NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: *BACHELOR OF COMPUTER SCIENCE (HONS DIGITAL FORENSICS)*	
QUALIFICATION CODE: 08 BHDF	**LEVEL: 8**
COURSE: ADVANCED INTRUSION AND LOG ANALYSIS	**COURSE CODE:** AIL811S
DATE: JULY 2022	**SESSION:** THEORY
DURATION: 1 HOUR 30 MINUTES	**MARKS: 50**

SECOND OPPORTUNITY/ SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	DR ATTLEE M. GAMUNDANI
MODERATOR:	MR MARSORRY ICKUA

THIS QUESTION PAPER CONSISTS OF 2 PAGES
(including 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

Question 1

(a) Identify and explain any four types of network attacks. [8 marks]

(b) Give and explain any three reasons why it is important to investigate network traffic?[6 marks]

Question 2

(a) Identify and explain the two types of Intrusion Detection Systems (IDS) giving an example for each. [6 marks]

(b) Outline a reason for (i) gathering evidence from an Intrusion Detection System (IDS) and (ii) any two challenges likely to be encountered when gathering evidence from an IDS. [6 marks]

Question 3

(a) Logs are invaluable for Forensic Investigators and system administrators. Explain by citing some examples any two scenarios for each user group where logs prove to be invaluable. [8 marks]

(b) There are four main ways of capturing traffic from a target device on switched networks, explain any two such ways. [4 Marks]

(c) Give and explain any two items that makes up control information in network packet analysis? [4 marks]

Question 4

(a) Generally, each packet analyser performs four steps to process packets, explain any two of the steps. [4 marks]

(b) The following code listing demonstrates what Snort rules are all about. Explain in detail what is displayed in the code below. [4 marks]

Snort Rules

alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 7210 (msg:"SQL SAP MaxDB shell command injection attempt"; flow:to_server,established; content:"exec_ sdbinfo"; fast_pattern:only; pcre:"/exec_sdbinfo\s+[\x26\x3b\x7c\x3e\x3c]/i"; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security- ips drop; reference:bugtraq,27206; reference:cve,2008-0244; classtype:attempted- admin; sid:13356; rev:7;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 21064 (msg:"SQL Ingres Database uuid_ from_char buffer overflow attempt"; flow:to_server,established; content:"uuid_ from_char"; fast_pattern:only; pcre:"/uuid_from_char\s*?\(\s*?[\x22\x27][^\x22\ x27]{37}/smi"; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop; reference:bugtraq,24585; reference:cve,2007-3338; reference:url,supportconnectw.ca.com/public/ca_common_docs/ingresvuln_letter. asp; reference:url,www.ngssoftware.com/advisories/high-risk-vulnerability-in- ingres-stack-overflow; classtype:attempted-admin; sid:12027; rev:11;)

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