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 BHDS	**LEVEL: 8**
COURSE: ADVANCED INTRUSION AND LOG ANALYSIS	**COURSE CODE: AIL811S**
DATE: JULY 2024	**SESSION: THEORY**
DURATION: 3 HOURS	**MARKS: 100**

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**PROF ATTLEE M. GAMUNDANI**
MODERATOR:	**MS NAEMI GERSON**

THIS QUESTION PAPER CONSISTS OF 3 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 following the numbering used in this question paper.

PERMISSIBLE MATERIALS

1. None

SECTION A: Scenario-Based Questions

Question 1: Secure Configuration and System Hardening

As the newly appointed security administrator of a medium-sized retail company, you have been tasked with enhancing the security posture of the organisation's IT systems.

(a) Outline the steps you would take to configure and harden the company's systems securely. **[6 marks]**

(b) Explain how these measures help in mitigating potential security risks. **[4 marks]**

Question 2: Incident Response Planning

Your organisation detected a significant security incident affecting critical data.

(a) As part of the incident response team, detail the initial steps you would take in response to this incident. **[6 marks]**

(b) Discuss the importance of having a predefined incident response plan and how it aids in managing the incident. **[4 marks]**

Question 3: Digital Forensics Fundamentals

You are a digital forensics analyst investigating a case of suspected corporate espionage.

(a) Describe collecting and preserving digital evidence from corporate devices while maintaining the chain of custody. **[4 marks]**

(b) Highlight the challenges you might face during the investigation and how you would address them. **[6 marks]**

Question 4: Understanding Encryption and Its Application

Your company's finance department has reported a breach in their data transmission over the internet.

(a) Propose a plan to implement encryption for securing data transmissions. **[4 marks]**

(b) Discuss different encryption methods and their effectiveness in protecting data integrity and confidentiality. **[6 marks]**

Question 5: Advanced Persistent Threats (APT) and Defence Strategies

Your organisation has been targeted by an Advanced Persistent Threat (APT) group. Outline a comprehensive defence plan against such threats. Include identifying APT activities, containment strategies, and long-term measures to prevent future attacks. **[10 Marks]**

Question 6: Artificial Intelligence in Cybersecurity

As a cybersecurity consultant, you are tasked with enhancing a large corporation's existing Intrusion Detection System (IDS) by integrating Artificial Intelligence (AI) capabilities. Describe the process of implementing AI into the IDS, including data handling, model training, and the deployment of AI models. **[10 marks]**

Section B: Case Study Questions [40 Marks]

Question 7: Security Policy and Governance

Case Study: Global Security in Disarray

A large multinational corporation with branches in Africa, Asia, and North America has grown rapidly through acquisitions and partnerships. This has led to a patchwork of security practices across their global offices:

- **Inconsistent Standards** - Some locations have robust password policies, while others do not. Data handling regulations differ by country of operation.
- **Lack of Central Oversight** - IT in each regional office determines its own security measures, creating confusion and making incident response slow and uncoordinated.

- Increased Risk - Recent audits discovered vulnerabilities in remote offices that could expose sensitive customer and financial data across the entire organisation.
- Compliance Concerns—Upcoming industry and country-specific compliance mandates are looming, and the company is unprepared to meet them globally.

This multinational corporation needs help maintaining its security posture due to inconsistent security policies and the cited issues across its global offices. Using the principles of security policy and governance, draft a unified security policy framework that addresses these challenges. Explain how this framework will be implemented and monitored for compliance across all offices. **[20 Marks]**

Question 8: Cloud Security and Risk Management

Case Study: "Leap of Faith, or Leap into Trouble?"

RapidRetail, a successful online retailer specialising in collectable toys and merchandise, has seen explosive growth over the past few years. Their existing on-premises infrastructure is under load, and frequent website outages frustrate customers during peak shopping. The CTO of RapidRetail strongly advocates cloud migration: the promise of scalability, cost-efficiency, and cutting-edge services are extremely tempting. However, a recent high-profile data breach at a competitor, which also operated in the cloud, has made the company's management hesitant. They want to jump, but only if they can be confident their customer's data is secure.

Develop a risk management plan that outlines the security risks associated with cloud computing and proposes mitigation strategies. Include data security, access control, and incident response considerations for RapidRetail. **[20 Marks]**

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