Study on Application of Honeypot in Campus Net Security

Huang xin, Sidong yu, rongze wan

Guangxi Agricultural-vocational Technique College, Nanning Guangxi 530007,China,
huangxin543@qq.com

Keywords: Honeypot; campus net security.

Abstract. With the development of digital campus construction, the campus network size has been rapid growth, but there are also many network security problems. The honeypot technology is introduced and based on the development of net technology, combined with the campus network security problem, the honeypot technology applied to the campus network in Guangxi Agricultural-vocational Technique College is put forward, which can make the security of campus network unobstructed

Introduction

With the development of economy, internet technology and education informationization, campus network has become the mainstream mode of network time's education. Especially with the expansion of digital campus construction, most colleges have their own campus network, which has become an important part of university informatization. The campus network, on the one hand, deeps the information and resources sharing degrees, improves the efficiency of study and work, and on the other hand, brings the network security problems along with the increase of network users, the hidden trouble of which cannot be ignored. Therefore, how to ensure the campus network security becomes the problem that various universities must be to face. At present, the main network information security protection technologies are firewall, intrusion detection, etc., but these security technologies are passive safety strategies which cannot able to make timely and effective response for unknown attack behavior. Face the growing new attack method, the security technology is always in a passive position. This article puts forward the honeypot technology which will be applied to the university network, and ensure the campus network security [1].

The analysis of the current situation of campus network security

In addition to the common occurrence of virus, campus network has to face three major security hidden dangers.

The limitation of the firewall: Many campuses only install a layer barrier-firewall, but there are many limitations in the firewall. The firewall is passive defense equipment, and the campus network has many obvious shortcomings as these limitations in firewall used in the campus network. The honeypot technology has the active defense characteristics, and can help campus network avoid being attacked [1].

Internal attack: According to relevant materials statistics, the percent of campus network attack by inside is more than 80%. With computer universalness, some students' computer level is already beyond school network management personnel's imagination, and these students affected by curiosity or motives eavesdrop someone else's code and other important information. This mischief damage even malicious attacks school management system.

Hacker attacks: The internet is a connection from one gateway to another gateway. Due to the safety consciousness and capital reasons, many campus exist the "heavy technology, light safety, light management" tendencies, and the builders of the campus network does not pay much attention to the security problems, and often set up one firewall. These weaknesses provide opportunity for hackers, and make them inverse school network through the campus internet connection, and cause serious damages to the system and data [1].

Honeypot technology

Introduction of honeypot technology

Published by Atlantis Press, Paris, France.

Honeypot is an idea to create a trap system. This system has a true or is based on other computer operating system, and it seems to have a lot of loopholes. By the use of legal documents, honeypot looks like a legitimate host, which makes the invaders believe that they obtain some important information. In fact, honeypot is a closely monitored network decoy system, and attracts attack through the real or virtual network services. Honeypot gathers and analyses the information of the invaders' behavior during their attack. Honeypot issues a warning to system vulnerability and does corresponding repair to a new attack, and at the same time, can also postpone attack and transfer target. Honeypot doesn't enhance network security, but with the intrusion detection system, firewalls, and antivirus software it can greatly improve the security of the system [2].

Honeypot key technology

The core honeypot technology generally includes data capture technology, data control technology and data analysis technology.

3.2.1 Data control technology

Honeypot collects the attacker's activity log, and must ensure their security. If a honeypot is attacked, the attacker will destroy or remove the collected activity log, or make the honeypot as a springboard to attack other networks. Honeypot system should not only restrict the system flow out, but also give the attacker certain activity freedom and honeypot network interaction. For the internal honeypot system connection records, honeypot system are permitted to enter, but the external connection is properly limited. The out connection packet destination addresses are modified, and are redirected to a new host, giving the attacker a normal network packet appearance [3].

3.2.2 Data capture technology

Data capture is in the invaders without noticing it, and complete records are all into the honeypot system connection behavior and its activities. To capture the data is the main source for data analysis. With the log analysis, we can find out the invaders attack method, attack purposes, attack technology and the use of attack tool. Generally speaking, there are two ways for honeypot system log collection: one is based on host information collection mode, anther one is based on the network information collection method [4-5].

3.2.3 Data analysis technology

Data analysis is the analysis process for the data captured in the honeypot system. It can extract intrusion rules, and analysis whether has a new intrusion characteristics. Data analysis includes network protocol analysis, network behavior analysis and attack characteristic analysis. The intrusion data analysis is mainly finding out which has the attack behavior characteristics, which is normal data flow form the collected data. There are two main purpose of the analysis: one is to analysis the attacker in the honeypot system of activities, scanning keystroke behavior, illegal access systems tools, attack intention and the feature extraction attack; The other one is to establish statistical model for the attacker behavior, to see whether it has the attack characteristic. If there is a warning, it protects the other normal network, avoiding being attacked by the same [6].

Campus net security system based on honeypot

System model

Honeynet is a highly interactive type honeypot, and it is designed to get the network current various threat information, including from external and internal. Honeynet is not a separate system but by many systems and many attack detection application systems. This network can be placed in your business or organization existing system, such as solaris, Linux, Windows, eisco routers and switches, which can create an environment reflecting the real network. In these systems you can put some extra information (such as some documents, database records, log and so on which can lure the attacker interactive information) and different application, and these applications are with the same level of the real system. Therefore, vulnerabilities and weakness found in the honeynet are real and need improvement. Honeynet scheme is a separated component trap network that will separate honeypot machine and protected system, and its composition are several honeypot machines switches, routers and so on [7]. Based on the honeypot technology, campus network security system establishes a P2DR security model. P2DR model includes security strategy, protection, detection and response

Published by Atlantis Press, Paris, France.

four parts, and the security strategy is its core. With the rational utilization of defense technology and based on P2DR, the new campus network system can not only response to the internal threat, but also play a role to prevent to the external threat. The system model is shown in figure 1.

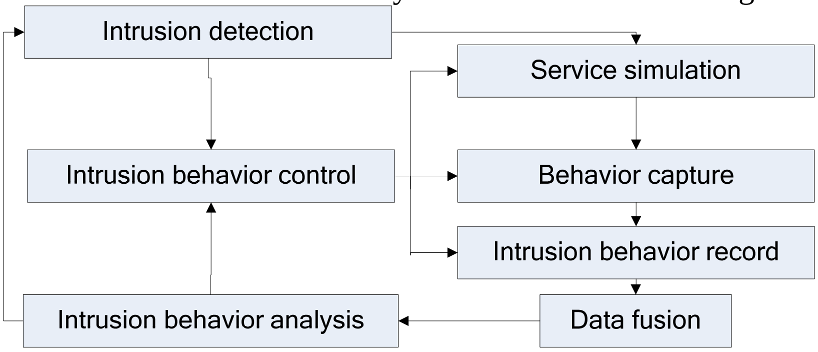
Intrusion detection
Service simulation
Intrusion behavior control
Behavior capture
Intrusion behavior record
Intrusion behavior analysis
Data fusion

Figure 1 System model

According to the goal of honeypot technology, the new campus network security system should solve the seven questions: find suspicious or intrusion behavior; control the intrusion behavior; service simulation, control the invasion behavior cut; or make active defense measures or make detailed log records to the intrusion behavior. Data fusion of intrusion behavior record data is transmitted and analyzed, which forms a dynamic security system structure.

System design

According to the system model, the safety system composes four blocks: data capture module, data control module, service module and log response module. Data capture module acquits all the system data, including network data and system data. Data control module is the core of the system, controlling and coordinating all suspicious behavior of each module in the work. Log module mainly produces log analysis and statistics to the system, in order to get the attacker information; Service module mainly responses to the suspicious behavior. The relationship between each module is shown in figure2. Under normal circumstances, the external data flow into the actual system and honeypot system at the same time. When the outside tapping stroke is mitten, according to flow, the honey pot system is more attractive to the attack behavior than real border system, therefore, the abnormal data flow first attack the honeypot system target, and at this time, honeypots system will add the results to intrusion detection rule library due to design of the data capture, data analysis. So, when the attacker again against the actual system with the same rules next time, it can block the intrusion detection system, and the active defense system realized. [8-9].

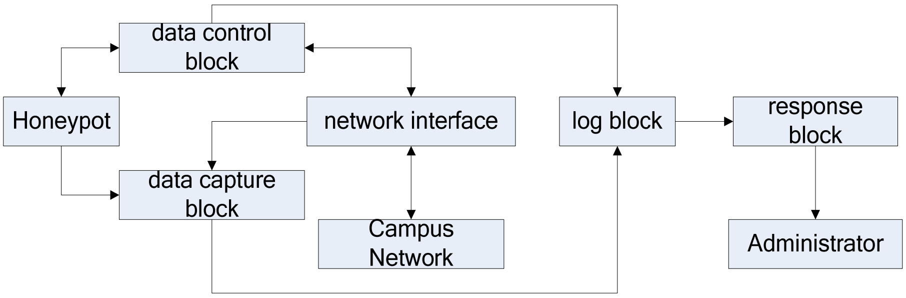

Figure 2. The relationship between each module

(1) Data capture block: Through the intrusion to the detection system, IDS can timely capture communication between invaders and honeypot server, and realizes the real-time network traffic monitoring and analysis. IDS can capture all of the network flow, and creates log files and database for the invaders, for later analysis and statistics.

(2) Data control block: Through the intrusion detection system, IDS can timely capture communication between invaders and honeypot server, and realizes the real-time network traffic analysis and control. Generating control logs, port redirection characteristics allow the operation of the application in terminal session to visit the client port, and let the invaders redirect into honeypot server.

(3) Log block: To the honeypot, IDS, firewalls and anomaly detection module, it will produce log information and transmit it to log server. For IDS, firewall produces log information, and can use the

remote MySQL log records. As the log produced by honeyd is stored on the local computer, it must carry out the honeyd log remote dumping, to ensure the safety of the log information in network transmission.

(4) Response block: At the same time on your system, when windows start up to create a thread to start monitoring service program, waiting for the invaders sending instructions. When an intruder sends the instruction invasion, it provides links to invaders. Using the intrusion detection technology, it monitors network current situation, analysis the collected information, and detects network system aggressive behavior or abnormal behavior, which can record and response to the aggressive behavior or abnormal behavior in time. IDS are mainly used for testing DMZ area.

Conclusion

Honeypot technology is a very effective resource. It can discover attack means and purpose through analyzing and recording the invaders attack behavior, and take the initiative defense measures. Combined with the campus network security existing situation, the introduction of honeypot technology in the campus network is active defense into the network security, and this technology has obtained more and more people's attention, which plays a very significant role in the campus network security protection. Through testing the honeypot system data control and data capture module function, it can clear indication that honeypot technology will provide effective security for campus network security.

References

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

[2] Honeynet Proje Ct, Know Your Enemy: Honeyllets in Universities. http://Project.honeynet.org,2004

[3] Edward Balas Camilo Viecco Towards a Third Generation Data 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 torsion Detection [M]. BeiJing: National Defense 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] Zi Chen Li,Xiao jia li,Lei gong.Proceedings of the Third International Symposium on Computer Science and Computational Technology(ISCSCT'10).August 2010.

[8] https://projects.honeynet.org/.[EB/OL].

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