Research of Computer Network Security Technology

Juan Tan

Weifang University of science & technology Shouguang City,Shandong Province 262700 China.

Keywords: Network; Firewall; Hacker; Internet

Abstract: This paper mainly explores the security technology of computer network. Firstly the network security is briefly introduced, and then the main threat to the network existing is studied. In response to these threats, this paper probes into the network security measures and analyzes the security problems of network openness and vulnerability in the security network. At the end of the article, the network security system at the present stage is studied.

Introduction

The network has become the most colorful virtual world, the rapid development of the network, has brought a huge change to people's work, study and life. Information can be got and shared through the Internet. Today, Internet is everywhere in the world, and anyone is welcome to use the Internet and to communicate with each other. With the extension of the network, the security problem is paid more and more attention to. In the increasingly complex and diversified network world today, how to protect all kinds of network and application of security and how to protect information security become the focus of this paper. Almost all contact with the network of people from all knows some pains into someone else's computer system, they use a variety of network and system vulnerabilities, illegal access to unauthorized access to the information in the network. Unfortunately, the attack network system and steal information have no need for advanced skills. There are plenty of attacks and attacks in the network resources, which can be used and shared. Do not have to understand how the attack program is running, and simply execute can cause a huge threat to the network. Even part of the program does not prescribe human involvement, very intelligent scanning and damage the entire network. This situation makes the attack frequency and density increase significantly in recent years, which brings more and more security risks to network security.

Network Security Overview

The concept of network security. Network security refers to the network system hardware, system software and data protected, not due to accidental or malicious reasons by damage, change, disclosure, the system can be in continuous and reliable normal operation, the network service is not interrupted. With the complexity of modern and advanced technology, such as local and wide area networks, Internet, security idea and the actual operation has become more complex, for the network, a person can define security for a continuous process.

Major network security threats. Trojan:

Since 2006, Trojans, hackers backdoor virus have become the professional virus writers paraphernalia, the Internet has gradually entered the Trojan, virus economic times. Jonathan released the first half of 2007, the security report shows that in the first half of 2007, the total number of new Trojan 68.71%, up to 76593 kinds.

In virus data being queried most ranked top 9 in 10 is a Trojan horse, one is set off hackers, worms, Trojans and Backdoors in a hybrid virus, its purpose is to steal network game account. Thus, the Trojan has replaced the traditional virus as the main threat to network security today.

Active attack and passive attack:

Attack classification at the highest level can be divided into 2 categories: active and passive attack.

The vigorous attack contains the intentional behavior of the attacker to access the information he needs. The passive attack is primarily to collect information instead of access, and the legitimate user of the data is not aware of the activity at this point. Passive attacks include sniffer, information collection and other methods of attack.

Malicious program:

A malicious program is usually a procedure written in an attack intent. The main malicious programs include: a trap door, logic bomb, Troy, worm, bacteria, virus and so on.

Factors affecting network security:

The development of information network security technology lags are behind the information network technology. The security of the TCP/IP protocol is not considered. Security of the operating system itself cannot control the malicious Java/ActiveX controls that is possible for the virus and Web from the mail that was the Internet. Security threats are from intranet users. Being lack of effective means to monitor and evaluate the security of the network system. Due to being lack of security awareness, many application service systems in access control and security communication aspects of the consideration is less, and if the system set the error, it is easy to cause damage.

Network security basis

Network threats.

1) Hacker attack

Depending on statistics, almost every 20 seconds global hacking incident occurred, the United States alone caused more than $10000000000 annual economic losses. They use various vulnerabilities of network, or modify page pranks; or illegal entry into host destruction procedures; or broke into the bank network transfer funds; or to steal online information to stir up trouble; or e-mail harassment; or cast the viruses in the network paralyzed and so on.

2) Defects of management

A lot of enterprises, institutions and users of the site or system management. According to the IT community enterprise group survey, 90% of the IT enterprise hackers of the United States are eager to attack. At present, there are 75% to 85% site (of what????)can't resist hacker attack. About 75% of the enterprise online information are stolen. 25% of the business losses are more than $25 million. China's ISP, securities companies and banks have repeatedly been domestic and foreign hackers attack. But there are still many units on the security of their own network is not understanding, and even the hacker attacks are not known.

3) The shortage of hardware and software

Foreign advanced countries in information technology especially network technology to implement monopoly, at present domestic network construction whether network hardware, and software is basically the ISM, which will be the fully established information system of our country in the products of other countries on the basis that national information security is very dangerous, which on the network security proposed deeper needs. At the same time, there are a lot of loopholes and bugs in the network technology and the software technology, and it is a lack of corresponding security mechanisms.

The flaw of firewall.

1) Firewall difficult to prevent

It is generally believed that: as long as the firewall holds network portal and does not allow hackers to enter, everything will be fine. Indeed, setting up a firewall to ensure network security gateway is of great importance, but it does not carry all before one. Firewall can prevent the attacks from the internal network. Statistics of the past few years show that a deliberate attack by about 75% - 80% of the internal staff initiated, because they know the security strategy of enterprises.

2) Firewall difficult to manage and configure, easy to cause security vulnerabilities

Management and configuration of the firewall are quite complex, have quite profound understanding to successfully maintain a firewall and the firewall administrator of network security attack means and its relationship and system configuration. The security policy of the firewall can't concentrate management. In general, the firewall, which is composed of multiple systems (routers, filters, proxy servers, gateways, and fortress hosts), is unavoidable in management. At present, many of the hardware firewalls used in China are imported products, and its complex interface and English instructions make many administrators prohibitive.

3) The security control of the firewall is mainly based on the IP address, and it is difficult for users to provide consistent security policy inside and outside the firewall

Many firewalls on the user's safety control are mainly based on the user IP address of the machine and not user identity. This renders is extremely difficult for the same user in inside and outside the firewall provides a consistent security policy, limiting the scope of enterprise network physics.

4) Firewall just to achieve the coarse granularity of access control, and not for the enterprise to use other security mechanisms (such as access control) using the integrated. In this way, the enterprise must maintain a separate database for internal authentication and access control management.

The necessity of intrusion detection. At present, there are many methods that can detect the network intrusion behavior, but almost all these methods use log file or tracking file. However, the vast majority of these file records are generated at the normal operation of the system. If there is no third party tool to distinguish between normal and abnormal situation when the contents of the record, then the intrusion behavior is sometimes difficult to detect. At present, for the majority of enterprises network in the presence of external intrusion and malicious attacks, information leakage, resource abuse status, intrusion detection technology are supplement of firewall technology in a reasonable and effective (??), firewall can make up for the deficiencies, from the computer network system in a number of key point to collect information and analysis these information, to see whether the network security policy violations and attack on the behavior of the signs. Provide real-time intrusion detection and protective measures for network security, such as the record of evidence for tracking, recovery, disconnection, etc.. Intrusion detection is considered as the second security gate behind the firewall, which does not affect the performance of the network, but detects the network, thus providing real-time protection to internal attack, exterior attack and misoperation.

The security problem of network openness

The openness of the Internet and other factors cause many security problems in computer system under the network environment. To address these security issues, various security mechanisms, strategies and tools are examined and applied. However, even in the case of the existing security tools and mechanisms, the network security still has a big hidden trouble. These security risks can be summarized as the following:

1) Each security mechanism has a certain range of application and application environment.

2) The use of safety tools is influenced by human factors.

3) The back door of the system is hard to take into account the traditional security tools.

4) As long as there are procedures, there may be bugs. Even the security tool itself may have a security flaw.

5) Hackers attack means constantly updated, almost every day there are different systems security issues. However, security tools update speed is too slow. The vast majority of cases need human to be able to participate in the discovery of previously unknown security issues, which makes them on the security problem is always too slow in responding.

Discussion on network security system

At this stage in order to ensure that the network work is usually as follows:

1) Prevention of network virus

In the network environment, the spread of the virus spread quickly, and it is difficult to remove the virus completely by using stand-alone anti-virus products. It must be appropriate for the full range anti-virus products of LAN. The campus network is the internal LAN, which needs a server operating system platform for anti-virus and anti-virus software for various desktop operating system. If you connect to the Internet, you need to prevent the virus from the gateway, and strengthen the security of the Internet computer.

2) Configure firewall

Firewall technology and data encryption transmission technology will continue to use and development, multi-directional scanning monitoring, the management of back door channels, preventing infecting virus software and file transmission, therefore, many problems will be solved properly.

3) Intrusion detection system

Intrusion detection technology is to make sure that computer system safety design and configuration can detect and report unauthorized or anomalies of technology, which is a for the detection of computer network security policy behavior of violation of. In the intrusion detection system, the intrusion detection system can identify any activity that does not wish to have the restriction of the activity and to protect the security of the system.

4) Web, Email, BBS security monitoring system

5) Vulnerability scanning system

Find network security vulnerabilities, evaluate and propose modifications to the proposed network security scanning tools, using the optimized system configuration and patching and other various ways possible for the latest security vulnerabilities and eliminate potential safety problems.

6) Solution to IP embezzlement problem

Bundle IP and MAC address of the router. When an IP accesses the Internet through a router, the router checks whether the MAC of the workstation that sends the IP broadcast packet is in line with the MAC address table on the router, if it is released. Otherwise, a warning message is forwarded to the workstation that sends the IP broadcast packet without passing the router.

7) Use of network monitoring and maintenance subsystem security

8) Key backup and recovery

Conclusion is order to guarantee the security of data, which should regularly update key and recovery of accidental damage to the key is very important. Sound key management schemes are designed and implemented to ensure safe key backup, update and recovery, but also related to the PKI system is strong, safety, availability of critical factors.

Conclusions

Research on information network security in China has experienced two stages: communication security and data protection, which is entering the stage of network information security research and development has developed firewall, security router, gateway security, hacker intrusion detection, vulnerability scanning software etc.. But because information in the field of network security is a comprehensive, cross discipline which combines long-term accumulation of many disciplines of the mathematical, physical and biochemical information technology and computer technology and the latest achievements of development, the proposed system, complete and collaboration to solve network security scheme, at present from security architecture, security protocol, modem cryptography, information analysis and monitoring, and information security system, research is carried out to make the parts cooperate with each other to form an organic whole.

References

[1] Lijun Cai. "Network security technology". September 2006 first editions. Beijing Northern Jiaotong University presses.

[2] Ji Deng, Jing Liu. "Hacker attack and defense combat.". January 1, 2005 issues. Electronics Industry Press.

[3] The "basic" network security, the editorial board of the first edition in May 2008. People's Posts and Telecommunications Press.

[4] The "basic" network and information security committee, the first edition in March 1, 2008. Beijing Institute of Technology presses.