Wireshark Introduction

1 Overview

This exercise introduces the the Wireshark network traffic analysis tool. The student will use Wireshark to view network traffic captured in a "PCAP" file and locate a specific packet. PCAP files contain copies of network traffic stored in a format that can be processed by various network analysis tools such as Wireshark and *tcpdump*. PCAP is short for "packet capture".

1.1 Background

This exercise assumes you have received instruction TCP/IP networking. In this lab you will be asked to analyze packets from a Telnet session. Telnet is a communications protocol that allows a user to issue shell commands to a remote host. Telnet network traffic is not encrypted, which simplifies traffic analysis. Refer to the *telnetlab* for further background.

This lab exercise only touches on some of the most basic features of Wireshark. Details on using the tool can be found at `https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html`

2 Lab Environment

This lab runs in the Labtainer framework, available at `http://nps.edu/web/c3o/labtainers`. That site includes links to a pre-built virtual machine that has Labtainers installed, however Labtainers can be run on any Linux host that supports Docker containers.

From your labtainer-student directory start the lab using:

```
labtainer wireshark
```

A link to this lab manual will be displayed.

3 Tasks

3.1 Explore

Use the `ls -l` command to view the content of the directory in the terminal that opened when you started the lab. That `telnet.pcap` file contains the network traffic you will analyze. Use

```
file telnet.pcap
```

to view information about the file.

3.2 Run wireshark to perform PCAP Analysis

Start Wireshark using the `wireshark` command. Then use `File->Open` to open the telnet.pcap file. **NOTE:** If you encounter a black or corrupt window while using Wireshark, try to resize the window a bit. if the window will not resize, try stopping the applicaiton and starting it again.

3.3 Find a specific packet

Locate the single packet which contains the password provided when the user attempted to use Telnet to login as the ”john” user.

Hint: If you type `telnet.data` into the field that says “Add a display filter” (see Figure 1), the tool will display only Telnet data packets. Press `return` to apply the filter.

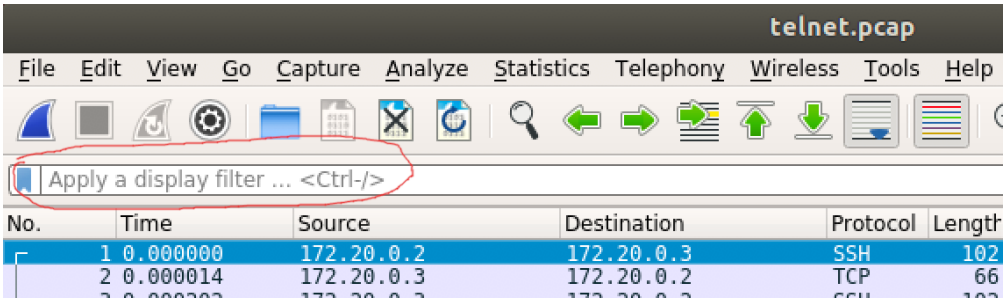

Figure 1: Display filter

Once you locate the single packet containing the invalid password, use `File=>Export specified packets` to save the single packet that you located. Save the single packet as *invalidpassword.pcap*. Be sure to select the `Selected packets only` radio button in the Export dialog and be sure to get the file name exactly right.

After you save the packet, you might then use `File=>Open` to open your new pcap file to confirm it contains the correct packet.

3.4 Explore some more

Look through other packets and experiment with filters. Try selecting one of the TELNET packets and use the `Analyze=>Follow=>TCP stream` function to view the entire TELNET conversation.

After you complete this lab, consider performing the *packet-introspection* lab to delve deeper into traffic analysis with Wireshark.

4 Submission

After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:

```
stoplab
```

When you stop the lab, the system will display a path to the zipped lab results on your Linux system. Provide that file to your instructor, e.g., via the Sakai site or email using the VM’s browser.

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under sponsorship from the National Science Foundation.