International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Special, Issue 43 (March 2017), PP. 90-93

INTRUSION DETECTION USING HONEYPOTS AND HONEYWORDS

[1] Omkar Madhavi, [2]Avdhut Nalawade, [3]Tejas Nagpure, [4]Bharati Kavitake
[1,2,3,4] Computer Science Department, Mumbai University
Terna Engineering College, Nerul, Navi Mumbai, India
[1]omi_omkar@yahoo.com, [2]avsnalawade31@gmail.com, [3]tejas1805nagpure@gmail.com, [4]bhartikavitake4@gmail.com

***Abstract*— Honeypots are the important tools for the network and system security as well as for computer forensics investigations.. They are helpful for detecting any ntrusions in a system, as well as gathering the informations about the attacker like, source, attack patterns, final targets and purpose. Honeypots are most useful, since they reveal a lot of information about intruders' behaviours and skills. Honeynet is an integration of various honeypots. They help in further deceiving the intruders. Accordingly, we describe architecture for honeypot system aiming to detect password cracking by means of honeywords and also detecting the intruder's activities.**

***Index Terms*— Intruders, Honeypots, Honeywords, forensics, password cracking .**

I. INTRODUCTION

An ID (Intrusion Detection System) detects the unwanted manipulation to the computer network in a system. An intrusion detection system is used to detect various malicious attacks, actions, alterations, fraudulent logins etc.[1].

In today's world more number of hackers are present and the computer and data are insecure from all directions. Moreover, most of these people feel as though the hackers will never fall victims to such crimes [2]. But there are some new inventions and technologies that allow users to set traps for attackers or hackers and also virtually fight back [1]. This is known as honeypots which are used to set traps for intruders.

For every web applications, in authentication process, password become the most important aspect for login. But usually users choose weak passwords which can be accessed by brute forve attacks, sql injection etc. [1]. An attacker can recover a users password using brute force attack on hashed passwords. So honeywords are defense against the stolen or hacked files.[3].

Honeypot consist of a computer, data or a network site that seems to be a part of network but actually it is not .It is an isolated ,protected and monitored terminal which seems to have valuable information for the attackers Honeywords are defense against stolen password files to deceive attackers. [5].

Honeypots can be defined in three layered networks:

• Prevention: Honeypots can be used to reduce the automated attacks.

• Detection: It is used to detect unauthorized activity acts and unknown activities.

• Response: Production type can be used to respond to a attack through break-in [4].

A. Aim & Objectives:-

Password hijacking attacks are an extremely common and dangerous threat on the Internet, due to the large number of networked systems and services that share the same users' credentials and passwords. Honeypot attracts intruders to acquire valuable information regarding previously unknown vulnerabilities, new attacks' dynamics [3].

The honeypot technology can be combined with honeywords for creating fake accounts and raising the aforementioned alarms when an attacker is attempting to log in by using an inverted stolen password. Honeypot is not a traditional defense framework whose goal is to improve the security of a computer network .[7]

An attacker who steals a file of hashed passwords and converts the hashed functions cannot tell if he has found the password or a honeyword . The honey checker can difference between the user password from honeywords for login routine, and set off alarm if honeyword is submitted.

Clearly, when used for the aforementioned password attack detection purpose, the honeypot should offer to the attacker a perfect imitation of a real system so that it cannot distinguish real authentication credentials from fake ones, and hence cannot avoid detection. In addition, by providing the illusion of a genuine compromised system, the honeypot is able to track the user activity for a certain time as well as its origin on the network, so that an effective reaction is possible, also against sophisticated hacker organizations, giving the chance to prevent future outbreaks.

In particular, the proposed architecture aims at detecting password-cracking attacks by means of honeywords and, moreover at collecting plenty of information about the attacker's activity by featuring a fake, persistent login session leveraging container-based virtualization [7].

B. Motivation:

Intrusion has become common in all the domains of the technology. The most common attacks that have been done on a network caused damaged too many servers of the organizations. Different attacks are done by first fingerprinting on the web servers due to which the information of the organization is leaked and therefore to

prevent this step has to be taken which will not only help to stop this attack but also to analyse type of attack for further security.

OWASP (Open Web Application Security Project) is a project which surveys Organization of report of different intrusion attacks done on the servers and they find the top ten most powerful attacks which has caused more damage to the organization. The injection attacks are the most damaging attack on the OWASP list [10].

C. Organization of report:

Rest of the report is organized as follows. Chapter 2 describes honeypots and honeywords from a security perspective. It includes notes on recent works on security assessment of Honeywords. Chapter 3 describes the problem and the methodology used in honeypot and honeywords system. In Chapter 4 the analysis of risks and specification requirements for the system is given. Chapter 5 provides the implementation of the framework and it also describes the performance of the framework. Chapter 6 provides concluding remarks.

II. LITERATURE SURVEY

Compared with traditional password based authentication methods and systems, Honeywords can be utilized to show better results and opportunity to recognize the threats and intruders.

A. The Dangers of Weak Hashes.

K. Brown in 2012 discussed that damage caused by password leak can be minimized by some practices. Secure system should not have vulnerabilities which may allow hashed passwords altered by the attackers. In this paper it is discussed about best practices to avoid attacks followed while password storage [3].

B. Honeywords: Making Password-Cracking Detectable.

Juels and Rivest in 2013 improving the security of hash functions. To improve the security of the hashed password, honeywords (false passwords) needs to be generated for each user account. An attacker steals the file of hashed passwords and inverts hash function cannot tell if he has found the password. If the attacker attempts to login with honeyword the auxiliary server will set off an alarm. When honeywords are used a successful brute-force password break does not give confidence that he can log in successfully without detection. Proposed system includes honeyword generation algorithms and comparison with different factors [3].

C. Guess again: Measuring password strength by using password-cracking methods.

In this study in 2012 authors understood the effects of password generation methods on guessing ability of passwords. Text based passwords are the leading authentication methods used in any computer systems, in spite of being advanced to perform password cracking. based passwords is the leading authentication method. Considering this threat, password composition methods are becoming complex day-by-day. But, there is less research work defining the metrics to outline password strength. In this paper a new, efficient technique for calculating the password strength which can be implemented for a variety of password-guessing algorithms and tuned using a variety of training sets to gain insight into the comparative guess resistance of different sets of passwords is introduced [3].

D. Achieving Flatness: Selecting the Honeywords from Existing User Passwords.

The system proposed in this paper works on the issue to overcome the security problems. A new honeyword generation algorithm which shows better result and DOS resistance. It selects the honeywords from existing user passwords in which provides realistic honeywords and reduces cost of honeyword scheme [3].

III. METHODOLOGY

A. Limitations of existing system:

The existing system is protected using firewall, but there are some scans that are done by the intruders. These scans are known as fingerprinting. The intruders can intrude into our network using the information gained by fingerprinting. Hence it is necessary to hide such information from the attackers which the existing system fails to do so.

SQL injection and other password cracking attacks are not detectable to the system. This can cause the damage to the network system. Hence there is a need to create a solution for above problems.

B. Problem Statement:

In the era of information and technology network security has become an basic issue in any organizations networks. Honeypots are combined in network with firewall and Intrusion detection system to provide secured platform to an organization [1]. Firewall provide filtering and generates log files to analyse whenever further any malicious activity or violation policeis. Intrusions detection system will silently monitor the system and tell us about the type of intruder in a system. A number of issues were with IDS too as facing with an increasing number of false negatives and false positives. Honeypots then introduced in the network to utilize the network's unused IPs and the attacker's behaviour is analysed on these honeypots. Honeypots improve IDS too by decreasing the numbers of false positives [3].

Password hijacking attacks are an extremely common and dangerous threat on the Internet. Detecting and avoiding any kind of malicious activity based on previously obtained sets of passwords is very difficult. There is a need for a mechanism which will help in avoiding such attacks. In some cases a sophisticated attacker may steal some of the password files which are used for authentication. In such cases attacker could find the password for a user using

offline brute force [7]. This brings in the need for a mechanism which will fool the attacker. Honeywords, Honeycheckers and Honey files can be used to do the job for us.

C. Scope of Project:

The trend of using honeypot is very traditional in network security. It has become necessity of the security for information to lure attackers to some other fake sites in the network than the actual site, where real resources of information are available. Even these honeypots could be extended to a concept called "honeynets", where attacker deals with te bunch of honeypots. The log files analysed through these honeypots and honeynets could be used to enhance Intrusion Detection system to make it smarter in catching the intrusions. Honeypot is most popular and widely used because of its ease of deployment but there are some disadvantage like it may not detect all the attacks and gathers limited information only. Whereas high-interaction honeypot is complex to manage and deploy but gathers more precise details. Future challenge will be combining both types of Honeypot and design a hybrid kind of Honeypot which will have advantages of both the approaches. This can have moderate complexity and it should obtain more precise information of the intruder [2].

IV. SOFTWARE ARCHITECTURE:

A. HONEYPOTS:

We propose a distributed honeypot system approach which is independent of the centralized control and information can be traced automatically about the source of attack. This helps in providing better security, better durability, independent of the underlying honeypot network and the centralized control. Honeypots can be logically classified into low-interaction and high interaction ones.

1) Low-interaction:

A typical low-interaction honeypot is also known as a Gen1 honeypot. This is a simple system which is very effective against automated attacks or beginner level attacks. Honeyd is one such Gen1 honeypot which enhances services and their responses for typical network functions from a single machine, while at same time making the intruder believe that there are numerous different operating systems. [1][4].

2) High-interaction:

A typical high-interaction honeypot consists of following elements: resource of interest, data control, capturing data and external logs. They provide a better data capture and control mechanisms. They are more complex as compared to the low interaction honeypots. With the help of them we can collect in-depth information about the procedures of an attack. They are useful to identify vulnerable services for any operating system.[1][4].

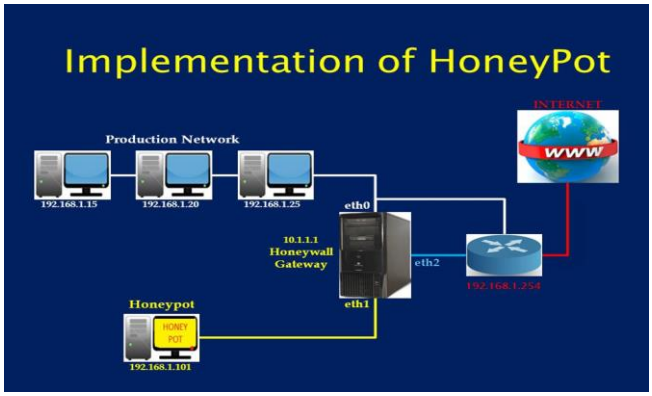

Fig.1-Implementation of Honeypot

As shown in Fig.1, when server receives a request, first it bypasses the firewall. If the request is found to be taking server information the honey checker redirects the request to a honeypot. This helps in hiding the server information from the intruders. If the request is legitimate then the request is send to the server to provide the required services.

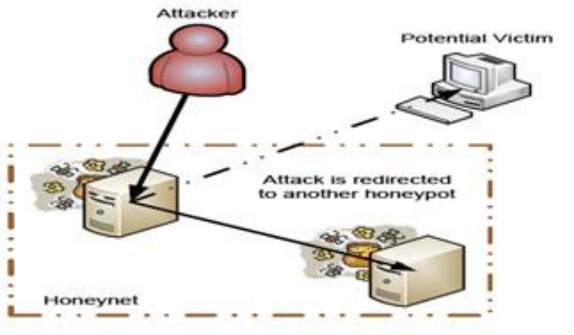

Fig.2 Honeynet

Honeynet as shown in Fig.2 is a concept in which the attacker realizes that they have been redirected to one of the honeypot. In this scenario, the user can cancel the current session and start a new one. By the information gathered in the previous session, the user machine is redirected to another honeypot. Thus, a mesh is created and the attacker is trapped in the created net.

B. HONEYWORDS:

Password hijacking attacks are an extremely common and dangerous threat on the Internet, due to the large number of networked systems and services that share the same users' credentials and passwords. Username is useful to find the particular user and the password for the authorization of the user. The username-password checking is more important in the security system, so to protect password from third party we implement honeywords concept. In honeyword system we are creating honeywords i.e. multiple fake password and username for the single user. New password is the combination of existing user passwords called honeywords .Moreover, entering with a honeyword to login will trigger an alarm inform the administrator about a password file an

infraction, so we introduce a easy and capable, solution to the detection of password file exposure events.

1) For creating Honeywords:-

Chaffing-by-tweaking:-

- In this algorithm username and password is separated by character and digit.
- For that specific character and digit we generate random value using random function.
- After creating random character we merge them in single password and username and store it on database using hash value so it can't be modify by attacker.
- E.g.:- Username :- avdhut12 Password:-Avdhut345
- For username:- char- avdh digit-12 randomchar: pqrs randomdigit:89

New Username:pqrs89

For Password:- char : Avdh digit-345 randomchar-Dqpe randomdigit-890

New Password: Dqpe890

2) Procedure:-

1) First user register from registration from and enter his user name and password along with that at that time data is store on database and simultaneously on a excel file.

2) After first stage data is deleted from database and file is also deleted from database and from local machine.

3) Before deleting file from server a system admin will fetch all the data from file and store in it new database.

4) After inserting data in new database by chaffing by tweaking algorithm generates a honeywords.

5) This honeyword will insert in first register database and also creating lots of fake database and inserting honeywords in them.

C. Login Procedure

For login procedure we have to consider both real user and attacker. To prevent attacker from getting access we make some extra database and insert honeywords into them. When user enter his credentials its check in each hoenywords database. If that credentials present in that honeywords then user gets block and that user throw in honeypot system to capture his next activities. If user is real user then his credentials bypass all honeywords and check that user in real database. If his credentials is correct then system will give access.

V. HONEYWORDS AND HONEYPOT INTEGRATION

We are integrating both system in such way that it will reduce cost of system and will provide better security for database. When attacker attack on hoeyword system at that time honeypot will catch that attacker but to catch a attacker some time is required so for that we made lots of database so attacker will confuse where is actual data is store and which one is actual database. When attacker checking this all database then attacker's activities will trace by the honeypot and attacker is caught by the honeypot. If attacker again change the session and try to login then attacker will be in honeynet system.

A. PHP File encryption

To provide security for source code that will written by Developer we used PHP FILE ENCRYPTION tool that will encrypt the php source code and store it.

CONCULUSTION

We present an approach where business data and personal data can be secured. We propose a monitoring of a person or intruder, also its illegal actions performed on any system are seen. Decoy documents stored in a system containing user's real data serve as sensors to detect an unauthorised access. Once the data gathered is suspected and later verified, we can block the malicious insider with fake information in order to dilute the user's real data. Such methods can be used to reduce the number of hacks and also provide security at social level.

In future we would like to refine our model by involving hybrid hash algorithm to make the inversion process more harder, where the chances of attackers to hack or attack on any system gets reduced. The admin keeps the data of the tracked IP's with them and use them to block access on their network. Use of honeywords is very useful and can be used by any user account .By developing such methods two objectives can be maintained-Total efforts for getting plaintext passwords and hashed list and detecting password disclosure.

REFERENCES

[1] Luigi Catuogno, Aniello Castiglione, Francesco Palmieri "A Honeypot system with Honeyword-driven Fake interactive Sessions".

[2] Imran Erguler," Achieving Flatness: Selecting the Honeywords from Existing User Passwords", DOI 10.1109/TDSC.2015.2406707, IEEE Transactions on Dependable and Secure Computing.

[3] Generating Honeywords from Real Passwords with Decoy Mechanism.

[4] http://en.wikipedia.org/wiki/Honeypot

[5] [5]https://it.slashdot.org/story/13/05/08/1948251/honeywords-honeypot-passwords

[6] A practical guide to Honeypots http://www.cs.wustl.edu

[7] L. Spitzner, Honeypots: definitions and value of honeypots

[8] I. Koniaris, G. Papadimitriou, and P. Nicopolitidis, "Analysis and visualization of SSH attacks using honeypots," in EUROCON, 2013 IEEE. IEEE

[9] Honeywords: Making Password-Cracking Detectable - Ari Juels

[10] https://www.owasp.org.