Advances in Engineering Research, volume 138

2nd International Conference on Machinery, Electronics and Control Simulation (MECS 2017)

Information Security Protection System based on Intrusion Detection from Real Time Angle

Yue Qian[a], Siyuan Zhang

Lijiang Teachers College, Lijiang, China

[a]iift6109485@126.com

Keywords: Intrusion detection, real-time information, security protection system, technique.

Abstract. Intrusion detection technology is a kind of active security technology of computer network, which can detect all kinds of malicious attacks in time and respond to the network system. It is a reasonable complement of traditional security technology, such as firewall, is a new network security technology, but also a hot spot in the research of computer network security theory. This paper mainly introduces the main function, structure model, main types and defects of intrusion detection system. Active defense is one of the basic ideas of information security. This paper gives a detailed analysis of the intrusion detection system (IDS) in the application of active defense in the shortcomings and deficiencies, further elaborated the intrusion prevention system (IPS) design idea, technical characteristics and development direction, and demonstrates the important role of IPS in active defense. Research and application show that the transition from intrusion detection to intrusion protection is the inevitable choice of information security.

1. Introduction

With the rapid development of the Internet and the construction of the global information highway, the information technology and the network space have injected new vitality into the social economy, science and technology, culture, education and management. Using the Internet, enterprises can improve work efficiency and market reaction speed, enhance market competitiveness. The network makes the data transmission and access more convenient, but also brings many problems, especially the security problem.

In order to protect network security, firewall technology. In the traditional sense, the firewall is set up between different networks or different network security domains, which can control the information flow in and out of the network according to the security policy of the enterprise. It has strong anti-attack ability, is to provide information security services, network and information security infrastructure [1-2].

Through the development of security policy, firewall can monitor, restrict and change the data flow through the firewall. In essence, the firewall follows the network communication security mechanism, provides the controllable network communication, and only allows the authorized information to pass. From the formal point of view, the firewall can be divided into boundary firewall and distributed firewall. A boundary firewall is placed between two networks to provide a secure network for different network environments.

Distributed firewall is a kind of host - based security system, which can protect the server, data and workstation from the illegal intrusion. NetEye IDS intrusion detection system and NetCop security protection system are typical representatives of the two firewalls.

In recent years, with the popularity of computers and the rapid development of the Internet, WEB services as the representative of the mass information services are increasingly widely accepted. The information service platform of B/S structure has been widely used in many fields, such as education, government and enterprise, scientific research and so on. However, in the process of knowledge acquisition and information processing more and more convenient, fast, system security and data security issues. The security problem is solved effectively, which is the key to the success of information technology and the stable development of enterprises.

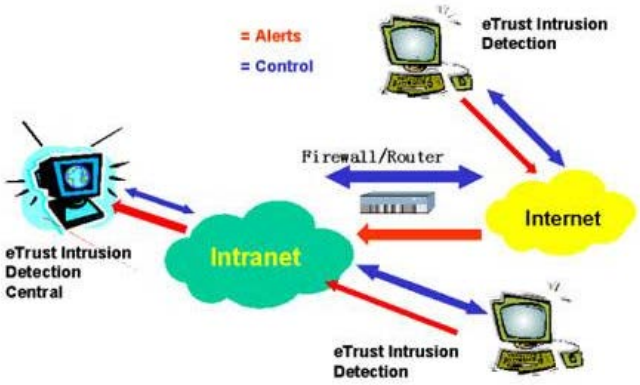

Figure.1 Intrusion detection system

2. The Proposed Methodology

2.1 The concept of intrusion detection

Intrusion detection is a new generation of security technology after firewall, information encryption and other traditional security protection methods. It monitors the events occurring in a computer system or network, and analyzes them in an attempt to find intrusions that compromise confidentiality, integrity, availability, or bypass security mechanisms. Intrusion detection system (IDS) is a software or hardware product that automatically performs the monitoring and analysis process [3].

The general process of intrusion detection is: information collection, information (data) preprocessing, data detection and analysis, response to security policy. Among them, the information source is the data which contains the most original intrusion behavior information, mainly the network, the system audit data or the original network data package. Data preprocessing refers to the pretreatment of the collected data, which can be transformed into the data format which can be accepted by the detection model, and the redundant information is removed. Detection model is a detection and analysis model based on various detection algorithms. Generally, it is the result of data input and data output.

Due to the low detection rate of a single detection model, it is often necessary to use multiple detection models for parallel processing. A security policy is a policy set according to security requirements. Response processing mainly refers to the comprehensive security policy and the test results of the response process, including the generation of test reports, notify the administrator, disconnect the network connection or change the configuration of the firewall and other active defense measures.

The intrusion detection system as a kind of active security tools, provides real-time protection to internal and external attacks and misuse, alarm, intercept and respond before the computer network and system attacked.

2.2 Structure model of intrusion detection system

A complete intrusion detection system should include the detector, analyzer, and user interface. The detector is responsible for collecting any system data that may contain intrusion behavior, such as network packets, log files, and system call logs, and then sends the data to the parser.

The task of the parser is to find out the information contained in the data collected from the detector, and provide relevant measures [4].

The user interface is convenient for the user to control the behavior of the system.

2.3 Main types of intrusion detection systems

The host based intrusion detection system is usually installed on the host, which is mainly used to analyze and check the network connection and the system audit log. When suspicious behavior and security violations are detected, the system will alert the administrator to take action.

Network based intrusion detection system (IDS) is usually installed in the network segments which need to be protected. If an intrusion or suspicious event is detected, the intrusion detection

system will issue an alarm or even cut off the network connection. Network based intrusion detection system is a system, its operation will not increase the burden on the original system and network.

The intrusion detection system can be divided into two types: misuse detection and anomaly detection.

Misuse detection is also known as feature detection, which assumes that the intruder activity can be represented by a pattern. It can check out the existing intrusion methods, but can not do with the new intrusion methods. The difficulty lies in how to make the design pattern can express the invasion phenomenon, and will not include the normal activities.

The typical features of this kind of detection technology are feature pattern matching, protocol analysis and protocol analysis. The feature pattern matching technique is to compare the collected information with the known network intrusion and misuse pattern database, and find the intrusion behavior that violates the security policy. The feature pattern matching has high accuracy for the detection of the underlying network, and the technology is mature and easy to implement. But the weakness is that the technology needs to be constantly upgraded to deal with emerging attacks, and can not detect unknown attacks.

Statistical analysis method can be used to create a statistical description of the system object, statistics of the normal use of some measurement attributes. The average value of the measurement attribute will be used to compare the behavior of the network, the system, any observation values outside the normal range, it is considered to have occurred. The advantage of this system is that it can detect unknown intrusions and more complex intrusions. The disadvantage is that the false positives and false negatives are high, and they are not suitable for the sudden change of the normal behavior of users. The specific statistical analysis methods are based on expert system, model-based reasoning and neural network. Data reorganization is the analysis of the data flow of the network connection, and not just a single packet. Behavioral analysis technology is not only a simple analysis of a single attack, but also based on the events before and after the event to confirm whether there is an attack, the effectiveness of the attack is the highest level of intrusion detection technology.

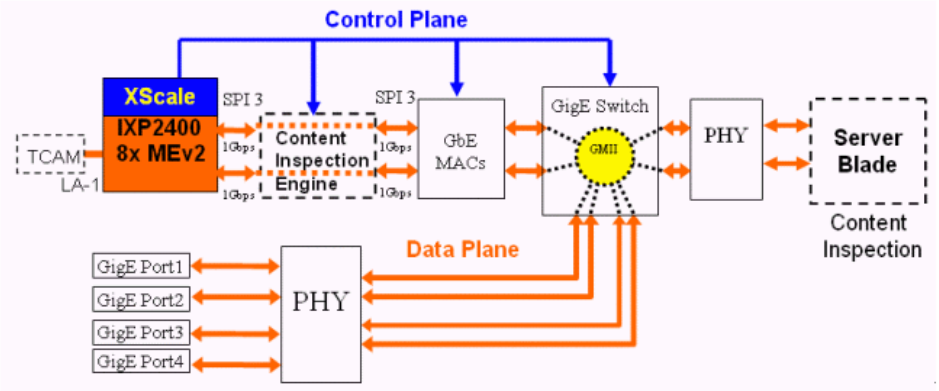

Figure 2. Intrusion detection systems

2.4 Offline detection and online detection

Off line detection system is a system that works in real time. It analyzes the audit events afterwards, and checks the intrusion activity. After the intrusion detection by the network management personnel, according to their computer system of the user operation history of the audit records to determine whether there is intrusion, if there is a disconnect, and record evidence of intrusion and data recovery.

The online detection system is a real-time on-line detection system, which includes the analysis of real-time network data packets and the analysis of real-time host audit. The work is the process of real-time intrusion detection in network connection process, the system according to the storage model, user actions in the computer expert knowledge and neural network model to the user to judge the current operation, once found signs of intrusion connection immediately disconnect the invaders with the host, and the collection of evidence and the implementation of data recovery.

2.5 The main disadvantages and shortcomings of intrusion detection system

Intrusion mainly refers to the unauthorized use of information system resources. Intrusion detection collects and analyzes the information of some key points of the information system to judge

whether there is any violation of security policy and the indication of invasion. However, research and practice show that IDS has the following major shortcomings and deficiencies.

Increasing knowledge of the attacker, mature, and various automated tools are becoming more and more complex and detailed methods of attack, forcing the intrusion detection system must keep track of the latest security technology, can not be far beyond the attacker.

Difficult to identify malicious information using encrypted transmission. Network intrusion detection system by matching network packet finding attacks, intrusion detection systems are often assumed to attack information through clear transmission of information, so the change detection may deceive the intrusion detection system.

It is difficult to cope with the increasing network traffic. Users often require intrusion detection system to alert as soon as possible, so it is necessary to analyze the data in real time. This leads to the system of the increasingly high demand, though, for hundreds of megabytes of traffic, a single intrusion detection system is still very difficult to deal with.

Switch causes changes in the network environment. The traditional intrusion detection is a hybrid mode by setting the network card, so as to read the network data packets transmitted in the lan.

The intrusion detection system is lack of interoperability in the standards. Changing intrusion detection market is difficult to purchase and maintain intrusion detection system. The intrusion detection system needs to be upgraded in order to ensure the security of the network, and there are great differences between the different manufacturers in the upgrade cycle, upgrade means. Therefore, it is difficult for users to make a decision at the time of purchase, while maintenance is often in a very passive situation.

High false alarm rate. A large number of false positives and false reports make it difficult to find the real security vulnerabilities, and can not analyze a blocked network.

Perfect intrusion detection system cannot be achieved. The main reason for this phenomenon is that the intrusion detection system must be clear about the operating conditions and even the details of all operating system network protocols. Different operating systems, or even different versions of the same operating system between the details of the protocol processing are different, and strive to be comprehensive is bound to violate the principle of efficient intrusion detection system.

3. Conclusion

The intrusion detection system in the future will be combined with other network management software to form a tool for intrusion detection, network management and network monitoring. The emergence of powerful intrusion detection software greatly facilitates the management of the network and in fact, the alarm for network security has increased the protection of another. Although there are still many technical problems, but as the development of attack technology, intrusion detection will continue to update, mature. Even with the most powerful intrusion detection system, if you do not fix the security vulnerabilities in the network, there is no way to talk about security. It is not difficult to see that the intrusion prevention system as the key technology of active defense is an important part of the new generation of security defense strategy. Computer and network are not the most safes place to store information, we have to store important information in the computer, and how to enhance the ability of real-time monitoring and computer network with high reliability is very important.

References

[1] Sun, Huibin, et al. "Smart responsive phosphorescent materials for data recording and security protection." *Nature communications* 5 (2014).

[2] Wang, H. and Wang, J., 2014, November. An effective image representation method using kernel classification. In Tools with Artificial Intelligence (ICTAI), 2014 IEEE 26th International Conference on (pp. 853-858). IEEE.

[3] Xu, Yanyan, et al. "A content security protection scheme in JPEG compressed domain." *Journal of Visual Communication and Image Representation* 25.5 (2014): 805-813.

[4] Anisimov, V. G., et al. "A risk-oriented approach to the control arrangement of security protection subsystems of information systems." *Automatic Control and Computer Sciences* 50.8 (2016).