Design of LAN Security Defense System Based on Honeypot Technology

Zhifang Yao(✉), Hongyan Chen, Kaicheng Wang, Heng Dong, Junwei Wan, and Li Zhang

Beijing Institute of Tracking and Telecommunications Technology, Beijing 100080, China
2508331028@qq.com

Abstract. Aiming at the problems that the existing network security protection system adopts traditional and passive defense, which cannot respond effectively to unknown attacks quickly and has poor defense capability, this paper designs and develops a LAN security defense system based on honeypot technology. The system uses honeypots deployed to guide attackers' invasion direction and capture vulnerability information in attackers and network servers. At the same time, the access control module is used to restrict the attacker's access rights and improve the security defense capability of the LAN. The system test and experiment results show that when the LAN deployed with the system is subject to illegal intrusion, it can accurately record the abnormal access information and network activity information of the intrusion host, which is convenient for the subsequent analysis and processing of the administrator. The effectiveness and reliability of the system are fully verified by comparative experiments.

Keywords: Honeypot technology · Network security · Active defense · Real time monitoring · Network spoofing

1 Introduction

There are often various security risks in the network. Common network attacks include virus attacks, hackers illegal intrusion, data eavesdropping and interception, denial of service, internal network security and e-commerce attacks. This paper mainly discusses how to use honeypot technology to effectively prevent virus intrusion. In our daily life, network security is mainly based on anti-virus software, firewall and other defense technologies. Most of these technologies are passive defense, but honeypot systems mainly simulate vulnerable systems, and then actively set network traps to entice hackers to attack them, and analyze and interpret them by using relevant logs, Formulate relevant plans to provide relevant guidance for future defense [1]. Honeypot technology is a valuable technology in the security field, because it has a strict monitoring system and belongs to an active defense technology in the network information system. Compared with the traditional network security technology, honeypot technology can collect information about the tools used by intruders in a targeted and efficient way in the eavesdropping mode, so as to better protect the system. Honeypot system can lure website intruders to

J. Yen et al. (Eds.): ICBIS 2023, AHCS 14, pp. 904–911, 2023.
https://doi.org/10.2991/978-94-6463-198-2_94

attack the system website actively, and then use relevant tools to analyze which tools and means the intruder uses and how to complete the attack, and sort out all the phenomena, so that some targeted methods can be taken in future work to avoid the damage to the system caused by the intruder. How to use honeypot technology to solve problems is the main topic of this paper [2].

2 Application of Honeypot Technology

Honeypot technology has two main functions: The first one is to understand the relevant technical means and tools used by the intruder by adjusting the security policy, and then collate and analyze the data after the successful deception, using this method to ensure the stability and security of the business system; The second is to lure attackers to attack the system by protecting the security of the business system and then building a honeypot environment [3].

2.1 Honeypot Technology Classification

2.1.1 Real Honeypot System

The actual honeypot technology does not need to install specific patches to create vulnerabilities. It mainly uses specific physical devices. Generally speaking, the system itself has vulnerabilities that can be used by the honeypot system. When using a real honeypot, you can directly connect the honeypot to the network environment where it is located. Compared with the traditional patching method, this access method is more covert. Intruders will regard this access method as a common access, which is not easy to be found by the intruders. Although the honeypot system will clearly record the activities of intruders, the honeypot is connected to the monitoring program [4].

2.1.2 Pseudo System Honeypot

Pseudo system honeypot is a system with loopholes that is specially built or set up by staff. The most important way to build a pseudo system honeypot is to build virtual machines. Generally speaking, a pseudo honeypot system is to create some loopholes in a system with perfect and good operating environment [5]. Virtual machines can build many pseudo systems on the same hardware platform, and then arrange multiple loopholes to record various intruder information and intrusion methods, to improve the monitoring efficiency. The advantage of this system is that the intrusion behavior of the intruder will not have a great impact on the system itself. For the monitoring personnel, even if the intrusion is successful, the secret data can be separated from the intrusion content to avoid causing large losses. This system also has some shortcomings. Many high-tech talents can easily identify the pseudo system because its authenticity is limited.

2.2 Advantages and Disadvantages of Honeypot

2.2.1 Advantages of Honeypot System

In terms of data analysis, honeypot system has great advantages. Through a series of comparative analysis such as the system, it can effectively extract important activity data

generated by the intruder, speed up the time to find key data, and greatly help to take relevant control measures in the future. At present, there are many intrusion methods for website servers and mail servers, but the actual attack traffic of the two is relatively small. When analyzing the attack traffic, you need to analyze a large number of data flows to find abnormal data [6]. This analysis requires high requirements for system equipment. Honeypot technology can effectively control the size of traffic in and out, so as to improve the value of data, so as to achieve the purpose of data analysis.

2.2.2 Disadvantages of Honeypot System

The honeypot system induces the intruder to complete a series of activities on the premise that some traps are prepared before the intrusion. The firewall cannot play an effective role at this time. Instead, it can only use the data collection method to take some targeted methods to reduce the risk of the system being broken as much as possible. At the same time, under the influence of this feature, the intruder can directly invade the real honeypot system by taking advantage of the security risks of the honeypot system, causing the computer to be damaged. In addition, if no one attacks the honeypot system, this way will become meaningless [7].

3 Overall Design of Honeypot

At present, the main operation methods used in the honeypot system include data capture, intrusion data control analysis and network deception. Through mutual rehearsal and combination of these methods, the behavior of intruders can be analyzed, so as to provide guiding opinions and suggestions for the follow-up work.

3.1 Ways of Network Deception

The fundamental means used by the honeypot system is deception, so whether there are sophisticated deception means is the direct factor determining the value of the system. During the implementation of the honeypot system, the staff will deliberately set up some vulnerabilities, and then lure the intruders to attack the system. The honeypot system looks like an ordinary system when using network deception, which can reduce the vigilance of intruders [8]. Common deception means mainly include simulation opening of service ports, simulation of system vulnerabilities and traffic simulation. In order to improve the authenticity and feasibility of the system, many means are often combined in the actual operation process.

3.2 Data Capture Method

Capturing data information requires relevant tools to accurately and completely find out which part of the data is generated by the behavior of the intruder. This is the most important work focus after the intruder enters the honeypot system, which is also the core of designing the honeypot system. In the process of data capture, it is the moment when the intruder enters the honeypot system, and at the same time, it is necessary to

ensure that the intruder does not find the data in the process of data capture. The first step is to use the outermost data log in and out of the firewall, and then use IDS to capture data packets [9]. After data capture, it is necessary to analyze the previous large amount of information. Finally, the honeypot system captures all user keyboard sequences and system logs, In actual analysis, this is a work with high technical difficulty.

3.3 Data Control

The target of the intruder in the actual process is often not fixed to a specific system, that is, the intruder is likely to use the honeypot system as a springboard, and then further invade other systems. When using the honeypot system, the internal isolation must be done well to ensure the safety and reliability of other equipment in the system. In other words, the data generated by the honeypot system must be strictly controlled to ensure that the various data generated by the system in the work can be operated and controlled by people. In real life, the main means used are to control the content of network traffic through routers and shield unnecessary connections to avoid uncontrollable factors such as data loss during data transmission.

4 Key Technologies of Honeypot

4.1 Network Deployment of Honeypot

Honeypot systems can be deployed in two ways. The first way is that the honeypot system is relatively simple in network deployment. First, you need to prepare a server of the honeypot system to install an operating system on this machine. Secondly, directly create some system vulnerabilities in the case of bare metal. Finally, connect to the Internet. In this case, the intruder is very easy to invade, but also has a high risk. At this time, if the computer is controlled, other computer systems in the network are also prone to major hidden dangers. In addition, the experienced intruder will easily find that this is a honeypot system and may upgrade the intrusion mode. The second way is to establish a virtual machine [10]. In this way, the real data in the computer will be physically isolated. The firewall technology has been widely used in the current network system. When deploying the honeypot system with virtual machines, technicians can fully consider the position of the combination between the honeypot system and the firewall, and then give full play to the value of the honeypot system itself. For example, when setting the honeypot system, the honeypot should be placed in front of the firewall first, In this way, a large number of intrusion attacks can be attracted to the honeypot system in front of the firewall to prevent intrusion attacks from entering the system. However, this method also has shortcomings. It has no way to detect attacks from the network. If you want to set the honeypot system inside the network, you need to carry out a series of targeted processing on the firewall, but the firewall will still produce some vulnerabilities. If the intruder successfully enters the real system, it will inevitably cause some losses, as shown in Fig. 1.

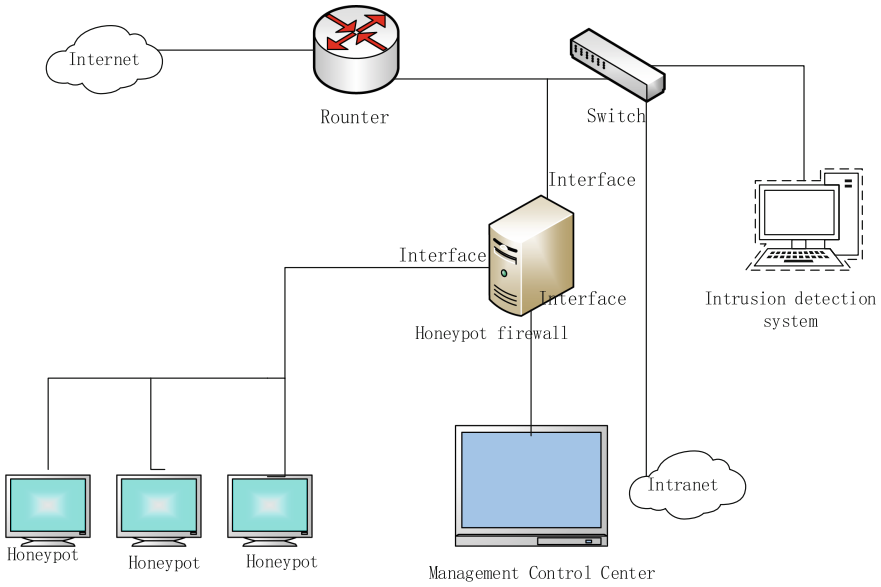

Fig. 1. Network location of honeypot

4.2 Honeypot and Intrusion Detection System

Intrusion detection system is a security device that will give warning or alarm when encountering suspicious transmission. It can monitor network transmission in real time, also known as IDS, as shown in Fig. 2. IDS is a proactive protection technology, which is a feature that other network systems do not have. Due to the lack of substantive technical means, in traditional intrusion detection methods, the staff in most cases compare the abnormal data in the work process with the data in the database, and then find the specific cause of the problem. Although the comparison method can detect which part of the data is abnormal, in the actual process, if these data are comprehensively analyzed and compared, a large amount of data information needs to be processed, which will bring greater processing pressure to the system server. Comparatively speaking, honeypot system can be well integrated with intrusion detection system, so as to reduce the probability of problems as much as possible. Honeypot system can monitor the time when an intruder attacks the network system in real time, that is to say, it can effectively control abnormal data in a relatively small comparative range, so as to improve the ability of intrusion detection system to resist network risks.

4.3 Honeypot and Botnet System

At present, the most common method of intrusion is botnet system. As shown in Fig. 3, botnet system has very obvious distributed characteristics compared with a single attack system, and an all-round attack approach can be achieved by botnet. Botnet, also known as Botnet, is a network system that uses one or more propagation methods to spread the bot program (botnet) virus infected by a large number of hosts. In this way, the infected

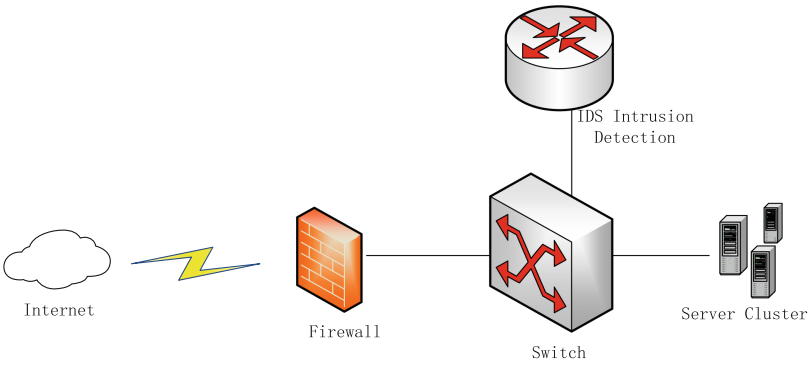

Fig. 2. Intrusion detection system

host and the controlled system can form a one to many network system, on which the virus can be widely spread. Hosts in the same network can be interfered by virus attackers by various means, while the infected hosts send instructions to the attacker's server by establishing a control channel, and then infect the entire network, thus forming a botnet system. The name of botnet is used to make people more vividly understand the danger of botnet. Honeypot system can be used for reverse tracking. It can use the monitoring characteristics of botnet to carry out targeted attacks on the attacked network system. In the actual work situation, the operator needs to first establish a relatively complete honeypot system, and then capture the useful information for us through the associated monitoring system, which is used as a tag backtracking method for attackers to obtain some special traffic information in the botnet.

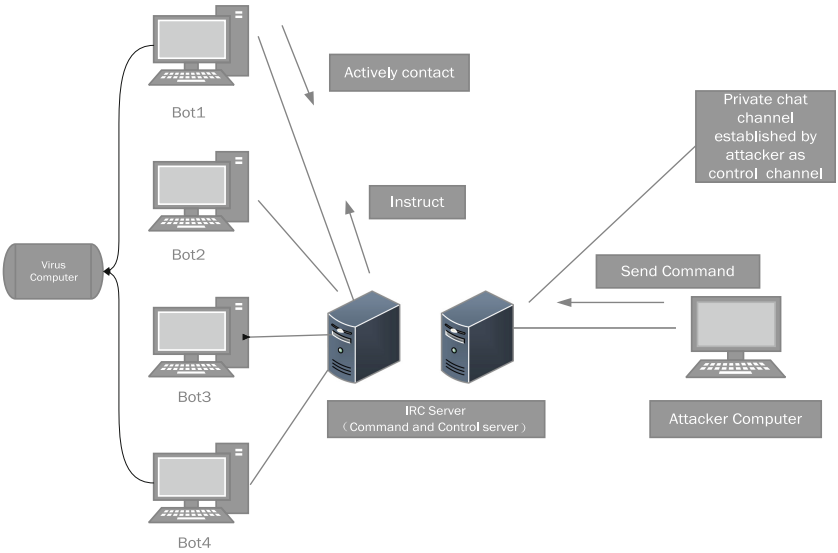

Fig. 3. Botnet system

4.4 Honeypot and Anti Worm

VirusWorm is also one of the common network attacks. Honeypot technology can also take targeted ways to control and defend worm viruses. Honeypot systems can classify worms according to their characteristics of replication, transmission, infection and scanning. Worm attacks mainly include the following steps:

Item 1: Scanning and infection: find the host that can be the target of attack, scan a large number of hosts to find the vulnerabilities that can be used by the worm, and then determine the corresponding attack method.

Item 2: Attack: The virus enters the system and attacks the target host to gain control.

Item 3: Destruction and propagation: use infected hosts to continue to infect other hosts by modifying configuration files, deleting files, destroying firewalls, installing trojans, etc. The honeypot system needs to analyze the working path of the worm virus.

First of all, in the infection and scanning phase, various server ports must be open, so that the worm can be the target of the honeypot system. This requires the use of a detector to scan the worm, and then send the worm to the honeypot system through port redirection. Secondly, in the attack phase, the honeypot system does not provide any protection capabilities to facilitate worm attacks on the honeypot system. Finally, in the destruction and propagation phase, analyze the worm virus by intercepting the network traffic or viewing the new binary files on the hard disk, and then use the recorded information to analyze the attack behavior of the worm virus. For known worm viruses, the honeypot system can detect the type of the worm virus and check and kill it, for example, by modifying IDS rules or using the rules for setting firewalls, then guide it to redirect to the honeypot system, and use the log analysis function of the honeypot system to help maintenance personnel solve related problems. The unknown worm virus can be processed by using the reverse detour method. In order to delay the scanning speed and response speed of the system, the forged data packets for the special virus can be used. At the same time, the system's analysis log and auxiliary software can be used to block the connection while analyzing The obtained attack information can be divided, and then relevant features can be extracted. IDS or firewall can be reset according to different feature points, In order to prevent the next worm attack, the intrusion detection system can warn its behavior. The honeypot system can actively record the whole process of worm virus invasion by actively guiding the worm virus to attack, which provides a corresponding information means for analyzing the working process and mechanism of the worm virus.

5 Conclusion

With the continuous development and updating of the network era, users will encounter various network attacks when using the network. At present, most of the security defense systems are passive, which will have a certain impact on the system functions. How to take precautions to ensure the network security needs can use the combination of traditional defense technology and honeypot technology to further improve the security of the system network. As a new technology, honeypot system can relatively quickly collect relevant information about intruders, Thus, effective measures can be taken to minimize the unknown risks in advance, ensure that the system can operate efficiently

and stably, and play a certain role in the prevention and optimization of the subsequent system.

References

1. Song Chunliang, Wei Huang, Hao Wu. Research on Safety Risk of Physical Isolation Network [J] .Computer Engineering and Design, 2008 (23).
2. Xiangfeng He. Application of honeypot technology in network security[J]. Network Security Technology and Addlication,2014(1).
3. Wu Jianguo. Design of Security System for Things Network [J]. Digital Technology and Application, 2011 (06).
4. Hongmin Li, Guangping Chen, Ronghui Ling, Min Lu. Sensitive. Internal and external network information exchange mode design and implementation [J]. Communication Technology, 2009 (04).
5. Zhongwa Sun. Application and research of honeypot technology in network security system[J]. Computer and Network,2014(17).
6. Rui Yin, Qi Hu, Bei Zhou. Discussion and Implementation of Internal and External Network Information Exchange Safety Solution [J]. Privacy Science and Technology, 2013 (02).
7. Hongyan Chen, Junwei Wan, Qi Wang. Design and Implementation of High Performance Sorting Algorithms for Large Data [J]. Journal of Spacecraft TT&C Technology, 2015, 34(02): 120-127.
8. Hongyan Chen. Optimization Research And Application Of Enterprise Website Based On Web Service[A]. Research Institute of Management Science and Industrial Engineering.Proceedings of 2017 2nd International Conference on Materials Science, Machinery and Energy Engineering(MSMEE 2017)[C]. Research Institute of Management Science and Industrial Engineering(Computer Science and Electronic Technology International Society), 2017: 7.
9. Junwei Wan, Hui Zhao etc.. The development status and application analysis of autonomous controllable information technology [J]. Journal of Spacecraft TT&C Technology, 2015, 34(04): 318–324
10. Hongyan Chen, Junwei Wan, Hongwei Qi. Research on cloud smart office integrated management system solution based on Internet of things [J/OL]. Modern electronic technology, 2018(10): 85–89[2018–05–30]. https://doi.org/10.16652/j.issn.1004-373x.2018.10.022.