Undergraduate Academic Research Journal

Volume 1 | Issue 1 Article 23

July 2012

Overview of Honeypot Security System for E-Banking

Prajakta Shirbhate
Department of Computer Technology, YCCE, Nagpur, Maharashtra, India, prajakta.2888@gmail.com

Vaishnavi Dhamankar
Department of Computer Technology, YCCE, Nagpur, Maharashtra, India,
vaishnavi.dhamankar@gmail.com

Aarti Kshirsagar
Department of Computer Technology, YCCE, Nagpur, Maharashtra, India, aartikshirsagar729@gmail.com

Purva Deshpande
Department of Computer Technology, YCCE, Nagpur, Maharashtra, India, purva.13deshpande@gmail.com

Smita Kapse
Department of Computer Technology, YCCE, Nagpur, Maharashtra, India, kawadesmita@gmail.com

Overview of Honeypot Security System for E-Banking

Prajakta Shirbhate, Vaishnavi Dhamankar, Aarti Kshirsagar, Purva Deshpande & Smita Kapse

Department of Computer Technology, YCCE, Nagpur, Maharashtra, India
E-mail : prajakta.2888@gmail.com, vaishnavi.dhamankar@gmail.com, aartikshirsagar729@gmail.com, purva.13deshpande@gmail.com, kawadesmita@gmail.com

Abstract **-** 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. Honeypot security system can be best defined as follows:

"A honeypot is a security resource whose value lies in being probed, attacked or compromised.[1] However, the electronic banking system users still face the security risks with unauthorized access into their banking accounts by non-secure electronic transaction hence it need to build reliable system which holds the identity of both the sender and the receiver."

Keywords **-** *Honeypot security system, Intrusion detection system, Firewall protection, Security for banking services, Decoy system.*

I. INTRODUCTION

Honeypot is an exciting new technology with enormous potential for the security community. It is resource which is intended to be attacked and compromised to gain more information about the attacker and his attack techniques [3]. 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. After acquisition of the same the hackers would very conveniently trespass the security walls of authentication and authorization and thereby making the transaction official [2].

Honey Pots are fake computer systems, setup as a "decoy", that are used to collect data on intruders. A Honey Pot, loaded with fake information, appears to the hacker to be a legitimate machine. While it appears vulnerable to attack, it actually prevents access to valuable data, administrative controls and other computers. Deception defenses can add an unrecognizable layer of protection. As long as the hacker is not scared away, system administrators can now collect data on the identity, access, and compromise methods used by the intruder. The Honey Pot must mimic real systems or the intruder will quickly discover the 'decoy'. Honey Pots are set up to monitor the intruder without risk to production systems or data. If the Honey Pot works as intended, how the intruder probes and exploits the system can now be assessed without detection. The concept of a Honey Pot is to learn from the intruder's actions. This knowledge can now be used to prevent attacks on the "real", or production systems, as well as diverting the resources of the attacker to a the 'decoy' system.[3][4]

The remaining of this paper is organized as follows. Section 2 provides related work, section 3 provides Review on Honeypot security system and section 4 provides conclusion.

II. RELATED WORK

Many different approaches to building detection models have been proposed. A survey and comparison of detection techniques is given in this paper presents an approach for modeling normal sequences using look ahead pairs and contiguous sequences. This paper presents a statistical method to determine sequences which occur more frequently in intrusion data as opposed to normal data. This paper uses neural networks to model normal data and examines unlabeled data for anomaly detection by looking at user profiles and comparing the activity during an intrusion to the activity under normal use [1].

The paper shows following a point which summarizes some key events [5].

In 1997 - Version 0.1 of Fred Cohen's Deception Toolkit was released, one of the first honeypot solutions available to the security community.

In 1999 - Formation of the Honeynet Project and publication of the "Know Your Enemy" series of papers.

This work helped increase awareness and validate the value of honeypots and honeypot technologies.

In 2000/2001 - Use of honeypots to capture and study worm activity. More organizations adopting honeypots for both detecting attacks and for researching new threats.

In 2002 - a honeypot is used to detect and capture in the wild a new and unknown attack.

This paper proposes that any security system can be made more reliable and effective using Honeypot security system because it not only prevent the person illegally accessing accounts but detect him. It also shows the list of attacks and counts the no. of appearances [2]. Same concept is introduced in paper but more it tells that the attack is being done on the dummy database remaining true database unaffected [3].

Some research states that it can be used in military field to detect unknown codes[7] while other paper suggest it can be used in banks and various financial company[10].

III. REVIEW ON HONEYPOT SECURITY SYSTEM

Traditionally, honeypots have been used to detect or capture the activity of outsider or perimeter threats. The purpose of these honeypots varied. Some organizations are interested in learning what threats exist and gaining intelligence on those threats, others want to detect attacks against their perimeter, while others were attempting early warning and prediction of new attack tools, exploits, or malicious code.

A. *Intrusion Detection Honeypot Security System (IDHPSS)*

False positives are a constant challenge for most organizations. But a honey pot is a host that captures unauthorized activity.

The honey pot reduces false negatives by capturing absolutely everything that enters and leaves itself. This means all the activity that is captured is most likely suspect. As to unknown activity, even if Intruder Detection system (IDS) misses it, we have captured the activity. We can review all of the captured activity and identify the attack.

The Architecture of the Intruder Detection Honeypot Security System (IDHPSS) is shown in Figure 1. This figure shows eight essential components of the architecture: “Remote Log Server”, “Sniffer Server”, “Honey Pot”, “IDS”, “WWW Server”, Switch, Router and Fire Wall. “IDS” is the host for intrusion detection and “WWW Server” is the secured host in the network. Switch is used for the Data Control and Router for the Route Control. Another function to set up the Router is to create a network environment that is more realistically mirrors a production network. So the trap of the honey pot is not easy to be found. Traditional IDS is purely defensive. But in IDHPSS, there is enough information about threats that exist. New tools and attack patterns can be discovered. Hence, future compromise can be predicted.

1) *Architecture*

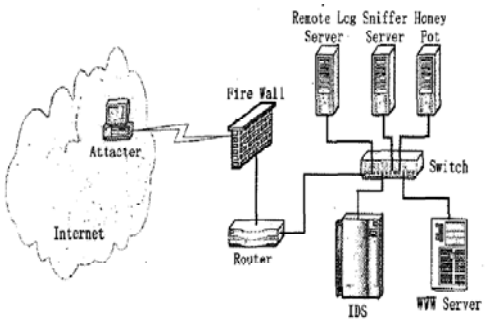

Fig. 1: Architecture of IDHPSS

The honey pot system can cooperate with Fire Wall. The system will refuse the visit of the intruder whose IP address is set in the Fire Wall as blacklist by the honey pot.

By combining data from multiple systems, the attack of the system can be predicted and attacker is sent to Honeypot for further processing.

2) Characteristics in the IDHPSS

The main characteristics that will be achieved in the AAIDHP are flexibility, configurability and security.

- *Flexibility* - Honey pot creates a network environment that more realistically mirrors a production network.
- *Configurability* - IP trap, Data Control and Route Control can be deployed dynamically.
- *Security* - Intruders can be trapped in the honey pot before an attack is made on real assets.

It is obvious that AAIDHP solves the information overload, unknown attacks, false positives and false negatives.

B. *Honeypot security system for E-Banking*

Often most users have a lack of precise information dealing with attacks on the Internet. In most cases, we just see the *results* of attacks against networks *or* specific computers. We do not have precise quantitative predications of attacks against computer systems and the tools, tactics, and motives involved in computer and network attacks are often not known in detail. Following

flowchart shows how system will work according study of proposed system.

Fig. 2: Flowchart of Honeypot security system

Honeypot system secures data and data transmission from being hacked. This system represents fake version of original system. General security system provides denial of services but Honeypot security system allows hackers to enter into fake system which is this honeypot system and gathers the information of the intruder.

There are three layers to gather the information of intruder which includes:

1) IP address tracing:

This step includes the IP address tracing. Once person logins into the system first of all IP address is noted down.

In this, both the IP tracing as well as Login test is performed. If he fails to login for couple of times he will be entered into the fake system. In security systems which are present currently there will be denial of service if a person fails to login for defined iterations.

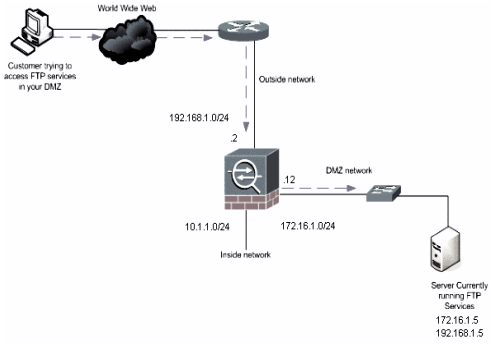

Fig. 3 : IP addressing

2) Psychometric test:

This test is performed to detect that is the person a regular and real customer or a hacker hacking other person's account.

There will be some set of questions which will be asked to the person. The answers to the questions will be known to the actual user only. If the person fails to answer the questions more than two times then he will be transferred into the fake system.

3) Captcha image:

Captcha image is used to check whether the logged person is a person or machine.

Many times it is possible that a person can use software to perform iterations and will get the password. If the password is 6 letters long then there will be 6 loops and by the combination he can get the password.

Hence captcha image phase is used to avoid this type thread. Captcha looks like following:

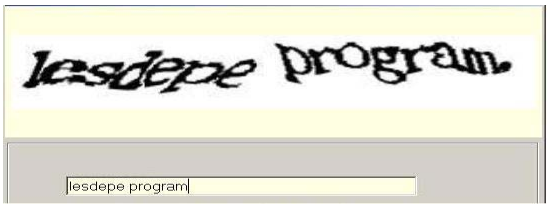

Fig. 4 : Captcha image.

Honeypot security system (HPSS) keep the records of action performed by intruder i.e. which data he is downloading, sites he is visiting. All the interactions and transmissions will be fake but he will think it is taking place actually. Hence, he will be trapped by the system and we will get the information to perform necessary action. By gathering all information about hacker HPSS will make crime report and will send it to the crime branch to perform specific actions according to his crime.

C. *Advantages Of Honey pots*

1) Small Data Sets: Honey pots only collect data while interacting with them. Many organizations logging thousands of alerts a day may log a hundred alerts with honey pots. This makes the data honey pots collect much higher value, easier to manage and simpler to analyze.

2) Reduced False Positives: One of the greatest challenges is the generation of false positives or false alerts. The larger the probability that a security technology produces a false positive the less likely the technology will be deployed. Honey pot security system reduces false positives.

3) Catching False Negatives: Another challenge of traditional technologies is failing to detect unknown attacks. The traditional computer security technologies rely upon known upon statistical detection which also suffers from probabilistic failures. Honey pots on the other hand can easily identify and capture new attacks against them. Any activity with the honeypot is an anomaly, making new or unseen attacks easily standout.

4) Encryption: It does not matter if an attack or malicious activity is encrypted, the honeypot will capture the activity. Honey pots can do this because the encrypted probes and attacks interact with the honeypot as an end point, where the activity is decrypted by the honeypot.

5) Highly Flexible: Honey pots are extremely adaptable, with the ability to be used in a variety of environments, everything from a Social Security Number embedded into a database, to an entire network of computers designed to be broken into.

6) Minimal Resources: Honey pots require minimal resources, even on the largest of networks.

7) Resources: Network Intrusion Detection Devices may not be able to keep up with network activity, dropping packets, and potentially attacks while centralized log servers may not be able to collect all the system events. Honeypots do not have this problem; they only capture that which comes to them [3].

8) Lossless: The Honeypot system creates the environment to attract the intruder and all the transactions and processing done on the system is fake. Hence it does not make any loss to accounts or data which is being hacked [2].

IV. OUTPUT

Until now we have discussed about how honeypot security system works. Following snapshot shows actual implementation of this system developed by us. This snapshot shows three layers of test that we are performing i.e. login, psychometric and capcha image. Also while login IP address is traced as shown.

Fig. : Home page

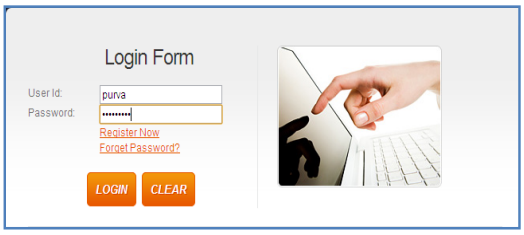

Fig : Login test

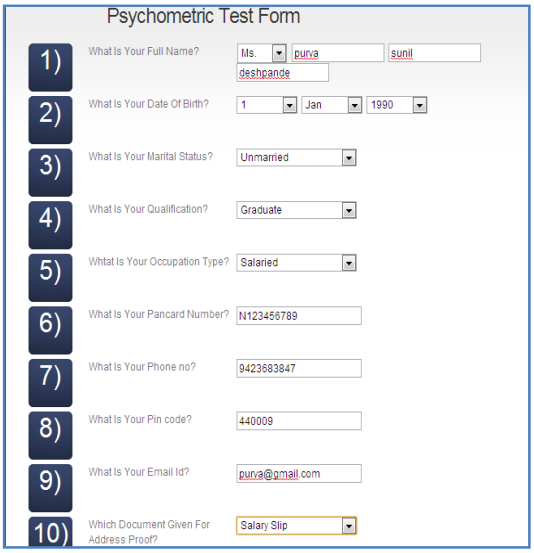

Fig. : Psychometric test

Fig. : Capcha image test

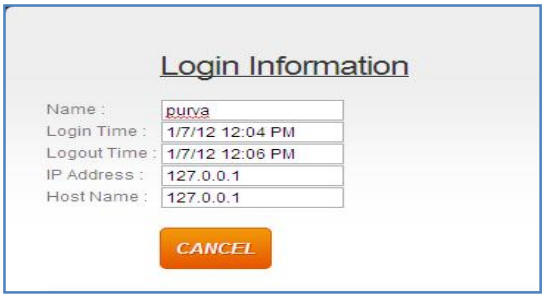

Fig. : IP tracing

After performing these tests user, if he is hacker, will be transferred to fake system and if he is real user, he will be transferred to real banking system.

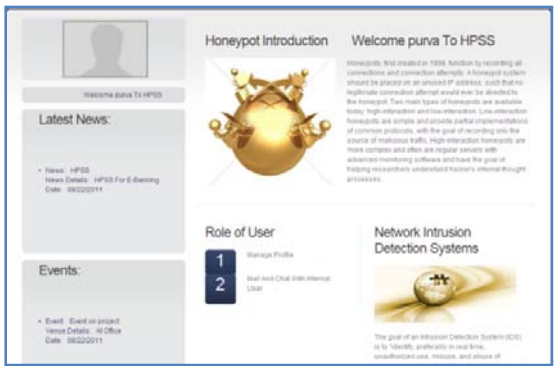

Fig. : Users account

V. CONCLUSION

Network security is a matter of social stability and national security. Honeypots are clearly a useful tool for luring and trapping attackers, capturing information and generating alerts when someone is interacting with them. The activities of attackers provide valuable information for analyzing their attacking techniques and methods. The honey pot system can cooperate with Fire Wall. The system will refuse the visit of the intruder whose IP address is set in the Fire Wall as blacklist by the honeypot. According to the destroy degree, the term of refusing the malicious visit can be short-term or long-term. By combining data from multiple systems, these data can be used for such things as early warning and prediction, statistical analysis, or identification of new tools or trends.

In future Honeypot security system can be used in various banks for their online procedures such as E-banking. It can be used for scientific or government purposes where confidential data is to be remained confidential

REFERENCES

[1] Zhi-hong Tian,Bin-xing Fang, “An Architecture For Intrusion Detection Using Honeypot”, Second international conference on machine learning and cybernetics 2003.

[2] Christian Doring,” Improving network security with honeypot.”

[3] Lanz Spitzner, “Know Your Enemy: Learning with User-Mode Linux Building Virutal Honeynets using UML”

[4] Lanz Spitzner, “Know Your Enemy: GenII Honeynets,”.http://www.honeynet.org,May, 2005.

[5] Lanz Spitzner, “Know Your Enemy: Honeywall CDROM Roo 3rd Generation Technology”, 2005.

[6] Jungsuk SONG-Kyoto University, Hiroki TAKAKURA-Kyoto University, Yasuo OKABE-Kyoto University, Cooperation of Intelligent Honeypots to Detect Unknown Malicious Codes, IEEE, 2008 .

[7] The Government of the Hong Kong Special Administrative Region, “Honeypot security” February 2008.

[8] http://www.seminarprojects.com/Thread-honeypots-seminar-report#ixzz1YOSPf8Ka Cormac Herley and Dinei Florencio, “Protecting Financial Institutions from Brute-Force Attack.

◈◈◈