Analysis and Research of Computer Network Security Emergency Response Technology Based on Large Data Mining

Chenglong Du

Guangdong University of Science and Technology, Dongguan, Guangdong, 523073, China

email: 179074904@qq.com

Keywords: Data Mining; Computer Network Security; Emergency Response

Abstract: With the continuous development of the Internet, computer network security issues have become increasingly prominent, in this case, data mining technology is particularly important. Information on the Internet has brought great convenience to human life, but the characteristics of the network itself, such as openness, freedom and interconnection, have led to the unavoidable security risks of the network. The interests of the vast number of network users have been seriously damaged. This paper will analyze various potential safety problems in the current computer network operation, and on this basis, build a network security emergency response system, and analyze the working mechanism of the system.

1. Introduction

With the continuous integration of computer technology and communication technology, and the accelerating process of network and informationization in China, the Internet is increasingly inseparable from political, economic and cultural life, and various Internet applications are integrated into all aspects of people's lives [1]. The so-called computer network security actually refers to the components of the computer network system, that is, the hardware system and software resources and related supporting information data, which are effectively protected from being damaged, altered and leaked. With the continuous development of the Internet, due to the openness of the network and other characteristics, it is easy to have network security problems such as information leakage during the use of the network, and data mining technology has emerged [2]. Data mining is a newly developed computer technology in recent years [3]. It includes aspects that need to be addressed. The most confusing is the tasks in the fields of data mining and information retrieval. Only when the network has complete security measures can it play its due role, otherwise it may bring some harm to the network users and even affect the national security. Therefore, applying data mining technology to the field of computer network security is of great significance for effectively avoiding network security incidents and maintaining network order.

2. Basic Principles of Data Mining Technology

Data mining technology is an important component of computer network technology. Data mining technology, as its name implies, refers to the application of computer network technology to screen out the required data information from massive information and make statistical analysis of this information. For example, using DBMS to find records or searching for information in the search box are all information retrieval [4]. Obviously, information retrieval relies on keywords and features of information. After defining the objects and targets of data analysis, relevant information is collected, and the data related to it are filtered, leaving behind the core data. At the same time, however, a large amount of data often prevents users from identifying information that is hidden in it and can support and help decision-making [5]. Traditional query and reporting tools are no longer sufficient for mining this information. With the increasing number of Internet users, the Internet has become more convenient and faster, and it has become more dangerous. Through the Internet, we can more easily obtain the information we need. In addition, the specific analysis results should be presented to the

Copyright © (2019) Francis Academic Press, UK DOI: 10.25236/mmmce.2019.078

network users. In this process, the unsafe information attached to them should be filtered and filtered to better ensure the security of the user's computer network.

3. Network Security Emergency Response Technology

3.1. Operating system hardening optimization technology

The operating system is the basis of computer network applications and services. Only a safe and reliable operating system environment can ensure the security and stability of the overall system. It has the function of identification, analysis and evaluation. Through the system's internal event generator, analyzer, database and response unit, it can effectively detect the computer network [6]. It is characterized by the fact that all communication records are known to be generated by the network Trojan and botnet programs during the communication process. The source and source ports are information of the controlled host, and the destination and destination ports are information of the controlled host. The reinforcement and optimization of the operating system can be realized through two ways: establishing the service and application on the operating system with higher security level; Constantly improve the existing operating system, through self-learning, self-improvement, and constantly revise the loopholes found in the operating system [7]. Different from the passive defense of firewall technology, it integrates the three functions of intrusion detection, network management and network monitoring, and has the characteristics of intelligence and comprehensiveness, forming an active protection mode.

3.2. Digital encryption technology

The so-called digital encryption technology is to carry out special coding on the information to be protected in the network, transforming the information into information that cannot be recognized by illegal users. In this way, even if the information in the network is stolen by illegal users, the content of the information cannot be identified. In practice, we have seen that since the data information encryption technology can only be opened by the other party if both parties are authorized, the performance of this technology in protecting information and data security is very significant [8]. Among the computer network emergency response methods, a timely and active emergency response technology is attack suppression technology. For information security incidents that have already occurred, effective measures such as attack source isolation must be taken immediately to suppress them to prevent the continued expansion of adverse consequences. Also pay attention to the backup of data information, that is, before the computer network information is destroyed, modern important information data is backed up, so as to avoid data loss, tampering and other problems after the network is invaded or after a failure. In order to prevent information leakage, information must be encrypted so that when the LAN is connected to the Internet, the security of the information can be fully guaranteed.

3.3. Access control technology

Access to the computer network must be effectively controlled to filter illegal users and reduce network security risks. For e-mail inside the network, in order to effectively identify some viruses hidden in mails or attachments during the information exchange process, an effective anti-virus software based on the e-mail server system must be added. This technique is primarily analyzed and processed by the attacker's trajectory throughout the network. The tracking technology of computer network can be divided into two types: one is active tracking technology, and the other is passive tracking technology. Its theoretical basis is that it will display different network data characteristics according to different states of computer network. The rules that must be followed in establishing access network are constrained for every user and must be followed unconditionally by every network user. The purpose of restraint is to limit the scope and extent of the impact of events. It is to isolate and deal with the fault system or area effectively at the first time of the event, or according to the resource status and event level. These principles include the steps of accessing the network, the way of authorization, the strategy of control, the form of access and the division of security level.

4. Research on Network Security Emergency Response System

Network security emergency response technology is one of the frontier research fields in information security. With the deepening of the research, it breaks through the original PDRR model and organically combines the two security mechanisms of "response" and "recovery" into a relatively perfect emergency response system. Network security emergency response technology is one of the frontier research fields in information security. With the deepening of the research, it breaks through the original PDRR model and organically combines the two security mechanisms of "response" and "recovery" into a relatively perfect emergency response system. Computer network mining technology is of great significance to network security. From this perspective, we must actively start from the theoretical knowledge and strengthen the training and education of network technicians. The network detection attack is discovered by the intrusion detection module, and the collected attack information is analyzed and organized by the analysis processing module, and a preliminary disposal plan is formed according to the preset policy and event disposal rules, and the disposal plan and the attack information are notified to the management platform. The system organically realizes the linkage of various types of safety emergency response technologies. The schematic diagram is shown in Figure 1.

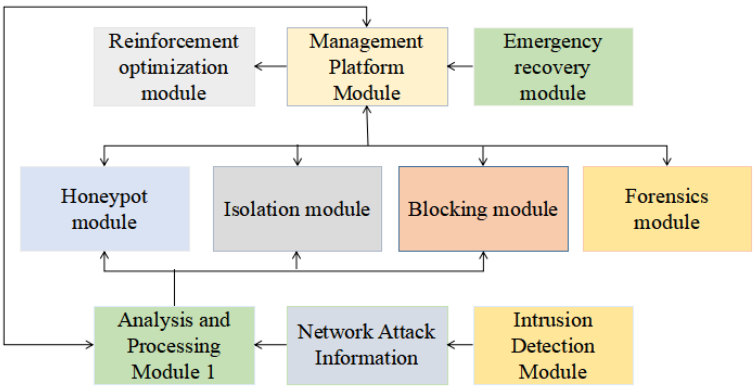

Fig.1. Schematic diagram of network security emergency response system

Many network administrators have not received formal education, and their sense of responsibility and technical level have not reached the quality that a qualified network administrator should have. This is often reflected in the actual work, and there will be many unreasonable human management mistakes. In order to ensure the effective detection capability of computer system, the model needs to be upgraded in time. And compare the differences between them and normal computer users' activities, build corresponding models through analysis and research, and organically count the occurrence probability and quantity of these abnormal model users' behavior states. For a high-risk attack behavior, the attacker's attack operation is recorded by the system while the blocking or isolation module is started, and the tracking module is called to track the attack source to collect and determine the attack information. For a specified type of security event, the system generates a security event propagation curve by calculating the number of source addresses that have sent such events within a fixed event interval. This curve reflects the propagation process of a specified type of event.

The administrator adjusts the information collected by the management platform, system module and tracking module to adjust the automatic protection scheme, and can take further measures, such as forensics on the attack site through the forensic module. The security situation assessment algorithm is the core of the project research. When conducting the security situation assessment, it is necessary to construct a series of benchmark indicators that can reflect the security status of the network, and quantify the massive attack events into specific indicator values, and evaluate the current network. Security status. The administrator will make a comprehensive analysis of this attack and the emergency protection measures taken, further improve the analysis and processing mechanism, and set more reasonable protection rules to ensure that the emergency protection system can take more effective and timely protection measures for the next similar attack. If some

administrators cannot prevent and limit the potential security risks in time and give too much authority to network users, these practices will easily bring great harm to computer networks.

5. Conclusions

With the continuous development of information technology, network security threats are becoming more and more prominent. In order to better deal with various network attacks and virus damage and improve the timeliness and effectiveness of emergency response, new emergency response technologies and tools are continuously developing and improving, but the actual challenge is still greater than the opportunity. The development of the future society cannot be separated from the network, therefore, in order to ensure the safety of the computer network, various possible security strategies and emergency response technologies should be adopted. In general, data mining technology is of great significance to network security. We must attach great importance to it and give full play to the positive significance of data mining to network security, so as to better ensure China's network security and promote China's social stability and harmony. On the basis of traditional computer network security, relevant security technicians should exert their subjective initiative to carry out security technology research and bring into play the great potential of data mining technology.

References

[1] Dupont Q, Fidler B. Edge Cryptography and the Codevelopment of Computer Networks and Cybersecurity. IEEE Annals of the History of Computing, 2016, 38(4):55-73.

[2] Jakalan A, Gong J, Su Q, et al. Social relationship discovery of IP addresses in the managed IP networks by observing traffic at network boundary. Computer Networks, 2016, 100:12-27.

[3] Krzysztof S, Liqiang W, Xiangyang L, et al. Big Data Analytics for Information Security. Security and Communication Networks, 2018, 2018:1-2.

[4] Stasiuk O I, Grishchuk R V, Goncharova L L. Mathematical Differential Models and Methods for Assessing the Cybersecurity of Intelligent Computer Networks for Control of Technological Processes of Railway Power Supply. Cybernetics and Systems Analysis, 2018, 54(4):671-677.

[5] Ni Z, Li Q, Liu G. Game-Model-Based Network Security Risk Control. Computer, 2018, 51(4):28-38.

[6] Bisht N, Ahmad A, Bisht S. Application of Feature Selection Methods and Ensembles on Network Security Dataset. International Journal of Computer Applications, 2016, 135(11):1-5.

[7] Ender Yüksel, Nielson H R, Nielson F. A Secure Key Establishment Protocol for ZigBee Wireless Sensor Networks. The Computer Journal, 2018, 54(4):589-601.

[8] Collins J, Agaian S. Trends Toward Real-Time Network Data Steganography. International Journal of Network Security & Its Applications, 2016, 8(2):01-21.