Chapter 60
Research on Campus Network Security Problem and Protection Strategy

Yongli Liu
College of Engineering and Technology, China University of Geosciences, Baoding, China

Weifang Zhai
China University of Geosciences, Baoding, China

Song Ji
China University of Geosciences, Baoding, China

ABSTRACT

With the "Internet +" era of arrival, the major colleges and universities are in the construction of the wisdom of the campus, students and teachers living with the campus network is more and more closely related, Campus network security has become the protection of the wisdom of the campus construction. Campus network security issues become increasingly serious; a single security protection has been unable to meet the current security needs. This paper analyzes the major security threats facing the campus network, and presents the campus network security protection measures from the physical layer, network layer, system layer, application layer and management of five aspects, thus constructing the campus network's overall security defense system. The system has multiple security protection for Campus Network, thus improving the security of the campus network.

1. INTRODUCTION

With the "Internet +" era of arrival, global information has become the trend of social development, the major colleges and universities are in the construction of the wisdom of the campus. Campus network has become an important means of teaching, research, and office and information exchange. On the one hand, Campus network contains a large number of valuable data, such as learning data, teaching

DOI: 10.4018/978-1-7998-7705-9.ch060

data, research data, reward and punishment data; on the other hand, the application of campus network is becoming more and more perfect, scale is gradually increasing, facing more and more users, and management is relatively loose. In this context, Campus network security is becoming more and more serious, such as physical security, worms, system vulnerabilities, cyber-attacks, unauthorized access, and so on. These insecurity factors threaten the safety of the campus network constantly, when the campus network encounters problems, the school's teaching and daily management work will be seriously affected. For such a serious security threat, once the network is compromised, the attacker may not be found, the use of attack tools, attack methods, attack targets are ignorant. Currently, Campus network security protection mainly uses firewall, intrusion detection and other passive defense measures, these security measures are generally based on rules and feature matching, can only prevent known attacks, cannot prevent new attacks (Liu et al., 2015; Zhu et al., 2015; Chen, 2016).

Honeynet technology is an active defense technology, by simulating multiple vulnerable hosts, attract and trick those who try to illegally access someone else's computer, giving the attacker an easy attack target. Through the Honeynet to capture and control all the data into and out of the Honeynet, after analysis, get the tools, strategies, and motivations that hackers used, and thus with the firewall, intrusion detection technology together to form a linkage defense, to protect the safety of the campus network (Li, 2015; Li and Li, 2015).

The authors take the Great Wall College as an example, on the basis of analyzing the security of campus network; a multi-protection system of campus network is constructed, and presents the campus network security protection measures from the physical layer, network layer, system layer, application layer and management of five aspects.

2. CAMPUS NETWORK SECURITY ISSUES

2.1. Physical Security Risk

The primary threat facing the campus network security is the physical security. Physical security threats may come from natural, environmental and technical failures and other non-human factors, for example, if the physical location of the campus network equipment design is unreasonable, it is possible to suffer water, electricity, fire or lightning damage; Physical security threats may also come from personnel failures and malicious physical attacks, such as network equipment theft or physical damage (Du, 2015).

2.2. System Vulnerabilities and Virus Intrusions

Each server in the campus network is equipped with Windows operating system or Linux operating system. On one side, in the design and implementation of the operating system itself there are some security risks, it's difficult to avoid security vulnerabilities, computer viruses and hackers may use the operating system security vulnerabilities on the campus network attacks; on the other side, in the campus network running educational administration, personnel management, attendance management, financial management and other important application services, these applications and teachers and students are closely related, the software is generally from third-party software vendors, because the software update is not fast enough, there will inevitably be some loopholes. In the process of using the software, if found that the vulnerability is not timely, nor is it maintained, it is easy to become the object of hacking, will