NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY
FACULTY OF APPLIED SCIENCE
COMPUTER SCIENCE DEPARTMENT
DECEMBER 2002 EXAMINATIONS

SUBJECT: COMPUTER SECURITY
CODE: SCS 4207

Instructions to candidate:

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

3 HOURS

QUESTION ONE

a) Define the following

i. Patch

ii. Fix

iii. MIME

iv. Bastion Host

v. Network firewall

[5]

b) Robert Morris Senior was responsible for unix security, whilst Robert Morris Junior was responsible for the Internet worm. The father did more damage to Internet security than the son. Discuss. [8]

c) By first defining the following: (i) Technical safeguards (ii) Operational safeguards (iii) Virus safeguards, distinguish the differences between them? [7]

QUESTION TWO

a) A hospital de-identifies patient record by removing names and addresses, leaving only the patient's postcode and date of birth as an identifier. These records are then sold to researchers and drug companies. What risks is the hospital running, give reasons? [5]

b) By first defining each, distinguish between firewalls, screening router and proxy server [7]

c) When implementing security measures for a company certain factors come into the fray, e.g. the relative sensitivity of the company's information resources, company philosophy, business imperative for using various technologies etc. But when implementing the company's Internet, intranet, and WWW security strategies, a number of objectives should be addressed, describe or explain five of these objectives. [8]

QUESTION THREE

a) What is SSL and how does it differ from TSL. Which would you choose over the other in a given situation, explain the reasons behind your choice. [5]

b) What vulnerabilities where poised by the Server Message Block Protocol (SMB) on systems running on the Microsoft Platform? What potential damage could a hacker do on systems running this protocol, before a Microsoft released a fix for it? [8]

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? [7]

QUESTION FOUR

a) Explain what is:-

i. Social engineering?

ii. Firewall environment?

[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. [6]

c) Controls for providing computer security can be classified as either preventive or detective. Three other types of controls supplement preventive and detective controls. They are usually described as deterrent, corrective, and recovery. Explain in detail what each of these five controls is? [9]

QUESTION FIVE

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

i. threat

ii. risk

[5]

b) As a consultant employee of Mbokodo Computer Security Consultancy, you have been asked by the Manager Director of Siswabile Finance Co. to give a talk on ***"Good Security Practices for Computer Users "*** What are the eight salient points (with brief decription) that you will put across [8]

c) Are firewalls foolproof? Discuss. [7]

QUESTION SIX

a) What are the common types of threats to information security? [5]

b) 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? [7]

c) Most forms of protection against (and prevention of) trojans are based on a technique sometimes referred to as *object reconciliation*. Explain how the technique of *object reconciliation* works giving an appropiate an example in your explanation. [8]

END OF QUESTION PAPER

GOOD LUCK!