Design of a worm isolation and unknown worm monitoring system based on Honeypot

AlFraih AbdulAziz Nasser A
The School of Information Science and Engineering
Lanzhou University, Lanzhou, China
alfraih13@lzu.edu.cn

Wenbo Chen
The School of Information Science and Engineering
Lanzhou University, Lanzhou, China
chenwb@lzu.edu.cn

Abstract—It has been proved being cumbersome and ineffective to prevent attacks in computer networks. However, the detection strategies have been found to be effective and less costly. The use of Intrusion Detection Systems (IDS) as a detection technique has been widely implemented in computer networks. Meanwhile, there is another strategy can reduce the occurrence of network intrusion, namely Honeypot. Honeypot is a proactive defense technology, introduced by the defense side to change the asymmetric situation of a network attack and defensive game. Through the deployment of the honeypots, i.e. security resources without any production purpose, the defenders can deceive intruders to attack the honeypots, then capture and analyze the attack behaviors in order to understand the attack tools and methods, and to learn the intentions and motivations. The paper analyzed the characteristics and the harms of worm virus, put forward a kind of custom honeypot system. Which according to the intrusion detection, virtual honeypot and data mining technology, using guile address space technology for the purpose of capturing known worms, isolating and delaying the unknown worms scanning speed, and analyzes the log by data mining, update the intrusion detection system rules set, and make timely response and take defense.

Keywords- network security; Intrusion Detection Systems; Honeypot; Snort; Worm;

I. INTRODUCTION

As the attackers are becoming mature, attack tools and methods are more complex, the firewall, the intrusion detection method has been unable to meet the demand of security sensitive departments, the network defense must adopt a deep, various means. The network environment is becoming more and more complex, series of complicated equipment need to constantly upgrade or take patch, and these make the job of the network administrators increasing. In this condition, the honeypot technology has become a new network security solution, not only by more and more people's attention, and has been started in different environments play a key role.

With the advent of the Internet era, the worm's harm on the network becomes more and more intense, especially it can produce a wide range of variation in the short term and spread rapidly, has brought the serious security problem to the network. In recent years, there have been multiple algorithms for worm early detection, e.g. Much of the recent work has suggested the need for large (host) networks to detect worm outbreaks [1-3]. Thus, many have called for the creation of a cyber "Center for Disease Control" (CDC) [4]. Researchers have also used honeypots to distract attackers, early warnings about new attack techniques and in depth analysis of an adversary's strategies [5,6]. Traditionally, honeypots have been used to gather intelligence about how human attackers operate [5]. Using honeypots to gather and identify attacks was also proposed and implemented [7]. In the use of honeynets to detect vulnerabilities of the system across large enterprise networks [8], researchers used honeypots inside a university to detect infected machines behind a firewall. At present, the honeypot technology is recognized as a network worm detection technology is better, it can invade into the worm, and the worm propagation characteristics to find the worm, catch the worm's copy. In this paper, based on honeypot technology, combined with Snorts [9] intrusion detection technology, design a simple system of isolating and detecting the unknown worm. It can detect and prevent new worms, especially suitable for early worm's attack, inhibiting its spread, capture worm sample, released worm signature by the control center, so as to achieve the common immune to all network area.

II. PREVIEW OF WORM

The worm is a kind of malignant virus through network dissemination, it has some similarities common viruses, such as the dissemination, concealment, destructive, etc. And with its own characteristics, such as not parasitic on other documents, often combined with hacker technology lead to network denial of service. Most worm programs were written by computer hackers, network security researchers and virus writers, mainly combined with social engineering technique to spread. The general propagation steps are: First, the worm detect the existence of loopholes in the host by the scanning module. Then infection module according to the loopholes in the attack steps automatic infect the object found in the scanning process, obtain the permission of the host authority and get a shell. Finally the copy module will copy the worm program to the new host by interaction with the original host and start it.

© 2014. The authors - Published by Atlantis Press

The characteristics of worm virus is mainly focused in the following aspects:

1) Using the operating system and application vulnerabilities to initiate attacks.
2) Diversified propagation.
3) Making technology is difference in traditional virus.
4) Often combined with hacker technology.

Since the release of the first worm from laboratory since 1988 Maurice, computer worms with its rapid, diversified communication brings disaster to the network world. Especially since 1999, high-risk worms such as (Slammer, Red code, Nimdar, Blaster, Mydoom etc.) appeared to make the world economy suffered huge losses. One well-known worm is called "the 2003 worm king", it spread quickly and hit down the world network, the Internet network was seriously blocked, caused direct economic losses of at least 1.2 billion dollars.

III. PREVIEW OF HONEYPOT

Different researcher may give different definitions according to particular scenarios. We incline to take the following definition, “Honeypot is a security resource whose value lies in being probed, attacked or compromised” [10]. Honeypot is one of IDS which often imitates the function of a vulnerable computer [11]. As a result, honeypot is able to lure an intruder. It will record the activities of an intruder when he tries to attack the computer. The contents in the log file would be audited, then lead to the identification of attack signatures. These signatures will be stored in the database and then be used by IDS [11]. Honeypot does not have any purpose and the network does not have any connections to the honeypot entrance, it also did not authorize any person to visit, so any access to the honeypot can only be the random detection by worm scanning or hacker attack. It will greatly reduce the analysis of data flow and improve the pertinence and accuracy of analysis based honeypot analysis.

One main characteristic of a honeypot is its level of involvement. The level of involvement does measure the degree an attacker can interact with the operating system [12]. Two groups of involvement are built:

1) Low-involvement: Just run in an emulation services on existing systems, in particular port monitor and records all incoming packets, providing a small number of interactive commands and the attacker only action within a preset range of simulation services. A low-involvement honeypot can be compared to a passive IDS, as both are systems that do not alter any traffic or interact with the attacker or the traffic flow. They are used to generate logs and alerts if incoming packets match their patterns.

2) High-involvement: Built by the real operating system, it provided the true system and services to attacker. All the actions of the attacker can be recorded and collected, it will get a lot of useful information including the new attacks technique which we didn't know. Unfortunately the attacker has to compromise the system to get this level of freedom. He will then have root rights on the system and can do everything at any moment on the compromised system. As per se, this system is no longer secure. Even the whole machine can’t be considered as secure anymore.

In general, we set the honeypot has two purposes: The first is to monitor the activities of the attacker who is not to be aware of the circumstance and to collect all the information about the attacker; The Second is to contain them, let them spend the time and resources spent in attacking the honeypot system, keep them away from the actual work network.

The worm differs from ordinary viruses is that the worm can exploit vulnerabilities, including software vulnerabilities and human vulnerability. At present, the traditional means of defense in network security, such as intrusion detection systems, firewalls, etc., due to their own inherent deficiencies in against worm attacks still exist certain defects. Therefore, we consider to introduce the honeypot technology for proactive defense.

IV. INTRUSION DETECTION SYSTEM AND SNORT

An Intrusion Detection System (IDS) is an essential part in a good network security environment. It enables detection of suspicious packets and attacks. As the name already says, an intrusion detection system is used to detect intrusions or possible intrusions into an observed environment. Intrusion detection is a reasonable supplement of the firewall, help the system to deal with attack from external or internal, expand security managerial ability of the system administrator (such as security audit, monitoring, attack recognition and response), and increase the integrity of information security infrastructure.

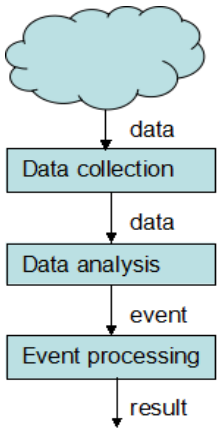

Figure 1. The data flow in IDS

The main work of intrusion detection system is to collect data from the key points of information system, and then analysis these data, to obtain the network has no breach of security strategy and attacked signs, its general model shown as Fig. 1.

Snort is a freely available intrusion detection system which can be distributed and modified under the GNU General Public License. Snort can perform real-time data flow analysis and record IP network data packets, can perform protocol analysis and content match search, can detect various attacks and exploration, such as buffer overflow, stealthy port scanning, common gateway interface attacking, server message block protocol (SMB) detection and operating system fingerprint attacking, etc. Snort has become the best choice for intrusion detection tools. Overview shown as Fig. 2.

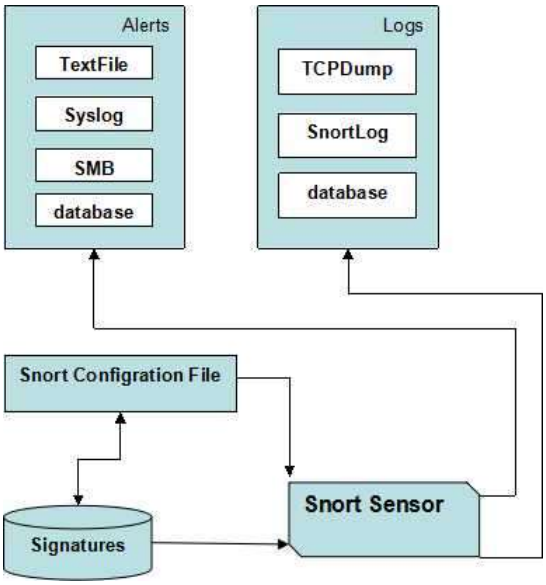

Figure 2. Snort Overview

There are two ways in the common worm detection technology:

1) Detection technology based on signature: its core is pattern matching. When a new worm appeared, the researchers studying on it and extract the characteristics string which can fully identify the worm and formed a signatures, added to the corresponding signature database. These signatures may be malicious network load, may also be part of the worm executable code's sample. Once you have the worm's signature, and then when there is such a worm outbreak or elsewhere of the worm outbreak can be identified by the IDS to take further preventive measures to stop it.

2) Detection technology based on data flow: It takes full advantage of the difference data flow between the absence of worms and the presence of worms to achieve the worm detection. Typically, the average flow of a host or a LAN in the case of normal operation of the daily is almost the same, even a slight change also fluctuate within a small range, but on the whole is stable. After the invasion of the network traffic from the worm will change greatly, all the worms must first through the scanning module to find the target to be attacked before the attack, and after the attack success it often need take its load transmission, because the whole process is worm initiative, the detection frequency is very high usually, so it will produce a lot of scanning probe packets in the short term, so that the network flow is increasing rapidly and even cause network congestion.

V. A WORM ISOLATION AND UNKNOWN WORM DETECTION SYSTEM BASED ON HONEYPOT

Worm detection technology which based on honeypot has the characteristics of low resource cost, simple configuration and easy recovery. When the worm to spread, it will randomly or pseudo-randomly scan some of the IP address. In these target address, some IP addresses may not be used, but they will still be scanned by the worm. So we can use honeypot system monitor these IP addresses, masquerading as the host which was vulnerable infection and thus to find and attract the worm attack. The honeypot technology to deal with the worm is very useful, especially to capture and analyze them, so as to obtain the latest worm signature, and then updates the worm signature database of the IDS, makes the IDS with the new worm defense.

The design of our system referenced the thoughts of the literature Sweetbait [14] and Honeystat [15], and the filter component of the known attack and the worm signature detection scheme was introduced in snort IDS. In this system, the honeypot group's mission is to provide services for the worm attack, the traps was arranged to complete its capture scanning worms and automatically generate the new worm signature. Network intrusion prevention system (NIPS) is used to monitor the communication of the signature generated by honeypot to prevent the further spread of the worm, filtering and preventing such worms into or out of the production network, to achieve the purpose of blocking worm. The principle of the system was shown in Fig. 3.

VI. DISCUSSION AND CONCLUSION

The system uses a high interaction honeypot, so it is possible that an advanced hacker fled the VMWare environment and gain complete control the honeypot host. Although the IDS outbound filtering can block any known malicious packets, it can prevent any connection establishment request come from the honeypot, but if all honeypot hosts were captured then the worm detection system will be useless. Therefore, it is important that the system administrator need to do regular inspection to prevent this happening.

Referenced the basic thoughts of Sweetbait and Honeystat and introduced the snort IDS the paper designed a worm isolation and unknown worm detection system.

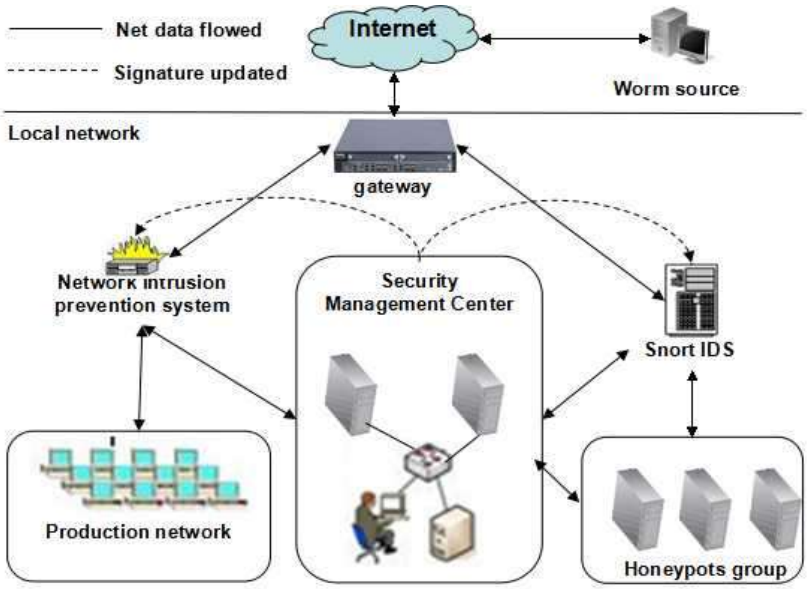

Figure. 3 The principle of the system.

Aiming at the characteristics of the worm, it integrated using of the NIPS, Snort IDS and honeypot technology and using the shared signature mechanism, and thus enables the distributed detection system in each subnet collaborative work to effectively detect and block unknown worms spread throughout the network.

The prevention of worm propagation is a major issue in computer networks. Utilization honeypots active probing worm virus is, therefore, the best strategy to counter attacks in a computer network. The use of Honeypots in worm propagation has been effective in the sense that it solves the issue of false negatives that have been associated with snort IDS.

REFERENCES

[1] C. C. Zou, L. Gao, W. Gong, and D. Towsley.Monitoring and early warning for internet worms. In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS’03), October 2003.

[2] V.H. Berk, R.S. Gray, and G. Bakos. Using sensor networks and data fusion for early detection of active worms. In Proceedings of the SPIE AeroSense, 2003.

[3] J. Wu, S. Vangala, L. Gao, and K. Kwiat. An efficient architecture and algorithm for detecting worms with various scan techniques. In Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS’04), February 2004.

[4] S. Staniford, V. Paxson, and N.Weaver. How to Own the Internet in Your Spare Time. In Proceedingsof 2002 Usenix Security Symposium, 2002.

[5] Lance Spitzner. Honeypots: Tracking Hackers.AddisonWesley, 2003.

[6] E. Skoudis. Counter Hack. Upper Saddle River,NJ: Prentice Hall PTR, 2002.

[7] Honeynet Project. Know your enemy: Honeynets. http://project.honeynet.org/papers/honeynet/.

[8] John Levine, Richard LaBella, Henry Owen, DidierContis, and Brian Culver. The use of honeynets to detect exploited systems across large enterprise networks. In Proceedings of the 2003 IEEE Workshop on Information Assurance, 2003.

[9] http://www.snort.org/,April,2014.

[10] Lance Spitzner. Honeypot: Definitions and Values.May, 2002. http://www.spitzner.net

[11] Chaware, S. Banking security using Honeypot. International Journal of Security and Its Applications, 5(1), 31-38. 2011.

[12] Reto Baumann,Christian Plattner,Honeypots,Diploma Thesis in Computer ScienceFebruary,p19,2002.

[13] Lance Spitzner. Honeypots - Definitions and Value of Honeypots. Oct 2001. http://www.enteract.com/lspitz/honeypot.html.

[14] Georgios Portokalidis and Herbert Bos. SweetBait: Zero-Hour Worm Detection and Containment UsingHoneypots. 2005. http://www.cs.vu.nl/~herbertb/papers/sweetbait-ir-cs-015.pdf.

[15] David Dagon, Xinzhou Qin, Guofei Gu, et al. HoneyStat: Local Worm Detection Using Honeypots. 2004.