Research of LAN Security Attack and Defense Technology

Ying Peng [1], Rongfu Wang [1]

[1] Nanchang Institute of Science & Technology, Nanchang, Jiangxi, China, 330108

KEYWORDS: LAN; Security Attack and Defense; Network Technology

ABSTRACT: With the continuous development of information technology era has arrived, LAN has been gaining in popularity in the use of people's daily work, at the same time, LAN security issues prominent. In this paper, LAN security for analysis, testing their safety and make relevant recommendations to its reasonable security policies.

Introduction

LAN refers to a network system within a fixed area network servers and multiple computers composed, easy to install, easy to expand, easy management, high mobility characteristics. In recent years, with the rapid development of wireless communication technology, LAN has also been a rapid development, and gradually has been widely used in the field of corporate office. However, in the office for people to bring convenience, virtual LANs, openness also allows users facing some new information security issues. So how to ensure that information and data do not destroyed, changed or deleted, the network will not be interrupted, the network system to normal operation? This requires us to do security attack and defense testing and analysis for LAN security issues faced, and effectively improve the security of the LAN.

LAN Antivirus Overview

In general, the LAN security includes two aspects, one anti-virus, and second, anti-hacker. About anti-virus problem, LAN users in particular, should be stressed. According to the author many years of experience working in the network, many companies internal LAN users have this misconception - that since they have in the network, and that they do not have what the machine is equipped with anti-virus software, network management will naturally stop those viruses in outside the network. This is obviously very funny, because who does not NMS genetic immunization virus, if any, are so many viruses also fail to do so over. And it is out of the work of anti-virus neglect important information many companies are inevitably "brutally tea charcoal." Study the fundamental reason, because most viruses have self-replicating feature, they will not be limited to only attack on a computer network, "poisoned" the computer tends to hurt the other LAN users. And this kind of virus proliferation in the LAN, it is also far from a stand-alone virus stubborn degree comparable to staff A virus on your machine often happens after a clean kill, because the staff will B virus yet again been infected with the virus Happening. For example, the notorious FunLove, simply lingering representative for!

So, for LAN users to attack from viruses, undoubtedly the most important is to install anti-virus software, and its timely upgrades (preferably as Panda AntiVirus and Norton AntiVirus as automatic upgrades), this and single user requirements are the same. Also, if you need to share folders with other users, we recommend that you never completely open with no password sharing. When almost all of the virus outbreak in the LAN, no password is completely shared folder are the primary entry point for the virus, because it does not require any write operation can be verified, the virus can quietly enter your computer, and began to replicate itself so that the rapid expansion of the entire system.

In short, the main LAN security issues facing are: Computer system itself loopholes provided an opportunity to hackers. Electromagnetic radiation of wireless networks is difficult to precisely control within a certain range, the signal easily be intercepted or tracked, such as any wireless device within the AP service area can receive a signal to the LAN, the intruder to install a device on the LAN to access MAC address of the network can be obtained in a legitimate site, and change the MAC address and service set identifier, thus masquerading as legitimate LAN MAC address and service set identifier, using the legal status of the network to modify or steal information. Scalability and openness of the network to create a larger space for the upgrade of computer viruses, thereby enabling enhanced destructive virus, so that the normal operation of computer software and network systems face security threats. Hackers unauthorized access to computer systems are attacked, resulting in paralysis of the network, a lot of important information and data is lost.

LAN Security Attack And Defense Strategies

LAN settings are divided into two types, one is to set up a shared network user, the other is by the router to the LAN connection in computer network security is the most important thing is the data flow between the control. A firewall is computer hardware and software within the constitution, which can effectively two network connection control, and can effectively access the LAN computer security protection.

Computer system Windows 2000/XP, Linux these two major operating systems are also vulnerable, the network criminals often take advantage of these we do not know the loopholes left attack. Specific action is being attacked by computer scanning to find vulnerabilities, select the attack software based on the scanned information out vulnerability to attack, because it is the loopholes in the system, which makes computer without any defensive measures can only "any people kill.

Create LAN, users need to do security authentication, all users on the LAN require authentication by an entity allowed to participate, includes the main servers, clients, users, and other related equipment. Among these the most important is the client and user authentication is particularly important part. Second question is about the authorization of management, making management settings on all the resources you want to have a detailed and comprehensive record in the LAN, only the internal management system attention, in order to ensure their safety. All make all LAN users understand the importance of the safe use of the LAN, can enable enterprises to establish a set of sound management mechanism and security technical maintenance program, so as to enable LAN security to get some protection.

LAN Security Offensive and Defensive Test

Intruder masquerading access point can be normal access to the LAN or local area network reaches attack damage, change, delete the destination computer important information data. For this purpose, it can be detected by the following ways: to install two detectors, a normal operation, the other LAN monitor, or install an investigation detector with two wireless network card, a network card running, another card LAN is listening. Once the detector to capture two of the same access point MAC addresses, immediate access to the ping command legitimate access point, time to find camouflage access point, and then take measures against illegal access point for processing, to ensure network security. This function can be provided in support of the wireless access point to access the list, use the MAC address of unauthorized personnel limited by the access list, and often view the AP logs, early detection of intruders. Wi-Fi MAC address filtering configuration shown in Figure 1. In addition, since the wireless encryption protocol Challenge question is transmitted in the clear, the intruder would exploit this vulnerability by masquerading as legitimate users send a request by rogue AP authentication, for business users to increase measures firewall, network isolation, or use SSH, IPSec, WEP encryption and other means to ensure data security.

LAN's own openness, vulnerability, survivability and weak characteristics that make it vulnerable to denial of service attacks, intruders LAN systems use their own security vulnerabilities, attacks by special services server, causing the server resources are used, so that the server can not be provide services, and finally to the collapse of the entire LAN. Most of the physical layer denial of service attacks and MCA layer appears.

Centre for the physical layer, should strictly implement the relevant national standards, the construction of the user LAN when away from strong magnetic fields to choose the role of the environment as much as possible, try not to be disposed in the antenna near a window position, but on the target coverage area Meanwhile, not only to avoid the destruction of natural disasters on the LAN, but also to prevent human error. Denial of service attack can work using direct sequence spread spectrum devices have a greater role in order to detect such an attack, the situation can be controlled by the use of radio spectrum by spectrum monitoring method, thus achieving the communication signal control, but due to the large volume, high cost, and the LAN can only be disposed of spectrum monitoring equipment to key parts of the future so we do not need to need to find a reliable method of detection and analysis spectrum of service attacks such as denial of Queensland attack. For the MAC layer, the use of intrusion detection systems in real-time transmission of data LAN to detect the existence of the illegal invasion analyze problems and then monitor, analyze, judge attacks the intruder and the specific type of intrusion events, network traffic found abnormal situation, to take timely measures to deal with.

LAN related security management is also very necessary. In practice, we should strengthen the management of network hardware, time detection of network hardware devices working conditions, to ensure that it works to prevent aging equipment; the use of a router on the network traffic, packet and port monitoring; set up a special staff workstation hardware and software equipment for regular maintenance to ensure the normal operation of the LAN; often to back up important data and routers, servers, switches and other systems on the LAN so vulnerable to attacks result in data loss when the system is damaged, before the full backup rapid recovery of data and systems, enabling the network to resume normal operation as soon as possible.

On local area network construction of China has a very clear requirements and regulations, in the choice of the environment on the area to stay away from the strong magnetic field, and to do all kinds of unexpected natural disasters and man-made damage prevention measures, so as to avoid damage to the LAN. In addition to these protective measures, but also respect for the power supply make the appropriate protection, let the power always in working condition, if a sudden power failure occurs when there is standby power must be able to ensure the use of the top, which can guarantee its in the safe use of electricity on. Hackers can hack into your computer is often overlooked because the general system vulnerabilities and hide the shared settings. As long as the computer LAN hidden share closed, the computer can make the security and defense capability would be enhanced, while making access settings, establish identity authentication system, and a computer important data and information for backup, so in order to reduce losses after the invasion.

Conclusion

All in all, along with the rapid development of wireless communication technology, LAN has also been rapid development, greatly changing the way people work and live, but it is precisely because of this, related to the growing problem of network security, intruders masquerading access point or use LAN security vulnerability itself a denial of service through a special method can steal, alter or delete important information on the computer or the network breaks, causing the network system is not functioning properly, these problems could have caused no small personal or business loss. To this end, we have to use the computer in the process, pay more attention to safety precautions work for camouflage access point, denial of service attacks caused by security problems, and enhance network security attack and defense testing and analysis, security attack and defense policy in order to ensure the safe operation to ensure that information on the local area network and information security in the communication process.

Reference:

[1] Xu Sung. Security Defense Test and Analysis LAN [J]. Management & Technology: Xunkan, 2014 (3).

[2] Li Haiyan, Security Attack and Defense Testing and Analysis of Li Yuan. LAN [J]. Coal Technology, 2012 (2).

[3]. Zhang Xifeng Construction Quality of Building Waterproof Engineering Controls [J]. Heilongjiang Science and Technology Information, 2011 (13): 254.

[4] Shen Lijun. Construction Quality Control of Construction Waterproofing Explore [J]. Quality of Goods and (Science And Law), 2014 (4): 78.