INTERNATIONAL UNIVERSITY OF EAST AFRICA
'Learning to Succeed'

FACULTY OF SCIENCE AND TECHNOLOGY

END OF SEMESTER EXAMINATIONS -APRIL 2025

PROGRAMME: MIT

YEAR/SEM: I / II

COURSE CODE: MIT - 727

NAME: INFORMATION AND NETWORK SECURITY

DATE: 23/04/25

TIME: 2:00pm – 5:00pm

<u>INSTRUCTIONS TO CANDIDATES:</u>

- **THIS IS A PRACTICAL EXAM CONSISTING OF THREE QUESTIONS**
- **ATTEMPT ONLY ONE QUESTION**
- **DO NOT OPEN THIS EXAMINATION UNTIL YOU ARE TOLD TO DO SO**
- **ALL ROUGH WORK SHOULD BE IN YOUR ANSWER BOOKLET**
- **THE TIME ALLOWED FOR THIS EXAMINATION IS STRICTLY THREE HOURS**

- **ON THE FIRST PAGE OF YOUR ANSWER BOOKLET**

  - **WRITE YOUR REGISTRATION NUMBER PROPERLY**
  - **WRITE THE COURSE NAME AND COURSE CODE**
  - **WRITE EXAMINATION VENUE**
  - **DO NOT WRITE, DRAW OR SCRATCH ANYTHING ELSE ON THE FIRST PAGE**
  - **WRITING UNNECESSARY INFORMATION LIKE PHONE NUMBERS IN THE FIRST PAGE SHALL ANNUL YOUR EXAM**
  - **ANSWER BOOKLETS THAT DO NOT CARRY THE REQUIRED INFORMATION, OR THAT HAVE UNNECCESSAY WRITING IN THE FIRST PAGE SHALL NOT BE MARKED**

INTERNATIONAL UNIVERSITY OF EAST AFRICA
'Learning to Succeed'

FACULTY OF SCIENCE AND TECHNOLOGY

END OF SEMESTER EXAMINATIONS -APRIL 2025

QUESTION 1. (60 MARKS)

You are hired as a cybersecurity consultant to assess the security of a company's network infrastructure. The company suspects that its network may have vulnerabilities that could be exploited by attackers.

Task:

a) **Reconnaissance & Scanning: [20 Marks]**

- Conduct a network reconnaissance and scanning exercise using tools like **Nmap** or **Zenmap** to identify active hosts and open ports.
- Document the results and highlight potential vulnerabilities.

b) **Exploitation Attempt: [20 Marks]**

- Use ethical hacking tools such as **Metasploit** or **Hydra** to simulate an attack on one of the identified vulnerabilities (with justification).
- Explain your methodology and findings.

c) **Risk Analysis & Mitigation: [10 Marks]**

- Analyze the risks associated with the discovered vulnerabilities.
- Recommend security measures to mitigate these risks, including network hardening strategies.

d) **Report Writing: [10 Marks]**

- Prepare a **Penetration Testing Report** summarizing your approach, findings, and recommendations.
- Your report should follow a standard structure, including an **executive summary, methodology, results, risk assessment, and remediation plan**.

INTERNATIONAL UNIVERSITY OF EAST AFRICA
'Learning to Succeed'

FACULTY OF SCIENCE AND TECHNOLOGY

END OF SEMESTER EXAMINATIONS -APRIL 2025

QUESTION 2.

You have been assigned to conduct a **security assessment** of a wireless network in a small business environment. The business uses a **Wi-Fi network secured with WPA2 encryption**, but there are concerns that it may be vulnerable to attacks.

Task:

a) **Wireless Network Analysis [20 Marks]**

- Use tools such as **Acrylic Wi-Fi Analyzer, Kismet, or Wireshark** to scan and analyse the wireless network.
- Identify potential vulnerabilities, including weak encryption, rogue access points, or misconfigurations.
- Document the network's security posture based on your findings.

b) **Vulnerability Testing [20 Marks]**

- Attempt to test for vulnerabilities in the network using ethical penetration testing techniques such as **WPA handshake capture and decryption attempts** (e.g., using **Air crack-ng**).
- Explain the process and limitations of your test while ensuring ethical and legal compliance.

c) **Security Recommendations [10 Marks]**

- Based on your findings, propose **at least five security recommendations** to improve the wireless network's security.
- Justify each recommendation with supporting evidence.

d) **Report Writing [10 Marks]**

- Compile your findings into a **Wireless Security Audit Report**, structured as

QUESTION 3.

A **newly established financial firm** is setting up its **internal network infrastructure**. As the network security engineer, you have been tasked with designing and implementing a **secure and well-structured network** using **GNS3**. The network will serve different departments and ensure secure communication across all devices.

a) **Network Design & Topology (20 Marks)**

- Design a network consisting of: Two routers, One switch per router and Four computers per switch
- Ensure full connectivity between all devices.
- Use a suitable IP addressing scheme of your choice and document it.

b) **Routing & Connectivity (20 Marks)**

- Configure routing to **ensure full communication** between both networks.
- You are allowed to use **static routing, or Default routing**.
- Verify connectivity using **ping**.

c) **Security Implementation (10 Marks)**

- Implement at least three security measures, such as:
- Access Control Lists (ACLs) to restrict access.
- Router Security Hardening (e.g., disabling unnecessary services, setting strong passwords).

d) **Come up with excellent ddocumentation & a report (10 Marks)**