Research on the Risk Assessment Standard and Method of Computer Network Information Security

Shi Jing[a], Dong Jingjing, Wang Gang, Song Jingjing

Qingzhou High-tech Institute, 262500, China

[a]shijingqz@126.com

Keywords: Risk Assessment, Computer Network, Information Security, Information Technology, Threat

Abstract: More and more people have paid attention to the problem of network security, which has become an important factor affecting the development of information technology. The system security construction, which is marked by the temporary solution of a problem, is far from meeting the requirements of the development of network security protection. Network security assessment, also called network risk assessment, refers to the assessment of threats, impacts and weaknesses of network information and network information processing facilities and the possibility of their occurrence. It is a process of identifying security risks and their magnitude. That is, using appropriate risk assessment tools, including qualitative and quantitative methods, to determine the risk level and priority risk control order of network information assets. The paper presents research on the risk assessment standard and method of computer network information security.

1. Introduction

With the rapid development of computer network technology, global information technology has become a major trend of world development. In today's information society, computer network plays an increasingly important role in politics, economy, military affairs and daily life [1]. Therefore, the dependence of people on computer networks has been greatly strengthened. Most of the existing computer networks have neglected security problems at the beginning of their establishment, and most of them adopt TCP/IP protocol or TCP / IP protocol, which is flawed in their design. Because the TCP/IP protocol is designed to run efficiently, it itself is the main factor that causes the network insecurity.

More and more people pay attention to the problem of network security, which has become an important factor affecting the development of information technology. And the system security construction, marked by the temporary solution of a certain problem as the end of the process, has been far from being able to adapt to the development requirements of network security protection now. This mode often lacks systematic consideration and takes matters into account, with a lot of blindness. Often spent a lot, little effect, resulting in a huge waste of funds and personnel.

The problem of computer network security cannot be solved completely by technology alone. Its solution involves all aspects of policies, regulations, management, standards, technology, etc. Any single level of security measures can not provide a true omnidirectional security; the solution of network security problems should be considered from the point of view of system engineering. In this system engineering, network security evaluation plays an important role. It is the foundation and premise of network security.

Computer network security means that the hardware, software and data in the network system are protected from being damaged, altered or leaked due to accidental or malicious reasons, the network security is essentially the information security on the network. In a broad sense, it involves the confidentiality, integrity and usability of the information on the network. The related technologies and theories of authenticity and controllability are the research fields of network security.

Network physical security: physical conditions of computers, safety standards for physical

environments and facilities, installation and configuration of computer hardware, ancillary equipment and network transmission lines, etc.

Software security: such as protection of network systems from unlawful intrusion, system software and application software from illegal copying, tampering, and protection from viruses, etc.

Data security: such as the protection of network information data security, against illegal access, to protect its integrity, consistency, etc. It is Network security management, such as the security handling of unexpected events during operation, including the adoption of computer security technology, the establishment of a security management system, the conduct of security audits, risk analysis, and so on.

With the development of computer network, its openness, sharing, interconnection degree is expanding, the importance of network and its influence on society are becoming more and more great. However, the problem of network security is becoming more and more important. The network has its own vulnerability. Risk analysis is a fundamental work in building a network protection system and implementing risk management procedures [2]. The purpose of risk management is to ensure that reasonable steps are taken. In order to prevent all incidents that poses a threat to the security of the network.

The security threat of the network and the security measures of the network are intertwined. Improper network security protection may not only fail to reduce the security risks of the network, Waste a large amount of money, and may cause greater security threats. Therefore, careful network security risk analysis is a necessary prerequisite for reliable and effective security protection measures. Network risk analysis should be in the network system, The design phase of an application or information database, so that security requirements can be identified from the beginning of the design, Identify potential losses [3]. Because it is far less economical to implement security control at the design stage than to take the same control after the network system runs. Even if it is considered that the current network system analysis is well established, when establishing security protection, Risk analysis will also identify some potential security problems.

2. The necessity of computer network security evaluation

The network security assessment technology includes two parts: security scanning and subsequent evaluation. It can detect the security vulnerability of remote or local systems, and evaluate the overall security of the system accordingly. This is done automatically by the program, which not only lightens the work of the manager, but also shortens the detection time and makes the problem detection faster. In short, the security assessment technology can quickly and deeply test the vulnerability of the network or local host.

Network security scanning technology is based on Internet remote detection of the target network or local host security vulnerability. Through network security scanning, the system administrator can find the distribution of various TCP/IP ports of the maintained Web server. Open services web services software versions and the security vulnerabilities that these services and software present on the Internet. A nondestructive way to verify that the system is likely to crash. It uses a series of scripts to simulate the attack on the system. This technique is usually used to simulate attack experiment and security audit. Network security scanning technology and firewall, security monitoring system can provide high security for the network.

This kind of attack is the biggest threat to computer network. Malicious attack can be divided into active attack and passive attack. Active attack is to destroy the validity and integrity of information selectively in various ways. Passive attack is to intercept, steal and decipher important confidential information without affecting the normal operation of the network. These two attacks can cause great harm to the computer network. And lead to the leakage of important data. The network software used now has some defects and vulnerabilities more or less. Network hackers usually use the means of trespassing on important information systems, eavesdropping and obtaining, the attack invades important information about sensitivity, modifies and destroys the normal working state of the information network, causes data loss or system paralysis, and causes great political and economic

losses to the country.

A computer virus is an executable program that can be stored, executable, hidden in executable programs and data files without being discovered, triggered and controlled by the system. It is contagious and latent. Computer viruses are mainly transmitted by copying files, transferring files, running programs and so on [4]. In daily use, floppy disk, hard disk, hard disk, etc. The optical disk and network are the main ways to spread the virus. After the computer virus runs, it may reduce the efficiency of the system, damage the file, even delete the file, make the data lose and destroy the hardware of the system. Many malignant viruses that have emerged in recent years have been spread on the Internet. These computer network viruses are very destructive, such as the CIH virus and the panda burning virus. It brings serious losses to the network.

The first stage of PING scanning for network security scanning can help us to identify whether the system is active. Ping sweep is also called ICMP sweep, which is one of the basic network security scanning techniques. A single ping can help us identify whether a host is active in the network, while ICMP straps contain ICMP ECHO (ICMP response request packets. If the host address is alive, it will respond to the ICMP ECHO. ICMP strafing applies to small or medium networks, which is slow for some large networks.

There are many tools that can be used for ICMP shooting, such as the pinger software of Unix system fpinggpingnmaprhino9, which is used for ICMP straining of Solar Wind in Windows system. Both pinger and ICMP can send multiple packets at the same time and allow users to parse the host address. Store the data in a file. The administrator will stop shooting if the ICMP repeats requests from the outside. But you can also detect the host by using ICMP timestamp requests and address mask requests.

3. Research on computer network information security and protection strategy

Buffer overflow: the most common system vulnerability in a buffer overflow computer system. It is also the most frequently used vulnerability by hackers because many software systems are designed, the designer does not have the function of designing a check program and a buffer in order to pursue the speed of the design. If the computer receives the length of data when it uses the software, it will automatically place the overflow part in the stack, and the system will automatically determine that the stack is running properly and the stack capacity is limited [5]. If the data is stacked too much, it will inevitably affect the normal operation of the system. This will also give hackers a loophole that can be fully exploited by sending out a large amount of length data to the computer. When the amount of data in the stack exceeds the storage capacity of the buffer, the computer system will run slowly and the serious computer system will no longer be able to run.

Denial of service vulnerability: denial of service refers to distributed denial of service, which is also a common system vulnerability used by hackers. This attack is persistent by disrupting the TCP/IP connection order in a software system. The most representative of these attacks is the Synnood attack, which relies on sending a large number of legitimate requests to connect and block the system's communication and data transmission channels. Slow down the system until the system fails to function properly. The distributed denial of service DDoS is developed on the basis of Doss. It is much more destructive than normal Dos.

Information security evaluation involves all aspects of safety standards is also very complex, various evaluation criteria focus is not the same, such as the evaluation criteria for information technology security (CC) > and < DOD trusted computer evaluation criteria (TCSEC) evaluation > and so is more focused on the technical indicators of the system and products; "system security engineering capability maturity model (SSE-CMM) > focus more on security product development, system integration and other safety engineering safety management in the process of.ISO/IEC 17799 (also known as ISO 27001 and ISO 27002) has irreplaceable status of daily safety management information system at present, therefore, many foreign companies to accept the ISO 27001:2005 (BS7799-2) certification, information security management system certification.

The domestic situation is relatively simple, due to a security risk assessment research started late,

the overall domestic and reference in the initial stage, in the study of standard security risk assessment is still in the initial stage of exploration following the international standard. The national quality and technical supervision in 2001 according to the international standards promulgated by the CC GB/T 18336< information security technology information security technology the evaluation criteria for GB17859< >, computer information system security classification standards for relevant standards and on the basis of the TCSEC and the red book published in 1999, and China's specific information system security risk assessment standard "information security technology, information security risk assessment specification (GB20984-2007) and" information security risk management guide.

One of the most famous functions of operating system detection, also known as Nampan Nmap, is to use TCP/IP protocol stack fingerprinting to detect remote operating systems. Nmap sends a series of TCP and UDP messages to remote hosts. Check each bit in the response. After performing a dozen tests such as TCP ISN sampling options support and sorting IP ID sampling, and initial window size checking, Nmap compares the results to the fingerprints of more than 1500 known operating systems in the database nmap-os-fingerprints, if there is a match, print out the operating system details. Each fingerprint includes a free-form description of the OS, and a classification information.

4. Research on the risk assessment standard and method of computer network information security

In order to maximize user friendliness, many companies configure complete tool software to improve system management and quality of service on their software systems products. This software is indispensable for users to use and maintain the system. But in the hands of hackers, it becomes an important tool to attack network security [6]. In fact, hackers can easily use software tools provided by software vendors to collect all kinds of illegal information. For example, in the case of the most commonly used system tool, Packetsnifer, which is mainly used to monitor and distribute network packets, in the case of such attacks, Hackers usually use the attack method of information explosion, that is, put a large amount of information in the system tool Packetsniffer. In a short period of time, the system is paralyzed.

In the process of using the computer system, the user needs to maintain the system regularly, remove the garbage generated when the system is running, and increase the running speed of the system. And if the system's maintenance measures also leave a lot of security risks to computer information and network security. In general, the method of patching is used. But as the use of the depth will also appear new vulnerabilities, although through system maintenance and software upgrades, can effectively maintain the security of the system, but large-scale routers, Firewall filtering rules have not changed, this is not simply relying on software upgrades and patches can be resolved.

At present, the "information system security level protection" in our country is also an important form of information security evaluation, which is no less important than the first time the United States conducted in two and a half years at the beginning of 60s.

The domestic situation of information system security level protection is similar to that of the Federal Information Security Management Act (FISMAA) issued on 2002 in the United States, which seeks to ensure federal agencies by taking appropriate security control measures. Information system security, it is an important development plan in the field of information security in the United States.

In recent years, FireWall has become a new technical measure to protect computer network security. It is a kind of isolation control technology, which sets up a barrier between an organization's network and an insecure network (such as Internet) to prevent illegal access to information resources. Firewalls can also be used to prevent important information from being illegally exported from the enterprise's network. FireWall, a security protection software for Internet networks, has been widely used.

The FireWall software is set up between the enterprise network and Internet. The enterprise information system adopts the selective receiving method for the access from Internet. It can allow or

prohibit the access of a kind of specific IP address. You can also receive or reject a specific type of application on the TCP/IP. If you have information or dangerous users that need to be banned on an IP host, if an enterprise only uses Internet's e-mail and WWW servers to provide information to the outside, then you can set up data packets on the FireWall that only these two types of applications can pass through. For the router, it is necessary not only to analyze the information of the IP layer, you also need to learn more about the TCP transport layer or even the application layer to make a choice.

Firewall is typically installed on a router to protect a subnet, or it can be installed on a host. Protect this host from invasiveness. Operating system detection can be performed on other tests that can take advantage of information gathered during processing, such as runtime detection, Using the TCP timestamp option RFC1323) to estimate the host's last restart time, this applies only to the host that provides this information.

The other is the TCP sequence number prediction classification. The possible difficulty of testing a fake TCP connection against a remote host. This is important for exploiting a trusted relationship based on the source IP address, firewall filtering, etc.) or an implicit source address attack. Scam attacks are rare now. But some hosts still have this vulnerability. The actual difficulty value is based on statistical sampling, so there may be some fluctuations. For example, "worthy challenge" or "trivial joke". Output in detail mode only in a normal way. If -O is used simultaneously, IPID sequence generation numbers are reported. Many hosts have serial numbers of "add" category, adding an ID field value to each packet's IP header is a vulnerability to some advanced information-gathering and spoofing attacks.

5. Conclusions

The information security of the network is a changing and fast updating field. This means that it is impossible to guarantee the information security of the network by using a certain kind of protection measures. Therefore, we must use various protection strategies comprehensively, and cooperate with each other so as to establish a protection system for network information security. Therefore, we must be very cautious about the protection of the information security of the network, minimize the possibility of the hacker ' s invasion, and thus protect the security of the network information.

References

[1] Zhao Qingxiang, Liu Ziqiang, Jin Yongjie. Analysis of computer Network Security in the Information Age. Information Security and Communication Security, 2012.11:12-23.

[2] Feng Qiuyu, Sun Yulan. Analysis of computer Network Security and Prevention Technology. Heilongjiang Metallurgical Technology 2015,3:50-60.

[3] Huang Wei. Intranet Information Security based on Digital Signature Technology. Computer knowledge and Technology, 2014.3.

[4] Song Yunhui, white. Xinguo digital signature technology principle and application. Fujian computer, 2015:100-105.

[5] Peng Xiaoming. Exploration of Security Technology to deal with the rapidly developing computer Network. Silicon Valley, 2015, 26 (6): 285-287.

[6] Su Xiao-qing, Sheng Zhihua. Development of computer network security technology and discussion of firewall technology. Scientific and technological Innovation Guide,2016:20-30.