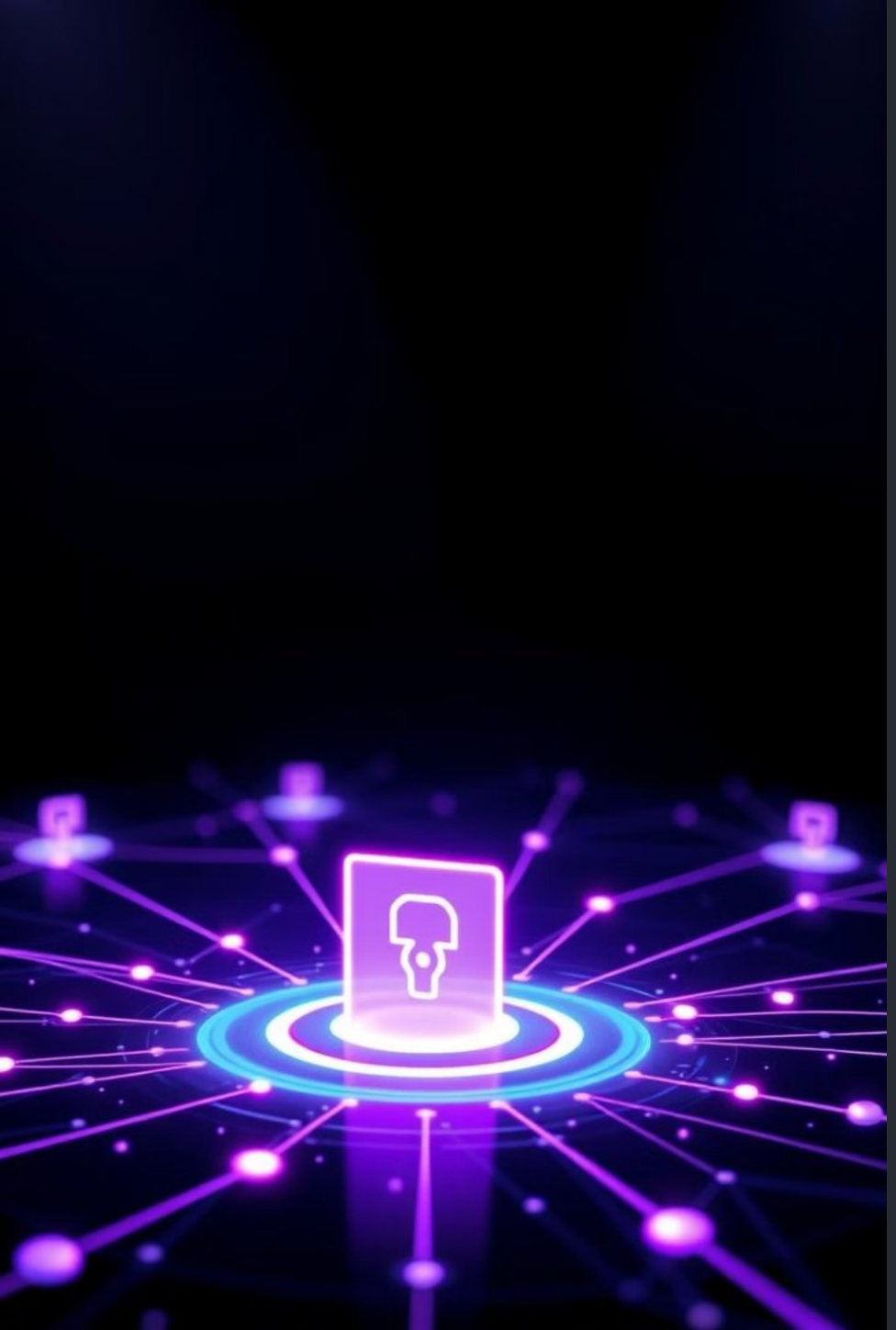
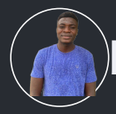


Network Intrusion Detection System (NIDS)

In today's interconnected world, the internet is essential for many activities, making home networks increasingly vulnerable to attacks. This project addresses the critical need for network security by developing a functional Network Intrusion Detection System (NIDS).

The NIDS monitors network traffic for signs of intrusion, such as DoS, DDoS attacks, port scanning, unauthorized access, and brute-force attempts. Designed to analyze traffic in real time, the system raises alerts upon detecting malicious activity, offering a practical tool for protecting organizational networks from potential threats.



by Maigari Timothy

What is an Intrusion Detection System (IDS)?

Defense Mechanism

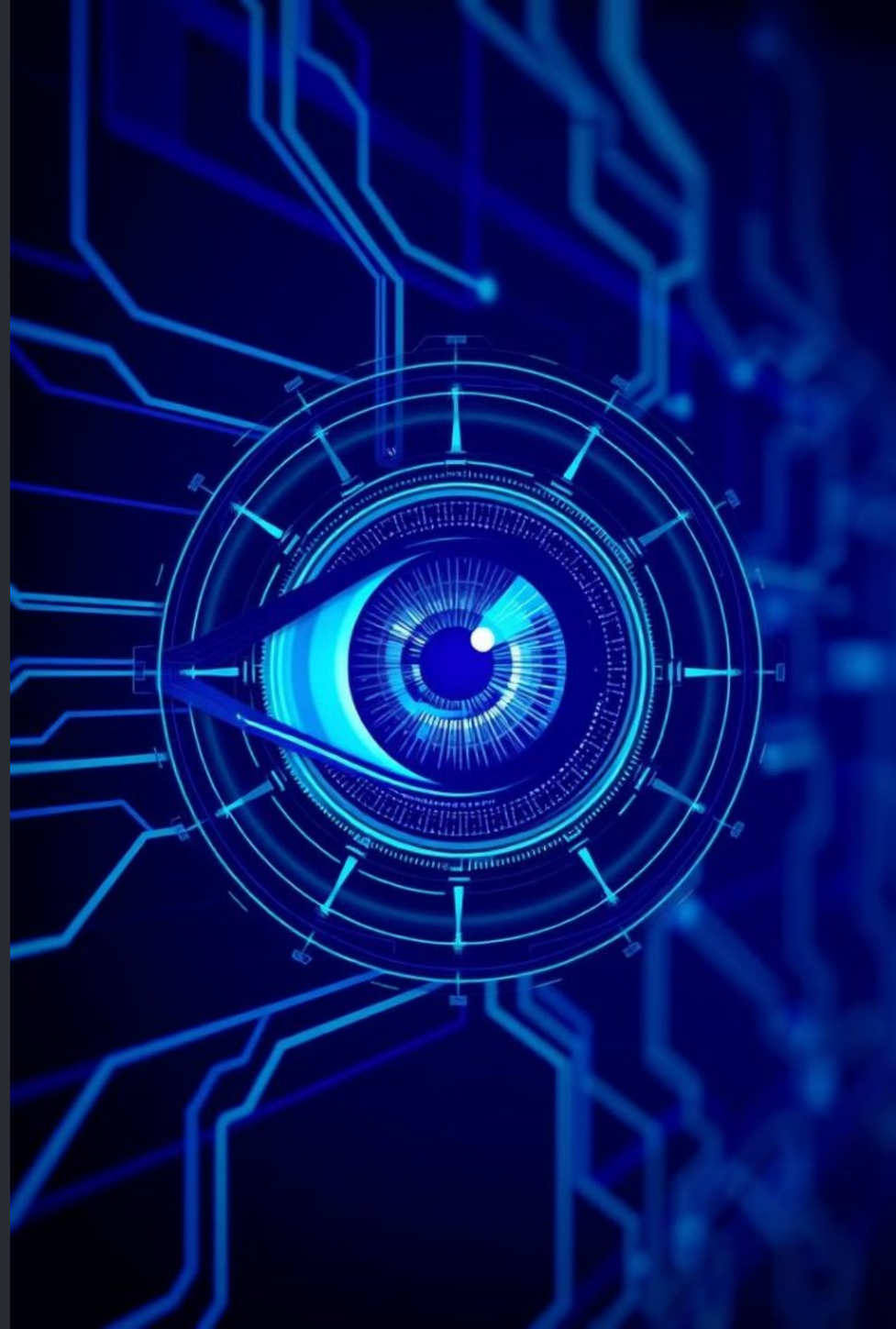
An Intrusion Detection System (IDS) is a defense mechanism designed to detect hostile activities within a network (Kazienko and Dorosz, 2003). Without proper detection and prevention, systems are vulnerable to compromise.

Key Benefit

A key benefit of IDS is its ability to monitor unusual or unscrupulous activities, providing critical insights into network security.

Intrusion Detection

As Amoroso (1999) defines, intrusion detection is “a process of identifying and responding to malicious activity targeted at computing and networking resources.”



Internal vs. External Intrusions

Internal Intrusions

Originate from within the network, often involving insider threats from trusted individuals. Internal attacks can be particularly damaging, as attackers leverage trust and local access.

External Intrusions

Come from outside the organization, typically over the internet. As the number of internal intrusions rises, organizations face increasing challenges in protecting sensitive data while adhering to regulatory compliance requirements.

The Growing Need for Network Security

Cyber Threat Complexity

As cyber threats become increasingly complex, the need for effective network security solutions has never been more critical. Attacks can cause significant damage, ranging from system downtime to data breaches.

Prevalent Threats

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, port scanning, and unauthorized access are among the most prevalent threats that organizations face.

Industry Reports

Industry reports highlight the growing frequency of these attacks, with over 10 million DDoS attacks reported globally in 2022 alone (Jacob, 2023).

Statistics on IDS Usage and Challenges

90%

Breaches Detected

Nearly 90% of interconnected networks that utilize IDS detected security breaches in the past year, despite multiple firewalls being in place (Magalhaes, 2003).

$455M

Financial Losses

The Computer Security Institute (4/7/02) reported that 80% of surveyed organizations suffered financial losses exceeding $455 million due to intrusions and malicious acts.

0.1%

Budget Allocation

Only 0.1% of companies allocate an adequate budget for IDS (Magalhaes, 2003).

Types of Intrusion Detection Systems

1

Network-Based

Analyzes network protocols on virtual private servers, remote access servers, and routers (Sturmer, 2013).

2

Wireless

Protects wireless networks by monitoring wireless traffic (Adams).

3

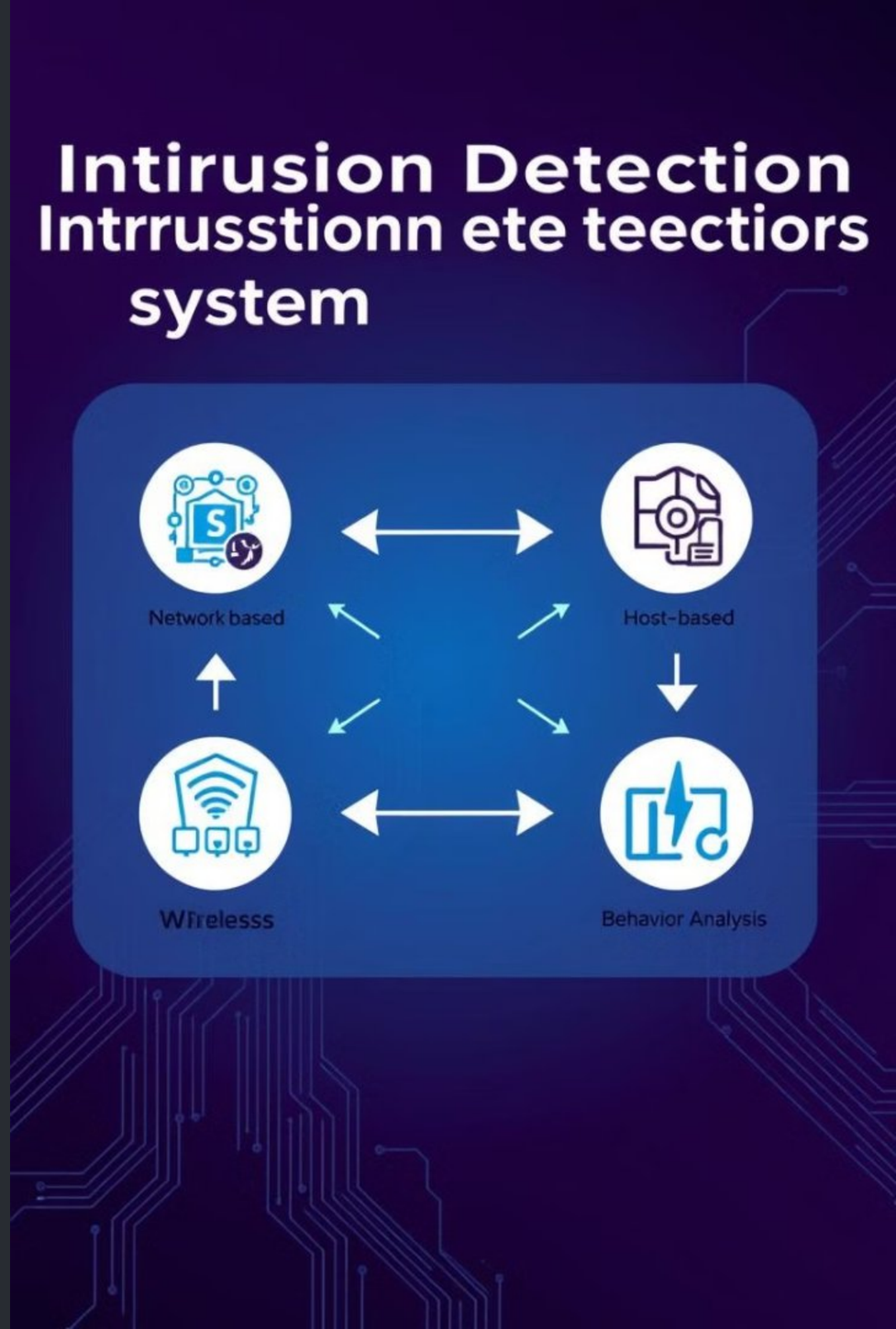
Host-Based

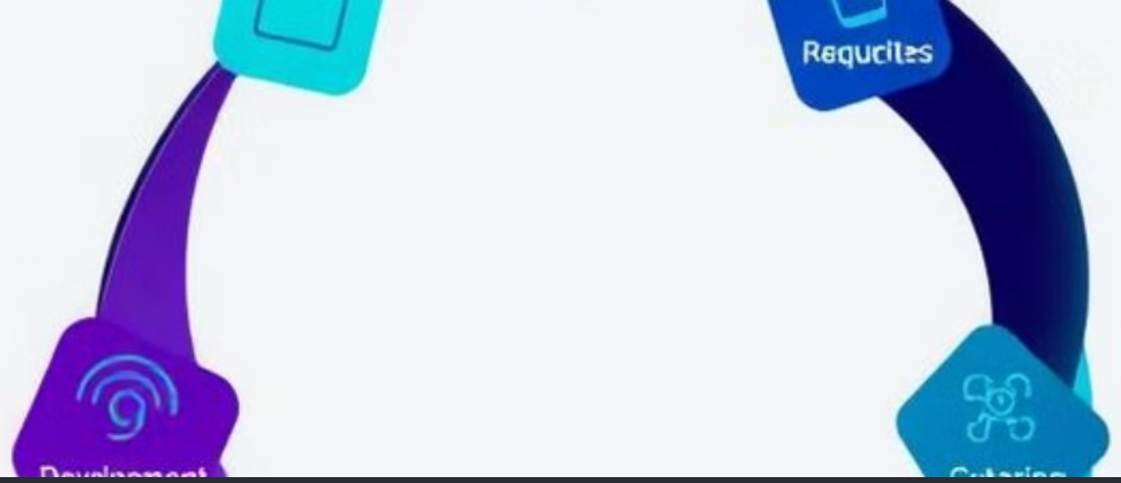
Operates on individual computers, monitoring changes in the file system and unusual network traffic (Sturmer).

4

Network Behavior Analysis

Detects irregularities in system behavior and monitors traffic flow (Seehorn).





Methodology: Iterative Development Model

1

Planning

To plan what is needed to be done to make sure this system can be implemented on time.

2

Analysis & Design

To determine the problem and solution.

3

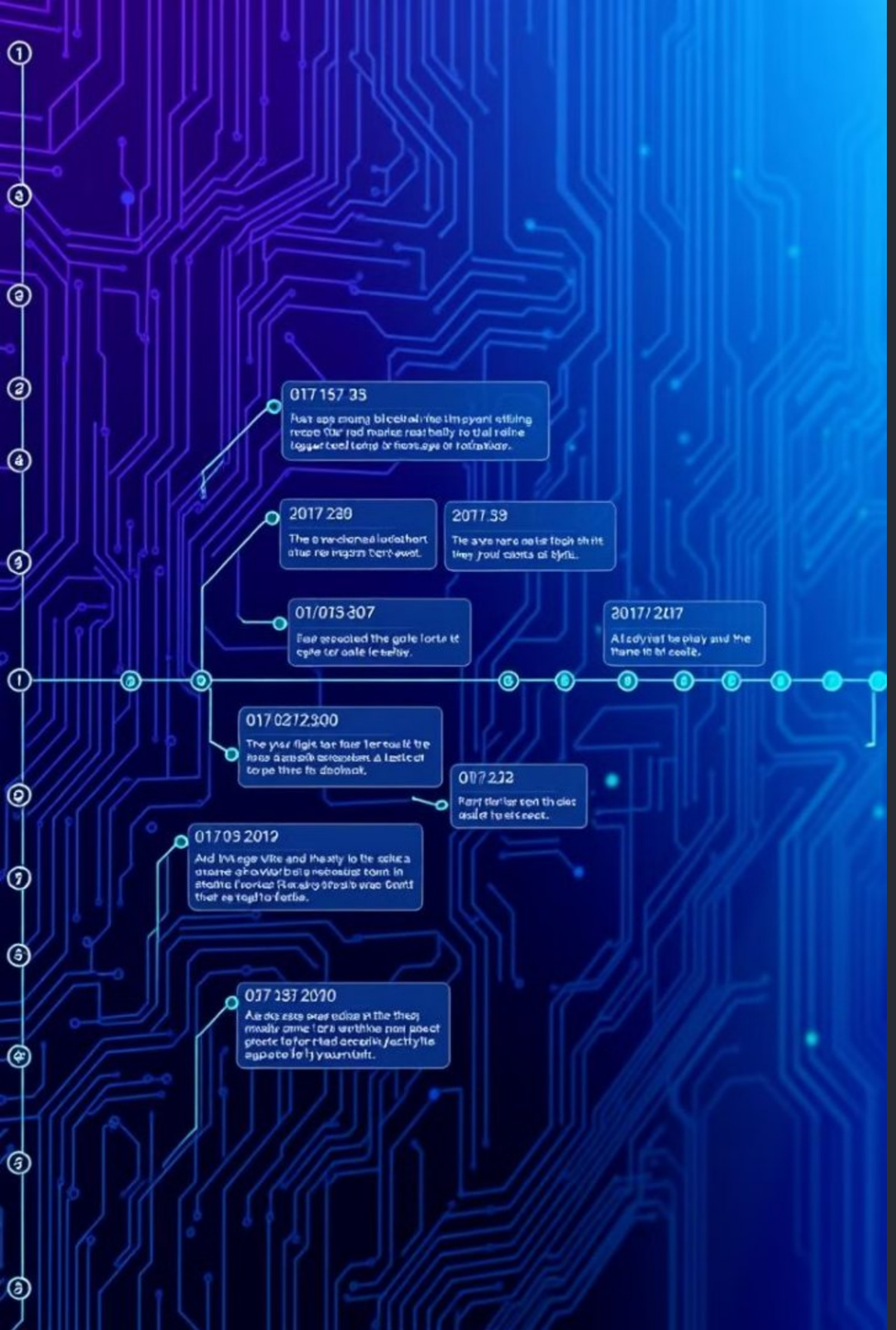
Implementation

To take the solution and implement it. Building the system.

4

Deployment

Install the system and provide user manual, training and maintenance.



Project Activities

1

Planning

Conducted during the early stages to determine the purpose of the system and the needs of the potential user.

2

Design

Of the system was done after the requirement has been identified by the developer based on the planning stage.

3

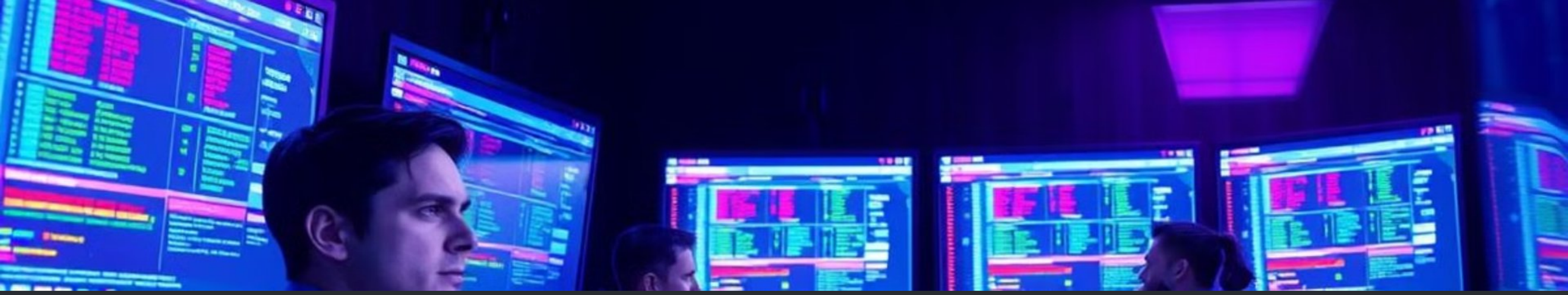
Construction

(implementation) of the system was made with code from the design stage.

4

Testing

Of the system was conducted in the testing stage to determine if the system meets the requirement gathers during the early part of the development.



Intrusion Detection Use Cases

1 **Anomaly Detection**

Abnormal network traffic triggers the alert system.

2 **Signature Recognition**

Attack patterns are matched against a database.

3 **Alert System**

Administrators are notified of detected intrusions.

Development Process & Tools

Python was the primary language. It ensured ease of development.

Scapy was used to capture packets. It allowed network packet analysis.

Bcrypt was used for security. User credentials were encrypted.

Challenges and Solutions

1

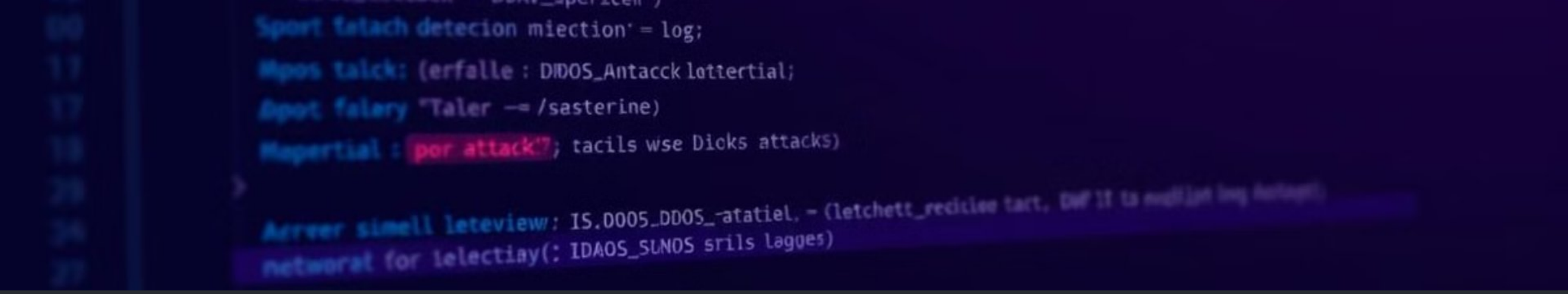
Real-Time Packet Sniffing

Managed using Python's multithreading. This prevents performance drops.

2

Multiple Attack Patterns

Detection algorithms were modularized. This ensured scalability.



IDS Detection Code Sample:

```
def detect\_dos\_ddos(packet):
    if packet.haslayer(IP):
        src\_ip = packet\[IP\].src
        packet\_count\[src\_ip\] += 1
        if packet\_count\[src\_ip\] > DOS\_THRESHOLD:
            alert = f"\[ALERT\] Possible DoS/DDoS attack from {src\_ip}"
            log\_alert(alert, critical=True)
```

Results: Intrusion Detection and Prevention

1 Successful Detection

The developed IDS successfully detected and logged intrusions, including DoS, DDoS, and port-scanning attacks.

2 Credential Security

The system also successfully secured login credentials and prevented unauthorized access after multiple failed attempts.

3 Real-Time Response

The system's real-time detection capabilities allowed for immediate response to intrusions, mitigating potential harm.

Key Findings and Analysis

Successful Detection

IDS detected intrusions effectively. It also logged DoS and port scans.

Objective Met

The prototype achieved its goals. It allowed immediate intrusion response.

Project Implications & Limitations

Cybersecurity Contribution

Lightweight solution for network intrusion detection.

Real-Time Importance

The project highlights real-time threat detection.

Restricted Environment

Testing was done in a limited network setup.

Future Work & Enhancements

1

Machine Learning

Incorporate ML for unknown threat detection.

2

Larger Network Deployment

Evaluate scalability and effectiveness in detail.

Summary and Final Thoughts

The NIDS project developed a system for threat detection. Python and open-source tools made it scalable. The project met its goals. It provided a prototype for future expansion.

This work deepened understanding of cybersecurity tools. It highlighted challenges in network protection. Future efforts will focus on machine learning.