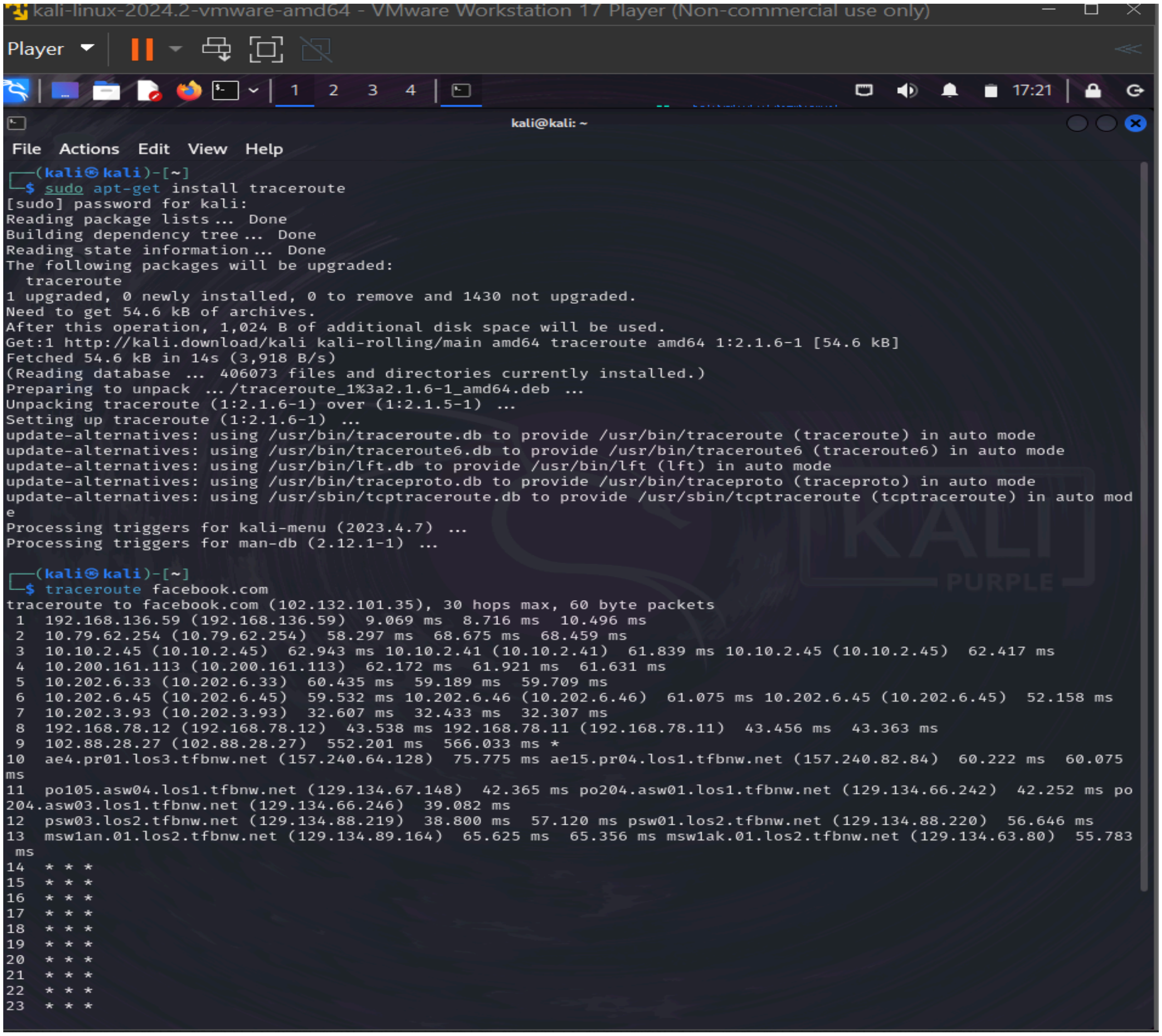
USING TRACEROUTE COMMAND IN LINUX

Tools : KALI LINUX [TRACEROUTE]
Project-Site : facebook.com

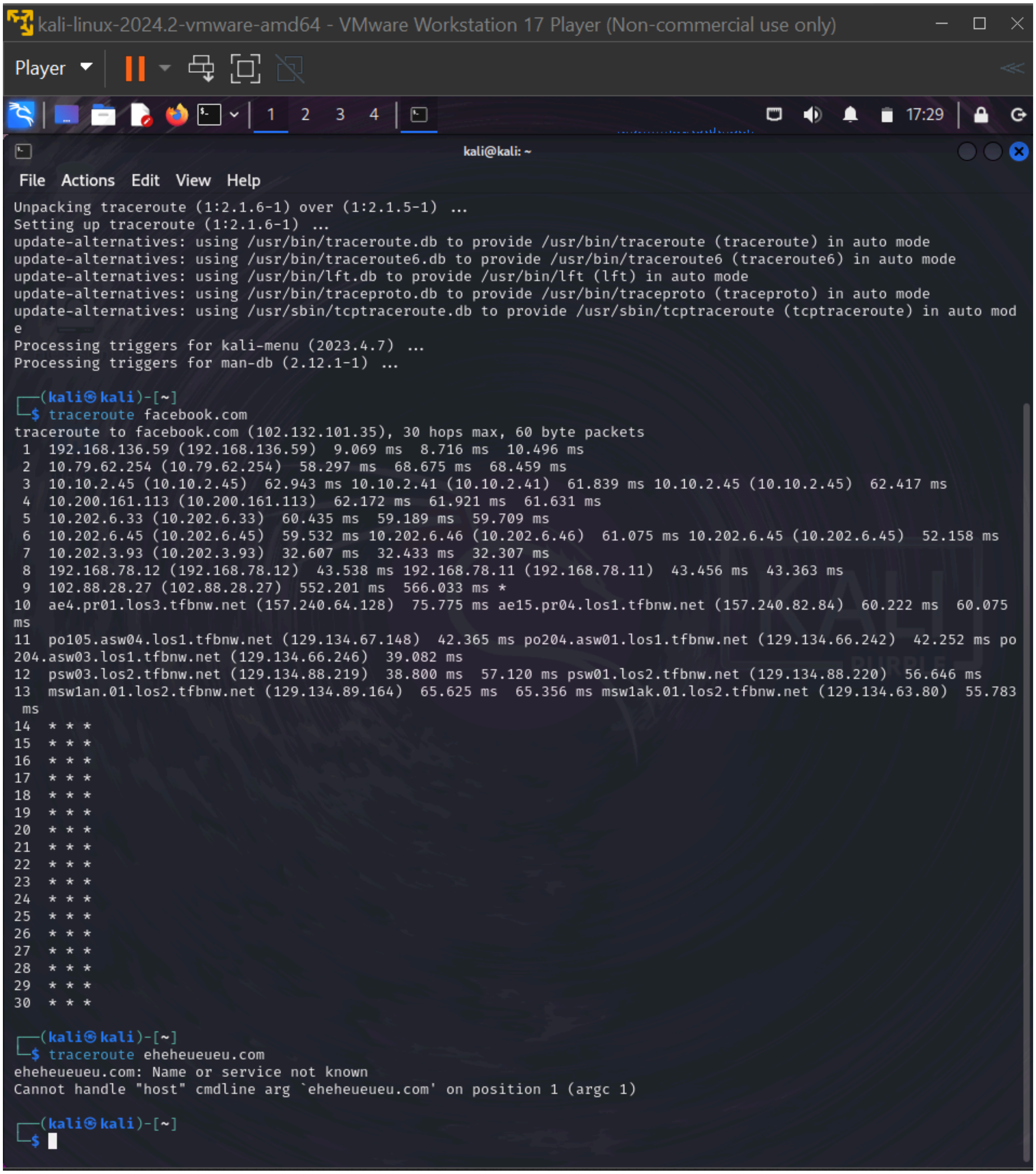
The `traceroute` command is a network diagnostic tool used to trace the path that packets take from your computer to a specified destination (like a website or server). It shows each hop along the route and measures the time taken for each segment.

Input from Kali : TRACEROUTE


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
17:21
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install traceroute
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages will be upgraded:
  traceroute
1 upgraded, 0 newly installed, 0 to remove and 1430 not upgraded.
Need to get 54.6 kB of archives.
After this operation, 1,024 B of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 traceroute amd64 1:2.1.6-1 [54.6 kB]
Fetched 54.6 kB in 14s (3,918 B/s)
(Reading database ... 406073 files and directories currently installed.)
Preparing to unpack .../traceroute_1%3a2.1.6-1_amd64.deb ...
Unpacking traceroute (1:2.1.6-1) over (1:2.1.5-1) ...
Setting up traceroute (1:2.1.6-1) ...
update-alternatives: using /usr/bin/traceroute.db to provide /usr/bin/traceroute (traceroute) in auto mode
update-alternatives: using /usr/bin/traceroute6.db to provide /usr/bin/traceroute6 (traceroute6) in auto mode
update-alternatives: using /usr/bin/lft.db to provide /usr/bin/lft (lft) in auto mode
update-alternatives: using /usr/bin/traceproto.db to provide /usr/bin/traceproto (traceproto) in auto mode
update-alternatives: using /usr/sbin/tcptraceroute.db to provide /usr/sbin/tcptraceroute (tcptraceroute) in auto mod
e
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.1-1) ...

┌──(kali㉿kali)-[~]
└─$ traceroute facebook.com
traceroute to facebook.com (102.132.101.35), 30 hops max, 60 byte packets
 1  192.168.136.59 (192.168.136.59)  9.069 ms  8.716 ms  10.496 ms
 2  10.79.62.254 (10.79.62.254)  58.297 ms  68.675 ms  68.459 ms
 3  10.10.2.45 (10.10.2.45)  62.943 ms 10.10.2.41 (10.10.2.41)  61.839 ms 10.10.2.45 (10.10.2.45)  62.417 ms
 4  10.200.161.113 (10.200.161.113)  62.172 ms  61.921 ms  61.631 ms
 5  10.202.6.33 (10.202.6.33)  60.435 ms  59.189 ms  59.709 ms
 6  10.202.6.45 (10.202.6.45)  59.532 ms 10.202.6.46 (10.202.6.46)  61.075 ms 10.202.6.45 (10.202.6.45)  52.158 ms
 7  10.202.3.93 (10.202.3.93)  32.607 ms  32.433 ms  32.307 ms
 8  192.168.78.12 (192.168.78.12)  43.538 ms 192.168.78.11 (192.168.78.11)  43.456 ms  43.363 ms
 9  102.88.28.27 (102.88.28.27)  552.201 ms  566.033 ms *
10  ae4.pr01.los3.tfbnw.net (157.240.64.128)  75.775 ms ae15.pr04.los1.tfbnw.net (157.240.82.84)  60.222 ms  60.075
ms
11  po105.asw04.los1.tfbnw.net (129.134.67.148)  42.365 ms po204.asw01.los1.tfbnw.net (129.134.66.242)  42.252 ms po
204.asw03.los1.tfbnw.net (129.134.66.246)  39.082 ms
12  psw03.los2.tfbnw.net (129.134.88.219)  38.800 ms  57.120 ms psw01.los2.tfbnw.net (129.134.88.220)  56.646 ms
13  msw1an.01.los2.tfbnw.net (129.134.89.164)  65.625 ms  65.356 ms msw1ak.01.los2.tfbnw.net (129.134.63.80)  55.783
 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
```


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
17:29
kali@kali: ~
File Actions Edit View Help

```
Unpacking traceroute (1:2.1.6-1) over (1:2.1.5-1) ...
Setting up traceroute (1:2.1.6-1) ...
update-alternatives: using /usr/bin/traceroute.db to provide /usr/bin/traceroute (traceroute) in auto mode
update-alternatives: using /usr/bin/traceroute6.db to provide /usr/bin/traceroute6 (traceroute6) in auto mode
update-alternatives: using /usr/bin/lft.db to provide /usr/bin/lft (lft) in auto mode
update-alternatives: using /usr/bin/traceproto.db to provide /usr/bin/traceproto (traceproto) in auto mode
update-alternatives: using /usr/sbin/tcptraceroute.db to provide /usr/sbin/tcptraceroute (tcptraceroute) in auto mod
e
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.1-1) ...

┌──(kali㉿kali)-[~]
└─$ traceroute facebook.com
traceroute to facebook.com (102.132.101.35), 30 hops max, 60 byte packets
 1  192.168.136.59 (192.168.136.59)  9.069 ms  8.716 ms  10.496 ms
 2  10.79.62.254 (10.79.62.254)  58.297 ms  68.675 ms  68.459 ms
 3  10.10.2.45 (10.10.2.45)  62.943 ms 10.10.2.41 (10.10.2.41)  61.839 ms 10.10.2.45 (10.10.2.45)  62.417 ms
 4  10.200.161.113 (10.200.161.113)  62.172 ms  61.921 ms  61.631 ms
 5  10.202.6.33 (10.202.6.33)  60.435 ms  59.189 ms  59.709 ms
 6  10.202.6.45 (10.202.6.45)  59.532 ms 10.202.6.46 (10.202.6.46)  61.075 ms 10.202.6.45 (10.202.6.45)  52.158 ms
 7  10.202.3.93 (10.202.3.93)  32.607 ms  32.433 ms  32.307 ms
 8  192.168.78.12 (192.168.78.12)  43.538 ms 192.168.78.11 (192.168.78.11)  43.456 ms  43.363 ms
 9  102.88.28.27 (102.88.28.27)  552.201 ms  566.033 ms *
10  ae4.pr01.los3.tfbnw.net (157.240.64.128)  75.775 ms ae15.pr04.los1.tfbnw.net (157.240.82.84)  60.222 ms  60.075
ms
11  po105.asw04.los1.tfbnw.net (129.134.67.148)  42.365 ms po204.asw01.los1.tfbnw.net (129.134.66.242)  42.252 ms po
204.asw03.los1.tfbnw.net (129.134.66.246)  39.082 ms
12  psw03.los2.tfbnw.net (129.134.88.219)  38.800 ms  57.120 ms psw01.los2.tfbnw.net (129.134.88.220)  56.646 ms
13  msw1an.01.los2.tfbnw.net (129.134.89.164)  65.625 ms  65.356 ms msw1ak.01.los2.tfbnw.net (129.134.63.80)  55.783
 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *

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

┌──(kali㉿kali)-[~]
└─$ 
```

RESULT AND EXAMPLES OF USING TRACEROUTE COMMAND.

Here we used traceroute in linux to trace the route to a host. 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.

We first start by installing traceroute on kali linux with the following command. [sudo apt-get install traceroute] 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]. I would explain the result briefly

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 sometimes 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 gone through to reach our target.

We can also use traceroute for determining if a host is up. For example we can try targeting the following host [traceroute eheheueueu.com]. We can see that this hostname doesn't exist through traceroute. We can also see if the hostname exists but is down To determine if a hostname exists but is down, you can look for specific responses from commands like `ping` or `traceroute`.

Response Interpretation

When you ping a hostname, you might receive different responses:

1. **Successful Response**: If you receive replies from the IP address, the hostname is reachable and likely operational.
2. **Destination Unreachable**: If the response indicates "Destination Host Unreachable," this means the host may be down or there is a network issue.

3. **Request Timed Out**: If you get a timeout, the host could be down, or it may not be responding to ICMP requests due to firewall settings.

Using `ping` and `traceroute`

Ping Command:
bash
Copy code

```
ping example.com
```

-

Traceroute Command:
bash
Copy code

```
traceroute example.com
```

-

Conclusion

By combining the results from these commands, you can assess whether a hostname is down or if the issue lies elsewhere in the network. If `ping` fails but `traceroute` shows responses up to a certain hop, it suggests that the hostname is likely down, while the network path is otherwise operational.