CSN09105 Assessment Specification

Details

Module name:	SFC
Module number:	CSN09105
Session:	Semester 1, 2013
Weighting:	50%
Submission:	Week 12

Coursework Assignment

Title: Intrusion Detection System for Malicious Activities

Outline Requirements

You have been assigned the tasking of creating a new IDS for a company, and have been allocated the following tasks:

- Develop, implement and test a strategy to detect the networking scanning of their system. This scanning can be by local or remote intruders.
- Develop, implement and test a strategy to detect activities which involves the login of an administrator through remote access.
- Develop, implement and test a strategy of detecting the sending and receiving of email messages with the words which might relate to fraud.
- Develop, implement and test a strategy to detect a malicious Bot agent (to be given). There are also a number of associated files with the Bot, which you have been asked to analyse.

You should create a prototype of a system which outlines how the system could work. For this you should implement an agent-based system, either using: your own agent (using Winpcap and .NET or Java); a stand-alone version of Snort; or using a graphical management system which interfaces to Snort (a mixture of Snort, Winpcap and .NET). Overall the alerts should be useful, and, possibly, stored in a secure manner. The Bot and the associated files are available at:

http://buchananweb.co.uk/1.zip

Marking schedule

The coursework should be submitted via Turnitin (submit.ac.uk), in a PDF format, if possible. It will be marked as follows:

- **Requirements Analysis** [20%]. This should show the analysis related to the main requirements, and an outline of the Web system, with the main design features. This should also include an analysis of the Bot, and how it can be detected.

- **Outline implementation** [25%]. This should define an outline implementation of the system which demonstrates the key implementation elements of the proposed system.
- **Evaluation** [25%]. This should outline the results of any tests that you have made.
- **Conclusions** [15%]. This should reflect the methods you have used in the report, and to assess their strengths and weaknesses, and any observations that you have gained.
- **References/Presentation** [15%]. All references must be defined in an APA/Harvard format, and should be integrated in the report.

The report should use the APA/Harvard format for all of the references, and, if possible, should include EVERY reference to material sourced from other places. Also, the report should be up to 14 pages long (where appendices do not count in the page count number).