KISII UNIVERSITY
UNIVERSITY EXAMINATIONS

FIRST YEAR EXAMINATION FOR THE AWARD OF THE DEGREE OF MASTER OF INFORMATION SYSTEMS
SECOND SEMESTER 2023/2024
[JANUARY-APRIL, 2024]

ISYS 822: INFORMATION SYSTEMS SECURITY

STREAM: Y1 S2 **TIME: 2 HOURS**

DAY: MONDAY, 9.00 A.M. – 12.00 P.M. **DATE: 27/05/2024**

INSTRUCTIONS

1. ***Do not write anything on this question paper.***
2. ***Answer question ONE and any other TWO questions.***

QUESTION ONE

a). Public key infrastructure refers to the CAs and digital certificate procedures that are accepted by all parties. Identify FOUR items found on a digital certificate. [4 Marks]

b). Penetration testing is a methodical probing of a target network in order to identify weaknesses in the network. Describe the FOUR phases involved in security assessments [4 Marks]

c). Explain what is meant by social engineering attack on a password

[4 Marks]

d). Using examples explain the role of the logic of authentication [4 Marks]

e). An ideal password authentication scheme has to withstand a number of attacks. Describe FIVE of these attacks. [4 Marks]

QUESTION TWO

a). Human element is an important consideration in any security issue because it contributes heavily to realization of attacks primarily because a human attacker is behind the development of an attack tool and will still be the one to run the first attack command. Describe FIVE phases of the hacking methodology. [8 Marks]

b). Using illustrations describe the terms honeypot, honeynet and padded cell systems when used in relation to information security and describe how each can be used to protect and secure an organisation's assets. [6 Marks]

c). Highlight the benefits that can be provided by intrusion detection systems and Intrusion Prevention Systems in protecting an organization records [6 Marks]

QUESTION THREE

a).i). How is infrastructure protection (assuring the security of utility services) related to information security [2 marks]

ii). How can the practice of information security be described as both an art and a science? [2 marks]

b). Tim is a computer forensic specialist who intend to create a hard drive disk image. Discuss any two forensic tools for imaging hard drives that Tim would use. [8 Marks]

c). A major data breach has been witnessed in Kisii University and you have been called as an expert to conduct an audit into its Information Systems.

a. What would be your main objective and scope of conducting the audit? Explain your answer. [2 marks]
b. State all major equipment/ entities that will be assessed in your audit. [2 marks]
c. Is there need to interrogate the personnel in charge of information security in the university? Explain your answer. [2 marks]
d. In detail discuss any limitation that might be encountered in the audit process. [2 marks]

QUESTION FOUR

a). Briefly describe the first THREE steps of security risk assessment in an organization that has invested heavily in computer based systems [6 Marks]

b). While giving examples, give key differences between Discretionary access control and mandatory access control [6 Marks]

c). Bell and La Padula Model (BLP), Chinese Wall model, Biba model and Clark-Wilson models are commonly security models used to achieve different security services. Outline the security service achieved by each of the above security models. [8 Marks]

QUESTION FIVE

a). Describe while giving examples THREE types of controls that can be used to manage security risks in an organization [6 Marks]

b). As any other system and technology the biometric technology has its vulnerabilities. As a security expert in biometrics you have been requested to prepare a presentation on vulnerabilities and attacks on biometric authentication system for your colleagues. Use a diagram to demonstrate vulnerable areas in the system. [6 Marks]

c). Data is becoming a vital resource in any organization. Users must authenticate themselves to the system to ensure data remains secure. As a system administrator of an IT firm, discuss any THREE ways you would use for authenticating users to the server. [8 Marks]