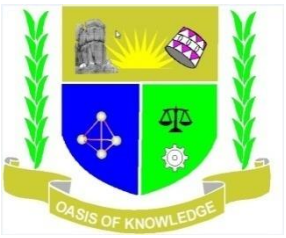

JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

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

4TH YEAR 1ST SEMESTER 2020/2021 ACADEMIC YEAR

RESIT/SPECIAL

COURSE CODE: IIT 3415

COURSE TITLE: NETWORK MANAGEMENT SECURITY

EXAM VENUE: **STREAM:**

DATE: 26/04/2018 **EXAM SESSION:**

TIME: 9:00 – 11:00

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 [30 marks]

a) Give the various motivations that would drive people to break into systems **(4 marks)**

b) Subnetting is the practice of dividing a network into two or more networks. Describe the uses of subnetting **(5 marks)**

c) Cryptography is one of the core concepts of security. What are its goals? **(4 marks)**

d) Intrusion detection and prevention systems add a line of defense behind firewalls and antivirus software. State its components **(4 marks)**

e) Elaborate the difference between a Threat and a Risk **(4 marks)**

f) Describe the requirements for securing systems **(4 marks)**

g) Information security is the protection of information and its critical elements. State the goals of Network security **(5 marks)**

Question 2 [20 marks]

a) Discus the phases of security policy life cycle **(8 marks)**

b) Rule base is a practical implementation of the organization's policy. Discuss the common guidelines that need to be reflected in the rule base **(12 marks)**

Question 3 [20 marks]

a) Cryptography is the process of converting readable text, programs and graphics into data that cannot be easily read or executed by unauthorized users. discuss the components of asymmetric cryptography **(10 marks)**

b) Routing is the process of transporting packets of information across a network form source to destination. Discuss the factors taken into consideration when determining which routing protocol is best **(10 marks)**

Question 4 [20 marks]

a) Whilst examining normal network traffic signatures as a security, there are some important TCP flags that one must be acquainted to. Discuss these TCP flags **(10 marks)**

b) Discuss the critical characteristics of information **(10 marks)**

Question 5 [20 marks].

a) Signature analysis is the practice of analyzing and understanding TCP/IP communications to determine whether they are legitimate or suspicions. Discuss the types of signature analysis carried out **(10 marks)**

b) Discuss the tunneling protocols that are employed by VPNs **(10 marks)**