Advances in Intelligent Systems Research, volume 147

International Conference on Network, Communication, Computer Engineering (NCCE 2018)

Design and Research on the Test of Internal Network Penetration Test

Lei Wang [a)]

School of Jianqiao University, Shanghai 201306, China.

Abstract. According to the increasingly serious network security problems, a complete set of internal network penetration testing method is proposed for the Windows operating system, and the key resources of the intranet are taken as the center, and a concrete solution to the protection is put forward. Finally, the contents of the article are summarized.

Key words: Intranet Penetration, Brute Force, Default Sharing, Trap Account.

INTRODUCTION

At present, the development of computer network is growing faster and faster, people are increasingly dependent on the network life, almost all the daily life is closely related to the network, but the security of the network environment is followed, the modern network security problems are facing huge challenges, computer viruses, and hackers maliciously invading. The problem of operating system security and information leakage is particularly prominent. Therefore, it is imminent to improve the awareness of network security and strengthen the learning of network security skills.

THE CONCEPT AND CHARACTERISTICS OF INTRANET SECURITY

When it comes to network security, people will first think of hacker invasion, computer virus and other cases, but it is not very concerned about the security of the internal network, but the security of the network is a very important node in the whole link of the network security. According to the results of the survey of the national information security assessment and certification center of China, 85 More than percent of the information security problems mainly come from leakage and internal personnel crime, intranet users because of poor personal security awareness, the use of operational habits, and other problems, the internal network caused huge security problems. The traditional network security is mainly to prevent the attack from the external network to the internal network, that is, the external network security, the external network security precautions are the premise that the internal network is safe. At present, the measures to prevent the external network include the firewall technology, intrusion detection technology, virtual private network technology, security mail gateway technology and so on. The firewall technology is the widely used external network prevention technology, through the data monitoring, restriction, strategy control filtering flow through the firewall related data, so as to ensure the security of the network.

The basic definition of internal network security refers to the problems of network security protection, information leakage prevention and terminal equipment security inside the LAN. The object of the internal network security focus is the internal network users, application environment, application environment boundary and internal communication security that cause security threats. Therefore, it is very important to detect safety problems through penetration test.

METHODS AND MEANS OF INTERNAL NETWORK PENETRATION TEST

At present, the method of penetration test for internal network can be divided into direct infiltration and indirect infiltration according to the type of protocol used by them [1]. Direct penetration refers to the penetration of the system username obtained by the target, combined with the cipher cracking. The indirect infiltration mainly refers to the use of various deception means to infiltrate the network. The experiments involved in this paper the content is mainly designed in the way of direct penetration.

The methods of penetration test include the following

Scanning technology: scanning can be divided into scanning for user information and scanning for vulnerabilities. The former refers to the valuable information of the host's operating system, user name and so on through connecting and asking some services. The latter refers to whether there are vulnerabilities and vulnerabilities that can be used for attack behavior by sending a special message to a specific port and judging the system platform based on the response [2].

Password cracking technology: this technology is mainly used in direct infiltration. After the attacker obtains the user name by scanning and other means, the password guesswork is used to test the password of the attacked system by using the dictionary or the exhaustive method. If it can be successfully cracked, the password can be legally entered into the system.

Network sniffing Technology [3]: network sniffing, or network monitoring, is mainly to capture data transmitted in the network by intercepting data packets on the network to obtain authentication information or other valuable information of the attacked system. If the data in the network is transmitted in plaintext, it will be able to obtain important information such as account order directly through network sniffing.

Deception technology: in a network, a certain identity is used to determine whether or not it is given a certain right to a target. If an attacker gets or camouflage the identity, it can get the access or operation of the target. This attack method is called deception. IP cheating, e-mail spoofing, DNS spoofing, ARP cheating, WEB cheating and cheating by social engineering are common [4].

Vulnerability utilization technology: system platform vulnerability, application service software vulnerabilities, program security defects, and network security vulnerabilities can all be the breakthrough point of Infiltrator attack [5].

SECURITY THREATS OF THE INTRANET

The security threats of the intranet include the following:

Security Threats from the External Network

Every intranet connected to the Internet will be threatened by the Internet. If the internal network does not take certain security measures, it will be vulnerable to intrusion and destruction attacks by external network hackers. The attacker from the outside will scan the detection, collect the important data resources in the inner network, excavate the loopholes, get the control of the host, and destroy the whole network security.

Security Threats from Internal Network

Another important problem of internal network threat is the internal personnel management, how to improve the security awareness of the internal network managers, strengthen the level of network security technology, observe the professional ethics of network security, ensure that the internal personnel are malicious, purposeful, or unintentionally reveal important information out of various purposes.

Security Vulnerabilities from the System Platform

There will be some security vulnerabilities in the design and development process of various operating systems. These vulnerabilities have great security risks for the internal network security.

Security Vulnerabilities from Applications

Intranet users will install a variety of application services in the operating system. These applications may have threats or security vulnerabilities in themselves. If hackers use these vulnerabilities to attack, they can also damage the security of the internal network, so it is necessary to reinforce the security problems of these applications.

THE MAIN OPERATION PROCESS OF INTERNAL NETWORK PENETRATION TEST

In this paper, the internal network penetration test is carried out by direct penetration and password cracking tools. The operating system takes Windows as an example, and the specific operation process is as follows:

Step 1: first, use various scanning tools to scan the target object, obtain the important information of the specific host in the inside network, including the host name, IP address, MAC address, etc., such as the internal network scanning tools, such as the LAN view tool, IP SCAN, etc.

Step 2: when you get the IP address of the tested intranet host, you can use a simple DOS command for exploratory testing, for example, using the command line net use k: \\192.168.10.11\c$to try to map the PC disk of the tested host to the machine, indicating that the host requires an account and a password to allow a connection. This explains the default shared function of the host system's operating system is in the open state, and has the possibility of penetration testing.

Step 3: use all kinds of brute force software to crack the account password. Only by breaking the password of the account can we achieve the next step of intrusion. This is a very classic violence cracking tool, Hydra, which is released by the famous hacker organization THC, an open source of violence cracking tool that can cross platform, have a corresponding version in Windows and Linux, and the software can be cracked for all kinds of services. It's a very practical tool for violence. The main needs to be cracked in the internal network infiltration is the related content of the network file sharing protocol, that is, to break the SMB. To the above host for example, the command line to break the SMB is Hydra -l administrator -P pass.txt 192.168.229.149 SMB, and the -l parameter is the specified crack account, the -P command is the dictionary that specifies the corresponding crack, through the read word. Each code in the code enumerates the password for the administrator, a violent attempt administrator account, until the success is cracked, and the specific results are shown as shown in Figure 1. By the result, the administrator password has been cracked, the password is 123456, and the administrator of the internal network host and the password of 123456 can achieve the next internal network penetration test.

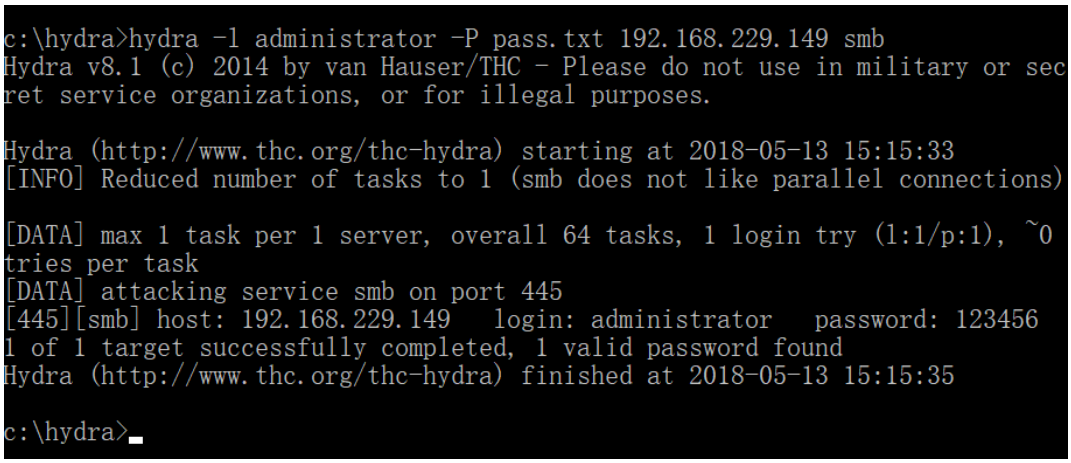

FIGURE 1. Brute force.

Step 4: Hydra the key to software cracking is that it has powerful dictionary files, and only the number of dictionary passwords is enough, it can crack the passwords of corresponding accounts. After the crack is completed, after getting the password of the administrator, we can execute step 2 again, carry on the mapping operation of the network sharing disk, and input the administrator's account and password when mapping, the basic operation of the

internal network penetration test can be completed, the administrator's right limit of the test host and the corresponding data resources are obtained, and the concrete execution node is obtained.

PROTECTION MEASURES OF INTERNAL NETWORK REINFORCEMENT

In view of the intrusion mode of the internal network penetration test, the specific protection measures are put forward to prevent the infiltration of this kind of internal network. The internal network infiltration operation described above is mainly aimed at the internal network host does not modify the original administrator account and the default sharing of the operating system and leads the hacker to use this loophole to carry out the internal network. The administrator's account password has been obtained, and the system resources have been obtained. Therefore, the relevant protection measures are as follows:

Step 1: delete the default sharing of the operating system, strengthen the system security, use the net share command line to delete the system default sharing, so that the system resources are safe, the specific command line is as follows net share c$/del, but the default share will be restored after each reboot of the system, so the batch file can be recommended. And place the file in the system startup folder, so that the default share can be automatically deleted at every time the system is launched.

Step 2: using the operation mode of trap account, making the trap for hacker, the specific steps are as follows. First, the original administrator name is testament, the strong password is set and forbidden, the original administrator account is protected, the new user guestadmin is built, and the strong password is set up, which is subordinate to the administrator group. For daily use, a new user called administrator, set up a strong password, and subordinate it to the guest's guest group, is a trap to deal with the hacker's invasion of the machine.

Step 3: change the administrator password regularly and set up a strong password with high complexity.

SUMMARY

Intranet security is an important part of network security. Only by strengthening the security and protection ability of the internal network and improving the network security awareness of the internal network managers, can we deal with the network threat from the external network. This paper proposes a basic penetration test method for the internal network security and aims at the proposed intrusion. The phenomenon gives specific solutions and provides solutions for users to enhance the security of Intranet, and the relevant operation skills, so as to ensure the security of intranet.

REFERENCES

1. Wang Xiao Cong, Zhang Ran, Huang Changwon. Analysis of penetration testing technology [J]. Computer science, 2012, 39 (S1): 86-88.
2. Chen Pieta, Chen Guangzhou. Computer network security and vulnerability scanning technology [J]. Electronic technology and software engineering, 2017 (02): 227.
3. Liu Guanine. Application of network sniffing technology in computer information security analysis [J]. Computer and telecommunications, 2014 (12): 52-53.
4. Jian Zhao Peng, Fang bin Xing, Liu Change, Liu Qi Xu, and Lin Jian Boa. Summary of network deception technology [J]. Journal of communication, 2017, 38 (12): 128-143.
5. Lu Gang, MS Chao, Goo Songhua, .2015 information security vulnerabilities research overview P [J]. Information security and communication secrecy, 2016 (05): 95-99.