Research on network information security penetration test based on IP port service technology

Xiaoyu Wang,1* Dandan Li

Electric Power Research Institute, State Grid Heilongjiang Electric Power Co., Ltd.
Harbin, Heilongjiang, 150030, China

*E-mail: jinggao-1@chinaums.com

Abstract. Network information security penetration test is an important means to intercept network information attacks after obtaining user authorization. At present, various network information security penetration testing technology system research work is also constantly improving and updating. However, due to the increasingly complex verification of hacker behavior, the research of network information security penetration test is still difficult to meet the requirements of the current information development. In this environment, this paper proposes a network information security penetration test method based on IP port service technology, and describes a set of penetration test ideas, steps and results, for network managers to reference, to achieve the network information security penetration test Finally, it was confirmed by experiments, The efficiency and ability of penetration test are improved, and the process of penetration test is optimized.

1. Introduction

Penetration detection is a new protection method in the field of information security. The network information security penetration test method based on IP port service technology can effectively prevent security risks by adjusting IP port service for vulnerability information mining and verifying network information security penetration value with IP port service concept attack[1]. Based on the user's authorization, the network information security threat is intercepted, and the advanced security penetration risk assessment is carried out for the network information security attack, so as to comprehensively and truly simulate the attack behavior and process of hackers, and achieve the purpose of evaluating the security risk level of computer system[2]. Penetration test is a very effective means to detect the degree of network security and information security protection, and is used to detect the degree of network security and information security protection There are potential risks or loopholes in network information, so as to improve the security of computer and network information[3]. Making network information more secure in use is the ultimate goal of preventing attacks. Network information security penetration test based on IP port service technology has become one of the important means to detect network security while ensuring the security of network information and data. After the completion of the penetration test process, the subsequent reports or documents will clearly describe the system vulnerabilities and relevant details, and put forward clear suggestions for modification, so as to improve the effectiveness of network information security penetration test based on IP port service technology.

Other paragraphs are indented (BodytextIndented style).
2. Research on network information security penetration testing

2.1. Network information security penetration test process optimization

In order to ensure the effect of network information security penetration test, we need to further simplify the test process. In the process of network information security penetration test, we need to follow the standard methods and procedures of IP port service, so as to provide guidance for security testing framework[4]. Based on the experience of penetration testers, penetration testing processes for specific IP port networks can be developed. Because of the different IP port network operating environment and the experience of different technicians, there are great differences between each penetration test scheme. In order to ensure the effectiveness of penetration testing for network information security, it is necessary to standardize the basic steps of penetration testing, and summarize the content of penetration testing in different stages of penetration testing, so as to simplify the complexity of the test. In the preparation stage of penetration test, it is necessary to further clarify the goal of penetration test, that is to help users determine the problem category and the expected goal of information system, and then propose the process of penetration test[5]. The preparation of permeability test is an effective guarantee for the whole process of permeability test. Penetration testing is a kind of policy testing, whose results are affected by factors such as business policy, business process, security requirements, system size and structure. In the preparation stage of penetration test, the purpose of penetration test, the scope of penetration test, the method of penetration test, the communication mechanism of penetration test, risk avoidance and emergency measures, formulation of operation plan and two-way contract should be clarified. The process of infiltration test should include preparation stage, information collection stage, infiltration attack stage, risk analysis stage, modification stage and report preparation stage.

The basic requirements of network information security penetration test are: prepare the test scheme, determine the network information security penetration test project information; collect the security information of the tested object, and provide important basis for the subsequent network information security penetration test work[6]. According to the information collected, the key tests are conducted in order to intercept the penetration attack. Further analysis of the vulnerabilities and hidden dangers found in the penetration attack, clear the potential risks of vulnerabilities and hidden dangers, and evaluate the risk level. Rectify the unacceptable risks found in the risk analysis, and complete the documents and reports. The collected data can be evaluated. Based on this, the network information security penetration cycle is further optimized.

The process of network information security penetration testing can be divided into active and passive. The corresponding vulnerability information can be obtained by the active and automatic detection of IP port service VPN or i-port network automatically detects the penetration vulnerabilities, such as general application layer vulnerability scanning, target enumeration and brute force cracking, application service version and vulnerability identification, etc., and carries out vulnerability detection through network vulnerability scanner.

2.2. Implementation of network information security penetration test

Penetration test of network information security can be basically divided into three stages: implementation goal; Detecting threat targets; As well as using broken targets or other targets to gain more benefits, each stage has different action targets, which is an active or passive measure to determine the network targets. The network information security penetration test process is divided into three main stages: information collection, scanning and counting to support the subsequent network information security penetration test. In order to ensure the accuracy of network information security penetration test, it is necessary to further standardize the risk level of network information security threat data. Based on this, a set of easy-to-understand and easy-to-use vulnerability risk assessment methods is proposed from three aspects: IP port service, database and application security. The four grades are A, B, C and D, and the detailed description is shown in the table 1.
Table 1. risk level of network information security penetration test

| Grade | Name         | Evaluation Criteria                                                                 | Example Description                                                                 |
|-------|--------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| A     | Emergency risk | The vulnerability can directly control the web server and implement large-scale attacks. | Some SQL injection vulnerabilities, some XSS vulnerabilities, file upload vulnerabilities, etc |
| B     | High-risk    | Vulnerability can cause security threats to sensitive data in database and normal operation of application business. | Some SQL injection vulnerabilities, some XSS vulnerabilities, CSRF vulnerabilities, etc |
| C     | Medium risk  | The vulnerability can reveal the information of web application and attack phishing and spoofing | Path traversal vulnerability, information disclosure vulnerability, partial reflection XSS vulnerability, etc |
| D     | Low-risk     | It will not pose a security threat to the server, database web application business, etc. | Application name and version and other basic information disclosure, some error information, etc |

In the above table, A-level vulnerability is an important risk. Once exploited by an attacker, it can directly control the IP port service. Its network information security penetration threat data is the most harmful. Level B vulnerability is mainly divided into emergency risk and must be repaired immediately. Level C vulnerability is a light risk, once exploited by the attacker, it will affect the sensitive data in the database and threaten the normal operation of IP port service application should be repaired as soon as possible. The vulnerability of D set is a slight risk, and the threat of D vulnerability to IP port service, database and business operation is very small. Attackers can use vulnerabilities at all levels to analyze the relevant threat information, carry out network attacks, directly pose security threats to IP port services, sensitive data in database, business operations, etc., obtain the most basic information, and position them as low risk. Through the research, it is found that there are some defects or open loopholes in IP port service, which can be used to attack network information. Therefore, in the process of network information security penetration test, it can be divided into three parts: initial threat, privilege upgrade and system maintenance under attack. When attacking the target network, the secret information of other systems can also be used or used as a springboard. The normal system will skip this step or jump to another operating system. Similar steps can simplify complex operations, penetration testers can penetrate into the target network through a series of methods. Of course, each step has its own multiple components, so the process of entering the target network is very difficult.
The penetration test of the first stage in the figure is the basis of the whole penetration test, and the penetration test results of the second stage can be used as the basis for subsequent work. In this stage, passive or active methods should be used to investigate and analyze the target network in detail, so as to determine and describe the target. This stage is mainly divided into three basic stages: data collection, collation and statistics. After successfully cracking the target system, it will not leave immediately, but will take some carefully designed measures to clear the attack trace and set up the back door. Attack test can simulate hacker attack behavior. After obtaining the corresponding permissions of the target network, the successful penetration test will not exit immediately. Again, it will act accordingly, known as the "post attack phase.". To verify the integrity of the target network owner information security measures and the effectiveness of emergency measures. Therefore, the accuracy of the penetration test of network information security by Youxia Ou Ting is analyzed.

3. Analysis of experimental results
In order to evaluate the performance of the test platform, we use the experience and technology of testers and the penetration test platform to conduct a comprehensive analysis, describe the characteristics of network information security penetration data, and optimize the basic steps of penetration test.

Based on the analysis of the above steps, when using the test platform for penetration attacks, set the IP address range, target network type, loading plug-in and other related parameters; through the network discovery function of the test platform, the network scanning, vulnerability scanning and other functions are used to collect the detailed information of the target network. By analyzing these information, we call the corresponding tools in the attack tool library to attack the target network. After obtaining the authority and sensitive information of the target network, the penetration trajectory is saved, the penetration attack is removed, and the preliminary detection report of penetration activity is completed. Based on this, the advantages and disadvantages of penetration test and conventional penetration test are compared, as shown in the following table 2:

| Table 2 difference between penetration test and conventional penetration test |
|---------------------------------------------------------------|
| This paper presents a penetration test                          | Routine penetration test                                      |
| Test objectives                                              | Test objectives                                              |
| Find the vulnerabilities and security risks of application    | Attack the target network system and obtain its control      |

Fig. 1 function optimization of network information security penetration test platform
service ports, and evaluate their harmfulness.

Test object
Application itself penetration testing
The whole network system includes host operating system, database system, application system and network equipment

Test basis
The application runs with exceptions, such as sensitive information exposure, unauthorized login, etc.
Whether the target network system can be broken.

Based on the analysis of the above table, it can be seen that the network information security penetration test effect based on IP port service technology proposed in this paper has more advantages than the traditional penetration test method. Further analyze the test results of the two methods and compare the test accuracy of the two methods. The results are shown in the figure 2.

![Comparison of two penetration test results](image)

Based on the above figure, the network information security penetration test method based on IP port service technology proposed in this paper has significantly higher accuracy in the actual application process. Based on the above detection results, it is easy to see that penetration testing is a security testing technology, and the application effect of this method in IP port service security testing is obviously better than that of traditional methods. However, from the test results, the network information security penetration test method based on IP port service technology still has a lot of empty test phenomena, and there are a few undetected penetration vulnerabilities. Therefore, the method still needs to be further improved. When setting sufficient access control and host security management at the network boundary, the network segmentation method should be adopted to strengthen the security protection of the user network. In order to better improve the test efficiency. As far as the current research standards are concerned, the network information security penetration test method based on IP port service technology has been retransmitted to meet the current research requirements.

4. Conclusion

The network information security penetration test method based on IP port service technology is to simulate the hacker's attack behavior and find the security vulnerabilities of the target system by combining the experience of the tester. The penetration network testing technology is basically similar to the hacker's attack means, which shows the process of scanning, guessing, attacking and gradually expanding. The biggest difference between penetration test and hacker attack is that penetration test is realized by choosing an attack mode that does not affect the normal operation of business system. By
infiltrating into the network as many ways as possible, it can show the vulnerability of the target network, help users understand the current system security status, understand the attack methods that attackers may use, and access to the network, so as to provide guidance for network reinforcement and information protection. Therefore, penetration testing is a very effective means to detect the degree of network security and information security protection.

Acknowledgment
This paper relies on SGCC science and technology project “Application of artificial intelligence technology in information security penetration test”, (Project No: 522437190014)’.

References
[1] Yuan C., Du J., Yue M., et al. (2020) The Design of Large Scale IP Address and Port Scanning Tool[J]. Sensors, 20(16):4423.
[2] Han J., Kim D. (2020) Security offloading network system for expanded security coverage in IPv6-based resource constrained data service networks[J]. Wireless Networks, 26(6):4615-4635.
[3] Nguyen H. V. (2019) An Easy In-Service Optical IP Network System for Residential Complex, Employing 1550 nm-Band CWDM and Layer-3 Switch[J]. Journal of Optical Communications, 40(4):423-428.
[4] Gao M., Chen M., Liu A., et al. (2020) Optimization of microservice composition based on artificial immune algorithm considering fuzziness and user preference[J]. IEEE Access, PP(99):1-1.
[5] Souza V. B., Masip-Bruin X., Marin-Tordera E., et al. (2018) Towards a proper service placement in combined Fog-to-Cloud (F2C) architectures[J]. Future Generation Computer Systems, 87(10):1-15.
[6] Qin X., Jiang Z. Z., Ip W. H., et al. (2018) Analyzing manufacturer and the insurance-based risk mitigation policy with equipment service contracting[J]. Enterprise Information Systems, 12(6-10):1359-1381.