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 2025	SESSION: THEORY
DURATION: 3 HOURS	MARKS: 100

SECOND OPPORTUNITY/SUPPLEMENTARY 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 following the numbering used in this question paper.

PERMISSIBLE MATERIALS

1. None

SECTION A: Scenario-Based Questions

Question 1: Reconnaissance and Active Attacks

A large enterprise experiences recurring brute-force login attempts originating from multiple IP addresses.

(a) Identify the reconnaissance techniques likely used before launching these attacks. **[4 marks]**

(b) Describe the steps involved in detecting and mitigating such brute-force attacks. **[4 marks]**

(c) Explain how to differentiate between legitimate login failures and brute-force attempts using logs. **[2 marks]**

Question 2: Evidence Acquisition from Host Systems

You are part of a digital forensics response team investigating insider threats at a public-sector institution.

(a) Outline the correct procedure for acquiring host-based evidence while ensuring forensic integrity. **[6 marks]**

(b) Highlight three challenges specific to acquiring volatile memory from running systems. **[4 marks]**

Question 3: Network Log Evaluation for Insider Threats

An internal user is suspected of data exfiltration using non-standard ports.

(a) What specific signs would you look for in firewall and NetFlow logs? **[5 marks]**

(b) Describe how deep packet inspection can assist in confirming the exfiltration. **[5 marks]**

Question 4: Memory Analysis for Detection of Fireless Malware

Fileless malware was suspected in a recent targeted breach of a legal firm.

(a) Discuss how fileless malware typically operates and avoids detection. **[5 marks]**

(b) Explain how tools like Volatility can help uncover the presence of fileless malware in system memory. **[5 marks]**

Question 5: Log Normalisation and Event Correlation

A government security agency maintains thousands of systems with logs collected centrally.

(a) Define log normalisation and explain why it is important in SIEM systems. **[5 marks]**

(b) Describe the process of event correlation and its value in detecting multi-stage attacks. **[5 marks]**

Question 6: Use of Open-source Tools in Intrusion Detection

You are mandated to deploy an open-source IDS solution for a non-profit organisation.

(a) Compare Snort and Suricata in terms of detection capabilities and performance. **[5 marks]**

(b) Discuss the benefits and limitations of relying on open-source intrusion detection tools in high-risk environments. **[5 marks]**

Section B: Case Study Questions [40 Marks]

Question 7: Case Study – Advanced Log Analysis and SIEM Investigation

Context:

The SOC team at a university receives the following alerts from their SIEM system:

- **Alert 1:** Multiple failed logins within 2 minutes on Student-Portal server
- **Alert 2:** Successful login from a foreign IP not previously recorded
- **Alert 3:** Unusual spike in outbound traffic from the same server
- **Alert 4:** PowerShell script executed via remote session

(a) Reconstruct the likely intrusion path based on the alerts. **[8 marks]**

(b) Propose investigative steps to confirm if the incident qualifies as a breach. **[6 marks]**

(c) List four types of evidence that should be preserved for a full forensic investigation. **[6 marks]**

Question 8: Case Study – Threat Intelligence and Attribution

Case:

A mining company was the target of a coordinated spear-phishing campaign that succeeded in breaching its document control systems. Forensic findings suggest the malware used has code overlaps with previously documented campaigns by an APT group known for targeting the natural resources sector.

(a) Based on this context, explain how threat attribution is conducted using malware artefacts and intelligence feeds. **[8 marks]**

(b) Outline the elements of a structured threat intelligence report for company executives. **[6 marks]**

(c) Discuss ethical considerations when naming threat actors and attributing attacks publicly. **[6 marks]**

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