Analysis of Computer Network Security Vulnerabilities and Preventive Measures Based on Big Data Thinking

Feijian Xu

Guangdong University of Science and Technology, No. 99 Xihu Road, Nancheng District, Dongguan City, 523083, Guangdong Province, China

email: 406877460@qq.com

Keywords: Big Data; Networks; Security Vulnerabilities

Abstract: In the era of big data, network technology has been fully popularized and applied, bringing great convenience to people's life and work. However, with the development of network technology, some network security problems follow. Computer network security is also a headache, once there are network vulnerabilities, information leakage or loss will bring us a painful loss. The protection of computer network security vulnerabilities has always been the focus of people's attention. It is necessary to analyze the causes of network security vulnerabilities in order to effectively protect and control them. Network security has both technical and management issues. Strengthening the security protection of computer networks, and taking effective preventive measures against the security problems of current computer network systems is an important way to ensure the safe use of the network.

1. Introduction

The concept of big data emerged in the context of cloud technology. Big data refers to a large amount of data existing in computer networks. Computer network system has the characteristic of resource sharing, which can satisfy the interaction and communication between users to the greatest extent [1]. It increases the extensibility of computer systems, but there are also many loopholes, which can be used to attack. The problems faced by network security also appear diversified phenomena. Network security vulnerabilities such as network virus intrusion and hacker pilferage affect people's use of the network, and also pose a serious threat to people's information security [2]. The specific meaning of computer network security essentially includes the hardware and software that make up the network system and the security of the information transmitted on the network. The emergence of big data is very close to the network, because with the development of networks and related technologies, large-scale data collection and detailed and reliable analysis are possible [3]. Today's social data and information are becoming more and more important, information technology is developing rapidly, and computer networks are widely used in people's production and life.

With the advent of the era of big data, the way people access resources has changed dramatically. The application of big data in the fields of networks, computers, terminals, etc. has great advantages [4]. The link is the basis of the computer system's work. When the link is transmitting and receiving network files, due to the vulnerabilities in the system, it will be attacked by files or systems more or less [5]. In the network, it is often found that a large amount of information of a user is stolen. Sometimes, when the network security problem is serious, the user's information is lost, and the computer is damaged [6]. Network security has both technical and managerial problems, which complement each other and are indispensable. Everything has two sides. Big data brings convenience to people's life, but also threatens the information security of computer network [7]. The current world is a digital world, which can comprehensively perceive, preserve and share all kinds of data resources [8]. To strengthen the security protection of computer network, in view of the current security problems of computer network system, adopting effective defensive means is an important way to ensure the safe use of network.

DOI: 10.25236/mmmce.2019.082

2. Relevant Network Security Problems in the Age of Big Data

2.1. Network Security Problems Caused by Network Systems

In the course of the development of computers, it can be seen that computers have gradually integrated into all aspects of people's lives. Up to now, people's lives and work have been inseparable from computers, and they have become extremely dependent on them. Security vulnerabilities are one of the common problems in the development of computer network technology, but hackers and virus makers are exploiting this vulnerability to attack computer networks. On the Internet, the use of passwords is the most common and important security method [9]. Therefore, access to passwords is also an important way for hackers to attack. In the process of the continuous development of network technology, network viruses are also constantly evolving. An attacker can send a large number of forged requests to the target host, thus causing system blockage. Make the target system deny access to normal services and can no longer provide services for other normal requests. Due to the limitations of current technology, there are many loopholes in a system itself, so it is necessary to install software patches after release, and constantly update and add patches.

2.2. Strengthen the Supervision of Computer Networks

The security vulnerabilities of computer networks are various, and the network viruses produced are also diverse. Some viruses are specially designed to steal user messages, while others are specially designed to destroy, destroying all data of users, which is totally destructive virus. In network operation, password is a common means set by users to protect personal information from being leaked and stolen. We always need to authenticate by password, which naturally makes deciphering the password an important way for attackers to attack. Due to the different manifestations of computer network security vulnerabilities, the classification methods are different. In order to prevent this kind of attack, users must set the password as complex as possible, or use multiple layers of passwords. When downloading data online, be sure to scan for viruses before using them and use decompilation software. Some bad software downloaded by users may cause security problems in the computer network due to some security risks in the software itself. The Figure 1 shows the framework of the security situation prediction model.

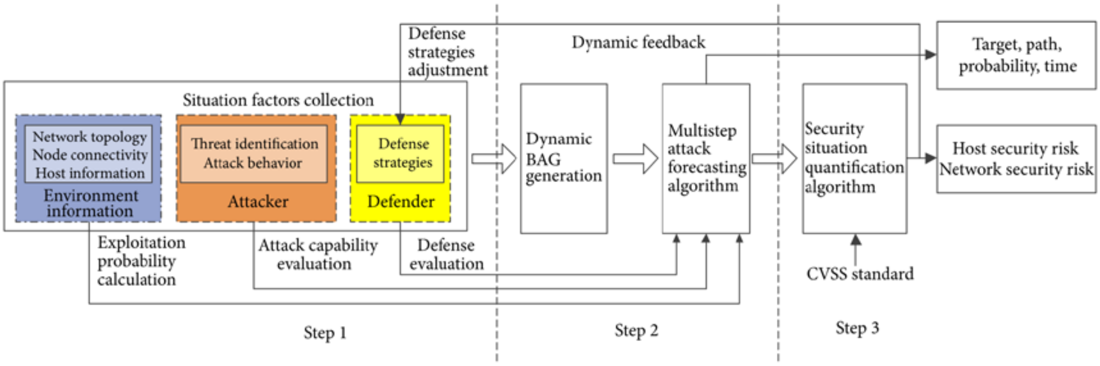

Fig.2. Framework of security situation prediction model

3. Cause Analysis of Computer Network Security Vulnerabilities

In order to fully maintain the security of network information, strengthening computer network management is an important means. If the user downloads and runs a program with a Trojan horse bundled without knowing it, the Trojan horse that is planted can directly invade the target host and destroy it. In order to effectively improve communication and interaction between users, it is necessary to continuously expand the functions of computer systems to meet the needs of users for various computer functions to the greatest extent. For personal Internet users, it is possible to be attacked by a large number of data packets, making it impossible to perform normal network operations. Therefore, the firewall software must be installed when surfing the Internet [10]. In some government agencies, the management of the network is particularly important. If the important internal information of government agencies is obtained by some illegal elements, the consequences will be unthinkable. Agent technology can directly analyze the data received by the program and generate encrypted list information for users to view.

If we do not take effective security defense measures, it will make the user's information unprotected, affecting the security of network information. A small experimental network is established, and its topology is shown in Figure 3. The network includes firewall, intrusion detection system, five victim hosts and one attack host. By presupposing the firewall strategy, the network is divided into two subnetworks.

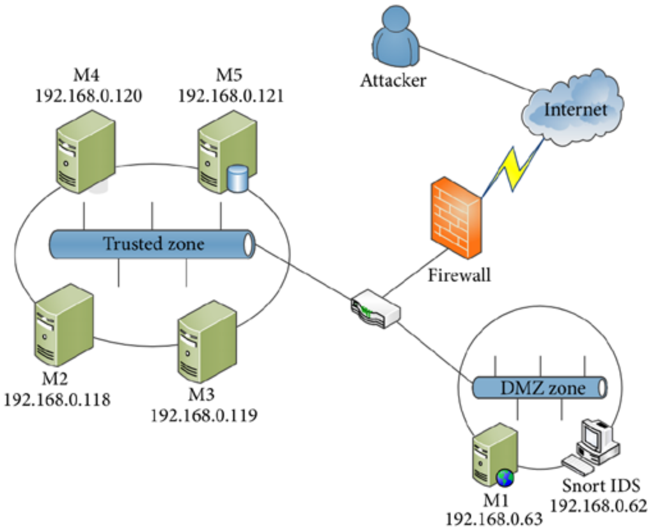

Fig.3. Experimental network topology

Big data has been applied in various fields in the process of development. Big data is also convenient for people, but it also creates certain security risks. The firewall can identify the security user, maintain its login rights, or restrict the user login by password or password, and control the illegal access in real time. Because the security problems in computer networks are various, when protecting computer network security vulnerabilities, it is necessary to analyze the causes of computer network security vulnerabilities according to the types of security vulnerabilities.Computer viruses have the characteristics of dependency, variability and so on. They are very powerful against security vulnerabilities. Once you enter the computer network, you can quickly find and enter the system through system vulnerabilities, complete the interference and destruction of the system. Computer network system has corresponding programs to protect users'basic information. Although this can protect users' basic information, users still need to enhance their awareness of network security.

4. Conclusions

With the arrival of the era of big data, great changes have taken place in people's lives. The development of computer network technology has played a positive role in human society. Computer network brings convenience to human beings, but also brings security risks. Because the technology is not yet mature and system vulnerabilities are everywhere, it gives illegal elements a chance to take advantage of it. In this paper, the network vulnerabilities in the era of big data are analyzed and discussed, and the corresponding solutions are put forward. As computer network security issues become more and more important, people have also strengthened their research on network security technologies. In order to effectively control the security of computer networks, it is necessary to analyze the computer network security issues in depth. In the specific work, it is necessary to make detailed and comprehensive multi-level security precautions according to the actual situation of the network, and improve the security and reliability of the network system as much as possible. In the specific protection process, it is necessary to comprehensively utilize firewall technology and anti-virus software control technology to protect network security. Scientific and reasonable development of network security protection measures can effectively improve the security of computer network systems.

References

[1] He D, Chan S, Guizani M. Small data dissemination for wireless sensor networks: The security aspect. IEEE Wireless Communications, 2014, 21(3):110-116.

[2] Signature Based Vulnerability Detection Over Wireless Sensor Network for Reliable Data Transmission. Wireless Personal Communications, 2016, 87(2):431-442.

[3] Busby J W, Cook K H, Vizy E K, et al. Identifying hot spots of security vulnerability associated with climate change in Africa. Climatic Change, 2014, 124(4):717-731.

[4] Afful-Dadzie A, Allen T T. Data-Driven Cyber-Vulnerability Maintenance Policies. Journal of Quality Technology, 2014, 46(3):234-250.

[5] Erlich Y, Narayanan A. Routes for breaching and protecting genetic privacy. Nature Reviews Genetics, 2014, 15(6):409-421.

[6] Delahoz Y, Labrador M. Survey on Fall Detection and Fall Prevention Using Wearable and External Sensors. Sensors, 2014, 14(10):19806-19842.

[7] Sorichetta A, Ballabio C, Masetti M, et al. A comparison of data-driven groundwater vulnerability assessment methods.. Ground Water, 2013, 51(6):866-879.

[8] Sliti M, Boudriga N. BHP flooding vulnerability and countermeasure. Photonic Network Communication, 2014, 29(2):198-213.

[9] Schafer B, Edwards L. “I spy, with my little sensor”: fair data handling practices for robots between privacy, copyright and security. Connection Science, 2017, 29(3):200-209.

[10] Taherifard M, Patooghy A, Fazeli M. Vulnerability modelling of crypto-chips against scan-based attacks. IET Information Security, 2018, 12(6):543-550.