ATLANTIS PRESS
Advances in Computer Science Research (ACSR), volume 76
7th International Conference on Education, Management, Information and Mechanical Engineering (EMIM 2017)

Research on Intrusion Detection System Based on Host Information Recognition

Xin Sui

College of Humanities & Sciences of Northeast Normal University, Chang Chun, 130117, China

Keywords: Network; Security; Firewall; Policy; Intrusion detection

Abstract. With the rapid development of the network, the network has been everywhere. The problem of network security becomes more and more important. A simple firewall cannot resist some attacks effectively, and it is vulnerable to attack. Intrusion detection technology uses active security policy and protection scheme to enhance network security. Using host feature recognition can provide data preparation for network security research. We hope to expand the function of security tools, especially the intrusion detection system to make it more efficient.

Introduction

With the rapid development of information technology and network, computer network communication has been applied to various fields of production and life .Computer and network security issues become more complex, and network security becomes particularly important. The size and application of the Internet in the last ten years has undergone tremendous changes in security, mobility, control and manageability. [1] Due to various defects existing in the protocol, management, service and implementation aspects of the Internet, and the defects existing in the design of the software system itself, so that the hackers can take advantage of these loopholes in the implementation of intrusion attacks on network. [2]

Existing security mechanisms have limitations. For example, the firewall can prevent illegal access to many systems, but cannot resist some attacks, especially in the presence of configuration errors that the firewall system is not defined or not clearly defined security policy system. The security of the entire system will be threatened. [3] Therefore, network security cannot rely only on the basis of a single security defense system, we need formulate the specific security policy, security mechanism, security defense which will be set up by the integration of multiple channels of various reliable (e.g., firewall, access control and authentication mechanism, security monitoring tools, vulnerability scanning tools, intrusion detection system). Only establish a multi-layer a comprehensive security defense system, in order to effectively resist from the system of internal and external attacks, to ensure network security. [4]

Intrusion detection is a kind of security mechanism to monitor, prevent and resist intrusion. [5] With the introduction of intrusion detection technology, the security of network and system has been further improved. [6]

Intrusion Detection Methods

Intrusion Detection. Intrusion detection system (IDS) is a kind of network security technology used to detect any damage or attempt to damage the confidentiality, integrity and availability of the system. [7] It protected by monitoring the state of the system and to identify activities for the computer system and network system, including the detection of malicious attacks or illegal intruders outside temptation, and illegal activities beyond the internal legal user. [8] As an effective complement to firewall, intrusion detection technique can help the system cope with the known and unknown network attacks, the expansion of the safe management of system administrator (including security audit, monitoring, attack recognition and response), to improve information security infrastructure integrity. [9-10]

Host Feature Information. The Host Characteristic Information used to describe various features of the target host information which is the host of the identity. Specifically include hardware configuration, operating system, software services, etc.. The host feature recognition

mainly provides important data needed for intrusion detection. It is the foundation to find all kinds of security risks and vulnerabilities, with a comprehensive assessment of its ability to host the security situation, and "an antidote against the disease".

Passive Identification of Host Feature Information. Feature recognition technology is based on host passive network monitoring, host computer and network communication equipment data obtained by sniffer, communication of information on the remote host and then get the characteristic information of the target host. The so-called "passive" refers to the host is not the initiative to send data packets, but through a long time to capture information and analysis. Therefore, the identification is a long-term, dynamic process. The main advantage of passive identification technology is that it has little influence on the performance of the network and can be updated dynamically with the network.

Flag information Banner refers to the server through the network to send a request to the client feedback application type, so master the name and version of the iconic information. In addition, due to the requirements software corresponding to certain services of operating system or the Banner itself will include the software where the operating system type and version information. So you can also get some information of the operating system. In the case of default, the user and server specific ports can send out the connection request to get the corresponding Banner information from the remote host. Through the analysis of these information, we can achieve the purpose of identifying the target host feature information.

In the article, Fyodor first proposed the use of target host Fingerprint identification host features.

Each person's fingerprints are different, biological scanning and image processing technology, the human fingerprint collection, analysis and comparison can accurately identify personal identity. Network fingerprints include solid fingerprint (hardware, software and services) and abstract fingerprints (various operations). The host fingerprint includes 4 categories Hardware (MAC address, clock, etc.) and software (operating system, browser type version), service (host name, port service system, etc.) and the users (online behavior, habits and flow etc.). Through passive sniffing, to capture network data to the target host, protocol analysis, features of packet sequence determination, extracting the corresponding fingerprint information, according to the results of matching decision is tracking or update the host identification.

Combine Flag and Fingerprint Information to Identify the Target Host. The combination of Banner and Fingerprint in the improved method, NIDS (Network-based Intrusion Detection System, based on the network intrusion detection system) prototype system, as a subsystem, the host passive recognition feature information.

Quick and accurate identification of host information depends on the fingerprint information is reliable. The HCI discovery system first builds the fingerprint database, used to host feature information mapping storage specific fingerprint information and the corresponding update and maintain. At the same time, the host feature information database (HCIDB) is established, which is used to store the host feature information found in the whole network.

Capture in the network using packet capture module, and may contain the feature information sent to the host packet analysis module, respectively, analysis of Banner and Fingerprint, after analyzing the identification of the host feature information into the host feature information database. The HCI maintenance system mainly carries on the maintenance to the discovered host characteristic information, in order to ensure the information is accurate, effective.

Evaluations

The host "IDS" with the improved intrusion detection system is placed in the network to detect the local area network. There are a number of internal LAN server (here mainly for example HTTP server) which fixed IP address, with a specific operating system and application software. The server in the LAN can work normal. There are a number of results for PC testing.

The purpose of the test is to verify the improved theory of intrusion detection system with data, but due to the improved intrusion detection system needs to be improved. So the overall performance is not good grasp, here for several specific aspects of the targeted test.

Through the host feature information is the identification of the system for a period of time to run, to detect all the host activities within the LAN and view the effect of passive identification. That is found in the efficiency and correctness. Test time span of 48 hours, the following table is the result of some tests.

Table 1 Passive discovery data testing

Host Name	Server1	Server2	PC1	PC2
IP Address	192.168.10.1	192.168.10.2	192.168.1.4	192.168.1.5
Actual OS	Unix	Red hat Linux	Win 7	Linux
Banner	6838/6838	10332/10332	0/0	253/253
Finger	2503/2503	566/566	8856/8856	2323/2323

The accuracy of the Banner and Fingerprint findings is guaranteed (100% correct).

References

[1] Qing Si Han. Cryptography and computer network security [M]. Beijing: Tsinghua University Press, 2009.

[2] Denning An Intrusion Model [J].IEEE on Software Engineering, February 1987 (2):222. D. (Detection) Transactions.

[3] Ge Yanqiang. Practical technology of computer network security [M]. China Water Conservancy and Hydropower Press, 2010.

[4] Chen Xi. Neural network intrusion detection system research and design based on [D]. of Soochow University, 2012, 4.

[5] Bi Zhanke, Xu Shengli. Intrusion detection technology research and development of. [J] Software Guide, 2011, 11 (9): 152-154.

[6] Zhou Xia. Intrusion detection technology based on data mining [J]. High Tech Industry Development.2011, 12:31-32.

[7] Liu Jianwei. Introduction to network security [M]. Publishing House of Electronics Industry, 2010:171.

[8] Wang Qun. Computer network security technology [M]. Tsinghua University Press, 2010.

[9] Lin orchard, Huang Hao, Zhang Yongping. Research progress of intrusion detection system [J]. Computer Science, 2008, (2): 69-74.

[10] Lin orchard, Cao Tianjie. Overview of intrusion detection system [J]. Computer Applications and Software, 2009, (3): 14-17.