Shri Ramdeobaba College of Engineering & Management, Nagpur
Department of Computer Science & Engineering(Cyber Security)
Session 2022-2023

SEMINAR ON

B.R.I.C.S Firewall - Behavioral Response and Intrusion Classification System

Guided By:
Dr. Rashmi Welekar

Presented By:
Group No. 11
Group Members :
Eeshan Wadodkar
Kalash Jaiswal
Ayush Kamde
Vedank Naidu
Vedant Madhwe

B.R.I.C.S

BEHAVIOURAL RESPONSE AND INTRUSION CLASSIFICATION SYSTEM

TABLE OF CONTENTS

Introduction

Firewalls

Firewalls are critical components of network security that act as barriers between a trusted internal network and untrusted external networks, such as the internet. They monitor and control incoming and outgoing network traffic based on predetermined security rules. Here's some more information about firewalls:

Introduction

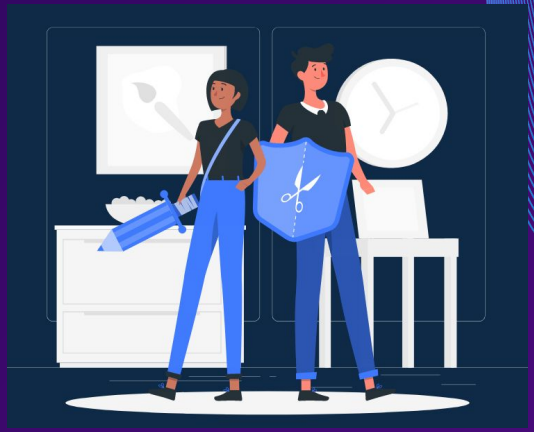
Types Firewalls

- Packet filtering firewalls
- Stateless firewalls
- Stateful inspection firewalls

Motivation

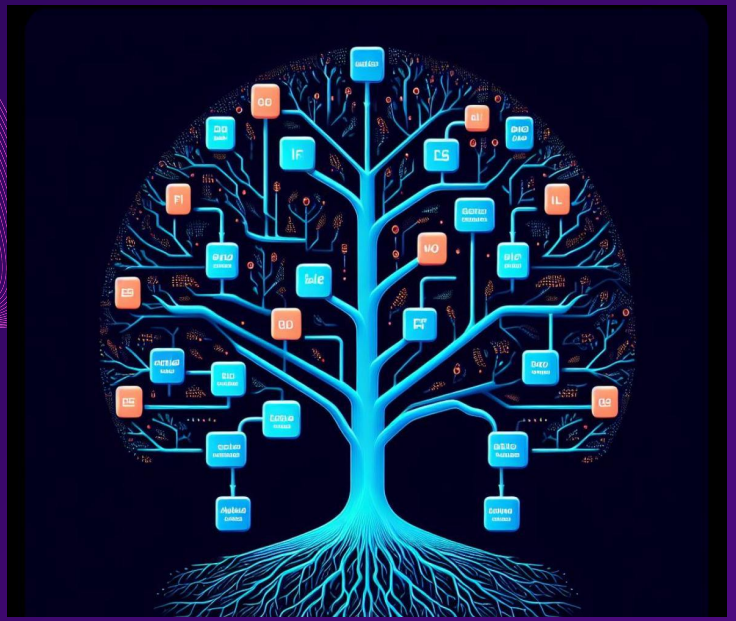
The motivation behind developing an adaptive firewall system stems from the shortcomings of traditional firewalls that require constant manual updates. In a rapidly evolving threat landscape, relying solely on manual intervention to update firewall rules is impractical and increases the risk of security breaches.

By implementing a self-correcting firewall system capable of automatically detecting and responding to threats, organizations can improve their overall security posture and reduce the likelihood of successful cyber attacks.



Introduction

THUS . . . . THE ADAPTIVE FIREWALL



Mycin - First Expert System

Mycin expert system was a pioneering project in the field of artificial intelligence and medical diagnosis.

Purpose: Mycin aimed to demonstrate the capabilities of artificial intelligence in medical diagnosis and treatment recommendation.

Rule-Based System: Mycin was built as a rule-based expert system. It encoded a large knowledge base of rules based on expert knowledge in the domain of infectious diseases, antibiotics, and patient symptoms.

Limitations: lacked the ability to explain its reasoning to users, which limited its acceptance in clinical practice.

Objectives

- The primary goal of the mini project is to create an adaptive firewall system.
- This system will incorporate an expert system utilizing if-else statements for intrusion detection and rule adaptation.
- Leveraging machine learning techniques, the firewall will have the ability to dynamically adjust its rules and regulations.
- The dynamic updates will be made in response to evolving threats.
- The ultimate aim is to enhance network security.
- This adaptive approach aims to reduce the necessity for manual intervention in maintaining firewall rules.

Proposed Plan Of Work

Integrating AI in pfsense firewall can be achieved through the following steps:

1. Choose an AI platform

2. Develop an AI model

3. Containerize the AI model: This will allow for easy deployment and management of the model.

4. Integrate the AI model with pfsense: Integrate the AI model with pfsense by creating a custom package or module, or package AI model into Docker container and run it alongside or by developing a plugin that can interface with the AI model.

5. Deploy the AI-enabled pfsense firewall: Deploy the AI-enabled pfsense firewall in your network environment or you could use a VM.

Proposed Plan Of Work

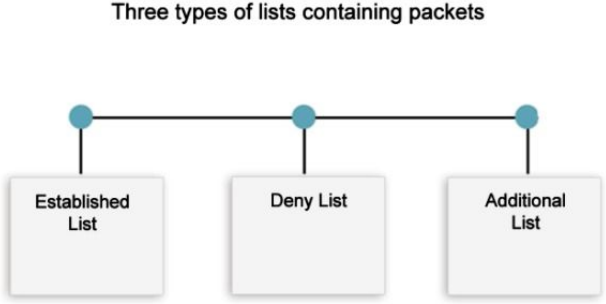


Fig. 4. List categories

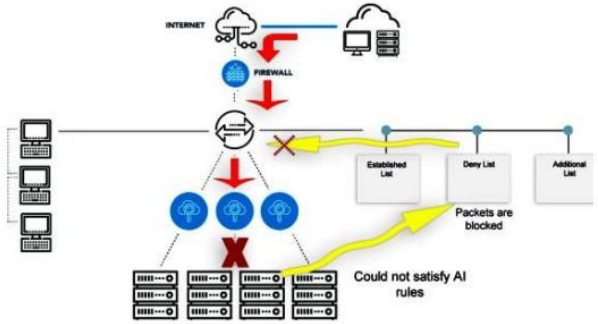


Fig. 7. Mismatched with AI rules

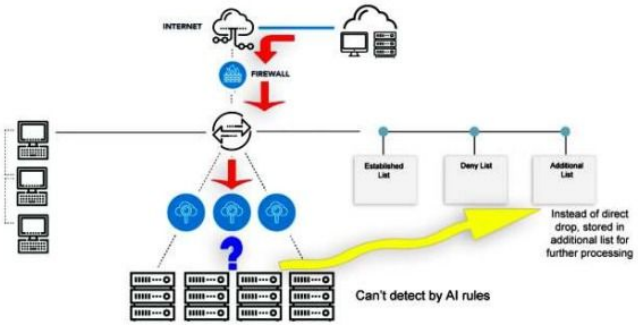


Fig. 8. Confusion with AI rules

TECHNOLOGIES TO BE USED

pfSense

Using their open source firewalls

Python

For developing AIML Model

Tensorflow, PyTorch

AI Platform

Docker

For Containerizing the AI model

Algorithms

Threat Detection:

Deep Packet Inspection (DPI):

Convolutional Neural Networks (CNNs)

Recurrent Neural Networks (RNNs)

Anomaly Detection:

K-means clustering

Gaussian Mixture Models (GMM)

Autoencoders

Machine Learning for Intrusion Detection:

Random Forests

Support Vector Machines (SVM)

Decision Trees

Reinforcement Learning (RL) for Policy Adjustment:

Q-learning

Deep Q-Networks (DQN)

Proximal Policy Optimization (PPO)

Ensemble Methods:

Bagging (Bootstrap Aggregating)

Boosting (AdaBoost, Gradient Boosting)

Stacking

Behavioral Analysis:

Markov models

Hidden Markov Models (HMMs)

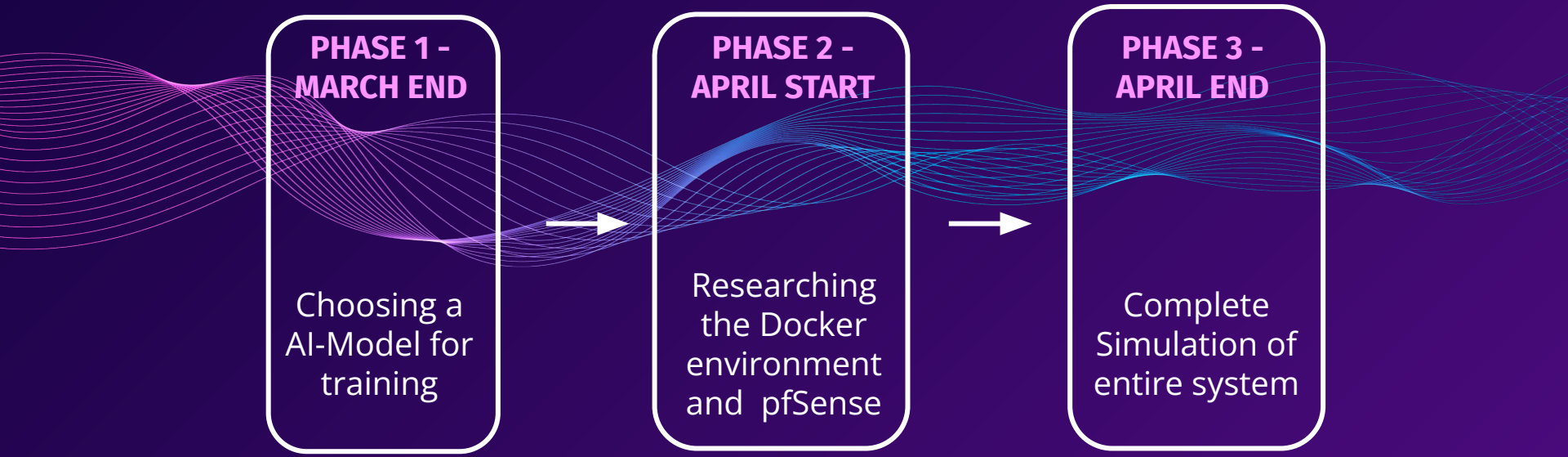
Clustering algorithms for behavior profiling

Expected Outcome

The expected outcomes of the mini project include:

- Development of a prototype adaptive firewall system capable of automatically detecting and mitigating intrusions.
- Demonstration of the system's ability to adaptively update its rules and configurations in response to evolving threats.
- Validation of the effectiveness of the adaptive firewall system through testing and evaluation in realistic scenarios.
- Documentation of the project findings and recommendations for future enhancements.

TIMELINE


PHASE 1 - MARCH END
Choosing a AI-Model for training
PHASE 2 - APRIL START
Researching the Docker environment and pfSense
PHASE 3 - APRIL END
Complete Simulation of entire system

Summary

In summary, the proposed project aims to address the limitations of traditional firewall systems by developing an innovative adaptive firewall solution. This adaptive firewall system will leverage advanced technologies such as machine learning and expert systems to enhance network security in dynamic and evolving environments.

By integrating machine learning algorithms, the adaptive firewall will be capable of analyzing network traffic patterns and identifying potential security threats in real-time. This proactive approach to threat detection enables the firewall to automatically respond to emerging threats without requiring manual intervention.

Furthermore, the incorporation of expert systems will empower the firewall to make intelligent decisions based on predefined rules and logic. The expert system will continuously learn from past incidents and adapt its behavior to effectively mitigate security risks and prevent unauthorized access to the network.

Overall, by automating threat detection and response mechanisms, the adaptive firewall system enhances the overall effectiveness of network defenses, mitigates security risks, and ensures the integrity and confidentiality of organizational data and assets.

References

- https://www.techtarget.com/searchsecurity/definition/threat-detection-and-response-TDR#:~:text=Threat%20detection%20and%20response%20(TDR)%20is%20the%20process%20of%20identifying,data%20breaches%20and%20data%20loss
- https://www.academia.edu/download/61385734/Building_New_Generation_Firewall_Including_Artificial_Intelligence20191130-88869-dl58qd.pdf
- https://dl.acm.org/doi/abs/10.1145/2007052.2007094
- https://www.researchgate.net/publication/377060591_Next_Generation_AI-Based_Firewalls_A_Comparative_Study
- https://marketing.pinecc.com/blog/part-1-using-ai-and-machine-learning-in-the-development-and-production-of-firewalls
- https://marketing.pinecc.com/blog/part-1-using-ai-and-machine-learning-in-the-development-and-production-of-firewalls

THANK YOU