PCAP ANALYSIS LAB

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893.

Overview

This lab introduces the analysis of PCAP files using the Tshark tool. You will analyze an existing PCAP file, looking for a specific invalid login attempt. PCAP stands for "packet capture", and is a standard file format for storing traffic recorded from a network.

Performing the lab
The lab is started from the labtainer working directory on your Linux host e.g., a Linux VM. From there, issue the command:

```
labtainer pcapanalysis
```

The resulting virtual terminal is connected to a computer that contains the PCAP of interest.

Tasks

1. **run tshark to perform PCAP Analysis**

A) To see various options available for tshark, do:

```
man tshark
```

B) Sample Tshark command to display specific fields:

```
tshark -T fields -e frame.number -e frame.time -e
telnet.data -r telnet.pcap
```

NOTE: this command should be issued as one line

2. **display the single packet containing invalid "`admin`" password**

Locate the single frame containing the password provided when the user attempted to login as the "`admin`" user.

Use Tshark to display just this frame by using the `-Y frame.number==N` option.
Note, `N` is the frame number.

Stop the labtainer

When the lab is completed, or you would like to stop working for a while, run

```
stoplab
```

from the host labtainer working directory. You can always restart the labtainer to continue your work. When the labtainer is stopped a zip file is created and copied to a location displayed by the stoplab command. When the lab is completed, send that zip to the instructor.