UACEE International Journal of Advances in Computer Networks and its Security – IJCNS
Volume 3 : Issue 2 [ISSN 2250 – 3757]
Publication Date : 05 June 2013

CAMPUS SECURITY USING HONEYPOT

AHER NISHA N.

Abstract: **-** Now a day the number of computer and network security incidents has been increasing remarkably in the past few years the importance of networks security and services at higher education institutions has never been higher than it is now. Users and institutions are demanding more and more network services and the exchange of more potentially sensitive information within these services. This has various impacts on the campus, ranging from the so-called Denial-Of-Service (DOS) to virus infection on end-users' desktop / notebook computers. Therefore, the issue of network security has become a priority to campus network management, While using network services in campus network it can be more easily attacked. This paper presents a new technology called honeypot whose purpose is to detect and learn from attacks and use that information to improve security. A network administrator obtains first-hand information about the current threats on his network. Undiscovered security holes can be protected gained by the information from a Honeypot .Honeypot is a new network security technology beyond most traditional passive network security defense model. Compared to other security mechanisms, honeypot is convenient and flexible to deploy and implement with less performance overhead, achieving competently collecting valuable data and information and protecting the productive network.

I. 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

Honeypot is a new network security technology based on the inveiglement theory developed in recent years. A honeypot is a network inveiglement system under strict surveillance [1], which attracts attacks by genuine or virtual network and services so as to analyze the blackhat's activities during honeypot being attacked by hackers, delay and distract attacks in the meantime.

Using honeypot technology, the network administrators of Campus Network could expand the network topology space, delude the attackers, delay attacking and distract targets, deplete the attackers' resource, protect productive network. Meanwhile network and information security community can track, record and analyze the hacker's actions focused on the honeypots comprehensively to discover and get acquainted with the internal and external threats to Campus Network, the common attacking tools, methods and rules, so as to amend the network security architecture, to revised security management principles of all levels, to adjust the firewall configuration to enhance the holistic security of Campus Network

II. 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

A. Insider Attack

An insider attack involves someone from the inside of Campus Network, such as a disgruntled employee of faculty or mischievous student, attacking the network. Insider attacks can be malicious or unconscious. Malicious insiders intentionally eavesdrop, steal, or damage information such as student's archives and teacher's information database and use information in a fraudulent manner or deny access to other authorized users. Unconscious attacks typically result from carelessness and lack of knowledge as performing a task.

Aher Nisha N. is with Pune University, computer department, JSPM'S P.V.P.I.T, Pune, Maharashtra, India
(Email- aher.nisha@gmail.com)

B. Active Attack

In active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are usually mounted against the backbone of Campus Network, exploit and intercept information in transition, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave.

C. Close-in Attack

A close-in attack involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network[2]. Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both. Because some network components and network laboratories of Campus Network are inevitably open to students and teachers, Close-in Attack are more likely to occur.

D. Distributed Attack

A distributed attack requires that the adversary introduce code programmed by deliberate students or teachers skilled in computer, such as a Trojan horse or back-door program, to a trusted component or software that will later be distributed to many other companies and users[3]. Distribution attacks focus on the malicious modification of hardware or software during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

E. Password attack

An attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a bruteforce attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. A bruteforce attack is when the attacker tries every possible combination of characters. Especially for attackers inside Campus Network is more potentially dangerous to network security.

F. Buffer overflow

A buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.

G. Spoof attack

In a spoof attack, the hacker modifies the source address of the packet, so they appear to be coming from someone else. This may be an attempt to bypass your firewall rules of Campus Network.

III. HONEYPOT TECHNOLOGY INTRODUCTION OF HONEYPOT TECHNOLOGY

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

L.Spitzner defines the term honeypot as follows:

A honeypot is a resource whose value is being attacked or compromised. This means that a honeypot is expected to get probed, attacked and potentially exploited. Honeypots do not fix anything whereas providing us with additional and valuable information [1].In this paper, a slightly different definition is proposed:

A honeypot is a resource which pretends to be a read target expecting to be attacked or compromised. The main goads are the distraction of an attacker and the gain of information about an attack and the attacker. Honeypots do not help directly in increasing a computer network's security. On the contrary, they do attract intruders and can therefore attract some interest from the Blackhat community on the network where the honeypot is located. The honeypots are valuable for developing new IDS signatures, detecting operating system vulnerabilities, analyzing new attack tools, detecting new ways of hiding communications or Distributed Denial of Service (DDoS) tools, etc [4]. In cooperation with available mainstream security measures such as Intrusion Detection System (IDS), firewall, anti-virus software, the honeypot can enhance the holistic security of Internet and Intranet

IV HONEYPOT KEY TECHNOLOGY

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

A. *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].

B .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].

C. 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

V. CAMPUS NET SECURITY SYSTEM BASED ON HONEYPOT

1) 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 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.

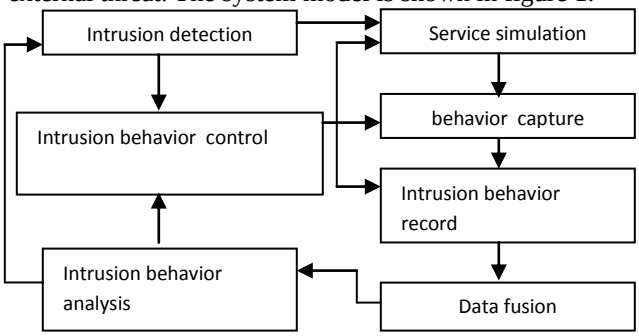

Figure 1 System model

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.

2) 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].

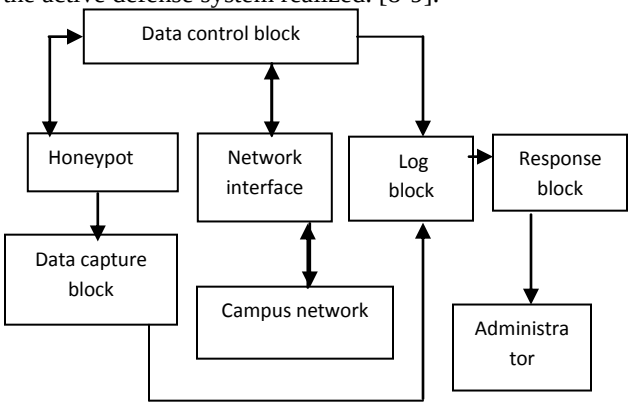

Figure 2. The relationship between each module

(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 is the new network security tool that works like a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated and protected, and which seems to contain information or a resource that would be of value to attackers. Therefore honeypot is promising technology to improve the security of Campus Network System effectively combining with the existing security measures

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] Lance Spitzner. Definitions and Value of Honeypots [EB/OL]. http://www.tracking-hackers.com /papers/honeypots.html, 2003-05-08.

[2] Liu Jie. Analysis of the Security and Countermeasure of the Campus Network. Journal of Shaanxi Normal University (Natural Science Edition), Vol.36. No.11, 2008.

[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] http://www.balabit.com/network-security/syslog-ng/, 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 5th Annual IEEE information Assurance Workshop, 2004.