DYNAMIC HONEYTOKENS

V.Maheswari
Department of Master of Computer Applications
Sathyabama University, Chennai, India – 600 119
Tel: 044-24501644 ext.5216,
maheswarikarthikeyan@hotmail.com

P. E. Sankaranarayanan
Dean, P.G and Research
Sathyabama University, Chennai, India – 600 119
Tel: 044-24501644 ext.5030

Abstract

Honeypot is a program, machine or system, which is used for network security. The basic idea is to deceive the attackers by making the honeypot seem like a legitimate system. It traps attacks, records intrusion information about the activities of hacking process and prevents attacks on the compromised system. Honeytoken is also a type of honeypot but not a computer. It is considered as an entity, which has been mainly used to catch the insider threat. In this paper we have discussed about the various proposals for implementing the dynamic honeytokens. The use of dynamic honeytokens to fool the spammers who try to harvest the email address is discussed here by providing fake email addresses whose access is done through HTML tags.

1. Introduction

When more and more traditional services has become web based and as the Internet usage has also increased, the attacks and intrusion to web application system has also become more and more popular. Honeypot is a valuable security tool to view the intruder's activities. This can be used as a network deception tool that deceives the intruders and records their activities. It can be active or passive in nature [1]. But the firewall and IPS are completely passive in nature. This makes honeypot more useful than other security tools. At the same time industry and academia also show growing interest in honeypot related research activities [2]. Taking into consideration the definition of the honeypot, as defined by [1] *"A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource."* A honeypot is a resource, which is to be attacked by the attackers and not merely a computer. Honeytoken is a variation of honeypot, which is not a computer, but it can be a type of digital entity [3]. Honeytokens can be implemented in any form, shape and size but their basic their functionality is that it is considered as a digital or information system resource whose value lies in the unauthorized use of that resource and hence all the activities can be logged. Honeytokens can be implemented in the form of a bogus login, credit card number, database field or record, Excel spreadsheet and PowerPoint presentation. All the honeytokens have no authorized use and value and hence no one should access it. Hence any access to honeytokens makes it an illegal attempt by the hackers.

Honeytokens are not used to solve specific problems as honeypots, but they are highly flexible and simple tools, which have many applications to security. Honeytokens are primarily used for catching the insider threat where the internal attackers know about the environment and have access to the files and information. This access may not be available for the outside access. Main advantage of using honeytoken is that it is simple, flexible and minimal cost.

2. Related Work

Since the honeytokens are new concept and are in the implementation stage from static honeytokens to dynamic honeytokens. In our earlier work we have developed a platform independent honeypot which implements this feature of honeytoken partially as a database file. This system was used to control and capture the insider threats. Data control and capturing was done by providing fake files to be accessed by the attackers and there by recording their activities [4]. Honeytokens as fake records were inserted in a database, which has been used for catching both insider and outsider threats [6]. Phishing attackers tracking were done by using web bugs and honeytokens. By using web bugs and honeytokens on the fake web site forms the phisher presents, one can log accesses to the honeytokens by the phisher when the attacker views the results of the forms [5]. The various forms of implementing dynamic honeytokens have been discussed in this paper.

3. Dynamic Honeytokens

3.1 spammers and Honeytokens

The primary method used by the spammers is to collect the email addresses as much as possible. They harvest these email addresses using various techniques [7]. They regularly scan the Usenet and collect the mail address. They also gather from the mailing lists, web pages, yellow pages, email address book and many other methods. Harvesting email addresses from the web pages is done by automatic programs which spider through the web pages looking for email addresse [Figure 1]. For each HTML web page found, such a program will check for a mailto: link ("send me an email by clicking here") and will follow the web links proposed to continue this sort of evil seeking. Honeytokens can be used to generate web pages, which contains fake email addresses. These honeytokens help to fill their database with fake email address, which will be of no use to them. These web pages, to be simple are created as HTML tags which contains only the fake email addresses. Any attempt to access to these addresses is none other than an unauthorized access. If any spammer programs crawl through these web pages, they collect the email

addresses. When these addresses are used by the spammers the honeytokens will dynamically create a mailto link to a fake email address. Any mail to this address is nothing but a Spam mail and hence it can be rejected. This also helps to identify the IP address used by the spammer and any further mails coming from that IP can be blocked. These HTML tags instead of being placed statically, if they are created in a random manner, it becomes more accessible and vulnerable to the spammer attack. The probability that the dynamic honeytoken is attacked is more when compared to the static honeytokens. By using this technique we try to fool the spammers by making them fill their target database with fake email address thus controlling their activities. Secondly honeytokens capture the information about the IP from the spammer harvest source has originated and hence this information can be used to prevent from further attacks.

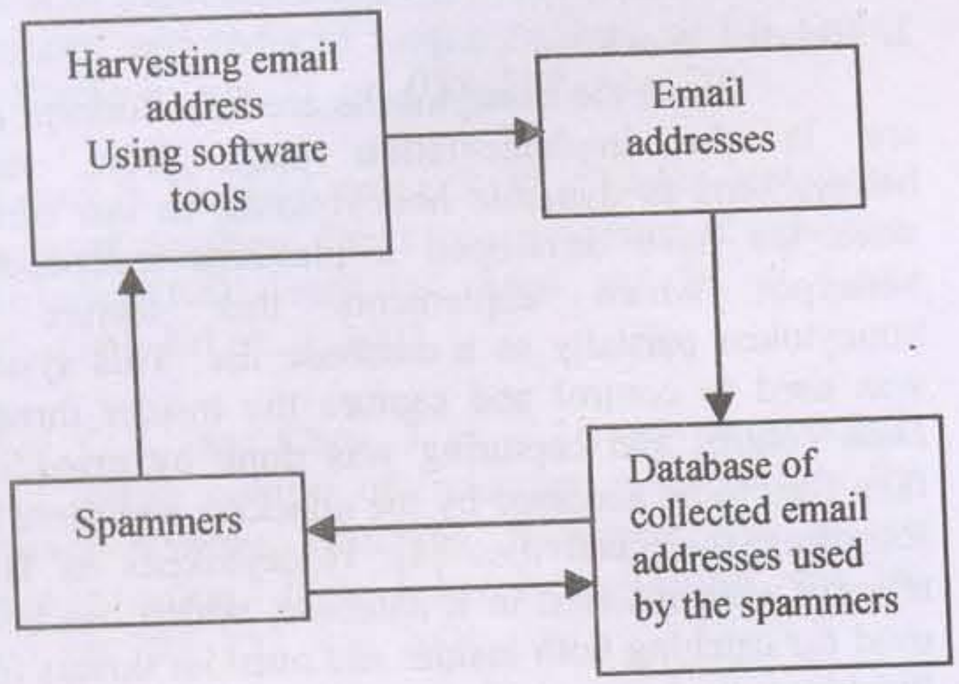

Fig.1: Spammers harvesting Email address

3.2 Honeytokens to Catch Insider Threat

Honeytokens play an important role in catching the insider attacks. Static honeytokens are inserted in the form of fake Database files [ref], fake records [ref] and bogus password and login information. Dynamic honeytokens can be implemented for catching the insider threat more effectively. Any insider who tries to access any illegal mails, which he is not, authorized to do can be easily detected by using honeytokens. They also identify whom the attacker is and what they are trying to hack. As an example honeytokens can be created in the form of a fake email and inserted into the organization's mail. Any intruder who reads this mail is nothing but an attacker as this mail is not intended for anyone. The fake email contains a bogus login and password which when logged is redirected to the honeypot system, which records his activity [Figure 2].

Any insider intruder who manages to read this mail will try to access the login password. Any such attempt is an illegal access and henceforth the activities of the intruder can be recorded. These fake emails can be generated dynamically with different messages and various login and password, to identify the motives of the intruder. The fake login password can be redirected to honeypot, which carries fake information files pertaining to secrecy of the organization.

To: Head of the Department
From: Intranet security team
In order to
improve the security measures you have been given a new login and password which you can use for discussing the confidential management issues
Login: HOD!@#
Password: fd45hjk

Fig. 2 : Sample email message

4. Conclusion

As the static honeytokens have the disadvantage of easily being identified by the attackers or have the possibility of not being attacked, the concept of dynamic honeytokens is introduced. We have discussed about the different ways of implementing the dynamic honeytokens. The proposal for implementing these honeytokens through the form of HTML tags to fool the spammers is given. The other method can be used to catch the insider threat by inserting honeytokens as fake email messages and thus capturing the intruders activities. We are under the implementaion of both proposals and have extended the proposal by redirecting the honeytoken activities to a dedicated honeypot, which can be used for recording their activities.

5. References

[1] Spitzner,L ., 2004. The honeynet project: Trapping the hackers, IEEE security and Privacy, March/April 2004:15-23.

[2] Mcgrew, R., Rayford.B., and Vaughn, J.R 2006. Experiences with honeypot systems: Development, deploymentand analysis. In Proceedings of the 39th Hawaii International Conference on system sciences.

[3] Spitzner, L., 2005, "Honeytokens: The Other Honeypots,",

URL : http://www.securityfocus.com/infocus/1713.

[4] Maheswari, V., and Sankaranarayanan, P.E. 2007, Defeating hackers through a Java ased honeypot deployment, *Information Technology Journal* 6(7): 1080-1084.

[5] Craig , M., and Rayford, B. 2007, Phighting the Phisher:Using Web Bugs and Honeytokens to Investigate the Source of Phishing Attacks. In Proceedings of the 40th Hawaii International Conference on System Sciences: 270c.

[6] Maheswari.V, and Sankaranarayanan P.E., (2008) "Capturing the hackers profile using Honeytokens", NCCT '08, organized by MEPCO Engineering College, Sivakasi, pp 242-244.

[7] Uri Raz, How do spammers harvest email address, Whitepaper.