(Knowledge for Development)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS
2017/2018 ACADEMIC YEAR

SPECIAL/SUPPLEMENTARY EXAMINATIONS
YEAR FOUR SEMESTER TWO EXAMINATIONS

FOR THE DEGREE OF BACHELOR OF SCIENCE
COMPUTER SCIENCE

COURSE CODE : CSC 474E

COURSE TITLE : SECURITY IN NETWORKS

DATE: 11/10/2018 **TIME: 09:00 A.M - 11:00 A.M**

INSTRUCTIONS TO CANDIDATES

ANSWER **QUESTIONS ONE AND ANY OTHER TWO.**

QUESTION ONE (COMPULSORY) [30 MARKS]

a) What is IPSec? **[2 marks]**

b) Differentiate between Authentication Header (AH) and Encapsulating Security Payload (ESP). **[3 marks]**

c) Explain the following terms

i. Eavesdropping **[2 marks]**

ii. Masquerading **[2 marks]**

iii. Denial of Service **[2 marks]**

d) Define social engineering? **[2 marks]**

e) Outline the important security functions provided by the IPsec. **[6 marks]**

f) Describe two features that help in defeating a root takeover attack. **[6 marks]**

g) State the typical attacks that are carried out on Wireless LAN. **[5 marks]**

QUESTION TWO [20 MARKS]

a) State the primary goal of network security **[3 marks]**

b) Describe the mechanisms defined by International Telecommunication Union (ITU), in its recommendation on security architecture X.800 to bring the standardization of methods to achieve network security. **[6 marks]**

c) What is IP Spoofing? What implications does it have on network security? **[5 marks]**

d) Explain the main eight differences between TLS and SSLv3 protocols. **[6 marks]**

QUESTION THREE [20 MARKS]

a) A Feistel cipher is used in the DES algorithm. Describe the operation of a Feistel cipher. **[5 marks]**

b) Briefly describe three modes of operation of DES. **[7 marks]**

c) Discuss the security of AES. **[12 marks]**

QUESTION FOUR [20 MARKS]

a) Explain the principle of least privilege. **[5 marks]**

b) Explain how capability lists are used to represent access control matrices. Discuss the main problem associated with the use of capability lists and its consequences.

[6 marks]

c) Explain how capability lists are now commonly implemented in the form of attribute certificates to get around the main problem associated with the use of capability lists for access control. **[3 marks]**

d) The permission bits associated with a program call Prog1 and a dataset called Data1 are as follows:

Prog1: 1 1 1 1 0 1 1 0 0

Data1: 1 1 1 1 0 0 0 0 0

State the permissions these bits give.

Describe the advantages and disadvantages of using permission bits for access control.

[6 marks]

QUESTION FIVE [20 Marks]

a) An ideal password authentication scheme has to withstand a number of attacks. Describe five of these attacks. **[10 marks]**

b) Describe the goals an ideal password authentication scheme should achieve.

[10 marks]