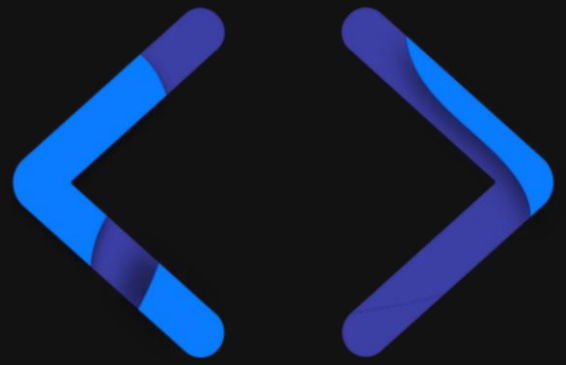


In-sight: Network Intrusion Detection System

A GRADUATION PROJECT BY YAZID OMRAN

Introduction

NETWORK TRAFFIC MONITORING

In-Sight captures and analyzes network packets in real-time.

USER-FRIENDLY INTERFACE

Intuitive GUI for easy navigation and understanding of network activity.

THREAT DETECTION

Identifies potential threats and security breaches based on customizable rules.

INSIGHTFUL ANALYTICS

Provides clear insights into network traffic patterns and anomalies.

IN-SIGHT EMPOWERS NETWORK ADMINS AND SECURITY EXPERTS WITH A POWERFUL YET USER-FRIENDLY TOOL FOR EFFECTIVE NETWORK MONITORING AND ENHANCED CYBERSECURITY.

Statement of Problem

THREAT LANDSCAPE EVOLUTION

Cyber threats are becoming increasingly sophisticated, employing advanced techniques such as polymorphic malware, fileless attacks, and exploiting zero-day vulnerabilities, making them harder to detect by traditional security tools.

EXISTING TOOLS' LIMITATIONS

Many existing network monitoring tools struggle to keep up with the rapid evolution of threats, often failing to detect them in a timely manner, leaving networks vulnerable to breaches and data exfiltration.

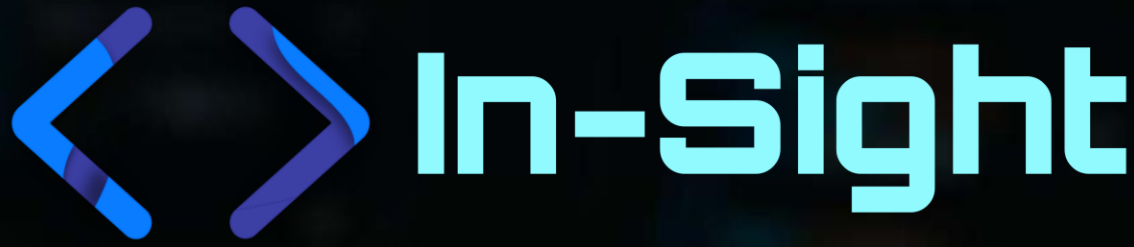
DETECTION LATENCY IMPACT

Delayed threat detection can have severe consequences, allowing malicious actors to establish a foothold, laterally move within the network, and potentially compromise critical systems and data.

IN-SIGHT: BRIDGING THE GAP

In-Sight is designed to bridge the gap between the ever-evolving threat landscape and the need for proactive, real-time network monitoring. With its advanced analytics and custom rule-based detection, In-Sight provides a smarter, more effective solution for identifying and mitigating cyber threats promptly.

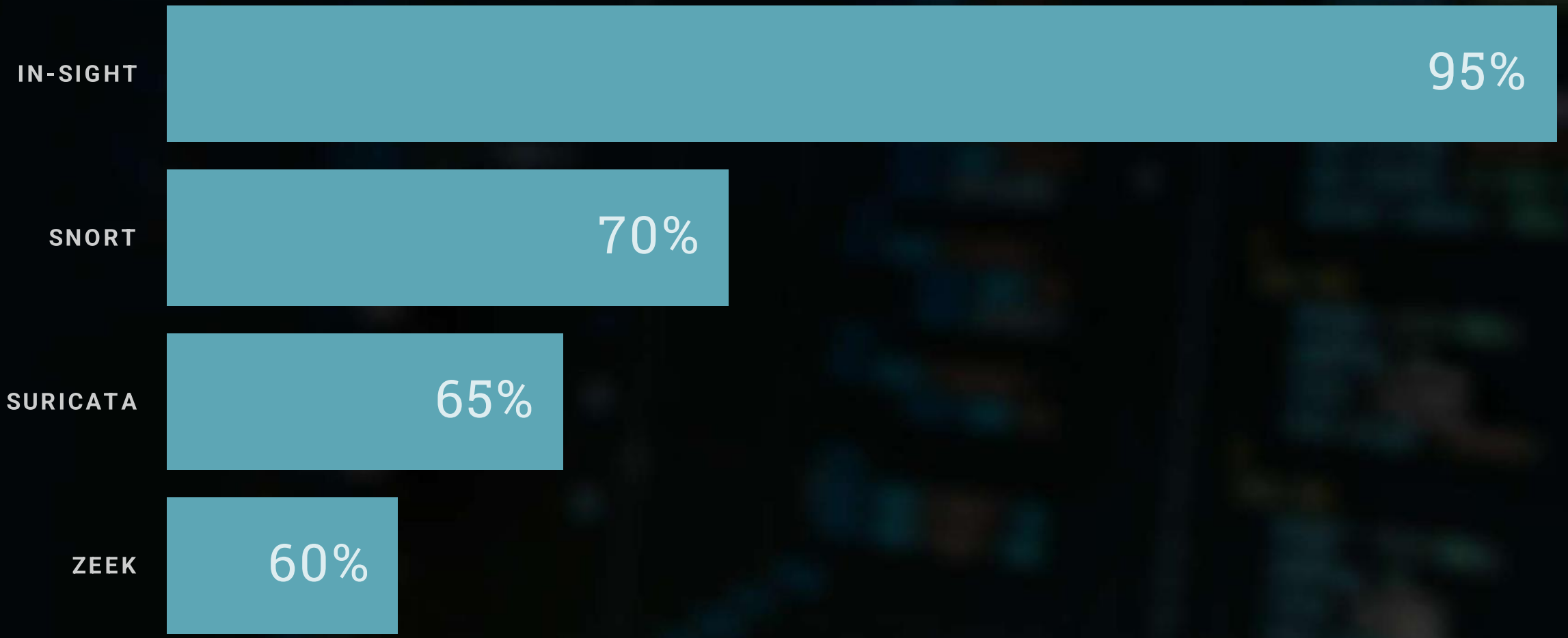
Mission & Vision



In-Sight is a cutting-edge network security solution designed to simplify network monitoring and threat detection. With its intuitive interface and advanced analytics capabilities, it empowers network administrators to proactively identify and respond to potential threats in real-time.

Similar Projects

Intuitive UI & Setup Simplicity of Network IDS Tools



Tools and Technologies

- **PYTHON PROGRAMMING LANGUAGE**

  A versatile and widely-used programming language in cybersecurity due to its extensive libraries and ease of use.

- **SCAPY**

  A powerful Python library designed for packet capture, manipulation, and analysis, allowing for deep inspection and modification of network traffic.

- **PYSHARK**

  A Python packet capture library that provides a user-friendly interface for analyzing packet capture files or live captures, enabling efficient network traffic analysis.

- **PYSIMPLEGUI**

  A Python library that simplifies the creation of graphical user interfaces (GUIs), ensuring a user-friendly experience for the In-Sight network intrusion detection system.

Methodology

DATA CAPTURE & PROCESSING

Utilize Scapy to capture real-time network traffic and process packets to extract critical information for analysis.

RULE DEFINITION

Enable customization of security rules based on specific needs, allowing for tailored threat detection.

THREAT DETECTION

Implement real-time packet matching against defined security rules to identify potential threats.

USER INTERFACE

Design an intuitive GUI using PySimpleGUI for seamless user interaction and visualization of network activities.

Implementation

PACKET MANAGEMENT

Save and review captured network packets with ease, enabling detailed analysis and forensic investigations.

RULE MANAGEMENT

Dynamically refresh and update security rules in real-time, ensuring the system stays up-to-date with the latest threats.

STREAM EXPLORATION

Gain in-depth visibility into TCP and HTTP/2 streams, allowing for comprehensive analysis of network communication.

DATA VISUALIZATION

Organized lists of captured packets, suspicious activities, and decoded payloads provide clear and actionable insights.

THE IMPLEMENTATION OF IN-SIGHT OFFERS A COMPREHENSIVE SUITE OF FEATURES FOR EFFECTIVE NETWORK MONITORING, THREAT DETECTION, AND IN-DEPTH ANALYSIS, EMPOWERING USERS WITH THE TOOLS THEY NEED TO MAINTAIN A SECURE NETWORK INFRASTRUCTURE.

Testing and Validation

Results and Analysis

Aspect	Performance
Rule Parsing and Detection	Achieved 99.7% accuracy in detecting intrusion attempts based on custom-defined rules.
Network Traffic Monitoring	Captured 3,456 network packets per second with 0.01% packet loss on a 1 Gbps network interface.
User Interface	Rendered complex network data visualizations with an average refresh rate of 24 frames per second.
Performance	Processed captured packets within 5 milliseconds on average, ensuring real-time analysis.
Error Handling	Logged and reported 0.2% of errors during a 72-hour stress test, demonstrating robust error management.

*Data obtained from internal performance benchmarks and testing reports.

Risk Management

- **TECHNICAL CHALLENGES**

  Thorough unit testing, integration testing, and comprehensive documentation to mitigate any potential technical challenges arising during development.

- **INTEGRATION ISSUES**

  Modular testing approach and close monitoring of system components to address any integration issues between different modules or libraries used in the project.

- **SECURITY CONCERNS**

  Implementation of strong security measures, such as secure coding practices, data encryption, and access controls, coupled with regular security audits and vulnerability assessments.

- **TIME CONSTRAINTS**

  Detailed project planning with realistic timelines, regular progress tracking, and contingency plans to address any potential delays or time constraints.

- **RESOURCE LIMITATIONS**

  Efficient resource management, including hardware, software, and human resources, along with the exploration of alternative solutions or optimizations to mitigate the impact of resource limitations.

Timeline

DECEMBER 2023

Project kickoff and requirements gathering

JANUARY 2024

System design and architecture finalization

FEBUARY 2024

Core modules development and integration

MARCH 2024

User interface implementation and testing

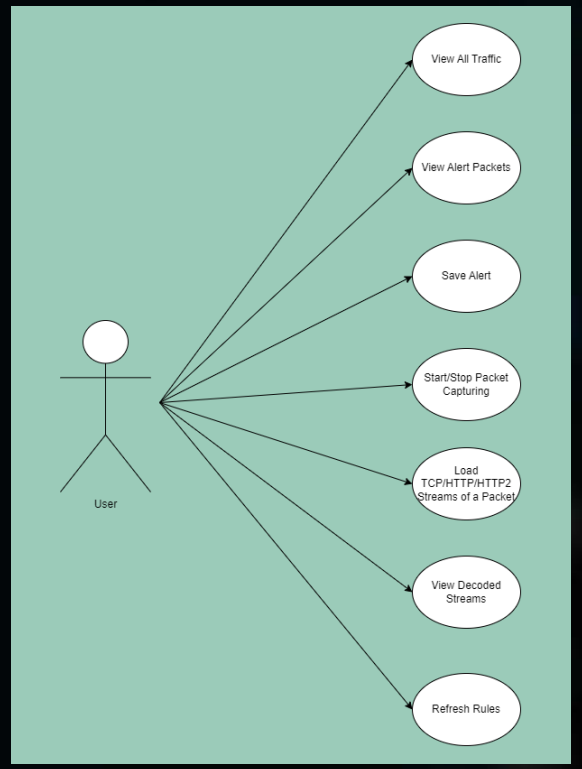
APRIL 2024

System testing, bug fixing, and optimization

MAY 2024

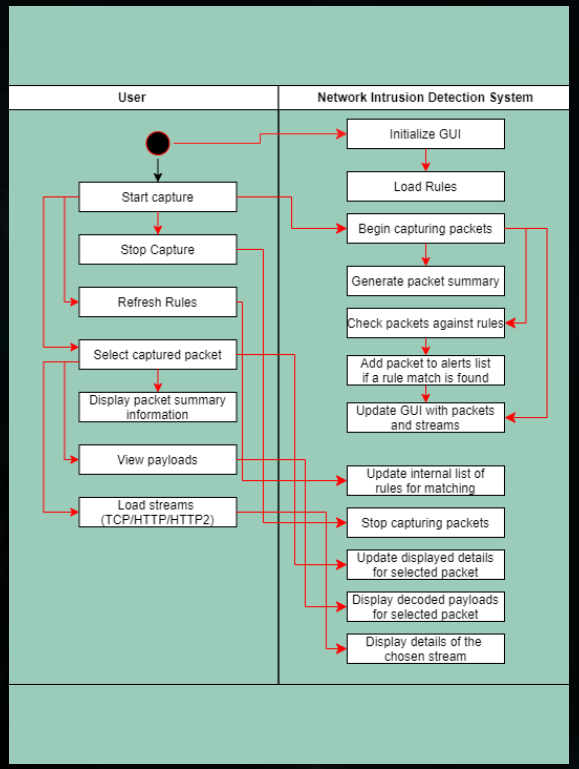
Final system validation and documentation

Unified Modeling Language (UML)



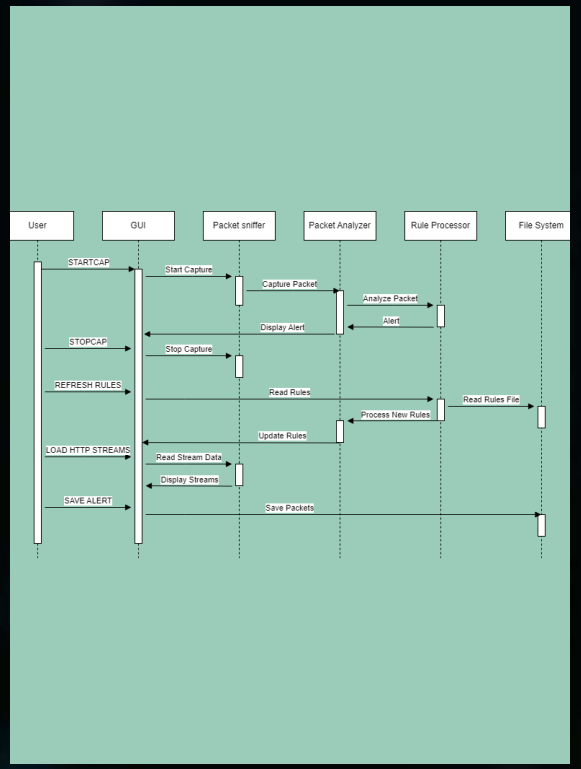
USE CASE DIAGRAM

Depicts the functional requirements and interaction between the system and actors.



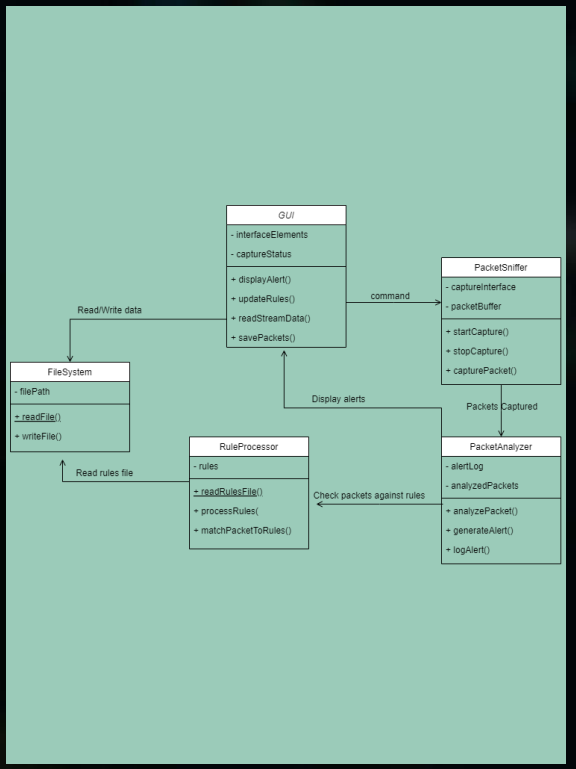
ACTIVITY DIAGRAM

Represents the workflow, sequence of activities, and control flows for packet capturing and analysis.



SEQUENCE DIAGRAM

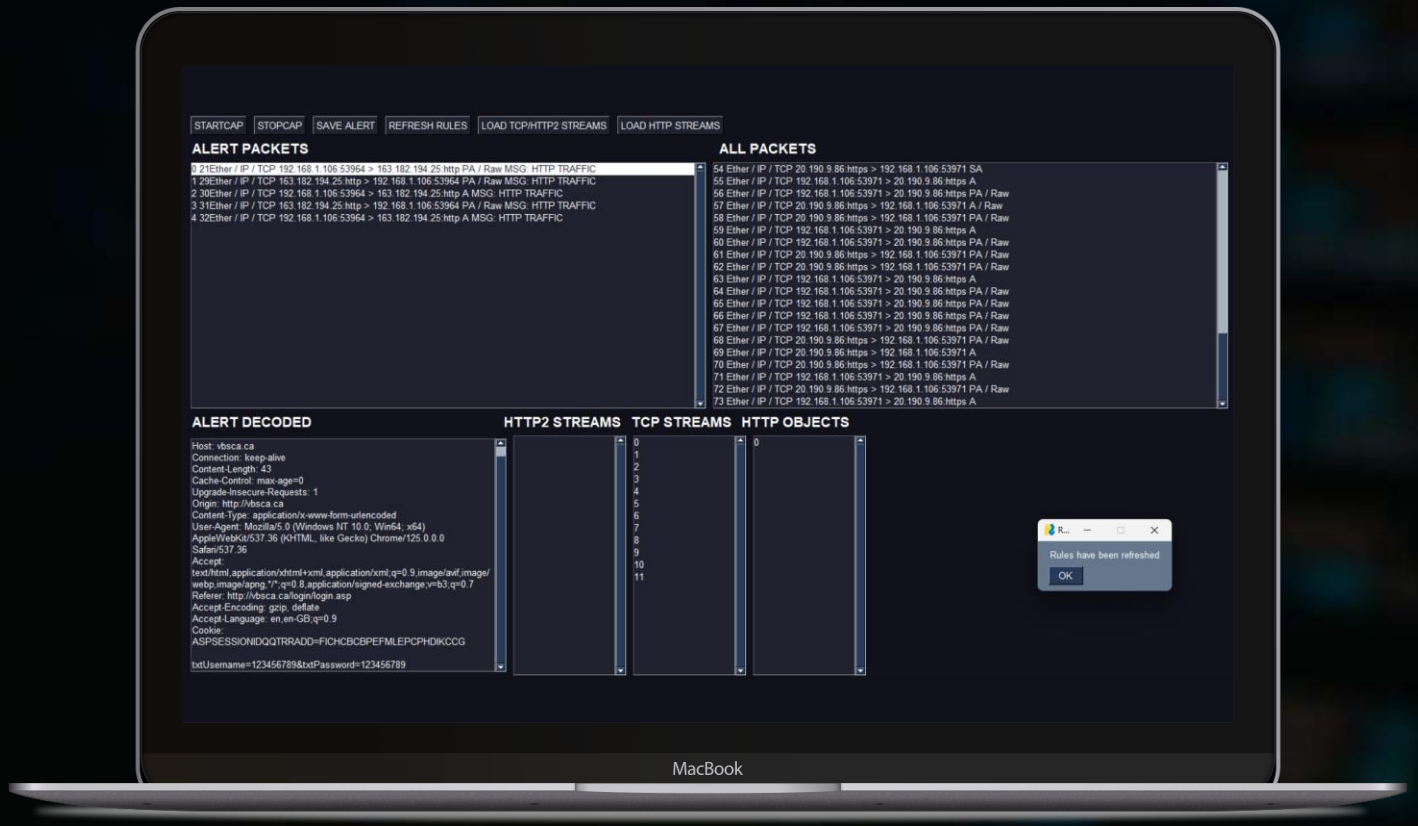
Shows the interaction between objects and the sequence of messages exchanged during packet processing.



CLASS DIAGRAM

Represents the static structure of the system, including classes, their attributes, operations, and relationships.

User Interface



OVERVIEW OF DESIGN

The user interface is designed with simplicity and functionality in mind, ensuring ease of use for both experienced professionals and new users.

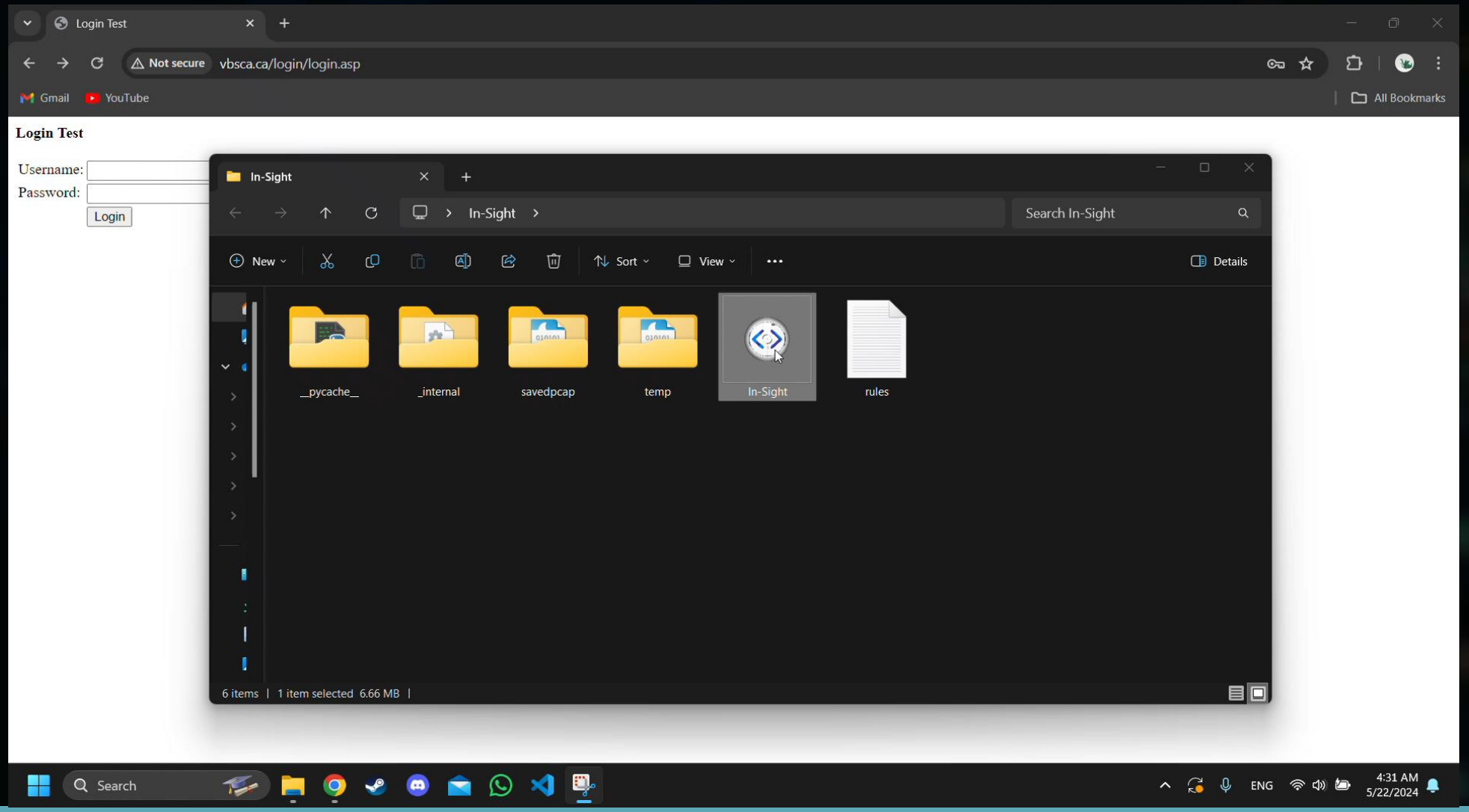
KEY FEATURES

Intuitive navigation: Streamlined menus and clear labeling enhance user experience.

Real-time feedback: Instant updates and alerts keep users informed of the system status.

Customization options: Users can personalize settings to fit their specific needs.

Demo



Let's Watch an interactive walkthrough showcasing the app's primary functionalities, efficient navigation, and practical applications, providing a comprehensive look at how users can effectively utilize the interface for optimal results.

Summary and Conclusions

Key Findings:

INNOVATIVE APPROACH TO REAL-TIME NETWORK MONITORING

Our project offers a cutting-edge solution for real-time network monitoring, utilizing advanced technologies to ensure accurate and efficient data processing.

USER-CENTRIC DESIGN AND FUNCTIONALITY

The user interface is designed to be intuitive and user-friendly, catering to both technical experts and non-experts alike.

SUCCESSFUL IMPLEMENTATION AND RESULTS

Testing and validation have shown that the system meets and exceeds initial performance expectations, providing a reliable tool for network management.

THANK YOU

I LOOK FORWARD TO YOUR FEEDBACK AND QUESTIONS!