Atlantis Highlights in Engineering, volume 3
3rd Joint International Information Technology, Mechanical and Electronic Engineering Conference (JIMEC 2018)

Research of Vulnerability Security Detection for Video Surveillance Equipment

Pang Tianyu[1], Chen Rui[1], Shen Quanjiang[1]
1.State Grid Shanghai Electric Power Research Institute
330825704@qq.com, 175433654@qq.com ,qjshen123@126.com

***Abstract*—Aiming at various security vulnerabilities in video surveillance system, the paper proposes a vulnerability security detection method for video surveillance equipment. The method scans the TCP / IP different ports services of the target video equipment remotely, records the response content of the target, extracts the vulnerability characteristics of the response content, and matches the vulnerability database with the self -vulnerability analysis engine to determine whether the equipment has vulnerabilities. The method can detect vulnerabilities in monitoring equipment of mainstream equipment manufacturers. It can discover common security vulnerabilities in batches, automatically, such as weak passwords, access violations and command execution.**

Keyword—video surveillance; vulnerability detection; equipment detection; vulnerability database

I. INTRODUCTION

The network video surveillance system has been widely used and popularized in different fields and occasions because of its rich and varied image information, high definition pixel, advanced technology and operation of the facilitation. Video surveillance system (including traditional cameras and smart cameras) as the "eyes of the Internet of Things", its security issues have become the focus of the Internet of Things security. With the continuous exposure of weak password vulnerabilities, command execution vulnerabilities, ultra vires reading and other issues of well-known monitoring equipment manufacturers, the related monitoring equipment has serious security risks, a lot of equipment has been controlled by illegal personnel, and large-scale DDOS attacks are triggered. And similar security events including research laboratories, factory internal monitoring screens, kindergarten home video information, and even computer camera screens are uploaded to the network. The network security incidents in the video surveillance system are frequent, and the situation is not optimistic. Each communication level of video surveillance system faces severe information security risks. It has many characteristics such as many vulnerabilities, wide range, and bad influence. Therefore, it is very necessary to study a vulnerability detection method for video surveillance system.

At present, like most network equipment, the security vulnerabilities of video surveillance equipment mainly includes weak password, bypassing authentication, plaintext transmission, injection vulnerabilities, cross-station attacks, denial of service attacks, command execution, over-authorized access and so on. Therefore, the vulnerability detection method is the same as the mainstream leak-sweeping tools in the market, and the vulnerability analysis result is obtained by scanning the equipment, extracting feature data, and matching the vulnerability feature. However, due to different products of different monitoring equipment manufacturers, feature data extraction and vulnerability database information are also different from traditional equipment manufacturers. Therefore, it is necessary to conduct expert analysis for video equipment and construct a dedicated vulnerability database. In addition, in response to the constant emergence of new security vulnerabilities, the vulnerability analysis engine needs plug-in design and dynamic scalability.

II VULNERABILITY SECURITY DETECTION FRAMEWORK

The principle of vulnerability security detection for video surveillance equipment is to record the response content of the target by remotely detecting the service of different ports of TCP/IP on the target host. After obtaining the response information of the target host TCP / IP port and its corresponding network access service, it matches the

vulnerability response characteristics defined at the beginning of this program design, and if the matching condition is met, it is considered as vulnerability. In addition, by simulating the attacking methods of hackers, an aggressive vulnerability scanning of the target host system, such as detecting weak passwords, is also one of the implementation methods of the scanning module. If the simulated attack is successful, it is considered vulnerability. On the principle of matching, the network vulnerability scanner adopts the rule-based matching technology, that is, according to the analysis of network system security vulnerabilities and hacker attack cases by security experts and the practical experience of system administrators on network system security configuration, a set of standard system vulnerability database is formed. Then the corresponding matching rules are constructed on this basis, and the analysis of system vulnerability scanning is carried out automatically by the program.

The main modules of vulnerability security detection framework include input and output module, program configuration module, port scanning module, control and scheduling module, plug-in analysis engine module and vulnerability database module.

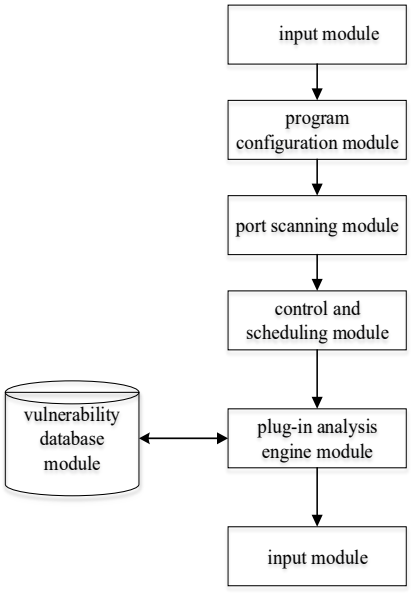

Fig. 1 vulnerability security detection framework for video surveillance system

III THE PRINCIPLE OF MAIN MODULE

A. *Input and Output Module*

The main function of the input and output module is the input interface and the final output feedback interface of the program. The input includes the IP range, port range and other parameters to be detected. The pointing function of the detection target can be realized by modifying the parameters of the module.

B. *Program Configuration Module*

The main function of the program configuration module is to select the module and password dictionary loaded by the program. By manually loading or not loading the specified module, the program running process can be reduced and the program execution speed can be accelerated. The password robustness of video equipment can be detected by choosing username and password dictionary. If the password of video equipment matches the username and password dictionary, the video equipment is judged to be weak password equipment.

C. *Port Scanning Module*

The main function of the port scanning module is to discover the surviving ports in the specified IP and port range. The module uses TCP three-way handshake detection mechanism to determine the openness of TCP ports, which is timely and accurate. The open port detected by the module scan will lay the foundation for the vulnerability detection of the surviving port.

D. *Control and Scheduling Module*

The main function of the control and scheduling module is to glue the port scanning, vulnerability detection, result analysis and other modules to control the operation logic of the program, and send the results generated during the scanning process to the result analysis module for analysis. At the same time, the operation interval is generated during the operation of the program, which prevents the logic confusion of the program and causes the failure of the test. It also controls the running and stopping of multithreads in the scanning process, and sends control messages and logs to the UI main thread by multithreads to prevent thread conflicts and deadlocks.

E. Plug-in Analysis Engine Module

Aiming at the data acquired by port scanning, the plug-in scanning engine is used to analyze and match vulnerability. A scanner with a plug-in structure allows anyone to construct their own attack detect scripts without knowing too much about the scanner's principles. This scanner can also be used as a platform for simulating hacker attacks. The scanner with this structure has strong vitality, such as the famous Nessus. This program can use Python script to expand plug-ins to better perform vulnerability scanning. In the running process of the program, there will be a lot of intermediate information to be printed, because the program is expanded in the form of Python plug-ins. Each plug-in may have a certain log output and result generation. It needs to set a unified format to summarize these results. The main function of the module is to integrate loose logs generated by Python plug-in module during scanning and detecting, and to form a visual and unified log format for output in the main interface log box.

F. Vulnerability Database Module

This module is an innovative feature of this program. The tools developed in the past are all designed in one step and the code is written in place. When the function of the same module needs to be added and modified, the source code of the program and tool must be recompiled and modified. The program cannot be modified by non-ordinary technical personnel and code writers. This situation leads to a significant reduction in the scalability of the program. As time goes on, a variety of vulnerabilities emerge in endlessly. Unable to extend or extending very troublesome programs make it difficult to update program in a timely manner and to effectively detect the latest vulnerability equipment. Therefore, we draw lessons from the previous tool writing, adopt UI and plug-in separation to design program and reserve a large number of interfaces in Python plug-in library for later expansion. As long as the Python script is modified according to the plug-in format and the code in the main program is slightly modified and recompiled, the plug-in library and vulnerability data can be updated. This greatly improves the scalability of the program.

IV EXPERIMENT ANALYSIS

According to the above design ideas, and based on the working principle of network scanner, we design a video surveillance system security automatic detection tool 。The tool incorporates the advantages of .Net and Python languages. It uses .Net to develop interfaces and logic, and Python to develop vulnerability plug-ins. It has the characteristics of platform consistency, multi-platform compatibility and high scalability. Moreover, the latest vulnerability disclosure in the network security industry is generally published in the form of a Python written POC. This tool can quickly modify the latest POC into a tool plug-in to expand the functionality of the automatic tool.

A. Weak Password Detection

At present, the default username and password exist in most of the monitoring equipment when they leave the factory. The manufacturers and users often have weak security awareness and do not modify the default password, which easily leads to weak password problems in the system and is easily accessed illegally. Weak password detection is based on the username and password dictionary in the common video surveillance system, using the weak password plug-in script to try to access the video system to determine whether the system has a weak password. The common username and password dictionary is shown in the following table I.

Table I The common username and password dictionary

manufacturer	username	password
Hikvision	admin	12345
Dahua	admin	888888
TIANDY	Admin	111111
Others	root,888888,666666	admin,user

The detection result of a video system using the detection tool is shown in Fig.2. As can be seen from the scan results, it is possible to scan to identify common username and password.

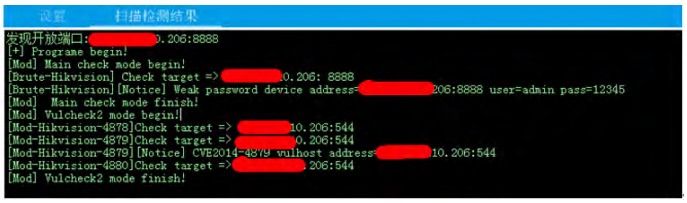

Fig.2 Weak password detection results

B. Code Execution Detection

The monitoring equipment uses a fixed buffer to accept user input when processing RTSP requests. If the user sends a larger data to request, it will eventually cause the server to overflow. An attacker can execute arbitrary code by changing the program execution flow of the server through overflow. The specific vulnerability numbers are: CVE-2014-4878, CVE-2014-4879, and CVE-2014-4880.

1）CVE-2014-4878：When the monitoring equipment processes the RTSP request, a fixed buffer is used to accept the body. When the attacker sends a larger body, an overflow may occur, causing a service crash and so on.

2）CVE-2014-4879：RTSP also uses a fixed buffer for the processing of the request header. The attacker can construct a long enough header to fill the buffer, resulting in an overflow.

3）CVE-2014-4880：RTSP also uses a fixed buffer when processing the underlying authentication header, which can cause an attacker to overflow through construction or even execute arbitrary commands.

According to the POC principle of the above three vulnerabilities, we develop a command execution vulnerability plug-in script and scan a vendor monitoring system. The scan results are shown in Fig. 3.

Fig. 3 command execution vulnerability detection results

V CONCLUSION

The various security vulnerabilities in video equipment monitoring system, the paper designs a vulnerability security detection method for video monitoring system, and develops an automatic security detection tool on this basis. The detection tool uses a modular structure, and the scan engine and vulnerability database are designed to be plug-in, so that the detection tool has the characteristics of automation, extensibility and easy operation. Through the analysis of two vulnerabilities in weak password and code execution, we find that the detection tool can meet the detection needs of common vulnerabilities in video surveillance system and has a certain practical value.

ACKNOWLEDGMENT

This work is supported by 2018 State Grid Shanghai Electric Power Research Institute mass innovation and technology project ("Hands-on" Pilot Implementation Project, 520940180024).

REFERENCES

[1]. Zhong WeiGuo,Yu Zhongchen. Security situation analysis and Countermeasures of video surveillance system. CHINESE RAILWAYS, 2015 (4) ,pp:103-107.

[2]. 80% home camera risk, family life or live webcast. [2016-05-07]. http://www. chinanews. com/.

[3]. US media: hackers control oil pipeline explosion, open network warfare Era. [2016-05-07].http://mil. cankaoxiaoxi.

[4]. Hikvision Black Swan soul prism door. [2016-0-07].http://www.xinhuanet.com/fortune /caiyan/ksh/11.html.

[5]. Fu Xin,Liu Lin,Zhang FanZhong. Research on information security evaluation technology of public security video surveillance system based on Grading Protection Evaluation.
POLICE Technology, 2016 (5),pp :75-78.

[6]. Wang Hui,Wu Hao,Li Zheng. Research on security evaluation system of video surveillance system. Information and Communications Technologies. 2016(3),pp:43-48.

[7]. Liu Bin,Tang Chaojing,Zhang SenQiang.lassification and scanning analysis of network security vulnerabilities. Information and Electronic .2004,Vol.2,No.4,pp:318-320.

[8]. Song JinKe.Large-Scale Automatic Analysis of Surveillance Devices.BeiJIng: Beijing Jiaotong University. 2017.

[9]. MAO Yan-fei, HUANG Zhong-dong. Research and design of web DVR system based on real-time streaming protocol. Computer Engineering and Design 2011, Vol.32, No.7,pp:2523-2530.