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 1st SEMESTER 2019/2020 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1401

COURSE TITLE: IT SECURITY ARCHITECTURE AND DESIGN

EXAM VENUE: **STREAM:**

DATE: **EXAM SESSION:**

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.(30 marks)

a) The number one leading threat to Network security actually comes from its employees briefly explain at least four reason as to why an employee would decide to become malicious. **(4marks)**

b) Distinguish between Proxy server and Reverse proxy **(4marks)**

c) Explain two ways in which VLAN communication can take place **(4marks)**

d) Briefly explain three primary purposes of a Honeypot **(3marks)**

e) Why is it important to achieve buy-in from users, managers, and technical staff for the security policy? **(2marks)**

f) Distinguish between statefull and stateless packet filtering **(2marks)**

g) What do you understand by term convergence in relation to network design? **(2marks)**

h) What do you understand by NAT, what are the two important functions it provides on a network **(3marks)**

i) What is a demilitarized zone **(2marks)**

j) What is a Non-routable address? **(2marks)**

k) What are cookies, how do they pose a risk on a network **(2marks)**

QUESTION 2. (20marks)

a) Monitoring network traffic helps to identify and troubleshoot network problems explain two ways Monitoring traffic can be done **(4marks)**

b) Explain what you understand by these two secure network technologies **NAC** and **PAT** (**4marks)**

c) Briefly explain what you understand by a cookie and what risk they pose on a network **(2marks)**

d) Explain five Major Threats against Network Security **(10marks)**

QUESTION 3. (20marks)

a) State and briefly explain the functions of at least 5 Network Security Devices **(10 marks)**

b) State five reasons as to why you would want to subnet a network **(5marks)**

c) What benefits would an organization archive as a result of converging its network? **(5marks)**

QUESTION 4. (20marks)

a) Distinguish between Port forwarding, NAT, Route Add, and VLAN and explain their role in securing the Network architecture **(8marks)**

b) Securing a network begins with the design of the network and includes secure network technologies, explain at least three secure technologies available and how they are used to secure networks **(6marks)**

c) Briefly explain at least six functions a Network Intrusion Detection Systems can perform **(6marks)**

QUESTION 5. (20marks)

a) Assume you are an attacker state and explain five steps that you would use to conduct an attack on a network scenario. **(10 marks)**

b) State and explain the functions of at least 5 Network Security Devices. **(10marks)**