EXTERNAL INTEGRATED SUMMATIVE ASSESSMENT

STUDENT NAME & SURNAME	
ID NUMBER	
EISA REGISTRATION NUMBER	
ASSESSMENT CENTRE	
ASSESSMENT CENTRE ACCREDITATION NUMBER	
QUALIFICATION	
SAQA ID	
CREDITS	
PAPER	
DATE OF EISA	
DURATION	
TOTAL MARKS	

General EISA Rules

1. Students are **only** allowed to use the supplied EISA booklets.
2. Students are **only** allowed to use a black pen for their answers.
3. Students to ensure that their name, surname and EISA registration number appear on the front of your EISA booklet.
4. This is an open-book Assessmentination.
5. All EISA booklets must be handed back to the invigilator intact. No pages may be torn off from the EISA booklet. The removal of EISA booklets from the Assessmentination room is prohibited.
6. Students may make use of a calculator in this EISA.
7. Unless this is an online Assessmentination where access to a computer will be made available to you, the use of any communication devices, including smart watches, cell phones, tablets, iPads, headphones and laptops, is prohibited.
8. All cell phones are to be switched off for the duration of the EISA.
9. The invigilator will not assist you with the explanation of questions related to the EISA.
10. Students are prohibited from conversing in any manner with other students.
11. Students may not leave the Assessmentination venue within one hour of the start of the Assessmentination and in the last 10 minutes of the allotted Assessmentination period.
12. Students who are found to be disruptive and unruly in the assessment centre will be requested to leave the assessment centre by the invigilator.

I HEREBY CONFIRM THAT I HAVE READ THE ABOVE EISA RULES AND DECLARE THAT I UNDERSTAND AND ACCEPT THE RULES.

_____

SIGNATURE OF STUDENT

Candidate Instructions

- Candidates must complete all questions in this EISA.
- Candidates must ensure that they use only a black pen when completing this EISA.
- Should you require additional space to complete your answer, please request additional paper from your invigilator. Ensure that you indicate your name, surname and EISA registration number at the top of the additional paper. Also, ensure that the question number is clearly marked on your additional paper.

Required Deliverables and Naming Convention

- For each scenario that requires screenshots, please follow the standard naming format: Your Initials>_<Scenario#>_<Step#>
  Assessmentple: AB_Scenario1_Step1
- Ensure that all screenshots are saved and organised before submission to the invigilator.

Technical Setup

- Where applicable, you will work with a simulated server or network environment.
- Please ensure that you only scan or interact with the provided IPs or resources.
- If using Nessus Essentials or similar software, the setup may be pre-configured on the assessment platform.
- Refer to your invigilator if any software-related issues arise.

Organisation and Submission

- Ensure all files are named according to the format provided.
- Group all related files for this task together in a folder named [YourInitials_Scenario#]. Eg. AB_Scenario1
- Double-check all screenshots and documents to ensure they show relevant configurations and details clearly.

Section 1: Theory Assessment (100 Marks)

Question 1: Multiple Choice Questions (20 Marks)

1. What is the primary goal of cybersecurity?

a) Enhance user interface.

b) Protect data and systems.

c) Improve processing speed.

d) Boost data storage.

2. Which law regulates data protection in South Africa?

a) GDPR

b) ISO27001

c) POPIA

d) HIPAA

3. Which three principles make up the cybersecurity CIA triad?

a) Confidentiality, Integrity, Availability.

b) Cryptography, Integrity, Authentication.

c) Compliance, Integrity, Availability.

d) Confidentiality, Accountability, Access.

4. What type of malware pretends to be legitimate software?

a) Worm

b) Ransomware

c) Spyware

d) Trojan

5. Which device is commonly used for input in computing?

a) Monitor

b) Mouse

c) CPU

d) Speaker

6. Which network security device helps filter unauthorised access?

a) Hard drive

b) Firewall

c) Printer

d) Webcam

7. What is SQL mainly used for in cybersecurity?

a) Encrypting data.

b) Querying databases.

c) Scanning for vulnerabilities.

d) Securing networks.

8. Which phase in the Design Thinking process focuses on identifying user needs?

a) Define

b) Empathise

c) Prototype

d) Test

9. What is the focus of the Fourth Industrial Revolution (4IR)?

a) Manufacturing

b) Digital technology and AI.

c) Printing press

d) Telephone networks

10. In logical thinking, what is a binary number?

a) A decimal number.

b) A number represented by 1s and 0s.

c) A negative number.

d) A hexadecimal number.

11. Which type of attack involves tricking individuals into revealing confidential information?

a) Phishing.

b) Denial-of-Service.

c) SQL Injection.

d) Malware Infection.

12. Which of the following is a common feature of a secure password?

a) Repeating characters.

b) All lowercase letters.

c) A mix of letters, numbers, and symbols.

d) Simple and easy to remember.

13. What does GDPR stand for in data protection?

a) General Data Policy Regulations.

b) Government Data Privacy Requirements.

c) General Data Protection Regulation.

d) General Database Protection Rules.

14. What kind of device is used to store data long-term?

a) RAM

b) CPU

c) SSD

d) Cache

15. Which of the following best describes a vulnerability?

a) A new feature added to the software.

b) A weakness that can be exploited.

c) A program that performs regular updates.

d) A user's password.

16. Which concept in cybersecurity ensures that information is accessible only to those with permission?

a) Integrity

b) Availability

c) Confidentiality

d) Authentication

17. Which of the following is a key benefit of multi-factor authentication (MFA)?

a) Easier login for all users.

b) Reduces network traffic.

c) Provides an extra layer of security.

d) Automatically updates passwords.

18. What does "DoS" stand for in cybersecurity?

a) Denial-of-Security.

b) Denial-of-Service.

c) Defense-of-Systems.

d) Disruption-of-Service.

19. Which of the following is a method used to prevent unauthorised access to data in transit?

a) Encryption

b) Compression

c) Sorting

d) Caching

20. What is a key aspect of the Design Thinking process?

a) Directly testing solutions on users.

b) Ignoring user feedback.

c) Prioritising speed over accuracy.

d) Focusing on understanding user needs.

Question 2: Short Answer Questions (20 Marks)

1. Explain two main purposes of a firewall in cybersecurity. (2 marks)

Answer:

To block unauthorised access to a network.

To filter incoming and outgoing traffic to ensure only safe data passes through.

Mark Allocation: *1 mark for each correct purpose.*

2. What is identity theft, and why is it harmful? (2 marks)

Answer:

Identity theft is a cybercrime where someone steals another person's personal data to commit fraud.

It is harmful because it can lead to financial loss, damage to one's reputation, and unauthorised use of personal accounts.

Mark Allocation: *1 mark for defining identity theft, 1 mark for explaining why it is harmful.*

3. Describe two key principles of cybersecurity ethics. (2 marks)

Answer:

Confidentiality: Ensuring private information remains secure and accessible only to those with permission.

Integrity: Ensuring data is accurate and unchanged by unauthorised sources.

Mark Allocation*: 1 mark for each correct principle.*

4. Why is data encryption important in data security? (2 marks)

Answer: *Data encryption converts data into a code to prevent unauthorised access, ensuring that even if data is intercepted, it cannot be read without the decryption key.*

Mark Allocation: *2 marks for a complete explanation.*

5. What is the primary role of design thinking in innovation? (2 marks)

Answer: *The primary role of design thinking is to understand user needs deeply and develop solutions that are user-centric and innovative.*

Mark Allocation: *2 marks for a complete explanation.*

6. List two components essential for computer processing. (2 marks)

Answer:

Central Processing Unit (CPU): The main component that performs most of the processing inside a computer.

Random Access Memory (RAM): Temporary storage used by the CPU to store data that is actively being used or processed.

Mark Allocation: *1 mark for each correct component.*

7. Identify two ways the Fourth Industrial Revolution is changing the workplace. (2 marks)

Answer:

Automation and AI: Increased use of robots and AI for routine tasks.

Remote Work: Enhanced digital communication tools facilitating remote work.

Mark Allocation: *1 mark for each correct way.*

8. What is a network vulnerability? Give an Assessmentple. (2 marks)

Answer: *A network vulnerability is a weakness in a network that can be exploited by attackers.*

Assessmentple: An unpatched software bug that allows unauthorised access.

Mark Allocation: *1 mark for the definition, 1 mark for the Assessmentple.*

9. Explain the process of 'reconnaissance' in a cyber threat context. (2 marks)

Answer: *Reconnaissance is the initial phase in which attackers gather information about a target system to find potential vulnerabilities.*

Mark Allocation: *2 marks for a complete explanation.*

10. Why is binary logic essential for cybersecurity professionals? (2 marks)

Answer: *Binary logic is essential because it forms the foundation of computer systems, enabling professionals to understand how data is processed and secured at the most basic level.*

Mark Allocation*: 2 marks for a complete explanation.*

Question 3: True/False (20 Marks)

1. **True or False:**

The goal of a Denial-of-Service (DoS) attack is to make a system or network unavailable to its intended users.

Correct Answer: True

Explanation: *A DoS attack floods the target with traffic, making it unavailable to legitimate users.*

2. **True or False:**

Only public networks, such as Wi-Fi in cafes, are vulnerable to cyber-attacks.

Correct Answer*: False*

Explanation*: Both public and private networks can be vulnerable to cyber-attacks if not properly secured*

3. **True or False:**

Data encryption protects information by converting it into code, making it unreadable to unauthorised users.

Correct Answer: *True*

Explanation: *Data encryption secures information by encoding it, ensuring that only those with the decryption key can access the original data.*

4. **True or False:**

Ransomware encrypts files on the victim's device and demands payment for decryption.

Correct Answer*: True*

Explanation*: Ransomware is designed to lock access to files until a ransom is paid.*

5. **True or False:**

Data masking is used to display sensitive data in its original form but only to authorised users.

***Correct Answer**: False*

***Explanation**: Data masking obscures the data and does not show the original form, even to authorised users.*

6. **True or False:**

Public key encryption uses two keys—a public key for encryption and a private key for decryption.

***Correct Answer**: True*

***Explanation**: Public key encryption uses a pair of keys for secure communication.*

7. **True or False:**

Anti-virus software is designed to protect against all forms of cyber threats, including social engineering.

***Correct Answer**: False*

***Explanation**: Anti-virus software primarily protects against malware and cannot fully protect against social engineering.*

8. **True or False:**

Ethical hacking is conducted by cybersecurity professionals to identify weaknesses in systems before malicious hackers exploit them.

***Correct Answer**: True*

***Explanation**: Ethical hackers test systems for vulnerabilities to strengthen security.*

9. **True or False:**

The term "malware" includes viruses, worms, ransomware, and spyware.

***Correct Answer**: True*

***Explanation**: Malware encompasses various types of malicious software, including viruses, worms, and ransomware.*

10. **True or False:**

Cloud storage eliminates the need for regular data backup.

***Correct Answer**: False*

***Explanation**: Regular data backups are still necessary to protect against data loss or corruption.*

11. **True or False:**

Firewalls can be configured to block both incoming and outgoing traffic based on specific rules.

***Correct Answer**: True*

***Explanation**: Firewalls can filter and block traffic based on custom rules.*

12. **True or False:**

The principle of least privilege ensures that users have only the access necessary to perform their jobs.

***Correct Answer**: True*

***Explanation**: This principle minimises security risks by limiting user access.*

13. **True or False:**

Social engineering relies on manipulating human behaviour rather than exploiting technical vulnerabilities to gain unauthorised access.

***Correct Answer**: True*

***Explanation**: Social engineering attacks manipulate individuals into revealing confidential information or performing actions that compromise security, leveraging psychological tactics rather than technical methods.*

14. **True or False:**

Data encryption only protects data at rest, not data in transit.

***Correct Answer**: False*

***Explanation**: Encryption protects data both at rest and in transit.*

15. **True or False:**

An Intrusion Prevention System (IPS) can both detect and block potential threats in real-time.

***Correct Answer**: True*

***Explanation**: An IPS monitors network traffic and can actively block threats as they are detected.*

16. **True or False:**

Zero-day vulnerabilities are security flaws that have been publicly disclosed and patched.

***Correct Answer**: False*

***Explanation**: Zero-day vulnerabilities are unknown to the vendor and have not been patched.*

17. **True or False:**

Social engineering attacks exploit human behaviour rather than technical vulnerabilities.

***Correct Answer**: True*

***Explanation**: Social engineering manipulates human behaviour to gain unauthorised access.*

18. **True or False:**

The Fourth Industrial Revolution focuses mainly on advances in manufacturing processes.

***Correct Answer**: False*

***Explanation**: 4IR focuses on integrating digital technologies like AI, IoT, and data-driven solutions.*

19. **True or False:**

Public Wi-Fi networks are generally safe to use without additional security measures.

***Correct Answer**: False*

***Explanation**: Public Wi-Fi networks are often insecure and require additional precautions to use safely.*

20. **True or False:**

Antivirus software can detect and remove all forms of malware, including previously unknown threats.

***Correct Answer**: False*

***Explanation**: Antivirus software is effective but cannot guarantee detection and removal of all unknown threats.*

Question 3: Scenario-Based Questions (40 Marks)

Scenario 1: Email Phishing Detection (4 Marks)

You receive an email from a source/sender that appears to be your bank, requesting you to verify your account details by clicking a link.

1. What type of attack does this represent? (1 mark)

Answer: *Phishing*

Explanation: *Phishing attacks are attempts to trick individuals into revealing personal or sensitive information by impersonating legitimate sources.*

2. What are two indicators that could help you identify this type of cyber-attack attempt? (2 marks)

Answer: *Unusual or mismatched email sender address.*

Urgency in the message, such as "Act now" or "Verify your account immediately."

Mark Allocation: *1 mark per correct indicator.*

3. Describe one safe action you should take upon receiving this email. (1 mark)

Answer: *Do not click the link, and report the email to the IT department or delete it.*

Mark Allocation: *1 mark for a correct safe action.*

Scenario 2: Data Breach Response (4 Marks)

Your company experiences a data breach, potentially compromising customer information.

1. Identify two immediate actions your company should take. (2 marks)

Answer: *Notify affected parties and relevant authorities about the breach.*

Secure and isolate affected systems to prevent further data loss.

Mark Allocation: *1 mark per correct action.*

2. Explain one long-term measure your company can implement to prevent future breaches. (2 marks)

Answer: *Implement comprehensive encryption protocols to secure sensitive data and conduct regular security audits.*

Mark Allocation*: 2 marks for a correct long-term measure.*

Scenario 3: Network Security and Threat Detection (8 Marks)

Your company has installed network monitoring tools and has noticed unusual traffic from several IP addresses. You suspect it might be a security threat.

1. What initial action would you take to address this potential threat? (4 marks)

Answer*: Conduct a preliminary investigation by reviewing logs to confirm the source and nature of the unusual traffic and temporarily block suspicious IP addresses.*

Mark Allocation: *4 marks for a thorough explanation.*

2. ***Describe two ways a firewall or intrusion detection system can help manage this type of threat. (4 marks)***

Answer:

A firewall can block traffic from suspicious IPs based on configured rules.

An intrusion detection system (IDS) can monitor and alert on unusual activity for immediate response.

Mark Allocation: *2 marks per correct description.*

Scenario 4: Data Privacy Compliance (8 Marks)

An online service is planning to collect detailed personal information from users, including their location and browsing history.

1. ***What are two important legal considerations the company should review before collecting user data? (4 marks)***

Answer:

Ensure compliance with data protection laws such as GDPR or POPIA.

Review policies for data collection, ensuring minimal data is collected and only with user consent.

Mark Allocation*: 2 marks per correct consideration.*

2. ***Explain why gaining user consent is crucial when collecting sensitive data. (4 marks)***

Answer: *User consent ensures transparency and builds trust, showing that the company respects user privacy and adheres to legal standards.*

Mark Allocation: *4 marks for a complete explanation.*

Scenario 5: Security Measures for Personal Devices (6 Marks)

An employee is using their personal laptop for work, which includes handling sensitive company data.

1. ***List and describe two cybersecurity practices the employee should follow to protect company data on a personal device. (4 marks)***

Answer:

Use strong, unique passwords for accessing company applications.

Enable device encryption to protect stored data.

Mark Allocation: *2 marks per correct practice and description.*

2. ***Describe one risk of not following security practices on personal devices. (2 marks)***

Answer: *The risk of data breaches or unauthorised access, which could lead to sensitive company information being exposed or stolen.*

Mark Allocation: *2 marks for a complete risk explanation.*

Scenario 6: Basics of Logical Problem-Solving (5 Marks)

While Assessmentining security data, you need to calculate the impact of a recent system error that led to inaccurate reporting of user activities.

1. ***Explain how logical problem-solving can help identify the cause of this error. (2 marks)***

Answer: *Logical problem-solving allows for a systematic approach to analyse the data, identify inconsistencies, and trace the origin of errors in the reporting process.*

Mark Allocation: *2 marks for a thorough explanation.*

2. ***Provide an Assessmentple of a simple calculation or data verification step that could help confirm if the error is resolved. (3 marks)***

Answer: *Cross-referencing reported user activity counts with raw log data or recalculating totals to ensure reported data matches verified data.*

Mark Allocation: *3 marks for a clear and practical Assessmentple.*

Scenario 7: Design Thinking in Cybersecurity (5 Marks)

Your company wants to introduce a new feature for their app that will use AI to detect and respond to cyber threats.

1. ***List two steps in the design thinking process that would help develop this feature effectively. (2 marks)***

Answer: *Empathise: Understanding user needs and challenges.*

Prototype: Developing a working model of the AI feature for testing.

Mark Allocation: *1 mark per correct step.*

2. ***Explain why understanding user needs is critical in designing a cybersecurity feature. (3 marks)***

Answer: *Understanding user needs ensures that the feature is user-friendly and addresses specific security challenges, leading to better adoption and effectiveness.*

Mark Allocation: *3 marks for a complete explanation.*