IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10219

Malicious User Detection Using Honeyword and Honeypot

Unnimaya V. S[1], Jasmine Jose[2]

MSc Scholar, Department of Computer Science, St. Joseph's College(Autonomous), Irinjalakuda, India[1]

Assistant Professor, Department of Computer Science, St. Joseph's College(Autonomous), Irinjalakuda, India[2]

Abstract: In today's world the important security threat is the disclosure of password files. To prevent such password file breaches, the Honeyword mechanism is introduced. Honeywords are decoy or fake passwords and it is a set of words which are very similar to the real passwords that is submitted by the user for a particular account. For every user's account, the set of Honeywords are generated. Thus, the attacker get confused to detect the real passwords and Honeywords. The Honeyword concept was introduced to detect the failure and an unauthorized access. The mechanism of Honeypot is basically introduced for confusing the attacker and making difficult to distinguish between the actual data from the decoy data. Through this we can collect the attacker's details without knowing them. Fake or decoy files are made available only when unauthorized access is detected by the Honeyword generation mechanism.

Keywords: Honeyword, Honeypot, SIM Blocking, Decoy data, Intruder.

I.INTRODUCTION

Computer Security is the process of prevention and detection of unauthorized access of a system. For ensuring the security of a system. Everywhere, the system has become an important part of day- to- day life. The all relevant data is stored on the system. So it is very necessary that the system should be secure enough to store the important data and files. We uses authentication based on password for ensuring the security of our data. So it is important that our passwords must be protected to avoid the attacks. Password protection helps us to protect our sensitive information from unauthorized users. Reveling of password files is a serious security problem which is faced by many organizations in our current society. In today's world, it is easy for an intruder to get the username and password by using different cracking techniques. So we have to protect our passwords safe and secure and we have to use different hashing techniques to encrypt our passwords. So to avoid such a situation and related issues, Honeyword concept was introduced. Honeywords are decoy passwords which will make the attackers confused to detect the original password. The Honeypot is another concept which is a decoy mechanism which helps to trap the attackers and collect their information without their knowledge. For every single user false login attempts with few passwords will generate a honeypot accounts also called decoy pages (fake accounts) so that the malicious behavior is caught. The honeyword concept is used to detect an intruder who attempts to login with cracked passwords. The concept is that for each user account, a set of honeywords (false passwords) are generated with the actual passwords. When an intruder tries to get access using any of the honeyword a notification is produced which notifies the actual user about the password file breach. The aim of this study is to validate whether the data access is authorized or not and the abnormal access is detected. Confusing the attacker with decoy data which is called the honeypot protect against the misuse of user's real data. So that the concept of honeypot secures the data of actual user. Here we also introduce the concept of SIM number blocking which helps to keep track of the intruder and block them which helps to avoid the gain access to the account.

II.HONEYWORDS

Honeywords are decoy passwords or false passwords. For each account, the actual password is stored a set of honeywords. If the intruder selects the honeyword and try to login to the account, it will generate a notification to the user about unauthorized access. Honeyword is a useful technique to avoid unauthorized access.

A. ADVANTAGES OF HONEYWORDS

- **Make attacker get confused:** These are the fake passwords which is very similar to original passwords. So that the attacker get confused to detect the actual password from the set of honeywords.
- **Security:** Generating honeywords provide more security to the actual password.

III.HONEYPOT

A Honeypot is actually a logic which is used to attract and trap people who is try to login to the system using honeywords. It contains some data which is originally some decoy data and it will looks like original page and the attacker's details are collected without knowing them. The aim of honeypot is to detect and learn from attacks and use that information to improve security of the system.

A. ADVANTAGES OF HONEYPOT

- **Simplicity:** Honeypot is very simple and flexible and no need of complicated algorithms.
- **Discover details**: It will collect the details of the attackers without knowing them.

IV.PROPOSED MODEL

Here, we use honeyword mechanism to prevent access of malicious user and confusing and preventing them from using the actual data from the fake, worthless data. Here, we use well established method of honeyword generation and have used the logic of random number generation for honeywords and MD5 algorithm for hashing. The attempted use of honeyword for login will generate a notification through email to the actual (registered) user and the intruder lead to a decoy page and their SIM number is tracked and will get blocked which helps in another attempt of unauthorized access using the same number.

A. WORKING PRINCIPLE

- Registration

Here, user who has the authorized access to the system can register into the system. While registration, the user needs to provide his/her details and should create a password for their account. During account creation, for the given password given by the user the system generates honeywords using honeyword generation techniques. The modified honeyword generation technique based on MD5 algorithm but also the random number generation technique will also added more security to the system. The hashes for both honeywords and actual passwords are generated and stored in tables in database. During registration it should be necessary to provide a valid email address.

- Login

The user can login to the system using their username and password. If the user entered the password correctly then he/she can upload their files and other important documents so that the files are stored in cloud safely. The user may make errors while typing password so it will be considered as invalid login attempt. If an attacker enter the honeyword for login, then the system will alert the actual user through email notification about the unauthorized access and the number will get blocked to prevent any other access from the same number. So that there may be given 2 chances and if the attacker exceeds the limit, he will get access but to the decoy file. In the decoy page, he can download the files in which it contains some worthless data and these files will be downloaded only if the attacker give their details in the decoy page. By giving the details of the attacker by themselves, it will be stored in a table in database and can be used for any further legal actions. So this is the decoy page in which the honeypot concept is introduced. Honeypot concept is that we collect the details of the attacker or the hacker without their knowledge.

- File Upload

Here, when the user login into the system using correct username and password, they can upload their files and important documents and can view and download the files that they uploaded. While uploading their files first time, they have to make a secondary password to provide more security to their files and documents. After that they need to be login for uploading and downloading their files.

- SIM Number Blocking

While login, when the attacker uses honeywords and enter into the decoy page the SIM number of the attacker will be tracked and get blocked automatically. So that the attacker cannot use that number for login into the system the second time.

B. HONEYWORD GENERATION

The proposed system uses the Message Digest Algorithm 5 (MD5) and the logic of random number generation. Here, the user register with username, passwords and other details. The original password is taken and using the MD5 algorithm the password is encrypted and hashed using random number generator algorithm. Using the algorithm, the similar honeywords are generated and hashed using the random number generator algorithm. The actual passwords and the set of honeywords are stored together in a table in database. Using this method for hashing, it will be difficult to distinguish between actual password and honeyword.

V.CONCLUSION

Password security is one of the main area which needs more focus. So we know the need of a strong data security strategy to protect ourselves and our data files from various threats and attackers. So that for entry into a system it requires username and password. So we have to ensure the security of our password. So to improve the password security, the honeyword concept is introduced. So in honeyword system, it is sure that the attacker will be detected. The detected one will be trapped with the help of honeypot concept which collects the related data of the intruder and blocks them. This completely different technique will protects against the exploitation of user’s real data. So that the system will validate whether the data access is authorized or not and give more security to our system.

REFERENCES

[1]. http://www.ijritcc.org/download/conferences/ICEMTE_2017/Track_1_(CSE)/1487792121_22-02-2017.pdf
[2]. https://seguranca-informatica.pt/detecting-data-breaches-with-honeywords/
[3]. https://www.researchgate.net/publication/262251991_Honeywords_Making_password-cracking_detectable
[4]. https://www.irjet.net/archives/V2/i8/IRJET-V2I8234.pdf
[5]. https://www.researchgate.net/publication/338795732_Malware_Detection_Using_Honeypot_and_Machine_Learning#:~:text=Honeypot%20can%20be%20used%20as,a%20solution%20to%20detect%20malware.
[6]. https://ieeexplore.ieee.org/document/8965419
[7]. https://www.ijtra.com/special-issue-download.php?paper=intrusion-detection-using-honeypots-and-honeywords
[8]. https://seguranca-informatica.pt/detecting-data-breaches-with-honeywords/
[9]. http://ijaerd.com/papers/finished_papers/Honeyword-Achiving%20secure%20Passwords%20using%20HoneyEncryption-IJAERDV03I1152040.pdf
[10]. https://www.researchgate.net/publication/262251991_Honeywords_Making_password-cracking_detectable
[11]. https://www.semanticscholar.org/paper/Malicious-user-detection-using-honeyword-and-IP-Ms/d33621d0ff4e43e249be02d5efdd180b1e2a2bf9