MACHAKOS UNIVERSITY

University Examinations for 2020/2021

SCHOOL OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTING AND INFORMATION TECHNOLOGY

FOURTH YEAR FIRST SEMESTER EXAMINATION FOR

BACHELOR OF SCIENCE (MATHEMATICS AND COMPUTER)

SCO 406: COMPUTER SYSTEM SECURITY

DATE: 18/8/2021 **TIME: 8:30 – 10:30 AM**

INSTRUCTIONS

Answer Question One and Any Other Two Questions

QUESTION ONE (COMPULSORY) (30 MARKS)

a) Describe briefly the following terms as used in computer security:
   i) Malware (1 mark)
   ii) Hackers (1 mark)
   iii) Virus (1 mark)
   iv) Worms (1 mark)
   v) Spyware (1 mark)

b) List and explain the common security goals (4 marks)

c) Explain the three main countermeasures used to stop threats. (4 marks)

d) Employees are the people who can be dangerous to systems, Explain (3 marks)

e) Discuss briefly cyber-crime (2 marks)

f) Risk to computer security can apply to a number of people using examples, explain (4 marks)

g) Clearly differentiate between firewalls and gateways. (4 marks)

h) How does social media platforms influence computer security. (4 marks)

QUESTION TWO (20 MARKS)

a) Using examples, describe any FOUR security control measures. (10 marks)

b) Discuss the types of damages that can be done to computer systems. (10 marks)

QUESTION THREE (20 MARKS)

a) Describe the top ten database security threats (10 marks)

b) Discuss the following category of vulnerability

   i Physical natural (3 marks)

   ii Hardware/software (4 marks)

   iii Human (3 marks)

QUESTION FOUR (20 MARKS)

a) Discuss the five principles of risk management (10 marks)

b) Describe the organizational security policies towards security planning. (10 marks)

QUESTION FIVE (20 MARKS)

a) You are an IT security consultant and have been approached by the system administrator for the Interim Electoral and Boundaries Commission (IEBC) web server. She is worried that a hacker might launch a Distributed Denial of Service attack against the server.

You have been asked to write a report using the following points to guide you

i) the workings of such an attack, (2 marks)

ii) how to detect it, (2 marks)

iii) and how to prevent it. (4 marks)

b) While giving examples, describe authentication methods used in distributed systems (8 marks)

c) Distinguish between public-key cryptography and symmetric-key cryptography (2 marks)

d) Give one advantage and one disadvantage of public-key cryptography over symmetric-key cryptography. (2 marks)