EXPERIMENT-4

MAPPED COURSE OUTCOME: CO1

CO1: Understand concepts of information security and tools

AIM:

Using Windows/Linux tool to trace the route of a packet and explain the terminology

MANUAL OF THE EXPERIMENT:

What is Tracert?

The **Windows Tracert** tool determines the route to a destination by sending ICMP packets to the destination.

In these packets, **Tracert** uses varying IP Time-To-Live (TTL) values.

The TTL is effectively a *hop* counter, where a *hop* is a location that the packet stops at, to reach the destination.

The tool may take some time to complete (particularly if there is a problem), as the tool waits for responses (which may not come).

What is Traceroute?

Traceroute is the route tracing tool used on Unix-like Operating Systems (including **Mac OS X**).

On **Mac OS X**, you can access Traceroute through the Network Utility.

How do I use Tracert?

To use tracert, you must be running Microsoft Windows.

1. Open a **Command Prompt**
- Click on the **Start Menu** and in the search bar, type 'cmd', and press **Enter**.
- **OR** press **Windows Key + R** to open the **Run Prompt**. Type 'cmd', then click **OK** (or press **Enter**)

1. In the **Command Prompt** window, type 'tracert' followed by the destination, either an IP Address or a Domain Name, and press **Enter**.
- e.g. tracert google.co.nz
- **OR** tracert 216.58.196.131

1. The command will return output indicating the hops discovered and time (in milliseconds) for each hop.

Figure 1: The output of the TraceRT command

How do I use Traceroute (via Network Utility)?

To use Traceroute via the Network Utility, you must be running Apple Mac OS X.

1. Open the **Network Utility**

- Open **Spotlight** (**Left Cmd + Spacebar** or Click the **Magnifying Glass** on the right of the **Menu Bar**). Type **Network Utility** and press **Enter**.

Figure 2: Searching for Network Utility in Spotlight

- In OS X Mavericks and later, Network Utility is in **/System/Library/CoreServices/Applications**.[2]
- In OS X Mountain Lion, Lion, and Snow Leopard, Network Utility is in the **Utilities folder** of your **Applications folder**.[2]

1. In Network Utility, choose Traceroute. Enter a destination into the box, either an IP Address or a Domain Name, and click **Trace**.

- e.g. google.co.nz
- **OR** 216.58.196.131

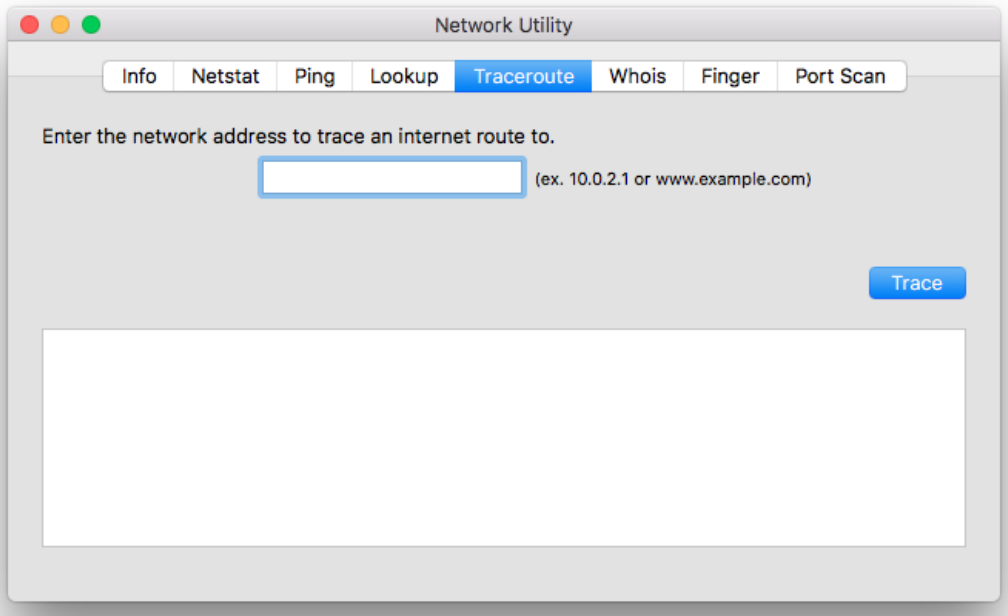

Figure 3: The Network Utility on Mac OS X (Sierra). The Traceroute tool is selected.

1. The results will be printed in the window. You may have to scroll down to see all results (by mousing over the white window and scrolling.)

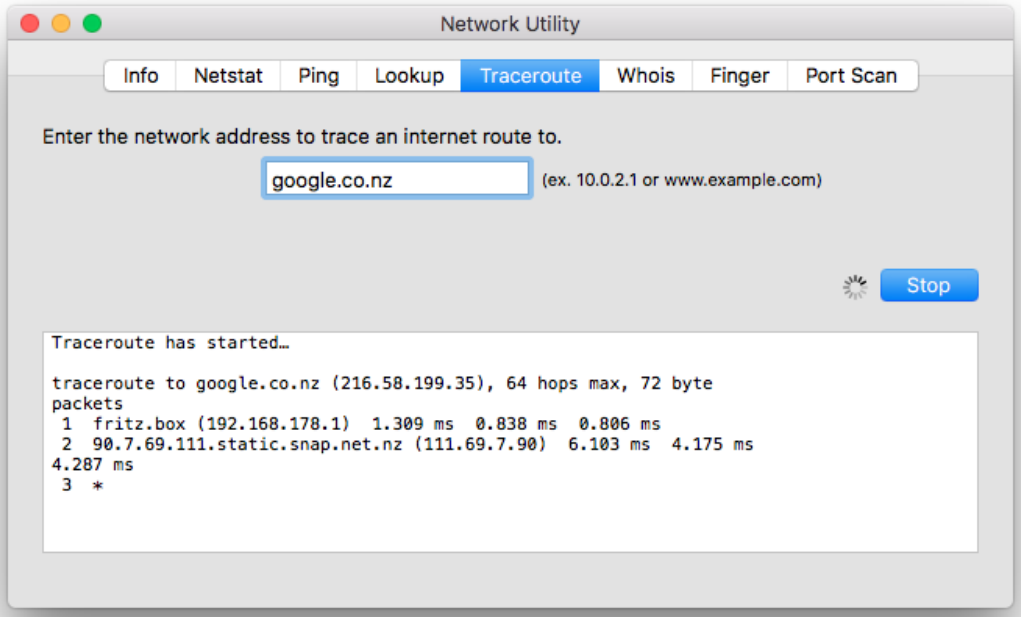

Figure 4: The Traceroute utility running. The button will change from Stop back to Trace when the trace has completed

Interpreting the results

Each entry, or *hop*, is a location that the packet passes through to reach its final destination.

If the trace **times out** on a certain *hop* it can mean there is a problem at that location, or that the route is incorrect, preventing the packet from reaching the destination.

This example trace result is from a PC inside an N4L Managed Network school, to an External IP Address (22.110.0.1):

H:\>tracert 22.110.0.1

Tracing route to 22.110.0.1 over a maximum of 30 hops

1 <1 ms <1 ms <1 ms 172.16.0.5

2 <1 ms <1 ms <1 ms 192.168.0.50

3 6 ms 2 ms 3 ms 122-56-168-186.n4l.sparkdigital.co.nz [122.56.168.186]

4 2 ms 3 ms 3 ms 122-56-99-240.n4l.sparkdigital.co.nz [122.56.99.240]

5 3 ms 3 ms 3 ms 122-56-99-243.n4l.sparkdigital.co.nz [122.56.99.243]

6 3 ms 4 ms 2 ms mdr-ip24-int.msc.global-gateway.net.nz [122.56.116.6]

7 16 ms 4 ms 2 ms ae8-10.akbr6.global-gateway.net.nz [122.56.116.5]

8 * * * Request timed out.

Trace complete.

H:\>

Figure 5: A trace from within an N4L Managed Network to a 'bad' IP address - 22.110.0.1

The first hop is to a routing device upstream of the computer - it returns a response quickly.

The second hop is to the N4L Managed Router on site at the school, on its internal IP address (192.168.0.50).

The third through seventh hops are to routers external to the school. The responses take slightly longer as the hops are located on the other side of the school's Managed Router (2 - 16ms).

The remaining hops show **Request Timed Out** - including the final hop - no packets reach the destination IP address.

This indicates that **no route** for **traffic** to this **destination** can be found outside of N4L's Managed Network (in this case because there is a problem with the destination 22.110.0.1)

Here is a trace from within an N4L Managed Network school to **google.co.nz** (216.58.200.99)

H:\>tracert google.co.nz

Tracing route to google.co.nz [216.58.200.99]

over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 172.16.0.5
2 1 ms 1 ms <1 ms 192.168.0.50
3 3 ms 5 ms 2 ms 122-56-168-186.n4l.sparkdigital.co.nz [122.56.168.186]
4 2 ms 2 ms 3 ms 122-56-99-240.n4l.sparkdigital.co.nz [122.56.99.240]
5 3 ms 3 ms 5 ms 122-56-99-243.n4l.sparkdigital.co.nz [122.56.99.243]
6 * * * Request timed out.
7 2 ms 3 ms 3 ms ae8-10.akbr6.global-gateway.net.nz [122.56.116.5]
8 4 ms 2 ms 3 ms ae7-2.akbr7.global-gateway.net.nz [122.56.119.53]
9 27 ms 27 ms 27 ms xe5-0-0.sgbr3.global-gateway.net.nz [202.50.232.242]
10 27 ms 27 ms 25 ms ae2-10.sgbr4.global-gateway.net.nz [202.50.232.246]
11 28 ms 27 ms 26 ms 72.14.217.100
12 27 ms 27 ms 27 ms 108.170.247.33
13 27 ms 27 ms 27 ms 209.85.250.139
14 27 ms 27 ms 27 ms syd09s14-in-f3.1e100.net [216.58.200.99]

Trace complete.

H:\>

Figure 6: A trace from within an N4L Managed Network to a 'good' IP address - 216.58.200.99 (google.co.nz)

Hops one to five are similar to those in the above example, though **this time a different route is taken**.

Hop six does not necessarily indicate a problem, perhaps instead this router is not responding to ICMP requests.

This trace does not go up to Hop 30 as in the previous example, because Hop 14 is the Destination, and the trace ends.

This trace indicates that **there is a route** through to the IP address 216.58.200.99 (google.co.nz)

RELEVANT DEMONSTRATIVE VIDEO:

- https://youtu.be/xhL5Usvklpo

RELEVANT BOOKS:

T1: Whitman, Michael E. and Herbert J. Mattord. Principles of Information Security. Boston, MA: Course Technology, 2011

T2: Umesh Hodeghatta Rao and Umesh Nayak. The InfoSec Handbook: An introduction to Information Security. APress OpenAccess

OTHER RESOURCE MATERIALS:

R1: Michael Stewart, James. Chapple, Mike. Certified Information System Security Professional Study Guide. Fourth Edition. Wiley Publishing

R2: Rhodes-Ousley, Mark. Information Security: The Complete Reference, Second Edition.

VIVA- QUESTIONS:

1. Ping sweep is also known as _____

A) ICMP sweep

B) SNMP sweep

C) SGNP sweep

D) SICMP sweep

ANSWER: A

2. According to the CIA Triad, which of the below-mentioned element is not considered in the triad?

A) Confidentiality

B) Integrity

C) Authenticity

D) Availability

ANSWER: C

3. _____ is the method used to locate all the DNS-servers and their associated records for an organization.

A) DNS enumeration

B) DNS hacking

C) DNS cracking

D) DNS server hacking

ANSWER: A

4. This is the model designed for guiding the policies of Information security within a company, firm or organization. What is "this" referred to here?

A) Confidentiality

B) Non-repudiation

C) CIA Triad

D) Authenticity

ANSWER: C

5. When you use the word _____ it means you are protecting your data from getting disclosed.

A) Confidentiality

B) Integrity

C) Authentication

D) Availability

ANSWER: A