Final Project Submission and Documentation

You are required to submit detailed documentation outlining your HoneyNet design, your testing procedure and results, and all your reconnaissance and attack activities. You must also include a CD that contains all the documentation, exploit sources, and your IDS/tcpdump/firewall logs.

The following is a suggested (minimum) format that may be used to prepare your final submission:

- An **introductory** section that introduces the reader to the purpose of the report and the objective behind the exercises presented within. Within this section you must also provide a summary of your level of success in the war games.

- A section detailing the **design** and **testing** of your Honey Net, the exploits you selected and why; as well as a detailed description of how you tested your own exploits. Provide supporting data in the way of all the exploit code and test results.

- A section detailing the **reconnaissance** and all the **attacking** activities that your team carried out during the war games. Also provide evidence of your successes.

- Provide all the **tools** you used on disk. These include all the tools that were used in the defensive and attacking activities. For the more common defensive tools such as Snort, nmap, etc, you may simply provide a link to where the tools may be obtained. However, ALL the exploit tools must be provided on disk.

- You **must** provide detailed data from IDS logs, firewall logs, system log files on your CD in a separate directory. Provide this data in the form of zipped tar files.

- Close out your report with all the lessons learned from this "war games" exercise. Comment on how your attitudes/thinking has changed (or not) as a result of this project. What skills have you acquired? How would you use them? Provide recommendations for both defense and attacks for typical networks.

- Provide an appendix that lists all your references, etc. Also provide a directory listing of your CD.