Study of Computer Network Security and Its Countermeasures

Jun Qian[1, a], Song Guo[2 b]

[1] Nanchang Institute of Science and Technology, Nanchang, Jiangxi, 330108

[a] email, [b] email

Keywords: Computer Network, Security System, Countermeasures

Abstract. Computer technology is developing rapidly, so that the development of today's society can not do without information network. Since the information transfer computer network involved in all areas of finance, science and education, and military, which contains significant economic or national interests, it ultimately forms from cyber attacks on all sides, and also a variety of network attacks, such as virus infection, data theft, tampering delete information add more. From the aspect of network information security vulnerabilities, network security technology major, common network attacks and countermeasures, network security, construction and other analyzes the main problems of the current network information security presence, and common network attacks from the technical level proposed solutions We hope the gradual elimination of network information security risks through the network security building.

Introduction

Computer technology is developing rapidly, so that today's society is inseparable from the development of information networks already. Since the information transfer computer network involved in all areas of finance, science and education, and military, which contains significant economic or national interests, it ultimately forms from cyber attacks on all sides, and also a variety of network attacks, such as virus infection, data theft, tampering delete information add more. Computer crime-prone, but also the convenience of their crime, offenders do not have to visit the site and there is much evidence of a crime is difficult to stay relevant. Countries today are for protection of computer network security has become a serious computer crime to curb social problems.

Network information security related to the development of the national security of the nation, as the global information technology more widely, it plays an increasingly important role. We promote network security, vigorously protect the network information security is to protect the network hardware and software, the main data protection system, so as not to be destroyed, change, disclosure, and ultimately makes the entire network system to normal operation and provide service.

Network and Information Security Techniques

Network information security refers to the computer network system hardware, data, programs, etc. will not be accidental or malicious reasons, destruction, alteration, disclosure, to prevent unauthorized access to or use, the system can maintain a continuous service resistance, and the ability to reliably run.

Firewall security technology is primarily connected to the Internet in order to protect the internal network or individual nodes. It has a simple and practical feature, and high transparency, can reach a certain safety requirements without modifying existing network applications situation. On the one hand through the firewall inspection, analysis and filtering net outflow of workers from inside the package P, as far as possible be protected information networks or nodes, the network structure of the external shield, on the other hand internally shielded from external addressing some danger, to achieve internal protection network.

A firewall is a network device or a group, the main role is to enforce access control in two or more networks. Its basic principle is very simple, such as a pair of switches, one to prevent signal transmission, the other to release. Firewall represents the principle of access to a network whose

primary purpose is to protect a network from other network attacks. Usually we set the firewalls to protect their networks, and for the external network, we set firewall rules, namely the security policy of the network, and from the information used to filter networks, check the information, consistent with the principles of the release, does not meet the barrier.

We need a measure to protect our data against by some people with ulterior motives have seen or destroyed. In the information age, information is to help groups and individuals, enabling them to benefit from the same information can also be used to threaten them, causing damage. In the fierce competition of large companies, commercial espionage often get other information. Therefore, the objective would need a strong security measures to protect confidential data from being stolen or tampered with. Data encryption and decryption from a macro perspective is very simple, easy to understand. Encryption and decryption methods are very straightforward, easy to learn, easy to confidential data encryption and decryption.

To verify a network user, the usual practice is authenticated, but it does not tell the user authentication can do, network access control technology can solve this problem. Access control is a set of strategies and mechanisms that allow for limited resources from unauthorized access. It also protects resources, prevent malicious access to those resources, users do not have access or accidental access. Access control is the core of information security mechanism, which is the main means to achieve data confidentiality and integrity. It is an important measure to protect information system resources, but also the computer system the most important and most basic security mechanisms. However, it can not prevent the organization is authorized to vandalism. The user as an entity (actually a person or that person's application on behalf of the operation), the entity wants to access a resource. Including access to read the data, change data, run programs, initiate connections. Resources may be in some way (e.g., read, write or modify operation) to make any operation of objects, those objects may also be forced to perform an operation (such as running a program or sending a message). The customer may be a user entity, may be the server resources. In short, access control to limit access to the body (or called the initiator, is an active entity, such as users, processes, services, etc.) access to access objects (in need of protection resources), so that the legitimate scope of computer system internal use. Access control mechanisms determine what users and on behalf of certain interests of users of the application can do, and to what extent.

VPN is one of the latest and most successful techniques to solve the current problem of information security issues, the so-called Virtual Private Network is to establish a private network over public networks, so data through a secure encrypted channel propagation in the public network. To build on the public communication network VPN, there are two main mechanisms of these two mechanisms route filtering technology and tunneling. Currently the main use of VPN technology to ensure the safety of the following four: tunneling, encryption technology, key management and user authentication technologies and equipment. Previously, in order to achieve interconnects two remote networks, mainly used leased line connection. Although this method is safe, there is a certain efficiency, cost is too high. With the rise of the Internet, resulting in the use of network simulation work nternet better security technology LAN a Virtual Private Network. This technique has the advantage of low cost, but also to overcome the weaknesses of unsafe work nternet. In fact, the data transfer is simply the process of adding encryption and authentication of network security technology.

Technical information security certification is an important element, authentication techniques may be more important than the information itself is encrypted. For example, in online shopping, the buyer does not require shopping information confidential, but need to confirm the authenticity of the shop (which requires authentication), third-party buyers and sellers of the transaction information is not modified or forged, and shop businesses can not repudiate (which requires message authentication), for the business as well.

Intrusion detection technology for internal intrusion, external intrusion and misuse in real-time defense, its greatest feature is endangered in the network system to intercept before, so it is a proactive security protection technology. With the development of the times, intrusion detection technology will develop three directions: distributed intrusion detection, intrusion detection and

intelligent comprehensive security defense programs. Intrusion Detection System (Workers DS) is intrusion detection software and hardware combination, and its main function is to detect, in addition to detecting portion able to stop the invasion; threatened degree of network assessment and recovery features such as intrusion events .

Common Attack Methods and Its Countermeasures

Common Attack Methods. The denial of service attacks Dos cause is called DoS attacks, its purpose is to make a computer or network can not provide normal services. The most common DoS attacks attack computer network bandwidth and connectivity attacks. Bandwidth refers to attacks with great impact of the network traffic, so that all available network resources are depleted, leading to legitimate user requests can not pass. Connectivity attack with plenty of connection requests refers to the impact of the computer, so that all available operating system resources are exhausted, the final user computer can not handle legitimate requests.

Using type attack is a type of machine you try to directly control the attacks, the following describes a common means of defense three kinds of attacks: (l) password guessing: set difficult to guess passwords, such as a variety of symbol combinations. Ensure as NFS, Netl3 work S and Telne seven such services are not available in the public exposure range. If the service supports locking policies will be locked. (2) Trojan: do not download, do not perform suspicious programs, install Trojan firewall. (3) buffer overflow: use SafeLib, tripwire system such procedural protections, or browse the latest security bulletin updated operating system.

Using automated tools database has known response type of response for bad data packet transfer made from the target host to be checked. By applying different system response in response to the database known response comparison, you can determine the target host operating system is running. Defense method is to remove or modify various Banner, including the operating system and various application services, blocking the port for identification disrupt each other's attack plan.

Network Attack Strategy. Noven network itself has a comprehensive network security system, which controlled the operation of the directory login restrictions, the largest directory permissions trust permissions, file properties, the above operations can improve the security of data. We take the following measures to prevent or limit network virus: (1) Hard disk using Netware partition. Using a floppy disk to start the network server, security is greatly improved. (2) The use of diskless workstations. Diskless workstation so that the user can only read but not write, greatly reducing the chance of the virus implanted. (3) To restrict user access permissions. Try not to use super-user login system, ordinary users only allow access to their own directories and files, generally does not allow multiple users access to the same directory or file in order to prevent cross-infection network virus. The case must then notify users of the group directory can not upload executable files, directories only allow the group to store data resources. (4) To enhance system management. For shared directory the file is set to read-only attribute, to avoid being falsified; the system directory does not give permission to modify the program so that the virus can not infect the system files, it will not spread to other users.

Sooner or later computer users find that occasionally lost files. Lost files There are many reasons: users accidentally delete files, bugs can cause damage data files, hardware failure will damage the entire disk, and so on. Damage caused by the missing files vary, and very time-consuming to repair. To ensure that the file is not lost, the basic responsibility of the system administrator of the system is to copy all the files to another location. The administrator also ensure timely backups, and backup tapes (and other media) need to be safely stored. A combination of normal and incremental backups to back up data, you need a minimum of storage space and is the quickest backup method. However, to restore files is time-consuming and difficult because the backup set may be on several disks or tapes, and a combination of normal and differential backups to store backup data more time-consuming, especially when the data changes often, but it's easier restore the data because the backup set is usually stored on only a few disks and tapes. Backup exactly the reverse is restored in the system file is missing or attack paralyzed the situation, we can use the previous data backup data recovery to achieve the purpose of maintaining information security.

System is user-centric, legitimate users can legally operate a series of circles on the system. How to limit the user's illegal operations, which requires the system administrator to control user rights, in order to avoid intentional or unintentional destruction. However, additional security measures must be done by the user, such as:

The user should have a good password security awareness, a user corresponds to a password, the password is the user login or use of resources legitimate path, users must right. Own passwords responsible, to enhance the strength of the password, we can not forget their passwords, especially not at liberty to divulge their passwords to avoid being used by others and result in system damage.

Users must be responsible for their own files. The creator of the file to the file has full control over property or other rights to the file is determined by the user, some sensitive files (such as confidential data, executable files), the user should clear it can be accessed, ensure that the No legitimate users can access it.

On this level, the system temporarily to the virus is not well controlled way. This requires the user when running the program must scan.

Firewall is to protect themselves and prevent external attacks prerequisite software, antivirus software is used to scan documents to and from, and identify the virus killing virus tools, we should update their signatures on the network in order to ensure their own as little as possible He suffered unknown viruses.

Summary

User needs for security will be increasingly high demand for network security and networking services for personal or business will grow. Now we are one by one single application security products, the future will be on integrated defense system on request, which is from a single to a comprehensive change; we now only self-level security requirements for the construction of the future will be the overall safety requirements for construction this is from a point of transition to the global. Overall network security development ideas will change the security network application security, security management discipline will be hot.

Both management and technology complement each other, are indispensable, the proportion of management even more important. No matter how skilled management mess, the same can not reach the network information security requirements. Under the premise of the country, it will gradually establish a network information security system, to provide legal protection for network security and economic security. For enterprises, network information security management as a business course onto the stage, to the best of management companies to reduce costs and expand the efficiency of enterprises, more and more enterprises will gradually establish itself in the next few years information security management system.

References

[1] Bruce Schneier. Secrets and Lies: Digital Security in a Networked World [M] John Wiley & Sons Inc, 2007.

[2] Allen, Julia. Improving the Security of Networked Systems [J] Crosstalk: The Journal of Defense Software Engineering, 2006, 13 (10).

[3] Luo Tao of Computer Network Security and Countermeasures [J] SME Bank management and technology (HEAD), 2010, (4): 205.

[4] Xiong Xiaomin, Wang Zhongrong. Public security information sharing method [J] Political Science and Law, 2005, (12): 85-86.