JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN SECURITY AND FORENICS

4TH YEAR 2ND SEMESTER 2014/2015 ACADEMIC YEAR

SPECIAL RESIT

MAIN CAMPUS

COURSE CODE: IIT 3413

COURSE TITLE: OPERATING SYSTEMS

EXAM VENUE: LAB 1 **STREAM: BSc SEC & FORE**

DATE : 04/05/ 2016 **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 ONE (30 MARKS)

a) Define the following terms
   a. Data integrity **(3 mark)**
   b. Data confidentiality **(3 mark)**
   c. Access control **(3 mark)**
   d. Authentication **(3 mark)**
   e. Operating system security **(3 marks)**

b) Identify and discuss any five operating system security threats. **(5 marks)**

c) Discuss the three computer security objectives **(3 marks)**

d) Briefly discuss *four* ways to authenticate a user's identity? **(4 marks)**

e) Discuss *three* broad mechanisms that malware can use to propagate? **(3 marks)**

QUESTION TWO (20 MARKS)

a) A secure operating system provides security mechanisms that ensure that the system's security goals are enforced despite the threats faced by the system. State and briefly explain three security goals that should be achieved by a secure operating system **(6 marks)**

b) Differentiate between Discretionary access control systems and Mandatory protection systems. **(6 marks)**

c) State and briefly explain any five vulnerabilities that can lead to the compromise of Windows operating system **(5 marks)**

d) The reference monitor concept defines the necessary and sufficient properties of any system that securely enforces a mandatory protection system. State and briefly explain any two guarantees that constitute a mandatory protection system **(3 marks)**

QUESTION THREE (20 MARKS)

a) Compare and contrast Windows protection system and UNIX protection system **(6 marks)**

b) Describe the different components of a mandatory protection system. **(9 marks)**

a) A reference monitor is a classical access enforcement mechanism that takes a request as input, and returns a binary response indicating whether the request is authorized by the reference monitor's access control policy. Explain the functions of the components of a reference monitor. **(3 marks)**

b) Distinguish between access control list and capability list **(2 marks)**

QUESTION FOUR (20 MARKS)

a) Explain the type of protection system that is implemented by UNIX operating system **(6 marks)**

b) Use appropriate example to demonstrate how UNIX mode bits are used to specify the access rights of identities to files. **(4 marks)**

c) State and briefly explain any five vulnerabilities that can lead to the compromise of the UNIX trusted computing base. **(10 marks)**

QUESTION FIVE (20 MARKS)

In order to handle information security incident effectively, it is important to identify information security incidents and establish best practices for handling these incidents. A critical step in effective incident response is establishing an Incident Response Team. The goal of the team is to quickly and appropriately handle an incident. Discuss five elements for successful incident handling and the individuals responsible for taking the action. **(20 marks)**