SMART INDIA HACKATHON 2022

Basic Details of the Team and Problem Statement

Ministry/Organization Name/Student Innovation: Ministry of power

PS Code: SIH1451

Problem Statement Title : **Develop a AI/ML tool to detect whether a system firewall router network is compromised**

Software Team Name: **Byte Tech**

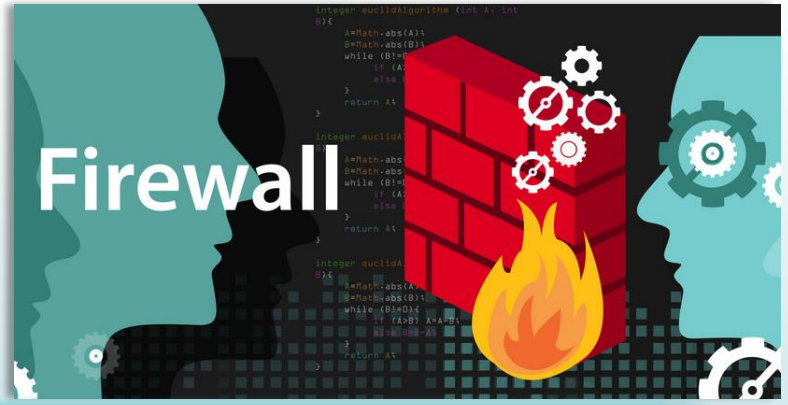
Team Leader Name: Atharva Katurde

Institute Code (AISHE): C-41484

Institute Name: Anantrao Pawar College of Engineering & Research

Theme Name: Blockchain and Cybersecurity

Introduction



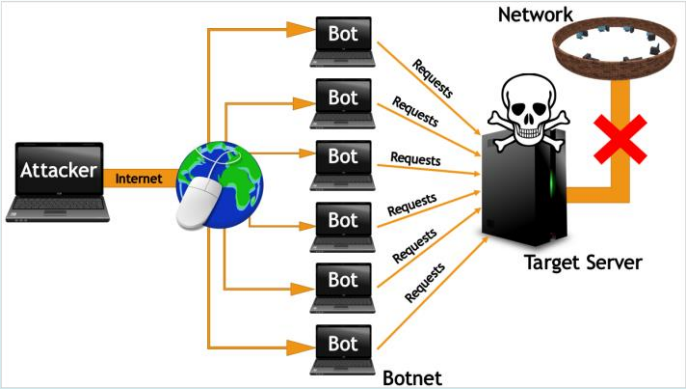
Anomaly Detection:

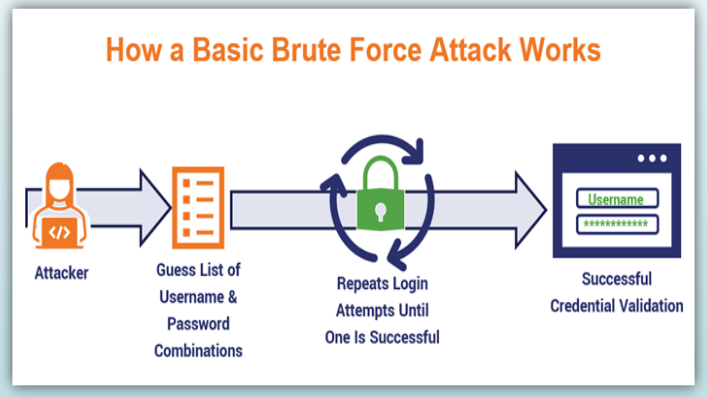
- Identifying abnormal instances or values within dataset.
- Used in fraud detection, network security, healthcare, manufacturing, IoT, and more.
- Types: Supervised, Unsupervised & Semi-Supervised.
- Techniques used: Statistical Methods , ML , Deep Learning.
- Continuous Learning : Adaptation of changing data patterns sustained effectiveness.

Behaviour Based Detection of Attacks:

- Analyzing patterns of behavior within a system to identify potential security threats or attacks
- Malicious activities often exhibit distinct patterns that differ from normal system behavior.
- Analyzes system activities looking for deviations from established baselines.
- Techniques used: Anomaly detection & Machine Learning

Types of Attacks:





DOS (Denial of Service):

Cyberattack that aims to disrupt or suspend the normal functioning of a target system, network, or service, making it inaccessible to its users.

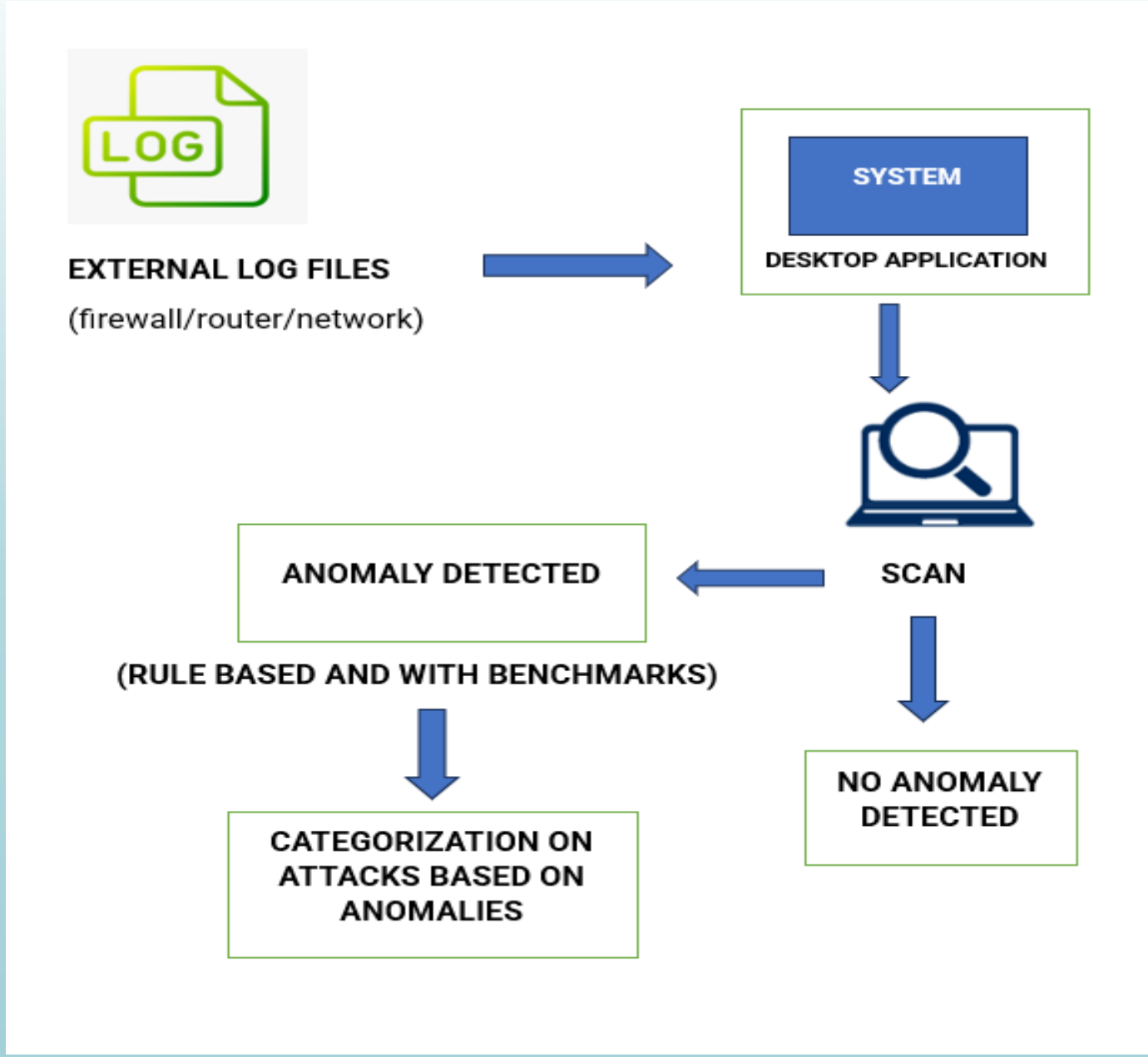
Brute Force Attack:

Trial-and-error method used by hackers to gain access to a system, website, or encrypted data.

AI/ML BASED TOOLS:

- ✓ Ai/ml introduction
- ✓ Isolation forest
- ✓ Data training and modelling
- ✓ Log files operations
- ✓ Displaying results

FLOW DIAGRAM:



FEATURES:

- Scalability
- Benchmarking and Rule Based Approach
- Proactive Approach for security
- Checking compromised System/Router/Network/Firewall by Desktop based Application.
- Using advanced Machine Learning techniques for Anomaly Detection.
- Learning Modules for new users.
- Categorization of anomalies efficient and secure.
- Efficient and Secure way of finding compromised System.

THANKYOU!!