Research on the Essential Network Equipment Risk Assessment Methodology based on Vulnerability Scanning Technology

Xiaoqin Song[1]

[1] Sias International University,
Xinzheng,Henan, 451150,China

Abstract. In this paper, we conduct research on the essential network equipment risk assessment method based on vulnerability scanning technology. A growing number of hackers wanton invasion of the computer, through the network to steal important information, or destroy the network, the paralyzed which caused huge losses to the state and society. Find a known vulnerability rather than to find the unknown vulnerabilities much easier, which means that most of the attacker's use is common vulnerabilities. Therefore, we adopt the advantages of the technique to finalize the methodology for the essential network equipment risk assessment which will be meaningful.

Keywords: Risk Assessment; Vulnerability Scanning; Network Security; Essential Equipment.

Introduction

With the constant improvement of China's socialist market economic environment, the Internet has become the wings of the social development to take off. More and more units will be their key business on Internet, and got excellent grades. However, with the development of the network, the security of network is more and more important. A growing number of hackers wanton invasion of the computer, through the network to steal important information, or destroy the network, the paralyzed, caused huge losses to the state and society. Facts have shown that with the increasing popularity of the Internet, also more and more in criminal activities on the Internet, especially the Internet a wide range of open and finance network, making more and more systems are being threatened by the invasion of attack. But, no matter one offender from outside or from within a network attack, attack by mining the operating system and application service program weakness or defect. Security scanning involves testing technology could be generally separated into the following parts. (1) Based on the target of leak detection technology. It uses a passive, non-destructive way to check the system properties and file attributes, such as database, registration number, etc. Through the message digest algorithms, the test number of encrypted files. Implementation of this technology is running on a closed loop and constantly handles file, system target, system target attribute, and then check number, the check number compared with the original check number. The administrator will be informed once found changed. (2) Detection technology based on host. It uses a passive, non-destructive testing method for the system. Generally, it involves the system kernel, file attributes, patches of the operating system and other issues. (3) Based on the application of testing technology. It uses the passive and non- destructive inspection application software settings to find security vulnerabilities. (4) Based on the testing technology of the network. It uses positive and non-destructive method to verify system collapse if it is possible to be attacked. It uses a series of scripts and simulates the behavior of the attacks on the system, then analyze the results. It also tests against the known network vulnerability. Network detection technology is often used to

carry out through experiment and security audit [1].

Due to the development of the network technology is in high speed process, so a lot of network protocols and application design is not very perfect, there are some security vulnerabilities. Outlaw these holes can be used to attack other people's network, destroy the normal operation of the network or illegal invasion of other people's computer access to private information and so on. So regularly evaluate the security holes in the network have become an indispensable day-to-day work of the general network administrator of. Generally speaking, the popular vulnerability could be summarized as the follows. (1) CGI hole. CGI is to run on a Web server to provide client HTML page interface. Due to the negligence of the CGI program developers, many CGI programs exists all kinds of dangerous degree of vulnerability. For example some CGI program allows remote attackers on a web server to perform any command, possible damage to the server. Some CGI program itself, or the function called by their lack of user input data to the legitimacy of the inspection, failed to filter out some special characters, offender makes people can reach the purpose of invasion by constructing a request. (2) SQL injection vulnerabilities. For SQL injection attacks, Microsoft technology center is described from two aspects: the script injection attacks. The malicious user input lead to be executed SQL script. By their nature, use the SQL syntax, is for the loopholes in the process of programming application developers. (3) Weak password loopholes. Weak passwords vulnerability refers to the network users don't realize the importance of network security situation, in order to facilitate the memory for network applications such as FTP and POP3 set consist only simple passwords.

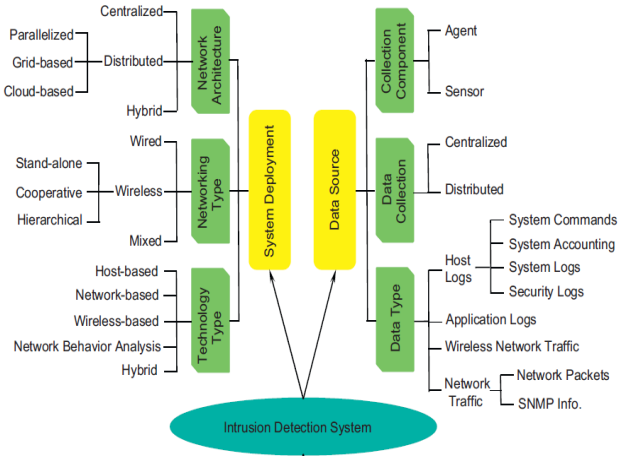

Figure 1.The General Composition of the Intrusion Detection System

In this paper, we conduct research on the essential network equipment risk assessment method based on vulnerability scanning technology. In the figure one, we illustrate the general composition of the intrusion detection system. Security scanning technology is a kind of important network security technology. Security scanning technology, can be used for local area network, web site, the host operating system, service system and firewall system security vulnerability scanning, can understand unsafe network security configuration and operation of application services, timely find security vulnerabilities and system errors in the configuration and do it in advance [2]. In the following sections, we will discuss the corresponding issues in detail.

Our Proposed Risk Assessment Methodology

The Concept of Network Security. With the popularization and application of computer network and distributed computer, network security becomes more and more important. At present, in addition to the computer itself security mechanism, computer network security is mainly a firewall, but with the development of hacking technology, system vulnerabilities are increasingly exposed, firewall weaknesses make its attacks on a lot of helpless, especially that from internal attack and is what to do. Each

system has loopholes, no matter how much you people in the system security resources, the attacker can still find some available features and configuration of defects but most of the attacker, usually to do simple things. Find a known vulnerability, than to find the unknown vulnerabilities much easier, which means that most of the attacker's use is common vulnerabilities. The use of appropriate tools, can before hackers make use of these common vulnerabilities, detect network weaknesses, now popular vulnerability scanner can detect the above two kinds of holes.

Vulnerability scanner is able to automatically detect remote or local host security vulnerabilities, network administrators can learn about the application of network security configuration and operation service, timely detection of web server maintenance by various TCP port, provides the service, the distribution of the Web service software version and these services and software is presented in the Internet security vulnerabilities, objective assessment of network risk level. According to the principle of the vulnerability scanning technology, we can see that in general, a complete network security vulnerability scanning can be divided into three stages: the first stage, found the target host or network. After the second stage, found the target host further collection including operating system class, the operation service and target information such as service software version if the target is a network, can be further found that the network routing equipment, topology structure and the information of each host. The third stage, according to the information collected with holes and comparison between the library and related standards to judge or whether there are any further test system security vulnerabilities. Computer network users and administrators, using vulnerability scanning technology, you can check out the host system has been installed the eavesdropping program [3]. Check out of the running of network system in the presence of unsafe network services, check whether there is in the operating system can lead to a buffer overflow attack or denial of service attack security vulnerabilities and check out whether there is a firewall system configuration errors or security vulnerabilities.

The Vulnerability Scanning Technology. Vulnerability scanning system is used to automatically detect remote or local application of host security vulnerabilities. Vulnerability scanning is mainly through the following two kinds of methods to detect the target host whether there is a loophole: after the port scan that target host open port and port network services, network vulnerability scanning system of the related information and vulnerability database matching, see if any loopholes exist, and satisfying the matched condition through the simulation of the hacker attack technique, to attack the target host system security vulnerability scanning, such as testing a weak password. Once simulation attack, suggests that the target host system security vulnerabilities, two methods of the realization of vulnerability scanning listed below. However, there are some challenges needs to be solved. Because the operating system fingerprinting fingerprint is concluded through the experiment, the results may have deviation; Service temporarily not on the identification of have the ability to identify any port any service; Some protection system has already have the ability to identify some security scanning tools, scanning probe packets may be filtered, thus, the intelligent level of network security scan system research still remains to be further improved, through the study of scanning strategy, smart intelligent scanning technology to optimize the scanning process, improve the efficiency of the scanning, concealment, and the accuracy of scanning. In the process of safety evaluation, the function of a single security products and performance has its limits, need comprehensive several scanning tools is analyzed, and some security scanning tools do not leak data sharing and standardization, not well share the scan results, interoperability

between the systems is bad. The port scanning, vulnerability detection, risk assessment, safety recommendations, such as integrated together, and with the invasion of monitoring system, such as firewall security tools to realize data sharing, interactive interoperability is an important direction of the development of the security scanning technology. In the figure two, we show the technique adopted by our system.

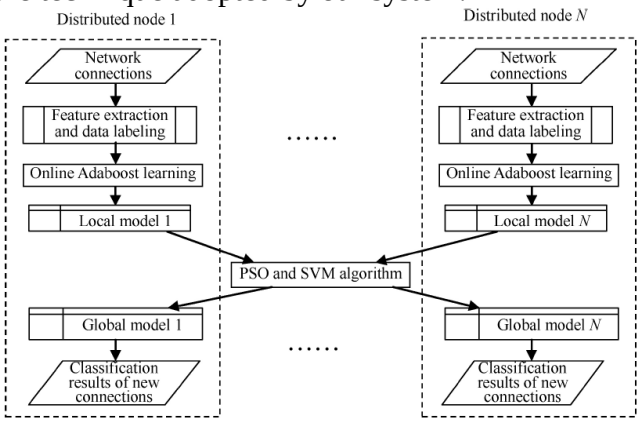

Figure 2.The Vulnerability Scanning Technology by Our Methodology

Based on a key part of the network vulnerability database system vulnerability scanning is that it uses a loophole in the feature database. Feature matching technology based on rules through the use of model, namely, according to security experts on network system security vulnerabilities, hacking case analysis and system administrators to practical experience of network system security configuration, can form a set of standard network system vulnerability database, and then on this basis the corresponding matching rules, by scanning program automatically vulnerability scanning. Plug-ins is written by scripting language subroutine, the scanner can be performed by calling its vulnerability scanning, to detect the existence of one or more loopholes in the system. Add new plug-ins can make vulnerability scanning software to add new features, scan out more holes. Vulnerability database establishment is not only to the safety network services for each set up corresponding vulnerability database file, and should be able to meet the performance requirements for previously proposed.

The Essential Network Equipment Risk Assessment. Host-based vulnerability scanning, is through the log in as root target hosts on the network, record all main parameters of the system configuration, vulnerability analysis configuration. In this way, can collect a lot of the target host configuration information. Under the condition of the target host configuration information, will be compared with standard library security configuration and matching, that do not meet is regarded as hole. Is usually installed on the target system an agent or a service, so that you can access all the files and process, it also makes the host-based vulnerability scanner to scan more loopholes. Host-based vulnerability scanner working principle is: the vulnerability scanner console installed in a computer; Installed in the enterprise network vulnerability scanner manager. All of the target system needs to be installed vulnerability scanner agent. When vulnerability scanner agent received vulnerability scanner scan code from the manager, the vulnerability scanner agent alone this target system vulnerability scanning task and after the scanning, vulnerability scanner agent will result to the vulnerability scanner manager. End users can through the vulnerability scanner console scan report. Firewall technology is passive defense, invasion detection is a passive monitoring, the host vulnerability scanning technology is own initiative on safety testing. Therefore, from the general angle of three-dimensional depth active security vulnerabilities detection gets people's attention.

Conclusion

In this paper, we conduct research on the essential network equipment risk assessment method based on vulnerability scanning technology. Network intrusion if some hacker or an intruder using scanning tools to scan to invasion of the goal, and then find weakness or

flaw in the target system, and then for illegal invasion and destruction of this system. Produce is the vulnerability of the programmer to write programs, written in incorrect or unsafe habits or programming method. Programmer at the beginning of the realization of software functions, devotion to the software meets the function requirements, no comprehensive safety into consideration. Late software in use process, because the user's incorrect operation and improper configuration, even illegal operation, could lead to a hole. Our proposed approach combines the vulnerability scanning technology with the essential network equipment risk assessment applications. In the near future, we will conduct more corresponding experimental and numerical simulation to test the robustness and feasibility of the methodology.

References

[1] Du Q, Kishi K, Aiura N, et al. Transportation Network Vulnerability: Vulnerability Scanning Methodology Applied to Multiple Logistics Transport Networks[J]. Transportation Research Record Journal of the Transportation Research Board, 2014.

[2] El-Rashidy, R. A., & Grant-Muller, S. M. (2014). An assessment method for highway network vulnerability. Journal of Transport Geography, 34(2), 34–43.

[3] Chiu C H, Wen T H, Chien L C, et al. A Probabilistic Spatial Dengue Fever Risk Assessment by a Threshold-Based-Quantile Regression Method[J]. Plos One, 2014, 9.