The Dynamic Honeypot Design and Implementation Based on Honeyd

Xuewu Liu[1], Lingyi Peng[2], and Chaoliang Li[3]

[1] Hunan University of Commerce Beijin College
[2] Hunan First Normal University
[3] School of Computer Hunan University of Commerce, Changsha, China
{12870595,494680234,522396825}@qq.com

Abstract. Along with the rapid development of Internet technology, Network security has become a very serious problem. At present the main security technologies include firewall technology intrusion detection technology, access control technology data encryption technology and so on. These safety technologies are based on the passive defence, so they are always in a passive position when thay are face to the up-to-date attack means. So,we put forward a kind of active defense network security technology -Honeypot technology and research detailedly the dynamic honeypot design and implementation based on Honeypot.

Keywords: Network security, Honeyd, Dynamic honeypot, Virtual honeypot.

1 Preface

Along with the the rapid development of Internet technology, Network information safety has to be face to a serious threat. The current network security technologies mainly use the passive defense methods, but these methods are very tough to deal with complex and changeable attacks from hacker. Since passive defense modes are difficult to deal with the complex and changeable attacks, we must solve the problem of defensive measure which is from the passive into active.This is also our research new topic. In this context , We put forward a kind of active defense network security technology—Honeypot. The Honeypot system elaborate network resources for hackers, which is a strict monitoring network deception system.The system aims at attracting hacker attacks through offerring real or analog networks and services ,,collecting the information and analyzing its attack behavior and process during the hacker attacks.In this way,we can hold the hackers' motivations and goals, repair security holes The system attacked before , which can avoid the attacks occurred.

2 Honeyd Analysis and Research

The Honeyd is designed by the Niels Prowvos from the Michigan university.It's a application-oriented honeypot with low interactive. The Honeyd's software frame

S. Lin and X. Huang (Eds.): CSEE 2011, Part I, CCIS 214, pp. 93–98, 2011.

includes configuration database, central bag dispensers, agreement processor, personality engines and an optional routing component several parts. The structure is shown in figure 1:

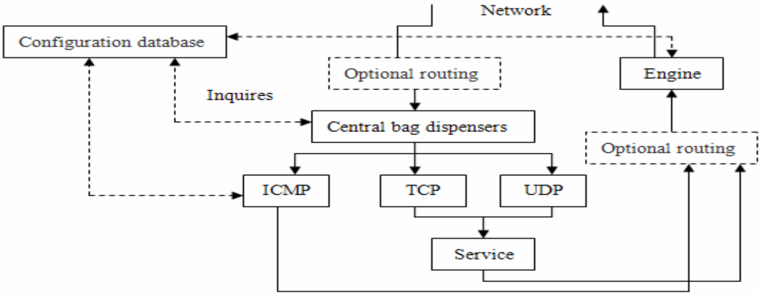

Fig. 1. Logical frame of honeyd

After Honeyd receives packets, The central bag splitter will check IP packet length and confirm bag checksum. Honeyd main response three Internet protocols which are ICMP, TCP and UDP , Other protocols are discarded after credited into log .Before Packets are processed, The central bag splitter will search the honeypot configuration corresponding with the packet destination address. If they can't find the corresponding configuration, the System uses a default configuration..After the configuration is given, Packet and corresponding configuration will be assigned to specific protocol processor.

3 The Dynamic Honeypot Design Based on Honeyd

3.1 The Design of Dynamic Honeypot Environment Obtain

The main purpose obtaining the environment around is to learn about the Internet environment. It’s the necessary conditions to solve the honeypot system configuration , That is, to solve allocation problems must know surrounding network environment first.

1) Active detection technology

In order to get the network operating system and server types, We can use tools Nmap in detecting the entire network, After that ,we can get the feedback of target system that help us to determine its operating systems and services provided by it. But if active detection by excessive used can also cause faults, Namely excessive active detection will consume extra bandwidth,,which may cause the system shutdown.

2) Passive fingerprint identification technology

Passive fingerprint identification technology is based on the principles which each operating system IP protocol has its own characteristic, maintains a fingerprinting database, Records data packets characteristic of different kinds of operating system . After it catches data packets in the network ,it will compare with the record of the database ,thereby it can judge the operating system categories.

3) Design of the active detection combining with the passive fingerprint

According to the above active detections and passive fingerprint designs, we will be able to determine approximately the kind of operating system and obtain the basic situation of the environment. Its design is shown in figure 2:

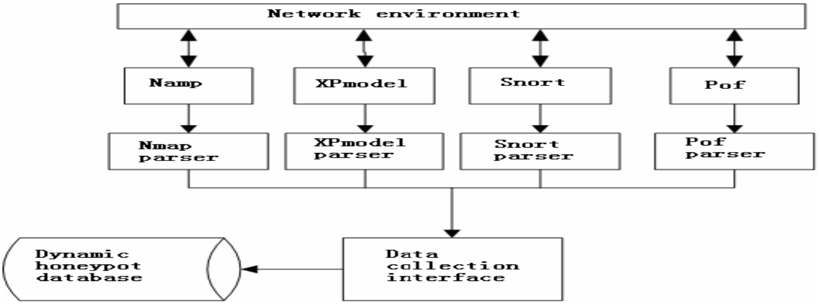

Fig. 2. Design of the active detection combining with the passive fingerprint

3.2 The Architecture Design of the Dynamic Honeypot System

Dynamic honeypot technology is first proposed as a kind of design method by the honeynet organization. For the challenge existing in the honeypot configuration and maintenance, we have to analyze it with dynamic honeypot technology. The system mainly uses active detection technology, passive fingerprint identification technology and Honeyd technology. The overall structure design which is made for the above content is in the following figure 3:

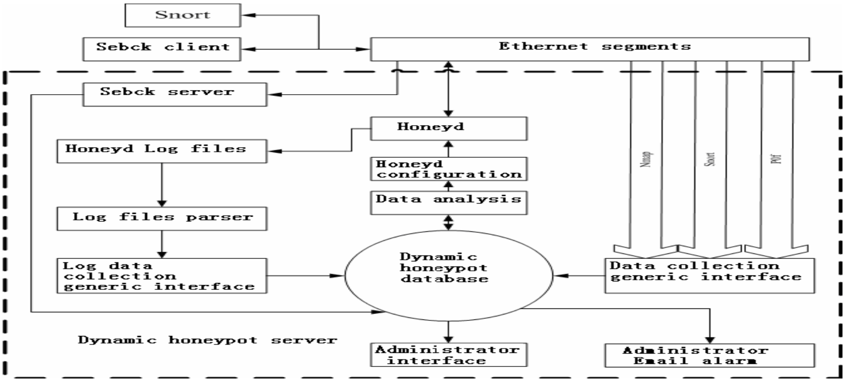

Fig. 3. The dynamic honeypot overall design based on Honeyd

4 The Dynamic Honeypot Realization Based on Honeyd

4.1 Set Virtual Machine

We can use installing Linux operating system hosts to do the honeypot host, Linux is main operating system in the machine honeypot mainframe, And let the system with bridge function, Another installation Vmware virtual machine, Used to support multiple guest operating system. Also installed the virtual machine to support guest operating system. In this honeypot system, We adopt Settings gateway for 2 Bridges mode, Through the use of two-layer gateway, Honeypot system with real system in a network environment, So in tracking and understand the external network attack, Can understand the internal network security problems. In addition, we through the source code to realize system support bridge mode.

4.2 Establish Honeyd Configuration Files

The system through the Honeyd to simulate the virtual honeypot. Through creating Honeyd.config files to configure the template. The system created a default host templates, Used to store those not in other templates defined in packets, In addition, also created a Windows operating system template and a XP operating system template and router template.

4.3 Data Control

Honeyd usually has two layers of data control, Respectively is a firewall data control and router data control, Firewall data control mainly through a firewall to control the honeypot out connection, Firewall adopt "wide into severe out" strategy, In fire prevention wall of honeypot machine from outside sends the number of connections set a rational threshold, Generally allow outside sends number of connections Settings for 5 to 10 more appropriate, Won't cause invaders doubt, Also avoid honeypot system become the invaders against other systems and tools. Routing control by routers completed, Basically is to use routers to go out the access control function of the packet filtering, Lest honeypot is used to attack other parts of a network. Mainly used to prevent Dos attack, IP deception or some other deceptive attack. In this system, we adopt gateway to replace, The advantage of using gateway is: Gateway no network address, Control operation will more latent, Hackers perceive is not easy. We adopt Honeynet development of rc. Firewal scripts to the configurations and realization, And using IPTables to restrict. IPTables is Linux self-contained open source firewall, According to the need to Forsake a bag, In a given period allowed only a certain number of new connection, Possibly through discard all packages to completely isolate the honeypot system. Every time the connection initialization out the connection, Firewall count, When the total limit is reached then, IPTables will block any Honeypot launched from any connection. Then IPTable reset itself, Allow each time period allowed out connection number. In this script installed per hour allow TCP and UDP, ICMP or other arbitrary IP packet out number of connections, When an intruder outside sends a packet to specified value, Automatically cut off all foreign connections, To reduce the network risk.

4.4 Data Capture

Data capture is the key of the honeypot system, We need to use data capture information to determine the invaders behavior and motivation, In order to determine the invaders gain access after had done, We need to capture data can provide invaders keystroke records and attack effect.

1) Realize data capture by snort

Snort is a lightweight intrusion detection system, It has three working mode: Sniffer, packet recorder, network intrusion detection system. We mainly use Snort intrusion detection model. Above configuration files is Snort collected data output to local called Snortdb Mysql database, The user name is Snortoper, Verification code is Password. At the same time will be recorded in Tcpdump format packets Snort.log file.

2) Realize data capture by sebek

Sebek is a based on the kernel's data capture tools, It can be used to capture the honeypot concealed all activities. Sebek caught in the packet encryption has great advantage, Because no matter what kind of encrypted data to the destination host to have after action, Will be decrypted to call system calls. Hackers who get packets, Use its own agreement will the packet on the Internet, Thus obtained by the Sebek Server. Sebek Client are through some hidden technology makes the invaders feel oneself be monitored, Convenient for us to capture the real data. Sebek Client capture the data package into UDP packets, Through the nic driver sent to the Internet, Avoid being invaders may install the sniffer to detect. Sebek consists of two parts: The client and the server. The client from the honeypot capture data and the output to network lets server-side collection. The server have two ways to collect data: The first kind is directly from the network activity packet capture, The second from Tcpdump format preservation packets files. When data collected can upload the relational database, Also can instantly display keystroke records.

4.5 Log Record

log record is mainly to the honeypot host capture data recorded, Its main function is to collect and record hackers behavior, For the future analysis hackers the tools used, strategies and their attack purposes or take lawsuit hackers crime to provide evidence. In order to ensure that capture hacker attacks data security, We design a log oportunidades programme to the backup data in the system. The honeypot host is running with Linux ep-red Hat 9.0 operating system of real host,the Syslog of Linux Red Hat 9.0 function is powerful, Syslog can send recording system kernel and tools generated information. We can configure their Syslog. Conf files, To realize the virtual honeypot collected log message transferred to log server. By modifying Syslog. Conf, Realized the local log information transfer to remote log server for backup. Finally, we began to capture the hacker information for analysis, Thus learning hackers means and methods, In view of its attack means to take corresponding defensive measures, To this, the Honeyd based on dynamic honeypot is realized basically.

5 Summary

Dynamic honeypot although is based on virtual honeypot, But it is a low interaction of honeypot, With the interaction between the attacker is very limited, Capture data also is very limited, Improve the honeypot interactivity can gain more attack information, To study the attacker to attack has very great help. We can interact with high virtual honeypot honeypot combined, To capture more attacks, information. Dynamic virtual honeypot on network security role is mainly indirectly, Namely recognition threat, divert attacks flow. Thus the honeypot with other security technology, Such as firewall technology and intrusion detection system combining but also the future of a very important developing direction. Along with the development of honeypot technology, Some problems will be solved step by step, Some new techniques and applications will further development, Make honeypot technology better for network security provided protection.

References

1. Fu, X., Yu, W., Cheng, D., et al.: On Recognizing Virtual Honeypots and Countermeasures. In: The 2nd IEEE Interational Symposium on Dependable, Autonomic and Secure Computing, vol. 9, pp. 220–230 (2006)
2. Leita, C., Mermoud, K., Daeier, M.: SeriptGen:all automated script generation tool for honeyd. In: 21st Annual Computer Security Applications Conference, vol. 9, pp. 125–135 (2008)
3. Zhang, F., Zhou, S., Qin, Z., et al.: Honeypot:a supplemented active defense system for network security. In: Proceedings of the Fourth International Conference, PDCAT 2009, vol. 8, pp. 231–235 (2003)
4. Kreibich, C., Crowcroft, J.: Honeycomb-Creating intrusion Detection Signatures Using Honeypots (EB/PDF), http://www.sigcomm.org/I-IotNets-II/papershaoneycomb.pal.2010
5. Domscif, M., Holz, T., Mathes, J., Weisemoller, I.: Measuring Security Threats with Honeypot Technology, 21–29 (2009)
6. Kwong, L., Yah: Virtual honeynet srevisited.SMC Information Assurance Workshop. In: Proceedings from the Sixth Annual IEEE, vol. 9, pp. 230–240 (2010)