(Knowledge for Development)

KIBABII UNIVERSITY

UNIVERSITY EXAMINATIONS
2020/2021 ACADEMIC YEAR

END OF SEMESTER EXAMINATIONS
YEAR FOUR SEMESTER TWO EXAMINATIONS

FOR THE DEGREE OF
BACHELOR OF SCIENCE COMPUTER SCIENCE

COURSE CODE : CSC 477E

COURSE TITLE : **SECURITY IN NETWORKS**

DATE: 29/09/2021 **TIME:** 02:00 P.M – 04:00 P.M

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE (COMPULSORY) [30 MARKS]

a. i. What is your understanding of network security [2 Marks]

ii. How does network security work? [4 Marks]

b. i. Differentiate between intrusion prevention and intrusion detection systems [4 Marks]

ii. Your organization can afford to purchase one of the above for use. With reasons, what will you advice the CEO to buy? [4 Marks]

iii. Differentiate between a hub and a switch [2 Marks]

c. Describe resources found in your internal network that could be at risk of attack either internally or externally. [4 Marks]

d. Define the following terms as used in network security

i. Risk [2 Marks]

ii. Threat [2 Marks]

iii. Vulnerability [2 Marks]

iv. Brute force [2 Marks]

v. Burst error [2 Marks]

QUESTION TWO [20 MARKS]

a. Zoom has been criticized for poor security: bad cryptography, lack of end-to-end encryption, guessable meeting IDs that can lead to Zoom-bombing, apparently poor quality code per CyberITL's metrics, abuse of privileged mechanisms on Macs, etc. Suppose they respond by saying "we're going to put a firewall in front of our servers; all participants' computers should also be behind a firewall."

i. What is a firewall? [2 Marks]

ii. What type of traffic is denied when a firewall is deployed? [3 Marks]

iii. Will this help zoom? Explain [6 Marks]

iv. What is a VPN and will it be of help in the above scenario? [3 Marks]

ABNO is an ERP currently used by Kibabii University for student and staff management. It has a University web site that doesn't even support, let alone require, multi-factor authentication (MFA). It's also one of the most security-sensitive, since among other things it's used by lecturers to submit grades. The reason it doesn't use MFA is that due to an old platform incompatibility with the "Common Authentication System", ABNO does its own authentication. Partially to compensate, there is auditing, email confirmation of major actions, etc.

b. Discuss the advantages and disadvantages of this approach compared with MFA. [6 Marks]

QUESTION THREE [20 MARKS]

a. As a computing student who has studied network security, describe five types of network security features that are available for use today. [10 Marks]

b. As a network administrator, recommend to your employer ways that your organization will use to ensure data loss prevention in the organization. [5 Marks]

c. What do you see as the objective of information security within a business or an organization? [5 Marks]

QUESTION FOUR [20 MARKS]

a. Discuss factors that affect the performance of a Network [8 Marks]

b. i. What is ransomware? [4 Marks]

ii. How does ransomware work [4 Marks]

c. Compare and contrast how the early computer security worked against what we currently have in today's world. [4 Marks]

QUESTION FIVE [20 MARKS]

a. i. Describe three basic means for user authentication [6 Marks]

ii. What is two level authentication [2 Marks]

b. Can police track an IP address after it has been changed? [4 Marks]

c. You discover an active problem on your organization's network, but it's out of your sphere of influence. There's no doubt that you can fix it, though; so what do you do? [4 Marks]

d. Why are internal threats usually more effective than external threats? [4 Marks]