# Abstract

This project proposes a hybrid Intrusion Detection System (IDS) that combines the robust packet inspection capabilities of Snort with the simplicity and automation potential of Python scripting, offering an accessible and efficient solution for network threat detection. Recognizing the complexity of configuring Snort on Windows, the project adopts a Linux-based architecture using WSL with Kali Linux for enhanced control and performance. Snort is compiled from source using CMake, incorporating dependencies like libdaq, libdnet, PCRE2, OpenSSL, and LuaJIT. Python manages automation tasks such as scan detection, real-time log analysis, and alert display through a streamlined interface, ensuring scalability and ease of integration into broader cybersecurity frameworks.

# Objectives

1. Develop a high-performance, real-time IDS using Snort as the core engine, combined with a Python-based interface for automation and usability.
2. Compile Snort from source using C++17 and configure it with essential dependencies such as libdaq (Packet I/O handling), libdnet (Low-level network tasks), LuaJIT (Scripting support), PCRE2 (Advanced pattern matching), OpenSSL (Secure communication), zlib (Compressed payloads), and hwloc (CPU and memory affinity management).
3. Create a Python-based GUI that enables one-click start/stop monitoring, real-time log visualization using tools like tail and subprocess, and custom rule creation and integration.
4. Implement a modular, scalable architecture where Snort handles packet-level detection and Python manages alert processing, UI, and configuration logic.
5. Enhance detection of scanning tools like Nmap, suspicious TCP flag patterns, and known vulnerabilities through a customized Snort ruleset.
6. Reduce operational complexity and false positives through rule tuning and automated log filtering.

# Methodology Overview

The vSecure IDS project employs a structured methodology to achieve efficient network threat detection. It begins with capturing network traffic via a designated interface using Snort, which analyzes packets against predefined rules to identify malicious activity. Alerts are generated and logged in real-time, simultaneously displayed through a Pythonbased Tkinter GUI for user visibility. The GUI enables seamless user interaction, allowing one-click start/stop monitoring and log visualization, while Python scripts automate log processing and rule management, ensuring a user-friendly and scalable system.

# vSecure IDS – Lightweight Python-based Intrusion Detection System Using Snort

## Project Overview

The vSecure IDS project addresses the challenge of detecting sophisticated network attacks with a lightweight, user-friendly Intrusion Detection System (IDS). Traditional IDS solutions often require complex setups and advanced expertise, limiting their accessibility for beginners or small-scale deployments. vSecure IDS overcomes this barrier by integrating the robust rule-based detection capabilities of Snort with a custom Python-based graphical user interface (GUI). This design enables users with basic Python knowledge to initiate real-time network traffic monitoring effortlessly, making the system ideal for educational purposes and lightweight environments. The system focuses on detecting known vulnerabilities and suspicious scanning behaviors, such as those generated by tools like Nmap, and provides real-time alerts through an intuitive interface.

## Methodology

The methodology of vSecure IDS is structured around the following core components:

1. **Traffic Monitoring**: Network traffic is captured from a designated network interface (e.g., eth0) using Snort, which processes incoming data from potential attackers, such as port scans or suspicious requests, in real time.
2. **Detection Engine**: The system employs Snort’s rule-based engine to analyze traffic against predefined patterns and signatures, leveraging both snort.rules (signature database) and snort.lua (Snort 3 modular detection) files for enhanced detection accuracy.
3. **Alert Generation**: Upon detecting suspicious or malicious traffic, Snort logs alerts to alert\_fast.txt and simultaneously relays them to the Python GUI for realtime visualization, ensuring immediate user awareness.
4. **User Interaction**: The Python GUI enables users to start or stop detection and view alert logs without relying on manual terminal commands, facilitated by seamless backend integration between Snort and Python scripts.

## System Architecture

The architecture of vSecure IDS is designed for efficiency and clarity:

* **Attacker**: Sends packets to the network interface.
* **Network Interface**: Captures incoming traffic and forwards it to the IDS.
* **Detection Engine**: Analyzes traffic using snort.lua and matches it against the snort.rules signature database.
* **Alert System**: Generates alerts displayed via the Python GUI and logged to alert\_fast.txt for further analysis.

## Technology Stack

The project leverages a carefully selected set of tools and technologies to ensure functionality and accessibility:

* **IDS Engine**: Snort (open-source intrusion detection system).
* **Programming Language**: Python.
* **GUI Framework**: Tkinter (Python’s standard GUI library).
* **Packet Capture**: Snort with libpcap.
* **Configuration Files**: snort.lua and snort.rules.
* **Log File Handling**: Python File I/O for processing alert\_fast.txt.
* **Additional Tools**:
  + Wireshark: For traffic analysis and debugging.
  + Nmap: Used to simulate attacker behavior for testing.
  + Linux Terminal: For configuring and managing Snort.

## Achievements

The vSecure IDS project was showcased at IBM Technovate-2025, hosted by Assam Down Town University. Among numerous innovative student projects, vSecure IDS stood out for its practical impact, simplicity, and effective detection capabilities. The project received recognition from IBM experts, including Mr. Aman Bakshi, and the creator was awarded IBM goodies and a branded bag as a token of appreciation.