NETWORK INTRUSION DETECTION IN DNS TRAFFIC

Presented by

Raja Muppalla

STATEMENT OF PROJECT OBJECTIVE

Intrusion detection systems are used to detect abnormalities in order to apprehend hackers before they cause serious network harm.

The DNS is a naming database that locates and converts internet domain names to IP addresses.

Network intrusions frequently entail the theft of important network resources and virtually always compromise network and data security.

Generally, the unauthorized action on a digital network is known as a network intrusion.

HOW THE DNS WORKS

The Basic steps of a DNS resolution is

The user enters a web address or domain name into a browser.

Browser sends a message, called a recursive DNS query, to the network to find out which IP or network address the domain corresponds to.

Query goes to a recursive DNS server, which is also called a recursive resolver, and is usually managed by the internet service provider (ISP).

The three server types work together and continue redirecting until they retrieve a DNS record that contains the queried IP address.

(1) sends the information to the recursive DNS server,

(2) The webpage the user is looking for loads.

(3) DNS root name servers and TLD servers primarily redirect queries and rarely provide the resolution themselves.

The entire process querying the various servers takes a fraction of a second and is usually imperceptible to the user.

APPROACH

TOOLS USED :

JUPYTER NOTEBOOK (GOOGLE COLAB)

TECHNIQUES :

1. FEATURE SELECTION
2. DATA ANALYSIS
3. EVALUATION METRICS

MODELS USED

- k-nearest neighbors (KNN).
- Decision Tree
- Logistic Regression
- Naive Bayes Classifier

DATASET

Downloaded the Dataset from Kaggle.

Dataset link : https://www.kaggle.com/sampadab17/network-intrusion-detection

The dataset contains a wide range of intrusions that were simulated in a military network. By mimicking a typical US Air Force LAN, it established an environment in which raw TCP/IP dump data for a network could be acquired.

For each TCP/IP connection, 41 quantitative and qualitative features are obtained from normal and attack data (3 qualitative and 38 quantitative features) .

The class variables are two categories.
(1) Normal
(2) Anomalous

DELIVERABLES

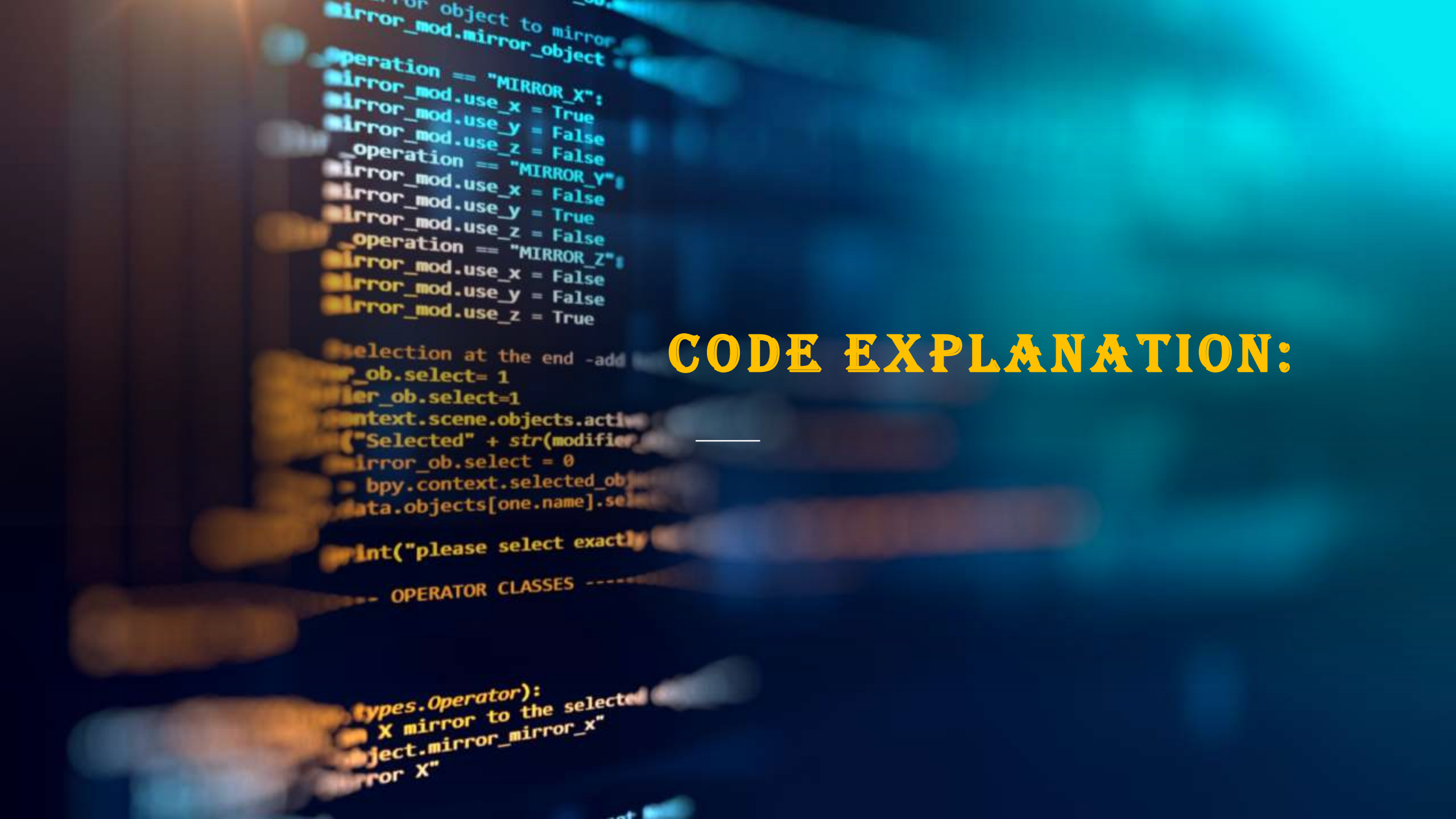
- Documentation report (README.md)
- Developed programming Algorithms (.ipynb files)
- GitHub repository link
- YouTube video
- PPT slides

EVALUATION METHODOLOGY

Normal and Anomaly are two classes used in detecting techniques to measure accuracy, which aids in the calculation of True Positive Rate (TPR), False Positive Rate (FPR), Precision, and Accuracy scores.

The success of the project is determined by the successful implementation.

The methodology for evaluating network intrusion detection algorithms comprises of dataset usage guidelines, assessment metrics to offer, and the evaluation of anomaly or normal networks.


CODE EXPLANATION:

YouTube Video Link :

https://youtu.be/XOES5QhCD-g

THANK YOU