JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

EXAMINATION FOR THE DEGREE OF MASTERS OF IT SECURITY & AUDIT

2ND YEAR 1ST SEMESTER 2015/2016 ACADEMIC YEAR

KISUMU LEARNING CENTER

COURSE CODE: IIT 5215

COURSE TITLE: ADVANCED CYBERCRIME INVESTIGATION

EXAM VENUE: **STREAM: IT SECURITY & AUDIT**

DATE: **EXAM SESSION: 3 HOURS**

TIME:

INSTRUCTIONS

1. **Answer ANY THREE 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 [20 MARKS]

a) Define the following terms
   i) Phishing **(2 marks)**
   ii) Cyber-stalking **(2 marks)**
   iii) Cybersecurity **(2 marks)**
   iv) Cyber-terrorism **(2 marks)**
   v) Critical infrastructure **(2 marks)**
   vi) Data breach **(2 marks)**

b) Security is about more than simply protection. It allows companies the freedom to operate without fear. And while sophisticated security systems and due diligence will help protect against cyber-crime, there is one key weapon that will keep defenses as strong as possible: collaboration. Explain? **(4 marks)**

c) Briefly discuss the future trends and issues (at least six) the criminal justice system must contend with regarding digital crime. Your answer should include the general forecasts and the future impacts. **(6 marks)**

QUESTION 2 [20 MARKS]

a) In 2013 a workshop on effective cybercrime legislation in East Africa was held in Dar es Salaam, Tanzania, to deliberate on the fight against cybercrime in East Africa. Cybercriminals have taken advantage of weaknesses in cybercrime legislation and the ineffective law enforcement leading to proliferation of illicit activities. The workshop proposed a model for addressing cybercrime as part of the cyber security strategy. Discuss the components articulated in this model. **(10 marks)**

b) During the conference participants from Kenya proposed strategies on cybercrime and electronic evidence. Identify any five strategies that were proposed by the Kenyan delegation. **(10 marks)**

QUESTION 3 [20 MARKS]

a) Cyber-enabled crimes are traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT). Unlike cyber-dependent crimes, they can be committed without the use of ICT. Discuss six forms of cyber-enabled fraud. **(12 marks)**

b) Cyber criminals may seek to obtain personal and financial data for fraudulent purposes. Cyber-enabled data theft is therefore an integral part of any discussion on fraud. Valuable forms of data may include: personal information (names, bank details, and National Insurance numbers); company accounts; client databases; and intellectual property (for example, new company products or innovations. Below are some cases related to cyber-fraud and theft. Identify the type of cyber-enabled data fraud and explain how personal and financial information is compromised

i) Customers of a telecommunications firm received an email explaining a problem with their latest order. They were asked to go to the company website, via a link in the email, to provide personal information – like their dates of birth and Social Security numbers. Both the email and the website were bogus.(FBI, 2009) **(4 marks)**

ii) A debt-ridden accountant who stole more than KShs 2,400,000 from her pension fund employer was warned that she was 'lucky' to avoid jail. [The cyber fraudster] siphoned off the cash over a two-year period to buy groceries and pay her mortgage after substituting her own bank details for those of suppliers. [She] stole around KShs100,000 a month until a trainee became suspicious about outgoing payments that were recorded on her own computer login, but that she could not remember processing. **(4 marks)**

QUESTION 4 [20 MARKS]

The Kenyan cyber security landscape is evolving fast as more organizations re becoming vulnerable to intrusions and exploitation according to the Kenya Cybersecurity Report 2014.

a) Based on this report identify the top seven Cybersecurity threats in Kenya **(7 marks)**

b) According to the report the fastest growing cyber-threat was anonymous proxy servers located in Kenya. In the period under review, we detected a total of 290,000 attacks originating from anonymous proxy servers compared to 50,000 similar attacks in 2012.

i) What is a proxy server? **(2 marks)**

ii) Explain the likely reason for the faster growth of cyber-attacks in this area? **(3 marks)**

c) According to the same report the top three attacks of the year were Proxy attacks, DNS attacks and Web app attacks. Briefly explain why. **(6 marks)**

QUESTION 5 [20 MARKS]

The 2015 Kenya Cybersecurity Report has identified the top ICT trends that influence Cybersecurity in Kenya today. Discuss these trends and explain how they have/will impact Cybersecurity in Kenya. **(20 marks)**