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: JUNE 2025	**SESSION: THEORY**
DURATION: 3 HOURS	**MARKS: 100**

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**PROF ATTLEE M. GAMUNDANI** **DR ARPIT JAIN**
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 by the numbering used in this question paper.

PERMISSIBLE MATERIALS

1. None

SECTION A: Scenario-Based Questions – 60 Marks

Question 1: Analysing System Storage

A digital forensic investigator is tasked with examining a compromised workstation suspected of unauthorised data exfiltration.

(a) Explain how the investigator would apply Master File Table (MFT) and Registry analysis to determine evidence of user activity. **[6 marks]**

(b) Discuss how the Autopsy tool assists in forensic analysis and how it differs from traditional log examination. **[4 marks]**

Question 2: Analysing System Memory

During an advanced persistent threat (APT) investigation, the attacker used fileless malware suspected to reside in memory.

Describe the end-to-end methodology for memory analysis, including tool selection (e.g., Redline and Volatility) and the indicators of compromise (IoCs) that should be extracted. **[10 Marks]**

Question 3: Reporting After Log Analysis

You have completed an investigation into an insider threat that involved the exfiltration of confidential documents.

Draft an outline of a professional incident response report that includes incident status, findings, timelines, technical analysis, and recommendations. **[10 marks]**

Question 4: Intrusion Detection and Network Forensics

You have completed an investigation into an insider threat that involved the exfiltration of confidential documents.

Draft an outline of a professional incident response report that includes incident status, findings, timelines, technical analysis, and recommendations. **[10 marks]**

Question 5: Threat Intelligence Application

A telecommunications company wants to proactively mitigate threats. Explain how the organisation can use threat intelligence platforms and sources to build predictive defence capabilities. Include types of intelligence (strategic, operational, tactical, technical). **[10 marks]**

Question 6: Log Management Systems

A multinational enterprise is evaluating centralised log management solutions. Compare and contrast the benefits of using a Security Information and Event Management (SIEM) system with traditional syslog-based monitoring.
Include discussion on alert correlation, normalisation, and scalability. **[10 marks]**

Case Study Based Questions [40 Marks]

Question 7: AI- Driven IDS Model Development

A cloud services provider is deploying a machine learning-based Intrusion Detection System (IDS) to enhance detection accuracy and reduce alert fatigue. They have shortlisted three ML algorithms (Random Forest, SVM, and K-Means) and are using a labelled dataset from their past incidents.

(a) Design a pipeline for implementing this IDS, from data preprocessing to model evaluation. **[8 marks]**

(b) Discuss the importance of feature engineering and how dimensionality reduction techniques (e.g., PCA) can improve model performance. **[6 marks]**

(c) Propose a strategy for dealing with false positives and model drift over time. **[6 marks]**

Question 8: Case Log Analysis – Industrial IoT Breach

Scenario:

A smart manufacturing plant is using Industrial IoT (IIoT) devices. A security audit found the following log excerpts from the central monitoring dashboard:

- **Log Entry 1**

```
Time: 2025-03-10 14:23:15
Device: PLC-001
Event: Unauthorised Modbus write request
Source IP: 192.168.50.23
Action: Command blocked
```

- **Log Entry 2**

```
Time: 2025-03-10 14:25:02
Device: PLC-001
Event: Device rebooted unexpectedly
Reason: Remote command
Source IP: 192.168.50.23
```

- **Log Entry 3**

```
Time: 2025-03-10 14:30:45
SIEM Alert: Lateral movement attempt detected
Source IP: 192.168.50.23
Target: SCADA-CORE-01
```

(a) Identify the indicators of compromise and classify the stages of attack using the MITRE ATT&CK framework. **[10 marks]**

(b) Recommend immediate response actions and suggest long-term mitigation strategies using log management and intrusion prevention best practices. **[10 marks]**

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