Unix for Telecommunications

Portfolio Task – P-Lab-08-tcpdump
Credit 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 **Pass** level task **P-Lab-04-tcpdump-P**.

IV. Methodology

After analysing Lawrence's activities in task **P-Lab-04-tcpdump-P**, you are now required to graph the network traffic pattern generated over time.

A. Generating Graphical Output

1) Explore the functionality of the commands **cut**, **tr** and **grep**
2) Use the above commands (and possibly others) in combination with **tcpdump**, pipes and redirection to produce a text file consisting of three columns, the first showing flow ID (IP addresses and port numbers), the second showing time in seconds+milliseconds and the third showing packet size for each packet sent from the server to Lawrence
3) Open this document in Excel or OpenOffice (or other graphing software), split the data into multiple groups, one for set of flows mapping to the four protocols used by Lawrence
   Hint: *Put one set of flow data to each worksheet*
4) Generate a new column containing cumultative bytes transferred against each time stamp
5) Plot graphs of *time (x-axis) versus cummulative bytes (y-axis) transferred* for each flow ID on each group of flows
   Hint: *You should have four graphs, one for each protocol used by Lawrence*
   Hint: *Each graph may have more than one unique flow*
   Hint: *Each flow within a graph should be plotted with a different colour – colour defines flow tuple*

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 the graph generated in 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 graph 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