JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF BUSINESS INFORMATION SYSTEMS

4TH YEAR 2ND SEMESTER 2024/2025 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ITB 2407

COURSE TITLE: INFORMATION SYSTEM SECURITY

EXAM VENUE: LR 2 BSC. INFORMSTION SYSTEM

DATE: 17/4/2025 EXAM SESSION: 15.00-1700

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

Question 1 (30 marks)

a) Describe Four ways in which micro-segmentation enhances security in advanced architectures. 4mks

b) State and explain three reasons why threat modeling is important 3mks

c) What is the difference between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) in terms of functionality? 2mks

d) List and describe Four tools which are commonly used in penetration testing? 4mks

e) What three strategies can organizations implement to protect sensitive data? 3mks

f) State and explain three ways how the multi-tenancy model in cloud environments impact security. 3mks

g) A large organization wants to use AI/ML for anomaly detection to identify insider threats. An employee recently exfiltrated sensitive data by uploading it to a personal cloud storage account. What Four challenges might the organization face? 4mks

h) A company with a bring-your-own-device (BYOD) policy has noticed an increase in malware infections on employee mobile devices, leading to data breaches. What Four tools or policies should it implement? 4mks

i) A multinational corporation has adopted a hybrid cloud environment, with employees and contractors accessing corporate applications from various locations and devices, including unmanaged personal devices. A recent ransomware attack exploited a stolen employee credential to gain access to sensitive systems. Explain three ways how you would apply the Zero Trust security model to secure this environment 3mks

Question 2 (20 marks)

a) A university breached GDPR by failing to secure student data, resulting in a fine. Explain Five ways of how you would implement a data governance framework post-incident to prevent recurrence? 10mks

b) A bank discovers an employee fell for a vishing (voice phishing) attack, revealing a one-time password (OTP) that allowed attackers to access a customer account.

i) State and explain four ways how would you simulate this attack in a penetration test? 6mks

ii) What Four countermeasures would you propose? 4mks

Question 3 (20 marks)

a) A software company is developing a web-based financial application that processes customer transactions and stores sensitive data, such as payment details and personal information. As part of the security design process, you've been tasked with performing threat modeling.

i) How would you apply the STRIDE methodology to identify potential threats to this application? 4mks

ii) What three specific threats might you uncover in the process, include mitigation strategies on each of the threats? 6mks

b) A logistics company is using a micro services architecture on Docker containers, with services for shipment tracking, billing, and customer notifications. An attacker exploited a misconfigured service to gain access to the billing database, leading to a data breach. State and explain Five approaches on how would you secure the architecture to prevent such incidents? 10mks

Question 4 (20 marks)

a) A financial institution is experiencing an increase in sophisticated phishing attacks targeting its employees. The attacks often evade traditional signature-based detection systems. Explain five ways how AI/ML can be applied to improve phishing detection? 10mks

b) A cybersecurity firm is considering using blockchain to create a decentralized threat intelligence sharing platform, allowing organizations to anonymously share indicators of compromise (IoCs). Explain Five security benefits of this approach 10mks

Question 5 (20 marks)

a) Your security team is struggling with low morale due to frequent after-hours incident response calls and a lack of recognition for their efforts. As the security leader, explain steps how you would address these issues to improve team engagement and retention? 12mks

b) Your organization's Chief Finance Officer (CFO) has challenged your proposed security budget, arguing that the requested increase is unnecessary given the lack of recent incidents. Explain eight approaches you would use to justify the budget increase and ensure resources are allocated effectively? 8mks