PRIFYSGOL ABERYSTWYTH - ABERYSTWYTH UNIVERSITY

DEGREE EXAMINATIONS 2011-2012 SEMESTER 1

FACULTY OF SCIENCE

Computer Science, CHM5410: Forensic Computing and Ethical Hacking

Time allowed: 2 hours

Calculators are not allowed in this examination.

Answer **TWO** *from* **THREE** *questions.*

All questions carry equal marks.

1. A "hack" can often involve multiple techniques in order to circumvent various layers of security therefore, audits should encompass all types of security.

   Citing examples that you have studied, discuss the range of issues that the auditing process needs to consider if it is to achieve a complete analysis of the organisation's security framework.

   Ensure that you address all the possible attack vectors that may be used to compromise a large system, not just the usual network perimeter test. I am looking for a description of a full-spectrum security audit, discussing at least five *distinct* issues.

   [50 marks]

2. In the 1980s, Clifford Stoll arguably became the first person to use forensic techniques to investigate computer misuse.

   Some of the techniques that Stoll used were very primitive by today's standards, for instance he attached printers to serial lines. Other techniques he used were quite sophisticated, for instance creating false accounts containing dummy data. Discuss the similarities between the techniques that Stoll used and the techniques that are currently used, and give an overview of how techniques have evolved and become more formalised.

   You should discuss at least five techniques in your answer.

   [50]

3. Imagine you are employed as an information security professional and are called to a crime scene in a company where there are a number of computers.

   There is a strong suspicion that a crime has been committed using the computers in the building. Describe the ways in which you should capture data, and the order in which you should examine and catalogue machines in the affected area, including when and how they should be turned off and removed. Consider at least seven issues as part of your answer.

   [50]