JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BSC IN COMPUTER SECURITY AND FORENSIC

1ST YEAR 2ND SEMESTER 2016/ 2017 ACADEMIC YEAR

COURSE CODE: **IIT 3125**

COURSE TITLE: **EMERGING THREATS, ATTACKS AND DEFENSES**

EXAM VENUE: **MAIN CAMPUS**

DATE: **STREAM: BSC FORENSICS**

TIME: 2 HOURS **EXAM SESSION:**

INSTRUCTIONS:

1. **Answer question 1 in Section A (Compulsory) and any other two questions in Section B**
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 ONE (30 MARKS)

a) Explain the meaning of the following terminologies (4 marks)

   i. Cybercrime

   ii. Cyberspace

b) Explain the difference between intrusion detection system and intrusion prevention system and their role in computer security. (4 marks)

c) Discuss four biometric mechanisms that can be used to identify users of a system.

(4 marks)

d) Explain the meaning and importance of authentication, authorization and accountability with respect to information system security. (6 marks)

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

f) Explain why system updates are important in computer security. (1 mark)

g) Discuss the following information systems security threats and the methods that can be used to counter them: (6 marks)
   i. SPIT
   ii. Ransom ware

QUESTION TWO (20 MARKS)

a) With the aid of a well labeled diagram, exhaustively discuss the concept of defense-in-depth in information system security. (8 marks)

b) Explain what the following threats are and how they can be controlled in an organization. (6 marks)
   i. Vishing
   ii. Drive-by-pharming
   iii. IP spoofing

c) 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. (6 marks)

QUESTION THREE (20 MARKS)

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. Identify any two computer threats that a firewall can prevent (2 marks)

iii. Identify any two logical threats that a firewall cannot prevent (2 marks)

iv. Discuss how a proxy server firewall works (4 marks)

QUESTION FOUR (20 MARKS)

a) Explain any three ways you can improve the internal utilization of bandwidth provided by an Internet Services Provider to your company. (6 marks)

b) Discuss any two economic factors you would consider while implementing information system security in your organization. (4 marks)

c) Identify and explain any five logical computer vulnerabilities in a typical corporate LAN environment. (10 marks)

QUESTION FIVE (20 MARKS)

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: crime ware, rootkit, Trojan horse, logic bomb and adware. (5 marks)

c) After the risk management process, there are mainly five ways an organization can choose to respond to the risk management report. Discuss these ways, explaining reasonable professional circumstances that can lead to each decision.(10 marks)