Research and Application of Information Security Offense and Defense Exercise in Electric Power Industry

Mingxuan Li[1], Zhushi Yang[2],Ling He[1], YangXin Teng[1]

1.Information and Communication Technology Center, State Grid Xinjiang Electric Power Research Institute, Urumqi, China
2.State Grid Xinjiang Electric Power Limited Company, Urumqi, China
xuanxuan218@126. Com

***Abstract*—The smart grid is a new type of grid integrating traditional grid and information technology. With the rapid development of information technology, information security as a requisite part of information technology is profoundly affecting people's work and life. While the development of science and technology brings convenience to characters, it also exposes many security issues. In particular, in recent years, information security incidents such as information leakage, SQL injection vulnerabilities, network penetration, and hacking attacks have triggered irreparable losses to enterprises, society, and individuals. The power industry as an energy supply involves the majority of the information, business value, and state secrets of state-owned assets. Nevertheless, the huge information data has huge value, which makes the possibility that the grid enterprise information network is vulnerable to hackers and the risk of information leakage is overwhelmingly large. According to the characteristics of the power industry, this paper discusses the significance and value of network offensive and defensive drills in the power industry, and proposes a network offensive and defensive shooting range construction and implementation scheme for the characteristics of the information disclosure loopholes in the power industry. The purpose of this article is to improve the information security awareness of personnel engaged in information security work in power grid companies and to respond to emergency information security incidents, and indirectly ensure safe, stable, and reliable operation of the power grid..**

Keywords—Information security; Network attack and defense; Smart grid; Security vulnerabilities; Electrical industry

I. INTRODUCTION

As is well known, the Internet era promotes the rapid development of information technology, followed by a variety of network attacks and forms of different network viruses. The “Wannacry” virus that broke out in May 2017 is a good example and lesson. Electricity is an important energy support for the country’s “energy saving and emission reduction” and green development. And the stable supply of electricity can maintain social stability and development. It can be seen the rapid development of smart grid depends on the support of information technology. Without the support of information technology, smart grid is just an empty talk. Nevertheless, with the rapid development of smart grids, the safety issues of the information technology relied on are gradually exposed. Once there is severe information security case, the consequences will be unthinkable. The network information network has a feature that the grid has high real-time and reliability to information, so it is bound to require centralized management of information. The information security of the power grid will directly or indirectly affect the safety of the entire power grid system, which one can imagine that if the control information goes wrong, the "donomi domino effect" is overwhelmingly likely to happen. Finally, it may eventually affect the entire power system and cause irreparable damage. There may be information security threats in power generation, transmission, transformation, distribution and electricity use, once it breaks out, the consequences are also unimaginable. As a national energy strategy enterprise, power grid enterprises have made the informationization of the power industry higher in recent years , so it is necessary to ensure the information security of smart grids. Facing the threat of malicious network attacks, in order to ensure the security of cyberspace information and prevent the explosion of major information security threats, the information security technicians in the power industry must build or entrust a network attack and defense range (drill platform) to carry out an attacking and defensive drill. In view of various common information security vulnerabilities and hacker attacks to carry out rehearsal, it is necessary to improve the security level of the information system and improve the ability of anti hacker attack..

With the development of the grid company information system and the rapid growth of the number of systems in recent years, various security risks for information systems are also increasing. In order to ensure the safe and stable operation of the power grid information system, managers and maintainers are required to keep pace with the times and grasp the potential safety hazards, relevant safety knowledge as well as necessary skills of a great variety of information systems in the power grid. It is a must for us to get familiar with the methods and principles of all kinds of vulnerabilities in grid information system, only in this way we can do our own system security protection. Therefore, through the research and application of the actual core system of the network attack and defense range, we will enhance the ability to analyze and attack the new loopholes in the power grid.

II. Information Security Loopholes and Potential Risks in the Electric Power Industry

In December 23, 2015, Ukraine power grid was suffered a sudden blackout, which triggered about 700,000 households in western Ukraine to have power outages for several hours. After the event, the researcher at iSight Partners of Dallas information security company, he said that this is a devastating incident given rise to by the BlackEnergy malware code. December 17, 2016, there was a downtime at the 330kV Substation in Northern Kiev, Ukraine, which contributed to widespread power outages in Kiev. At the CyberTech 2016 conference, Israel's Minister of Energy and Hydraulic Infrastructure disclosed that the Israeli Power Authority was suffered a serious cyber attack on January 25, 2016. After the incident, Israeli authorities were forced to shut down the infected computers in the power facilities. In 2016, there were two of the top 10 internet security incidents in the world that had a direct relationship with the power grid. This depict that in the power grid, the importance of information security is irreplaceable.

Information security is both an ancient and modern vocabulary. It’s said to be ancient is that the previous flight of pigeons and mail letters have already been. The reason why it is modernized is that it has been continuously updated with the advent of wire technology and computer technology in the 1990s, which will usher in a new era of development. Information security should ensure the security performance of software, hardware, and data resources in the information network, at the same time it can continuously and reliably provide you with services for users without interrupting services due to attacks. And the major goals of information security include: authenticity, confidentiality, integrity, availability, controllability, auditability, and non-repudiation. At present, China’s cyberspace information security situation is grave.

The application of various new technologies, such as big data and cloud computing, intelligent information processing, artificial intelligence, Internet of Things, and mobile Internet, making the smart grid face various attacks such as viruses, Trojans, system vulnerabilities, and DDoS. Traditional network protection systems based on physical protection have brought challenges. The following will introduce and analyze possible information security loopholes in the power industry.

A. Information Leakage

Information leakage is a severe topic. Due to various public services, state-owned enterprises and public institutions often require users to submit various information and the grid as an energy supply operator is certainly no exception. At the same time, there are many secret informations within the power grid company that needs to be secured. Information leakage is due to improper settings of the Web server's permissions, non-standard operations, improper handling of some special user requests and services can result in sensitive information such as user names, secrets, background source code, server configuration information, and other file paths. Leaked information is vulnerable to use by malicious individuals and provides stepping stones for subsequent attacks. In enterprise-level Web applications, information leakage includes: disclosure of database information, disclosure of website configuration information, leakage of website directory structure information, etc.

B. Cross-site Scripting Vulnerability

XSS Cross-Site Scripting (XSS) has been undergoing more than ten years of evolution since it was born in 1996. As with the acronym for Cascading Style Sheets (CSS), the original CSS is simply referred to as XSS to prevent confusion. In various web application security vulnerabilities, XSS Cross-Site Scripting Vulnerability has been rated as one of the Top Ten Application Security by OWASP (Open Web Application Security Project).

Unsolicited molecules will use cross-site scripting to inject malicious code into the web pages. This is due to insufficient filtering of user input by WEB applications. When users browse these web pages, they will execute malicious code. For the reason that HTML code and client-side JavaScript scripts can be executed on other people's browsers, illegally obtaining user-sensitive information otherwise controlling the logic of the Web client. On this basis, hackers can easily initiate various kinds of attacks such as cookie theft, session hijacking, and fishing fraud. Under normal circumstances, we can either understand XSS as a WEB application security vulnerability or else understand it as an attack.

C. SQL injection vulnerability

SQL is a database query and operation language, it is to insert or add SQL code to the input parameter, and then submit to the server. If the server does not detect and filter the SQL statement, it will resolve and execute the malicious intent of your attacker. For example, the login system of a website needs to enter a username and password, submitting username admin and password SdfG#345! to background SQL execution, fnally it will execute Select * from table where user = ‘admin’ and Pwd= ‘SdfG#345!’. Nevertheless, provided that the user inputs 123’ or ‘1=1 in the password, the background runs Select * from table where user= ‘admin’ and pwd= ‘123’ or ‘1=1’. The condition where the statement is always true, you can log in successfully, other users can also use this password to successfully log in. Provided that the administrator does not check the parameters of the SQL statement, an attacker can use the corresponding language logic loopholes to override the illegal operation.

D. Arbitrary Files Contain Bugs

Since developers write source code to write reusable code into a single file and include them in special function code files when needed, which the code in this include file will be interpreted and executed. If you do not filter the function entry contained in the file that exists in the code, it will give rise to the client to submit a malicious construct statement and send it to the server for interpretation. The file contains an attack that may exist in the WEB server's source include() –this file contains the operation function, and the file path is constructed by the client. This is the most important trigger for the successful attack.

E. Directory Traversal Vulnerability

Usually webpage URL address is added by http:// domain name and path, the attacker can append "../" to a meaningful directory in the URL or add some other special characters to get other directorie as well as fulfill the directory jump and get sensitive files for each directory, thus we can get sensitive files for each directory. As a result, attackers can access directories and files outside of authorization and even execute commands, which can be extremely harmful.

F. Arbitrary File Upload Attack

File upload attack means allowing users to upload arbitrary files so that cyber attackers can upload dangerous content or malicious code to the server and execute. The technical threshold of arbitrary file upload vulnerability is low and easy to implement. For example, a PHP source code site does not strictly limit the uploaded file's suffix name and actual file type. This allows an attacker to upload a PHP file and pass it to the PHP interpreter for execution. It is then possible to remotely execute arbitrary PHP scripts and perform illegal intrusions.

III. INFORMATION SECURITY OFFENSIVE DRILL PRACTICE

With the development of power information systems and the complexity of various businesses, various security risks in the power industry information system are also increasing. In order to ensure the safe and stable operation of the power grid information system, management and maintenance personnel are required to keep abreast of the times to grasp the potential safety hazards and related safety knowledge as well as necessary skills of all types of information systems in the power grid. Nevertheless, due to developers are lack of safety awareness, there are still many security risks and loopholes in the online information system of power grid companies. Once a malicious attack spreads, it will contribute to huge losses to the power industry. Therefore, it is necessary for information security technicians to master the methods and principles of various types of loopholes in the grid information system to be attacked. We need to do well the security protection of their own systems and improve the awareness of information security as well as emergency response to sudden network attacks. Finally, through the research and application of the actual core system of the network offensive and defensive shooting range, the analysis of the new network loopholes and the ability of offensive and defensive drills are enhanced to meet the needs of the development of enterprise information.

A. Platform Environment for Information Security Attack and Defense Exercises

The overall structure of the network offensive and defensive shooting range is shown in Fig.1, it combines the characteristics of the power grid industry with common vulnerabilities in enterprise Web systems, using highly simulated network offensive and defensive shooting ranges for information security offensive and defensive drills.

Research is based on cloud platform, and it supports remote access and operation of the network offensive shooting range platform, which provides dynamic and customizable training topics as well as network attack and defense tool library. In this way to guarantee the real-time and expansibility of the network shooting range, but most of all, it can flexibly cope with various network security risks under the new situation, reproducing the actual security problems in the power industrys. In order to improve the information security skills of information security management personnel and operation and maintenance staff, we imulate the attack and defense of actual security vulnerabilities.

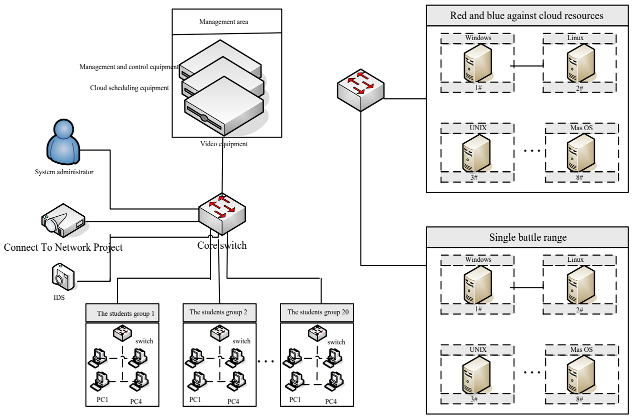


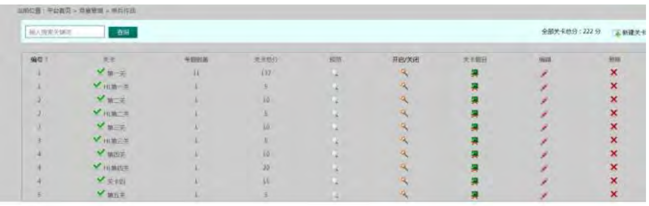
Fig. 1. Overall architecture of network attack and defense range system

B. Implementation of Information Security Offensive and Defensive Exercises

In the course of offensive and defensive drills, the implementation process can be divided into two stages: individual combat mode and red and blue confrontation.

(1)Individual Combat

In the problem-solving mode CTF competition, participating teams can participate through the Internet or on-site network. This model of CTF competition is similar to ACM programming competition and information science Orsay, and it addresses the trouble of network information security attack and defense. These topics may involve all aspects of information security technology, such as cryptography, digital signature technology, identity authentication technology, vulnerability infiltration technology, script programming, and cyberspace security laws as well as other relevant legal provisions. The main purpose is to examine the basic knowledge of the network information security technicians and the practical operation of common vulnerabilities. Give priority to the most basic principles of hacker exploits and use common security attacks such as BurpSuit, AWVS, and NMap. At the same time, it is necessary to repair and reinforce loopholes and security risks in the course of the offensive and defensive drills. The individual soldier battle interface is shown in Fig.2.



[illegible]

[illegible] 查询 全部关卡总分：222 分 新建关卡

编号	关卡	[illegible]	关卡总分	[illegible]	开启/关闭	[illegible]	[illegible]	[illegible]
1	✓ 第一关	11	137					✕
1	✓ HL第一关	1	5					✕
2	✓ 第二关	1	10					✕
2	✓ HL第二关	1	5					✕
3	✓ 第三关	1	10					✕
3	✓ HL第三关	1	5					✕
4	✓ 第四关	1	10					✕
4	✓ HL第四关	1	20					✕
4	✓ 关卡[illegible]	1	15					✕
5	✓ 第五关	1	5					✕

Fig.2 Individual problem-solving model

(2)Reds Fight Blues

In accordance with the reality of the security loopholes in the power grid, the information security equipment and its software, network equipment, information assets, etc. will be replicated in simulated honeypot technology. We will set up a typical network attack and defense simulation platform that simulates actual information networks and provide red against offensive and defensive drills, which Red Party launches cyber attack against Blue Party, mining network service vulnerabilities and attacking opponent services to score. The blue side repairs its own service vulnerabilities to reinforce the system defense attack and avoid losing points. After a round, the red and blue sides exchanged roles to carry out offensive and defensive countermeasures. As can be seen, the red and blue confrontation can reflect the progress of the game in real time and the competition is more than fierce. In the red-and-blue confrontation, not only the personal technical ability is examined, but the division of labor and cooperation between team members is also intensely important. Fig.3 shows the results of a team offense and defense drill.

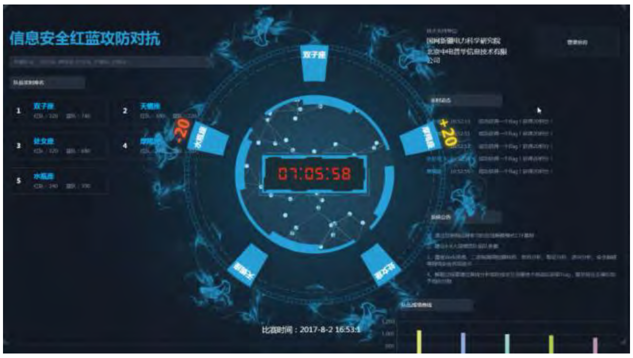


Fig.3. Actual combat scores in attack and defense range

IV. CONCLUSIONS

Smart grid is a new type of integration of traditional grid and information technology network. With the rapid development of information technology, information security as a requisite part of information technology is profoundly affecting citizen's work and life. The development of science and technology brings convenience to individuals while exposing an army of security dilemmas. Especially in recent years, information security incidents such as information leakage, SQL injection vulnerabilities, network penetration and hacking attacks have given rise to irreparable losses to the Internet community. Faced with the development of network technology and the complexity of cyberspace, the power industry as an energy supply involves the majority of the information, commercial value, and state secrets of state-owned assets. Nevertheless, the huge information data has huge value, making it overwhelmingly easy for the grid enterprise information network to be vulnerable to hack and trigger information leakage risks. Over the years, the phenomenon of attacks on smart grid information systems and user data has frequently occurred, which has brought about extraordinary effects on the safe operation of the power grid and the reliability of power supply. In accordance with the characteristics of the power industry, this paper discusses the significance and value of offensive and defensive drills in the power industry, which is by analyzing the common security risks and vulnerabilities in the grid information system, and addressing the characteristics of the vulnerability of the information disclosure network in the power industry, the construction and implementation plan of the network offensive and defensive shooting range and the ability to handle emergent information security incidents are proposed to protect the grid enterprise information system, which ensure the safety of power grid enterprise information systems.

REFERENCES

[1] Zhu Y, Yan J, Tang Y, et al. Joint Substation-Transmission Line Vulnerability Assessment Against the Smart Grid[J]. IEEE Transactions on Information Forensics $Security, 2017 10(5):1010-1024.

[2] Huang Jianming, Zhang Hengwei. Improving Replicator Dynamic Evolutionary Game Model for Selecting Optimal Defense Strategies[J]. Journal on Communications.January 2018 Vol.39 No.1.

[3] BURKOVSKY R N, DORASIELSKI U, KRYUKOV Y. A user’s guide to solving dynamic stochastic games using the homotopy method[J]. Operation Research, 2015,58(4):1116-1132.

[4] SHEN S G, HUANG L J, FAN E, et al. Trust dynamics in WSN: an evolutionary game-theoretic approach[J]. Journal of Sensors, 2016,32(4):34-43.

[5] Ling A P A,Masao M.Smart Grid Information Security(IS) Functional[J]. International Journal of Emerging Sciences,2011,1(3)