GFT CREW Hackathon Submission Document

Team Information

- **Team Name**: GFT CREW
- **Team Leader**: Abdulazeez Jamiu
- **Team Members**:
    - Ayinde Mukthar
    - Anuoluwapo Oluwapo

Project Title

Automated Incident Response for National Security

Problem Statement

As the world becomes increasingly digital, national security is facing evolving threats, particularly in cyberspace. Traditional security methods are no longer sufficient to handle the speed and complexity of modern cyberattacks. Quick detection and response are essential to minimize damage, contain threats, and maintain public trust. Currently, slow response times in identifying, isolating, and mitigating cyber threats create increased vulnerability, system downtime, and potential breaches, which jeopardize national security.

Our Solution: AI-Powered Automated Incident Response System

Our solution leverages Artificial Intelligence (AI) to create a fully automated system that identifies, isolates, and responds to cyberattacks in real time. By utilizing machine learning algorithms and advanced data analysis, the system monitors network traffic, identifies anomalies, and automatically initiates a response to contain threats without human intervention.

Key Features

1. **Real-time Threat Detection**: AI algorithms analyze vast amounts of data, identifying potential security breaches or anomalies in real time.

Documentation for AI-Powered Intrusion Detection System (IDS)

Project Overview

This project focuses on building an AI-powered Intrusion Detection System (IDS) designed to enhance national security by predicting potential cyberattacks. Using the XGBoost model, we

classify both `attack labels` and `attack categories`, providing insights into the types and severity of threats. This system aids cybersecurity personnel by automating detection and categorization, supporting rapid and informed response actions.

Objectives

1. **Automated Detection**: Identify potential threats based on network traffic data and log files.
2. **Categorization of Threats**: Classify intrusions into categories to prioritize and streamline responses.
3. **Real-Time Analysis**: Enable real-time detection to prevent or minimize damage from intrusions.

Datasets Used

Three prominent datasets were used to ensure robustness and a comprehensive model that captures various types of intrusions:

1. **UNSW-NB15**: Contains modern network attack data, providing a diverse set of attacks and benign network traffic. This dataset is critical for identifying and classifying malicious behavior with features like `src_bytes`, `dst_bytes`, and `protocol_type`.
2. **CICIDS2017**: Emulates real-world traffic, offering a variety of normal and abnormal behaviors that help the model recognize attack patterns in real environments. Key attributes such as `service` and `duration` are essential in detecting and distinguishing between different attack types.
3. **KDD Cup 99**: A benchmark dataset for intrusion detection research, which offers insights into widely studied and legacy attack types, helping with model generalization. Features such as `duration` and `protocol_type` contribute to detecting both established and emerging threats.

Data Preprocessing and Feature Engineering

1. **Data Cleaning**: Removed duplicate records and handled missing values, standardizing formats for consistency across datasets.
2. **Feature Engineering**:
    - Extracted network traffic features like `IP addresses`, `port numbers`, and `protocol type`.
    - Incorporated statistical features such as `mean` and `variance` for traffic patterns.
    - Used temporal patterns, capturing variations over time to improve detection accuracy.
3. **Feature Scaling**: Applied scalers (StandardScaler, MinMaxScaler, RobustScaler, MaxAbsScaler) to normalize data values, which helped improve model stability and convergence.

Model Selection and Training

The XGBoost model was chosen for its ability to handle large datasets, fast computation, and robustness with imbalanced data—key attributes for an intrusion detection task. The model predicts:

- **Attack Label**: Identifies if traffic is benign or malicious.
- **Attack Category**: Classifies the type of attack, such as DoS, probing, or U2R.

The model was trained on labeled data from all three datasets. Hyperparameter tuning was performed to optimize parameters like learning rate, max depth, and the number of estimators for enhanced performance.

Model Deployment and Real-Time Processing

For real-time intrusion detection, we integrated the model with **Apache Kafka** for streaming data and **Spark Streaming** for processing. This setup allows the IDS to continuously monitor traffic and immediately alert security teams to anomalies.

Model Evaluation

Evaluation metrics used include:

- **Precision, Recall, and F1-score**: To assess the model's accuracy in identifying benign and malicious traffic.
- **ROC-AUC**: To measure the model's effectiveness in distinguishing between attack types.

How This Model Supports National Security

1. **Rapid Threat Identification**: The system quickly flags unusual activities, allowing security personnel to respond promptly and reduce potential damage.
2. **Automated Response**: Integrated with incident response protocols, the IDS can automatically isolate affected systems and initiate containment, minimizing the spread of attacks.
3. **Enhanced Decision-Making**: By categorizing attack type and severity, security teams can prioritize responses, focusing on critical threats first.
4. **Scalability**: The model can be scaled to monitor various networks, from national databases to critical infrastructure, making it adaptable for diverse national security needs.

Conclusion

This AI-powered IDS provides a comprehensive solution for addressing cybersecurity threats, facilitating real-time detection and response to intrusions. Leveraging datasets like UNSW-NB15, CICIDS2017, and KDD Cup 99, the model is equipped to handle both legacy and modern threats, making it a significant asset for national security.