JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN COMPUTER SECURITY AND FORENSIC

3rd YEAR 1st SEMESTER 2014/2015 ACADEMIC YEAR

SPECIAL RESIST

MAIN CAMPUS

COURSE CODE: IIT 3125

COURSE TITLE: EMERGING THREATS, ATTACKS AND DEFENSES

EXAM VENUE: LAB 1 **STREAM:**

DATE: 05/05/16 **EXAM SESSION: 9.00 – 11.00 AM**

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

Question 1

a) Explain the meaning of computer systems security (2 marks)

b) A strong security protocol addresses all major areas IT security. Discuss any four of these areas giving priority to the information system security triad (4 marks)

c) Computer security can also be analyzed by function. It can be broken into five distinct functional areas. Exhaustively discuss these areas. (5 marks)

d) Discuss the following information systems security threats and the methods that can be used to counter them: (6 marks)
   i. Phishing
   ii. Drive-by-pharming

e) Explain the meaning of identification and authentication and describe how this should be done in a secure information system (5 marks)

f) Passwords are your main and most common defense against intruders. To protect your system and your data, you must select good passwords, and you must protect them carefully. Explain how you would do this. (6 marks)

g) Differentiate between encryption and hashing as used in IT security. (2 marks)

Question 2

a) After the risk management process, there are mainly four ways an organization can choose to respond to the risk management report. Discuss these ways. (8 marks)

b) Explain any three application defenses you would implement in your organization in order to enhance security of you system. (6 marks)

c) Discuss economic factors you would consider while implementing information system security in your organization. (6 marks)

Question 3

a) With the aid of a well labeled diagram, exhaustively discuss the concept of defense-in-depth in information system security. (12 marks)
b) The threats that we see today typically adopt a six-stage lifecycle which make them more difficult to manage than the threats of the previous generations. Discuss these stages. (8 marks)

Question 4

a) Computer security is also frequently defined in terms of several interdependent domains that roughly map to specific departments and job titles. Discuss any five of these security domains. (5 marks)

b) Explain the meaning of the following terminologies with regard to IT security: threat, vulnerability, risk, attack and residual risk. (5 marks)

c) Selecting proper security controls and implementing those will initially help an organization to bring down risk to acceptable levels. Control selection should follow and should be based on the risk assessment. Controls can vary in nature but are fundamentally classified into three. Exhaustively discuss them, giving appropriate examples. (10 marks)

Question 5

a) Explain the meaning of risk management and discuss exhaustively the risk management process in an organization with regard to information systems. (10 marks)

b) Many organizations currently use firewalls to enhance security of their systems.

   i. Explain the term firewall. (2 marks)

   ii. Discuss any two types of firewalls and their functions (8 marks)