Research on network security technology of industrial control system

Kai Jin[1], Zhanji Niu[2], Jieping Liu[3], Jinxue Bai[4], and Lei Zhang[5,*]

[1]College of artificial intelligence and data science, Hebei University of Technology, China
[2]Information Security Evaluation Center of Hebei province, China
[3]Thermal Power Corporation of Qinhuangdao, China
[4]Lanke Network Engineering Group Co., Ltd of Hebei province, China
[5]College of artificial intelligence and data science, Hebei University of Technology, China

Abstract. The relationship between industrial control system and Internet is becoming closer and closer, and its network security has attracted much attention. Penetration testing is an active network intrusion detection technology, which plays an indispensable role in protecting the security of the system. This paper mainly introduces the principle of penetration testing, summarizes the current cutting-edge penetration testing technology, and looks forward to its development.

Keywords: Industrial control system, Penetration testing.

1 Introduction

The Industrial Internet, as a product of the deep integration of a new generation of network information technology and manufacturing, is an important infrastructure and key technical support for the realization of industrial digitization, networking, and intelligent development. It is widely regarded as an important cornerstone of the fourth industrial revolution. my country's industrial Internet has basically started at the same time as developed countries. In recent years, the construction of 5G infrastructure has been continuously improved, and the integration of new technologies, new applications and industrial Internet technology has continued to develop and promote the use, which has brought huge opportunities for the development of my country's industrial Internet. [1] my country's industrial Internet is also facing severe challenges. As a typical industrial control system, the heating system has gradually grown in scale, with a very complex structure and many hidden safety hazards. During the operation of the heating system, once a safety accident occurs, it is extremely easy to cause very serious social harm. With the modernization of the heating system, the network security aspect of the system has also been paid more attention. Penetration test is a mechanism provided to prove that network defense is operating normally according to the expected plan, and it has an important position in industrial control system in network security. This article mainly introduces the centralized testing method of penetration testing in industrial control system.

[*] Corresponding author: zhanglei@hebut.edu.cn

2 Introduction to penetration testing technology

Penetration testing is an evaluation method to evaluate the security of computer network systems by simulating the attack methods of malicious hackers. This process includes active analysis of any weaknesses, technical flaws, or vulnerabilities in the system. This analysis is carried out from a location where an attacker may exist, and from this location, conditionally and actively exploit security vulnerabilities.

In other words, penetration testing means that infiltrators use various methods to test a specific network in different locations (such as from the internal network, from the external network, etc.)in order to discover and mine the vulnerabilities in the system. Then output the penetration test report and submit it to the network owner. Based on the penetration test report provided by the infiltrator, the network owner can clearly understand the hidden dangers and problems in the system. Penetration testing can help an organization understand the current security situation by identifying security issues. This has prompted many units to develop operational plans to reduce the threat of attack or misuse.

The main purpose of network testing is to find out the weaknesses and shortcomings in the network environment, integrate own experience and advanced technology to improve the problem, and prevent hacker attacks and system crashes[2].There is a certain similarity between the network penetration technology and the attack methods used by hackers. The function display is mainly through scanning, attack, testing and function expansion. The main difference between the network attack technology and the network attack technology is that there is no It will affect the normal business development of the system, and the attack methods used will not damage the internal structure of the system. If the network penetration technology can be applied reasonably, various problems in the network system can be found, helping staff to better understand the operating status of the system, and preventing criminals from malicious attacks on the network. In addition, the application of network penetration technology is also the main direction for the future development of network security, and it is also a very important means to ensure the security of information transmission and the security of the network environment.

3 Penetration testing methods

3.1 Port scan

Port scanning is one of the very common test methods. Testers scan a section of ports or designated ports one by one to obtain information on the computer, and then they can attack through the provided known vulnerabilities. At present, scanning and attacks on TCP ports have become very common[3].Ding Lin uses the port scanning tool nmap to scan UDP ports. The UDP protocol is a sub-protocol of the TCP/IP protocol suite, which belongs to the same transport layer protocol as the TCP protocol.

Through the three common scenarios of whether the device has a comprehensive operating system, whether it has a firewall module, and whether it has configurable items in the firewall configuration, the port is filtered and the CLOSE function is returned. In the UDP port security protection, the packets sent to this port are filtered and discarded, and ICMP packets are returned to indicate that the port is unreachable.

3.2 Dynamic external injection test

Dynamic injection testing is to make the code under test run in a controlled manner in a real environment, observe the function, logic, behavior, structure, etc. of the code at runtime from multiple angles, and check the difference between the running result and the expected result to find out. It also analyzes the security requirements such as operating intensity and robustness[4].

In the dynamic injection test, a large amount of real external input data should be obtained as much as possible, and the data source is very important for the test. When conditions are limited and real data cannot be obtained, a large amount of data should be simulated as much as possible. Data preparation includes correct data and incorrect data. The processing of erroneous data and system recovery are the key to fault tolerance testing.

3.3 Intrusion trojan detection

Web page hanging horse is not a specific Trojan horse program, but a way of spreading Trojan horse. It refers to the implantation of malicious code in the source files of web pages through illegal means. When users browse such sites, if their computer systems have corresponding Security vulnerabilities, the malicious code in the webpage will induce the user, The host will download and run the corresponding Trojan horse program, thereby stealing the computer's confidential information, tampering with important data, monitoring voice and video communications, and even completely controlling the infected computer.

Guotian Xu use the Referer field recursive method to analyze the webpage hanging horse, re-browse the webpage on the infected host, and use wireshark to replenish the communication data, select the file restoration function provided by wireshark to restore all the files from the communication data, and then use the mainstream The antivirus engine scans these files for viruses, and records the name and download path of the Trojan horse program[5]. Afterwards, the referer field recursive analysis method of this article is used to restore the complete planting process of the Trojan, find out the website that is linked to the horse and the corresponding page, and extract the malicious code implanted in the web page. As a result, the relevant information of the website that was linked to the horse was obtained, the storage location of the malicious code was accurately located, and the website administrator was prompted to remove the malicious code and strengthen protection measures to block the transmission of the Trojan horse from the source.

4 Summary and outlook

As the relationship between industrial control systems and the Internet is getting closer, the networking of industrial control systems has become a future development trend. The network security of industrial control systems has received unprecedented threats, and industrial control systems have received more and more attention in network security. . Among them, as a very important defense method, penetration testing technology has become a very important research direction for the security of networked industrial control systems.

Compared with traditional computer systems, industrial control systems are very complex, and the differences between different systems are large. Even the same type of control system, because of different production requirements and process parameter standards, etc., lead to different requirements. And different protection methods. Therefore, in actual operation, individualized customization is required for different industrial control systems. With the continuous development of the scale of industrial control systems, the scale of data in industrial networks will become larger and larger, and the difficulty of detection algorithms will become greater and greater. Therefore, in the future penetration testing, the use of deep learning methods will increase. The more extensive, the various algorithm ideas will collide and combine, the comprehensive performance of the test will also be greatly improved, and the effect will be better and better. In industrial control systems, data transmission is in various forms. It is no longer in the form of a single data packet, but also in other forms such as electromagnetic waves. These multi-domain spatial information transmissions also make the industrial control system threatened more diverse ways. The intrusion channel industry has become more abundant, and the difficulty of penetration testing has also increased sharply. In the future, research on industrial control systems in network security will still be an urgent research need in industry and academia, and testing technology will still have a long way to go.

References

1. Fan Yong. Industrial control system network security construction[J]. Shandong Industrial Technology,2019,15(08):141.
2. Liu Jun. Research on Network Penetration Testing Process and Method [J]. Network Security Technology and Application,2020,30(12): 16-17.
3. Ding Lin. Attack and protection of UDP port in power system network[J]. Network Security Technology and Application,2020,60(10): 48-49.
4. Dong Li, Zhao Qi, Zhou Jian. Research on Embedded Software Security Analysis and Testing Method [J]. Information System Engineering,2021,44(05): 70-71.
5. Xu Guotian.Research on Webpage Trouble-shooting Inspection Method Based on Recursive Analysis of Referer Field [J]. Criminal Technology,2016,41(06): 431-436.