Computer networks - Administration 1DV202 – Lab 3
Data and packet analysis

Marcus Wilhelmsson
marcus.wilhelmsson@lnu.se

May 2, 2013

Instructions

Organisation and implementation

The lab consists of a number of steps that should be fulfilled and questions that should be answered. The lab is to be done individually.

Preparations

Before the lab is implemented, it must be read through and relevant preparations made. This may include, but is not limited to, the following:

- An understanding of the techniques used during the laboratory
- The look-up of terms
- Planning the implementation

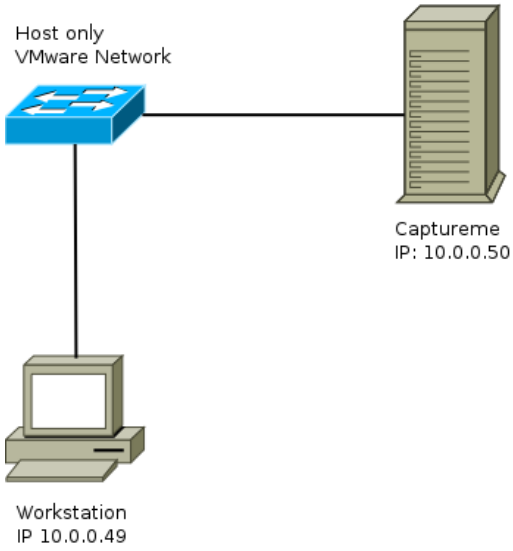
Presentation

Presentation of the lab will be in the form of a written report. The report shall consist of a cover page, table of contents, ideas and paths to the matters covered in the lab. Where it is possible to reason about a problem or come up with different solutions, it is especially important that these interpretations are included in the report and how you have motivated them. The text should be readable and cohesive text that can be read without having access to this laboratory-PM, a bulleted list or the like with short answer is not permitted.

Contents

1 Introduction

The aim of this lab is to get an understanding of packet capturing, how it can be utilized to monitor network traffic and conduct an analysis of the captured network traffic.



1.1 The virtual lab network

The network will be set up using VMware or VirtualBox. The Linux server (called Captureme) is provided on the course page as OVF file. It can be imported in VMware and VirtualBox. Make sure you set the machine to the correct virtual network. If you, for some reason, need to log in to the Linux machines the credentials are *user* and *password*. You can then use sudo to gain root privileges. The workstatin machine isn't downloadable, you'll have to install it yourself. You can download a trial version of Windows from Microsoft, which version of Windows you choose does not matter. If you're more comfortable using a Linux workstation, that will be fine too, since Wireshark runs in both Windows and Linux (among other OSes). Before you continue, make sure you have Wireshark installed and can ping Captureme from your workstation client.

2 Data collection

In this step you'll use Wireshark to collect data from the network. Each student collects his or her own data set on the computer following the instructions bellow.

2.1 What data to collect

You are supposed to collect three types of data:

- background traffic from the network
- application traffic generated on behalf of you
- supporting traffic generated indirectly by you in order for the host to perform the application task you order

Make sure to save the data once it's collected.

2.2 Background data

Most local area networks have some form of background traffic. In order to catch it, just run Wireshark on a idle line (don't generate any network traffic). Collect data for a couple of minutes and then save it to a file.

2.3 Application and supporting traffic

Clear the ARP cache on your capturing computer (use the command arp). Make sure that the cache of the web browser on the computers is empty and, while using Wireshark, connect to the following pages:

- http://10.0.0.50/test1.html
- http://10.0.0.50/test2.html

If successful, the pages should have a heading with the text "TEST 1" and "TEST 2" respectively. When done with the browsing, make a telnet connection to Captureme, take a look at the contents of your home folder and end the session by logging out. Make sure to capture all the data in the exchange.

3 Data analysis

Use the files from the previous step to answer the following questions:

- What protocols are present in the network without the active participation of the user, what is the purpose of those protocols?
- How many HTTP commands are sent during the browsing of the two pages, what are the purpose of those commands? Are there any difference in the number of commands used to display the two pages?
- Apart from the "background noise" found in the background data, are there any protocols that are used to support HTTP? What are the purpose of those protocols?
- What information can be gathered from the telnet session? Are there any supporting protocols and if so, what are their purpose?
- What else of interest can be gathered from the captured traffic?

4 Report

Write a report containing the following:

1. A brief Introduction to what you have done (90-110 words).
2. A description of the Method used when the traffic data was analyzed (90- 110 words).
3. A Discussion summing up the thoughts from the analysis that also makes sure to answer all the questions posted in the third step (180-220 words).

The report is an individual effort and each student writes and sends in his or her own. The report will be grades as "Pass" or "Fail" and a "Pass" is required in order to complete the course. Team work is considered cheating and will be reported as such if discovered. References should be written in the IEEE style. The report should be sent as a PDF to *marcus.wilhelmsson@lnu.se* no later than May 13 2013. The lab will be discussed and presented during the seminar on the 17th of May.