A Security Reinforcement Scheme for the Server

Guofang Zhang[1], Weitao Li[1]

[1]Hainan College of Software Technology, Qionghai, China

Keywords: server reinforcement; attack tools; access policy

Abstract: With the rapid development and progress of computer network technology, information and computer network system has now become an important guarantee for social development. In the information system composed of information and computer network system, the protection of the server is the weakest, vulnerable, and relatively lacking protection. The server is the direct carrier of sensitive information in the information system, and it is also a platform for all kinds of applications. Therefore, the protection of the server is the basis of ensuring the security of the whole information system, and the security of the server operating system is the core of the server security. In this paper, a server reinforcement scheme is proposed from the network threats, possible vulnerabilities, services, process and directory permissions, which can guarantee the security of the data on the server and the safe operation of the server.

1. Introduction

For a long time, we pay more attention to the external defense technology based on network application, but we often neglect the "end-point problem" of information security. Security network management is to monitor and manage the overall security and network status of the information network through the network layer, link layer and analysis of audit information. We know that all attack sources and targets will eventually come to the terminals and servers that carry the information business of enterprises and institutions. Although the server has done a lot of security precautions, the loopholes in the operating system are endless. Once the last line of defense is broken, even if we have monitoring evidence and management measures, the impact of the important data loss of the server is incalculable. The database in the business system is not longer a high reliability network. Slowly, the database is connected to multiple applications, and the network is unreliable. The data in the database is the life blood of the unit information business, and the information stored is also important and extensive. The unauthorized access to database has attracted people's attention and created new problems. It and security administrators have successively configured security policies and technologies, but few enterprises are able to withstand attacks and protect their own databases. In the face of growing risks, the government has formulated relevant industry laws and regulations. Enterprises need to ensure that their data protection is constantly improving, such as protecting privacy, protecting data, and long-term storage and archiving of important information.

In the face of the business pressure of demand change, more and more enterprises want to achieve a certain level of database security in addition to the security control of standard database packages, especially, they want to be able restrict the access of people to view important data items in the database. The pressing question now is how to achieve this. How to configure access control and how to encrypt to achieve strict security policy without affecting daily database operation? This paper suggests that customers grasp the key points in data security construction, that is, safe servers and secure operating systems.

2. Security Risks Faced

2.1 Internal Attacks.

Intranet refers to an internal information system based on TCP/IP protocol, which provides

network services for users. With the development of network applications, many enterprises and government departments often integrate a variety of applications in their own internal intranet, including browser based WWW applications and database based Client-Server applications. The user enters the application with the user name and password. The application also identifies the user's identity according to the user name and password, and determines the user's authority. This application brings two problems to the internal network. For users, it will have multiple usernames and passwords, and how users can manage their respective usernames and passwords effectively in each application. If a user forgets a username or password that will affect his work, it may cause a great loss to himself. If the user uses the same username and password in every application for the convenience of memory, or records the username and password on paper, it will bring a great risk of leakage of the password. Most web services use plain text to transmit user names and password, which are easily intercepted by others. Even have good password, because of the limited length of passwords, can not resist dictionary attacks.

2.2 External Attacks.

With the continuous growth of computers on the internet, there is a strong dependency among all computers. Once some computers have been invaded, it may become the habitat and springboard of the invaders, as a tool for further attack. Attacks on network infrastructure such as DNS systems and routers are also becoming more and more serious security threats. The following are some of the main trends in network attacks.

Trend 1: automation of attack process

Scanning the potential victims. Rapid update of attack tools. The automation of attack tools continues to grow. The new scanning tool uses more advanced scanning technology to become more powerful and faster.

Invading the system which have loophole. Previously, attacks on vulnerable systems occurred after a wide range of scanning. Now, the attack tool has been designed the invasion of the vulnerability as part of the scanning activity, which greatly accelerate the speed of intrusion. Attack tools can automatically initiate new attack processes. Such tools as red code and Nimda virus spread all over the world in 18 hours.

With the emergence of distributed attack tools, attacker can manage a large number of attack tools distributed over internet to launch attacks. Now, attackers can launch a distributed denial of service attack more effectively. Synergetic functions take advantage of a large number of popular protocols such as IRC (Internet Relay Chat) and IR (Instant Message).

Trend 2: the attack tools are becoming more complex.

The writers of attack tools adopt more advanced technology than before. The feature code of the attack tool is becoming more and more difficult to find through analysis, and it becoming more and more difficult to find the system based on characteristic code. New attack tools have the following characteristics:

Strong anti detection ability. Attackers use techniques that hide attack tools. This makes it more difficult and time-consuming for security experts to judge new attacks through various analytical methods.

Dynamic attack method. Previous attack tools launched attacks according to a predetermined single step. Now automatic attack tools can change their features in different ways, such as random selection, predetermined decision paths, or direct control aim through an intruder.

Modularization of attack tools. Compared with previous attack tools that only implement one kind of attack, the new attack tool can be changed quickly by upgrading or replacing some modules. Moreover, attack tools can run on more and more platforms. Many attack tools use standard protocol such as IRC and HTTP for data and command transmission, so it is more difficult to analyze attack features from normal network traffic.

Trend 3: The loopholes are found faster.

New types of loopholes are found every year. Analysis of code instances for new vulnerability types often leads to hundreds of other software vulnerabilities found. It's very difficult for

administrators to keep pace with patches. Moreover, intruders are often able to identify these vulnerabilities before software vendors correct these vulnerabilities. With the automation trend of finding loopholes, the time for users to patch is getting shorter.

Trend 4: Permeating firewall

The firewall provides a secure major border protection for intranet. However, there are some technologies that bypass the typical firewall configuration, such as IPP and WebDAV. Some of the protocols that advertised firewall applicability are actually designed to bypass the configuration of typical firewalls.

3. The Limitations of Network Security Technology and Tools.

Current network security technologies and tools are mainly: firewall technology, intrusion detection system technology (IDS), scanner technology, VPN technology and anti-virus technology, but each technology has its limitations. The firewall is a gateway to a certain extent and simplifies the security management of the network to some extent, but the intruder can find the open door behind the firewall, which can not be prevented for the intruder in the network inside the firewall. IDS is hard to track the new intrusion mode and false alarm. Scanner is hard to track new vulnerabilities, and can not really scan the vulnerabilities in real time.

According to shown above, it is due to the limitations of the common network security technology and tools, so the construction of a three-dimensional network system protection system, which combines the application layer network security products and the kernel reinforcement technology, will become a development trend of the network security protection technology. As a strong backup and supplement of application layer network security technology, the kernel reinforcement technology plays a more and more important role in the network security system and plays its prominent role.

4. The Solution of Server Reinforcement

The reinforcement of the server's system kernel to protect the security, integrity and reliability of the user information effectively, in order to keep the last line to protect the user's data, the reinforcement of server is becoming an effective technical means after the application layer network security products. The super user‘s privileges of the operating system are very high. Once the intruder obtains super administrator privileges, it will pose a great threat to the system.

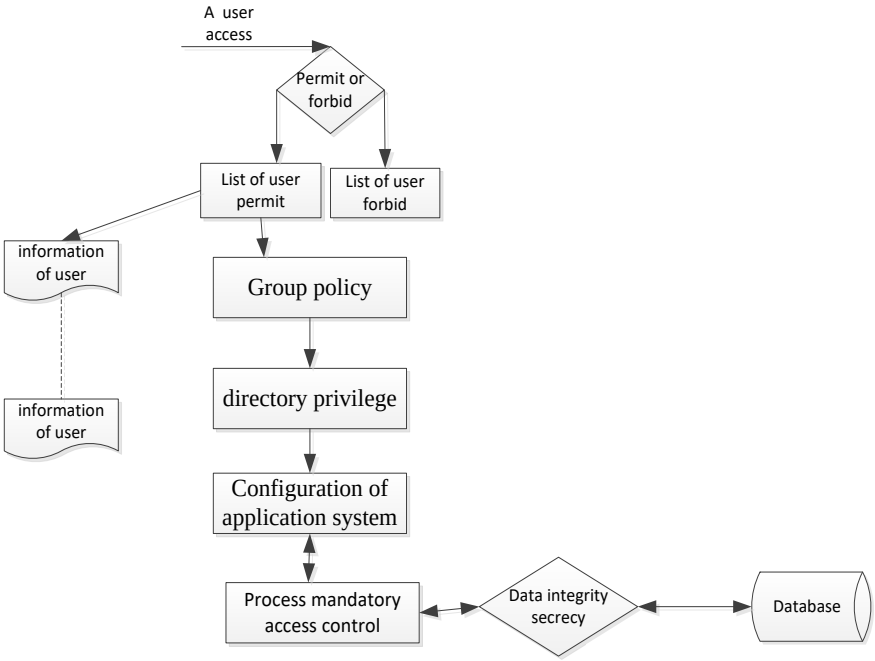

Fig 1 the new server reinforcement policy

After the investigation and analysis of the current network security construction and threats faced, this paper put forward a design idea based on advanced trusted computing technology, taking effective access control as the core, operating system security to support the security of the application system, and constructing a complete and credible security system of information security.

In order to ensure the normal operation of the server and ensure the security of the data, the server is needed to be reinforced. The scope of reinforcement includes server operating system, such as WIN series, Redhat, CentOS, Debian, Ubuntu; the other scope of reinforcement is application service including MySQL, Apache, IIS, Nginx, FTP and so on.

4.1 Safety reinforcement of the system.

By configuring directory permissions, system security policies, protocol stack strengthening, system service and access control to strengthen server system, overall improve the security of the server.

Configuration of directory privilege. All partitions, except the partition of the system, give Administrators and SYSTEM full control, and then separate directory permission to their subdirectories. For the WEB site directory, you should assign an anonymous access account corresponding to its directory permissions and give it modified permissions. In order to make the website more secure, reading permission can be allocated and writing permissions could be allocated to special directories. The root directory in the partition of the system is set to not inherit the parent authority. After that, Administrators and SYSTEM are only give full control for the partition.

For only administrator has the local login authority, the directory permission of the Documents and Settings is only the full control of administrator, and the subdirectories are the same. For the Program files directory, give administrators and system full control beyond the common files directory.

Under the SYSTWM32 directory, it is needed to deny anonymous accounts to access the programs such as cmd.exe, ftp.exe ,net.exe,scrrun.dll,shell.dll and so on.

Group policy configuration. Anonymous access to SAM accounts and sharing is not allowed. No allowing verify the storage credentials or passport for the network. Delete DFS$ and COMCFG that allow anonymous login in sharing file. Do not show the last username. The hash value of LANMAN is not stored. IIS anonymous users are forbidden to login locally. Password policy is set for users: password complexity requirement is enabled, the minimum password length is 6 bits, forced password history 5 times, the longest password remains 30 days. Account locked 3 times wrong login.

4.2 Security reinforcement of application system.

The program that involves user name and password is better encapsulated on the server side, as little as possible in the ASP file, and involves the minimum permissions to the username and password connected to the database. A validated ASP page can track the name of the file on the previous page, and only the session that is transferred from the previous page can read the page. Prevent UE and other editors from generating some asp.bak file lead to leaks. Apply all the required service pack must be update manually regularly. Installing and configuring antivirus protection. Installing and configuring firewall protection. Web data is regularly backed up to ensure that the problem can be restored to the nearest state after problems occur. Delete unnecessary application mappings. By default, hackers are very clear about the location of IIS logs, so it is best to modify their storage paths. Since SQL server can not change the SA user name or delete this super user, this account must be protected. It is best not to use the SA account in the SA in the database application. A new super user with the same authority as SA is established to manage the database. At the same time, develop a good habit of revising the password regularly.

5. Conclusion

Through the above configuration, the server is prohibited from opening unnecessary ports to prevent the service the being implanted in the backdoor program. By configuring directory

permissions, the invaders can be prevented from getting the webshell lift, the security of the server is strengthened, the attack on the server is avoided, and the TCP protocol stack is strengthened.

Acknowledgement

This paper is supported by “Hainan Provincial Natural Science Foundation of China: 618MS080".

References

[1] GUO-FANG ZHANG. The solution and management of VPN based IPSec technology. International Journal of Technology Management 2014.7.

[2] Bai Maren, Security reinforcement of the server. http://baijiahao.baidu.com/s?id=1569896489965322&wfr=spider&for=pc.

[3] Samland, server security reinforcement and service optimization. https://wenku.baidu.com/view/fe2d56b0312b3169a551a4ef.html

[4] Windows 2003 server safty reinforcement scheme.

[5] D. G. Park, C. Boyd, S. J. Moon. Forward Secrecy and Its Application to Future Mobile Communications Security. in: Matt Blaze ed. Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptosystems. Berlin: Spring-Verlag, 2000. 433~445

[6] Harn Lein, Hsin Wen-Jung. On the Security of Wireless Network Access with Enhancements. in: W. Douglas Maughan, Adrian Perrig eds. Proceedings of the 2003 ACM workshop on Wireless security. San Diego, CA, USA: ACM Press, 2003. 88~95.