Analysis on the Quantitative Evaluation Method of Hierarchical network Security Threat Situation

Sun Zuntao, Wang Yuping, Wu Huiyun

Information Affairs Office, Shanghai Maritime University, Pudong New Area, Shanghai, China

Keywords: hierarchical network; network security; evaluation method

Abstract: Assuring safety is an important prerequisite for the smooth progress of each industry. The evaluation of safety is also one of the important measures of the management system. The reasonable use of the evaluation method can identify the security risks of the system in time, so as to effectively prevent it. Starting from a hierarchical network, research and analysis of security assessment methods for hierarchical networks.

1. Introduction

What is the hierarchical network security assessment method, with the importance of network services and the importance of the board host as the main starting point to make an intuitive analysis based on the network threat situation. The use of security assessment methods can not only reduce the workload of hierarchical network staff to a certain extent, but also provide a straightforward and effective basis for staff to revise security countermeasures. In summary, network staff should strengthen the layering. Analysis and research of network security assessment methods to improve work efficiency.

2. Hierarchical network security threat situation existing research

The network security situation is the operating state of the various configurations that make up the network. It is also the hierarchical network state and the possible change situation. Under the situation that the user's behavior of using the network changes, the network situation will also change, the network situation In terms of popular language, it is the changing trend of network security status. How to conduct security assessment of network situation requires the use of a large-area monitoring network system to collect network security information. Since the introduction of computer network system, the security problems in the network have only increased. Without any reduction, the use of the network's group distribution is widely understood. The existence of network security issues not only threatens the information security of network users, but also threatens the national network information security to a certain extent, and quantitatively evaluates the security threats of hierarchical networks. It can strengthen the management of hierarchical network security in the current year. Nowadays, China's guidance label for network security assessment is relatively simple, and the method of obtaining network security information is also one-sided. It can't complete the effective evaluation of network security. On the other hand, in the layered network space. In the construction of the ideological framework, a circular network system has not yet been constructed. Therefore, it is difficult to achieve effective evaluation for the security assessment of cyberspace. Most of the current methods for network security assessment are SSAER. SSAER can effectively detect the attack form and state of the computer network, and then use the intrusion detection system (IDS) for sampling and analysis. Strengthen the understanding of the state of the computer, and establish an evaluation system of the network security situation according to the state of the computer, so as to evaluate from the network status, host status, system service and other aspects of the computer.

  DOI: 10.25236/aisct.2019.031

3. Method for assessing network threats and quantifying security postures

3.1 Construction evaluation system prototype

Before evaluating the network threat and security situation, we must first establish an evaluation system. As shown in Figure 1, the network system is divided into three aspects: network state, host state, and system service according to the network structure and system scale. More network threats are system services provided by computers. Therefore, it is possible to start from the subtlety, start by evaluating the local system, and then gradually evaluate the whole computer. In this way, build the prototype of the evaluation system and pass the intrusion detection system. (IDS) early warning and data obtained from system vulnerability scanning are admissible information, and then assess the degree of risk of intrusion in the system service level of the computer, and perform quantitative analysis of the system according to the degree of danger [1].

On the other hand, DoS-type intrusion poses a threat in the computer's main control system. Such an intrusion attack poses a serious threat to network information and system services. In this case, when constructing the prototype of the evaluation system, it needs to be considered. The intrusion path of the computer main control system and the impact on the system service are analyzed in depth, and the analysis and evaluation of the computer state form and the network level state index are carried out. Throughout the evaluation process, the service level of the main control system must be analyzed and studied in depth, and the threat level and the data occupied by the computer network and the probability of secondary intrusion are analyzed in depth. Comprehensive assessment of computer indicators [2].

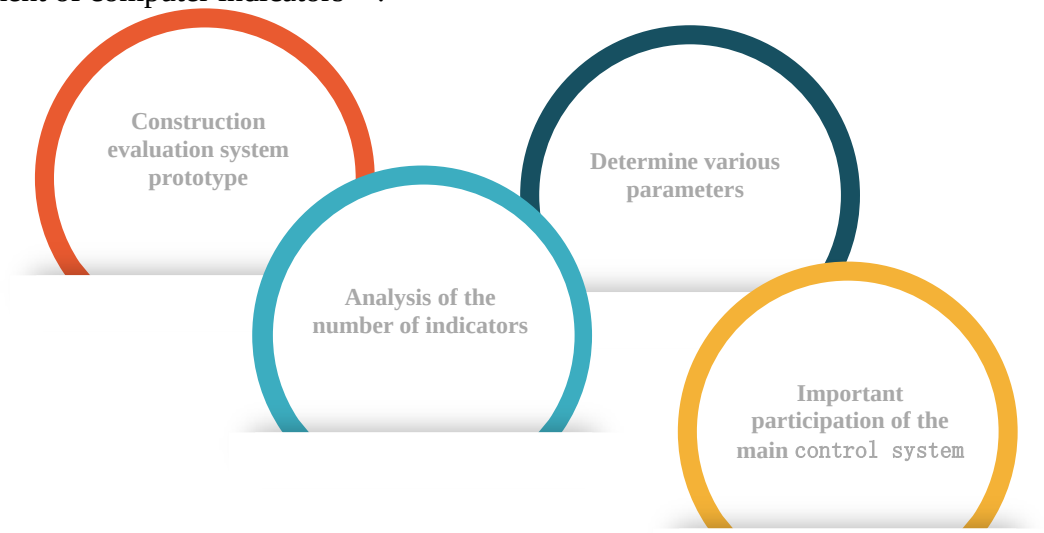

Figure 1 Evaluation method

3.2 Analyze the number of indicators

For computer networks, the danger caused by system services is a major aspect of network security problems. For system services, the degree of intrusion, the consequences of intrusion, and the access volume of system services will threaten the security of computer networks to a certain extent. According to the size of the intrusion and the number of accesses to the system service, the final evaluation will cause errors. Therefore, when evaluating and calculating the security of the network system, the number of indicators should be analyzed first. First, analyze the intrusion. Time, and specific to a certain period of time, system services may be subject to the possibility of intrusion, in the calculation of time work, according to different time periods, one by one, you can divide the time of day 0:00-9:00, then 9:00-12:00 in the noon, then 12:00-18:00, and 18:00-24:00, for different time periods The number of visits calculates the average number of visits for four periods of the day, and then calculates the average based on the normal number of visits. The

amount of visits is calculated by means of assignment, that is, the levels of access to different levels, such as extra low, low, high, high, and extra high, are sequentially represented by numbers 1 to 5, and the adopted data are processed one by one, and then The vector value of the normal number of visits can be obtained, and then under the condition that the vector value of the normal access quantity is obtained, the in-depth investigation and analysis are performed according to the different degrees of the intrusion, thereby obtaining the risk index, determining whether it is effective, and ensuring that the evaluation result is reasonable. And accurate, the relevant research shows that the degree of threat can be divided into first-level and second-level. When the first-level and second-level attacks occur once and ten times respectively, the risk indicators obtained are consistent. When calculating the risk indicator, the intrusion threat index should be strengthened to avoid the difference between the intrusion risk indicator and the normal indicator due to sudden or extremely special conditions [3].

3.3 Determine parameters

When conducting network threat and security situation assessment, we must first establish an evaluation system, and divide the network system into three aspects: network status, host status, and system service according to the network structure and system scale, and conduct network system security evaluation and When calculating, we must first determine and analyze the number of indicators and the parameters of various aspects. When determining the intrusion index of different levels of the computer, the first thing to determine is the importance of the level and the possession of the network broadband data, and determine the intrusion index. Try to exclude intrusion attacks that do not pose threats in the early warning mechanism, so that the network security assessment is more accurate. On the other hand, determining the intrusion attacks that do not pose a threat can greatly reduce the possibility of successful intrusion. The network data possession is determined. Since the effective attack requires the computer to stop running by exhausting the network data usage, determining the network broadband data occupancy situation can provide a scientific basis for the risk analysis of the intrusion times, through the computer state form and the network level. shape Analysis and Evaluation Index. Throughout the evaluation process, the service level of the main control system must be analyzed and studied in depth, and the parameters of various aspects, the degree of threat to the invasion, the data occupied by the computer network, and the probability of secondary intrusion are determined. Conduct an in-depth analysis to complete a comprehensive assessment of computer indicators [4].

3.4 The importance of the main control system

The importance of the computer's main control system is reflected in the different nature of the service terminal. The data of the service terminal is evaluated by different data, such as dynamic data, human causes, different variables, etc. There is no accurate data for the evaluation criteria of the main control system. The data displayed by different levels of the main control system is different. In the regional network, the main control system is very important.

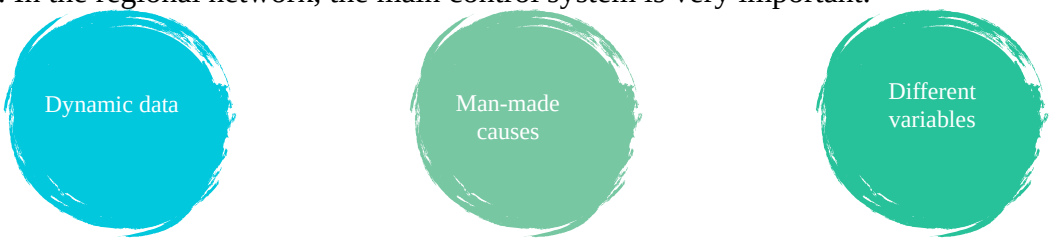

Figure 2 Influencing factors of the main control system

4. Experiments and analysis for network security assessment

Set up an experimental environment, such as the CNSLS local area network, sharing a C-bit address in the area network to use the network together, assuming that the protected server system is configured as Red hot Liunx 6.2 and 7.2, and different servers are mail, fpt, and Samba. The

information generated by each intrusion detection system is stored in the information base as the original data of the network security assessment, and the system service importance degree and weight vector of different main control systems are determined through the importance degree identification measures of the system service. Arrange the relevant personnel to simulate the hacker, and carry out the intrusion of the protected server mail, fpt, samba within the specified time and the computer main control system. The attacks include effective and invalid. In the 24-hour test time, the SSAER is used for detection. The attack form and state of the computer network are then sampled and analyzed using an intrusion detection system (IDS). Strengthen the understanding of the state of the computer, and establish an evaluation system of the network security situation according to the state of the computer, so as to evaluate from the network status, host status, system service and other aspects of the computer. Analyze the IDS early warning mechanism and the use of resources to obtain dangerous situations at different time periods. In-depth investigation and analysis according to the degree of invasion, to obtain the risk indicators, and determine whether it is effective, to ensure that the assessment results are reasonable and accurate.

Through the above experiments, it is necessary to establish a prototype of a hierarchical network security assessment system. The dangerous situation at each time period is inextricably linked with the degree of intrusion and network status, and is integral. When determining the intrusion index of different levels of the computer, the first is to determine the hierarchical importance and the network broadband data possession, determine the intrusion index, and try to exclude the intrusion attacks that do not pose threats in the early warning mechanism, so that the network security assessment More accurate, on the other hand, determining an intrusion attack attempt that does not pose a threat can greatly reduce the possibility of successful intrusion and determine the network data possession, since effective attacks need to be exhausted by network data usage. The computer stops running. Therefore, determining the network broadband data occupancy situation can provide a scientific basis for the risk analysis of the number of intrusions, evaluate the intrusion vulnerability data and the less harmful intrusive attacks to reduce the level of processing, and improve the network security situation. Guiding value.

5. Conclusion

This paper studies and analyzes the security assessment methods for hierarchical networks by starting from a hierarchical network. Reasonable use of assessment methods can identify the system's security risks in a timely manner, so as to effectively prevent and make intuitive analysis based on the network threat situation. The use of security assessment methods can not only reduce the workload of hierarchical network staff to a certain extent, but also provide a straightforward and effective basis for staff to revise security countermeasures.

Acknowledgement

2019 Shanghai Maritime University Teaching Reform and Management Reform Project “Educational Informatization 2.0 Action Plan Implementation Path Study”(20190509)

References

[1] Chen Yahui. Research and analysis of hierarchical internal threat situation quantitative evaluation model [D]. Changsha: National University of Defense Technology. 2018.

[2] Zhang Yong. Research and System Implementation of Network Security Situational Awareness Model [D]. Hefei: University of Science and Technology of China, 2017.

[3] Cheng Wencong. Research on Key Technologies of Time Series Data Mining for Large-scale Network Security Situation Analysis D] Changsha: National University of Defense Technology. 2017.

[4] Xiao Haidong. Network security Situation assessment and trend perception analysis [D] Shanghai: Shanghai Jiaotong University, 2017.