Unix for Telecommunications

Portfolio Task – P-Lab-08-tcpdump

Pass 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

Download a copy of the packet trace file for examination from Doubtfire and place it on your rule host for examination prior to the lab.

Also you can read the **tcpdump** documentation at http://www.tcpdump.org

IV. Methodology

A. *tcpdump Introduction*

1) **tcpdump** has already been installed on your rule host, how would you go about installing **tcpdump** under FreeBSD?
2) After reading the **tcpdump** documentation, in what way is the name **tcpdump** misleading?

B. *Exploring the packet trace file*

1) Don't forget to uncompress the packet trace file you have downloaded (*Hint: man gzip*)
2) You can examine the trace file as a regular user but live capture requires **root** privileges, why?
3) What do each of the fields before the '`:`' in the output of **tcpdump** mean?
4) What are the IP addresses of the two hosts in the traffic trace? What are the hostnames assigned to these hosts?
5) How would you tell **tcpdump** to give you:
   a) Only the web traffic from the trace file
   b) Packet information in HEX format
   c) Packet information in ASCII format
   d) Full versus summarised packet information
6) How are these options useful in exploring traces using **tcpdump**?
7) What is the purpose of **tcpdump**'s `-n` option? When is it useful?

C. What did Lawrence do?

With your basic **tcpdump** skills, answer the following questions about the packet trace file:

1) Over what time frame was the trace file captured? (duration of session in *seconds*)
2) What four protocols did Lawrence use and in what order?
3) What web site did Lawrence visit that was hosted on `136.186.229.138`?
4) What happened the first time Lawrence tried to log in using **ftp**?
5) What file did Lawrence retrieve using **ftp**?
6) What commands were issued by Lawrence across the **ssh** session?
7) What was the contents of the email sent to Lawrence? Who sent it and when?
8) What is Lawrence's password?

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 a brief answer to all the questions in Section IV-C.

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

A. Completion of task in Doubtfire

You will need to upload your PDF file containing the answers 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