INDIA INTERNATIONAL SCIENCE FESTIVAL 2023

SPACE HACKATHON

In Association with

Team Name: Equators

Name of College/University: PSG College of Technology

Team Member Details:

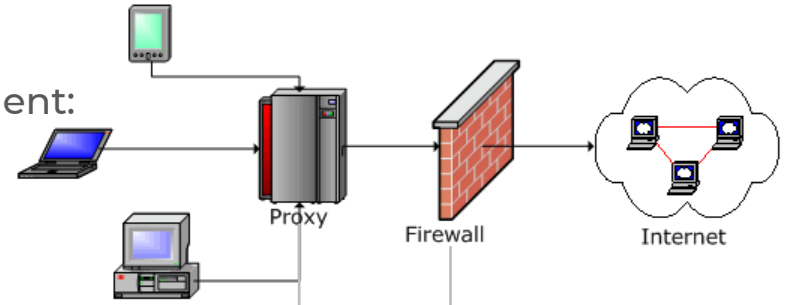
- Aaditya Rengarajan
- S Karun Vikhash
- Hareesh S
- Ashwant Krishna

Problem Statement:

Explain your understanding on Problem Statement:

The Objectives are to:

- Analyze behavior of cyber adversaries using AI/ML
- **Identify:** Flag packets that are suspected to be malicious.
- **Protect:** Find Mitigation Strategies to any suspected attack, and suggest the same to the CISO.
- **Detect:** Detect true positives and separate them from the false positives.
- **Respond:** Firewall is to decide whether to Allow or Deny.
- **Recover**: Find Mitigation Strategies to any suspected attack, and suggest the same to the CISO.
- Develop a framework for analyzing security logs collected.
- Anomaly detection based on pattern recognition of user access logs.



Solving the major problems with firewalls:

Insider Intrusion

- Behavioral Analysis: Utilizes AI/ML models to monitor user access patterns, detecting anomalous behavior indicative of potential insider threats.
- Log Monitoring: Processes system logs to flag users exhibiting suspicious activities or unauthorized access, identifying potential insider intrusions.
- Access Controls: Implements firewall rules and access controls to limit sensitive data access, preventing unauthorized internal breaches.

Direct Internet Traffic

- Packet Inspection and Filtering: Uses packet sniffers and specialized YARA rules to inspect incoming and outgoing network traffic, flagging potentially malicious packets before they enter or leave the network.
- Firewall Implementation: Utilizes firewalls, both hardware and software-based, to control and filter direct internet traffic, preventing unauthorized access and blocking suspicious traffic based on predefined rules.

Virus Attacks

- Malware Detection: Applies YARA rules and ML-based classifiers to identify known virus patterns or malware signatures in network traffic, flagging suspicious packets or behaviors associated with virus attacks.
- Threat Intelligence Integration: Incorporates threat intelligence from MITRE ATT&CK Framework, enabling the identification and classification of known attack vectors or methods used in virus attacks.
- Vulnerability Scoring and Prioritization: Uses CVSS scores to assess the severity of identified vulnerabilities exploited by viruses, allowing for prioritized responses and mitigation strategies.

Brief about your approach:

Collect Logs ← Compare with Community-Sourced Rules ← Map to MITRE ATT&CK Framework ← Prioritize by calculating NIST CVSS Scores ← Present in Dashboard, along with mitigation techniques

Detailed Proposal & Solution Approach

SCREENSHOTS GO HERE

SCREENSHOTS GO HERE

Cybersecurity Dashboard

Confidentiality	**Availability**	**Integrity**
Packets suspected for Interception	Packets suspected for Interruption	Packets suspected for Modification

Score every flagged packet using NIST NVD's CVSS (Common Vulnerability Scoring System) and order requests or responses by priority

Artificial Intelligence

AI	Map the flagged packets to MITRE ATT&CK Framework by most general unification so as to categorize under an attempt of breach of Confidentiality, Integrity or Availability.	Use the MITRE ATT&CK Framework to learn more regarding the issue to protect and mitigate
ML	Match with YARA Rules using supervised learning using ANN Models and Binary Sigmoidal Function as we are classifying it into categories of Safe or Unsafe	Specialized YARA Rules are collected from open source YAML files (https://github.com/projectdiscovery/nuclei-templates/), and are used to match each log entry to flag for suspicion
NLP	Data Preprocessing (Cleaning) -> Tokenize Data -> Convert to Vector Embeddings	

Server Logs | Firewall Logs

Problem Statement Objective	Solution Approach
To implement AI/ ML based security analysis model for finding the behaviors of the cyber attacker and to analyze the user traffic who are accessing Bhuvan Geo- Portal.	Utilizing AI/ML algorithms, like Artificial Neural Networks (ANNs), the model processes Bhuvan Geo-Portal traffic logs. It identifies behavioral patterns of cyber attackers and user access behavior, distinguishing normal from malicious activities.
The framework / model Should Identify, Protect, Detect, Respond and Recover from the cyber security attacks.	Creating a next generration framework involves integrating MITRE ATT&CK knowledgebase for attack techniques, scoring flagged packets using CVSS, and employing YARA rules via supervised learning.
Develop a Framework/ Model for analyzing security patterns on the fire wall logs collected.	By processing system logs, the model identifies flagged users, analyzes transferred data packets, and automatically detects user access patterns to distinguish suspicious activities from normal behavior.
Model / Framework should include anomaly detection, pattern recognition of user access and report from the logs collected.	The model for analyzing firewall logs involves anomaly detection through packet sniffing and network traffic analysis. It scrutinizes incoming and outgoing traffic, detects anomalies, and matches logs against specialized YARA rules for potential vulnerabilities.
Packet Sniffing or Network Traffic Analysis is the process of tracking all incoming and outcoming traffic, network traffic, and availability using packet sniffers. Packet sniffers are used for comparing real-time networks and past data for detecting a nomalies and potential vulnerabilities.	MITRE ATT&CK Framework is utilized to categorize flagged packets, mapping potential vulnerabilities, and anomalies detected in network traffic. CVSS scores are assigned to flagged packets based on their severity and risk level, aiding in prioritizing responses to potential threats.
Monitor the information contained in the packets or the intended source and destination of the packets.	Packet inspection involves parsing packet content, determining source-destination pairs, and analyzing packet headers. This information helps identify potentially malicious or suspicious traffic patterns and sources.
Process the system/ traffic logs and detect the users that are flagged.	System logs undergo preprocessing, applying YARA rules via supervised ANN models to flag users and traffic.
Analyze the data packets transferred over the network	Analyzing data packets entails preprocessing logs, converting them to vector embeddings, and employing specialized YARA rules to classify packets as safe or unsafe.
Analyze the user access pattern and develop a model to automatically detect.	User access logs undergo pattern recognition using AI/ML algorithms, detecting anomalies in access behavior.
Generate a report after analyzing the packets	A cybersecurity dashboard presents a comprehensive report of flagged packets categorized by Confidentiality, Integrity, and Availability, highlighting potential interception, modification, or service interruption attempts.
Develop software for detecting any data breach or ensuring the safety of the packet transfer process.	Using AI/ML models, the software analyzes network traffic, matching it against known attack patterns from MITRE and assessing vulnerabilities through CVSS scores, contributing to breach detection and ensuring secure packet transfers.
The accuracy of the model in identifying the malicious users will be evaluated.	The accuracy of the model in identifying malicious users is evaluated through metrics such as precision, recall, and F1-score, assessing the efficacy of the ANN models in distinguishing between safe and unsafe network behavior.
The reporting mechanism will be evaluated through mail alerts dashboard integration	Evaluating the model's accuracy in identifying malicious users is essential. The reporting mechanism includes mail alerts and dashboard integration, ensuring efficient communication and reporting of identified threats and anomalies.

Tools and devices used on development

- MITRE ATT&CK Framework for threat intelligence and detection.
- YARA for writing and using rules to identify malware or suspicious patterns.
- CVSS Calculator tools for assigning Common Vulnerability Scoring System scores
- High-performance cloud computing resources for data processing and machine learning model training.

Technologies involved/used

- Artificial Neural Networks (ANNs)
- Supervised Learning algorithms (used for training models)
- Natural Language Processing (NLP) for log preprocessing
- Pattern Recognition for anomaly detection
- Pandas, NumPy for data manipulation
- Python, scripting languages for development

Working Prototype at: https://intellx.in/

References/Acknowledgement

- Hardik Solanki, Limiting Attack Surface for Infrastructure Applications using Custom YAML Templates in Nuclei Automation (https://norma.ncirl.ie/6546/1/hardikvinodsolanki.pdf)
- Malak Aljabri,Amal A. Alahmadi,Rami Mustafa A. Mohammad, Menna Aboulnour,Dorieh M. Alomari and Sultan H. Almotiri, Classification of Firewall Log Data Using Multiclass Machine Learning Models (https://www.mdpi.com/2079-9292/11/12/1851)
- Hajar Esmaeil As-Suhbani, S.D. Khamitkar, Classification of Firewall Logs Using Supervised Machine Learning Algorithms (https://www.ijcseonline.org/pub_paper/49-IJCSE-07560-20.pdf)
- NIST National Vulnerability Database, Common Vulnerability Scoring System Calculator (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator)
- Saxe J., Yaraml (https://github.com/sophos-ai/yaraml_rules/)