Enhanced Intrusion Detection System With Automated Screen Capture And Account Deactivation

Rakshana P[1], Rishika Vashinisv[2], Amshumathypr[3], Ms.Subbulakshmi[4], Dr.R.Shoba Rani[5]
[1, 2, 3, 4, 5] Dept of B.sc ISCF
[1, 2, 3, 4, 5] Dr.M.G.REducationalandResearchInstitute,DeemedtobeUniversity,Chennai.

Abstract- *In the realm of cybersecurity, the need for robust intrusion detection systems (IDS) is paramount to safeguard sensitive information and prevent unauthorized access. This abstract introduces advanced IDS that go beyond conventional methods by incorporating automated screen capture and proactive account deactivation. The proposed system focuses on user authentication and response to suspicious activities, particularly the repetitive entry of incorrect passwords. Upon detecting three consecutive failed login attempts, the system initiates a multi-faceted response mechanism. First, it captures a screenshot of the unauthorized user's activity, providing valuable visual evidence of the intrusion. Subsequently, this screenshot is discreetly sent to the authenticated user's email address, serving as an immediate alert. To mitigate the potential risks associated with the intrusion, the system takes a proactive approach by automatically deactivating the compromised account.This swift action aims to prevent further unauthorized access and limit the potential damage caused by the intrusion. Users can recover their accounts by employing a secret recovery password, thereby adding an additional layer of security to the restoration process. The proposed IDS not only strengthens the security posture of systems but also empowers users with timely information and control over their accounts. By combining advanced intrusion detection capabilities with automated response measures, the system provides a comprehensive solution to address emerging cybersecurity challenges.*

I. INTRODUCTION

The constant danger of illegal access and data breaches, along with the ever-changing cybersecurity landscape, highlights the crucial need for modern Intrusion Detection Systems (IDS). When faced with highly intelligent invaders, traditional approaches frequently fail to offer an adequate defense. Our novel and strengthened intrusion detection system (IDS) not only detects but also reacts to possible threats in a proactive and multi- pronged manner is our answer to this difficulty.

By supplementing conventional intrusion detection methods with automatic screen capture and account deactivation,our technology ushers in a new paradigm. Strengthening user authentication and quickly responding to suspicious activity, especially in cases of several failed login attempts, are the main priorities. In order to protect sensitive information, provide users with timely alerts, and reduce risks related to unauthorized access, this abstract proposes a strong framework.

After three failed login attempts in a row, the system starts responding. The system then starts a series of steps to block the incursion. It takes a picture of the intruder's screen, so there's visual proof of the hack. To promptly notify the authenticated user of any possible illegal access, this screenshot is discreetly sent to their email address.

The system immediately deactivates the compromised account in order to proactively address the breach. This next step is to reduce the intrusion's potential damage by preventing further unwanted access. An extra safeguard for the restoration procedure is the use of a secret recovery password, which facilitates account recovery.

OBJECTIVES

- Implement a feature that captures screenshots upon detecting three consecutive failed login attempts, providing visual evidence of unauthorized access.
- Develop a mechanism for automatically deactivating compromised accounts upon detection of unauthorized access, mitigating the potential risks associated with security breaches.
- Integrate real-time alert mechanisms to notify users of potential security incidents, enabling them to promptly take control by deactivating their accounts and actively participating in the security process.
- Establish a deterrent system by combining automated screen capture and immediate account deactivation, discouraging potential intruders from unauthorized access attempts.
- Implement adaptive response mechanisms to enable swift and dynamic reactions to potential security threats,

reducing the time window for attackers and enhancing overall system responsiveness.
- Seamlessly integrate the proposed system with user interfaces, ensuring clear and user-friendly alerts to enhance user understanding and responsiveness to security incidents.

AIM

The aim of the proposed Enhanced Intrusion Detection System with Automated Screen Capture and Account Deactivation is to develop an advanced cybersecurity framework that goes beyond traditional Intrusion Detection Systems, incorporating innovative features to enhance threat detection, provide swift responses to security incidents, empower users with real- time control, and contribute to a more comprehensive and resilient defense against evolving cyber threats.

II. EXISTING SYSTEM

In the current landscape of Intrusion Detection Systems (IDS), traditional approaches predominantly revolve around signature-based detection, anomaly detection, and heuristic-based methodologies. Signature-based systems excel in identifying known threats but falter against emerging exploits and novel attack vectors. Anomaly-based solutions analyze behavior for deviations from established norms, yet their precision may be compromised by false positives. Heuristic-based methods offer flexibility but may struggle with accurately distinguishing between legitimate and malicious activities. Network- based and host-based IDS focus on monitoring network traffic and individual systems, respectively, with a recommended combination for comprehensive threat detection. However, the existing paradigm exhibits limitations in user-centric security, providing users with limited involvement and control over their accounts. Additionally, IDS responses are typically reactive, lacking deterrent measures to discourage potential intruders. The proposed Enhanced Intrusion Detection System seeks to address these shortcomings by introducing automated screen capture and proactive account deactivation, aiming for a more adaptive, user- centric, and responsive security framework that actively involves users in the intrusion detection and prevention process

Drawbacks

- Existing Intrusion Detection Systems (IDS) often struggle to keep up with new and evolving cyber threats, relying heavily on known patterns and signatures.
- Anomaly-based IDS can generate false alarms, flagging normal behavior as suspicious or failing to detect subtle but malicious activities.
- Users are typically notified of security incidents after they occur, reducing their ability to actively participate in threat detection and response.

IDS responses are often reactive, allowing attackers to exploit vulnerabilities before countermeasures can be initiated.

PROPOSED SYSTEM

The proposed Enhanced Intrusion Detection System (IDS) with Automated Screen Capture and Account Deactivation introduces a transformative paradigm in cybersecurity, offering innovative features to address the shortcomings of traditional IDS. By automatically capturing screenshots upon detecting three consecutive failed login attempts, the system provides tangible visual evidence of unauthorized access, augmenting forensic analysis and acting as a deterrent for potential intruders. The proactive measure of swift account deactivation upon detection aims to contain breaches promptly, preventing further unauthorized activities and safeguarding sensitive information. Emphasizing user-centric security, the proposed system actively involves users in the intrusion detection process, delivering real-time alerts and empowering them to take immediate control of their accounts. With adaptive response mechanisms, the system goes beyond reactivity, ensuring a dynamic and swift reaction to potential threats. It enhances insider threat detection, discourages unauthorized access through deterrence measures, and seamlessly integrates with user interfaces for clear and contextualized alerts. The inclusion of automated screen capture not only aids in immediate threat response but also provides visual evidence for forensic analysis, enhancing the system's capabilities in identifying and understanding the nature of intrusions. Overall, the proposed system aims to redefine cybersecurity by combining advanced intrusion detection
capabilities with proactive, user-centric, and comprehensive response measures, creating a resilient defense against emerging cyber threats.

ADVANTAGE

- The system excels at identifying potential security threats by capturing screenshots when detecting repeated failed login attempts.
- Unauthorized access triggers an immediate deactivation of the compromised account, limiting the impact of security breaches.

- Users receive real-time alerts and can promptly deactivate their accounts, giving them direct control and participation in the security process.
- The system's combination of automated screen capture and instant account deactivation acts as a deterrent, dissuading potential intruders.
- Seamless integration with user interfaces ensures clear and user- friendly alerts, aiding users in understanding and responding effectively to security incidents.
- Immediate account deactivation efficiently handles compromised accounts, reducing the impact of security incidents and limiting incidents and limiting exposure to sensitive information.
- The proposed system offers a holistic cybersecurity solution, combining advanced threat detection with proactive and user- centric response measures for enhanced overall security

III. REQUIREMENTS SPECIFICATION

HARDWARE REQUIREMENTS

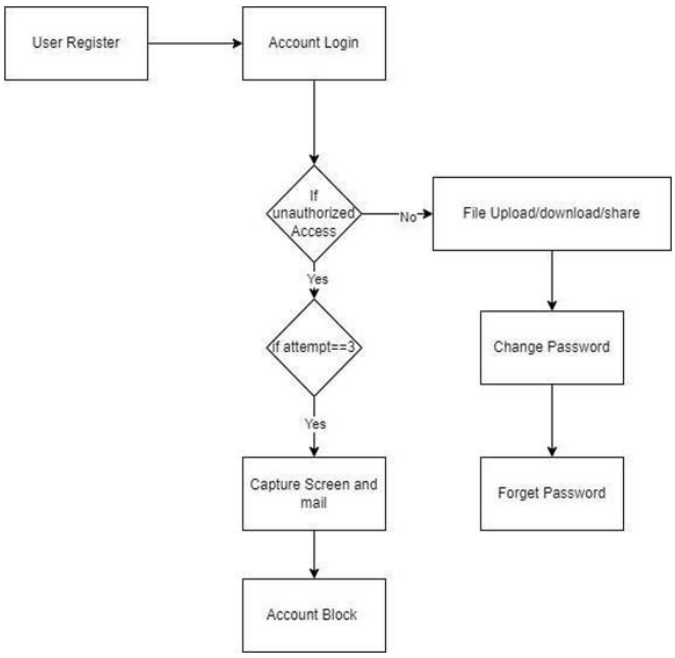
- System: Intel core I3 3.80 GHz 64 bit.
- Monitor: LED.
- Mouse: Logitech.
- Ram: 4.00 GB.

SOFTWARE REQUIREMENTS

- Operating system : Windows 10
- Platform : Anaconda3
- Development Framwork: Flask
- Frontend : python
- Backend :Mysql

IV. SYSTEM ARCHITETURE

(system framework with components) The system architecture is the model that defines the structure, behavior and more views of a system. ArchitectureThiarchitectureshowstheprocessofdetectingwheth erthegiven address is legitimate or not legitimate and also need to fetch the maximum detail s of the given.



V. MODULE DESCRIPTION

File Upload and Storage

This module handles the upload of files to the server. It includes a feature to check the file type and size, followed by the integration of the VirusTotal API for virus scanning. Clean files are then securely stored on the server

Access Control

The Access Control module enables users to set permission levels for file access. This includes defining access locks, ensuring that only authorized individuals can download specific files. It provides a granular level of control over who can view and retrieve shared content

URL Generation and Sharing

This module generates uniqueURLs for each uploaded file, allowing users to easily share them. The URLs are secure and can be sent via email or other communication channels. The system ensures that only individuals with the correct URL and access permissions can download the corresponding file.

Email Integration

This module facilitates the seamless sharing of files through email. Users can send shareable URLs directly from the application to recipients' email addresses. The integration

ensures a user-friendly experience and promotes efficient collaboration users, enhancing the overall user experience.

File Delete

The File Delete module handles the secure deletion of files from the server. Authorized users can initiate the deletion process for files they own or have permission to manage. Proper validation and confirmation mechanisms are implemented to prevent accidental deletions. Once a file is deleted, it is moved to a temporary or recycle bin area before permanent removal.

File Restore

The File Restore module provides users with the ability to recover deleted files within a specified timeframe. Deleted files are temporarily retained in a recycle bin, allowing users to restore them if needed. This feature adds an extra layer of data protection and ensures that users can recover important files in case of accidental deletions. The restoration process involves reassigning access permissions and returning the file to its original location.

REFERENCES

[1] Toya Acharya et.al(2023), "Efficacy of CNN-Bidirectional LSTM Hybrid Model for Network-Based Anomaly Detection", Published in: 2023 IEEE 13th Symposium on Computer Applications & Industrial Electronics (ISCAIE) Date of Conference: 20-21 May 2023 Date Added to IEEE Xplore: 03 July 2023

[2] Jesmithaa S; Sherin Eliyas (2023), "Detecting phishing attacks using Convolutional Neural Network andLSTM", Published in: 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) Date of Conference: 12-13 May 2023 Date Added to IEEE Xplore: 24 July 2023

[3] V. V. R. P. V. Jyothsna, V. V. Rama Prasad, and K. Munivara Prasad, “A review of anomaly based intrusion detection systems,” Int. J. Comput. Appl., vol. 28, no. 7, pp. 26–35, 2011.

[4] G. Ciaburro and B. Venkateswaran. Neural Networks With R: Smart Models Using CNN, RNN, Deep Learning, and Artificial Intelligence Principles. Birmingham, U.K.: Packt Publishing, 2017.

[5] J. Kiefer and J. Wolfowitz, “Stochastic estimation of the maximum of a regression function,” Ann. Math. Statist., vol. 23, no. 3, pp. 462–466, 1952.

[6] L. Bottou, F. E. Curtis, and J. Nocedal, “Optimization methods for large-scale machine learning,” Siam Rev., vol. 60, no. 2, pp. 223–311, 2018.

[7] M. Roopak, G. Yun Tian, and J. Chambers, “Deep learning models forcyber security in IoT networks,” in Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf., Las Vegas, NV, USA, 2019, pp. 0452–0457.

[8] S. Yeom and K. Kim, “Detail analysis on machine learning based malicious network traffic classification.” in Proc. Int. Conf. Smart Media Appl., 2019, pp. 49–53.

[9] Y. Gu, K. Li, Z. Guo, and Y. Wang, “Semi-supervised K-means DDoSdetection method using hybrid feature selection algorithm,” IEEE Access, vol. 7,