Unix for Telecommunications

Portfolio Task – P-Lab-08-tcpdump
Distinction Level Task

I. Introduction

In this lab you will use the program **tcpdump** to perform some 'detective' work on packets captured in the situation shown below.

A Unix for Telecommunications student (Lawrence Slowman) is sitting at the client machine. He connects to the server using a number of different services and performed a number of different tasks. Using the packet trace file captured on the 'sniffing' machine and the program **tcpdump** – it is your job to discover as much as possible about what Lawrence did during this session.

II. Purpose

To gain and/or enhance the following practical skills:

- Learn how to use **tcpdump** for traffic analysis
- Explore and use appropriate **tcpdump** options
- Understand the value and implications of **tcpdump**

III. Preparation

You should not attempt this task until you complete the **Credit** level task **P-Lab-04-tcpdump-C**.

IV. Methodology

After analysing Lawrence's activities and graphing the network traffic patterns generated over time for each of his online activities, you are now required to discuss its nature.

A. Discuss the nature of the graphs

For each of your four graphs (online activity session)

1) What do the graphs say about the nature of the traffic generated?
2) If there is more than one unique flow, provide insight into what is happening?
3) Is the traffic bursty/smooth? What does this mean in terms of impact on a typical home gateway?

V. Assessment

The due date for completion of practical work is **11:00pm**, exactly **six** days after your scheduled class.

Note: *The nominated submission day/time holds regardless of whether that day is a non-teaching day or public holiday*

To complete this lab you need to submit (to Doubtfire) a simple (unformatted) PDF document containing brief 1-2 sentence answers to the questions from Section IV-A.

Note: *A PDF upload is required as Doubtfire cannot currently accept uploads of image files*

A. Completion of task in Doubtfire

You will need to upload your PDF file containing your question responses to your Doubtfire portfolio before the due date

B. Tutor Discussion

In order for the submission to be marked as complete, you must discuss your work with the tutor