JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SECURITY AND FORENSICS 2ND YEAR 2ND SEMESTER 2020/2021

ACADEMIC YEAR

SPECIAL RESIT TWO

Main Campus

COURSE CODE: IIT 3313

TITLE: LEGAL ISSUES, ETHICS AND INCIDENT RESPONSE IN IT SECURITY

COURSE EXAM VENUE:

STREAM:

DATE: **EXAM SESSION:**

TIME: 2HRS

INSTRUCTIONS

1. **Answer ONE (COMPULSORY) and ANY 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. Briefly explain why attackers target applications installed on server rather than operating system (2marks)

b. State and explain your answer whether corporate protection would or would not cover the following:

i. Authors word describing the dark and stormy night on which occurred the murder at the centre of the mystery novel. (3marks)

ii. The idea of making the events of a dark and stormy night central to murder mystery. (3marks)

c. Explain the following terms:

i. Foot printing (2mark)

ii. Session hijacking (2mark)

iii. Net Stumbler (2mark)

d. State and briefly explain four basic knowledge in hacking methods (8marks)

e. S

tate and briefly explain three security measures that can be deployed to inspect all inbound and outbound network activities and identification of suspicious patterns that may indicate a network or system attacks from intruders attempting to break into or compromise a system (8marks)

Question 2 [20 marks]

a. What are patents and where do they come from? (2marks)

b. What does a patent do ? (2marks)

c. State six reasons why patents should be enforced? (6marks)

d. Explain why organizations should minimize frequency of incidents? (3marks)

e. At what three levels of I.T resources and Infrastructure should be given priority of security (3marks)

f. Explain why problem prevention is cost effective than reaction to them after they occurred (2marks)

g. Why do you think incident prevention is important compliment to an incident response capability (2marks)

Question 3 [20 marks]

a. State why you think it is important for an organization to document guidelines they use in handling computer incidents (4marks)

b. Different types of computer incidences merit different response strategies. State and briefly explain some six attacks vectors. (12marks)

c. Why should organizations create written guidelines for prioritizing incidents (4marks)

Question 4 [20 marks]

a. R
isk management encompasses three processes. State them and explain (6marks)

b. W
hat are the fundamental reasons why organizations implement risk management process for I.T systems? (4marks)

c. S
tate five phases of an I.T system's SDLC (5marks)

d. W
hat is the objective of performing risk management in an organization and how can organization carry out this? (5marks)

Question 5 [20 marks]

a. W
hat is "insider threat"? outline five impacts of insider threats to information system resources of an organization (7marks)

b. Vulnerability is a significant aspect and a stage for many networked computer incidents. Identify three vulnerabilities and discuss how each can be responded to, to avoid further incidents (9marks)

c. Give four reasons why you think information technology workers must be in the forefront setting examples in enforcing policies regarding ethical use of I.T infrastructure in an organization (4marks)