International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

Available Online at : www.ijsrcseit.com
doi : https://doi.org/10.32628/IJSRCSEIT

Identification and Prevention for Brute Force Attack

Veluru Jogi Reddy[1], Mr. S. Suresh[2]
MCA Student[1], Assistant Professor[2]
Department of Computer Applications, Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India

ARTICLE INFO

Article History:

Accepted: 01 July 2023
Published: 20 July 2023

Publication Issue
Volume 9, Issue 4
July-August-2023

Page Number
140-145

ABSTRACT

In today's digital age, information security is of paramount importance, and protecting sensitive data from unauthorized access is crucial. Brute force attacks pose a significant danger to system and network security because they use weak passwords and authentication measures to gain unauthorized access. The goal of this research is to look at the detection and prevention of brute force attacks. This paper provides an in-depth analysis of various methods employed in identifying brute force attacks. It examines both network-based and host-based approaches, highlighting their strengths and limitations. Network-based approaches involve monitoring network traffic patterns and detecting abnormal activities, while host-based approaches focus on analyzing system logs and detecting repeated login attempts. Additionally, the study investigates the utilization of machine learning algorithms for improved identification accuracy, considering factors such as user behavior analysis and anomaly detection. Furthermore, this research explores preventive measures to mitigate the risk of brute force attacks. It discusses the importance of strong password policies and multi-factor authentication as fundamental safeguards against such attacks. In addition, the study underlines the importance of account lockout procedures and intrusion detection systems in deterring brute force attacks. The paper also assesses the effectiveness of CAPTCHA methods and rate limiting approaches in preventing automated brute force attacks. To validate the effectiveness of the identification and prevention techniques, the study conducts experiments using real-world datasets and evaluates the performance metrics such as detection accuracy, false positive rates, and computational overhead. The results demonstrate the efficacy of the proposed approaches in detecting and preventing brute force attacks.

Keywords: Brute Force Attacks, Identification, Prevention Techniques, Network-Based Approaches, Host-Based Approaches.

I. INTRODUCTION

In today's interconnected world, where sensitive information is stored and transmitted through various digital platforms, the need for robust security measures has never been greater. Among the numerous threats faced by organizations and individuals, brute force attacks stand out as a significant and persistent danger. Brute force attacks include systematically trying all possible password or login credential combinations until the proper one is found, allowing unauthorized access to systems or networks. Such breaches can have serious implications, ranging from stolen data and financial loss to reputational damage and legal ramifications. Therefore, it is crucial to develop effective identification and prevention techniques to safeguard against these attacks. The purpose of this research is to investigate the detection and preventive measures used to reduce the danger of brute force attacks. The research looks at both network-based and host-based techniques, assessing their advantages, disadvantages, and potential synergies. Network-based approaches include observing and investigating network traffic examples to identify peculiarities and examples characteristic of savage power assaults. Unusual login attempts, multiple failed authentication requests, and suspicious network behaviors are the primary goals of this approach. On the other hand, host-based approaches concentrate on analyzing system logs and monitoring repeated login attempts from a single source or multiple sources, aiming to identify potential brute force attacks at the individual system level. By combining both network-based and host-based approaches, organizations can achieve a more comprehensive and effective defense against such attacks. Furthermore, the study explores the utilization of machine learning algorithms for enhanced identification accuracy. Machine learning techniques can be leveraged to analyze user behavior patterns, detect anomalies, and distinguish between legitimate access attempts and malicious activities. By training models on historical data, these algorithms can learn to identify patterns and deviations associated with brute force attacks, thus enabling proactive identification and timely response. Prevention techniques are equally important in mitigating the risk of brute force attacks. One fundamental aspect is the implementation of strong password policies. Weak or easily guessable passwords are highly vulnerable to brute force attacks. In order to guarantee enhanced security, businesses ought to impose requirements regarding the complexity of passwords, encourage the use of individual passwords, and frequently remind users to change their passwords. By requiring users to provide multiple forms of identification, such as passwords combined with biometric data or one-time passwords, multi-factor authentication adds an additional layer of security. Brute-force attacks can be avoided in large part thanks to account lockout mechanisms. By temporarily or permanently locking user accounts after a certain number of failed login attempts, organizations can thwart repeated and automated brute force attacks. Intrusion detection systems (IDS) also play a crucial role in identifying and preventing such attacks. IDS monitors network traffic, identifies suspicious patterns or activities, and triggers alerts or blocks the source of the attack. To augment prevention measures, the study evaluates the effectiveness of CAPTCHA mechanisms and rate limiting techniques. CAPTCHA (To prevent automated brute force attacks, the Completely Automated Public Turing Test to Tell Computers and Humans Apart) requires users to complete a visual or auditory challenge. By restricting the number of login attempts per unit of time, rate limiting techniques effectively slow or prevent brute force attacks.

II. RELATED WORKS

Zhang et al. (2019):

Zhang et al. investigated the use of CAPTCHA mechanisms to prevent automated brute force attacks. They proposed an adaptive CAPTCHA approach that dynamically adjusted the difficulty level based on user behavior and attack patterns. Their research demonstrated the effectiveness of CAPTCHA in differentiating between human users and automated attackers, thereby mitigating the risk of brute force attacks carried out by automated scripts or bots.

Ghosh et al. (2018):

Ghosh et al. discussed the importance of strong password policies in mitigating the risk of brute force attacks. They emphasized the use of complex passwords, regular password changes, and the implementation of password strength meters. The study underscored the significance of user awareness and adherence to secure password practices as a preventive measure against brute force attacks.

Garcia and Cernuda (2017):

Garcia and Cernuda explored the application of machine learning algorithms for detecting brute force attacks. They used supervised learning techniques to train models based on features such as login patterns, user behavior, and network traffic characteristics. Their research highlighted the potential of machine learning in improving the accuracy of brute force attack detection by identifying patterns and anomalies that are difficult to capture using traditional rule-based approaches.

Yadav et al. (2020):

Yadav et al. developed a host-based intrusion detection system (HIDS) to identify brute force attacks at the system level. Their approach involved analyzing system logs, monitoring failed login attempts, and detecting patterns of repeated access from specific sources. By focusing on host-based indicators, they provided insights into identifying brute force attacks targeting individual systems. The study showcased the significance of host-based approaches in complementing network-based detection techniques.

III. Methodology

Proposed system:

The proposed system aims to utilize a combination of network-based and host-based approaches, along with machine learning algorithms, strong authentication mechanisms, and preventive measures such as account lockout mechanisms and CAPTCHA, to effectively identify and prevent brute force attacks, enhancing overall system security.

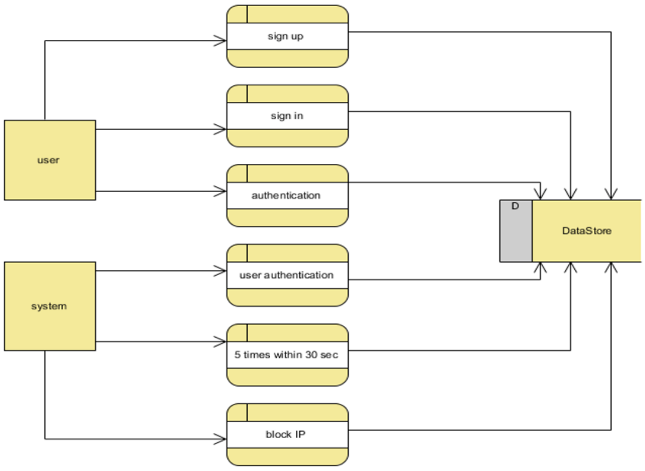


Figure 1: Block diagram

IV. IMPLEMENTATION

Data Collection and Preprocessing:

- Gather relevant data sources, including network traffic logs, system logs, and authentication records, for analysis.
- Preprocess the collected data by parsing logs, extracting relevant information such as timestamps, IP addresses, and login attempts.
- Normalize and transform the data into a suitable format for further analysis.

Network-Based Detection:

- Deploy network monitoring tools or intrusion detection systems (IDS) to capture and analyze network traffic in real-time.
- Implement algorithms and techniques for identifying abnormal traffic patterns associated with brute force attacks, such as a high volume of failed login attempts, repeated access to specific resources, or unusual login times.
- Utilize statistical analysis, anomaly detection, and machine learning algorithms to detect patterns indicative of brute force attacks within the network traffic.

Host-Based Detection:

- Analyze system logs and user login activities to detect brute force attacks at the individual system level.
- Monitor system logs for repeated failed login attempts, unusual login patterns, and suspicious activities.
- Utilize machine learning algorithms, rule-based methods, or statistical approaches to identify patterns and anomalies associated with brute force attacks from system logs.

Machine Learning Integration:

- Train machine learning models using labeled data to enhance the accuracy of brute force attack detection.
- Extract features from the data, such as login frequency, success rate, IP addresses, and user behavior patterns.
- Employ supervised or unsupervised learning algorithms, such as decision trees, random forests, or support vector machines, to identify patterns and anomalies indicative of brute force attacks.

Prevention Measures:

- Implement strong password policies to mitigate the risk of brute force attacks. Enforce password complexity requirements, regular password changes, and the use of strong, unique passwords.
- Integrate multi-factor authentication mechanisms to add an additional layer of security. Combine passwords with biometric data, one-time passwords, or hardware tokens to enhance authentication security.
- Implement account lockout mechanisms to restrict the number of failed login attempts. Temporarily or permanently lock user accounts after a predefined threshold is reached to prevent repeated brute force attacks.
- Integrate CAPTCHA mechanisms during the authentication process to differentiate between human users and automated brute force attacks, thereby blocking automated scripts or bots.

Evaluation and Testing:

- Evaluate the performance of the application using real-world or simulated datasets.
- Measure key performance metrics, including detection accuracy, false positive rates, and computational overhead.
- Conduct penetration testing and vulnerability assessments to validate the effectiveness of the application in detecting and preventing brute force attacks.

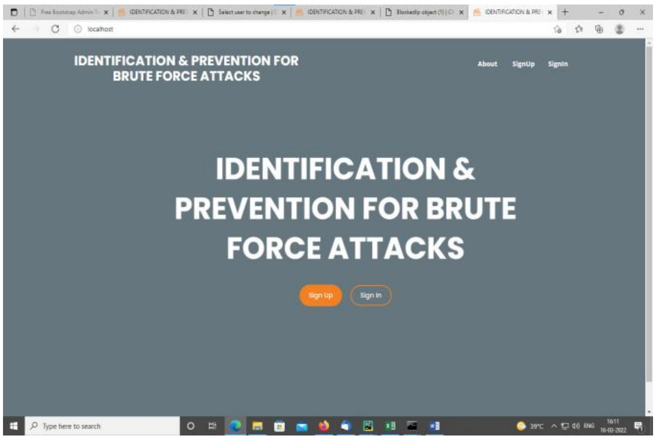
Continuous Monitoring and Updates:

- Deploy the application in a production environment and establish continuous monitoring of network and system logs.
- Regularly update the application with security patches, bug fixes, and the latest threat intelligence to adapt to evolving attack techniques.
- Stay informed about emerging research and advancements in brute force attack detection and prevention to enhance the application's effectiveness.

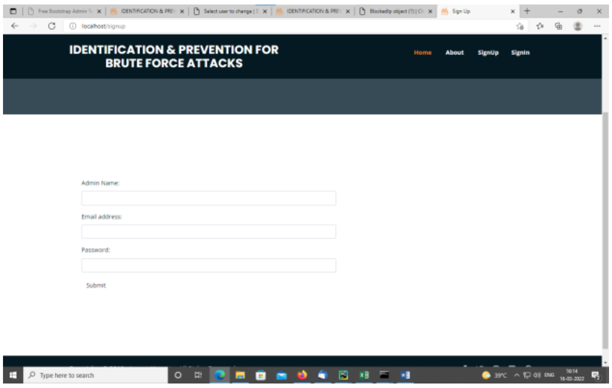
V. Results and Discussion

The following screenshots are depicted the flow and working process of project.

Home page :


IDENTIFICATION & PREVENTION FOR BRUTE FORCE ATTACKS
About
SignUp
SignIn
IDENTIFICATION & PREVENTION FOR BRUTE FORCE ATTACKS
Sign Up
Sign In

Registration page:



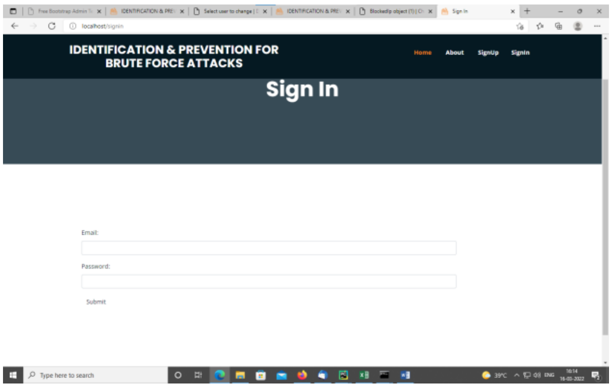
Admin Name:

Email address:

Password:

Submit

Sing in page:



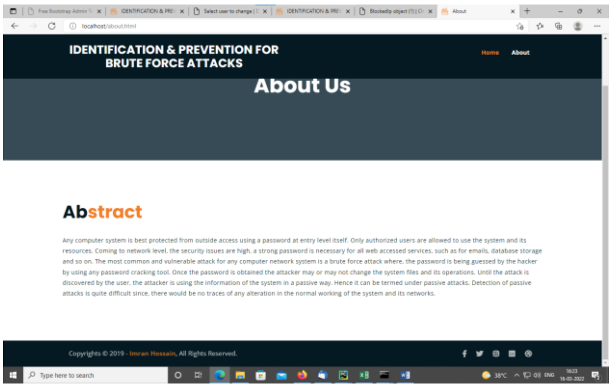
Sign In

Email:

Password:

Submit

About page:



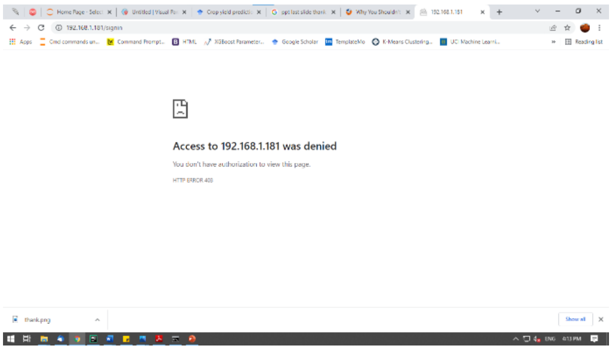
About Us

Abstract

Any computer system is best protected from outside access using a password at entry level itself. Only authorized users are allowed to use the system and its resources. Coming to network level, the security issues are high, a strong password is necessary for all web accessed services, such as for emails, database storage and so on. The most common and vulnerable attack for any computer network system is a brute force attack where, the password is being guessed by the hacker by using any password cracking tool. Once the password is obtained the attacker may or may not change the system files and its operations. Until the attack is discovered by the user, the attacker is using the information of the system in a passive way. Hence it can be termed under passive attacks. Detection of passive attacks is quite difficult since, there would be no traces of any alteration in the normal working of the system and its networks.

Copyrights © 2019 - Imran Hossain, All Rights Reserved.

Blocked IP:



Access to 192.168.1.181 was denied

You don't have authorization to view this page.

HTTP ERROR 403

VI. Conclusion

the project on Identification and Prevention for Brute Force Attacks presents a more accurate, comprehensive, and proactive approach compared to traditional processes. By leveraging machine learning, advanced analytics, and preventive measures, it offers improved detection rates, faster response times, and enhanced security against brute force attacks. This project's implementation has the potential to significantly improve the resilience of systems and networks, offering solid defense against one of the most prevalent and persistent threats to cybersecurity.

VII. REFERENCES

[1]. Bonjak, L.; J Sreš; B Brumen "Animal power and word reference assault on hashed genuine passwords" ,2018 41st Worldwide Show on Data and Correspondence Innovation, Hardware and Microelectronics (MIPRO) pp 1161-1167.

[2]. Diego Garcia; Franklin Mayorga; Vargas, Javier; Renato toasa; David Guevara, "The use of anonymous communication in electronic government services: in the prevention of passive attacks on a network," Proceedings of the 2018 13th Iberian Conference of Information Systems and Technologies (CISTI), pages one through four.

[3]. Stiawan, D. S. Sandra; E. Alzahrani; R. Budiarto, "Comparative analysis of the K-Means method and the Naive Bayes method for brute force attack visualization," ICACC 2017, pp. 177-182, 2017.

[4]. Kinam Park; Song of Youngrok; "Classification of Attack Types for Intrusion Detection Systems Using a Machine Learning Algorithm," Yun-Gyung Cheong, pages 282-286, 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService).

[5]. Aung Yi Yi; MyatMyat Min, "Half breed Interruption Recognition Framework Utilizing K-Means and Characterization and Relapse Trees Calculations" 2018 IEEE sixteenth Global Meeting on Programming Exploration, The board and Applications (SERA), pp 195-199.

[6]. Nabhoneil Chattopadhyay; Souvik Bhattacharya; Rahul Ghosh ; Abhillash Paal , "Information

Interruption Discovery with essential Python coding and anticipation of other meddlesome appearance by the utilization of interruption application" , 2018 IEEE 9thAnnual InformationTechnology, Hardware and Portable Correspondence Meeting (IEMCON), pp 1094-1100

[7]. Wahal Mrinal; Choudhury, Tanupriya; Manik Arora , "Interruption Identification Framework in Python" , 2018 eighth Worldwide Meeting on Distributed computing, Information Science and Designing (Conjunction) , pp 348-353

[8]. The Maulana Ridho Arifianto; Sukarno's Parman; ErwidMusthofaJadied, "An SSH Honeypot Architecture Using Port Knocking and Intrusion Detection System," in Proceedings of the 2018 6th International Conference on Information and Communication Technology (ICoICT), pages 409-415

[9]. “An improved Linux firewall using a hybrid frame of network,” Nivedita and Rakesh Kumar, 2017 International Conference on Trends in Electronics and Informatics (ICEI), pages 657-662.

Cite this article as :

Veluru Jogi Reddy, Mr. S. Suresh, "Identification and Prevention for Brute Force Attack", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 4, pp.140-145, July-August-2023.