Anomaly Detection in Communication Networks

PROJECT TEAM MEMBERS: GOWRI V S , SUMEDHA J S, SRILIKHITA BALLA , MUKESH VANIKA

SUPERVISOR NAME: DR. ABHAY GANDHI
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
VISVESVARAYA NATIONAL INSTITUTE OF TECHNOLOGY, NAGPUR-INDIA

INTRODUCTION

Types of intrusion detection mechanisms include Misuse detection(signature-based) and anomaly detection(behaviour-based)

Misuse based methods are highly effective to detect known attacks. Anomaly detection methods use the normal system activity to detect anomalies that deviate from these.

Types of anomalies include : Point anomalies, contextual anomalies, collective anomalies

Different types of attacks include - DoS attack (flooding/crashing services), DDoS attack etc.

LITERATURE SURVEY

- Types of intrusions and attacks
  - DoS and DDoS- A DoS is a type of cyber attack which is a tactic used to flood and overload a system using a single or multiple attackers.
  - Man In Middle - attack by a person who is a middle man in the conversation between user and an application. The goal of attack is to steal personal information.
  - SQL Injection - Uses malicious SQL code to manipulate the backend databases and access private information.
  - Unauthorized Access - Accesses an organization's data without receiving permission.
  - Privilege Escalation
  - Insider Threats

TIMELINE

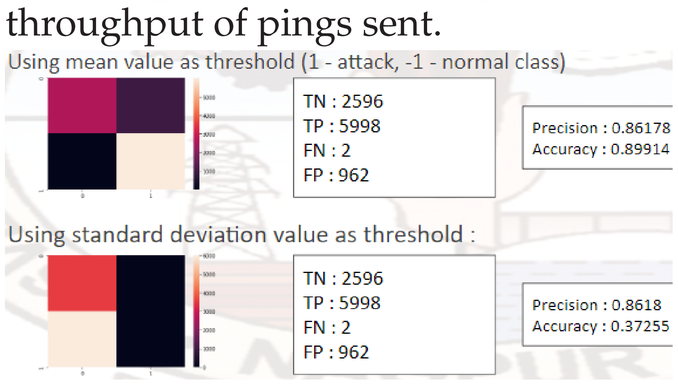
Proposed Model **Figure 3:** Flow process of the proposed method

METHODOLOGY

1. Set up a virtual Windows machine using Oracle VM VirtualBox.
2. Researched into various intrusion simulators like DDoS Simulator, Metasploit, BSQL Hacker.
3. Simulated few of these attacks and collected data using the packet sniffer Smartsniff.
4. DoS and DDoS simulation
   - DoS attack was simulated using Oracle Virtual box by sending ping floods from the system to the virtual machine and then tracing the packets using Smartsniff.
   - DDoS attack was simulated by sending ping floods to one ip address from 4 different ip addresses at the same time
5. The packet sniffer data for idle system, normal system in working condition and system under attack was traced and analysed.
6. Cleaned the Data and Preprocessed it.
7. Applied Thresholding Algorithm and Entropy Based Algorithm and compared the results of the both.

RESULTS

Detecting anomaly using threshold of throughput of pings sent.



Mean value as threshold gives more accurate and precise results.

Detecting anomaly using entropy change in throughput

CONCLUSION

1. The numerous variety of attacks make it a necessity to have an intelligent learning based algorithm to detect the attacks
2. Firewalls and other current IDS use statistical methods to detect anomalies and intrusions
3. Need to find the best parameters/features to train the model on to get best accuracy

REFERENCES

1. A. L. G. Rios, Z. Li, K. Bekshentayeva and L. Trajković, "Detection of Denial of Service Attacks in Communication Networks," 2020 IEEE International Symposium on Circuits and Systems (ISCAS), 2020, pp. 1-5, doi: 10.1109/ISCAS45731.2020.9180445.
2. Ismail et al., "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," in IEEE Access, vol. 10, pp. 21443-21454, 2022, doi: 10.1109/ACCESS.2022.3152577.
3. Bonte, Pieter Hautte, Sander Lejon, Annelies Ledoux, Veerle De Turck, Filip Hoecke, Sofie Ongenae, Femke. (2020). Unsupervised Anomaly Detection for Communication Networks: An Autoencoder Approach. 10.1007/978-3-030-66770-212.
4. Kumari, Kimmi, and M. Mrunalini. "Detecting Denial of Service Attacks Using Machine Learning Algorithms - Journal of Big Data." SpringerOpen, 28 Apr. 2022,