Intrusion Detection System (IDS) (both Standard Approach and Machine Learning)

Vladyslav Furda

July 6, 2024

Abstract

This specification presents the design and future implementation of an Intrusion Detection System (IDS) that combines traditional detecting methods with machine learning techniques to effectively detect anomalous network packets. The IDS aims to enhance network security by identifying potential threats and unusual patterns that may indicate malicious activities such as pinging, mapping or ddosing. This documentation provides an overview of future system's features, possible libraries used, and the methodologies that will be applied in developing of this IDS.

1 Introduction

Intrusion Detection Systems (IDS) are critical components in securing network environments. Traditional IDS methods rely on predefined rules and signatures to detect known threats. However, these methods can be limited in identifying new or evolving attacks, moreover, they can be fooled. To address this limitation, my IDS integrates machine learning techniques to detect anomalies in network traffic, providing a more robust and adaptive security solution, that can generalize similarities and ehance performance.

2 System Overview

The IDS is designed to monitor network traffic in real-time (or near real-time), analyze packet data, and identify potential security threats. The system will incorporate both signature-based detection and anomaly-based detection using machine learning.

3 Features

- **Real-time Monitoring:** Continuously monitors network traffic for suspicious activities.

- **Signature-based Detection:** Utilizes predefined rules and signatures to detect known threats.
- **Anomaly-based Detection:** Employs machine learning models to identify unusual patterns and anomalies in network traffic.
- **Alert System:** Generates alerts and logs for detected intrusions and anomalies.
- **User Interface:** Provides a command line interface (CLI) for configuring the IDS and viewing alerts and logs.

4 Technologies and Libraries

The IDS system is implemented in C#. The following libraries and frameworks will be utilized:

- **SharpPcap:** A packet capture library for .NET, providing capabilities to capture and analyze network packets.
- **PacketDotNet:** A .NET library for decoding and analyzing network packets captured using SharpPcap.
- **ML.NET:** A machine learning framework for .NET, used for building and training machine learning models for anomaly detection.
- **Spectre.Console:** For developing a cute graphical user interface.
- **NLog:** A logging library for .NET, used for logging alerts and system events.

5 Methodology

The IDS employs a hybrid approach to detect intrusions:

5.1 Signature-based Detection

- Predefined signatures and rules are created based on known threats and attack patterns.
- Incoming network packets are compared against these signatures to detect potential threats.

5.2 Anomaly-based Detection

- Network traffic data is collected and preprocessed.
- Machine learning models are trained using historical network traffic data to learn normal behavior. Dataset will be taken from Kaggle.
- The trained models are deployed to identify anomalies in traffic.

6 Implementation Details

6.1 Packet Capture and Analysis

- SharpPcap is used to capture live network packets.
- PacketDotNet decodes the captured packets for analysis.

6.2 Machine Learning Model

- ML.NET or TensorFlow.NET/Keras.NET is used to build and train the machine learning model.
- Various algorithms, such as Random Forest, Decision Trees, and Neural Networks, are explored for anomaly detection.

6.3 Alert Generation

- The system generates alerts for any detected threats or anomalies.
- Alerts are logged using NLog (maybe) and displayed in the user interface.

7 Work to be done

- Get familiar with dataset.
- Train model and test it.
- Get information about signature based detection.
- Implement first versions of the IDS, combining two approaches.
- Enhance CLI for better usability.
- Enhance the machine learning model with more training data and feature engineering.
- Integrate the IDS with other security tools and systems for comprehensive security management.