Application of New Active Defense Technology in Power Information Network Security

Jing Li1*, Jie Huang1, Li Tian2, Jie Wang2
1State Grid Hubei Electric Power Co., Ltd, Hubei Wuhan, China, 430077
2Electric Power Research Institute of State Grid Hubei Electric Power Co., Ltd, Hubei Wuhan, China, 430070

*Corresponding author e-mail: gmq1988@126.com

Abstract. With the rapid development of the Internet and the expansion of the network scale, while the network brings unlimited convenience to people, the problem of network security has become increasingly prominent. Network security has become one of the main factors hindering the development of the Internet. In the operation of power network systems, in order to ensure network security, many security technologies are also being continuously applied. In the traditional network security defense technology, passive defense technology is used, all its defense measures are static and all rely on network administrators to implement equipment and manual configuration. In the new network era, the illegal attacks on power network information systems have become more and more frequent, at the same time, hackers’ offensive methods will also be updated and become more sophisticated. Therefore, traditional network security defense technologies have been unable to resist or even cannot withstand. Based on this, this paper focuses on new active defense technologies, analyzes its application in power information network security, and proposes defense of power information network security based on attack detection using honeypot technology suggestions.

Keywords: Active Defense Technology, Power Information, Network Security, Honeypot Technology

1. Introduction

With the widespread construction of wind power stations and solar power stations, more and more power grids need to be connected to the grid, and in the process, smart grids have to be developed [1]. Compared with the traditional grid, the smart grid is a new type of grid that is highly integrated with power flow, information flow and business flow. At the same time, the smart grid can maximize the
reasonable integration of information, sensors, automatic control technology and grid infrastructure, can quickly isolate faults, achieve self-recovery, and avoid large-scale power outages [2-3]. However, due to the intervention of some computer equipment and microcomputer equipment, if this virus invades the national grid, can we deal with it? With the continuous deepening of Internet applications, the security of many computers themselves and the network security are facing unprecedented tests, network defense technology has become increasingly stretched, especially in the new era of automated, large-scale network attack behaviors, therefore, passive defense technology, active defense technology, honeypot technology, are widely used in modern network defense technology [4-5].

During the operation of the power information system, although the overall system has been greatly developed, there are still security issues to be resolved. Specifically, it is mainly manifested in the following two aspects. On the one hand, some system vulnerabilities still exist. Because part of the enterprise's network system is connected to the external network, during the system operation, the overall system is set up with a defense system, which has been in a passive defense state for a long time, there are some shortcomings, which makes many system vulnerabilities invade the system and cause network system failures [6-7]. In fact, although passive defense technology can play a role in ensuring the security of the system, the active defense system has greater flexibility, so it is necessary to apply the system to improve the security of the system [8]. On the other hand, in terms of technical practice, the effects of many technical operations still need to be improved. Because many systems still use traditional system protection technology, the perception of security issues during operation is not sensitive enough, and system problems cannot be achieved at the same time, handle in a timely manner, the application of active defense new technologies is conducive to the efficient development and progress of power information systems [9-10].

In order to avoid the shortcomings of passive defense technology, this article studies the principle and technology of new active defense technology, and uses the characteristics of honeypot technology to introduce honeypot technology into the intrusion detection system to build an active security protection system, which can effectively to make up for the lack of traditional intrusion detection [11-12]. In this paper, based on the new dynamic defense technology, the advantage of honeypot technology in capturing unknown attacks is used to make up for the lack of traditional intrusion detection systems in detecting unknown attacks.

2. Method

2.1 New Technologies for Active Defense

(1) The concept of active defense new technologies

Active defense technology, as its name implies, 'active' requires the use of artificial means or high-tech to actively prevent potential security risks and malicious attacks in the power information network. A more academic statement is that if we want to enhance the security performance of the local network, we must also ensure that the internal network is not protected from illegal intrusions. When an illegal attack occurs, there is a strong system that can detect and detect the illegal attack that is being experienced, predict and Efficiently identify unknown attacks. At the same time, the most important thing is to take reasonable and effective measures to prevent attackers from achieving their goals.
Active defense, as an effective modern network defense technology, integrates traditional network defense technology and cutting-edge instruments that have emerged in recent years, allowing all technologies to be organically combined and coordinated to ensure network security and power systems information security. The core of all technologies is built on the existing foundation, and the active defense technology is also built on the traditional network defense technology. Its soul is still the traditional network defense technology, but it only adds some new technical means.

(2) New technologies for active defense

Intrusion response technology in power information network security when the power information network is invaded and the monitoring system installed in the power system can detect it, then we must vigorously counteract and respond to the intrusion and use it to detect the intrusion event. At the same time, the processing results are fed back to the system, and the defense capability is continuously improved. In the active defense system, intrusion response technology plays a role in coordination of multiple technologies. It shows initiative in network defense, which is the essential difference from traditional network defense technology. The active defense new technology system mainly includes intrusion prevention technology, intrusion detection technology, intrusion prediction technology and intrusion response technology. The main intrusion response technologies are as follows: 1) intrusion tracking technology; 2) attack absorption and transfer technology; 3) honeypot technology; 4) forensics technology; 5) active counterattack technology.

2.2 Honeypot Technology

(1) Honeypot technology

Honeypot is a computing resource that is strictly monitored. Honeypot technology is an active network security protection technology. By designing a deceptive environment, it tricks attackers into attacking it, and it expects to be detected, attacked, or captured. As a phishing tool, honeypot itself has no production value, any visit to the honeypot is considered suspicious. Its value can be measured by the information it captures, and valuable data can be obtained by analyzing various types of captured information.

(2) Principle of honeypot technology

As a decoy system, the basic principle of a honeypot can be briefly described as laying out security traps, deceiving attacks, and recording the process of attacks. The honeypot system collects more attack information by forging attackers by forging system vulnerabilities and laying out security traps. The honeypot system does not provide external services and has no available resources, so any attempt to connect to the honeypot is considered suspicious yes, honeypot systems are usually deployed in vulnerable networks. The honeypot system is basically camouflaged with the real host, which is difficult to find after an intruder successfully invades. The honeypot tracks and records the behavior of the intruder. The honeypot's log system records all operations on the honeypot and the attack information. Afterwards, all the collected data is analyzed and analyzed to determine whether an intrusion has occurred, and relevant attack behavior characteristics are extracted from it.

3. Experiment
3.1 Experimental Environment

(1) Experimental platform hardware environment

Attack simulator configuration: Intel Core i7 CPU, 500G hard drive, 4G memory; Honeypot host configuration: Intel Core i7 CPU, 500G hard drive, 4G memory; Honeypot client configuration: Use virtual mechanism Built, each honeypot is configured with 512M memory and 40G hard disk.

(2) Experimental platform software environment

Honeypot host: Windows7 operating system, VMWare virtual machine, MySQL database; Honeypot client: Windows7 operating system, Linux operating system, Honeypot simulation software Honeyd; Hole scanning tool: X-scan3.3; DoS attack simulation software: FakePing.

3.2 Experimental Steps

Step1: Data collection. Collect data for intrusion detection, which usually includes system data, host work logs, and network data packets. The system collects and analyzes these data.

Step2: Data processing. In order to improve the detection efficiency, the complicated original data collected from the network is processed, the data is filtered according to the preset rules, redundant and noisy data are eliminated, and the data is required to be standardized.

Step3: Data analysis. All activities in the network are monitored according to a well-defined security policy, data is collected, and processing analysis is performed to determine whether there are attacks or intrusions.

Step4: Response processing. The response processing module responds to the results obtained after the data analysis by the system. If an intrusion behavior is found, the corresponding response strategy is taken and the administrator is notified, or the intrusion behavior is processed according to the pre-agreed rules.
4. Discussion

4.1 Experimental Results and Analysis

In order to verify the feasibility of honeypot technology in power information network security, in the above experimental environment, simulate normal network connections, scan and detect attacks, and DoS attacks, respectively, and record the number of data records captured in various situations. Use KNN to identify and classify the data captured by the system's data capture unit. The detection results of normal records, DoS attacks, and port-scan attacks are shown in Table 1 and Figure 1:

|       | Normal | DoS  | Port-scan |
|-------|--------|------|-----------|
| correct | 2568   | 10620| 4118      |
| error  | 258    | 718  | 700       |
| accuracy | 90%    | 93.5%| 85%       |

![Figure 1. Detection effect](image)

4.2 Recommendations for Power Information Network Security

(1) Establishment of a dynamic security defense system

By using a combination of active defense technology and passive defense technology to implement a dynamic security defense system for electronic information networks, electronic information networks can be made more secure. The network firewall in the passive passive defense technology establishes the front line of the defense system, and combines the trap technology in the active defense technology to form network protection and prevent illegal access from the outside. And through the creation of system vulnerabilities in trap technology, it simulates the attacked network environment, allowing the attacker to change the attack direction of the system, and plays another layer of network security defense. In the establishment of the dynamic security defense system of the power information network, detection
and response also occupy a major position, and it can also be established using active defense technology. Trap technology can be designed through trap technology, combined with forensics technology to detect loopholes and attacks in the power information network, and retain evidence of intrusion. Especially in the response stage, forensic technology can be used to record and save network logs, analyze new viruses and attack methods, and generate new databases.

(2) Offensive and defensive drill of power information network security

With the continuous development of network technology, the power information network security will achieve further innovation. Correspondingly, the power information network security breach technology will also be improved. In this background, if the power information network security defense system is not simulated and practically drilled, it will cause its work to have a certain deviation when facing a real attack. Using active defense technology, the offensive and defensive drill of power information network security can realize the simulation and defense of real network attack environment, and propose better solutions to new network vulnerabilities and attack forms. The offensive and defensive drill of power information network security is of great significance for the development of the times. In traditional power information network security, there is no real simulation and drill for attacks, and the experience of security systems in actual defense is insufficient. Using the dynamic forensics technology in the active defense technology, the attack methods are analyzed and resolved during the offensive and defensive drills, and recorded in the database of the security system, making the "practical" experience of the power information network security guarantee system more sufficient. The work can better protect the security of the power information network.

5. Conclusion

Power system security is related to thousands of households. In recent years, the smart grid has been vigorously developed. The integration of some new generation power stations and the application of computer intelligent technology have brought convenience to the power supply system and increased hidden dangers. How to ensure the security of the power information network becomes more and more serious, which is worthy of in-depth study by each of our scientific researchers. As a new type of defense technology, computer network security active defense technology is widely cited in the power information network, and it is constantly updated and improved. Active defense technology can not only improve the power system safety index, but also promote the continuous high-speed development of intelligent power supply.

References

[1] Qingyun C, Kaimin S, Minhua S U, et al. Progress of Diamond-like Carbon Films[J]. Journal of Materials Engineering, 2017, 45(3):119-128.

[2] Satvinder Singh, Mamta Sharma, Nitika Rohilla. Assessment of Salivary Catalase, a-Amylase, and Cotinine Levels in Chronic Smokers: A Comparative Study[J]. Journal of Contemporary Dental Practice, 2018, 19(3):253-256.

[3] Zhenbing L, Zhixun X, Xiong D, et al. Research progress of dual synthetic jets and its flow control technology[J]. Acta Aerodynamica Sinica, 2017, 35(2):252-264.
[4] Hopkins Dawnkimberly, Wilson Candy. Polycystic Ovary Syndrome in Active Duty Service Women: A Retrospective Analysis[J]. Military Medicine, 2019(9-10):9-10.

[5] Rerucha C , Runser L , Ee J , et al. MILITARY HEALTHCARE PROVIDERS' KNOWLEDGE AND COMFORT REGARDING THE MEDICAL CARE OF ACTIVE DUTY LESBIAN, GAY, AND BISEXUAL PATIENTS[J]. Lgbt Health, 2018, 5(1):86-90.

[6] Snezana Zivancevic-Simonovic, Olgica Mihaljevic, Irena Kostic. Eosinophil Cationic Protein in Patients with Differentiated Thyroid Cancer Treated with Radioactive Iodine 131[J]. Annals of Clinical & Laboratory Science, 2017, 47(5):541-545.

[7] Wang F , Lei Z , Yin X , et al. Information Security in the Smart Grid: Survey and Challenges[J]. Computer Networks, 2017, 57(5):1344-1371.

[8] Tareq Alhmiedat, Ghassan Samara. A Low Cost ZigBee Sensor Network Architecture for Indoor Air Quality Monitoring[J]. International Journal of Computer Science & Information Security, 2017, 15(1):140-144.

[9] Acosta A J , E. Tena-Sánchez, C.J. Jiménez, et al. Power and energy issues on lightweight cryptography[J]. Journal of Low Power Electronics, 2017, 13(3):326-337.

[10] Emmanuel Fokides, Alexandra Maria Papoutsi. Using Makey-Makey for teaching electricity to primary school students. A pilot study[J]. Education and Information Technologies, 2019, 2019(1):1-23.

[11] Peter O'Connor, Michael Jacobs. Electrification and Challenging Our Preconceptions [Viewpoint][J]. IEEE Electrification Magazine, 2018, 6(4):94-100.

[12] Reza Tahmasebifar, Mohammad Kazem Sheikh-El-Eslami, Reza Kheirollahi. Point and Interval Forecasting of Real-Time and Day-Ahead Electricity Prices by a Novel Hybrid Approach[J]. Iet Generation Transmission & Distribution, 2017, 11(9):2173-2183.