

Lab 11 – Using Traceroute in Linux

Lab Objective:

Using Traceroute in Linux to trace the route to a host.

Lab 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.

Lab Tool:

Kali Linux

Lab Topology:

Using Kali Linux for this lab.

STEP 1:

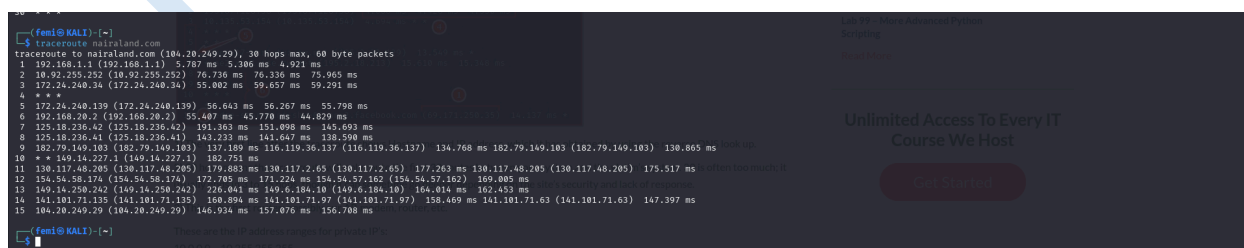
To install traceroute on Kali Linux, simply open a terminal and type the following:

```
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 nairaland.com
```



```
(femi@KALI)~$ traceroute nairaland.com
traceroute to nairaland.com (104.20.249.20), 30 hops max, 60 byte packets
 0  192.168.1.1 (192.168.1.1)  5.787 ms  5.306 ms  4.921 ms
 1  10.92.255.252 (10.92.255.252)  76.736 ms  76.336 ms  75.965 ms
 2  172.24.240.34 (172.24.240.34)  55.002 ms  59.637 ms  59.291 ms
 * * *
 5  172.24.240.139 (172.24.240.139)  56.643 ms  56.267 ms  55.798 ms
 6  192.168.28.2 (192.168.28.2)  55.487 ms  45.778 ms  44.839 ms
 7  125.18.236.42 (125.18.236.42)  191.363 ms  151.098 ms  145.693 ms
 8  125.18.236.41 (125.18.236.41)  143.233 ms  141.647 ms  138.598 ms
 9  182.79.149.103 (182.79.149.103)  137.189 ms  116.119.36.137 (116.119.36.137)  134.768 ms  182.79.149.103 (182.79.149.103)  130.865 ms  100.100 ms
 10 * * * 149.14.227.1 (149.14.227.1)  182.751 ms
 11 130.117.48.205 (130.117.48.205)  179.883 ms 130.117.2.65 (130.117.2.65)  177.263 ms 130.117.48.205 (130.117.48.205)  175.517 ms
 12 154.54.58.174 (154.54.58.174)  172.705 ms 171.224 ms 154.54.57.162 (154.54.57.162)  169.805 ms
 13 149.14.250.242 (149.14.250.242)  226.041 ms 149.6.184.10 (149.6.184.10)  164.014 ms 162.453 ms
 14 141.101.71.135 (141.101.71.135)  160.894 ms 141.101.71.97 (141.101.71.97)  150.469 ms 141.101.71.63 (141.101.71.63)  147.397 ms
 15 104.20.249.20 (104.20.249.20)  146.934 ms 157.070 ms 155.788 ms
(femi@KALI)~$
```

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.

STEP 2:

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

traceroute eheheueueu.com

```
15 104.20.249.29 (104.20.249.29) 146.934 ms 157.076 ms 156.708 ms
(femi@KALI)-[~]
$ traceroute eheheueueu.com
eheheueueu.com: Name or service not known
Cannot handle 'host' cmdline arg 'eheheueueu.com' on position 1 (arg 1)
(femi@KALI)-[~]
$
```

FEMILANA