IMPACT OF ACTIVE SCANNING ON THE INDUSTRIAL CONTROL NETWORKS

Ondřej Pospíšil
Doctoral Degree Programme (2), FEEC BUT
E-mail: xpospi89@stud.feec.vutbr.cz

Supervised by: Radek Fujdiak
E-mail: fujdiak@feec.vutbr.cz

Abstract: This article deals with the impact of active scanning on industrial networks. The impact on industrial networks is commented from the perspective of the penetration tester methodology. This topic is important because active scan tools are affordable and easy to use, and their intrusive impact on industrial devices can be critical. The article's main goal was to evaluate the impact on the industrial network from the penetration tester point of view using the most popular tools for active network scanning. In order to demonstrate and evaluate the results, an industrial testbed based on real industrial hardware was built for the article. The article also demonstrated how to use the information obtained by scanning for a Denial of Service attack.

Keywords: ICS, scanning, Nmap, Zmap, PLC, DoS, HMI

1 INTRODUCTION

Network scanning allows visualizing the network configuration and communication infrastructure. Network reconnaissance, whether an active or passive scan, is a significant part of cybersecurity. By scanning, it is possible to get an overview of the network and identify possible security holes. It is one of the fundamental pillars of cybersecurity, and it is the essential skill of a penetration tester. From the point of view of the penetration tester, the methodology, according to Certified Ethical Hacker (CEH) [1], contains seven steps:

1. **Check for live systems:** The step of determining which hosts are active on the network.
2. **Check for open ports:** The detected IP addresses are used to search for open ports.
3. **Scan beyond Intrusion Detection System (IDS):** Avoid detection from IDS.
4. **Perform banner grabbing:** Gathering information about running services on hosts.
5. **Scan for vulnerabilities:** Use the information from the scan to examine vulnerabilities.
6. **Draw network diagrams:** Reconstruct the network architecture.
7. **Prepare proxies:** Due to anonymity.

However, there is a problem with scanning industrial networks. Unlike conventional IT networks, industrial networks face security risks in these scanning procedures. This is due to the use of communication-sensitive industrial equipment and their configuration, where the emphasis is on a real-time operation. Network scanning can cause a complete failure of a Programmable Logical Controller (PLC) or increase the time delay, leading to unexpected situations in the process. An example is a robotic arm process. In this process, a slight delay means that the whole process can get into an unexpected or even dangerous situation. The solution may be to use security measures such as IDS, firewalls, and anti-malware as in IT networks. However, due to their nature and specific operating systems, this is not easy for industrial devices.

The key aim of this article is the impact of the behavior of active scanners in industrial networks. This behavior is described from the point of view of a penetration tester. The article demonstrates

the possibilities in scanning industrial networks and what impact his reconnaissance may have. It also demonstrates the possibility of using information obtained from scanning to perform a Denial of Service (DoS) attack. The following list details the main contributions of the article:

- Impact of active scanning on industrial networks.
- Impact assessment based on behavior according to the penetration tester methodology.
- Demonstration of a DoS attack based on the information obtained from the reconnaissance.

The article is structured as follows: The introduction outlines the issues and summarizes related works status. The following chapter describes the difference between passive and active scanning and the active scanning tools used for work. The next chapter deals with the description of the testbed environment. In conclusion, the results obtained by the performed experiment were evaluated.

1.1 RELATED WORKS:

The number of articles dealing with the possible impacts of scanning tools on industrial networks is minimal. The methodology for searching and selecting articles dealing with this issue was as follows: During the 9th of March 2021, a final set of keywords (*"Industrial control system*" AND (Reconnaissance or scan*)*) was used to query Scopus and Web of Science (WoS). This query identified 81 articles for Scopus and 52 for WoS. The results duplicates from databases were removed. After that, the systematic literature review identified a total of 15 articles. Only three articles [2, 3, 4] dealt with the issue of scanning in more depth, and only one [3] of them dealt with the impact of scanning on the industrial networks.

2 NETWORK SCANNING

According to Bou-Harb et al. [5] network scanning can be divided into three different categories: (1) Nature of cyber scanning, (2) Cyber Scanning Strategies, (3) Cyber Scanning Approaches. This article focused on the first category, on the division of scanning into passive and active.

- **Passive scanning:** Identifies network services by monitoring the traffic generated by servers and clients as they pass through the observation point. Specialized hardware, software, port mirroring, or hardware taps can be used. Alternatively, specialized software can be used. An example of the most commonly used passive scanning software is Wireshark.
- **Active scanning:** It identifies devices in the network by sending probe packets and then monitors the individual hosts' responses. An example of a probe packet might be a typical TCP handshaking procedure for establishing a connection. With the active scanning, information about the operating system can be obtained thanks to fingerprinting and possible processes and applications running on the hosts.

Thus, active scanning can provide information about open ports and whether these ports are protected. The main disadvantage of active scanning is that it is very intrusive because it requires the device's responses. This creates a problem when scanning industrial networks where the devices are very sensitive. This scanning can be revealed thanks to IDS, which are not a standard part of industrial networks. In contrast, passive scanning's main advantage is that it is not intrusive and cannot be detected by a third party. Within passive scanning, it is also possible to find out more information about what is happening on the network, especially since it can be turned on for a very long time without any detection. The main disadvantage of passive scanning is that it detects only active services. The article further deals only with active scanning.

2.1 TOOLS FOR ACTIVE SCANNING

Two prevalent open-source tools for active network scanning (Nmap and Zmap) were chosen for the article. The selection emphasized open-source applications as well as their documentation and popularity. To demonstrate how easy and affordable these tools are to use.

- **Nmap:** It is one of the most widely used active scanners in the world of penetration testers and attackers. Supports several types of scanning such as TCP-SYN Scan, Service Detection Scan, HTTP Banner Grab.
- **Zmap:** is a fast single packet network scanner designed for Internet-wide network surveys. Supports TCP-SYN Scan, ICMP Ping Sweep, NTP Scan.

3 TESTBED

To examine the impact of active scans on the industrial network, a testbed was created on real industrial hardware. The diagram of the testbed and communication architecture see in the Figure 1. Due to the fact that this problem concerns industrial equipment and elements in industrial networks in general, and also in order not to demonstrate vulnerabilities to a particular manufacturer, the description of the equipment and the scheme are described in general.

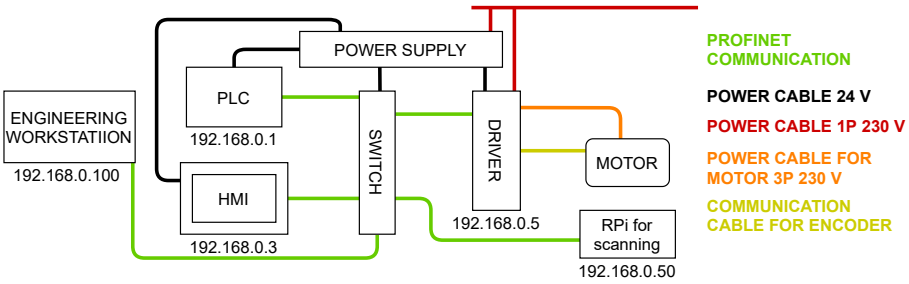

Figure 1: Scheme of industrial control system network tesbed.

The engineering workstation station is used for communication with devices, analysis, and supervision. It is also used to update processes and programs running on the devices. The PLC is a control unit for the entire network and provides the logic of its work. If the PLC communication is affected, the whole network is disrupted either by increasing the delay, significantly impacting the final process or a complete outage. There is also a Human Machine Interface (HMI) in the network with which the operator can monitor and make changes in the network's operation so that he does not have to access the engineering workstation, which is often elsewhere. The demonstration of the process output was servomotor with an encoder chosen. For this servomotor to work, a servo driver directly designed for this engine is connected to it. Servodrive is a frequency converter that enables communication with the PLC. The individual parts are connected using an industrial switch. The whole testbed is powered by a DC source with 24 V output and 5 A. The Raspberry Pi was used as an scanning device.

4 IMPACT OF ACTIVE SCANNING ON THE INDUSTRIAL NETWORK

The network's scanning will be described from the penetration tester point of view, and the impact on this network will be commented. The Nmap and Zmap tools have been selected for active scanning. First, the individual tools were tested to see how significant intrusive impact they would have.

4.1 ZMAP

During the initial test, it was found that the Zmap tool has a very intrusive impact on the entire network. The command was used to test the scan: *sudo Zmap -p 102 -N 100*. As can be seen

in Figure 2, this command disabled the PLC communication, and therefore, it is not possible to scan an industrial network at all with this scanning tool.

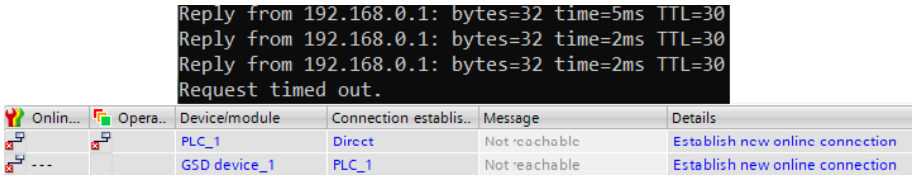

Figure 2: PLC communication failure.

4.2 NMAP

Scanning with Nmap had no as much intrusive effect. Therefore, a possible procedure of the penetration tester (described in the introduction) in the industrial network and what this procedure can have an impact is demonstrated here.

1. **Check for live systems:** The command *Nmap -sP 192.168.0.0/24* was used to search for live devices, and all devices were detected. Most attempts went without a harder impact on the network, but in one case out of many, the PLC communication failed, and therefore, the other devices stopped working.
2. **Check for open ports:** The command *sudo Nmap -sS -p- 192.168.0.0/24* was used to search for open ports. In most cases, it was not possible to capture the servo driver at .05. One of many attempts was to disrupt communication. Mostly without impact. To get more information, the -v (verbose) flag was used, so the *sudo Nmap -v -sS -p- -T5 192.168.0.0/24* command was used. At speed T5, the network usually remains stable. However, if the T4 speed is set or the targeted scan is directly on the device, more frequent outages occur. If there is no outage, there is a significant delay. The error messages are the same as for the Zmap scan.
3. **Scan beyond IDS:** This step was not necessary.
4. **Perform banner grabbing:** For gathering more information, the operating system detection command (*sudo Nmap -O*) was tested. The individual IP addresses were gradually tested. It was not possible to obtain operating system information from industrial devices. There was not a single network outage during this testing.
5. **Scan for vulnerabilities:** From the information obtained, it was possible to identify the devices in the network partially. It was possible to identify open ports on devices and some processes. It was also found that there is an open port 102 on which the iso-tsap process was running, which is vulnerable to a DoS attack.
6. **Draw network diagrams:** From the obtained information, it was possible to create a reconstruction of the network architecture.
7. **Prepare proxies:** This step was not necessary.

4.3 DOS DEMONSTRATION

From the information obtained, it was possible to test the DoS attack. The attack was aimed at the HMI device to demonstrate how the device can be loaded with queries, and it is then unable to respond. Due to this fact, the operator is then not able to control the network using the HMI. A program called hping3 was chosen to demonstrate the DoS attack.

A packet flood was sent to the HMI 192.168.0.3 using the command: *sudo hping3 -V -c 200000 -d 150 -S -p 120 —flood 192.168.0.3*. As a result, the device was taken out of service for the time of sending packets, and it was not possible to control the running of the servo motor with it. After the attack ended, the state returned to its original state, and it was possible to control the servo motor again using the HMI. Evidence of failure can be seen in Figure 3.

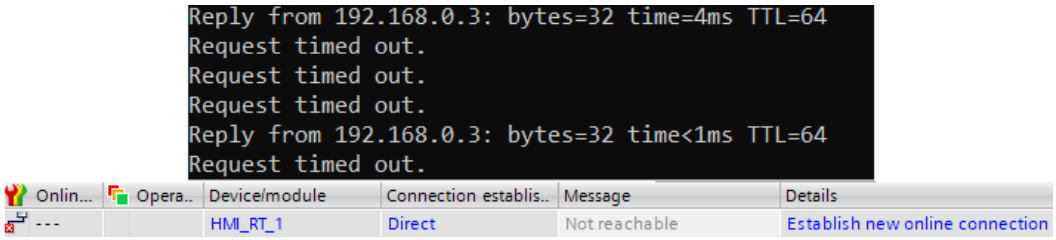

Figure 3: HMI communication failure.

5 CONCLUSION

It can be seen from the results in the article that it is not appropriate to use active network scanners for scanning industrial networks. The first described tool Zmap was very intrusive for the network communication. The impact on the device was with each attempt to scan. The second described tool was Nmap. This tool did not have as significant an intrusive impact as Zmap. For this reason, the procedure of a penetration tester methodology was demonstrated on this tool. In step 1) Check for live systems; a communication failure was detected in only one of 40 attempts. In step 2) Check for open ports; the impact was more significant, especially when using the -v (verbose) flag. The article also was demonstrated how to gather information. With this informations, a DoS attack was performed on the HMI. As a result, the operator was not allowed to control the device using this terminal. It is not advisable to use active scanning tools to improve security (gathering information about open ports and information about devices) in a real industrial network. From the network administrator's point of view, for the reasons mentioned above, it is better to switch to long-term passive scanning from which more information can be found.

ACKNOWLEDGMENT

The described research is part of the grant project registered under no. FV40366 and funded by the Ministry of Industry and Trade of the Czech Republic.

REFERENCES

[1] WALKER, Matt. 2019. *CEH Certified Ethical Hacker All-in-One Exam Guide*. 4th ed. New York: McGraw-Hill Education.

[2] TAMURA, Kensuke and Kanta MATSUURA. 2019. Improvement of Anomaly Detection Performance Using Packet Flow Regularity in Industrial Control Networks. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences: Special Section on Cryptography and Information Security*. 2019 (E102.A), 65–73.

[3] COFFEY, Kyle, Richard SMITH, Leandros MAGLARAS and Helge JANICKE. 2018. Vulnerability Analysis of Network Scanning on SCADA Systems. *Security and Communication Networks*. 2018, 1–21.

[4] ANTROBUS, Rob, Benjamin GREEN, Sylvain FREY and Awais RASHID. 2019. The Forgotten I in IIoT: a vulnerability scanner for industrial internet of things. *Living in the Internet of Things (IoT 2019)*. Institution of Engineering and Technology, , 1-8.

[5] BOU-HARB, Elias, Mourad DEBBABI and Chadi ASSI. 2014. Cyber Scanning: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials* [online]. 16(3), 1496-1519.