



CSE331: Computer Security Fundamentals

Assignment 5: Network Traffic Analysis

In this assignment, you will use the Labtainers platform. Labtainers provides a fully provisioned execution environment for performing cybersecurity laboratory exercises.

Task 0: Getting started

To get started, **read the student guide**. To use Labtainers you can either download the VM image or use the container available on the website.

Task 1: PCAP Analysis

Task 2: Packet Capturing

Task 3: PCAP Programming

Task 4: NetFlow

What to submit

Submit a tarball to Blackboard, using your student ID number as its name (e.g. “123456789.tar.gz”). The tarball should contain:

- A writeup, describing how you accomplished each task in PDF format titled “**report.pdf**”.
- The **zip file** produced by each task.

Lateness

Assigned work is due on 11:59PM on the dates listed in the class calendar. We strongly recommend that you get started early. Late submissions will be penalized by 10% of the maximum attainable score, plus an additional 10% every 4 hours until received. The instructors may grant individual extensions, but only under extraordinary circumstances.

Collaboration

Acts of cheating, plagiarism, and unacceptable collaboration will be reported to the Academic Judiciary. Cheating is when you copy, with or without modification, someone else's work that is not meant to be publicly accessible. Plagiarism is the practice of taking someone else's work or ideas and passing them off as one's own without providing attribution. Unacceptable collaboration is the knowing exposure of your own solutions, or the use of someone else's answers or solutions.

At the same time, we encourage students to help each other learn the course material. As in most courses, there is a boundary separating these two situations. You may give or receive help on any of the concepts covered in lecture. You are allowed to consult with other students about the conceptualization of a project, or the general approach for solving problems. However, all work, whether in scrap or final form, must be done by you.

If you have any questions as to what constitutes unacceptable collaboration or exploitation of prior work, please talk to an instructor right away. You are expected to exercise reasonable precautions to protect your own work, including not posting solutions publicly.