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

1st YEAR 1st SEMESTER 2016/2017 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3113

COURSE TITLE: PC SECURITY & PRIVACY

EXAM VENUE: **STREAM:**

DATE: DECEMBER 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) State and briefly explain three objectives as to why you would provide security to your personal computer **(3marks)**

b) Briefly explain four critical functions audit logs play in the protection of a PC system **(4marks)**

c) What's the difference between "Sniper style" and "Brute force" In the denial of service attack? **(2marks)**

d) What is an Insider Threat, why is it considered the most dangerous within an enterprise setup? **(2marks)**

e) What do you understand by the term social engineering? **(2 mark)**

f) Distinguish between port scanning and vulnerability scanning **(4marks)**

g) Explain what you understand by privilege escalation attack **(2marks)**

h) Distinguish between a *threat* and a *vulnerability* **(2mark)**

i) What do you understand by the terms least privileged and defense in-depth? **(2marks)**

j) What's the difference between an intrusion detection and intrusion prevention system **(2marks)**

k) Briefly Explain five fundamental security principles that are usually put into consideration when crafting defenses for computer systems **(5marks)**

QUESTION TWO [20 MARKS]

a) Define the following terms to computer security **(6marks)**

   i. Confidentiality;
   ii. Integrity
   iii. Availability;
   iv. Authentication;
   v. Authorization;
   vi. Accountability

b) You are contracted as a consultant to offer advice on setting up a computer security Laboratory at JOUST. What are some of the administrative and physical control measures would you advice the University to put in place **(8marks)**

c) Using diagram describe how "man in the middle" and "replay attack" can be perpetuated **(6 Marks)**

QUESTION THREE [20 MARKS]

a) You are requested to conduct a computer security risk assessment of the SIIS laboratory. From this exercise you are required to give your assessment of the possible threats pairing them with their respective vulnerabilities, impacts and possible control measures. **(10marks)**

b) Describe at least five types of vulnerabilities that a threat can exploit within a computer. **(10marks)**

QUESTION FOUR [20 MARKS]

a. Sate and elaborate at least five typical Characteristics of poor password practice **(5marks)**

b. The challenge of keeping information systems secure has never been greater, not only because of the number of attacks but also because of the difficulties faced in defending against these attacks. Briefly explain at least 10 reasons despite crafting and implementing controls, it's becoming increasingly difficult to mitigate attacks on information systems **(10marks)**

c. When you are accessing an a computer system what other aspects apart from C.I.A would help you conclude it's a secure system **(3marks)**

d. A corporation is considering a best authentication method for access control within their computers, which method has the best authentication strength explain you answer?**(2mark)**

QUESTION FIVE [20 MARKS]

a. Briefly explain five best practices for limiting access to computer systems which can help secure systems and their data. **(10mark)**

b. Passwords are one of the mechanisms of information systems access control it is advised that they shouldn't be the sole mechanism employed. Give reasons to justify the advice **(7 marks)**

c. For a user to access an information system, explain the conditions that should be met? **(3 marks)**