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 2020/2021 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3411

COURSE TITLE: IT SECURITY ARCHITECTURE AND DESIGN

EXAM VENUE: **STREAM:**

DATE: AUGUST 2016 **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 ONE [30 MARKS]

a) Information security is intended to protect information that has value to people and organizations This value comes from the characteristics of the information: state and explain **(3marks)**

b) One of the largest information security threats to a business actually comes from its employees briefly explain at least four reason as to why an employee would decide to become malicious. **(4marks)**

c) How can a network manager secure a wireless network? **(3marks)**

d) Distinguish between **Proxy server** and **Reverse proxy** **(2marks)**

e) Monitoring network traffic Helps to identify and troubleshoot network problems explain two ways Monitoring traffic can be done **(2marks)**

f) State two broad categories of network vulnerabilities **(2marks)**

g) Sate two characteristics that make Spyware very dangerous **(2marks)**

h) Cyber terrorist's motivation may be defined as ideology or attacking for the sake of their principles or beliefs briefly explain at least three Goals of a cyber attack **(3marks)**

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

j) Explain what you understand by the two these two secure network technologies **NAC** and **PAT** (**2marks)**

k) What way would you reduce the risk of attack in file transfer protocol **(1mark)**

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

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

QUESTION TWO [20 MARKS]

a) There is no simple solution to securing information This can be seen through the different types of attacks that organizations face today As well as the difficulties in defending against these attacks briefly explain seven ways as to why organization are experiencing Difficulties in Defending against Attacks on their system **(7marks)**

b) Briefly explain three scenarios where spoof attack would be used by an attacker **(3marks)**

c) State and explain the two common types of spyware **(2marks)**

d) Using a diagram explain how a proxy and reverse proxy server works **(4marks)**

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

QUESTION THREE [20 MARKS]

a) Explain and give example on what you understand by the following information security terminologies (7 marks)

I. Asset:

II. Threat:

III. Threat agent:

IV. Vulnerability:

V. Risk:

VI. Impact:

VII. Mitigation:

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

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

d) Explain two vulnerabilities associated with the File Transfer Protocol (FTP) **(2marks)**

e) How does a security plan differ from a security policy? **(2marks)**

f) Briefly explain two ways in which of privilege escalation can be performed **(2marks)**

QUESTION FOUR [20 MARKS]

a) Briefly explain the Major Threats against Network Security **(8marks)**

b) Image spam cannot be easily filtered based on the content of the message explain at least an approach that would be used to detect image spam **(2marks)**

c) Explain two ways in which VLAN communication can take place **(2marks)**

d) Briefly describe at least six different types of software-based attacks **(6marks)**

e) Explain two ways in which VLAN communication can take place **(2marks)**

QUESTION FIVE [20 MARKS]

a) Defenses against Attacks should be based on five fundamental security principles state and explain these principles **(10marks)**

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

c) Explain the following stateless packet filtering rules **(3marks)**

i. **Source address = any**

ii. **Destination address= internal IP address**

iii. **Port= 80**

d) Sate at least four desktop functions a HIPS would be monitoring **(4marks)**