**Cybersecurity Project: Simple IDS with Python**

In my second cybersecurity project, I developed a simple Intrusion Detection System (IDS) using Python. This IDS monitors network traffic in real-time and alerts on suspicious or malicious activity based on predefined rules inspired by techniques used in Snort.

**Key Features:**

* **Packet Sniffing**: Utilized Python's Scapy library for capturing and analyzing network packets.
* **Rule-Based Detection**: Implemented IDS rules to detect specific patterns in network traffic indicative of potential threats.
* **Alerting Mechanism**: Upon detection, the system triggers alerts providing details about the suspicious packet.
* **Flexibility**: Designed to be easily extendable with additional rules and adaptable to various network environments.

**Technologies Used:**

* Python, Scapy: for packet capture and manipulation.
* Regular Expressions (Regex): for defining and matching patterns in network traffic.

**Future Enhancements:**

* Integration with threat intelligence feeds for enhanced detection capabilities.
* GUI-based interface for real-time monitoring and configuration.

This project aims to provide a foundational understanding of IDS principles and practical implementation using Python, making it a valuable learning resource for cybersecurity enthusiasts and professionals alike.