Research on the application of honeypot technology in Intrusion Detection System

Xiangfeng Suo[a], Xue Han[b], Yunhui Gao[c]
Heihe university, Heihe, China
[a]79440487@qq.com,[b]hanhuaer@yeah.net,[c]gyh_26@163.com

***Abstract*—Detailed introduction of the related knowledge of honeypot and intrusion detection technology.From the adaptability, effectiveness and scalability to a detailed analysis of the current intrusion detection system in the existing problems and the honeypot technology is applied to the advantages of the system in Intrusion Detection System,At the same time put forward a detection model and describes the main functions of the model and the system structure based on the intrusion honeypot technology.**

Keywords-Intrusion detection; Honeypot technology; Network

I. INTRODUCTION

The rapid development of information technology, the network continues to expand in various fields, the network environment becomes more and more complicated, the threat is becoming the multi-source and dynamic. Safety technology in the past such as routing security, identity authentication and firewall are static, passive safety technology. The system to prevent illegal intrusion of static security technologies can play a certain role, but from the management perspective, the only defense is not enough, should also include random dynamic strategy. Intrusion detection is to protect the security of the computer system and network, a timely report network and system of unauthorized access or abnormal phenomenon of technology specifically designed. It can be seen as a second line of defense behind the firewall, greatly strengthened the security administrator management ability, its research and application has profound significance for the future network and system security.

II. HONEYPOT TECHNOLOGY

Honeypot is a system to collect intelligence. The honeypot designed deliberately to attack, to induce the hacker to attack. After such an attacker intrusion, we can know how he attacks, always grasp the server and cause new attacks. At the same time, also can use the relationship between the eavesdropping hackers, hackers to collect various tools used, and master hacker network between the social relationships. Honeypot is a kind of can be hack detection, attack even allow breached security leaks of resources, that is to say whether a honeypot technology is how to design, it is to be detected, even by the attack. Honeypot technology resources may be copy of the operating system. The application, can also be a real system live program, aims to build a deception environment, inducing the hacker attack, carefully check all things hackers made inside, at the same time these things in detail recorded and generates a log, and then carefully study and analysis tools, methods and purpose of hackers used. The more things the attackers do, grasp the things are more and more, but this risk is relatively large.

The honeypot technology to the general intruder behavior of audit, to save the log file, and detailed records of process began, compile, file, delete the file, add file modification and keystroke etc. The collection of these data can make safety improvements in overall. These data may be to judge the hacker grade, also used to track and identify the identity of the hackers. In short, the honeypot technology to help people to deal with the hacker attack, also can receive data from the analysis, the safety is improved, which can deal with more attack. The basic principle of honeypot, as shown in Figure 1.

III. INTRUSION DETECTION SYSTEM

Intrusion detection system is to detect all damage system integrity,availability and confidentiality of network security technology.Intrusion detection is the use of network and system audit, collect and analyze records of events and key information, whether there are violations of the security strategy of the event or intrusion phenomenon to find the network or system,and in response the process. The combination of hardware and software of this intrusion detection is called an intrusion detection system.Network intrusion detection generally have two kinds of misuse detection and anomaly detection.Misuse detection is the method of attack known employ some form of stored in the knowledge base, and then use the resolution knowledge base intrusion models have appeared over test.Using the method of detection accuracy is relatively high, but he can only detect known types of attacks,and attacks on aggressive behavior or camouflage new over the general is no way. Anomaly detection refers to the behavior of normal users is stored in the feature database, and then take the characteristics of the current user behavior and characteristics in the database comparisons between, if the gap is relatively large, it means that there is abnormal. Detection can detect unknown intrusion types, but the correct detection rate is relatively low. Anomaly detection is popular today, the field of intrusion detection. Using the real time analysis, the detection of specific attack mode, the system configuration or bugs and system or user behavior patterns, monitoring and security related activities are called intrusion detection. Intrusion detection system model as shown in Figure 2.

978-1-4799-6989-0/14/$31.00©2014 IEEE

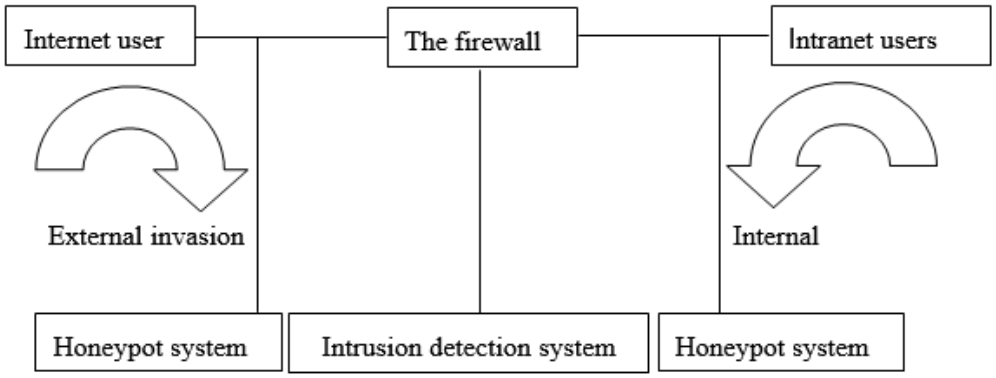

Figure 1 The basic principle of Honeypot Technology

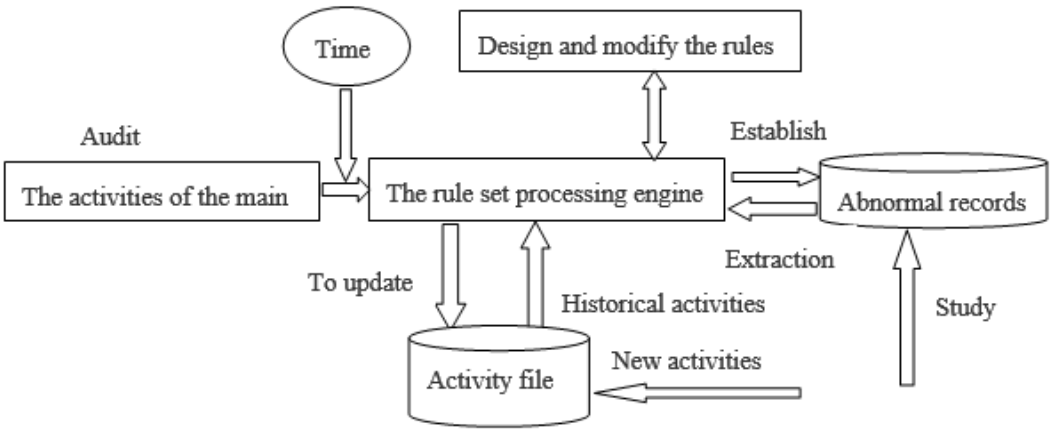

Figure 2 intrusion detection system model

IV. TECHNICAL DIFFICULTIES IN THE APPLICATION OF

Intrusion detection is an important criterion of quality intrusion detection effectiveness, adaptability and extensibility. The traditional intrusion detection, the weakness of aggressive behavior and classification system, statistical methods to select according to the type of test, and then artificial code, create a corresponding detection patterns and rules. With respect to the complexity of the network system, safety knowledge people along with the change of time and space will expose the limitations, so it is not conducive to effective detection of intrusion detection model is improved. People in the field of security generally only pay attention to attacks and known weaknesses and to analyze its, but the detection model for many later encounters system does not know the lack of adaptability of intrusion; and the security of the system upgrade cycle is long, the cost is too high, is not conducive to improving the adaptability intrusion detection model. Because the people rule and statistical method is generally used the soft, hardware platform specific, such serious damage to the system in the new environment of the reuse, and cause the detection module is embedded into the new very difficult, which is not conducive to the intrusion detection model scalability improvement, accompanied by the rapid development of network information, the network bandwidth and more big, the number of the collected audit data and network data packet is also increasing, causing data is very rich and the amount of information is very poor phenomenon, the key problem is how to find the intrusion detection system model representative in the audit data of numerous, to accurately describe the program and user behavior.

V. INTRUSION DETECTION MODEL BASED ON HONEYPOT TECHNOLOGY

Honeypot intrusion technology the honeypot technology and electronic forensics technology were combined and applied to the intrusion detection system, improve the standard of intrusion, reduce the useful information is missing, and hackers collect complete and effective evidence in the detection, find out source of hacker and proceedings. Honeypot model as shown in Figure 3.

A. Policy module configuration

Virtual machine port configuration open, choose to open or close some ports and holes.To complete the hacker to lure. Build a honeypot requires three key technologies, namely, control data, data capture and data collection. The biggest problem is how to operate and not let hackers suspicious.

B. Honeypot module

All flow in and out of honeypot network that is a problem, need to be recorded. Enter the network link is likely to be a sniffer, attack of malicious behavior, and from the honeypot initiate a connection to an external network is indicated that the system was breached. This not only control flow concept and definition of I/O is connected to a data acquisition and analysis completely simplifies. To do all of the data as much as possible accumulation can be used, mainly two aspects of system and network data, the existence of suspicious behavior of live connections are redirected to a honeypot module, and the use of network traffic simulation to entice the hacker, hacker attack disguised induced by the open port, but also set up special open vulnerability types, to allow hackers to be function.

C. Real time analysis

The honeypot module accumulation real-time analysis module of network and system information real-time analysis, and identify whether there are invasion. Analysis method can be used with pattern matching and statistical analysis of two. Pattern matching is the claim to receive data packet information and the known network intrusion data comparison. If the attack characteristic information and known as like as two peas, is regarded as the same kind of attack. It has the advantages of less error; drawback is not to detect attack method does not appear. So we must constantly upgrade to the new attack methods. Statistical analysis is to create a system of statistical description, create a system or user of the "normal" behavior feature template. By the comparison of network and system behavior is normal behaviour in the template to determine whether there are alien invasion. The characteristics of template is normal behavior in its main problem is the selection and update. It can detect the unknown intrusion.

D. Electronic evidence

Electronic evidence is the original data with the intrusion behavior have been identified for the preservation, reserved for later as the basis. Electronic evidence of very large amounts of data, so using the information fusion technology to compress the amount of information, using the information fusion technology to the same characteristic information merging. Using data compression, compression on the preservation of the fusion data.

E. The total control module

The total control module coordination between various modules management and data interaction, have been identified as the intrusion behavior event upload control subsystem alarm, and issued the command to each module of control system.

VI. CONCLUSION

Honeypot intrusion technology is mainly in order to realize intrusion detection, but also to the legal procedures can provide sufficient evidence. Honeypot intrusion technology has not yet become a more mature, systematic, standardized system, many new technologies are constantly updated development, along with the diversification of network intrusion,honeypot also need to diversify the deduction, but it has become an effective means of combating network crimes, has important research value in the field of network security.

REFERENCES

[1] Hongyan Zhang,Research and application of honeypot technology in network security[J]. Science&Technology information,2008.

[2] Tengyun Ma,Network security warning system based on Honeypot Technology[J].Shandong University.2013.

[3] Balas E,Viecco C.Towards a Third Generation Data Capture Architecture for Honeynets. Proceeedings of the 6th IEEE Information Assurance Workshop.2005.

[4] N.Provos,T.Holz.Virtual Honeypots:From Botnet Tracking to IntrusionDetection.Journal of Women s Health.2007.

[5] L. Spitzner.The Honeynet Project: Trapping the Hackers. IEEE Security and Privacy.2003.

[6] Thorsten Holz,and Frederic Raynal.Detecting Honeypots and Other Suspicious Environments. 2005.

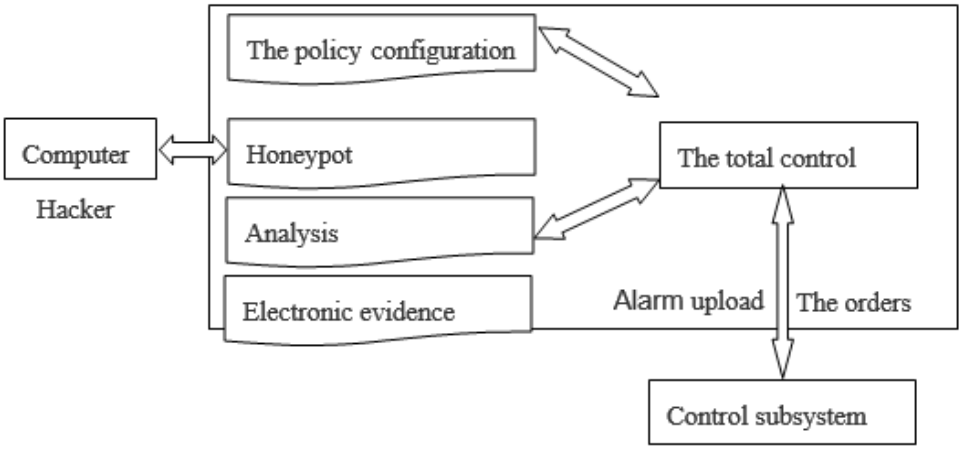

Figure 3 Intrusion detection system based on Honeypot Technology