The Research and Design of Honeypot System Applied in the LAN Security

Li Li, Hua Sun ,Zhenyu Zhang
School of Information Science and Engineering Xinjiang University
Urumqi 830046, China
e-mail: li_lixj@163.com, xj_sh@163.com,zhangzhenyu@xju.edu.cn

***Abstract*—For the hackers' attacks on the network is constantly updated, the traditional defense dealing with unknown invasion become powerless and can not effectively protect the network. This paper proposes the application of honeypots in the LAN system, where the virtual and physical honeypots are placed in a specific location. Honeypots can initiatively lure hackers to attack the internet, take the record of the ways and means of their invasion, and then analyze and study them. If necessary, the invasion records can be extracted to be evidence. In this way, you can learn about the latest attack methods and tools, updating Firewall and intrusion detection knowledge base and to some extent detering the intruder. This thesis focuses on the combination of a variety of defense technology to explore completely the advantages of Firewall, intrusion detection and honeypot technology to enhance the local area network security.**

Keywords-Honeypot; Honeynet; Firewall; Intrusion Detection;

I. INTRODUCTION

In recent years, hackers' attacks and intrusions on the LAN are increasing day by day. For the network administrators are busy with trivial routine maintenance, they do not have extra energy to analyze the means and methods used by hackers. The hackers, hidden in the corner, tirelessly focus on studying various invasive methods and look for opportunities to attack servers and hosts. When the system is found to be captured, the hackers have already left with satisfaction and nothing is known about them.

Firewall and intrusion detection, playing a very important role in LAN security system, have been widely used. Firewall and intrusion detection systems are firstly analyse the possible problems in the system, and then set the appropriate defensive strategy. They can discover the existed invasion, but they could do nothing for the unknown ones. [1] [4]Honeypot is designed for the purpose of active defense and has the following functions: It can lure hackers to attack it and protect the real goal; It can records and safely stores the evidence; It can records and identifies the purpose of hackers' attacks and their methods and tools. [2] [3]

This paper presents that both virtual honeypot[7] and physical honeypot are deployed in the LAN. Virtual honeypot is used to camouflage DMZ areas to protect the server's security and physical honeypot is adopted to disguise as a vulnerable host to lure hackers. According to information obtained by the hackers' invasion, means and methods adopted by hackers are analysed to update the firewall and intrusion detection knowledge base to enhance the LAN security.

This article is organized as follow: section 2, the system model; section 3, the work process of the system; section 4, Conclusion.

II. HONEYPOT-BASED SYSTEM

Honeypot used in the LAN can lure hackers to attack the host, record hacker's attacks, analyze recorded data and generate coping strategies to reach the goal of delaying attack, protecting objectives, collecting evidence and effective protection. [8]

A. System model

In a LAN, the server provides users with a variety of network services and saves some users' information. Therefore, compared with other computers, servers are more attractive to hackers, so to protect the server's security is the top priority of the LAN security. Virtual honeypot system in the LAN of this system is deployed to protect the security of the server. By installing a virtual computer software, a single physical computer has a zone that contains the virtual DMZ honeypot. For hackers, the vulnerable computer has considerable appeal to them, so in this system the physical honeypot should be deployed in a specific location to disguise a number of physical machines as vulnerable personal computers to lure hackers to attack, and then capture and record invasive methods and means. The overall deployment of the system is shown in Figure 1.

When suspicious dynamic connections are diverted into the virtual honeypot system, because of its inherent characteristics the virtual computer it can be identified by the experienced hackers. The reason why the real server is protected by the virtual honeypot server is that it can reduce the risk of being attacked, reduce costs and to some extent deter intruders. Once the invaders find they are attacking honeypot and the network has already set the trap, they will give up the attack on the server and escape quickly.

Obviously, many high-level hackers will not easily give up the attack, so in this system physical honeypot deployment is carried out in order to realize better camouflage to capture various attacks information. Several physical computers will be configured as ordinary personal computers, and many security vulnerabilities are deliberately left on the operating system of the trap host and then it is closely monitored. In the case of the unawareness of hackers, attack information has been

The work was supported by Xinjiang University under grant NO.XY080130.

978-1-4244-9698-3/11/$26.00 ©2011 IEEE

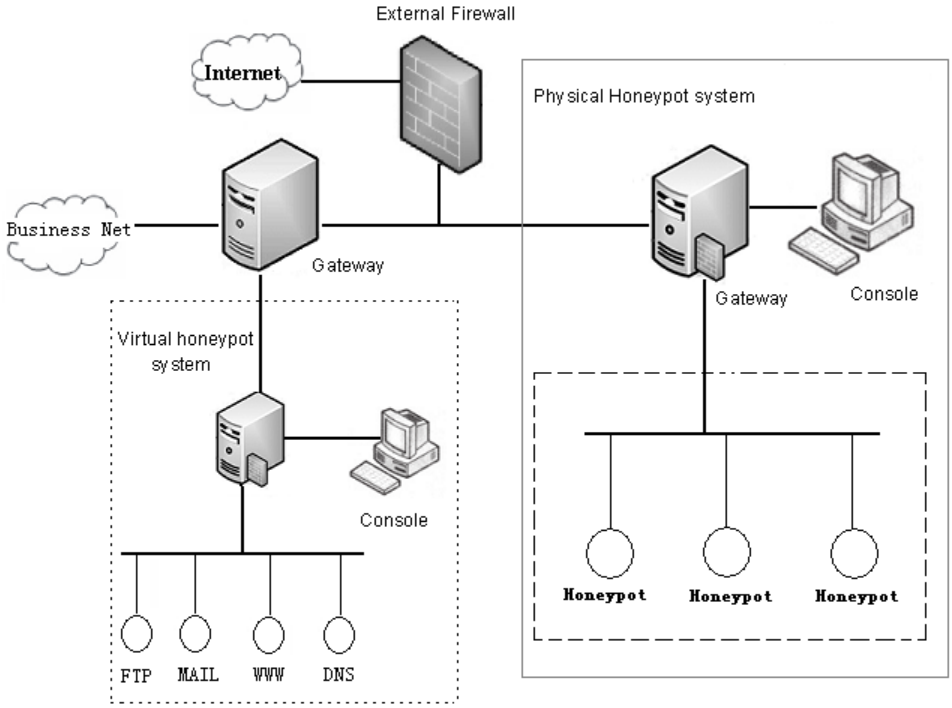

Figure 1. system deployment diagram

recorded, unknown invasion has been captured. Under the research and analysis of administrators, means of invasion is obtained, attack intention is predicted. Through correlation analysis and extraction of relevant information, the corresponding invasion knowledge base is updated.

B. System components

The main components involved in honeypot-based system:

1) Virtual honeypot

Virtual honeypot system consists of three parts: DMZ zone, virtual gateway, and console.

To protect the servers in DMZ zone, virtual computer software is installed on a single physical computer. Honeypot system is set up on virtual computer, and then similar structure like real DMZ zone is created in the virtual honeypot system. In order to confuse hackers, the appropriate network services are provided and when necessary, even some sensitive data are prepared. Furthermore, Sebek client software is also installed on virtual servers to record the invasion information.

Through the installation of sebek server program, Iptables, and Snort on the virtual gateway, data packets coming into or out of the DMZ zone can be recorded and monitored. It has no ristriction for the incoming data packets, but the outcoming data packets are correspondingly limited. Under different circumstances, it can restrict the number of outcoming connections or modify the destination address. Through operating analysis program on the console, corresponding analysis of the invasion recording can be made, intruders' methods and tools can be found, and invaders' intention can be infered.

2) Physical honeypot system

In order to make better camouflage, physical computers are used to build honeypots. In this system a number of physical computers are disguised as trap computers, on which many security vulnerabilities are deliberately left on the operating system and some personal information is added to enhance authenticity. Sebek Client Software is installed on the honeypot host to capture the invasion information. In this way, physical honeypot, gateways and console form a small Honeynet.

3) External Firewall

The firewall will be placed on the connection point between LAN and Internet. The data packets from the Internet can enter the internal network before the filtering of firewall. Those known malicious data packets can be prevented from entering the internal network system. The follow-up data packets of suspicious connection can be dynamicly shunted to the honeypot system.

4) Gateway

Since firewall can not filter data packets within the LAN, it is necessary to place gateway in the LAN. Honeypot through the gateway can link the systems and business networks, and monitor data packets going in and out of several subnets, especially external connection initiated from the honeypot system.

C. Structure of the honeypot host

In this system, both virtual and physical honeypot system will be applied and combined to give full play of their strength. Honeypot host is divided into two categories: the physical and virtual honeypot host. The following part will describe how this two types of honeypot hosts configurate accordingly.

1) Virtual honeypot host

In this system, virtual computer technology will be applied to pretend honeypot system. Virtual computer software is installed on the host, and simulate various servers in DMZ zone on virtual computer. Service softwares will be installed on servers to provide the necessary network and information services. The above will be shown in Figure 2. Network services, the same

with the services in DMZ zone, usually can be made into a copy of the form. Outdated information or false information can be applied in servers to enhance hackers' sense of trust. In addition, some loopholes in the system should be left to attract attackers.

In addition to make the trap computer have the function of the server, it still has to finish camouflage work. It mainly contains two types of camouflage: the system camouflage and network flow camouflage. System camouflage is to hide all of the major processes associated with the host and the outside processes related to trap computer. So hackers can not find they are visiting trap computer by looking at the process table. Network flow camouflage mainly refers to simulate the flow in the system and the system is disguised as a seemingly busy network, which makes the hacker believe that he enters a valuable network.

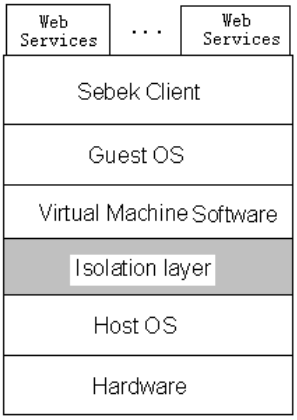

Figure 2. structure of the the virtual honeypot host

2) Physical honeypot host

It is easy to configurate and control the virtual computer, which make it widely used in the honeypot system. However, the virtual computer because of its inherent characteristics are sometimes easily found by experienced hackers, and make them escape quickly. In the physical honeypot system, the real system via strict protection is used as honeypot host. The above is shown in Figure 3. Honeypot host softwares are including five levels: the operating system layer, Sebek client, the basic system software layer, application software, processed personal information, and shaded and protected areas.

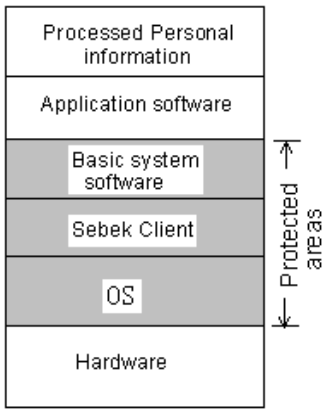

Figure 3. the structure of physical honeypot host

Protective mechanism can protect the operating system, Sebek client program and the basic system software. If the system is damaged, it can be resumed immediately. Plenty of application softwares, a variety of service software needed by users and user's personal information are installed in the honeypot host. Processed false information can be used in honeypot host to enhance the authenticity of the host. In addition, some loopholes can be left in the system to attract attackers.

III. WORK PROCESS

In this system, when the external data packet reaches the LAN gateway through the filtering of the outer firewall, it still has to go through the filtering of Iptables in the gateway. If it is properly connected to the service network, it will be shunted to the business net. Otherwise, If the connection is suspect, it will be connected to the honeypot system. If the suspect connection visits server, it will be shunted to virtual honeypot system and other suspicious connections are diverted to the physical honeypot system.

Suspicious packets arrive at the gateway of physical honeypot system and then go into the honeypot after the real-time monitoring of Iptables and Snort. Sebek client program installed in honeypot host, will silently record hackers' intrusion, and transfer and store them in Sebek server port in gateway.The database administrator uses console to make management, analysis and judgments on data in the base. Through comprehensive analysis and research of these data, the new strategies have been summed up to update the invasion knowledge base.

Outgoing connections initiated by honeypot host should be strictly controled, for it means that the honeypot has been captured, and these outgoing connections are likely used as springboard for attacks by intruders. Iptables installed at the gateway provides outgoing flow restrictions and the use of Snort will avoid the known attacks.The intercation framework diagram of physical honeypot is shown in Figure 4.

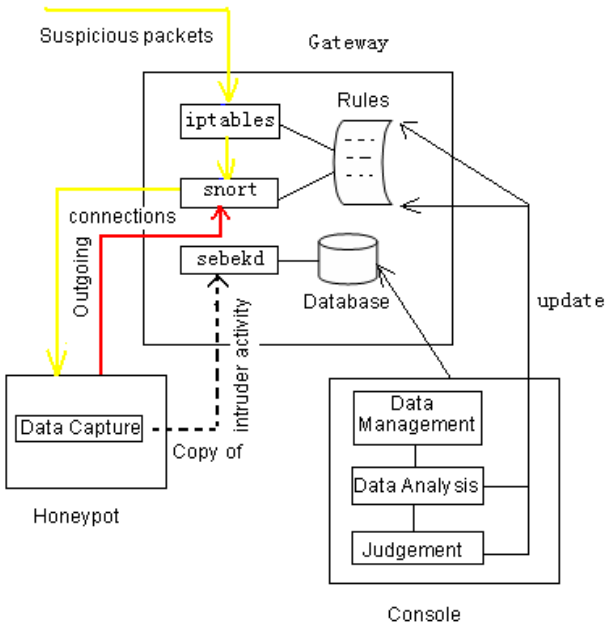

Figure 4. The intercation framework diagram of physical honeypot

Physical honeypot system consists of three parts: the console, honeypot host and gateway.

A. *Console functions*

a variety of analytical softwares is operated in the console. The administrator by means of a variety of tools makes management, analysis and judgments on attack data obtained from honeypot host. After a comprehensive analysis, the administrator infers the intruder's intention, learns methods and tools used by intruders, sums uptheir invasion strategies, converts them into regular format, and sents them to the Iptables and Snort regular base to make them updated.

B. *Gateway function*

Iptables, Snort, and Sebek server port program will be installed on the gateway. Iptables installed at the gateway provides outgoing flow restrictions. By limiting the allowed number of outer connections and flow rate initiated in unit time from the honeypot host, once the attacker tries to use captured honeypots host to initiate outside scanning, or deny service attacks etc., outgoing data packets beyond regulation will be discarded, and a warning will be generated to notify the network manager so as not to constitute a hazard to the third party network.

Snort operating on gateway have a real-time monitoring on the connection coming in and out of honeypot system. Through Snort watches each outgoing data packet, if characteristics of known attacks is found, an alert will be generated and choice will be made to discard the data packets according to configuration, or modify the data packets to make the attack invalid .

Sebek server port program extracts data from the network Sebek client port. Server port collects data in two ways: firstly, capture directly from data packets of network activity; Secondly, obtain data packets stored in Tcpdump file format. Then run the Sbk_extract program on server port to recover Sebek data.

C. *The function of honeypot host*

To enhance the interactivity, physical computer is disguised as honeypot host, and some loopholes can be deliberately left in the system to attract attackers. Sebek client module is installed in the honeypot host. Sebek is operated on the kernel space of honeypot host, which can record all of the data user extracted and used via read () system. The honeypot, which is operating Sebek, sents out those data to the port of server in a way difficult to be detected. The server port is responsible for data collection.

The operation of virtual honeypot system is similar to physical honeypot system, so it will not be repeated here. Since the freedom and camouflage of virtual honeypot system is weaker than physical honeypot system and the latter can capture more invasion information through the physical honeypot, the backup of physical system can be adopted to update invasion knowledge database in virtual system.

IV. CONCLUSION

The traditional defense usually gives inadequate performance in face of the new invasion, so the honeypot can be deployed to the LAN to conduct active defense. The network security solutions proposed in this paper are based on the honeypot system. To deal with some suspicious network connections, the system will no longer block them, but introduce them into the honeypot system. When virtual honeypot system is used to protect the security of the server, suspicious connections visiting the server are shunted to the virtual honeypot which can not only reduce the risk of server attacks, but also save cost. By the intrusion attraction and capture function of physical honeypot, attack information has been recorded without the awareness of hackers. Through the research of their methods and tools, we understand their means and intentions, which make us take the necessary and timely measures to protect the network system and enhance the security of local area network.

With the wide use of honeypot technology, hackers begin to study honeypot identification technology and they want to bypass the honeypot and capture it. Network security officer will start a long-term game with hackers, focusing on these issues in the future, such as how to enhance the camouflage of the honeypot system, how to make it become more confusing to hackers, and how to reduce the harm and minimize risk after the honeypot has been captured.

REFERENCES

[1] Zheng ChengXin.Network Intrusion Prevention Theory and Practice[M].BeiJing: Mechanical Industry Press.2006

[2] ZHUGE Jian-wei.Introduction to Honeypot and Honeynet.2004

[3] Edward Balas, Camilo Viecco. Towards a Third GenerationData Capture Architecture for Honeynets[C] . IEEE Workshop on Information Assurance and Security,2005.06.

[4] Hassan Artaila,Haidar Safa.A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks[J].Computers&security,2006,25(04).

[5] Brian Caswell.Snort 2.0 trusion Detection[M].BeiJing: National Defence Industry Press.2004.

[6] M. Stiemerling, J. Quittek, and L. Eggert, "NAT and firewall traversal issues of host identity protocol (HIP) communication," Network Working Group Request for Comments (RFC) 5207, April 2008.

[7] Niels Provos. A Virtual Honeypot Framework[EB/OL]. http://www.citi.umich.edu/techreports/reports/citi-tr-03-l.pdf, October 21,2003.

[8] Lance Spitzner. Honeypots Tracking Hackers[J].Addison Wesley,2002.

[9] Domseif M, Holz T,Klein C.NoSEBrEak-Attacking Honeynets[C]. Proceedings of 5th Annual IEEE information Assurance Workshop,2004.