Design and Implementation of Computer Network Vulnerability Assessment System

Tianli Li
{ litianli@126.com}

City Institute, Dalian University of Technology Dalian 116024, China

Abstract. In the field of computer security, especially in the field of network security, it is very important to assess the vulnerability of computer system. Connection on the network computer system in the presence of vulnerabilities may let elsewhere on the network malicious attackers invade inside the computer system, which led to the damage of the computer system of data integrity, availability and confidentiality. The ultimate goal of network vulnerability assessment is to guide the system administrator to find a balance between "security costs" and "intrusion possibilities". The vulnerability assessment method has experienced from the manual assessment to the automatic evaluation stage, and is now being evaluated by the local assessment to the overall development, from the rule based assessment method to the model based assessment method development. However, it can be applied to the product in the process of the evaluation method based on the rules. This kind of product is commonly called the vulnerability scanning product or the security hidden trouble scanning product. The system uses the client / server structure. Server is running on the Linux platform, achieve the goal of preserving scanning plug-in, save the default configuration parameters, loading scanning plug-in on the target system of security scanning, to client sends scan status and results, recording operation log function. The direct operation of the server is carried out by means of a special Shell which is limited to the minimum function. Run the client on the windows platform and is responsible for the management, control server to perform vulnerability scanning tasks, scanning to achieve the task management, scanning strategy management, state / news shows, scanning result report generation and output, user classification and management functions.

Keywords: Network security; vulnerability assessment; vulnerability scanning; crystal reports; XML

1 Introduction

Management security is the strategy and process of organization's security. For example, if the physical security concerns about whether the room is locked, then the security of the management of the key is placed in the hands of who. Management security not only includes the release of security policies, but also includes the implementation and monitoring of these policies. The purpose of data security is to ensure the authenticity of the data value when the data is transmitted by the system or by the system to change the data. There are usually a number of different techniques for ensuring data security, including hardware and software,

but the data security does not care about the implementation details of the technology, it is only concerned about whether the data itself is safe. Technical security to deal with specific details of security attacks against security attacks. This is what most people understand the concept of security, that is, the ability to attack resistance". Technical security is responsible for regularly, in advance to the user to publish and maintain information, to prevent possible attacks [1]. At the same time, once the threat has penetrated into the system, the technical security response team will analyze the source of the threat, to determine the threat of damage, improve defense and repair strategies. The "computer security" and "network security", which are concerned by this article, belong to the category of "technical security". If it is not specified, physical security, management security, and data security are not considered. The content of safety assessment for the organization is multifaceted. The emphasis on security of network can include the organization, the organization's physical security measure, organization existing strategy and process, the organization has preventive measures, staff, staff's work load, the attitude of staff, staff of the existing strategy process implementation. Computer vulnerability assessment is one of the important contents of the evaluation phase. Similar to the process of information security, computer vulnerability assessment is a cyclical process. It shows that the whole computer vulnerability assessment process includes 5 stages: analysis requirement, development plan, implementation evaluation, recovery and reinforcement, verification and validation, and the report and document produced at each stage.

2 System Design and Analysis

According to statistics, at present in the domestic development of firewall company has more than 200, the development of intrusion detection products company has more than 30, exploitation of the fragile assessment product of more than 20 companies, domestic vulnerability assessment products market is in its infancy. At the same time, because by increasing the level of the domestic products of the same category, and users in the domestic industry to the creation of a key information application system performance in foreign enterprises to provide the "black box" technology on the basis of the more and more doubts, domestic products market share continues to increase. In addition, CCID Consulting released the 2002 key industries of network security application report "pointed out that with the advance of the implementation of government informationization and e-commerce, security technology such as intrusion detection and network security assessment will be more used to the user's network security as a whole solution, product market is constantly on the rise, especially with the increasing of the demand of security products in finance, telecommunications, government and other key industries, market will have greater growth. 2002 in the first half of China's network security software products market, intrusion detection and security assessment has accounted for 10.5% of the share, far higher than the 2.3% in 2001. And the network security have higher requirements for the banking and government survey found that: with network security products, banking institutions [2], equipped with firewall to 76.8%, equipped with intrusion detection and vulnerability assessment has reached 53.3%. Among the government departments with network security products, the proportion of firewall is 39.1%, and the ratio of intrusion detection and vulnerability assessment is 30.2%.

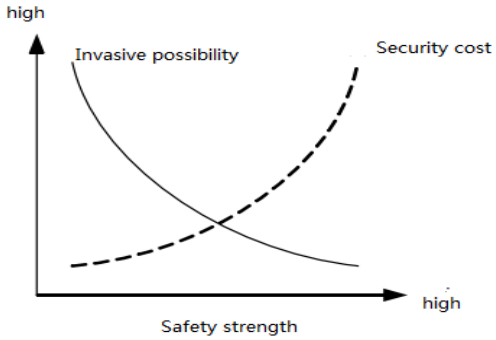

Fig. 1. The relationship between safety strength and security cost and the possibility of invasion

2.1 Basic Principle of Network Security Scan

Computer vulnerability assessment method can be divided into "rules" and "based on model two kinds. However, regardless of the method of vulnerability assessment must be evaluated object local vulnerability information based on. Network based vulnerability assessment system is the basic way to get these local information. This chapter details the basic principles of network security scanning. A full network scan is mainly divided into three stages: 1) to find the target host or network. 2) find the target information, including the operating system type, the operation of the service and the service software version, etc.. If the target is a network, it can also be found that the network topology, routing equipment and the host of information. 3) according to the information collected to determine the existence of the system or further detection of security vulnerabilities. The scanning techniques and methods used in these three phases will be described below. ICMP can be used for shooting a lot of instrument. In the UNIX environment, there are mainly Ping and fping. Traditional Ping in the execution when the fire is slow because it in before the detection of a potential host to wait for the current detection system gives response or timeout. While fping in bursts of multiple IP addresses, significantly faster than the speed of ping. There is a tool called gping is used with the fping, it is fping to generate bursts of IP address list. In the Windows environment, you can use the Pinger from the Rhino9. In addition, the nmap -s P option also provides the ability to ICMP [3].

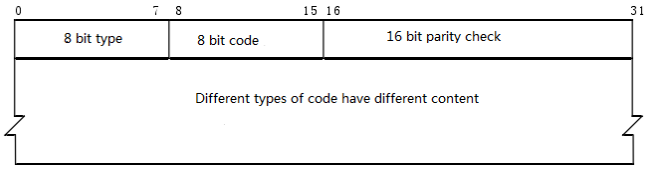

Fig. 2. ICMP message format

2.2 TCP Technology

Establish a connection to the TCP process and the SYN and ACK sections of the section. The whole process of "three handshake". The client first sends a serial number for the SEQ1

SYN section to the server. The server receives the segmented, if the corresponding port is listening response with a serial number for seq2 syn/ack sub section of, the segmented confirmation number for SEQ1+1; if the corresponding port is not listening, the response to a RST segment, refused to establish a connection. Client if you accept to correct the syn/ack segment, then sends an ACK segment to the server, the segmented confirmation number for SEQ2+1. At this point, the connection set up successfully. The most basic method used in port scanning is connect TCP () scan. It makes use of the connect () system calls provided by the operating system to connect to the ports of each of the target computers that are of interest. If the destination port is listening, connect () will be successful. Otherwise, the port is not available, that is, there is no service provided. This method has the following advantages: does not require any special permission, any user in the system has the right to use this call can be open at the same time a number of sockets, thus speeding up the scanning, using non blocking I / O also allows setting a low time to exhaustion cycle, while observing a number of sockets. This method has obvious shortcomings for the intruder: easy to filter or record. For security administrators, the only drawback to using this method is that it is slow [4].

3 System Design and Implementation

This system is a based on the computer network security scanning system, its purpose is to help the system administrator on the computer system safety assessment, find out the system may be exploited loopholes in the system, providing related vulnerability information and suggestions to solve the problem. Administrators with a network security scanning system to provide the report, you can minimize the risk of networked computer systems. This system can not repair the vulnerability of the system, it can only provide information and advice to the system administrator. The system is an independent system, but it is closely related to the intrusion detection system. Intrusion detection system is used in the network to listen to the passive network communication means, to detect the occurrence of network attacks or the purpose of the attack, so as to inform the administrator of the corresponding attacks to prevent. Network security scanning system is prior to the actual hacker attacks, by hacking simulation of network attack, looking for loopholes in the system and to inform the administrator to nip in the bud. Intrusion detection system can detect network security scanning system of simulation attack, so network security scanning system can also be used for testing intrusion detection system false alarm rate and false negative rate performance. Network security scanning system and intrusion detection system can share the vulnerability description information. The system user group is mainly for experienced system administrator. Users are not required to be familiar with all kinds of specific network attack methods, but require the user to understand the basic configuration of the computer system they are using. The system will also give and patch vulnerabilities related solutions and other information. The whole system adopts C / S (client / server) structure, the function of the whole system is to scan the target system on the network, and generate the relevant safety assessment report. Provide configuration and maintenance references to the administrator of the target system. GUI is the user's direct use of the interface, it's design should first meet the basic needs of the system function, that is able to allow users to complete all the basic functions of the system through the GUI. However, there is a very important point is that the design of the user interface must reflect the "people-oriented" principle. User interface design is divided into three parts: structure design, interaction design and visual design [5].

Structural design, also known as conceptual design, is the framework of the interface design. This part of the design is through the user research and task analysis, to develop the overall structure of the product. In the structure design, the logical classification of the catalog system and the definition of words are the important preconditions for the users to understand and operate easily. The purpose of interaction design is to make the product allows users to simply use. The realization of the function of any product is accomplished through the interaction between human and machine. The client program uses the document view (Document-View) structure, single document form. The whole framework is divided into three views. Tree view on the left to complete the management of the list of scanning tasks. The tree view on the right completes the management of the list of scanning strategies. At the bottom of the text view to complete the function of the message display at run time. The address of the three views is stored in three global pointer variables.

4 Conclusion

The main work of this paper is to design and implement a network vulnerability assessment system based on rules. This paper clearly illustrates the architecture design of the whole system and the design ideas of some details, which can be of some reference value for the future of such projects. At the same time, this paper also can be used as a reference for the maintenance and development of the project. Scan report detailed appearance. Detection report both a variety of detailed statistical data, there are detailed information on the vulnerability of a single target host. At the same time to provide a solution to fix the vulnerability of the reference program. Users can also be required to display the contents of the report customized.

References

[1] Liu Xuejiao, Ma Nian, Xiao Debao, Zhao Ning. Network vulnerability assessment based on risk theory. Journal of Wuhan University of Technology. No. 18. (2013)

[2] Deng Yaping, Wu Huilian, Chen Lin, Wang Bin. Design and implementation of network vulnerability assessment system. computer application research. No. 01. (2015)

[3]. Xing Xujia, Lin Chuang, Jiang Yixin. Study on vulnerability assessment of computer system. Journal of computer science. No. 01. (2014)

[4] Wang Peng. An information system network vulnerability assessment method. network security technology and application. No. 02. (2015)

[5] Zhou Haifeng. An analysis of the security vulnerability assessment of computer systems. science and technology information. No. 11. (2012)