NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY
FACULTY OF APPLIED SCIENCE
COMPUTER SCIENCE DEPARTMENT
Examination January 2013

SUBJECT: Information Systems and Auditing
CODE: SCIS 5204

Instructions to candidate:

1. Answer any four questions. Paper contains five questions.
2. Each question is worth 25 MARKS   **DURATION 3HRS**

QUESTION ONE

a) State the physical security threats and their mitigation methods.   [5 marks]
b) Explain the concept of physical security.   [5 marks]
c) Discuss the critical issues which need to be included in an organisation's computer security policy document.   .   [15 marks]

QUESTION TWO

a) Explain why a packet-filtering router should reassemble a packet that has been fragmented   in the network and check its authentication header, instead of forwarding the fragments to the destination.   [10 marks]

b) Identify the fields in the Ipv4 header that cannot be covered by the authentication header, and what can you do to protect them.   [10 marks]

c) Differentiate between a buffer overflow attack and a parameter tempering attack.
          [5 marks]

QUESTION THREE

a) Denial of Service is an attack on a computer system that denies authorised users access to the system. How is this is different from a distributed denial of service attack and what are the mitigation methodologies.   [5 marks]

b) Differentiate between session hijacking at the network layer and at the application layer.
          [5 marks]
c) Outline the impact that session hijacking may have on an organisation.   [5 marks]
d) Discuss the measures which may be implemented by network administrators to protect their networks from session hijacking.   [10 marks]

QUESTION FOUR

a) There are five steps taken by malicious users to breach the computer security of an organisation. Discuss.   [10 marks]

b) You have been tasked with writing a technical report to your organisation's CEO regarding which encryption system is suitable for securing information during data transfer, between a public key cryptographic system and a private key cryptographic system. Outline the major points you would include in the report.   [10 marks]

c)The simplest encryption techniques involve substituting the **plaintext alphabe**t (codeword) with a new alphabet known as the **ciphertext alphabet** . Given the following plaintext and ciphertext   determine the key for the ciphertext.

        plaintext: *computersecurity*
        ciphertext: *zljmrqbopbzrofqv*   [5 marks]
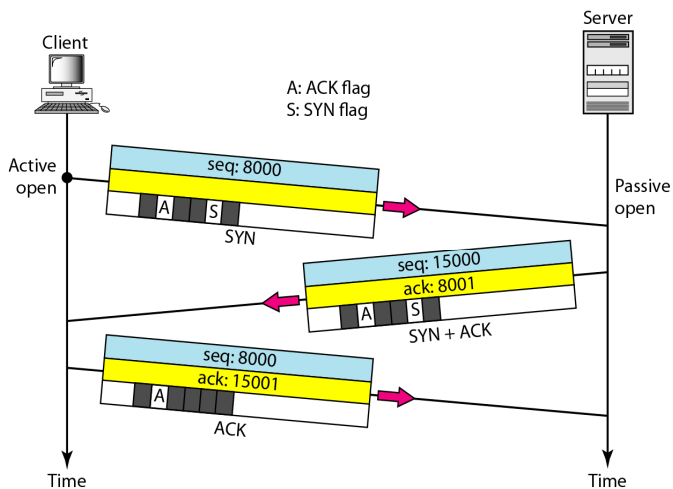
QUESTION FIVE

Figure 1

a) Figure 1 is an illustration of a process known as the Three – Way Handshake. Using the diagram explain how this process occurs.   [10 marks]

b) Discuss how maliciuos users are able to take advantage of the functionality of the Three – Way Handshake to breach the information security of an organisation.   [10 marks]

c) ***"Web applications are vulnerable to injection flaws"*** qualify this statement.

[5 marks]

End of Paper