Using Traceroute in Linux

Objective:

Learn how to use Traceroute in Linux to trace the route to a host.

Purpose:

Traceroute is used to trace the route to a host. This is useful for finding out if the host is up, where the host is located, and how many hops the server is away from you.

Tool:

Kali Linux

Topology:

We will use Kali Linux for this lab.

Walkthrough:

Task 1:

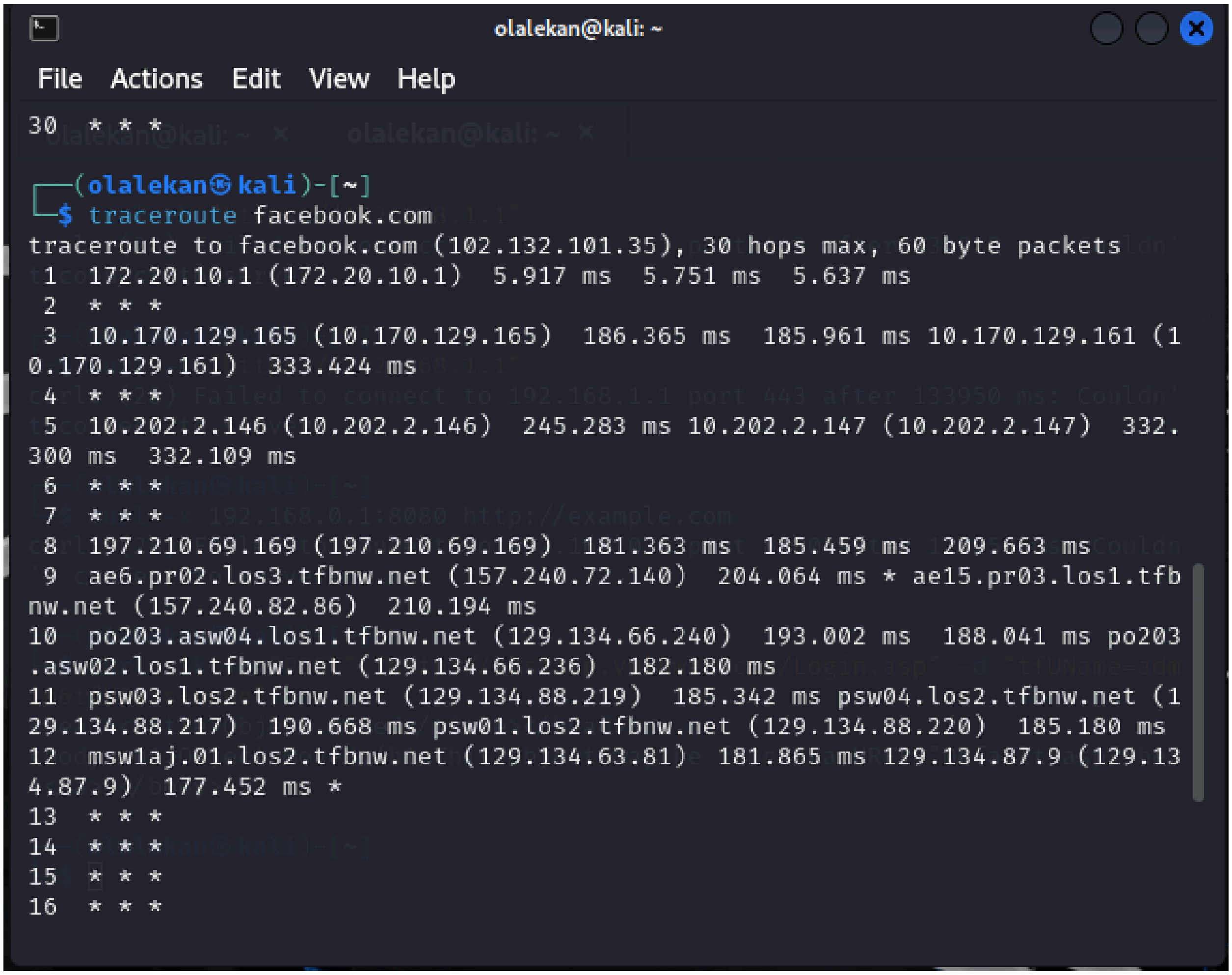
To install traceroute on Kali Linux, simply open a terminal and type the following:

```
sudo apt-get install traceroute
```

In this lab, we will demonstrate how this tool works by using Kali Linux. Begin by opening a terminal window. It is important to note that we can use “traceroute” for any host as it is considered public knowledge. Therefore, we can use any site as our target site for this lab without being “root” user.

We will begin by targeting a big site such as “facebook.com”. Type the following:

```
traceroute facebook.com
```



```
30  * * *

┌──(olalekan㉿kali)-[~]
└─$ traceroute facebook.com
traceroute to facebook.com (102.132.101.35), 30 hops max, 60 byte packets
 1  172.20.10.1 (172.20.10.1)  5.917 ms  5.751 ms  5.637 ms
 2  * * *
 3  10.170.129.165 (10.170.129.165)  186.365 ms  185.961 ms 10.170.129.161 (1
0.170.129.161)  333.424 ms
 4  * * *
 5  10.202.2.146 (10.202.2.146)  245.283 ms 10.202.2.147 (10.202.2.147)  332.
300 ms  332.109 ms
 6  * * *
 7  * * *
 8  197.210.69.169 (197.210.69.169)  181.363 ms  185.459 ms  209.663 ms
 9  ae6.pr02.los3.tfbnw.net (157.240.72.140)  204.064 ms * ae15.pr03.los1.tfb
nw.net (157.240.82.86)  210.194 ms
10  po203.asw04.los1.tfbnw.net (129.134.66.240)  193.002 ms  188.041 ms po203
.asw02.los1.tfbnw.net (129.134.66.236)  182.180 ms
11  psw03.los2.tfbnw.net (129.134.88.219)  185.342 ms psw04.los2.tfbnw.net (1
29.134.88.217)  190.668 ms psw01.los2.tfbnw.net (129.134.88.220)  185.180 ms
12  msw1aj.01.los2.tfbnw.net (129.134.63.81)  181.865 ms 129.134.87.9 (129.13
4.87.9)  177.452 ms *
13  * * *
14  * * *
15  * * *
16  * * *
```

1) The very first line after the traceroute shows Hostname and IP address, which it has obtained by using the reverse DNS look up.

2) 30 hops means that traceroute will only route the first 30 routes between your system and the victim's system. 30 is often too much; it usually ends in 3 to 15 hops, though it can sometime go deeper depending on the site's security and lack of response.

3) This is the first router; possibly our AP, modem, router, etc.

These are the IP address ranges for private IP's:
10.0.0.0 – 10.255.255.255,
172.16.0.0 – 172.31.255.255,
192.168.0.0 – 192.168.255.255,
224.0.0.0 – 239.255.255.255

4) These three columns display the round trip time(s) for our packet to reach that point and return to our computer. This is listed in milliseconds. There are three columns because the traceroute sends three separate signal packets. This is for display consistency—or a lack thereof—in the route.

5) This is the first column and is simply the number of the hop along the route.

6) This means that the target system could not be reached. Requests timed out. More accurately, it means that the packets could not make it there and back; they may actually be reaching the target system but encountering problems on the return trip. This is possibly due to some kind of error, but it may also be an intentional block due to a firewall or other security measures, and the block may affect tracing the route but not actual server connections.

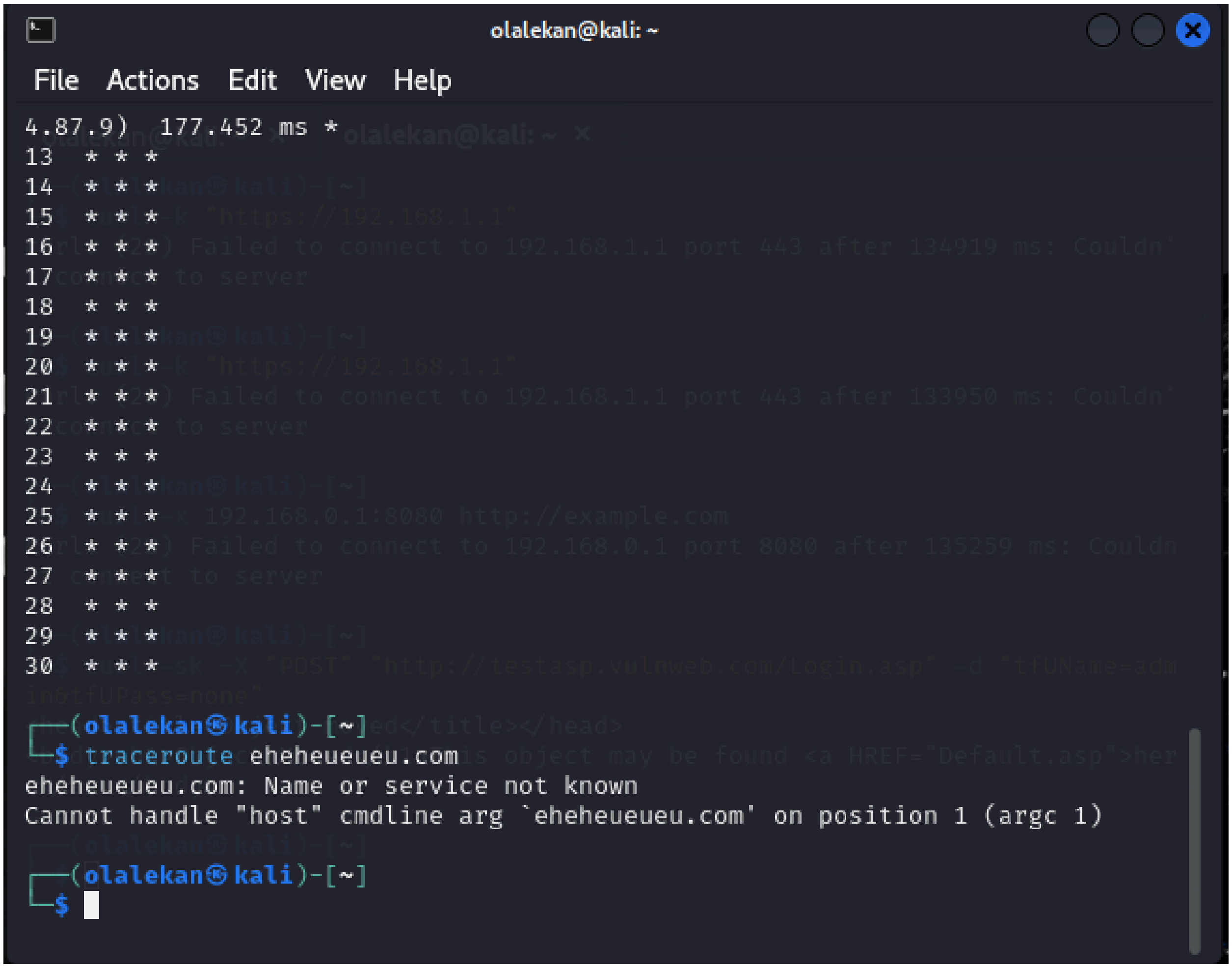
7) It shows our last destination, which has the same IP address as the first line.

This is extremely useful for finding a whole range of information, all of which will be displayed during the trace. We can also see that the host is two hops away from us, and the IP addresses of each of the servers our request had went through to reach our target.

Task 2:

Traceroute is also useful for determining if a host is up. For example, try targeting the following host:

```
traceroute eheheueueu.com
```



```
4.87.9)  177.452 ms *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *

┌──(olalekan㉿kali)-[~]
└─$ traceroute eheheueueu.com
eheheueueu.com: Name or service not known
Cannot handle "host" cmdline arg `eheheueueu.com' on position 1 (argc 1)

┌──(olalekan㉿kali)-[~]
└─$ 
```

We can see that this hostname doesn’t exist through traceroute.
We can also see if the hostname exists but is down. It is possible to understand this if we take the following response: