Study on Application and Design of Honeypot Technology

Tian Bin
College of Information Technology
Luoyang Normal University
Henan LuoYang, China
eduhuangweiye@163.com

Changhong Yu
Network and audio visual education center
Luoyang Normal University
Henan LuoYang, China

Abstract—This paper introduces the history of honeypot technology and its classification according to different criterions, and then gives the design principles of honeypot. The building principles of application and investigation honeypots are explained and a typical honeypot –DTK is given. Finally, this paper discusses the developing trends of honeypot technology.

Keywords-c Honeypot; Application Honeypot; Investigation Honeypot; Hacker; Network Security

I. INTRODUCTION

The Internet has become an indispensable part of the society. However, with the popularization of the Internet, the security problem is becoming more and more prominent, and it attracts more and more attention from all walks of life [1]. At present, the measures and results of many aspects of network security, honeypot is a kind of special network security solutions.

It has been a few years now. At first, foreign computer experts named it Honeypot. The accurate definition is, "the honeypot is a security resource, and its value is being probed, attacked or compromised". Then there was Honeynet (Honeynet), which defined that a single connected network is a honeypot and high interactive performance research honeypot.

II. THE DEVELOPMENT HISTORY OF HONEYPOT

Honeypot development can be divided into three stages.

1. From the early 1990s, honeypot concept was put forward until around 1998. Honeypot was only a kind of thought, being usually applied to the network security management to track by cheating a hacker. The essence of this phase of the honeypot is the real hacker attack and host system.

2. Starting from 1998, the honeypot technology began to attract the attention of some network security researchers; some devoted to cheating a hacker's open source tools. This phase of the honeypot is virtual; development tool for simulation becomes a virtual operating system and service on the Internet, in response to attacks by hackers, and cheating a hacker.

3 After 2000, security researchers tend to use the real host, operating system and application program to build a honeypot. Different from before, the honeypot has powerful data capture, data analysis and provide data control tool, allows researchers to more convenient to analyze the attacks by hackers.

Since the honeypot technology is put forward. Therefore, far there have been all kinds of, all kinds of honeypot, they in the function, performance, uses, and safety risk aspects are different. The following specific analyses are made.

The classification results and the honeypot products are listed as below.

A. By application

Honeypot can be divided according to its application and research. When applying honeypot, the user uses this honeypot on the network protection of the environment, in order to achieve the purpose of confusing hackers. When applying to research, honeypot is to study the mechanism of hacker behavior analysis of honeypot, and obtain information attack.

Application of honeypot is placed in a real network system, which is a kind of security resources. Its value is to be attacked and compromised, the goal is to delay or allow an attacker to give up the attack of the real network environment [2]. This generated honeypot is generally not hacker attacks during the data collection and analysis.

The purpose of research is to study the honeypot hackers use a variety of tools, attack strategy, attack and psychological motivation. The results of the study provide for everyone to share [3]. This honeypot is used in the study, not limited to any specific companies or individuals; the ultimate aim is to find the unknown type of attack. Its working principle can be summarized as follows: hackers to lure this system detection, attack, hackers in this system in all activities of the record, hackers in the attack system during the data saved position in the hacker can achieve, to analyze the recorded data, the hacker attacks and propose measures to prevent these attacks.

B. By the degree of interaction

According to the degree of interaction between the honeypot and the attacker, it can be divided into low interaction honeypot, interaction honeypot and high interaction honeypot. Low interaction honeypots only provide some special service false, does not provide a real operating system, the security of the system. Interaction honeypot also did not provide a real operating system, but provides more interactive information [4]. It provides the simulation of the real operating system. High interaction honeypot provides the real operating system; high interaction honeypots hackers to gain the real operating system attack information at the same time also brought great danger. Once it is controlled by hackers, it will become a great harm to network security. The honeypot can maximize access the hacker tools, motive, purpose, skills for all kinds of information, to achieve a more perfect data acquisition provides attack analysis and prevention function.

C. By the classification of Honeypot Technology

It can be divided into sacrificial type, appearance and measurement of honeypot. At the expense of the honeypot is a simple for a particular attack of design of computer, can be attacked the system can be built on any device, after being captured, not after the normal work [5]. Appearance of honeypots only for network service simulation and does not lead to real computer is attacked, so the safety of the honeypot is not threatened. This honeypot can only provide basic information about the potential threat. Measurement of honeypot built on the expense of honeypot and appearance of the type of honeypot based on it, and it is combined with the appearance of honeypot, low cost and sacrifice advantages both in terms of the details of the honeypot, the depth, can in the end user layer easy to configure and manage

III. THE CONSTRUCTION OF THE APPLICATION ORIENTED RESEARCH HONEYPOT AND PRINCIPLE

A. To build the application of honeypot principle.

Application of honeypot system to be placed in the network environment of a real application, so the compromised the safety is particularly important. Application of honeypot is used to shelter, hacker deception [6]. Therefore, it is necessary to simulate a real network environment, the simulation network environment to various security vulnerabilities; the best simulation is a variety of operating systems installed by default. Application of honeypots is not very strict design and strict security measures and because great harm to the use of the network security, or even be destroyed the hacker. The application of honeypot should be placed on the harm caused by the network to a minimum.

Constructing the application of honeypot, consider the following problem: how to create a simulation of the operating system, the operating system how to configure, whether to take the default installation, in the network environment how to place, also need to any other component of network, the network topology node how to construct and so on.

B. Construction Research honeypot principles

The research of honeypot system is mainly used for research; therefore, the security is broken after it seems not so important. The simulation research and application of honeypot environment is basically the same. This simulation environment also has a variety of security vulnerabilities [7]. Research honeypot than application of honeypot and more a management network and the main functions of the network management is data collected by hackers in the research activities of honeypot, and ensure the security of the data, to facilitate the analysis of these data. Now all network security measures are passive defense, active defense system is predicted to loopholes in the system or in an attack on the unknown species did not produce serious harm before it found. The possible is a, that is to find unknown type of attack, which is the ultimate goal of the research honeypot.

Building Research honeypot to consider the following problems: system simulation operating system configuration, configuration of the various components, like firewall and intrusion detection system, router configuration, how to capture the hacker's activities in research honeypot analysis data, how to ensure that the security of the data, whether to need to simulate all kinds of loopholes in the system, the honeypot system topology structure and so on.

C. Configuration issues

One of the great advantages of the honeypot is that the resources are extremely rare, including equipment and network bandwidth. Honeypot system using computer don't need very good performance, and even some other system abandoned the computer can be used in the honeypot system. Therefore, researchers can consider not needing to simulate a variety of operating systems on a computer, so that it reduces the difficulty of research and development.

IV. THE TYPICAL -DTK HONEYPOT SYSTEM

We take a typical honeypot system - DTK (Deception Toolkit, deception Toolkit) as an example, a further discussion on the honeypot system. DTK is a honeypot system with open source code, running in the Linux environment; it can simulate 9 common operating systems. DTK installation, configuration is very convenient. Below are the steps for the installation and configuration.

```
#mkdir  dtk-dist
#cd  dtk-dist
#tar  -xvof  ../dtk.tar
#./configure
```

After the DTK will display a variety of configuration options, users can choose according to their own needs, choose the number of contents of the etc directory will be changed [8]. Merge the contents of /dtk/dtk.hosts.allow into /etc/hosts.allow.

Change the contents in /etc/inetd.d, here to pay attention to, in linux2.2 kernel, the only change you can, in linux2.4 kernel, researchers have to manually add content in /etc/xinetd.d. According to the content /dtk/dtk.inetd.conf. In /etc/xinetd.d joined the contents of the corresponding. For example, in the /dtk/dtk.inetd.conf serv0 stream TCP nowait root working_dir/coredump such a line, researchers want to edit the following file:

```
service serv0
      {
       socket_type  = stream
       protocol     = tcp
       user         = root
       wait         = nowait
       disable      = yes
       server       = /dtk/coredump
      }
```

After editing the /etc/xinetd.d. Similarly, according to the corresponding line in /dtk/dtk.inetd.conf, researchers edit the corresponding file, in /etc/xinetd.d.

Merge the contents of /dtk/dtk.services into /etc/services.

Merge the contents of /dtk/dtk.rc.local to /etc/rc.d/rc.local.

Running PS - a inetd grep.

Kill - HUP to terminate the process.

Running localhost telnet 365.

So far, researchers have completed the installation and configuration of DTK, the computer is now a honeypot.

In the experiment, researchers use DTK to simulate the NT operating system, using another computer to scan the computer on the DTK [9]. From the scan results can be seen DTK is a very good honeypot system can completely simulate the common operating system common vulnerabilities. The DTK, if black guest attack, the system does not give hackers a lot of information, limiting the black guest attack response. Researchers can make a honeypot hackers aggravate the burden. For example, researchers simulate the windows system, and researchers set up a bogus password, Kuroki guests will spend a lot of time to crack the code, and the final result is nothing [10]. Honeypot is also recorded in the hacker's attack process and DTK can record black guest attack techniques, scanning port, crack password process. If the system uses the DTK, researchers will find them in the hacker attack before the real application system. If they think it is difficult to break through the system, they will turn to other systems. If a lot of systems are configured with DTK, the difficulty of the hacker attacks will be multiplied by the increase in the number of times they attack, the time will be increased by hundreds of times. This is the value of DTK.

V. The honeypot Internet/Intranet environment configuration

Fig. 1 shows a typical Internet/Intranet configuration under honeypot. In addition to mapping various operating system and honeypot, Log/Alert server are used for logging and alarm. Here, researchers use IDS system, because the IDS system is now still not mature, false, false negative phenomenon is serious [11]. Operating system for honeypot is the real operating system, using the default installation. Firewall, data recorded by the router and each honeypot hackers will spread to the server Log/Alert and by the server Log/Alert.

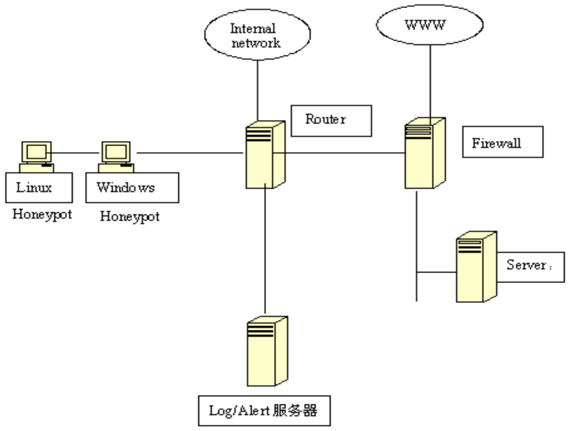

Figure 1. Typical Internet/Intranet configuration under honeypot.

The application of honeypot is not related to legal issues. The research honeypot will encounter some trouble with the law. In domestic and foreign laws, it is a kind of illegal behavior. The act of trapping refers to the use of law enforcement officers to induce others to engage in an illegal act without stopping, and using evidence collected by this method to charge the offender. Therefore, in the research researchers engaged in research of honeypot, should pay attention to the relevant legal provisions, the corresponding legal consulting institutions.

VI. Conclusions

Up to now, although there are researches on honeypot, honeypot technology is not perfect at present, which has not been applied in large scale. Although the simulation operating system of honeypot is simple to use, its function is limited, many are open source and easy to be exploited. In addition, honeypot system is now used by some application software, and the other system of the original application software should be organization development for application of honeypot. The application of honeypot after the main consideration should be given to the security problem of network environment. The goal is to find the research honeypot attack, analysis of unknown species, and not known type of attack. It takes into account the problem of data analysis, and the amount of data generated by a hacker attack is amazing. These problems need to be further explored and studied.

References

[1] Douglas E. Comer:Internetworking With Tcp/Ip Vol I:Principls,and Architectures (Forth Edition), Beijing: Publishing House of electronics industry, 2011

[2] Wang Xin-Liang, Lu Nan, Li Hui, Gao Qing-Hua, "Anomaly Traffic Analysis and The Experiment Statistic Model Based on Honeypot", JCIT, Vol. 8, No. 4, pp. 140 ~ 147, 2013.

[3] Chris Brenton,Cameron Hunt:Mastering Network Security Second Edition. Beijing: Electronic Industry Press, 2010.

[4] Li Hongxia, Chen Junming, "Research on The Theoretical Models and Applications of Functions of Management Honeypot", JDCTA, Vol. 6, No. 22, pp. 195 ~ 204, 2012.

[5] Milad Daliran, Ramin Nassiri, "Increase honeypot security through data analysis", IJIPM, Vol. 1, No. 2, pp. 34 ~ 39, 2010.

[6] Honeynet Project:Know Your Enemy, Beijing: China Electric Power Press, 2003.

[7] GuoYin Zhang , Heng Li, Rong Chen, Bin Luo, Ya Li, Hairui Wang, Sheng Wu, "Research and Design on Vulnerability Testing In Computer Network Security System", AISS, Vol. 5, No. 7, pp. 1 ~ 10, 2013.

[8] WANG Guo, DAI Dong, "Based on the Function Analysis of Integrated Intrusion Detection System for Network Security", JCIT, Vol. 8, No. 6, pp. 157 ~ 164, 2013.

[9] ZANG Weihua, GUO Rui, "The Application of Neural Network based on Evolutionary Strategy in Network Security Quantification Analysis", AISS, Vol. 4, No. 2, pp. 151 ~ 159, 2012.

[10] Shuja ul Islam, Dengshi Huang, "Pulling the Plug: Regulatory Focus Perspective, Project Completion and Anticipated Regret", IJIPM, Vol. 4, No. 2, pp. 27 ~ 35, 2013.

[11] Hong-Kyu Kwon, Kwang-Kyu Seo, "CAE simulation of HPDC Process with Automobile part (Oil Pan)", JDCTA, Vol. 7, No. 13, pp. 245 ~ 251, 2013.