**Classification & Domains:**

Cyber Security, Artificial Intelligence, Data Science, Machine Learning, Data Visualisation

**Project Aims:**

* This project aims to detect any intrusion in the system using machine learning techniques that will help users or organizations detect and respond to various types of system intrusions.
* It will also help reduce false positives, minimize the number of false alarms created by IDS, and help organizations focus on genuine threats.
* High accuracy and real-time detection with automated responses to the detected intrusions.

**Project Objectives:**

* Research on intrusion detection tools and how machine learning can help make it better.
* Research on AI tools that can help improve the detection process also provides real-time solutions.
* Visualizing the data for a better understanding of the anomaly and threats.
* Creating an artefact that can detect intrusion in real-time and provide quick action.
* Gathering resources and training the model using Machine Learning techniques.
* Training AI model for real-time solutions and quick action depending upon the attack.
* Deploying the artefact to check the accuracy of the model and look for any amendments if needed.
* Gathering the results and interpreting them.

**STAKEHOLDERS:**

* Academic Institutions
* End users
* Government Agencies
* Healthcare providers
* Telecommunication companies
* Cybersecurity service providers

**Tools and Technologies Required:**

* Python
* Machine Learning
* Scikit
* Artificial Intelligence
* Teamwork
* Scapy
* Dataset