ATLANTIS PRESS

Advances in Computer Science Research, volume 70

2nd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2017)

A Method of Scanning Industrial Control System Equipment

Guangkai Zhou [a,*], Jun Bai [b], Bailing Wang [c] and Jia Song [d]

School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China

[a]zgk_whhit@foxmail.com, [b]baijun69@sina.com, [c]wbl@hit.edu.cn, [d]songjia@hitwh.edu.cn

Keywords: Industrial control system equipment, NSE script, Modbus protocol.

Abstract. With the deep penetration and wide advancement of "Made in China 2025" and "Internet plus" in various fields, the continuous integration of industrialization and informationization process, more and more critical infrastructure related to national economy and people access to the Internet, industrial control system faces more and more security threats. Therefore, to find networked industrial control system equipment and take targeted protection measures is our only way, and find the network of industrial control system equipment is our prerequisite for targeted protection. This paper first introduces the existing network detection method, combined with MODBUS communication protocol research based on NMAP NSE script based on industrial control system equipment information detection method. Experiments show that, NSE script can be targeted to the industrial equipment control system letter to obtain information.

1. Introduction

Industrial Control Systems (ICS) is a process control component that collects and monitors real-time data from a variety of automated control components, a business process control system that ensures the automation of industrial infrastructure, process control and monitoring. Core components include supervisory control and data acquisition (SCADA), distributed control system (DCS), programmable logic controller (PLC), remote terminal Unit(RTU), intelligent electronic Device(IED), and to ensure that the components of communication interface technology[1]. Industrial control system is widely used in electric power, water conservancy, transportation, chemical industry, oil and gas and other industries, of which more than 80% of the people involved in the national economy and the key infrastructure, industrial safety has become an important part of national strategy.

"Made in China 2025"[2] and "Internet plus" has brought great development opportunities for the industrial control system, but also brought unprecedented challenges. The threat of industrial control systems from the initial stand-alone "isolated control" to the current network-level "complex uncontrollable". The pursuit of usability and ignore the security, which is now widespread phenomenon of industrial control system, the lack of a complete and effective security strategy and management process is the biggest problem of China's industrial control system, these problems directly lead to the industrial system is always facing the virus, hackers, denial of service and other information security threats.

Industrial control system security and traditional information security is very different. Industrial control system more emphasis on the process of industrial automation and industrial equipment availability, real-time, controllability, the traditional network protocols are standard and open, and industrial equipment data transmission is more industry-specific and private communication protocol , Such as modbus, IEC101/104, DNP3 and other general industrial control agreement, Siemens S7, Omron FINS and other private protocols[3].Therefore, the industrial control equipment to take targeted protection measures, the primary task is to find the network industrial control system equipment.

This paper briefly introduces the common network scanning technology and common tools, and for the network of Schneider PLC proposed a detection method based on NMAP NSE script. Experiments show that this method can effectively detect Schneider PLC and obtain specific information.

2. Common Network Scanning Technology

Network scanning technology is a security technology that uses simulated hacking to detect and evaluate the vulnerability of remote or local systems. Through the network scan detection, to find the network or host configuration information, the server specific information, TCP/IP port allocation and the provision of network services. Administrators through this information to better understand the network configuration and operation of services, timely detection and processing of existing security vulnerabilities in the network to improve network security [4].

Network scanning technology in accordance with the complete scanning process can be divided into three categories: one is the survival of scanning technology, the second is the target information collection technology, including port scanning technology, operating system identification technology and system service identification technology, the third is the vulnerability scanning technology [5].

2.1 Surviving Scanning Technology

This technology is also known as target discovery technology, Ping detection technology, the purpose is to confirm the target host IP address, and that is, whether the IP address of the distribution of the host. Ping detection technology is mostly based on ICMP protocol, constructed and sent to the target host an ICMP packet, according to the target host response to determine whether the target host to survive.

Ping detection common tools are HPing2, icmpush & icmpquery and Pinger and so on.

2.2 Target Information Collection Technology

After the host survivability judgment is completed, the target information is collected, including the target host port open information, the operating system type information and the open system service information. The technologies used include port scanning technology, operating system identification technology and system service identification technology.

Port Scanning Technology

The port is openning channel on the host, 0-1024 for the well-known port. The total number of ports is 65535. The port is actually the channel that maps from the network layer to the process. Through this relationship can master what kind of process to use what kind of communication, in this process which can be achieved through the process of information, common port scanning technology with TCP scanning and UDP scanning. TCP scanning is the use of three-way handshake process and the target host to establish a complete or incomplete TCP connection, such as TCP connect () scan, TCP SYN () scan. UDP scanning does not establish a connection, good concealment, but the packet is easy to lose.

Operating System Identification Technology

According to the difference between the TCP/IP protocol stack, the returned packet will be different, through the operating system fingerprint library comparison, to identify the operating system type. Operating system identification technology is mainly active identification and passive identification.

Operating system identification common tools are XProbe2 and THC-Amap.

System Service Identification Technology

System service identification is mainly based on the port having been scanned to determine, or HTTP response analysis, binary information detection (banner) and other means to achieve.

System services to identify common tools are Nmap and so on.

2.3 Vulnerability Scanning Technology

Vulnerability scanning is mainly throughing the following two ways to check whether the target host vulnerabilities, one is based on the vulnerability signature library matching, after the port scan that the target host open port and port network services, these related information and network vulnerability scanning The system provides loopholes to match to see if there are loopholes that meet the matching criteria[6].Second, based on plug-in technology, through the simulation of hacker attacks, the target host system for aggressive security vulnerabilities, such as testing the weak password. If the simulation attack is successful, it indicates that there is a security vulnerability in the target host system.

3. A Network Detection Method for Schneider PLC

Because the traditional network detection method cannot detect the network industrial equipment. The paper presents a detection method for Schneider industrial equipment. This method is based on an open industrial Ethernet protocol standard ---- MODBUS communication protocol. Under the Nmap scanning framework, we construct and send specific data packets to port 502 in network industrial control system equipment. Next, we receive the reply packet and parse the packet to get the detailed information of the industrial equipment.

3.1 Overview of MODBUS Communication Protocol

MODBUS is the application layer messaging protocol on Layer 7 of the OSI model. MODBUS is a request/reply protocol, and provides the function specified by the function code. MODBUS function code is elements in MODBUS request/response PDU. The MODBUS protocol defines a simple protocol data unit (PDU) that is independent of the underlying communication layer. The MODBUS protocol mapping on a specific bus or network can introduce some additional fields on the application data unit (ADU).

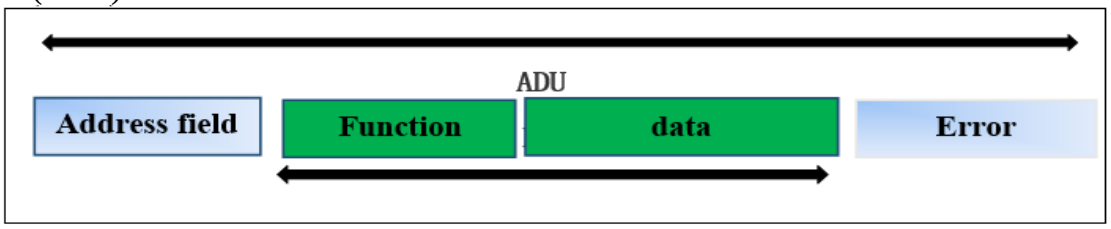

Figure 1. Universal MODBUS frame

The client that initiates the MODBUS transaction creates the MODBUS application data unit, and the function code indicates to the server what action will be performed. The MODBUS protocol establishes the client-initiated request format. The function code field of the MODBUS data unit is encoded in one byte. The valid codeword range is decimal 1-255 (128-255 is reserved for exception response). When the client sends a message to the server device, the function code field informs the server of what to do.

The MODBUS protocol common function code is defined in the following table.

Table 1. Common function code definitions

				Function code		
				code	Subcode	Hex
Data access	Bit access	Physical input	Read the input discrete	02		02
		physical coil	Read Coil	01		01
			Write a single coil	05		05
			Write multiple coils	15		0F
	16 bit access	Input memory	Read input register	04		04
		Internal memory	Read multiple registers	03		03
			Write a single register	06		06
			Write multiple registers	16		10
			Read/write multiple registers	23		17
			Mask write register	22		16
	File record access		Read the file record	20	6	14
			Write a file record	21	6	15
Encapsulation interface			Read the device identification code	43	14	2B

43 (0X2B) Reads the device identification code, which allows reading of the identification and additional messages associated with the physical description and functional description of the remote device. The read device identification code interface is simulated as an address space, which consists of a set of addressable data elements. The data element is the called object, and the object ID determines the data element.

The interface consists of three objects: the base device identification code, the normal device identification code, and the extension device identification code. The device identification table is shown in the following table.

Table 2. Device ID Table

Object ID	Object name/description	type	M/O
0x00	Vendor name	ASCII string	Forced
Object ID	Object name/description	type	M/O
0x01	Product code	ASCII string	Forced
0x02	Major revision	ASCII string	Forced
0x03	VendorUrl	ASCII string	Optional
0x04	Product name	ASCII string	Optional
0x05	Mode name	ASCII string	Optional
0x06	User name	ASCII string	Optional
0x07-0x7F	Reserved		Optional
0x80-0xFF	Optionally define the scope of the dedicated object	ASCII string	Optional

The MODBUS encapsulation interface with the assignment number 14 identifies the read alias request and requires several request/response transactions if it is not suitable for a separate response. The object ID gives the first object identifier obtained. For the first transaction, the client must set the object ID to 0. For the following transaction, the client must set the object ID to be in front of the server return value. If the object ID does not conform to any known object, the response starts from the beginning.

3.2 Overview of Nmap NSE script

Nmap is the Network Mapper, which is a port scanner. Nmap's core features include host discovery, port scanning, version detection, operating system detection, NSE scripting engine and so on. Nmap provides a powerful scripting engine----NSE, that supports Lua programming to extend Nmap functionality. At present the latest version of the Nmap already contains more than 500 commonly used Lua script, these scripts complement the enhanced Nmap scanning capabilities.

The Nmap script is divided into 14 categories on the official website, including auth (script for handling authentication certificates), exploit (exploited known vulnerabilities), fuzzer (fuzzy tests). In the command line parameters, the option of specifying a script or -A triggers the execution of the Nmap script. When executing a script scan, the script_scan () function is called from nmap_main (), and the core operation is handled by the run () function in the main () function. The flow chart for the NSE script is shown below.

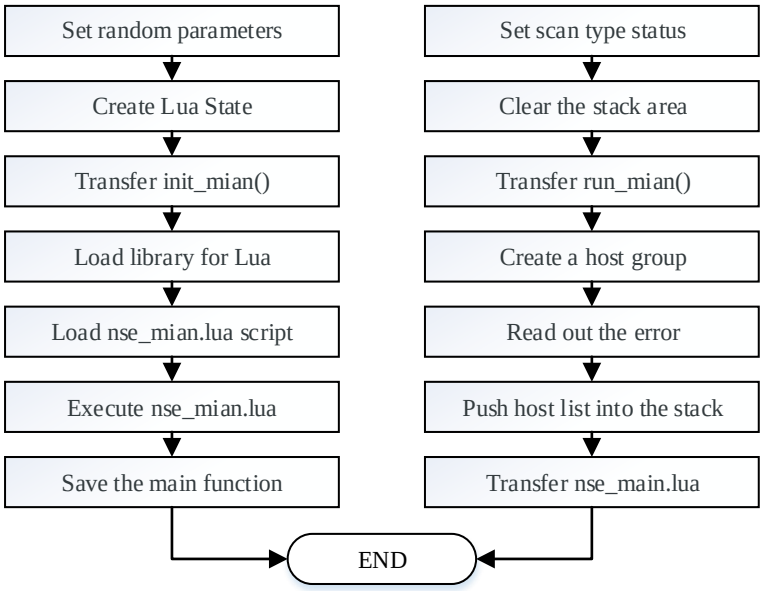

Figure 2. NSE script flow chart

3.3 Scanning for Schneider PLC

According to MODBUS TCP communication request data frame format of the 0x2B function code, we construct a MODBUS TCP packet, and connect to the Schneider PLC IP address to request the

recovery of industrial equipment. Next, through the reply to the data packet, we can analyze packet and extract the specific information of Schneider PLC. The flow chart shown in Figure 3, and the request PDU is shown in Table 3 below.

Table 3. Request PDU

Function Code	One Byte	0x2B
MEI Type	One Byte	0x2E
ReadDevId Code	One Byte	01/02/03/04
Object ID	One Byte	0x00-0xFF

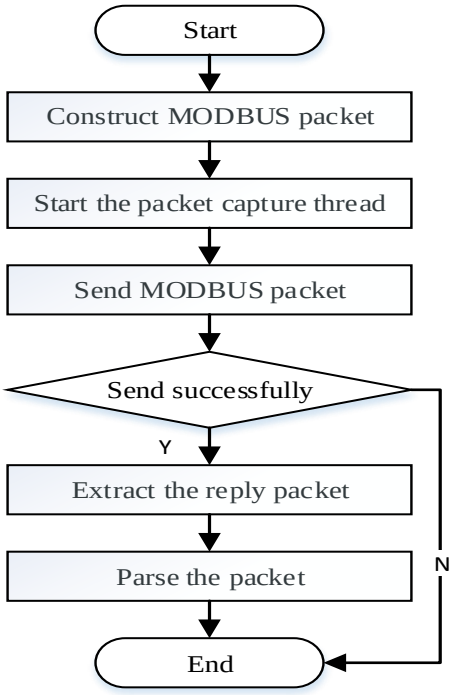

Figure 3. Industrial control equipment scanning flow chart

Start Capture Packet Thread: Used to capture packets.

Send MODBUS packet: The target address is set to the address of industrial equipment, and sending data packets to the destination address.

Extract the reply packet: Extract the data packet from the reply packet.

Analysis of the reply packet: According to response PDU structure of the 0x2B function code, we analyze the data packet, extract the required industrial equipment information.

4. Experiment Results and Analysis

We use the ‘shodan’ to get the IP address of the networked Schneider PLC, then under the Nmap framework, load the Nmap NSE script command to scan the Schneider PLC. The script begins using function code 43 to identify if there is a Modbus device at the targeted IP address. Schneider, unlike many vendors, supports function code 43 and will return some variant of Schneider in the response message. I should note that even if the Modbus device being queried does not support function code 43 the response can confirm it is a Modbus device. The purpose of modicon-info.nse is to first identify and enumerate Modicon PLC's made by Schneider Electric. The script first identifies if an IP connected device is sending a Modbus function code 43 request. The response is sufficient to identify Modbus devices even if they do not support function code 43. If the response vendor name contains the string Schneider, the script will enumerate the device using the Schneider Electric proprietary Modbus function code 90.

We can scan the Schneider PLC using the command parameter in Windows or Linux, the command is follows:

nmap -p 502 -script modicon-info.nse -sV <host>

Using the nse script to scan Schneider PLC, modbus function code 43 and function code 90 properties that are included in the script output are:

(1)Vendor Name - This script will ignore all devices that do not contain "Schneider".

(2)Network Module - The Ethernet communications module in the Modicon PLC.

(3)CPU Module - The CPU module in the Modicon PLC.

(4)Firmware - The firmware version on the CPU module in the Modicon PLC.

(5)Memory Card - The model number of the memory card in the CPU module.

(6)Project Information - Miscellaneous information about the project, such as the project name, the version of Unity Pro that was used to configure it, as well as the workstation name that programmed the PLC.

(7)Project Revision - The revision of the project running on the PLC, the project revision number increments by 1 each time a the project is built, and transferred to the PLC.

(8)Project Last Modified Date - A time stamp that is stored for when the last time the PLC was modified by a technician.

The results of scanning are shown below:

```
Nmap scan report for static-50-122-211-221.roch.ny.frontiernet.net (
Host is up (0.36s latency).
PORT    STATE SERVICE VERSION
502/tcp open  Modbus
| modicon-info:
|   Vendor Name: Schneider Electric
|   Network Module: BMX NOE 0100
|   CPU Module: BMX P34 1000
|   Firmware: V2.90
|   Memory Card: BMXRMS008MP
|   Project Information: Station - V4.0
|   Project Revision: 0.0.159
|_  Project Last Modified: 7/28/2016 0:47:48
```

Figure 4. Scanning results

Compared with the traditional scanner, the scanning informations from nse script under the nmap framework become more and more. The informations through traditional scanner are shown in Figure 5. The results are completed with Plcscan. PLCScan is a scanning tool developed by foreign hacker organization ScadaStrangeLove to identify online PLC devices and other Modbus devices. The tool is written in Python and detects two ports, TCP/102 and TCP/502.

```
[root@server246 zhgk]# python plcscan.py 81.133.
Scan start...
81.133.    :502 Modbus/TCP
  Unit ID: 0
    Device: Schneider Electric BMX NOE 0100 V2.80
  Unit ID: 255
    Device: Schneider Electric BMX NOE 0100 V2.80
Scan complete
```

Figure 5. The results with traditional scanner

5. Conclusion

This paper introduces the common network scanning technology and its common tools firstly, and points out that the common scanning tools can not effectively scan the detailed information of the networked industrial equipment. On this basis, through the study of MODBUS protocol, the NSE script based on the nmap framework can scan the Schneider PLC and extract the information of the device effectively. However, this method also exists the problem of the uniqueness of the scanning device, if the scanning of a variety of devices, the need to constantly expand the script library, which is the future need to improve the place.

Acknowledgements

This work was supported in part by the space support technology fund projects under Grant 2014-HT-HGD5,Natural Scientific Research Innovation Foundation in Harbin Institute of Technology(HIT.NSRIF.201723), Discipline Construction Guiding Foundation in Harbin Institute of Technology (Weihai)(WH20150211), National Natural Science of China (Grant No. 61170262，61371177), National Key Research and Development Plan under grant 2016YFB0800802, and Science and Technology Major Project in ShanDong under grant 2015ZDXX0201B04.

References

[1] Jie P, Li L. Industrial Control System Security[C]// International Conference on Intelligent Human-Machine Systems and Cybernetics. IEEE, 2011:156-158.
[2] Liu S X. Innovation Design: Made in China 2025[J]. Design Management Review, 2016, 27(1):52-58.
[3] Lighthouse Labs. Report on Organizational Behavior Analysis for Web Intelligence Critical Infrastructure Information Collection [R]. Lighthouse Lab Research Report .2016
[4] Mantere M, Sailio M, Noponen S. A module for anomaly detection in ICS networks[C]// International Conference on High Confidence Networked Systems. 2014:49-56.
[5] Gong J. Computer Network Safety and Leak Scanning Technology[J]. Jornal of Zhzho N of Hnology, 2005.
[6] Shan R, Xiaoyong L I, Li J. Technology of Active Detect Network Scanning[J]. Computer Engineering, 2003.
[7] Speake G. Securing industrial control system[J]. Intech, 2012.
[8] Hadziosmanovic D, Bolzoni D, Etalle S, et al. Challenges and opportunities in securing industrial control systems[C]// Complexity in Engineering. IEEE, 2012:1-6.
[9] Sireteanu N A. SECURITY TOOLS SOFTWARE IN AN OPEN SOURCE ENVIRONMENT[J]. Scientific Annals of the Alexandru Ioan Cuza University of Iasi Economic Sciences, 2008, 2008:392-400.
[10] Stohl R. Industrial comunication in distillation column model[C]// Programmable Devices and Embedded Systems. 2012:357-361.