TECHNICAL UNIVERSITY OF MOMBASA

INSTITUTE OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

UNIVERSITY EXAMINATION FOR:

BSCS/AUG2021/J-FT

CIT4411: NETWORK SECURITY

END OF SEMESTER EXAMINATION

SERIES: DECEMBER 2024

TIME: 2HOURS

DATE: Pick DateDec2024

Instructions to Candidates

You should have the following for this examination

-Answer Booklet, examination pass and student ID

This paper consists of **FIVE** questions. Attempt question ONE (Compulsory) and any other TWO questions.

Do not write on the question paper.

Question ONE

a)Confidentiality, Integrity and Availability are core attributes in security. Identify THREE (3) threats to a wireless network that could compromise security. [3Marks]

b) Briefly describe the term vulnerability in the context of network security and provide THREE (3) examples of vulnerabilities in a network. [4Marks]

c) IPsec is a suite of protocols for securing networks. Briefly outline how it provides confidentiality, integrity and authentication. [6Marks]

d) Explain encryption, and and it's uses in network security? [4Marks]

e) Software that replicates itself and sends the copies to other computers is best described as a programmed threat: Explain the following programmed threats to the network and computer.

i. Logic bomb [8Marks]
ii. Trojan horse
iii. Worm
iv. Backdoor

f) Using a diagram explain the encryption algorithm using a secret key. [5Marks]

Question TWO

a) Explain the difference between symmetric and asymmetric encryption? [1Mark]

b) Each network attack targets different vulnerabilities and aims to compromise network security Discuss the following common types of network attacks and their measures. [8Marks]

i. Phishing,

ii. Man-in-the-middle attacks,

iii. Denial of service (DoS),

iv. SQL injection,

b) Employees are accessing corporate data from personal devices, increasing the risk of data breaches. How can the organization secure these devices through. [6Marks]

i. Password Authentication

ii. Multi-Factor Authentication

iii. Biometric Authentication

Question THREE

a) A company's internal network is experiencing unusual traffic spikes. What steps should the IT team take to investigate? [3Marks]

b) What is VPN and explain how it enhances network security. [2Marks]

c) There are several methods of achieving secure remote access. One important method is to use a VPN. Explain how a VPN achieves each of the following requirements. [10Marks]

i. Authentication
ii. Access Control
iii. Confidentiality.
iv. Data Integrity
v. Availability

Question FOUR

a)Explain what is meant by the term firewall in network security and discuss how it is used in network architectures. [3Marks]

b) Firewalls use Access Control Lists (ACL). Explain what is meant by an ACL and typical contents. [10Marks]

c) Organisations define different access policies framework to secure their data. Explain Role-Based Access Control (RBAC) as a requirement in organization security. [2Marks]

Question FIVE

a) X.509 standard is used to describe public-Key certificates. Discuss its application in digital certicate. [5Marks]

b) Explain what is meant by a digital signature and describe how it is generated. [5Marks]

b) User A wants to digitally sign a document M and send it to B. Give a function that describes how the signing is performed (you must also describe all variables used) and explain what is sent from A to M. [5Marks]