Design and Implementation of Vulnerability Scanning Tools for Intelligent Substation Industrial Control System Based on Openvas

Yongjun Xia¹,*, jin Wang¹,b, Chang Liu¹,* and Kaiming Yu²,c

1State Grid Hubei Electric Power Research Institute, Wuhan, China
2School of Computer Science, Wuhan University, Wuhan, China

*Corresponding author e-mail: 12612209@qq.com,*375179012@qq.com,
²syywangjin@qq.com,*shallkry@gmail.com

Abstract. This paper analyses the current status of the intelligent substation industrial control system network and the main problems of security protection methods. Based on the analysis of the characteristics of intelligent substation industrial control network, a vulnerability scanning system based on OpenVAS is designed. The vulnerability scanning system is superior to the original vulnerability scanning system in performance and functionality, which effectively improves the security performance of the entire system and reduces system risk.

1. Introduction

The universal application of information technology in substation makes the information exchange and transmission between related equipment in the station more convenient and efficient, which greatly improves the intelligent level of substation and the intelligent substation emerges as the times require. The intelligent substation system eliminates the error caused by manual operation, and also improves the efficiency of information interaction and equipment control, which greatly improves production efficiency. However, with the application of computer technology, it also brings certain degree of security risks. Like traditional computer technology, intelligent substation industrial control systems are also facing many securities threats such as computer viruses, hacking and system vulnerabilities. Due to the particularity and importance of intelligent substations in the entire national production life, the threats they face are more targeted and destructive.

In order to reduce the threat to intelligent substation systems, a series of safety techniques must be adopted to ensure continuous, stable and efficient operation of the entire system [1]. As the scale of the system expands, more and more types of equipment need to be managed, and the workload and management difficulty faced by traditional security measures are greatly increased. Using the vulnerability scanning system to actively discover security risks is an indispensable key link in the intelligent substation security protection system. It can dynamically grasp the security situation of the entire system. Combine the active vulnerability scanning system with other passive security measures to improve the security and reliability of the entire system. This paper briefly analyzes the characteristics of intelligent substation network and the threats it faces, and then discusses the method of constructing a vulnerability scanning system suitable for the intelligent substation industrial control.
system. Finally, based on OpenVAS vulnerability scanning system, a vulnerability scanning platform suitable for intelligent substation industrial control system was designed and implemented.

2. The current threat status of intelligent substation industrial control system

With the application and development of computer information technology in more and more fields, the number of threats faced by information systems has also increased year by year. The National Information Security Vulnerability Sharing Platform released totally 14201 security vulnerabilities in 2018, including 5,381 “zero-day” vulnerabilities, a growth of 39.6% year-on-year. In particular, the number of industrial control system sub-vault vaul ts increased by 22.6% compared with 2017. In recent years, the number of vulnerabilities exposed by industrial control systems has also increased. When the National Internet Emergency Center conducted a random inspection of secondary power equipment in 2018, 232 high-risk vulnerabilities were discovered in 87 models of 35 domestic and foreign mainstream manufacturers [2].

2.1. Domestic and foreign intelligent substation security threat status

Foreign cases of attacks on power infrastructure are not uncommon. In the “Seismic Network” event in 2010, Iran’s nuclear power plant was attacked, and “Stuxnet” virus was reported all over the world [3]. On December 23, 2015, the Ukrainian power sector was attacked by malicious code, causing 80,000 users to power off for hours [4]. On March 7 this year, the Venezuelan power system collapsed, and the Venezuelan official claimed that the accident was caused by a network attack on the Raul Leoni Hydropower Station. The occurrence of these incidents reflects the fact that the current security status of power system is more and more serious, and attacks on infrastructure are becoming more and more harmful [5].

2.1.1. System architecture has inherent security risks. At present, China's intelligent substation mainly uses the IEC61850 standard, and the standard is mainly designed to achieve functional realization. All information is transmitted in plain text in the network. Because the IEC61850 standard does not specify a specific communication medium, the relatively mature Ethernet technology and TCP/IP protocol in computer networks are widely used in the communication network of intelligent substation [6]. This system architecture brings two security issues:

First, when the IEC61850 standard without any security measures is implemented, the data transmitted is transparent to the communication network [7]. Hackers can easily attack the infrastructure by intercepting or modifying data over the network.

Second, TCP/IP is a very common network protocol. Any attack based on this protocol can be transplanted and used in the industrial control system network of the intelligent substation through simple modification.

2.1.2. System device itself has a vulnerability. The devices that make up an intelligent substation can usually be divided into two categories: information system equipment and industrial equipment. These devices may have security vulnerabilities.

Information system equipment typically uses common equipment such as routers, switches, firewalls, and PCs. These devices are used in a wide range of applications and technology updates fast. Such equipment is often used as a supporting technology for network to assist the production function of the system intelligent substation, which is usually the basis of the network of intelligent substation systems. If such equipment is compromised, it will greatly increase the risk of systems, attackers can even directly obtain the information of the entire system and take control of the secondary equipment of the power.

Industrial equipment is typically dedicated to intelligent substations with a unique underlying system [8]. Due to the narrow scope of such systems, most power equipment factories use Cisco's third-party development kits when implementing IEC61850 equipment. The homology characteristics
are obvious. Due to the wide variety of devices, the risks of vulnerabilities in the device's own security protection measures and the underlying system design may exist. [9].

2.1.3. Main methods currently adopted. For the security threats faced by intelligent substations, the following methods are usually used:

(1) Physical isolation. At present, the construction of domestic intelligent substations generally tends to physically isolate the substation from the external network. In theory, physical isolation can completely eliminate threats from outside. However, due to the need for information interaction and the existence of a large number of device interfaces, complete physical isolation is difficult to achieve to a certain extent. When moving storage media or portable devices to access the site, there is also the possibility of bringing in malware [10]. Increasingly large internal networks mean more and more complicated work to manage network boundaries. Just relying on the current state of physical isolation does not completely eliminate the threat [11].

(2) Information security technology. Since the intelligent substation network usually uses Ethernet and the network protocol adopts the TCP/IP protocol, the network information security protection technology based on the protocol can also be used for reference [12]. Through improvement, network security technology can be directly applied to intelligent substation networks such as firewalls, identity authentication and other technical means [13].

(3) Vulnerability scanning technology. Static systems will continue to create new weaknesses as technology advances, which makes them vulnerable. In order to block the threat from the outside of system, it is necessary to find the vulnerability actively in conjunction with the world information security situation [14]-[18].

Vulnerability scanning technology is an active means of protection, mainly based on host deployment and network deployment. According to its deployment characteristics, the scanning effect is not the same. In theory, the host-based deployment method can find more vulnerabilities than the network-based deployment. However, due to the wide variety of devices in the industrial network, and most devices do not have an open system, the use of host-based vulnerability scanning technology is difficult and heavy workload. Intrusion into a device must first "arrival" the device, either network or physical. Due to the special nature of intelligent substations, physical "arrival" can be eliminated through strict personnel management systems and measures. The "arrival" path on the network can be discovered through network-based vulnerability scanning. In practice, network-based vulnerability scanning tools can also discover vulnerabilities that must be physically "arrived" to be used. Therefore, a network-based vulnerability scanning system is more suitable for networks with more types of devices and higher equipment closure.

3. OpenVAS-based vulnerability scanning system architecture

Network-based vulnerability scanning technology is an effective way to discover system vulnerabilities. The OpenVAS (Open Vulnerability Assessment System) is an open source vulnerability scanning framework that integrates multiple functions. It can scan the network device's related information through the computer network, and then analyze the threat of the target device according to the information contained in the library [19].
3.1. Basic Architecture

OpenVAS is mainly composed of client layer, service layer and data layer, as is shown in Figure 1:

![OpenVAS System Architecture Diagram]

The user communicates with the service layer through the OMP protocol at the client level. The OpenVAS server can be used by entering the OMP protocol command at the terminal.

The service layer is the core part of OpenVAS. It is mainly composed of scanning module, control module and management module. It is responsible for the management, use and resource allocation of the system. The data layer is used to store information about the script library, data information and configuration information of OpenVAS system. The script inventory is loaded with scan plugins for various vulnerabilities and must be kept up to date so that the system can discover the latest vulnerabilities. The data information mainly includes various types of open vulnerability database information and scan record information, and the vulnerability database information must be kept updated. And the configuration information mainly stores user information and basic configuration of the vulnerability scanning system.

3.2. NVT (Network Vulnerability Tests)

OpenVAS uses the NVT plugin for scanning for vulnerabilities disclosed in the vulnerability library. The NVT plugin is a vulnerability scanning method written in NASL language that corresponds to a vulnerability in the vulnerability library. There are many ways to get the NVT scan plugin containing official NVT open source plugin via the Internet and the NVT plugin released by other organizations or individuals. Writing or improving existing NVT plugins for specific vulnerabilities can also be implemented [20].

4. Design and deployment of OpenVAS system in industrial control network environment

In order to verify the function of the OpenVAS vulnerability scanning system, this paper designed and improved the functional architecture according to the network characteristics of intelligent substation industrial control system, and deployed the system to verify its functionality in an intelligent substation in Hubei Province.

4.1. System Design

4.1.1. System Architecture Design. The system design is mainly composed of two parts: server and client. The server uses Unix/Linux systems, installs OpenVAS and other related functional modules, and deploys them near the main network nodes of the intranet to reduce the impact of the network architecture. Unified integration of function modules to interact with the client by setting up a web server.

The client connects to the server through a browser. After authentication, OpenVAS can be operated and viewed using the already written OMP protocol command stack, and other functions such as network information collection and information browsing can also be used.
4.1.2. System update design. Vulnerability scanning is usually a scan of known vulnerabilities and relies heavily on updates to the vulnerabilities library and scan plug-in libraries. The intelligent substation industrial control network is usually an independent network, physically isolated from the Internet. Although it blocked attacks from the Internet, it was unable to automatically update the vulnerability scanning system over the Internet. Therefore, the original upgrade function must be redesigned so that the system can manually update the data package and have a reminder function.

![System update design](image)

**Figure 2.** System update design

4.1.3. System Vulnerability Library Design. OpenVAS is only updated according to the foreign CVE vulnerability database, and does not include China National Information Security Vulnerability Library CNNVD [21]. In order to comply with China's national conditions and master the domestic security situation, it is necessary to increase CNNVD on the basis of the OpenVAS original vulnerability database, especially the national information security vulnerability library sub-library industrial control system vulnerability library. Establish a complete local vulnerability database information to facilitate maintenance personnel to understand and protect against targeted attacks.

4.2. Scan Plugin Development for Specific Vulnerabilities

Vulnerability scanning relies heavily on known vulnerabilities. The OpenVAS scanning plugin is also written for known vulnerabilities. When a new vulnerability is discovered, a scan plugin for the vulnerability can be written in time to quickly discover the vulnerability. Using the combination of the update vulnerability library and the self-developed vulnerability scanning plug-in can better improve the vulnerability discovery probability and increase the security of the entire network [22]. OpenVAS is a branch of Nessus, also uses the NASL scripting language to write scan plugins [23]. Test scripts for various vulnerabilities can be developed through the NASL language. OpenVAS is a network-based vulnerability scanning. It sends carefully constructed data packets to the target through the principle or defect of the network communication protocol. By analyzing the returned data, it determines the state of the target and analyzes whether the target has a vulnerability. Vulnerability detection technologies mainly include port scanning, flag information analysis, and simulation attacks. The implementation of port scan is relatively simple, and the device status can be directly determined through the device port open condition. At the same time, port scanning is also the basis for other vulnerability scanning analysis.

The flag information analysis compares the system version of the device with the vulnerability database. If the system version is lower than the security version indicated by the vulnerability library, it can determine that the system has a corresponding vulnerability. The flag information analysis and
port scanning are simple to implement, no harm to the system, and the judgment logic is clear. It is the preferred industrial control system vulnerability detection technology.

The simulated attack simulates the hacker attack behavior through the NASL scripting language, then attacks the system and judges whether the vulnerability exists by analyzing the returned information. The methods of simulating attacks mainly include buffer overflow, weak password guessing and information acquisition. Because buffer overflow attacks are likely to cause system harm, if the system is running at this time, it may cause serious damage. Due to the particularity of intelligent substation system, the system should not be buffered by the buffer overflow in the running system to avoid system crash. Weak password guessing and information acquisition are less harmful and have higher applicability, which can be used universally.

When a major security vulnerability is discovered and the appropriate vulnerability scanning plug-in in the scanning library has not been updated, the vulnerability information can be proactively designed to disclose the vulnerability scanning plug-in to detect the vulnerability earlier.

5. Vulnerability scan results comparison and analysis

5.1. Scanning environment

The OpenVAS vulnerability scanning system was deployed in an intelligent substation network in Hubei Province to scan a certain segment of the network. At the same time, a vulnerability scanning system originally configured for the intelligent substation was used for comparison. The network segment of the intelligent substation network ranges from 172.16.142.1 to 172.16.143.255. The network segment includes common working environments such as routers, switches, database servers, etc.

5.2. Scan results

The network segment was scanned using two vulnerability scanning systems, and a total of 29 devices were scanned. The vulnerability scan results are shown in Figure 3.

As shown in the figure, the number of various types of vulnerabilities scanned by two vulnerability scanning systems is recorded. Among them, the vulnerability threat level is divided according to the CVSS score of the scanned vulnerability, 7.0~10 is divided into high threat, 4.0~6.9 is divided into medium threat and 0.1~3.9 is divided into low threat. "Record" means that the device may provide a service. The service is ostensibly flawless, but it is not certain whether the service is being used illegally, so it may have certain risks, which need to be viewed by the administrator and judged according to the specific situation.
Table 1. Vulnerability category statistics comparison table

| Vulnerability category         | Original vulnerability scanning tool | OpenVAS | Number |
|-------------------------------|--------------------------------------|---------|--------|
| Digital error                 | 1                                    | 1       | 1      |
| Configuration error           | 1                                    | 1       | 1      |
| Competitive condition         | 1                                    | 0       | 1      |
| Resource management           | 5                                    | 5       | 8      |
| Lack of information           | 2                                    | 5       | 6      |
| Security feature              | 11                                   | 22      | 27     |
| Information disclosure        | 4                                    | 38      | 40     |
| Input verification            | 6                                    | 10      | 12     |
| Unknown service               | 0                                    | 2       | 2      |
| **Total**                     | 31                                   | 84      | 98     |

According to the National Information Security Vulnerability Library (CNNVD) vulnerability classification specification, the detected system vulnerabilities are classified and counted. As shown in Table 1.

5.3. Analysis of results

A comparative analysis of the two scan results shows that the OpenVAS-based vulnerability scanning system is more functional than the original scanning tool. However, since OpenVAS is a network-based vulnerability scanning system, there are two shortcomings:

1) Unable to judge undisclosed vulnerability

The vulnerability scanning tool scans based on "known" vulnerabilities. To find unknown vulnerabilities, you need to integrate vulnerability mining technology and analyze network data to find abnormal data to determine threats. Because a large amount of unintended data is sent when the vulnerability is mined, it may cause damage to the device and the entire system. It does not apply to the vulnerability scan during routine maintenance. It is contradictory to discover all the vulnerabilities and ensure that the system is stable. And because the industrial control equipment is generally closed, the vulnerability exploration work is very difficult. Therefore, the missing tool relies heavily on the public vulnerability library and does not have the ability to actively exploit the vulnerability.

2) Weak vulnerability detection capability for non-networks

The vulnerability scanning tool is web-based and has its inherent flaws. Although in theory, all the vulnerabilities that are transmitted through the network can be found. But in practice, there are still some vulnerabilities that do not pass through the network, which can be exploited by hackers to deviate from the network by means of deception or u-shipping and pose a threat to the system. Although such vulnerabilities can be discovered through version detection, they may be spoofed when scanning devices that have been granted access.

There are two ways to solve these two problems. Firstly we need to update the vulnerability database in time to ensure that the missing tool can detect as many new holes as possible. The second method is to strengthen the formulation and implementation of the security system and prevent non-related equipment and non-related personnel from accessing sensitive networks and equipment.

6. Conclusion

Based on the analysis of security status of current intelligent substation industrial control system, this paper designs and implements a vulnerability scanning tool based on OpenVAS according to the characteristics of system network. From the experimental results, the performance of the vulnerability scanning tool is greatly improved compared with the original scanning tool. The original function of OpenVAS has been redesigned for the characteristics of industrial control network, which is more suitable for the intelligent substation industrial control system environment in terms of practicality.
This paper has explored an effective scheme and implementation way to improve the safety performance protection measures of intelligent substation industrial control system.

References

[1] XU Li-juan, XU Jing, TANG Gang. The Study of Industrial Control System Network Security Risk Analysis Method [J]. Electronic Science & Technology. 2015.2(6):679-684.

[2] A Summary of China's Internet Network Security Situation in 2018 [J]. Civil-Military Integration on Cyberspace, 2019(04): 36-39.

[3] YAN Xiao-feng, Stuxnet Trigger New Thinking of Network Security [J]. INFORMATION SECURITY AND TECHNOLOGY. 2011. (2):17-19.

[4] Comprehensive analysis of the attack on the Ukrainian power system [J]. Journal of Information Security Research, 2016, 2 (03): 243-243.

[5] JIANG Nan, JI Ling, YANG Xiao-fan, Information Security Technology of Smart Substation [J]. Electrical Automation. 2018.40(6):48-51.

[6] XU Kai-dong, WANG Hong, YANG Zhi-jia. Industrial Automation Network Based on Ethernet [J]. Information and Control. 2000.29(2):182-186.

[7] GUO Chang-xin, YU Bin, GUO Jia, WEN Bo-juan, ZHANG Jin-jiang, ZHANG Li, LU Hai-bo, LI Bo. Security Risk Assessment of the IEC61850-based Substation Automation System [J]. Proceedings of the CSEE.2014. (4):685-694.

[8] CHANG Hong-xia, Industrial Control System Network Security Protection Construction [J]. Gansu Metallurgy. 2018.40(6): 127-128.

[9] SHANG Wen-li, et al. Study on the Vulnerability Analysis Method for Industrial Embedded Devices [J]. Process Automation Instrumentation. 2015.36(10): 63-71.

[10] XU Qin, et al. Research and Application of Safety Isolation Measures for Intelligent Substation [J]. Electric Engineering. 2015. (12): 3-8.

[11] ZHAI Feng, et al, Study on Smart Substation Communication Network Security Protection Technology [J]. Automation & Instrumentation. 2015.30(3):6-9.

[12] ZHANG Xue-lin, et al. Network Security Technology & Application [J]. Network Security Technology & Application. 2015. (2): 140-144.

[13] WANG Yu-bin, Research on Industrial Control System Security Defense [J]. Netinfo Security, 2016 (9): 35-39.

[14] ZHANG Jia-jia, SONG Shi-tai, ZHANG Yan, et al, Research on Key Technologies of Network System Vulnerability Analysis and Evaluation [J]. Computer and Digital Engineering. 2017.45(11): 2248-2262.

[15] ZHAO Xi-ming, Computer network security and vulnerability scanning technology research [J]. Network Security Technology & Application.2014. (1): 123-125.

[16] WANG Liang, Design and Application of Network Scanning System [J]. Information Security and Technology. 2011(2): 44-46.

[17] WANG Xu, CHEN Tao, MIAO Gang, Role and Practice of Vulnerability Scanning Technology in Information Security Assurance of State Grid [J]. Electric Power Information Technology. 2011.09(2): 157-160.

[18] ZHOU Jin-cai, ZHU Lei-ming, Principle analysis and system design of network scanning system [J]. Journal of Anhui Vocational College of Electronics & Information Technology. 2004.3(5): 72-73.

[19] LI Rui, Design and Implementation of OpenVAS Based Vulnerability Scanning System [D]. 2015, Xidian University.

[20] XUN Fei-xian, WANG Jian-hong, ZHEN Qiu-sheng, Design and Implementation of Network Vulnerability Scanner Based on NASL [J]. Journal of Zhongyuan Institute of Technology. 2009.20(2): 1-10.
[21] QIN Yuan-yuan, et al, Research on Industrial Control Vulnerability Discovery and Analysis System Based on CVE Vulnerability Database [J]. Information and Communications Technologies. 2017(3):54-59.

[22] GAO Tian-yu, Research and Implementation of Vulnerability Scanning System Base on NASL [D].2014, School of Aeronautics and Astronautics. 1-93.

[23] YU Qin-yong, Construction of Nessus-based Security Scanning System [J]. Communications Technology. 2008.41(1): 96-98.