NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

# FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF CYBER SECURITY

| | |
|---|---|
| **QUALIFICATION:** *BACHELOR OF COMPUTER SCIENCE (HONS DIGITAL FORENSICS)* | |
| **QUALIFICATION CODE:** 08 BCCS | **LEVEL: 8** |
| **COURSE:** SECURITY ANALYTICS | **COURSE CODE:** SAS821S |
| **DATE:** NOVEMBER 2024 | **SESSION:** THEORY |
| **DURATION:** 2 HOURS | **MARKS: 70** |

| **FIRST OPPORTUNITY EXAMINATION QUESTION PAPER** | |
|---|---|
| **EXAMINER(S)** | PROF ATTLEE M. GAMUNDANI |
| **MODERATOR:** | MR MBAUNGURAIJE TJIKUZU |

**THIS QUESTION PAPER CONSISTS OF 2 PAGES**
(Excluding this front page)

**INSTRUCTIONS**

1. Answer ALL the questions.
2. Write clearly and neatly.
3. In answering questions, be guided by the allocated marks.
4. Number your answers clearly following the numbering used in this question paper.

**PERMISSIBLE MATERIALS**

1. None

## SECTION A: Case Study – 20 Marks

### QUESTION 1 — 20 marks

XYZ Corporation, a multinational company, has been experiencing suspicious activities on its network. There have been multiple unauthorised access attempts, and some servers have shown unusual traffic patterns. The company has vast amounts of network log data and wants to implement a machine learning-based Intrusion Detection System (IDS) to identify and prevent potential security breaches.

(a) Outline the steps you would take to preprocess the network log data before applying machine learning algorithms. **(5 marks)**

(b) Recommend and justify two suitable machine learning algorithms for building the IDS. Explain how each algorithm works and why it is appropriate for this scenario. **(10 marks)**

(c) Discuss potential challenges you might face when deploying the machine learning-based IDS in a real-world environment. Propose solutions to address these challenges. **(5 marks)**

## SECTION B – 50 Marks

### QUESTION 2 — 15 marks

(a) Explain how data analytics can detect Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Discuss the types of data you would analyse and the indicators of such attacks. **(7 marks)**

(b) Describe how you would design a simulation model to test the effectiveness of your DoS detection method. Include the steps and tools you would use. **(8 marks)**

**QUESTION 3** **15 marks**

**(a)** *Describe the process of using text mining techniques to detect phishing emails. Highlight the* key steps involved, from data collection to model deployment. **(7 marks)**

**(b)** Identify the challenges associated with text mining in security analytics, such as handling unstructured data and language nuances. Propose solutions to overcome these challenges. **(8 marks)**

**QUESTION 4** **20 marks**

**(a)** *Define adversarial attacks in the context of machine learning and explain their impact on* cybersecurity applications. **(5 marks)**

**(b)** Discuss two algorithms used for creating adversarial samples, such as the Fast Gradient Sign Method (FGSM) and Generative Adversarial Networks (GANs). Explain how they can be used to compromise machine learning models. **(10 marks)**

**(c)** Propose strategies to defend against adversarial attacks on machine learning models in cybersecurity. **(5 marks)**

*******END OF EXAMINATION PAPER*******