ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume2 Issue 8 August, 2013 Page No. 2541-2543

BRUTE FORCE ATTACK – BLOCKING TECHNIQUES

G. Sowmya, A. Naveen Kumar,
Asst. Prof, Department of CSE, Marri Laxman Reddy Institute of Technology Dhundigal, Hyderabad.
Asst. Prof Department of MCA, Jaya Prakash Narayan College of Engineering, Mahabubnagar.

Abstract

A common threat Web developers face is a password-guessing attack known as a brute-force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. If your Web site requires user authentication, you are a good target for a brute-force attack. An attacker can always discover a password through a brute-force attack, but the downside is that it could take years to find it. Depending on the password's length and complexity, there could be trillions of possible combinations. To speed things up a bit, a brute-force attack could start with dictionary words or slightly modified dictionary words because most people will use those rather than a completely random password. These attacks are called dictionary attacks or hybrid brute-force attacks. Brute-force attacks put user accounts at risk and flood your site with unnecessary traffic. Hackers launch brute-force attacks using widely available tools that utilize wordlists and smart rule set to intelligently and automatically guess user passwords. Although such attacks are easy to detect, they are not so easy to prevent

Keywords - Brute Force attack, Dictionary attacks, Hybrid Brute Force attacks

1. INTRODUCTION

A common threat Web developers face is a password-guessing attack known as a *brute-force* attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. If your Web site requires user authentication, you are a good target for a brute-force attack.

An attacker can always discover a password through a brute-force attack, but the downside is that it could take years to find it. Depending on the password's length and complexity, there could be trillions of possible combinations. To speed things up a bit, a brute-force attack could start with dictionary words or slightly modified dictionary words because most people will use those rather than a completely random password. These attacks are called dictionary attacks or hybrid brute-force attacks. Brute-force attacks put user accounts at risk and flood your site with unnecessary traffic.

Hackers launch brute-force attacks using widely available tools that utilize wordlists and smart rule set to intelligently and automatically guess user passwords. Although such attacks are easy to detect, they are not so easy to prevent

2. EXISTING SYSTEM

The present methods for blocking brute force attacks have some limitations. As in Locking of accounts has Denial of Service problem. Captcha has automated tools and also captcha cracker problem and so on. We have overcome those limitations.

3. PROPOSED SYSTEM

. In this project we have designed some methods which helps in blocking these brute force attacks. No System in this world is completely secure and also *internet* was not built keeping *security* in mind, but it was built keeping *functionality* as its target. So in our work we have tried to make the attackers work more difficult with our methods. The different methods used are Locking of Accounts, Time bound login, Query-based Authentication, One time password authentication,

4. IMPLEMENTATION

a) Working Principle of Blocking of Brute Force Attack

In this first we need to login by entering id and password and it will check the password by using different techniques which will block the account.

b) Locking of Accounts

The most obvious way to block brute-force attacks is to simply lock out accounts after a defined number of incorrect password attempts. Account lockouts can last a specific duration, such as one hour, or the accounts could remain locked until manually unlocked by an administrator. However, account lockout is not always the best solution, because someone could easily abuse the security measure and lock out hundreds of user accounts. In fact, some Web sites experience so many attacks that they are unable to enforce a lockout policy because they would constantly be unlocking customer accounts.

c) Time bound Login

In this method, the user will be given a choice to choose the time slot to access the services. So he can use the services in that time slot only.

d) Query - Based Authentication

In this method, the user will be provided with some queries after he has logged in. The user has to answer those queries correctly in-order to access his services. He will be given the queries until he answers them correctly. This is called Query-Based Authentication

e) One-Time Password Authentication

The purpose of a *one-time password* (OTP) is to make it more difficult to gain unauthorized access to restricted resources, like a computer account. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the password, as is done with a one-time password, this risk can be greatly reduced.

f) Using CAPTCHA.

A completely automated public Turing test to tell computers and humans apart, or CAPTCHA, is a program that allows you to distinguish between humans and computers. First widely used by Alta Vista to prevent automated search submissions, CAPTCHAs are particularly effective in stopping any kind of automated abuse, including brute-force attacks. They work by presenting some test that is easy for humans to pass but difficult for computers to pass; therefore, they can conclude with some certainty whether there is a human on the other end.

g) Unique IP address Login

For advanced users it is a best technique to login using a unique IP-address. In this method each user has to login through the IP address with which he is registered.

5. RESULTS

The implementation can be shown in a stand alone system (OS: Windows XP) where a comparator is used to compare the entered values with the stored values.

The user needs to enter the id and password to access their account. If any unauthorized person wants to access the account they may follow some Brute force attacks to get the password. In this approach we can use some

blocking methods to overcome the Brute Force attacks.

The attack information can be viewed in stand alone system by valid login.

6. CONCLUSIONS

In this paper we have presented a system with high security by providing blocking methods to overcome the Brute Force attacks. By this approach the hackers cannot access the user's accounts. In the Existing system have some limitations. As in Locking of Accounts has Denial of Service problem. In this project we have designed some methods which helps in blocking these brute force attacks. No System in this world is completely secure and also *internet* was not built keeping *security* in mind, but it was built keeping *functionality* as its target. So in our work we have tried to make the attackers work more difficult with our methods. My paper shows different methods namely Locking of Accounts, Time bound login, Using CAPTCHA, Unique IP address Login, One time password authentication, Query based authentication are used to block the accounts which will provide high security.

ACKNOWLEDGEMENT

The authors express their deep gratitude to the Principal and the Management members of JPNCE for their encouragement and extensive support in preparing and publishing of this paper.

REFERENCES

[1] *Hacking the code by Mark Burnett*

[2] *Computer Networks by Andrew.S.Tanenbaum*

[3] *CERT Coordination Center, "Trends in Denial of Service Attack Technology," October-2001*

[4] *J.D. Howard, "An analysis of security incidents on the Internet," PhD thesis, Carnegie Mellon University, August 1998*

[5] Electronic Frontier Foundation (1998). *Cracking DES - Secrets of Encryption Research, Wiretap Politics & Chip Design*. O'reilly & Associates Inc. ISBN 1-56592-520-3.

[6] Blaze, Diffie, Rivest, Schneier, Shimomura, Thompson & Wiener (1996). *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*

[7] K. Kendall. "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems." Master's Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1998.

[8] Eli Biham and Adi Shamir (1991). "*Differential cryptanalysis of DES-like cryptosystems*". Journal of Cryptology.

G.SOWMYA, **Working as Asst.Prof(CSE)** in MLR Institutte of Technology, Dhunidigal,Hyderabad. Her areas of Interest are in Web based projects.

A.NAVEEN KUMAR, Working as Asst.Prof(MCA) in Jayaprakash Narayan College of Engineering, Mahabubnagar, His are of interests are in Web based projects