Automated Alerts and Investigation Tool (AAIT)

Prathamesh Dhindore[1], Mrs. Guarav Punyani[2]
[1,2]*Assistant Professor, Department of Computer Applications, Ajeenkya DY Patil University, Pune, Maharashtra, India*

***Abstract*—Cybersecurity threats such as brute-force attacks pose significant risks to modern systems by attempting unauthorized access through repeated authentication attempts. These attacks exploit weak credentials and lack of monitoring, potentially leading to data breaches, system compromise, and service disruption. Traditional monitoring systems often lack real-time detection and automated response capabilities, resulting in delayed mitigation and increased vulnerability [1]. Moreover, many existing solutions rely heavily on manual intervention, which reduces efficiency in high-volume attack scenarios. This research presents the Automated Alerts and Investigation Tool (AAIT), a real-time cybersecurity solution designed to detect, analyze, and respond to cyber-attacks efficiently. The system continuously monitors authentication logs and network activity, identifying suspicious patterns using a sliding window mechanism that tracks multiple failed logins attempts within a defined time frame. Once a predefined threshold is exceeded, the system triggers immediate alerts to notify administrators. In addition to detection, AAIT performs automated investigation by analyzing attack patterns, identifying source IP addresses, and assessing threat severity based on predefined risk parameters. It correlates multiple events to distinguish between false positives and actual attack behavior, thereby improving accuracy. The system also maintains detailed logs and reports, which can be used for forensic analysis and future threat intelligence. Furthermore, AAIT incorporates automated response mechanisms such as IP blacklisting, firewall rule enforcement, temporary account lockouts, and rate limiting to prevent further unauthorized access attempts [2]. These proactive measures significantly reduce response time and minimize potential damage caused by ongoing attacks.**

***Index Terms*—API, web application API Automation tool.**

I INTRDUCTION

In today's digital era, the rapid growth of internet-based services and cloud computing has significantly increased the attack surface for cyber threats. Organizations and individuals rely heavily on online systems for communication, financial transactions, and data storage, making cybersecurity a critical concern. Among various cyber threats, brute-force attacks remain one of the most common and persistent methods used by attackers to gain unauthorized access to systems. These attacks involve systematically attempting multiple password combinations until the correct credentials are identified, often targeting weak or reused passwords [1].

Traditional security mechanisms such as basic logging and manual monitoring are no longer sufficient to defend against such attacks. These systems typically detect suspicious activity only after significant damage has occurred and lack real-time response capabilities. Additionally, the increasing volume of authentication logs generated by modern systems makes manual analysis inefficient and prone to human error [2]. As a result, there is a growing need for intelligent, automated solutions that can detect threats proactively and respond without delay.

To address these challenges, this research introduces the Automated Alerts and Investigation Tool (AAIT), a real-time cybersecurity system designed to enhance threat detection and response capabilities. The proposed system continuously monitors authentication logs and network events to identify abnormal patterns indicative of brute-force attacks. By utilizing a sliding window technique, the system tracks repeated failed login attempts within a defined time interval and triggers alerts when suspicious thresholds are exceeded [3].

Beyond detection, AAIT integrates automated investigation features that analyze attack behavior, identify malicious sources, and evaluate the severity of threats. This reduces dependency on manual analysis and accelerates decision-making processes. Furthermore, the system implements automated

response actions such as IP blocking, firewall updates, and temporary account restrictions to mitigate threats instantly [4].

The primary objective of this research is to develop a lightweight, efficient, and cost-effective solution that simulates the core functionalities of a Security Operations Center (SOC). By combining real-time monitoring, intelligent detection, and automated response, AAIT aims to improve system security, reduce response time, and minimize the impact of cyber-attacks.

II. LITERATURE REVIEW

Cybersecurity has evolved significantly over the years, with various techniques developed to detect and prevent unauthorized access. One of the earliest approaches includes Intrusion Detection Systems (IDS), which monitor network traffic and system activities for malicious behavior. According to Scarfone and Mell [2], IDS can be classified into signature-based and anomaly-based systems. Signature-based systems detect known attack patterns, while anomaly-based systems identify deviations from normal behavior. However, traditional IDS solutions often struggle with high false-positive rates and lack automated response mechanisms.

Brute-force attacks have been widely studied as a common method of unauthorized access. Stallings [1] explains that such attacks exploit weak password policies and insufficient monitoring systems. Attackers use automated scripts to repeatedly attempt login credentials, making detection difficult without real-time analysis. Research shows that early detection of repeated failed login attempts is critical to minimizing damage.

To improve detection accuracy, several researchers have proposed log-based analysis techniques. Axelsson [3] introduced a taxonomy for intrusion detection, highlighting the importance of analyzing system logs to identify suspicious patterns. Log monitoring enables systems to track authentication attempts, user behavior, and access patterns. However, manual log analysis is time-consuming and inefficient in large-scale environments.

Recent advancements focus on automated and intelligent detection systems. Behl and Behl [4] emphasize the need for automation in cybersecurity to reduce human dependency and response time. Modern systems integrate real-time monitoring with automated alert generation, enabling faster identification of threats. These systems often use threshold-based or time-window techniques to detect anomalies such as multiple failed logins attempt within a short duration.

Additionally, Security Operations Centers (SOCs) play a vital role in managing and responding to cyber threats. SOCs combine monitoring, detection, investigation, and response into a centralized system. However, setting up a full-scale SOC requires significant financial and technical resources, making it impractical for small and medium-sized organizations.

Despite these advancements, existing solutions still face challenges such as delayed response, high implementation cost, and lack of integration between detection and response mechanisms. Many systems focus only on detection without providing automated mitigation, which limits their effectiveness in real-world scenarios.

To overcome these limitations, the proposed Automated Alerts and Investigation Tool (AAIT) integrates real-time detection, automated investigation, and immediate response into a single lightweight system. By combining log analysis, sliding window detection, and automated action mechanisms, AAIT addresses the gaps identified in existing research and provides a more efficient and practical cybersecurity solution.

III. PROBLEM STATEMENT

With the increasing dependence on digital systems and online authentication mechanisms, cybersecurity threats such as brute-force attacks have become more frequent and sophisticated. These attacks exploit weak passwords and insufficient monitoring systems to gain unauthorized access, potentially leading to data breaches, financial loss, and system compromise [1].

Existing security solutions, including traditional Intrusion Detection Systems (IDS) and log monitoring tools, primarily focus on detecting suspicious activities but often fail to provide real-time response and automated mitigation. Most systems rely on manual analysis of logs, which is time-consuming and inefficient, especially in environments generating large volumes of authentication data [2]. This delay in detection and response allows attackers to continue their attempts, increasing the risk of successful breaches.

Furthermore, many organizations, particularly small and medium-sized enterprises, lack the resources to implement full-scale Security Operations Centers (SOCs). As a result, they operate with limited security infrastructure that cannot effectively handle continuous monitoring, threat analysis, and incident response.

Another major challenge is the absence of integrated systems that combine detection, investigation, and response into a single framework. Existing tools often operate in isolation, requiring multiple solutions to handle different aspects of cybersecurity, which increases complexity and cost.

Therefore, there is a critical need for a lightweight, cost-effective, and automated cybersecurity solution that can:

- Detect brute-force attacks in real time
- Analyze and investigate suspicious activities automatically
- Respond instantly to mitigate threats (e.g., blocking IPs, enforcing security rules)

This research aims to address these challenges by developing the Automated Alerts and Investigation Tool (AAIT), which integrates real-time monitoring, intelligent detection, automated investigation, and immediate response into a unified system, thereby improving overall system security and reducing the impact of cyber-attacks.

IV. OBJECTIVES

The primary objective of this research is to design and develop an efficient cybersecurity system capable of detecting and mitigating brute-force attacks in real time. The proposed Automated Alerts and Investigation Tool (AAIT) aims to continuously monitor authentication logs and system activities in order to identify suspicious behavior and potential security threats.

Another key objective is to implement a real-time detection mechanism using a sliding window technique, which enables the system to track multiple failed logins attempts within a specific time interval and identify abnormal patterns. The system is also intended to generate automated alerts whenever predefined thresholds are exceeded, ensuring timely notification of potential attacks.

In addition to detection, the research focuses on enabling automated investigation by analyzing attack patterns, identifying malicious IP addresses, and evaluating the severity of threats. This helps in reducing the need for manual analysis and improves the efficiency of the overall security process.

Furthermore, the system is designed to perform automated response actions such as IP blacklisting, firewall rule enforcement, and temporary account lockouts to prevent further unauthorized access. Another important objective is to reduce dependency on manual monitoring and significantly improve response time to cyber threats.

The research also aims to develop a lightweight and cost-effective solution that can be easily deployed in small and medium-scale environments. Finally, the system is intended to simulate the core functionalities of a Security Operations Center (SOC), including monitoring, detection, investigation, and response, while maintaining detailed logs for forensic analysis and future threat intelligence.

V. PROPOSED SYSTEM

The system design of the Automated Alerts and Investigation Tool (AAIT) is structured to provide a seamless integration of monitoring, detection, investigation, and response mechanisms within a unified framework. The design follows a modular architecture, where each component performs a specific function while interacting with other modules to ensure efficient and real-time operation.

At the core of the system is the log monitoring module, which continuously collects and processes authentication logs from the system. These logs include login attempts, timestamps, IP addresses, and user credentials activity. The collected data is then forwarded to the detection engine for further analysis.

The detection module is responsible for identifying suspicious activities using a sliding window mechanism. It analyzes repeated failed login attempts within a predefined time interval and compares them against a threshold value. If the number of failed attempts exceeds the threshold, the system flags the activity as a potential brute-force attack. This real-time analysis ensures early detection of threats before they can cause significant damage.

Once a threat is detected, the system activates the alert generation module, which immediately notifies the

administrator about the suspicious activity. Alerts can be generated in various forms such as console notifications, log entries, or email alerts, depending on the system configuration.

Following detection and alerting, the investigation module performs deeper analysis of the identified threat. It examines attack patterns, tracks the origin of the attack through IP addresses, and evaluates the severity of the threat based on predefined rules. This module helps in distinguishing between genuine threats and false positives, improving the overall accuracy of the system.

The response module is designed to take immediate action against detected threats. It automatically implements security measures such as blocking the attacker's IP address, updating firewall rules, and temporarily locking affected user accounts. These actions help in preventing further unauthorized access and minimizing system vulnerability.

Additionally, the system includes a logging and reporting module, which maintains detailed records of all detected activities, alerts, and response actions. These logs are useful for forensic analysis, auditing, and improving future threat detection strategies.

Overall, the system design ensures that all components work together efficiently to provide real-time detection, automated investigation, and immediate response. The modular and lightweight architecture makes AAIT scalable, easy to implement, and suitable for environments with limited resources while still delivering effective cybersecurity protection.

VI. SYSTEM DESIGN

The system design of the Automated Alerts and Investigation Tool (AAIT) is structured to provide a seamless integration of monitoring, detection, investigation, and response mechanisms within a unified framework. The design follows a modular architecture, where each component performs a specific function while interacting with other modules to ensure efficient and real-time operation.

At the core of the system is the log monitoring module, which continuously collects and processes authentication logs from the system. These logs include login attempts, timestamps, IP addresses, and user credentials activity. The collected data is then forwarded to the detection engine for further analysis.

The detection module is responsible for identifying suspicious activities using a sliding window mechanism. It analyzes repeated failed login attempts within a predefined time interval and compares them against a threshold value. If the number of failed attempts exceeds the threshold, the system flags the activity as a potential brute-force attack. This real-time analysis ensures early detection of threats before they can cause significant damage.

Once a threat is detected, the system activates the alert generation module, which immediately notifies the administrator about the suspicious activity. Alerts can be generated in various forms such as console notifications, log entries, or email alerts, depending on the system configuration.

Following detection and alerting, the investigation module performs deeper analysis of the identified threat. It examines attack patterns, tracks the origin of the attack through IP addresses, and evaluates the severity of the threat based on predefined rules. This module helps in distinguishing between genuine threats and false positives, improving the overall accuracy of the system.

The response module is designed to take immediate action against detected threats. It automatically implements security measures such as blocking the attacker's IP address, updating firewall rules, and temporarily locking affected user accounts. These actions help in preventing further unauthorized access and minimizing system vulnerability.

Additionally, the system includes a logging and reporting module, which maintains detailed records of all detected activities, alerts, and response actions. These logs are useful for forensic analysis, auditing, and improving future threat detection strategies.

Overall, the system design ensures that all components work together efficiently to provide real-time detection, automated investigation, and immediate response. The modular and lightweight architecture makes AAIT scalable, easy to implement, and suitable for environments with limited resources while still delivering effective cybersecurity protection.

VII. METHODOLOGY

The methodology adopted for the development of the Automated Alerts and Investigation Tool (AAIT) follows a systematic approach to ensure effective detection, analysis, and response to brute-force attacks.

The process begins with data collection, where authentication logs are continuously gathered from the system. These logs contain essential information such as login attempts, timestamps, usernames, and IP addresses, which serve as the primary input for the system.

Once the data is collected, it undergoes preprocessing to organize and filter relevant information required for analysis. This step involves removing unnecessary data, structuring log entries, and preparing them for real-time monitoring. Proper preprocessing ensures that the system operates efficiently and reduces processing overhead.

The next stage involves real-time monitoring and detection using a sliding window technique. In this approach, the system continuously observes login attempts within a defined time interval and counts the number of failed attempts associated with a particular IP address or user account. If the number of failed attempts exceeds a predefined threshold within the specified time window, the activity is identified as suspicious and classified as a potential brute-force attack.

After detection, the system initiates the alert generation process. Immediate alerts are triggered to notify the administrator about the detected threat. This ensures that security personnel are aware of ongoing attacks without delay.

Following alert generation, an automated investigation process is carried out. The system analyzes the detected activity by examining patterns such as frequency of attempts, source IP behavior, and repetition of login failures. Based on this analysis, the system evaluates the severity of the threat and determines whether it is a genuine attack or a false positive.

Subsequently, the system executes automated response actions to mitigate the identified threat. These actions include blocking the malicious IP address, enforcing firewall rules, and temporarily locking targeted user accounts. This proactive response mechanism helps in preventing further unauthorized access and reducing potential damage.

Finally, all activities, including detected threats, alerts, and response actions, are recorded in the system logs. These logs are used for reporting, forensic analysis, and improving future detection strategies. The overall methodology ensures a continuous cycle of monitoring, detection, investigation, and response, enabling the system to function efficiently in real-time cybersecurity environments.

VIII. RESULTS AND DISCUSSION.

environment to assess its effectiveness in detecting and mitigating brute-force attacks. Simulated attack scenarios were generated by performing multiple failed logins attempts within short time intervals to mimic real-world attack behavior. The system successfully monitored authentication logs in real time and accurately identified suspicious activities based on the predefined threshold values.

The results demonstrate that AAIT was able to detect brute-force attacks with high accuracy by utilizing the sliding window technique. When the number of failed login attempts exceeded the defined threshold within the specified time frame, the system consistently triggered alerts without significant delay. This real-time detection capability ensured that potential threats were identified at an early stage, reducing the risk of successful unauthorized access.

A key feature of the system is its Telegram-based alerting mechanism, which enhances real-time communication. Once a threat is detected, instant notifications are sent to the administrator via Telegram, including details such as the suspicious IP address, number of failed attempts, and timestamp of the activity. This approach ensures that alerts are accessible anytime and anywhere, significantly improving response time compared to traditional alerting methods such as email or local logs.

The investigation module further enhanced the system's performance by analyzing attack patterns and identifying malicious IP addresses. This helped in distinguishing between normal user errors (such as incorrect password attempts) and actual attack behavior, thereby reducing false positives.

The response module played a crucial role in mitigating threats. Upon detection, the system automatically executed predefined actions such as IP

blacklisting and temporary account lockouts. These measures successfully prevented further login attempts from malicious sources, effectively stopping the attack in progress. The automated response significantly reduced the need for manual intervention. Performance analysis indicated that the system operates efficiently with low computational overhead, making it suitable for deployment in small and medium-scale environments. The logging and reporting module maintained detailed records of all events, which were useful for analyzing attack trends and improving system performance over time.

Overall, the results confirm that AAIT provides an effective and reliable solution for real-time detection and mitigation of brute-force attacks. The integration of monitoring, detection, investigation, automated response, and Telegram-based alerting within a single system enhances operational efficiency and strengthens the overall security posture. Future improvements may include integration with machine learning techniques and deployment in large-scale environments to further enhance detection accuracy and scalability.

IX. CONCLUSION

This research presented the design and implementation of the Automated Alerts and Investigation Tool (AAIT), a real-time cybersecurity solution developed to detect and mitigate brute-force attacks efficiently. The system addresses key limitations of traditional security mechanisms by integrating continuous monitoring, intelligent detection, automated investigation, and immediate response within a single framework.

The results demonstrate that AAIT is capable of accurately identifying suspicious login activities using a sliding window technique and predefined thresholds. The system successfully generates real-time alerts and delivers them through a Telegram-based notification mechanism, ensuring that administrators are

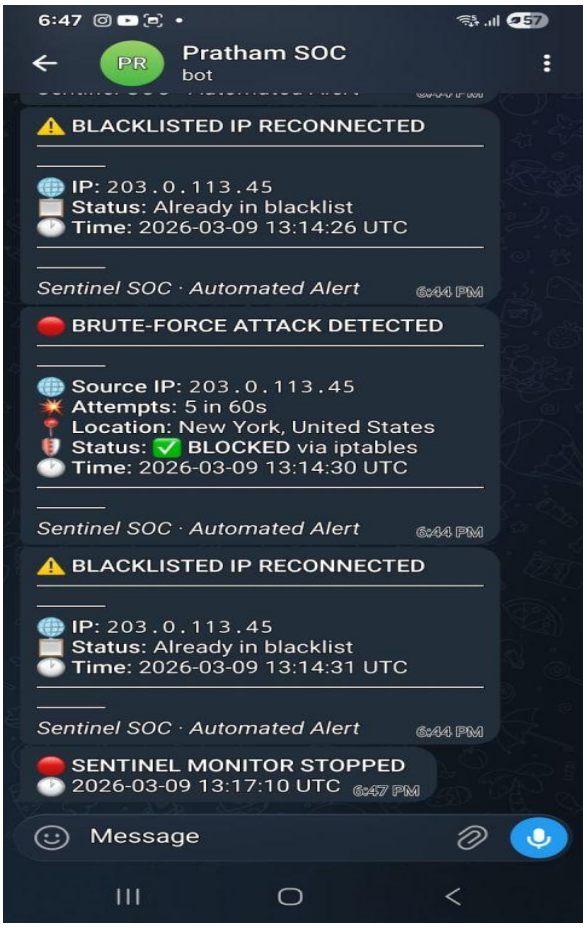

Fig. Alerts shown

This significantly improves response time and enhances situational awareness.

Furthermore, the automated investigation and response features reduce dependency on manual intervention by analyzing attack patterns, identifying malicious sources, and executing actions such as IP blocking and account lockouts. This proactive approach helps in minimizing potential damage and preventing unauthorized access effectively.

The lightweight and cost-effective design of the system makes it suitable for deployment in small and medium-scale environments, where implementing full-scale Security Operations Centers (SOCs) may not be feasible. By simulating core SOC functionalities, AAIT provides a practical and efficient alternative for improving cybersecurity posture.

In conclusion, the proposed system proves to be an effective solution for real-time threat detection and response. Future enhancements may include the

integration of machine learning techniques for advanced anomaly

REFERENCES

[1] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Pearson Education, 2017.

[2] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," *NIST Special Publication 800-94*, National Institute of Standards and Technology, 2007.

[3] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Technical Report No. 99-15, Chalmers University of Technology, 2000.

[4] R. Behl and R. Behl, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2017.

[5] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. Wiley, 2015.

[6] OWASP Foundation, "OWASP top ten web application security risks," 2021.

[7] National Institute of Standards and Technology (NIST), "Digital identity guidelines," *NIST Special Publication 800-63B*, 2020.

[8] M. Bishop, *Computer Security: Art and Science*. Addison-Wesley, 2018.