Application of Big Data Analysis Technology in Remote Network Attack Defense

Lili Gao

gaolily@126.com

Shandong Agriculture and Engineering University, Jinan, 250102, China

Abstract. In order to explore the application of remote network attack defense, a research on the application of big data analysis technology in remote network attack defense is put forward. Firstly, this paper describes that big data is a very advanced pattern recognition technology, which can find potential viruses or Trojans from massive network data resources. In this way, anti-virus defense software can be started in time to remove viruses or trojans from the network and ensure the normal operation of the network. Secondly, the basic theory of big data is described in detail, its application process in network security is analyzed, and an advanced network security defense model is constructed to improve the level of network security defense. Finally, using big data analysis technology, a new remote network attack defense software system is constructed, and global systematic attacks are added to the system to deal with them, so that various network threats can be perceived and corresponding interception treatment can be taken. After the defense function test, the response speed and interception rate of the system are ideal, and it can respond to network attacks in time, effectively ensuring network security.

Keywords-big data, remote network, attack defense

1 Introduction

The rapid development of Internet and mobile network has prompted people to enter the information society, and there are more and more Internet-based applications, such as RoyalFlush, East Money, MOOC Learning Network, China Commission for Discipline Inspection, Tmall Mall and JD.COM Mall, which have effectively promoted the office automation, intelligence and sharing of social government and enterprise units. The Internet provides convenient services for people, but at the same time it faces threats of attack, such as worms, ransomware, mutant Trojans, etc., and attacks the network by taking advantage of the loopholes generated by the integration of large-scale Internet, resulting in the paralysis of the network. With the increase of network access users, there are more software and hardware resources for Internet access. Therefore, there will be higher requirements for network security processing speed, so as to improve the processing speed of Trojan horses or viruses, reduce the infection range of network viruses, and actively respond to application software, which has important functions and significance [1].

ICBBEM 2023, May 19-21, Hangzhou, People's Republic of China

DOI 10.4108/eai.19-5-2023.2334420

2 Network security defense technology application and development status

At present, people have entered the era of "internet plus" and are facing more security threats, such as Trojan virus, DDoS attacks and data theft. Attacks on the Internet will also bring serious losses to people. For example, ransomware has attacked many large multinational companies and securities banks, which makes the office computers of these government and enterprise units all have blue screens, and users can't access the operating system for file processing. The ransomware requires these companies to pay a certain amount of ransom before they can use the system normally, which has caused many companies to lose a lot of money. Distributed Denial of Service (DDOS) is also very serious, which simulates a large number of users accessing the network server concurrently, resulting in normal users being unable to log on to the server. Therefore, in order to improve information security, people put forward security defense technologies such as firewall, antivirus software or deep packet filtering [2-3].

2.1 Design of network security defense model based on big data

Big data is a very advanced pattern recognition method, which can mine hidden and valuable data resources from massive data, and these resources can help people make effective decisions. At present, big data has been widely used in document retrieval, gene sequencing, weapons control and other fields, greatly improving the level of social intelligence. After years of research, big data has introduced more advanced technologies, such as convolutional neural network, fuzzy mathematics, support vector machine, information theory and statistics, which have improved the analysis accuracy of big data. With the arrival of the "internet plus" era, the network is facing more and more attack threats. Many viruses or Trojans adopt more advanced shelling technology and hiding technology, which can hide for a longer period and infect a wider range of networks, resulting in more serious economic losses. Therefore, using big data technology, this paper constructs an Internet data analysis model, as shown in Figure 1.

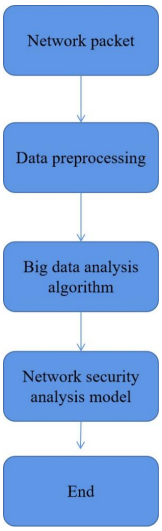

Figure 1. Data processing flow of network security defense system based on big data

3 Network security active defense system based on big data technology

The network security proactive defense system based on network security risk assessment system and network security audit system is an important factor to ensure the safe operation of the network in the era of big data. It is the main content of active defense technology to analyze the harmfulness of programs by monitoring their behaviors. According to the operating characteristics of Internet devices, the program will call a variety of application programming interfaces in the actual operation stage. It is an effective measure to analyze the harmfulness of the program by using the interface called by the program to understand the running state of the program. Active defense technology has strong ability to analyze and judge programs independently. The network security active defense system based on big data technology is not only based on the signature of the virus to analyze the nature of the virus. The original virus definition and program behavior can be regarded as the main basis for the network security active defense system to judge the virus [4].

The active defense technology of network security mainly consists of early warning technology, protection technology, detection technology and other technologies. The organic integration of the above technologies allows people to build a deep defense system at different levels of network security defense. The active defense system can also block the attack behavior in time after identifying illegal intrusion information and abnormal data, so as to restore the network system to normal operation. After the application of big data technology in the field of Internet security defense, the construction of dynamic simulation anti-virus expert system can make the system analyze the logical relationship between different actions on the basis of automatic monitoring of various program actions, and then complete the judgment of some new viruses with the help of virus identification rule information. The independent analysis function based on big data technology has the ability to automatically block the new viruses identified in the running stage of the monitoring program. The related registry automatic repair system can also help to improve the dynamic security control mechanism of the network [5].

In order to improve multiple protection systems such as network security active defense system, people can also apply dynamic simulation technology based on big data technology to multiple protection systems. According to the actual operation of the network system, dynamic simulation technology can automatically extract virus feature values after discovering new viruses, and update the local unknown feature database on this basis. The effective update of the local unknown feature library can make the same virus be effectively identified after the second appearance.

4 Development and design of remote network attack defense based on big data analysis technology

4.1 Remote network security defense system architecture

In the remote network security defense system, laas layer is mainly composed of identity authentication, data security, communication security, equipment security, etc. PaaS layer is

mainly composed of automated testing, API security gateway, coding security, etc. SaaS layer is mainly composed of vulnerability analysis and identification, application intrusion prevention and application security reinforcement. Table 1 gives the overall architecture of the remote network security defense system, which mainly involves defense policy generation nodes, sensor nodes and so on. Among them, the running state of the system is analyzed and reported by the sensor nodes, and the immune processing module is started, thus effectively intercepting network viruses or malware and protecting the security of the system. Under the big data analysis technology, the defense strategy generation node can collect the data sent by each sensor node, such as alarms and logs, match the corresponding defense rules by analyzing the data, form a specific defense strategy, and start the corresponding defense mechanism to ensure network security [6].

Table 1. Hadoop-based real-time intrusion detection system

Data lifecycle management	Passive protection	Active protection
data acquisition	Application of safety reinforcement	Threat detection
data transmission	Coding security	Safety early warning
data analysis	Equipment safety	Attack traceability

4.2 Defense Testing of Remote Network Attack Defense Software

(1) Build a long-range network attack structure

Based on the operating parameters of big data analysis technology, the control center selects Mininet+POX platform, simulates the virtual network environment through Mininet, follows the user-defined remote network interaction process, and the operating core selects the POX controller in the platform. Based on the connectivity of remote network attacks, six switches are used to connect with each other. Among them, one switch is used to connect to the remote subnet, and then one host is prepared to attack, and the network attack topology result is completed according to the remaining operating bandwidth of the switch. The built-in attack traffic generation tool Trafgen is used to form the attack traffic of the attack host [7-8]. According to the parameters of the attack traffic source P address and the source port number, the contents of the attack packets in the host file are continuously configured, and the relevant parameters for configuring the attack packets are generated by iPerf3.

(2) Interception result of attack traffic

According to the window parameters supported by three kinds of defense software, the defense software programming program is written and implanted respectively, and the programming program is run in Ryu controller. Set the attack flow value of the attacking host to 100 ~ 1000 MB to ensure the accurate test results. In this attack traffic mode, the fixed controller has 20 running windows. Based on the running window values and attack traffic parameters, the statistics of the actual intercepted traffic data of defense software are completed, and then the attack interception rate of defense software is calculated.

The formula F=(AR+TN)÷ (TA+TN+FA+AR)×100% is used to express the numerical relationship. Among them, f represents the interception rate of defense software attacks; AR

indicates the number of attack data correctly intercepted by defense software; TN indicates successful marking of attack data traffic; TA indicates the number of interception windows supported by the controller; FA means to set the attack traffic value. Statistics on interception rate of attack traffic of defense software are carried out based on different numerical grades of attack traffic, and the results are shown in Table 2 [9-10].

Table 2. Attack interception rate of three kinds of attack defense software

Host attack traffic /MB	Design defense software/%	Defense software based on OpenFlow protocol/%	Defense software based on in-band telemetry technology/%
100	95	86	76
200	95.2	58	76.3
300	96	60	80

5 Conclusion

In the field of network security defense, big data technology can connect all kinds of data information in series with its own data association function and data mining function to complete the construction of logical chain. With the rapid development of information network technology, the demand for the practicability of Internet security defense system will be continuously improved. On the basis of paying attention to user experience, improving the accuracy of big data attack detection is helpful to improve the effectiveness of network security defense system. The remote network attack defense software developed and designed in this paper based on big data analysis technology can achieve high defense efficiency and meet the practical application requirements.

References

[1] Qi, B. . (2021). Hyperspectral image database query based on big data analysis technology. E3S Web of Conferences, 275(1), 03018.

[2] Wang, X. , Li, Z. , Hong, H. , & Zhou, M. . (2021). Development and design of network security system software based on big data analysis technology. Journal of Physics: Conference Series, 1992(2), 022145-.

[3] Liu, H. X. , Zhou, S. H. , Chen, B. , Wei, C. F. , & Pan, X. . (2021). Research on the data driven practice teaching mode: take the didi data set as example. Advances in Science and Technology, 105, 3(4)8-355.

[4] Guan, X. , Zhang, L. , & Zhao, H. . (2021). Research on e-commerce supplier selection based on big data analysis technology. Journal of Physics: Conference Series, 1757(1), 012135 (8pp).

[5] Zhao, Y. , Zhang, J. , Xiang, S. , & Tang, Y. . (2021). Research on intelligent analysis technology of network security risk based on big data. Journal of Physics Conference Series, 1792(1), 012036.

[6] Zhang, Z. , & Wang, J. . (2021). Novel privacy preserving classification mining approach applied to a city public security big data analysis. Journal of Physics Conference Series, 1827(1), 012170.

[7] Chen, Q. , & Wang, W. . (2021). Analysis on the application of big data technology in medical and health industry. Journal of Physics: Conference Series, 1883(1), 012136-.
[8] Lu, R. , Liu, N. , Li, D. , Luo, X. , & Fan, Y. . (2021). Intelligent monitoring analysis of power grid monitoring information based on big data mining. Journal of Physics: Conference Series, 1992(3), 032132-.
[9] Zeng, F. , & Gao, Q. . (2021). Judgment and coping strategies of iape based on big data analysis. Journal of Physics: Conference Series, 1852(3), 032036 (6pp).
[10] Yang, F. . (2021). Influence and application of big data analysis in product design research. Journal of Physics: Conference Series, 1852(3), 032008 (6pp).