JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DIPLOMA IN LINUX ENGINEERING

2ND YEAR 1ST SEMESTER 2013/2014 ACADEMIC YEAR

CENTRE: KISUMU

COURSE CODE: ICT 2214

COURSE TITLE: FUNDAMENTAL OF IT SECURITY ENGINEERING

EXAM VENUE: AH **STREAM: Dip. Linux Engineering**

DATE: 5/12/2013 **EXAM SESSION: 9.00 – 10.30 AM**

TIME: 1 ½ HOURS

Instructions:

1. **Answer question 1 (Compulsory) and ANY other 2 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) Giving reasons, list any four security policies you would implement as a systems security manager. (4 marks)

b) What is a firewall? (2 marks)

c) Explain the two main types of firewalls: Packet Filters and Application Gateways . . (4 marks)

d) State any 3 Types of protections provided by firewalls (3 marks)

e) List any four importance of backups (4 marks)

f) Which three backup policies would you implement as a systems security manager. . (3 marks)

Question 2

a) Define each of the following terms with respect to information security. (6 marks)

   i. Cryptology
   ii. Encryption
   iii. Cipher text

b) Distinguish between Symmetric and Asymmetric cryptographic methods. (4 marks)

c) For each of the following cryptographic algorithms, classify as Symmetric or Asymmetric

   i. DES ii) RSA iii) ECC iv)RC4 (4 marks)

d) State any three advantages of using digital signatures (3 marks)

e) What are the key components of Public Key Infrastructure? (3 marks)

Question 3

a) Explain each of the following terms as far as security of information systems is concerned. (8 marks)

   i. Target System
   ii. Risk
   iii. Risk Management
   iv. Risk Appetite

b) Give at least one tangible and one non-tangible example of target systems. (2 marks)

c) Explain each of the following components of Control Systems. (3 marks)

i. Access and Authorization
ii. Logs and Trails
iii. Risk-based Audit

d) What sre the four main steps of risk assessment in security strategy flowchart. (4 marks)

e) List any 3 factors that may cause changes in risk. (3 marks)

Question 4

a) Stating core functions of each, Discuss the five functional layers of security Management. . . (10 marks)

b) State any four design goals of using the layered functional architecture in designing . security Management Systems. (4 marks)

b) Define clearly the six basic security services defined by the ISO. (6 marks)

Question 5 (20 Marks)

a) Differentiate between SSL and Kerberos Authentication. (4 marks)

b) State any four threats to network components with their possible consequences. . (6 marks)

c) State and explain the three main goals on network security. (6 marks)

d) What is eavesdropping? (1 mark)

e) Give any three implementations that would counter eavesdropping. (3 marks)