Research on automatic mining and utilization of vulnerability in power web system

Jin He*, Boxiang Shang¹, Yan Li¹, Bo Yin²

¹State Grid Tianjin Information & Telecommunication Company, Tianjin, 300010, China
²State Grid Tianjin Electric Power Company, Tianjin, 300010, China
*448768576@qq.com

Abstract. With the promotion of the ubiquitous power IoT strategy, as well as the extensive application of advanced information communication technology and Internet + in the power grid, the power system has gradually broken the previous closure and exclusivity. The construction and deployment of open, interactive, extensive and interconnected power web business system are becoming more and more widespread. The inherent vulnerability and hidden danger of power web system make power face the risk transfer from network and information security to power system. Aiming at the potential security problems of vulnerability in the massive power web system, an in-depth study is made on the automatic mining and utilization technology of the vulnerability in the power web system. By carrying out researches on the framework design of automatic mining and utilization of vulnerabilities in power web system and the intelligent new mode of exploiting vulnerabilities in power web system, the overall design is made for the mechanism and model of automatic mining of asset vulnerabilities in power information system.

1. Information security risk of intelligent terminal information of power system

In 2019, China's power grid company proposed the construction requirements of world-class energy internet enterprises "three types and two networks", and deployed the task of accelerating the construction of ubiquitous power IoT. On this basis, the Internet department of the company has defined the construction of the ubiquitous power IoT content in six aspects including security protection, so as to support the safe development of the capacity of the ubiquitous power IoT in four aspects including the perception, connection, sharing and innovation, and support the goal of the world-class construction of type iii and type ii networks. With the promotion of the ubiquitous power IoT strategy, as well as the extensive application of advanced information communication technology and Internet + in the power grid, the power system has gradually broken the previous closure and exclusivity. The construction and deployment of open, interactive, extensive and interconnected power web business system is becoming more and more widespread. The vulnerability and hidden danger of power information system is utilized and the risk of network attack is increased, which makes the company face a severe network security situation.

According to statistics, at present, the company has a total of about 2,700 sets of power web information system such as electric vehicle operation management system and new energy access control system, and more than 540 million sets of smart meters that are connected with monitor and management, such as intelligent electricity meters. The daily increment of data collection exceeds 60TB level. It is estimated that in 2025, more than 1 billion monitoring and management terminals will be
installed, and risk points such as external services and interactive sharing will be expanded continuously. With the increasingly severe security situation at home and abroad, the power grid has become one of the main attack targets of cyber war. Since the power grid network and information security incidents occur frequently, it is of great significance to carry out efficient and accurate mining and verification of hidden dangers in the power information system.

For this reason, this paper designs a framework for automatic mining and utilization of vulnerabilities\(^1\), which includes four parts: basic vulnerability mining, asset identification and vulnerability scanning, penetration attack and vulnerability verification, and vulnerability mining experience training\(^2\). Two modes of intelligent technology are designed and adopted to realize the intelligent use and verification of vulnerabilities. One is the intelligent utilization and verification mode of vulnerability on the basis of target drone, and the other is the intelligent utilization and verification mode of vulnerability on the basis of the artificial experience tree. The two methods are combined and utilized to realize intelligent, accurate and lossless vulnerability verification.

2. Framework design of automated mining and utilization of business
Taking the automatic mining and identification of vulnerabilities in the web information system of various business link of electric power as the purpose and artificial intelligence as the technical support, the whole business process is divided into six stages, including experience sample, asset identification, vulnerability detection, experience training, vulnerability verification and vulnerability warning. Automatic and efficient identification of web asset environment, automation mining of web system vulnerability, intelligent verification of web system vulnerability and other core technologies are mainly studied to realize automated mining analysis of web system middleware vulnerability, file system vulnerability, database vulnerability and other types of vulnerability. The specific stages are described as follows:

1. Experience sample: vulnerability database, vulnerability utilization sample database, attack experience tree and other basic resources are built through collection and independent construction;
2. Asset identification: basic information, system information, application information and version information of the target system are obtain as far as possible by means of active scanning and open search\(^3\);
3. Vulnerability detection: vulnerability scanning and other means are used to detect the vulnerability in the target system;
4. Experience training: The information collected in the previous steps is performed unified arrangement and utilization to build a penetration attack model, and penetration test training is conducted in integration with the target machine or range to obtain a more accurate and usable penetration attack experience tree;
5. Vulnerability verification: the vulnerability is exploited and verified according to the attack model scheme formed in the experience tree;
6. Form penetration test report: the penetration test report is generated according to the information of the previous stage, including vulnerability information, vulnerability causes, vulnerability repair recommendations and other information.

3. Research framework design of automatic mining and utilization technology
According to the above ideas, the paper designs a framework for automatic mining and utilization of vulnerabilities in the power web system, which includes four parts and adopts the modular concept as far as possible. The details are as Fig.1:
Basic vulnerability mining technology: the design of this part mainly includes basic vulnerability mining technology, tools or modules such as web crawler, brute force cracking, plug-in control, decode technology, multidimensional interface, etc. These modules can be combined to support asset identification, vulnerability scanning, penetration attack and other services through standardized interfaces. These modules can be combined to support asset identification, vulnerability scanning, penetration attack and other services through standardized interfaces. The link of asset scanning and identification provides modules including scanning and checking points for various network services, constructing login passwords of fake services collection, and password guesses. In addition, the auxiliary module also includes some attack payloads that do not need to be loaded. At the same time, it is often not the infiltration attacks that obtain remote control right of target system. Plug-in control can integrate some existing external security tools, such as Nessus and Open VAS vulnerability scanner, so as to provide some new functions for the user interface. In addition, this section also designs msfconsole control terminal, msfcli command line, msfgui graphical interface, armitage graphical interface, and msfapi remote call interface.

Part of asset identification and vulnerability scanning: aiming at the problems current of traditional vulnerability scanning system such as large interference to information network, low scanning efficiency and poor accuracy of vulnerability scanning currency, the technology improvement research is carried out from the aspects of asset scanning identification and vulnerability scanning. Firstly, in the aspect of asset scanning and identification, it mainly includes the host ports stateless scanning, target address random scanning, power Web system fingerprint scanning and other parts, which realizes the efficient power information system asset scanning and identification with small interference. In terms of vulnerability identification, this framework adopts vulnerability multi-mode identification technology, mainly including host port fingerprint matching, host port black and white list matching, power web system fingerprint matching and other parts.

Penetration attack and vulnerability verification: based on the traditional vulnerability scanning system, this part introduces two new technologies: automatic vulnerability penetration test and vulnerability penetration intelligent decision. Automatic vulnerability penetration test mainly includes the sample library of vulnerability utilization, vulnerability utilization technology, attack status monitoring, attack resource scheduling, which realizes the automatic verification of vulnerability based on EXP and PAYLOAD. However, simply using existing EXP to exploit vulnerabilities is essentially a way of violent penetration. On the one hand, the efficiency is low; on the other hand, the harm is difficult to be controlled. Therefore, this framework designs research on intelligent decision-making technology...
of vulnerability penetration. Through the way of building experience tree by training target drone and the way of building experience tree by the red team, the standard establishment of vulnerability is carried out using EXP to select the optimal attack sequence and attack load.

Vulnerability mining experience training part: the support is provided for the construction of vulnerability penetration experience tree. The design and establishment of framework is for target drone environment of power web service system, and integrated with power range system. On this basis, machine learning algorithms such as A3C and Bayes are introduced to make the training penetration test of target machine environment. The infiltration experience trees for different system fingerprint environments are formed through the training process.

4. Intelligent new pattern design Power web system vulnerability verification and utilization
Two kinds of intelligent technologies are adopted in this paper to realize the intelligent development of utilization and verification of power system vulnerability. One is the intelligent utilization and verification mode of vulnerability on the basis of target drone, and the other is the intelligent utilization and verification mode of vulnerability on the basis of artificial experience tree. The two methods are combined and utilized to realize intelligent, accurate and lossless vulnerability verification. The specific model is as Fig.2:
Fig. 2. The intelligent new mode of utilization and verification of power web system vulnerability

(1) Input penetration test target;

(2) Start host port scan, port service scan, web system fingerprint scan, etc., conduct information collection, and generate fingerprint data of target object.
3. Match and compare according to the fingerprint information and the vulnerability fingerprint information base to preliminarily identify the vulnerability information of the target system;
4. Analyze and organize vulnerability exploitation scripts such as EXP and Payload according to vulnerability information;
5. Submit the generated vulnerability exploitation script to the target machine platform;
6. Start the intelligent exploitation verification of vulnerability on the basis of target drone;
7. Generate target drone environment according to the decision-making, and generate the combination and utilization sequence of EXP and Payload;
8. Conduct target drone training;
9. Store EXP and Payload that are successful in training to generate accurate and usable EXP trees and Payload trees;
10. Record EXP and Payload that are unsuccessful in training, and enable the intelligent utilization and verification of vulnerabilities based on the artificial experience tree, recombined EXP and Payload that are unsuccessful in training according to the artificial experience tree, and intervene and redesign the relevant experience tree by red team;
11. Generate complete and accurate available EXP trees and Payload trees;
12. Submit and perform penetration test.

With various deep learning technologies\[8\], the intelligent utilization and verification mode of vulnerability based on the target drone comprehensively analyzes fingerprint information, EXP script and payload script, and adjusts the environment of the target drone to simulate the environment of the target host as much as possible. The utilization sequence and utilization results of EXP script are analyzed. At the same time, the decision-making generates corresponding Payload call relationship. Finally, the infiltration test training is carried out in the simulated target drone environment. The adoption of this mode will greatly reduce the risk of damage to production system caused by penetration test, and also reduce the impact of blasting attack on network and business.

In addition, the intelligent utilization and verification mode of vulnerability based on artificial experience tree is mainly based on expert system to realize the construction of penetration test experience tree.

5. Conclusions
Aiming at the problems of automatic utilization and accurate verification of potential vulnerabilities, the paper innovatively integrates asset analysis and vulnerability classification, and analyzes the key protection directions of information security of different information assets. In addition, the classified study is carried out for vulnerability from the aspects of attack life cycle, threat type and asset type of power information network Web system, respectively, and the utilization of this kind of vulnerability is evaluated to make targeted utilization and attempts for vulnerabilities in important business links. The integration makes the process of vulnerability utilization in Web system more macroscopic and comprehensive, and forms a framework of vulnerability utilization.

ACKNOWLEDGMENTS
This work was supported by the science and technology project of State Grid Tianjin Electric Power Company: "Research on power information system vulnerability mining and monitoring analysis technology based on machine learning"

References
[1] Guo Qiang. Application research on automatic mining and detection technology for security vulnerabilities in wind field industrial control system [J]. Applied energy technology,2019(04):47-49.
[2] Hou Feng, Zhao Qian. Research on the mining technology of input verification vulnerability on the basis of implicit mode [J]. Journal of sanmenxia vocational and technical college,2018,17(03):121-126.
[3] Ye Mengxiong. Design and research of SQL injection vulnerability scanning system on the basis of Web [J]. Electronic design engineering, 2019, 27(16):20-23+28.

[4] Dong Zhengming, Cao Shihua. Development and design of campus network alarm system on the basis of security vulnerability scanning [J]. Electronic design engineering, 2017, 25(20):109-111+115.

[5] He yijun. Research on penetration test on the basis of Kali Linux [D]. Central south university of forestry and technology, 2019.

[6] Li Xiaodong. Research on the security and protection of computer network information in the era of artificial intelligence [J]. Southern agricultural machinery, 2019, 50(16):186.

[7] Cheng Shaoliang. Design of network security vulnerability scanning system on the basis of deep learning in 2.0 era [J]. Information and computer (theoretical edition), 2019(13):86-87.

[8] Li Yuancheng, Huang Rong, Lai fenggang, Mao Yifan, Cai Lijun. Open source software vulnerabilities detection method based on the depth of the clustering [J/OL]. Computer application research: 1-6[2019-10-25], https://doi.org/10.19734/j.issn.1001-3695.2018.09.0721.