BIT3105 BAC 2303 BSD 2301 NETWORK PROGRAMMING ASSIGNMENT 1

Section One

In this section, you will explore the various tools that an end user can use to discover how a machine is connected to the network and what the network looks like beyond the first hop. You investigation will use the following tools:

1. netstat
2. traceroute
3. whois

All of these tools should be available on any machine running a UNIX-based operating system.

1. netstat

i). What is *netstat* and what is it used for?

ii). What parameters for *netstat* should you use to show all the TCP connections established? Include a printout of this list for your machine. Be sure to explain what all fields are.

iii). How can use netstat to detect *malicious software*

2. traceroute

i). Explain in detail how *traceroute* works.

ii). Perform a traceroute from your machine to two different locations

- In Europe
- In US

Include a copy of the output and explain what happened including a description of what each of the field's means.

iii). **traceroute** to *www.kca.ac.ke*, and identify each hop by using **whois** command. Note that whois takes IP addresses as parameter.

Section Two - Demonstrate the use of Wireshark tool

i). What is Wireshark and what's its purpose

ii). Capture and view network traffic

iii). View the detailed contents of the following packets in hexadecimal.

- IP
- TCP
- ARP

iv). Follow TCP stream