Study on Computer Security Focus and Its Key Technologies

Dongyan Jiao

School of Information & Engineering, the Open University of Guangdong, Guangzhou, Guangdong, 510091

Keywords: Computer Security Focus, Key Technology, Internet Technology

Abstract: The development of information technology poses new challenges to information security. Computer security monitoring system is an effective mechanism to ensure information security. It protects and monitors all kinds of information and user operations in local or remote computers through data acquisition, analysis and processing, rule identification, non-compliance and full record keeping. This paper mainly studies the key technologies of monitoring based on documents, texts and user operations. By comparing and analyzing the implementation mechanism and application environment of these key technologies experimentally, it is of great significance to strengthen system functions and improve monitoring efficiency and stability.

1. Introduction

With the rapid development of information technology, the application and coverage of computer networks have gradually increased, making computer networks an indispensable and important component in people's daily life. However, in the actual application of computer network, the computer network will be attacked by viruses and hackers, making the computer network security can not be effectively protected, and even cause a lot of user losses. Therefore, it is necessary to strengthen the protection of computer network security, analyze the influencing factors of computer network security, and combine with the actual situation of computer network, apply the key technology of virus protection rationally, and effectively improve the computer network security factor, to avoid the harm caused by computer viruses [1].

2. Main factors affecting computer network security

Internet security vulnerabilities caused by computer network security risks an important factor. At this stage, the computer network in the actual use of the process, will support multi-user operation and data transmission and sharing, resulting in computer network security loopholes, affecting the safety of computer networks. In addition, some related software are used in the actual application process of the computer network. However, in the actual application process of the software, some vulnerabilities will be generated. These security vulnerabilities cause the computer network to be attacked by hackers, a direct result of the computer network security, resulting in economic losses to users [2].

Computer virus is an important factor that affects computer network security. Computer virus has the characteristics of fast spread and wide range of influence. Computer virus has strong spread, and it is difficult for computer virus to be cleaned up and seriously affect the usage of computer network. Safety. Computer viruses can have an impact on the functions of computers and affect the normal use of computers, resulting in the loss of personal information inside computers and impelling criminals to take advantage of them. As a result, personal safety and property safety of computer users are threatened. Users in the actual use of the computer process, will use some of the information transmission and sharing, or the use of computer networks, some web pages and documents received, can give the virus the opportunity to spread, making the computer infected with the virus, resulting in computer network security can not be guaranteed. Users in the actual process of using computer networks, will use some software, and these software installation process, there may be a virus. Maliciously installed software is stubborn and not easily removed, resulting in the rewriting of the computer's internal procedures, to the customer's computer network security

risks [3].

Hackers are important factors that affect the security of the network. Hackers refer to those who have high computer network technology, through the use of hidden Trojans to computer virus implantation, and through special means of implantation of the virus to use, steal The user's personal information, damage the computer program. Making computer network security can not be guaranteed. At this stage, hackers will use electronic bait, mail, IP address, DOS attacks and other ways to achieve the computer network attacks, resulting in the loss of user-related information. Moreover, with the continuous progress of information technology, hackers constantly update the means of attack, the update of computer network security tools gradually can not meet the needs of the virus protection.

3. Host system vulnerability assessment

In recent years, the rapid development of network technology, at the same time, malicious attacks and illegal access activities are also more diverse and cumbersome, the most prominent network viruses, mainly in accordance with the automated way, spread through the software security vulnerabilities and spread, for computer systems attack on purpose. The security risks mentioned above pose a serious threat to the normal operation and steady use of computer systems. To increase system security and improve information reliability, system administrators and developers are striving to explore autonomous and effective techniques to prevent vulnerabilities, and triggering a high degree of hot debate. Weakness assessment specifically refers to the implementation of the computer, a clear network of security vulnerabilities under the effect of the amount of loss, vulnerability assessment, effective control of the actual security risk of computer systems to promote security, to provide them with scientific decision-making information, thereby preventing the danger The emergence of the incident. Weakness assessment technology is more active, and has a certain degree of advance, superior to intrusion detection technology. With reference to the evaluation object, the vulnerability evaluation can be divided into many types such as host system evaluation, computer firewall evaluation and network software system evaluation. The author will mainly discuss host system evaluation. The host system usually contains multiple software, and the software can be seen as a system component, the original assessment method is only the analysis of individual component vulnerabilities, regardless of the adverse threat caused by the association within multiple component vulnerabilities, while the original assessment The method only uses the quantity of weakness to express the systematic risk, this kind of form will induce the weakness misjudgment phenomenon. To make up for this deficiency, the author puts forward the assessment method based on the weak point correlation chart. This method not only applies the weakness correlation thought, but also applies the comprehensive analysis method and selects the index evaluation strategy to evaluate the security risk caused by the weakness in the organizational design, implementation and operation, and comprehensively compares each system with all versions in Security at any level [4].

It is well-known that at the host system level, an attacker can only rely on the same weaknesses contained in the same operating system when executing a multi-level attack. Therefore, there is a corresponding and unique vulnerability association subgraph for each operating system version. The weakness associated subgraph contains the independent weakness and the associated weakness chain. If we want to make a quantitative evaluation around the security trend within the operating system, we should provide the theoretical formula of risk calculation corresponding to the weakness and weakness chain, and calculate the risk according to the formula.

Under normal conditions, prior to the implementation of the assessment activities, the target should be clearly evaluated. For the evaluation of the host vulnerabilities explored in this article, the corresponding assessment objects mainly include the real operating system, basic components, various softwares, and different databases. The risk calculation based on the object of assessment is generally based on the calculation of the risk of the weakness. The Jones index is used to select the sequence of weaknesses with higher risk coefficient as the evaluation basis of the system as a whole, and the risk value of the object to be evaluated is represented by the matrix [5]. The main

application is micro and macro These two methods of analysis. According to the running status of the software, the vulnerability evaluation can be divided into two types: dynamic evaluation and static evaluation. The former also includes host scanning and network scanning evaluation. From this, we can see that the assessment method used to evaluate the weakness of the host system based on the weak point correlation diagram should generally involve the dynamic assessment based on the host scan, the dynamic assessment based on the network scan, the static assessment based on the network scan. Before formal implementation of the above evaluation algorithm requires the following two tasks to be fulfilled: First, pre-designed quantitative features exist for each known weakness; secondly, a VGR covering a variety of well-defined vulnerabilities can be generated.

4. Computer network security virus protection key technologies

Security scan is the discovery of hidden viruses, malware, vulnerabilities and other in-depth scanning of the computer, and with anti-virus software to clean up and killing the virus to improve the computer's safety factor. Computer network security scanning at this stage are: heuristic scanning, behavioral scanning, fuzzy matching and other scanning techniques, through the application of these scanning techniques, to computer network information content, invasion area, decoy area, etc. to scan, so as to effectively To improve the computer's virus protection, improve computer network security factor. For vulnerability scanning in computer network security scanning, it is necessary to periodically repair and improve the vulnerabilities of computer networks and improve the security factor of computer networks.

At this stage, the virus will spread through the USB, download files, electronic bait, mail, receiving files, etc., making the computer network users inadvertently infected, affecting the quality of the use of the computer. Therefore, a reasonable anti-virus software installation. After the software is installed, it can detect the U disk, software, files and so on. If there is a security problem, it will give a timely warning to avoid the acceptance of malware and hidden trojan files, effectively improve the computer network's virus protection and reduce the computer Network may be infected by the virus. Anti-virus software can judge the browsing webpage and prompt related warning information when webpage browsing and mail receiving, to avoid user's mistake.

The establishment of a security template is an effective measure to improve the security of computer networks. Initial establishment of a security module allows the initial interception of a virus, mainly allowing fixed users to enter and use it, specifying the time of use, and logging in to unauthorized users in time for processing. Security module, but also according to the use of computer network users, the process and the use of related processes to monitor and record, prompting users to understand the relevant information on the security situation of the computer network to prevent the computer from virus intrusion and did not find The situation, to avoid the occurrence of security risks.

Network encryption, network encryption is mainly for the computer's use, the establishment of a user's unique user name and password, and set the main control, limit other users log in operation, other users even through the login settings, the relevant operation will be limited, Can not complete the relevant information and data acquisition, thus avoiding the loss of data in the computer. Combined with advanced login methods, such as fingerprint scanning, iris scanning and other ways to achieve computer network encryption, thereby effectively increasing the computer's login restrictions.

Learning, adaptive, dynamic adaptive network security model PPDR can be a self-learning ability, self-adaptability of the security model, the application of the model can effectively improve the computer network virus protection. And dynamic adaptive network security model PPDR can intelligently control the virus intrusion, according to the computer scan and detect the situation, intelligent learning of the virus, the formation of a new type of virus defense system that can effectively target the type of virus and Type, complete the virus control and killing, improve the computer's safety factor.

5. Conclusions

At this stage, all sectors of society have reached a consensus in the development of computer networks and work together to build an information network platform. To achieve this goal, we must first provide a solid and reliable security guarantee. It is not difficult to find that putting forward feasible solutions to potential safety problems is of great concern to the whole society. Whether from the LAN level, or from the perspective of the Internet, are involved in the issue of information protection. Therefore, we should combine all kinds of potential safety hazards, put forward effective security measures, comprehensively weigh the characteristics of various threats, and effectively protect the network information and data, and constantly upgrade the level of security technology to achieve the sustainable development of computers.

Acknowledgements

Fund Project: Construction of Open Education Teaching Platform under the Background of Enterprise Transformation and Upgrade

Large Scientific Research Project (2016GXKJK241) Application of Big Data in Precision Fisheries and Research on Key Technologies Guangdong Provincial Department of Education (2016KTSCX191)

References

[1] Xia Wei. Talking about the computer security monitoring system technology [J]. Communication World. 2015 (19): 92~95.

[2] Zeng Feng. Computer security monitoring system technology [J]. Electronic Technology and Software Engineering. 2017 (23): 11~17

[3] that generalized. Computer security monitoring system technology [J]. Communication World. 2017 (02): 106~110

[4] Lin Junfeng, Li Ke. Construction of Safety Monitoring System for Construction Site Based on BIM Technology [J]. Automation & Instrumentation. 2017 (08): 81~85

[5] Wen Zhen. Multimedia security monitoring system [J]. Journal of University of Electronic Science and Technology of China. 2006 (01): 75~80