Exercise 1b: Working with Command Line Tools – traceroute

Date: 02.03.2023

What is traceroute?

- A Traceroute command is a command line tool that is generally used to locate the destination path from the host in the network.
- It will tell us about all the intermediate hops the data packet came across while traveling into the network to reach the destination host.
- This command is useful when you want to know about the route and about all the hops that a packet takes.
- Thus, it is used in tracing and troubleshooting network problems.

How to install traceroute in Linux?

To perform a trace route in Linux open Terminal and type in **"traceroute domain.com"** replacing domain.com with your domain name or IP address. If you do not have trace route installed you may need to install it.

- In the Linux system, install the traceroute **if it is not by default** installed on your PC.
- The traceroute command will execute the route to the host that the packet travels to reach the destination.
- **To install the traceroute on the Linux system, use the following commands:**
- For **Ubuntu or Debian** using the following syntax:

  $ sudo apt-get install traceroute
- So, when you execute the above command into Linux, it will install the traceroute into the system and is ready for use to trace the route of the packets.

How to use traceroute in Linux?

Syntax:

The underlying syntax of traceroute used in Linux:

```
traceroute [OPTIONS] <host address> [packet length]
```

- In this syntax, **traceroute** is the keyword that invokes the command to perform the action of traceroute,
- [OPTIONS] is an **optional parameter** that might or might not be required as per the requirement of the utility.

- In the <host address>we would be entering the address where we would need to trace the journey of the flow.
- [packet length] is again an **optional parameter** for specifying the size of the UDP (User Datagram Protocol) packets that need to be sent in order for the tracing to work effectively.
- In the [OPTIONS] in traceroute, we have multiple options which can be chosen as per the requirement of the developer.

Basic Usage

- The primary method for using traceroute is quite simple. A
- ll traceroute requires is the destination to perform the **probing**.
- The destination can be either a domain or an IP address.
- If a network is configured to block the traceroute signal, then this probe will be denoted with **asterisks** (*).

IPv4 or IPv6

By default, traceroute will use the default Internet Protocol with which your system is configured. To manually set the IP version, follow the procedure below.

- To tell traceroute to use IPv4, use the “-4” flag
- To tell traceroute to use IPv6, use the “-6” flag

Testing Ports

- If there is a need to test a specific port, the port can be specified using the “-p” flag.
- For UDP tracing, traceroute will start with the given value and increase with each probe.
- For ICMP tracing, the value will determine the initial ICMP sequence value.
- For TCP and others, this will be the constant destination port to connect.

Hiding Device Names

- In some situations, the device names in the output may make the output look messy.

- For more clarity, you can hide the device names from the output. To do so, use the "-n" (no mapping) flag.

Traceroute Timeout Limit

- By default, traceroute waits for 5 seconds to receive a response. In certain situations, you may want to change the waiting time to be greater or less than 5 seconds.
- To do so, use the "-w" flag. Note that the time value is a floating-point number.

Probing Methods

There are multiple methods that you can use to probe the remote address.

- To specify traceroute to use ICMP echo, use the "-I" flag.
- To use TCP SYN for probing, use the "-T" flag.

Setting the Maximum Number of Hops

- By default, traceroute will track 30 hops. Traceroute offers the ability to manually set the number of hops to track.
- Use the "-m" flag with the number of hops:

Specifying the Interface

- If there are multiple network interfaces connected to the computer, then it may help to specify the network interface to use for sending packets.

- To specify the network interface, use the "-i" flag.

Defining the Number of Queries for a Hop

- To define the number of queries for a hop, specify this number using the "-q" flag.

Routing Packets through a Gateway

- To route packets through a certain gateway, use the "-g" option, followed by the gateway.

Traceroute Help Page

- The above demonstrations are just some of the common usages of traceroute, and there are even more features for you to use.

- To get quick help, open the traceroute help page with the following command.

```
traceroute --help
```

Important Note:

As we can see the traceroute logs extracted from Linux machines,

The network packets before reaching from source to destination travels to various routers, hence whenever a packet is forwarded to the next router a hop occurs, and generally traceroute command fetches results of maximum of 30 hops, **the more the hops mean it indicates slower network connection, while, fewer hops mean fast access**.

Limits of Traceroute:
In some cases, Firewalls can block packets in between the source and destination making traceroute to reach maximum hops without getting any result, in such cases, the logs will be displayed with an asterisk in place of IP Address.
For Example: *$ traceroute google.com*
traceroute to google.com (209.85.231.104), 30 hops max, 52 byte packets

*1 * * **

*2 * * **

*3 * * **

*4 * * **

*****