JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

School of Informatics and Innovative Systems

MAIN CAMPUS

Academic Year: 2020/2021
Year Three Semester Two

Course Code: IIT 3321

Course Title: Enterprise System Security and Management

Stream: Computer Forensic

SPECIAL RESIT TWO

TIME: 2 H0URS

Instructions:

This paper contains FIVE questions

Question one is compulsory

Answer any other two questions

QUESTION 1 (30 MARKS)

a) Give five elements of information security. (5 marks)

b) Give five threats to information processing systems based on surveys that have been done. (5 marks)

c) Explain the following terms:

    i. Policy (1 mark)
    ii. Standards. (1 mark)
    iii. Procedures. (1 mark)
    iv. Guidelines. (1 mark)

d) To formalize the information security organization, consideration should be given to developing several key documents consistent with the organization's procedures and culture. Give five of these documents. (5 marks)

e) There are five keys to establishing an effective awareness program. Enumerate them. (5 marks)

f) What are the three reasons for any organization establishing contacts with the relevant authorities for purposes of information security? (3 marks)

g) Explain the following terms:

    i. Cryptology. (1 mark)
    ii. Cryptography. (1 mark)
    iii. Cryptanalysis. (1 mark)

QUESTION 2 (20 MARKS)

a) As an information security professional explain the main purpose of conducting a "walkabout" in your organization. (2 marks)

b) According to ISO 27002, confidentiality and nondisclosure agreements are designed to protect an organization's information and inform those signing the agreement of their responsibility for the information's responsible and authorized protection, use, and disclosure. Give five things that should be included in the confidentiality agreement. (5 marks)

c) What are the two requirements for an information security function to have the requisite level of authority in an organization? (2 marks)

d) Give five departments/individuals in an organization that may be involved in the protection of the information assets and the roles/responsibility that they play. (5 marks)

e) Security awareness programs are aimed at producing behavioral change or rein¬forcement. There are three change category indicators that can help tell us if the program's desired effects are taking place. Enumerate them and give an example for each. (6 marks)

QUESTION 3 (20 MARKS)

a) What is the goal if information security? (1 mark)

b) Enumerate Kerchkhoff's Six principles. (6 marks)

c) Explain briefly the following types of cryptanalysis methods.

Brute force. (2 marks)

Frequency analysis. (2 marks)

Man-in-the-middle attack. (2 marks)

d) List five strategies that you can use for selling the security awareness program to the organization. (5 marks)

e) Two-factor authentication is one of the methodologies being used by organizations for more sensitive systems and for users with higher privileged access. Two-factor authentication takes advantage of multiple authentication technologies to provide stronger security by relying on two of three factors. Enumerate the three factors. (3 marks)

QUESTION 4 (20 MARKS)

a) Each risk assessment process is divided into three distinct sessions. Discuss briefly each of the three sessions. (6 marks)

b) One way of categorizing access controls is by describing the way they are implemented, or what they are. Explain the three kinds of implementations that may be applied. (6 marks)

c) Describe the two roles that any policy in an organization plays. (4 marks)

d) User access management is about making sure authorized users have appropriate access to the system and preventing unauthorized system access. ISO 27002 out¬lines several areas where user access management must be considered. List the four areas concerned. (4 marks)

QUESTION 5 (20 MARKS)

a) Compromise or loss of information or inability to process it have associated costs. Enumerate and explain any three of those associated costs. (6 marks)

b) Give the steps undertaken in a risk assessment process. (4 marks)

c) Explain any three attacks that can be conducted on web applications. (6 marks)

d) In incident management there are three models of team structures that can be used for the incidence response team. Briefly discuss them. (6 marks)