... `M.p..E.
0010 00 34 ed 7d 40 00 40 06 97 03 0a 00 00 0b ac 10 .4.}@.@. ....
0020 00 28 91 36 00 50 f6 19 d5 39 0f d8 0d 0b 80 10 .(.6.P.. .9......
0030 00 3a b6 69 00 00 01 01 08 0a 13 02 0c 1a e6 25 .:.i.... ....%
File: "/home/analyst/capture.pcap" 7,... Packets: 50 · Displayed: 15 (30.0%) · Load time: 0:00.000 Profile: Default
17°C
Soleggiato
Cerca
10:49
23/10/2024


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications
[Welcome to nginx! - Mozilla...
[capture.pcap [Wireshark 2....
Terminal - analyst@secOps:~
Terminal - analyst@secOps:~
04:55
analyst
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
*** Stopping 5 hosts
H1 H2 H3 H4 R1
*** Done
[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 udpbutest mnexec ivs 2> /dev/null
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udpbutest 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 show
*** Killing stale mininet node processes
pkill -9 -f mininet:
*** Shutting down stale tunnels
pkill -9 -f Tunnel=Ethernet
pkill -9 -f .ssh/mn
rm -f ~/.ssh/mn/*
*** Cleanup complete.
[analyst@secOps ~]$
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ man tcpdump
[analyst@secOps ~]$ tcpdump -r /home/analista/capture.pcap tcp -c 3
tcpdump: /home/analista/capture.pcap: No such file or directory
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
04:43:55.997425 IP 10.0.0.11.37174 > 172.16.0.40.http: Flags [S], seq 4128888120, win 29200, options [mss 1460,sackOK,TS val 318901274 ecr 0,nop,wscale 9], length 0
04:43:55.997552 IP 172.16.0.40.http > 10.0.0.11.37174: Flags [S.], seq 2658173541, ack 4128888121, win 28960, options [mss 1460,sackOK,TS val 3861225662 ecr 318901274,nop,wscale 9], length 0
04:43:55.997590 IP 10.0.0.11.37174 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 318901274 ecr 3861225662], length 0
[analyst@secOps ~]$
CTRL (DESTRA)
17°C
Soleggiato
Cerca
10:55
23/10/2024