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 2024	**SESSION: THEORY**
DURATION: 3 HOURS	**MARKS: 100**

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

THIS QUESTION PAPER CONSISTS OF 4 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: Intrusion Methodologies and Artifacts

You work as a cybersecurity analyst in a financial institution. You notice unusual traffic patterns that suggest a potential intrusion. Describe the steps you would take to identify the intrusion methods and pre-intrusion actions. **[Include how you would distinguish between false positives and true negatives].** **[10 Marks]**

Question 2: Collecting Network Evidence

An e-commerce platform experiences a data breach. You are tasked with collecting network evidence to analyse the breach.

(a) Detail the process of collecting firewall and proxy logs and packet captures. **[6 marks]**

(b) Discuss the importance of each type of evidence in understanding the nature of the attack. **[4 marks]**

Question 3: Malware Analysis for Incident Response

Your company has been infected with ransomware. Outline a plan for responding to this incident. Include steps for classifying the malware, creating a malware sandbox for analysis, and the key aspects of dynamic analysis that will help formulate a response strategy. **[10 marks]**

Question 4: Acquiring Host-based Evidence

During a routine audit, suspicious activities are detected on several organisational workstations. Describe how you would acquire volatile memory and conduct a preliminary analysis, emphasising the significance of evidence acquisition and the challenges faced during memory analysis. **[10 marks]**

Question 5: Network Evidence Analysis

An ISP has noticed an anomaly in their network traffic that suggests a DDoS attack. Draft a comprehensive approach to analysing network evidence, including firewall, proxy logs, and packet captures, to confirm the attack and identify the source.

[10 marks]

Question 6: Classical Machine Learning and Its Application to IDS

Using machine learning techniques, you are developing an Intrusion Detection System (IDS) for a cloud service provider. Describe the process of selecting and training a machine learning model for IDS, including data preparation, feature selection, and model evaluation. **[10 marks]**

Case Study Based Questions [40 Marks]

Question 7: Log Management and Analysis

A healthcare provider has noticed irregularities in their system logs. Using the principles of log management and analysis, analyse the provided log excerpts to identify potential security incidents. Explain your methodology and the tools you would use to analyse the Windows event logs. **[20 Marks]**

Log Excerpts

A. *Excerpt 1: Windows Security Log*

Event ID: 4625
Source: Microsoft-Windows-Security-Auditing
Timestamp: 2024-04-12 03:12:12 AM
User: RDavis
Workstation: RECEPTION-PC
Status: Failure
Failure Reason: Unknown username or bad password.

B. Excerpt 2: Windows Security Log

Event ID: 4776
Source: Microsoft-Windows-Security-Auditing
Timestamp: 2024-04-12 10:14:56 AM
Computer: EHR-SERVER01
User: JSmith
Domain: HOSPITALDOMAIN
Workstation: NURSESTATION4
Source Network Address: 10.5.15.87

C. Excerpt 3: Windows System Log

Event ID: 6009
Source: Microsoft-Windows-Kernel-General
Timestamp: 2024-04-11 11:59:58 PM
Detail: The system has rebooted without cleanly shutting down first.

D. Excerpt 4: IIS Logs (The provider uses a web-based system)

Timestamp: 2024-04-12 01:26:41 AM
Client IP: 213.75.22.80
Method: POST
URI Stem: /patientrecords/access.php?id=5551212
Status: 500 (Server Error)

Question 8: Threat Intelligence

Case Study: "Operation Golden Hook"

A targeted phishing campaign has hit a multinational corporation specialising in technology and manufacturing. Key observations: -

1. **Sophistication** - Emails are exceptionally well-crafted spear-phishing attempts. They mimic internal communications and reference current projects, spoofing sender addresses of high-level executives.
2. **Payload** - Initial analysis suggests a previously unknown malware variant designed to steal intellectual property and exfiltrate sensitive research and development files.
3. **Victimology** - Attackers focused on engineers and research staff. In the past year, competitors have shown increased interest in the corporation's products and patents.

Using the threat intelligence methodologies, develop a threat intelligence report that outlines the threat actors, their methodologies, sources of intelligence, and recommended response strategies. **[20 Marks]**

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