NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

FACULTY OF APPLIED SCIENCE

COMPUTER SCIENCE DEPARTMENT

AUGUST SUPPLEMENTARY EXAMINATIONS 2004

SUBJECT: COMPUTER SECURITY
CODE: SCS 4107

Instructions to candidate:

1. Answer any four questions. Paper contains five questions.

3 HOURS

QUESTION ONE

a) By first defining each (in terms of computer security), distinguish between the following:-

   i. threat
   ii. risk [5]

b) In security vernacular, DAC is generally referred to as *discretionary access control* (DAC), and the degree to which a DAC system can control file and directory access is referred to in security vernacular as *granularity*. Explain both DAC and *granularity*, then give your view of Microsoft Windows NT DAC, i.e. NTFS security model, making reference to particular version e.g. NT 3.51 [10]

c) Explain what is Type enforcement? What is Information bucket? Differentiate between the two, if there is a difference? [10]

QUESTION TWO

a) Define a Trojan horse! Define a worm! Contrast the two [5]

b) "To perform a useful Self Hack Audit, the different types of hackers must be identified and understood." By first giving the objectives of the Self Hack Audit, give an overview of the methodology of the Self Hack Audit. [10]

c) "Why should I bother with doing risk assessment?!" "I already know what the risks are!" "I've got enough to worry about already!" "It hasn't happened yet …" Most resistance to risk assessment boils down to one of three conditions: Ignorance, Arrogance, and Fear. Discuss?? [10]

QUESTION THREE

a) Explain what is packet sniffing? [5]

b) With the aid of diagrams where appropriate, first explain and then differentiate between symmetric and a symmetric cryptography? [10]

c) There are two types of DOS attacks: flaw-based and flooding. By first defining what DOS is, explain these two types of DOS attacks and also explain how you would counter each of these attacks? [10]

QUESTION FOUR

a) In a LAN Setup , what are the role and functions of integrity controls? [5]

b) Define Risk Management? As an Information security officer of an Industrial firm, what are the a few key questions that would be at the core of the Risk Management process that you would carry out. [10]

c) For Internet security, the most simple authentication procedures use the IP address as an index. The IP address is the most universal identification index on the Internet. This address can be either a static or dynamic address. Explain in your words what is a Static and Dynamic address? [10]

QUESTION FIVE

a) Define hash functions and state what three properties that is possess.? [5]

b) Compare and Contrast Packet filtering and proxy server firewalls. [10]

c) There are two fundamentally different metric schemes applied to the measurement of risk elements, *qualitative* and *quantitative*. What are the Pros and Cons of Qualitative Approach? [10]

END OF QUESTION PAPER

GOOD LUCK!