TECHNICAL UNIVERSITY OF MOMBASA

INSTITUTE OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

UNIVERSITY EXAMINATION FOR:

DICT JAN 2015

EIT 2208: FUNDAMENTALS OF COMPUTER SECURITY

END OF SEMESTER EXAMINATION

SERIES: APRIL2016

TIME: 2HOURS

DATE: Pick DateSelect MonthPick Year

Instructions to Candidates

You should have the following for this examination

-Answer Booklet, examination pass and student ID

This paper consists of **FIVE** questions. Attemptany THREE questions.

Do not write on the question paper.

Q1Explain the following **techniques** used by malicious attackers on a computer based system.

i) E-mail Hacking (4 marks)
ii) Social Engineering (4 marks)
iii) Intrusion Attacks (4 marks)
iv) DOS Attacks (4 marks)
v) E-mail Bombing (4 marks)

Q2(a) A virus is a program that infects a computer by attaching itself to another program, and propagating itself when that program is executed**.**

Explain the following types of computer virus.

a. Memory-Resident Virus
b. Program File Virus

c. Polymorphic Virus
d. Boot Sector Virus
e. Stealth Virus
f. Macro Virus
g. E-mail virus (14 marks)

(b))Explain the following malicious code that can cause damage to computer or network

i. Active Content
ii. Zombies and Botnets
iii. Scare ware (6 marks)

Q3(a) Define the term intrusion detection system (IDS) as used in computer security. (2 marks)

(b) Explain the following intrusion detection system (IDS) as used in computer security.

i) Network IDS
ii) Host IDS
iii) Signature based IDS
iv) Anomaly based IDS
v) Passive IDS
vi) Reactive IDS (12 marks)

c) Explain any three Anti-virus Software kits (6 marks)

Q4(a) Explain the following protection terms as used in Security Web Environment.

i. Certificates
ii. Electronic Signature
iii. Encryption
iv. Decryption
v. Integrity
vi. Permissions

vii. PKI, public and private key
viii. Non- repudiation

(16 marks)

(b) Explain the following term

i. Accountability

ii. Nonrepudiation (4 marks)

Q5(a) Explain the term firewall as used in computer security. (2 marks)

(b) Describe the two types firewalls (6 marks)

c)) Describe the three methods used to control the flow of traffic in a firewall. (12 marks)