OLLSCOIL NA hÉIREANN
The National University of Ireland

NATIONAL UNIVERSITY OF IRELAND, GALWAY

SEMESTER 1 EXAMINATIONS 2003

THIRD YEAR EXAMINATION IN INFORMATION TECHNOLOGY
AND BSC EXAMINATION: 3IF1 AND 4BS2

CT412

COMPUTER SECURITY

Prof. P. Nixon
Prof. G. Lyons
Dr. C. Mulvihill

Candidates are required to answer any **THREE** questions
Answer all components of each question
All questions carry equal marks
Time allowed: **TWO hours**

1.
(a) Distinguish between the terms 'cryptography' and 'steganography' (7 marks)
(b) Outline how an image found on the Internet could be used to hide information, explaining the terms 'colour table' and 'LSB' in the course of your answer (12 marks)
(c) What transformations might an administrator apply to (i) a text file and (ii) an image file in order to destroy a message hidden by steganographic techniques? (6 marks)

2.
(a) Briefly explain how a typical social engineering attack works (11marks)
(b) In the context of Social Engineering, what do you understand by the term 'information chain'? (6 marks)
(c) Give two responses that you regard as effective in the presence of a social engineering attack (8 marks)

3.
(a) By considering a SYN flood, or otherwise, explain how a typical Denial of Service attack works (10 marks)
(b) Explain what is meant by the term 'kernel rootkit'(5 marks)
(c) Outline how a man in the middle attack can be used to defeat an SSL connection, explaining the term 'digital certificate' in the course of your answer (10 marks)

4.
(a) Explain the terms 'access control' and 'authentication' (8 marks)
(b) Give a brief account of four typical network security policies, explaining the terms 'due care' and 'due diligence' in the course of your answer (8 marks)
(c) Give an account of security issues involved in data backup, explaining the term 'offsite storage' in the course of your answer (9 marks)

5.
(a) In the context of computer forensics, explain why data may be found in each of the following: (i) unallocated disk space, (ii) slack space and (iii) deleted files (9 marks)
(b) Outline three components of a typical computer forensics tool (9 marks)
(c) Explain how a typical anti-forensics tool works (7 marks)