Research on Campus Network Protection Technology

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

Keywords: Campus network; Security; Intrusion detection; Measures

Abstract. With the popularity of the network, all colleges and universities have established their own campus network platform. With the increasing use of campus network, hacker attacks, worm infection, illegal invasion and other behaviors seriously affect the safety of campus network, campus network security is particularly important. This paper introduces the security status of campus network, the classification of Intrusion Detection System, the role and Intrusion Detection process, and puts forward the main measures of campus network security.

Introduction

Campus network plays an important role in many colleges and universities, but also faces many security problems. The security of campus network has become one of the security issues that must be paid attention to. The so-called [1] network security, hardware, software and network is the network all the data resources are required to protect, to minimize the possibility of data and resources are being attacked, not by chance or intentionally damaging attack, change, leakage, to ensure continuous and reliable system, normal operation. The security of campus network mainly refers to the information security of campus network, in addition to the protection and management of some equipment. Campus network plays an important role in many colleges and universities, but also faces many security problems. The security of campus network has become one of the security issues that must be paid attention to. The so-called network security, hardware, software and network is the network all the data resources are required to protect, to minimize the possibility of data and resources are being attacked, not by chance or intentionally damaging attack, change, leakage, to ensure continuous and reliable system, normal operation [1]. The security of campus network mainly refers to the information security of campus network, in addition to the protection and management of some equipment.

Common Security Protection Technology

Firewall. A firewall is a combination of hardware and software; it is through the implementation of security control strategy between two or more networks, refused to external non authorized users' access to internal cyber source, to prevent network users from network attacks. In practical applications, firewalls are usually deployed between Internet and campus networks, thus creating a security barrier between the intranet and the intranet. Firewall can discover unauthorized access from Internet and stop it in time. As a traditional defense technology, firewall still has an irreplaceable role. As the first gateway to resist the external network attack, it plays a pivotal role in the security of campus network.

The main technologies of firewall include packet filtering technology, proxy server technology and network address translation (NAT) technology. However, as a kind of static and passive defense technology, it can discover the known attacks, made after the discovery of the attack response is often "blanket" — or refused, or through. In addition, the internal network from attacks, firewall is often incapable of action [2].

Intrusion Detection. Intrusion Detection System is to collect information from a variety of computer system and network system, and through the information analysis system of network security intrusion features. [3] Intrusion Detection is a dynamic security mechanism to monitor, prevent or resist intrusion behavior. Its working principle is through the real-time monitoring of

network or host state, the captured packets reorganization and analysis, can be identified as information, then according to the characteristics of the rule database to determine whether there is network intrusion behavior [4].

Classification of Systems. According to the detection of host or network, it is divided into host based Intrusion Detection System and network-based Intrusion Detection system:

Host based Intrusion Detection system: detecting intrusion through monitoring and analyzing the audit records of the host. Real time monitoring suspicious links, system logs, illegal access to the intrusion, etc., and provide monitoring of typical applications [5].

Network based Intrusion Detection system, which uses network packet as the analysis data source, finds the attack characteristics in the network data stream of the monitored network. It usually uses a network card working in promiscuous mode to monitor and analyze the data flow through the network, and uses pattern matching and statistical analysis techniques to identify the attack behavior. To detect the attack behavior, the response module makes appropriate response, such as alarm, cut off the network link and so on.

The Function of Intrusion Detection system. Intrusion Detection as a proactive security protection tool, provides real-time protection for the internal and external attacks and misuse, alarm, response and intercept before receiving the harm of computer network and system. It has the following main functions.

By detecting and recording the security violations in the network, the network intrusion time is prevented.

Detect other security measures that fail to prevent attacks or security breaches.

Detect the detection behavior of hackers before attack, alert the administrator in advance.

Reporting security threats in a computer system or network.

Provide information about attacks, help administrators to diagnose security vulnerabilities in the network, easy to repair security vulnerabilities.

Deploying intrusion detection system in large and complex computer networks can significantly improve the quality of network security.

Intrusion Detection Process. Intrusion detection process is divided into four parts: information collection, information analysis, information storage and result processing [6].

Information collection: the first step of Intrusion detection is information collection, which includes the status and behavior of system, network, data and user activity.

Information analysis: general through three methods (analysis of pattern matching, statistical analysis and integrity) analyses the state and behavior of information collected on the system, network, data and user activity, trying to find the characteristics of intrusion activities, to determine whether the occurrence of invasion. When intrusion or misuse is detected, a warning is issued and sent to the console.

Information storage: when the Intrusion Detection system to capture the attack occurred, in order to facilitate the system management of the attack information view and attack behavior analysis, Intrusion Detection system will also need to collect information to be saved, this information is usually stored in a user specified log file, and store information for attack retain the evidence.

Results processing: the console responds automatically to the detected behavior in accordance with predefined response measures, such as reconfiguring routers or firewalls, terminating processes, cutting links, and changing file attributes.

Main Measures of Campus Network Security

Strengthen education, improve the safety awareness and protection ability of the vast number of personnel.

Increase investment, improve the network security protection technology; increase investment, the purchase of common protective equipment and protective systems, and correct configuration, designated regular maintenance, to play their respective roles.

A variety of techniques of firewall and intrusion detection, virus protection, prevent illegal access, network attacks and the spread of the virus, ensure the security of network system.

Encryption device is used to encrypt the secret information in the link layer and network layer.

Conclusion

The safety of campus network directly affects the students' learning and life, if not properly prevented; it will bring great adverse effects. Firewalls can't be used to identify attacks and unknown attacks from an intranet. The intrusion detection as a proactive security protection technology, the implementation of the real-time detection and monitoring, can identify not only from external attacks, attacks and illegal operation for authorized users from the network also can be found in a timely manner. In the construction of the campus network security system, firewall and other security technology at the same time, the introduction of intrusion detection system, which complement each other, division of defense layer, set up layers of barriers to intruders, to maximize the maintenance of system security. In the world of computer networks, there is only more security, no absolute security. In the campus network intrusion detection and firewall system linkage deployment, and cannot guarantee the absolute safety of the network, but at least can make the network relatively safe, to some extent, enhanced the security of the campus network.

References

[1] Li Hanjing. Analysis and Countermeasures of college campus safety [J]. Henan Education (Higher Education), 2017, (10): 26-28.
[2] Wang Shusheng. Analysis of information technology construction in Colleges and universities [J/OL]. contemporary educational practice and teaching research, 2017, (11): 194-195.
[3] Liu Liu. On the construction of network culture in Universities [J]. Journal of Yan'an University (SOCIAL SCIENCES EDITION), 2017,39 (04): 121-124.
[4]Sang Jing. Network security problem analysis and countermeasure research [J]. Fujian computer, 2017,33 (08): 50-51+57.
[5] Zhu Lin. Security and management of network access in the construction of campus informatization [J]. Journal of Liaoning Teachers College (NATURAL SCIENCE EDITION), 2017,19 (02): 41-43.
[6] Cai Chunying. Analysis and solution of network security in campus network [J]. digital communication world, 2017, (08): 205.