Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.60 – 65

RESEARCH ARTICLE

Honey Trap Security Server: An Efficient Approach of Securing E-Banking Network

Ashwini Gabhane[1], Kiran Bansule[2], Pradnya Kedar[3], Lekha Gahukar[4], Swati Sahare[5], Ketki Bhakare[6]

[1]Student, CSE & RTMNU, India
[2]Student, CSE & RTMNU, India
[3]Student, CSE & RTMNU, India
[4]Student, CSE & RTMNU, India
[5]Student, CSE & RTMNU, India
[6]Lecturer, CSE & RTMNU, India

[1] gabhaneaashwini2gmail.com; [2] kiranbansule12@gmail.com; [3] pkedar@yahoo.com;
[4] lekha.gahukar@gmail.com; [5] swatisahare86@gmail.com; [6] ketki.bhakare@gmail.com

Abstract— This paper presents a new way for securing an account. The Honey trap Security Server is use to secure an account from an attacker, intruder, hackers and crackers. Honey trap is nothing but "a security resource whose value lies in being probed, attacked or compromised". The honey trap contains no data or applications critical to the company but has enough interesting data to entice a cracker. A Honey trap system should be system to be easier prey for intruders than true production systems but with minor system modifications so that their activity can be logged of traced. An important goal of Honey trap Security Server is to trap an intruder and the methods which are used for intrusion before attacking on real server.

Keywords— Honey trap security system, Intruder, Entice, Hackers, Crackers, Attacker, Security for E-Banking, Intrusion detection system

I. INTRODUCTION

Most of the websites are having security on the basis of username and password. But now a day's the numbers of hacker and cracker are increasing so the security on the basis of username and password is not sufficient. To overcome this problem Network Security provides many techniques and one of the most important techniques is "Honey trap Security Server". Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

In network system, most of the attackers want to attack on user's account and hack an important data of user. In banking system an attacker wants to enter into the users account and hack all information present in account. Honey trap Security server can provide two types of server like real server and fake server. If user can qualify in all three levels then user can enter into real server and if user can disqualify in this levels then user can enter into fake server.

In Honey trap Security Server, the security provides by using three levels i.e. first is login level in which the user can enter the username and password. Second level is psychometric test in which user can enter the answer of security questions and third is CAPTCHA test in this user can enter the text which given in CAPTCHA image. If user can enter into the fake server then ipaddress of a fake user can be send to cyber crime by email. In login test the ipaddress can be traced of each user which can login into account.

The remaining of this paper is organized as follows, section II provides Literature review, section III provides proposed plan on Honey trap security system and section IV provides conclusion.

II. LITERATURE REVIEW

Most type of different algorithms is already define for detecting models have been proposed. The most of the attacks by a hacker would like to attack on the database concerning the username, the password and their respective account numbers. A survey and comparison of this techniques is given in this paper presents.

This paper will present the idea of using web-based technology and integrating it with a client honey pot by building a low interaction client honey pot tool called Honey ware [1]. For the shortcoming of traditional intrusion detection system (IDS) in complex and unknown attack detection. A distributed intrusion detection system based on honey pot was proposed. We make use of honey pot to collect the invasion characteristics on the network, and use the method of unsupervised clustering (UC) and genetic clustering to extract the data for analysis. In addition, in order to improve the detection performance of the IDS, it combined protocol analysis with signature detection modules. Experiments result show that this system can better detect intrusion and improve the overall safety performance of large-scale networks [2].

In this paper, a secure system for banking application using honey pots. Using this system, at least data integrity can be ensured along with monitoring the interaction to detect possible attack [3]. Honey pot technology can proactively detect and respond to the intrusion and the attack of the network. Compared with other security mechanisms, it has the feature of using simply, configurations flexibly, occupying less resource, and working effectively in a complex environment, furthermore, all the collected data and information has a good relevant and study value, so that it can capture and analyse the characteristic, which can effectively limit the spread of the aggressive behaviour on the network[4].

This paper presents a proactive defense scheme based on Honeypot security system (HPSS). We propose an improved approach based on Intruder Detector System (IDS) which enhances the security of cyber. HPSS provide improved attack prevention, detection and reaction information, drawn from the log files and other information captured in the process[5].

III. PROPOSED PLAN

Honey trap Security Server provide the techniques for trap an intruder and the methods of intrusion before hack the information of user's account. The fig. 1 shows architecture of Honey trap Security Server.

A) Architecture

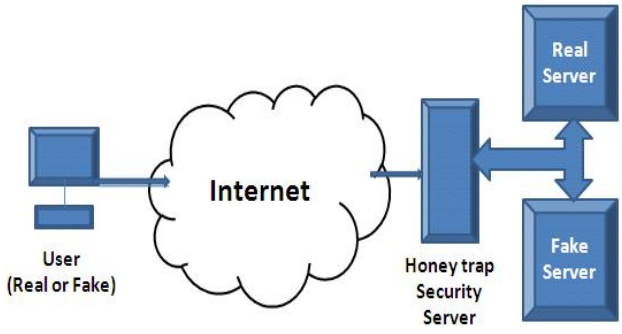

Fig. 1 Architecture of Honey trap Security Server

In the architecture of honey trap security server, the important components are user, system with honey trap and server (real and fake). Honey trap security server contains three levels of security. If user can be fake user then user can enter into fake serer otherwise enter into real server. Figure 1 shows the basic functionality of the honey trap. Honey trap Security Server is based on Intrusion Detection System. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Intrusion detection system is based on

monitoring events and reporting attempts. Intrusion Detection System is also use for identifying an attack and preserving of confidential data. Intrusion detection system is use as a tool for honey trap security server.

B) Working of Honey trap Security Server

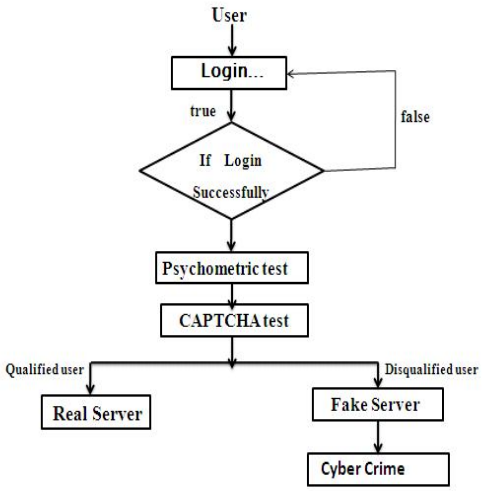

Fig. 2 Flowchart of Honey trap security server

In fig.2, the flowchart of honey trap security can be shown. When user want to login, user can enter username and password in login-id field and password field. After login successfully, user can give the answers of security questions in psychometric test. After psychometric test, user can enter into CAPTCHA test and if user can qualify all this three levels then user can be considered as real user and enter into real server otherwise user can be considered as fake user and enter into fake server.

C) Three levels of Security

1) Login test

In login test, by using username and password, user can enter into next level. If username or password is wrong then user cannot be entered into next step. Here, password can be encrypted by using encryption method. In this level IP address can be tracing by using IP address tracing algorithm. Both login and tracing an IP address can be done on same time. IP address can be trace of each person who want to login may be that person can be fake or real user.

2) Psychometric test

After login successfully, user can enter into second level i.e. Psychometric test level. In this test randomly three questions can be generated and user can only select their right answer from four options. If user can enter right answer then enter into next level but if user can enter wrong answer in first chance then one more chance can be given to an user but in second chance also user cannot given the right answers of three questions then user can be considered as fake user.

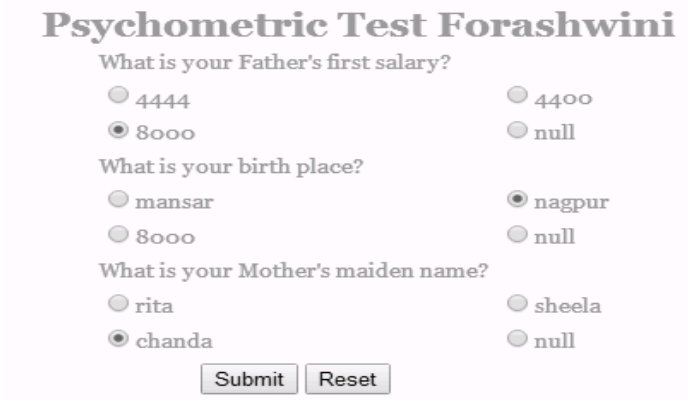

Fig. 3 Psychometric test

Fig. 3 shows example of Psychometric test in which randomly three questions can be generated. For randomly generating this three questions, "math.random" is used where math in predefined file and random is predefined function.

3) CAPTCHA test

CAPTCHA is abbreviated for "completely automated public Turing test to tell computers and humans apart". A common type of CAPTCHA requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Because the test is administered by a computer, in contrast to the standard Turing test that is administered by a human. Fig.4 shows some examples of CAPTCHA.

Fig.4 Examples of CAPTCHA

In this test, user can enter the text given in CAPTCHA image which is combination of alphabets and numbers. If user can enter wrong CAPTCHA in given text field then the new CAPTCHA can be generated. Fig. 5 shows the CAPTCHA test.

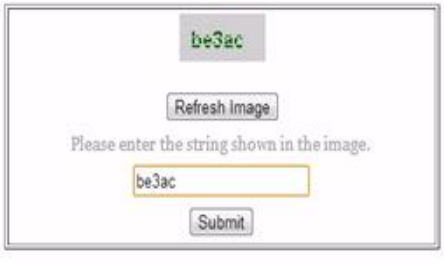

Fig. 5 CAPTCHA test

D) Users of System

1) Administrator

Administrator can checking an authentication of an user, monitoring on the system and if an user can be a fake user then administrator can send its IP address to the cybercrime.

2) Client

Client is a user of the system. Client may be a fake user or real user. The works of real user is enter into the account by passing three levels and then enter into account for performing transactions.

E) Benefits of Honey trap Security Server

1) Leave intruders exposed and isolated from your real network: Intruders can easily trap and enter into fake server so the data or information of real account can be saved from intruders.

2) Be given a valuable lesson on how crackers break into networks: Honey trap security server can save accounts from hackers and crackers and also tell that how to break the hackers and crackers.

3) Honey trap can give you the exactly the information you need in a quick and easy to understand format of an intruder.

4) Simplicity: The very simplicity of design, implementation and use makes a honey trap a desirable method to enhance security conditions in any organization.

IV. CONCLUSIONS

Network Security is very important for providing security to the networks. Network security provide this technique as honey trap security server. Honey trap security server in efficient and simple technique which provide security from hackers, crackers, and intruders. Honey trap security server provide two types of server i.e. fake server for fake user and real server for real user. In this way Honey trap security server can easily trace an ipaddress of an intruder and trap an attacker without knowing to an intruder.

REFERENCES

[1] Yaser Alosefer and Omer Rana, 'Honeyware: a web-based low interaction client honeypot', Third IEEE International Conference on Software Testing, Verification, and Validation Workshops (ICSTW), pp. 410 – 417,2010.

[2] Yun Yang and Jia Mi 'Design and Implementation of Distributed Intrusion Detection System based on Honeypot', 2nd IEEE International Conference on Computer Engineering and Technology (ICCET), vol. 6, pp. V6-260 - V6-263,2010.

[3] Sandeep Chaware 'Banking security using honeypot', IEEE International Journal of security and its Applications, vol. 5 No. 1,2011.

[4] Jian Bao and Chang-peng Ji, and Mo Gao 'Research on network security of defense based on Honeypot', IEEE International Conference on Computer Application and System Modeling (ICCASM), vol. 10, pp. V10-299 - V10-302,2010.

[5] Prajakta Shirbhate, Vaishnavi Dhamankar, Aarti Kshirsagar, Purva Deshpande & Smita Kapse,' Overview of Honeypot Security System for E-Banking', Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1,2010.

[6] Guanlin Chen, Hui Yao and Zebing Wang, 'Research of Wireless Intrusion Prevention Systems based on Plan Recognition and Honeypot', IEEE International Conference on Wireless Communications & Signal Processing (WCSP), pp. 1-5,2009.

[7] Chao-Hsi Yeh and Chung-Huang Yang, 'Design and Implementation of Honeypot Systems Based on Open-Source Software', IEEE International Conference on Intelligence and Security Informatics (ISI), 265-266,2008.

[8] Babak Khosravifar, Maziar Gomrokchi, Jamal Bentahar,'A Multi-Agent-based Approach to Improve Intrusion Detection Systems False Alarm Ratio by Using Honeypot', IEEE International Conference on Advanced Information Networking and Applications Workshops, pp. 97 – 102,2009.

[9] Wei Li-feng, Wang Xiao-bin, 'Research on Honeypot Information Fusion Based on Game Theory', Second IEEE International Conference on Computer Research and Development, pp. 803 – 806.

[10] Xinliang Wang, Fang Liu, LuYing Chen, Zhenming Lei, 'Research for Scan Detection Algorithm of High-Speed Links Based on Honeypot', 2nd IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC), pp. 66-70,2010.

[11] Yun Yang and Jia Mi, 'Design and Implementation of Distributed Intrusion Detection System based on Honeypot', 2nd IEEE International Conference on Computer Engineering and Technology (ICCET), vol. 6, pp. V6-260 - V6-263,2010.

