Tugas Cyber Security

Pertemuan 2

5.1.5 Lab – Tracing a Route

Nama	**: Lukas Febrian Laufra**
Kelas/Nim	**: TI22J/20220040076**
Dosen Pengajar	**: Pak Ir. Somantri, S.T, M.Kom**
Waktu Pengerjaan	**: 19.57/Kamis, 14 September 2024**

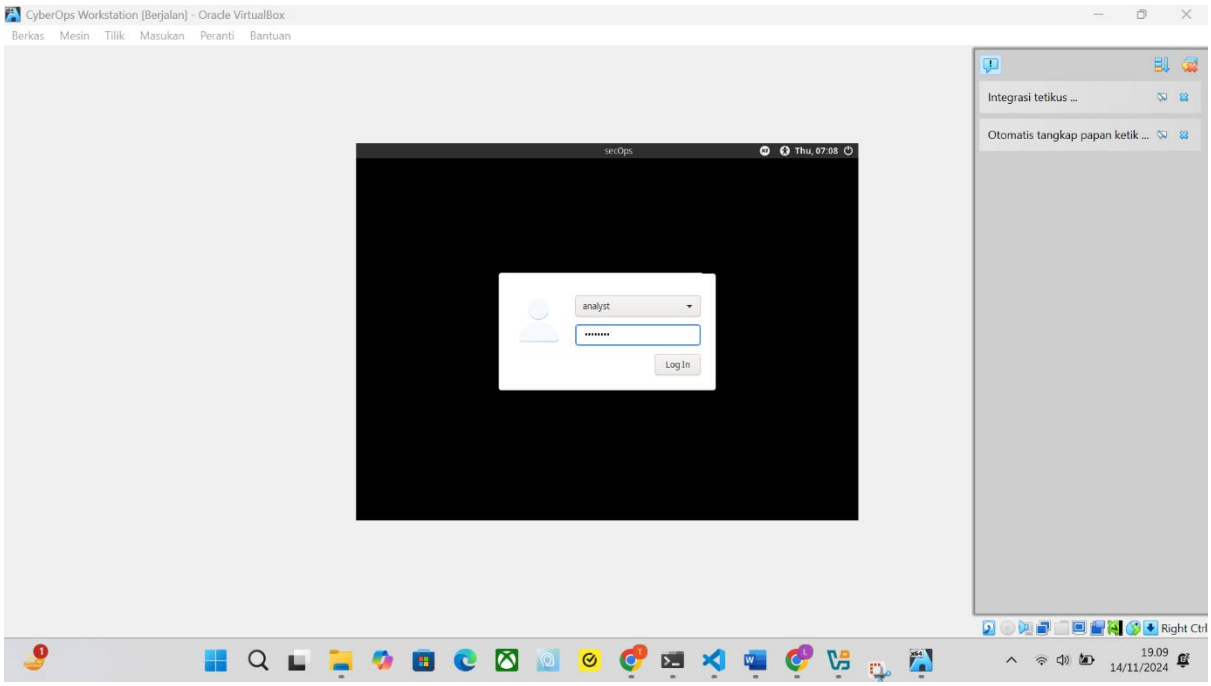
Instructions

Step 1: Verifying Network Connectivity Using Ping

a. Start the CyberOps Workstation VM. Log into the VM with the following credentials:

Username: **analyst**

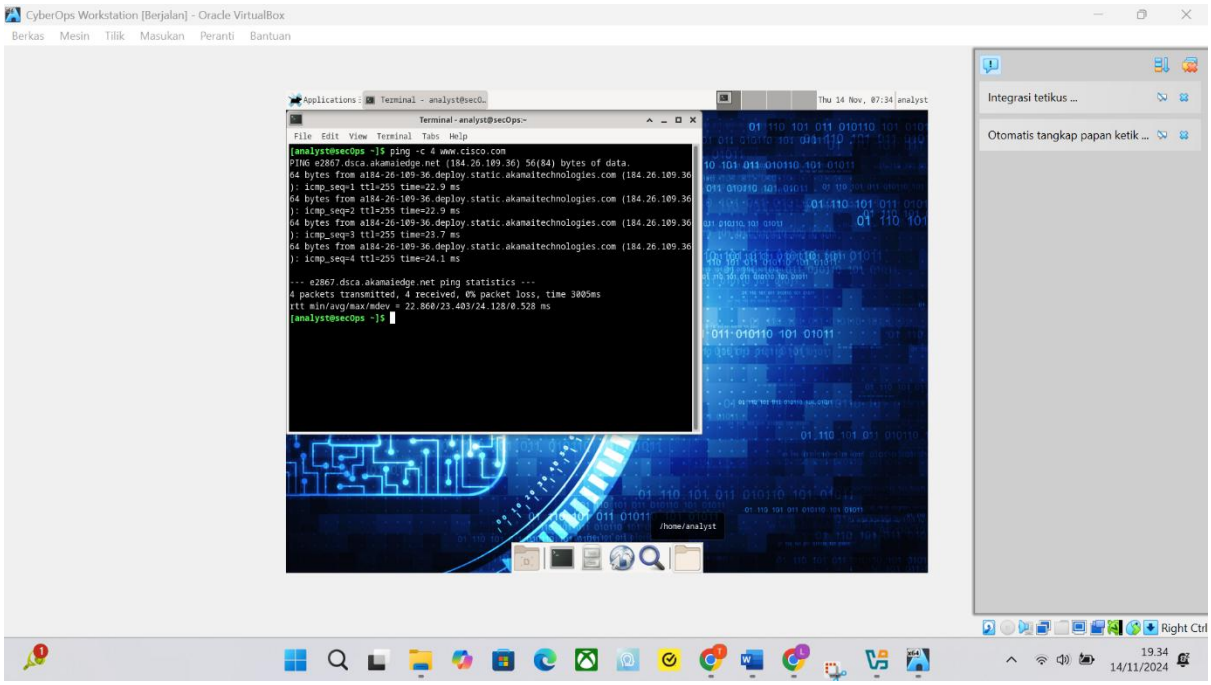
Password: **cybercops**



b. Open a terminal window in the VM to ping a remote server, such as www.cisco.com.

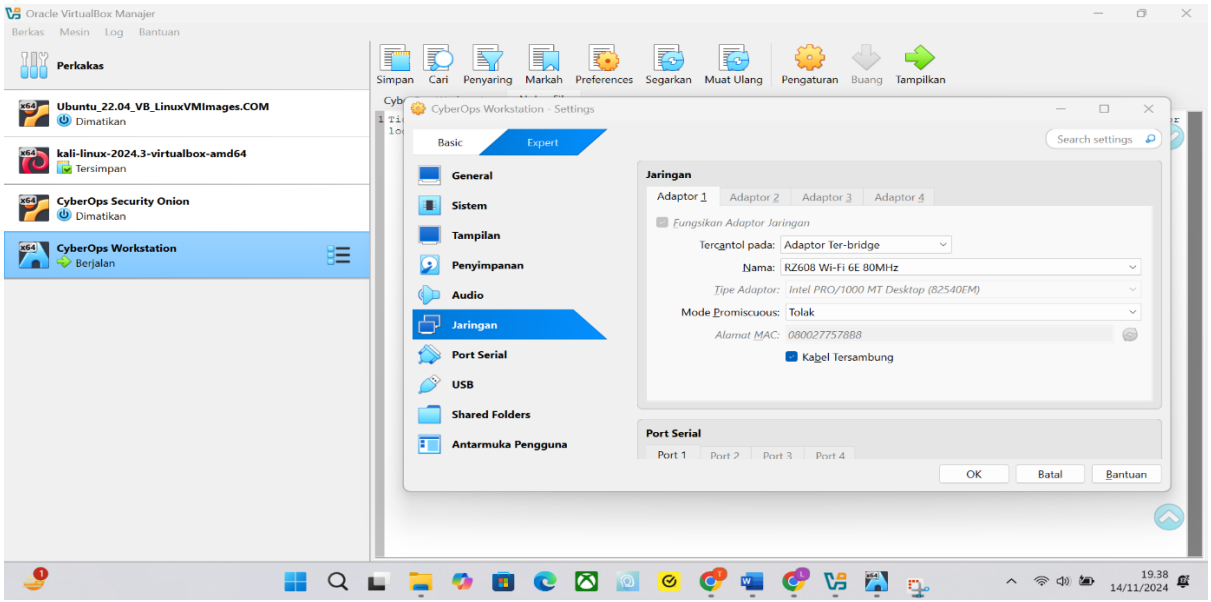
```
[analyst@secOps ~]$ ping -c 4 www.cisco.com
PING e2867.dsca.akamaiedge.net (184.24.123.103) 56(84) bytes of
data.
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com
(184.24.123.103): icmp_seq=1 ttl=59 time=13.0 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com
(184.24.123.103): icmp_seq=2 ttl=59 time=12.5 ms
```

```
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com
(184.24.123.103): icmp_seq=3 ttl=59 time=14.9 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com
(184.24.123.103): icmp_seq=4 ttl=59 time=11.9 ms ---
e2867.dsca.akamaiedge.net ping statistics --- 4 packets
transmitted, 4 received, 0% packet loss, time 3005ms rtt
min/avg/max/mdev = 11.976/13.143/14.967/1.132 ms
```



Step 2: Tracing a Route to a Remote Server Using Traceroute

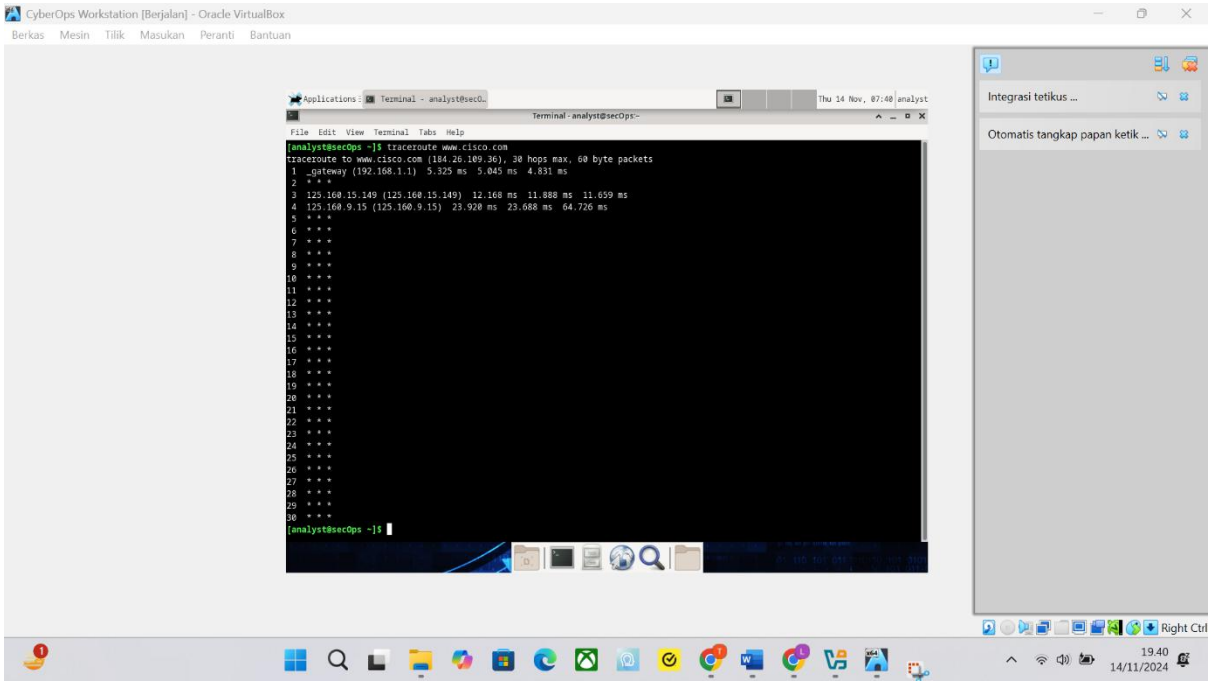
Note: CyberOps Workstation VM network settings may need to be set to bridged adapter if you are not getting any traceroute results. To check your network settings, go to: Machine > Settings, select Network, the tab Adapter 1, Attached to: Bridged Adapter.



To do this, the traceroute tool is used.

a. At the terminal prompt, type traceroute www.cisco.com.

```
[analyst@secOps ~]$ traceroute www.cisco.com
traceroute to www.cisco.com (184.24.123.103), 30 hops max, 60 byte packets
1. 192.168.1.1 (192.168.1.1) 6.527 ms 6.783 ms 6.826 ms
2. 10.39.176.1 (10.39.176.1) 27.748 ms 27.533 ms 27.480 ms
3. 100.127.65.250 (100.127.65.250) 27.864 ms 28.570 ms 28.566 ms
4. 70.169.73.196 (70.169.73.196) 29.063 ms 35.025 ms 33.976 ms
5. fed1bbrj01.xe110.0.rd.sd.cox.net (68.1.0.155) 39.101 ms 39.120 ms 39.108 ms
6. a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103) 38.004 ms 13.583 ms 13.612 ms
```



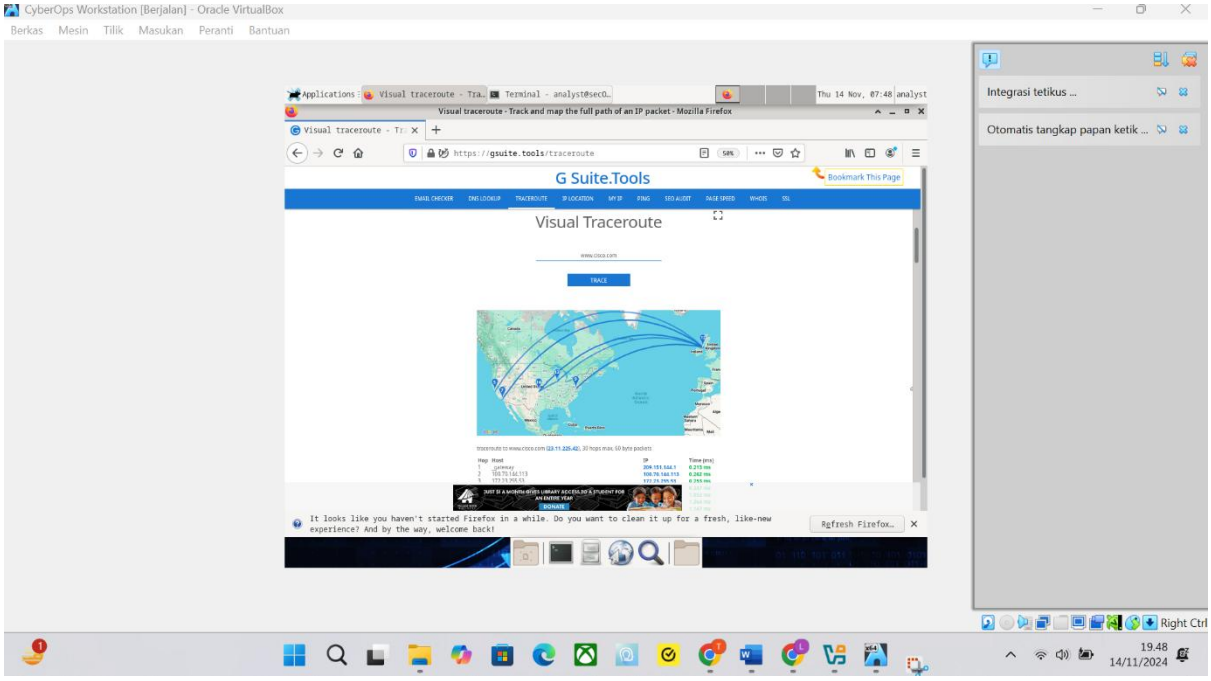
b. If you would like to save the traceroute output to a text file for later review, use the right carat (>) and the desired filename to save the output in the present directory. In this example, the traceroute output is saved in the /home/analyst/cisco-traceroute.txt file.

```
[analyst@secOps ~]$ traceroute www.cisco.com > cisco-traceroute.txt
```

You can now enter the cat cisco-traceroute.txt command to view the output of the trace stored in the text file.

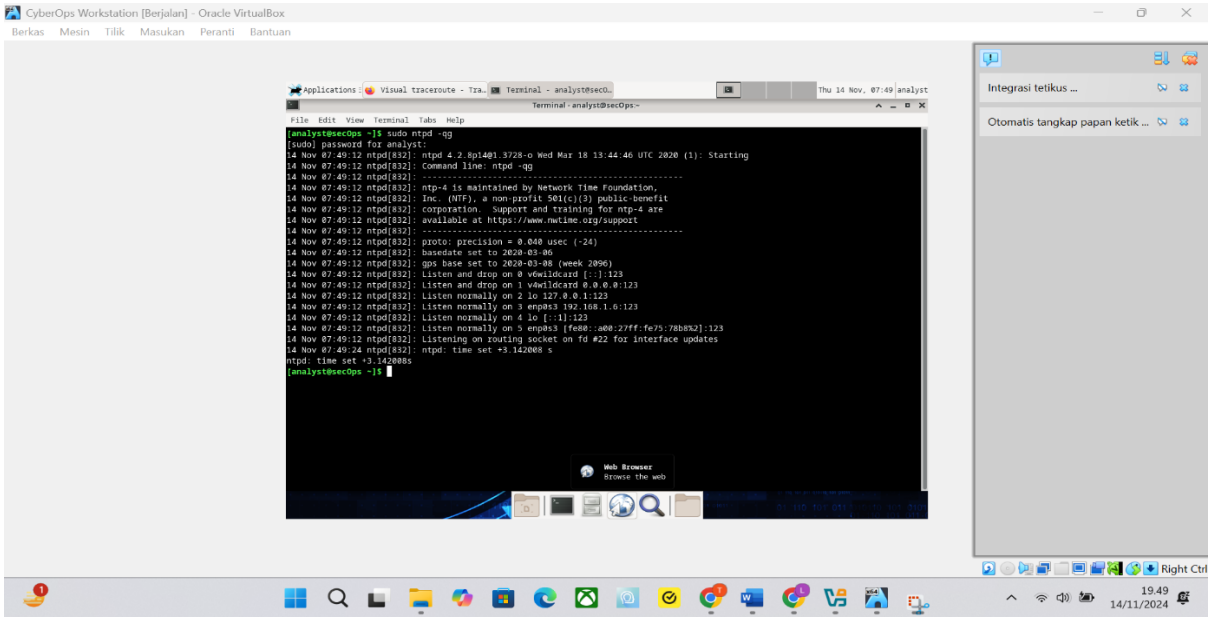
Step 3: Trace a Route to a Remote Server Using Web-Based Traceroute Tool

a. Open a web browser in the VM and search for a visual traceroute tool that you can use in the web browser.
   Try going to the following website: https://gsuite.tools/traceroute
b. Enter any website you wish. Example: www.cisco.com and press Trace.



Note: If you get the error "SEC_ERROR_OCSP_FUTURE_RESPONSE" in Firefox then the CyberOps Workstation clock/time is incorrect. To fix the time enter the following command to update the clock/time then refresh the web browser and enter the visual trace:

```
[analyst@secOps ~]$ sudo ntpd -qg
```



Review the geographical locations of the responding hops. What did you observe regarding the path?

- Saya mengamati dari satu titik ke 5 titik tertentu, dan didalam titik tersebut masing-masing memiliki angka yang satu titik itu 12 yang menghubungkan ke 5 titik dengan nomor 5, 7, 14, 13, dan 9.

How is the traceroute different when going to www.cisco.com or other websites from the terminal (see Part 2) rather than from the online website? (Your results may vary depending upon where you are located geographically, and which ISP is providing connectivity to your school.)

- Jika pada terminal yang terjadi adalah agak sedikit lama untuk mendeteksi ip address yang akan kita cari pada www.cisco.com, dibandingkan diwebsitenya langsung, karna website akan langsung memberikan datanya Ketika kita search, kalua menggunakan terminal dia harus import/export data dari www.cisco.com, itu yang saya rasakan.