Final Project Report/Data Set Submission and Documentation

Read all of the documents in the "Course Structure and Requirements" module which was posted at the start of the course. Ensure that all of the requirements and specifications are satisfied.

You are required to submit a detailed report outlining your HoneyNet design, your deployment procedure and the final results of the Honeynet exercise. You must also include a disk(s) that contains all report, the IDS/tcpdump/firewall logs, packet captures and all relevant logfiles.

Also provide a detailed manifest document that lists the complete file structure and the files submitted on the disk(s).

The following is the required directory format for submitting the documents and the data sets:

- Create a separate directory for each machine (name) on the disk. In that directory create subdirectories for:
  - logfiles
  - tcpdump packet captures
  - IDS logs and alerts captures

- Note that submitting tens of gigabytes of packet captures will not get you more marks, in fact it may become a liability. For very large packet captures what you **must** do is cull the data set so you have data for a period of time before, during, and after a compromise or incident. That way the size of the packet captures will be kept to a reasonable and manageable size.

- Clearly outline (in your report) the main events (time and capture references) in your data sets.

- For each machine that was compromised, create a separate directory and label it "**malicious files**". This directory will contain all of the files and data that the attacker(s) uploaded to your machine.

- You **must** submit your data set in the form of zipped tar files.

- Read the project report requirements provided at the start of the course again and ensure that your report conforms to the specifications therein.