Comp 8006 Computer Systems Technology March 2010.

Network Administration and Security Level 2

Final Practical Project

Due: April 15 - 1330 hrs. Late submissions will **NOT** be accepted. This is an individual assignment.

Objective:

- To apply the principles of intrusion detection and packet analysis in a practical application.
- To perform a security audit on a data set consisting of captured network traffic.

Your Mission:

This project consists of analyzing network traffic captured over several days, analyzing the raw data and performing a security audit on the complete data set.

The objective of this report is to analyze the raw data and present a report that will allow the administrator of the network on which the traffic was captured to get an accurate idea of benign as well as anomalous and dangerous network activity in and out of the network.

The data will be provided to you in three directories:

- Network 1
- Network 2
- Network 3

Each directory contains snort as well as other logfiles (for each network) captured by a sensor positioned at the perimeter of the network or in some cases on the key server itself.

You are required to provide a summary of all the data in spreadsheet form together with some basic statistics. Be particularly vigilant for signs of compromised machines.

Your report will analyze and present the results as the following general areas of interest:

- A summary of detects prioritized by number of occurrences for each of the three networks.
- Malicious traffic, reconnaissance traffic and benign traffic.
- The top sources of traffic to and from each network.
- A list of source addresses together with their registration information. These are selected on the basis of posing a high risk to the security of the network.

Constraints

- Automate your analysis process as much as possible (Snort, SnortSnarf, Excel, Databases, etc).
- You may have to develop some scripts to analyze specific signatures in the large amount of data. Linux tools such as grep, sort, sort and awk may be useful here.
- You may also write analysis programs using C/C++, Perl, or MATLAB, etc.
- It is very important to note and understand that the data produced by your analysis tools is only the first step. The substance of the report will be to use this data to support your analysis and audit of the network. In other words, just providing the data from the tools as the substance of your report is **NOT** acceptable.
- Your practical report submission must be of **professional quality** and it must demonstrate a solid understanding of the concepts presented in lectures. Your report must follow the standard technical report format.
- The basic components of this format include the following sections:

- Summary
- Introduction.
- Body of the report (Analysis, descriptions, etc)
- Conclusions.

- Use tables and graphs to present and explain your results in the report.

To be Submitted:

- A soft copy of your report (PDF, ODT, or Word format) on disk.
- A brief description of all the tools you used as well as copies of any programs or scripts used for the analysis.
- You will be required to submit a signed document that the work you have presented is your own original work and analysis.