JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

School of Informatics and Innovative Systems

Academic Year: 2020/2021
Year FOUR: Semester ONE

Course Code: IIT 3414

Course Title: Cyber Crime Investigation

Main Campus

TIME: 2 H0URS

Instructions:

I. **This paper contains FIVE questions**
II. **Question one is compulsory**
III. **Answer any other two questions**

Question 1 [30 marks]

a) E
xplain four basic steps in computer forensic investigation. (4 marks)

b) B
riefly describe the policy and procedure development stage of computer investigation. (4 marks)

c) D
escribe three computer-based investigation methodologies. (6 marks)

d) E
xplain why an investigator needs a search warrant to carry out an investigation. (3 marks)

e) B
riefly describe the evidence collection process during Cyber Crime investigation (6 marks).

f) D
escribe in detail the process of evidence assessment and analysis (5 marks).

g) B
riefly Explain any two various methods of examining digital evidence. (2 marks)

Question 2 [20 marks]

a) To be effective, a risk analysis process must be accepted as part of the business process of the enterprise. Identifying a threat is just the first part of the analysis phase. It is also necessary to determine just how vulnerable the enterprise is to that threat. There are a number of factors that impact a threat. There are nearly as many factors affecting the threat and its impact on the enterprise as there are threats.

i) Discuss briefly any six factors can increase or decrease the level of impact an attack may have on an enterprise and its assets. (6 Marks)

b) Given that the majority of security problems are internal to the organization, it is incumbent upon management to review system administration policies and procedures at least once a year to ensure required security levels are being followed. Obtaining a third party audit and certification of the processes is also a prudent approach. State any five specific items to note in administrative security policies. (5 Marks)

c) The goal of an IT risk management organization should be to ensure potential risks are identified and assessed and, where the business considers it necessary, to implement controls that mitigate the potential impact of the risk.

i) State five ways how this is achieved. (5 Marks)

d) The response to the introduction of risk or threat can result in one of four decisions. Explain briefly each of the four possible decisions (4 Marks)

Question 3 [20 marks]

a) B
riefly describe what constitutes Cybercrime in Kenyan Laws as outlined in the Cybercrimes and Computer related Crimes Bill 2014 **(8 marks)**

b) D
iscuss three challenges you can face during Cyber Crime investigation process in Kenya **(6 marks)**

c)
Security models provide guidelines and frameworks for implementing security policies to protect the confidentiality, integrity, and availability of information on devices or networks. In this regard, discuss the following security models:
(i) Lattice Model **(2 Marks)**
(ii) Bell-LaPadula (BLP) Model **(3 Marks)**
(iii) Define the hash function and its role in computer security. **(1 marks)**

Question 4 [20 marks]

a) W
hat is the purpose of a verbal formal report? (2 marks)

b) W
hen can you rely on a verbal informal report? (2 marks)

c) D
escribe four roles of a formal investigation report. (8 marks)

d) C
ompare and contrast the forms on cybercrime in Kenya and other Continents such as Countries in Europe (6 marks)

e) S
tate two functions of an investigation report in a court of law (2 marks)

Question 5 [20 marks]

a) S

enior management defines information security policies to communicate how information assetswithin the organization will be protected. Generally there are three security policy types that affectsenior management. Briefly, list and describe each of these policies. [4 Marks]

b) A computer user downloads large files of pornographic material, filling up the disk. This violatespolicy, but the system manager does not enforce this policy very carefully, so users can ignore it.Here the trust goes both ways. The system administrator trusts that most users will not break thisrule, and the users trust that the system administrator will not enforce it. List any five reasons whypeople will violate policy. [5 Marks]

a)

Suppose you are starting a new business which deals with a secret new technology. Describe, in overview, how you would design a secure work environment for the company. Think of physicalissues, software issues and work practices. [5 Marks]

b)

Define the following terminologies as used in information systems security:

(i) Reference Monitor (RM) [2 Mark]

(ii) Biometrics [2 Mark]

(iii)Computer Forensics [2 Mark]