Vulnerabilities and Methods of Unauthorized Gaining Access to Video Surveillance Systems

Tetiana Vakaliuk[1,2,3], Dmytro Talchenko[1], Viacheslav Osadchyi[4], Yelyzaveta Bailiuk[1], and Oleksandra Pokotylo[1]

[1]Zhytomyr Polytechnic State University, 103 Chudnivsyka str., Zhytomyr, 10005, Ukraine
[2]Institute for Digitalisation of Education of the NAES of Ukraine, 9 M. Berlynskoho str., Kyiv, 04060, Ukraine
[3]Kryvyi Rih State Pedagogical University, 54 Gagarin ave., Kryvyi Rih, 50086, Ukraine
[4]Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine

Abstract

The article discusses vulnerabilities and ways of gaining unauthorized access to video surveillance systems. With the help of the analysis, the main shortcomings in the protection of IP video surveillance systems were identified; possible methods for implementing attacks on such systems were identified using the example of Hikvision IP cameras. The search for vulnerable IP video systems can be divided into two categories: manual and automatic. Each of the methods was demonstrated using specialized software: manual—using the Shodan search engine, automatic—using KPortScan, RouterScan, and IVMS-4200. The analysis of the results of the study was carried out, and the main vulnerabilities and methods for their avoidance were identified.

Keywords

Vulnerabilities; video surveillance systems; IP cameras; unauthorized access

1. Introduction

News about unauthorized access to computer systems has ceased to be unusual, but with the gradual replacement of analog video surveillance with digital, functioning as part of a network, the question arose: how protected are IP cameras from unauthorized access? Therefore, it is important to know how IP cameras from different manufacturers are attacked to ensure that video surveillance systems are properly protected.

1.1. Theoretical Background

An analysis of studies on this topic has shown that there are many ways to gain unauthorized access to an IP video surveillance system due to a large number of vulnerabilities. In particular, an article by Brian Cusack and Zhuang Tian [1] tested the GeoVision GV-FD220D 2MP H.264 IR fixed dome IP camera for security vulnerabilities. Although the methods of using the code and walking through the directory were rejected, many other vulnerabilities were discovered as a result. The two camera system entry points were open and accessible through Windows Explorer or the GeoVision DMMultiView client. The password was easily cracked into the system due to the factory default setting and the GvIP Device Utility gained control access to the IP camera. A more complete study of the entire video surveillance system showed the scope of several tools and the possibility of profiting from unauthorized access to critical information. In addition, the necessary countermeasures were given to protect the IP camera from hacking and the use of communication resources. The study found that IP cameras are vulnerable to exploitation, and the authors advocate a more urgent distribution of countermeasures.

The work of Naor Kalbo, Yisroel Mirsky, Asaf Shabtai, and Yuval Elovici [2] considered the security of modern video surveillance systems. Initially, an overview of the security of these systems was presented along with their

CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine
EMAIL: tetianavakaliuk@gmail.com (T. Vakaliuk); dimatalchenko2001@gmail.com (D. Talchenko); v.osadchyi@kubg.edu.ua (V. Osadchyi); liza.bailiuk@gmail.com (Y. Bailiuk); a.a.polish4uk@gmail.com (O. Pokotylo)
ORCID: 0000-0001-6825-4697 (T. Vakaliuk); 0000-0002-7961-0076 (D. Talchenko); 0000-0001-5659-4774 (V. Osadchyi); 0000-0002-4961-7816 (Y. Bailiuk); 0000-0002-1587-235X (O. Pokotylo)

components. Using this information, the authors determined the attack surface of the system, consisting of attack agents, vulnerabilities, actions, and consequences. This information has been used to illustrate several attack vectors. After describing the attacker's capabilities, the authors summarized recent research on countermeasures and best practices that can be applied to better secure IP-based video surveillance systems. The review concluded with a discussion of the threat horizon and proposed future work in this area. As such, this study has provided the reader with a better understanding of the attack surface and recent advances made by both attackers and those involved in video surveillance security over the past ten years.

Research by Vennam, P., Pramod T. C., Thippeswamy B. M., Yong-Guk Kimn, and Pavan Kumar B. N. [3] includes various types of attacks on camera-based video surveillance systems along with precautions. The current developments in authentication methods to prevent various attacks are described. Most of the considered methods tried to ensure the security and methods of processing the video stream in video surveillance systems and smartphones. It has been determined that the existing security methods such as firewalls, access control, and IDS/IPS available to the public safety net may not be entirely suitable for these environments. Mitigating vulnerabilities and attacks require modern security, tools, and techniques.

The work of Topchey N.V. and Belevskaya A.S. [4] identified the main types of threats to video surveillance systems. In addition, the authors noted that video surveillance systems can be used not only to solve technical problems but also to organize the business processes of enterprises and organizations. The very principle of operation and the advantages of using such systems were also described. The important point discussed in the article is that it is necessary to ensure the security of not only the video surveillance systems themselves but also the entire infrastructure of an enterprise or organization as a whole since only one weak point is enough for attackers to gain access to the entire system. Particular attention in this work was paid to recommendations for protecting Wi-Fi wireless networks.

A study by Costin A. [5] conducted a systematic review of existing and emerging threats in CCTV, CCTV, and IP cameras based on publicly available data. A set of recommendations was also provided to help improve the level of security and privacy provided by hardware, firmware, network communications, and video surveillance systems.

In an article by Johannes Obermaier and Martin Hutle [6], a study was made on compliance with privacy requirements in the video surveillance market. The authors considered two attacker models and tested the cameras for weaknesses. The security implementation was also redesigned and a vulnerability was identified in every system tested.

Deeraj Nagothu, Jacob Schwell, Yu Chen, Erik Blasch, and Sencun Zhu [7] investigated a real-time frame duplication attack. The feasibility of spoofing live video streams as the camera environment changes has been demonstrated. Also proposed is a technique for detecting such attacks using a real-time power grid frequency (ENF) reference database for the corresponding grid frequencies.

An article by Balasubramanian Muthusenthil and Hyun Sung Kim [8] provides a 360-degree view of evaluating various video surveillance systems of the recent past and present. In addition, an attempt was made to compare different video surveillance systems with their operational capabilities and attacks on them. Several future directions of research in the development and implementation of video surveillance systems were also presented.

A study by Hyungheon Kim, Youngkyun Cha, Taewoo Kim, and Pyeongkang Kim [9] identified various types of security threats that can arise from a cloud-based surveillance system and eliminate the risk of breaching privacy and personal information. A hierarchical cloud-based video surveillance system has also been proposed that takes into account security in the 5G network.

During the analysis of publications devoted to this topic, it was found that they paid little attention to the tools themselves for obtaining unauthorized access to video surveillance systems, which is an important element in ensuring the protection of such systems from intruder attacks. In addition, the vulnerabilities considered in these studies are limited. In this article, in addition to the analysis of the vulnerabilities of video surveillance systems, specialized search engines for vulnerable IP video systems are presented manually and implementations of hacking video systems by an automatic method using special software are demonstrated [10–13].

1.2. Research Methods

To achieve the set goals, the analysis method and the empirical method were chosen. Using the analysis, the vulnerabilities of IP video surveillance systems were identified, and possible methods for implementing attacks on such systems were identified. In addition, a manual search for vulnerable video surveillance systems was performed using the Shodan search engine. An automatic search for vulnerable IP video systems was also performed using tools such as KPortScan, RouterScan, and IVMS-4200.

The **purpose** of the article is to study various types of vulnerabilities and methods of unauthorized gaining access to IP video surveillance systems using the example of Hikvision brand IP cameras using specialized search engines and programs designed for port scanning.

2. Results

IP video surveillance systems are designed to be viewed by authorized users only. But if they are not properly protected, then anyone can access and use someone else's confidential information for their purposes. An IP camera is protected from hacking by three parameters: its IP address, username, and account password. It is these data that are needed to display the IP camera on a PC monitor.

When attacking video surveillance systems, an attacker can have the following goals:

1. Violation of confidentiality—unauthorized access to video content, user credentials, and network traffic. In this case, the attacker intends to view the video material for selfish purposes. As a result, this target endangers the confidentiality and physical safety of the premises.
2. Violation of integrity—manipulation of video content or active interference with secure channels in the system (for example, POODLE SSL downgrade attack). In this case, the attacker intends to change the content of the video (either at rest or during transmission). Changes can include freezing a frame, repeating an archived clip, or inserting other content. This misinformation can lead to physical harm or theft. An attacker can compromise the integrity of the system for purposes not directly related to video content. For example, an attacker may aim to exploit system vulnerabilities to gain access to internal assets. The system can be used as a "stepping stone" to gain access to internal assets such as:
   a) Intranet-Surveillance systems (especially closed systems) can be connected to an organization's intranet for control purposes. An attacker can use this to gain access to an organization's internal assets.
   b) Users of the system can become the target of an attacker. For example, an attacker may aim to install consumer software on a browsing terminal or steal personal user accounts.
   c) Botnet recruitment. A "bot" is an automated process running on a compromised computer that receives commands from a hacker via a control server. A collection of bots is called a "botnet" and is commonly used to launch DDoS attacks, mine cryptocurrencies, manipulate online services, and perform other harmful activities. An example of a botnet that infects IP cameras and DVRs was the Mirai malware botnet. In 2016, the Mirai botnet generated a 1.1 Tbps DDoS attack on websites, hosts, and service providers. Another example is a worm called Linux. Darlloz targeted and exploited vulnerable devices due to a PHP vulnerability (CVE-2012-1823).
3. Violation of availability is a denial of access to saved or live video channels. In this case, the attacker's goal is to turn off the feeds of one or more cameras (hide activity), delete stored video content (remove evidence), or launch a ransomware attack (make money). For example, the attack on the Washington tracking system in 2017 [10].

The video surveillance system usually comes with a default username and password. And often, consumers leave this data unchanged until the first hack occurs. True, some manufacturers of video surveillance equipment force you to change the password the first time you connect the device. At the same time, the system analyzes the given password for efficiency and often requires the use of a combination of numbers and letters in different registers, which causes user dissatisfaction. But such a framework has a positive effect on security and allows you to give access to information to those who are allowed to.

Depending on the manufacturer, some cameras (for example, Samsung) do not allow you to leave the factory password at all, and Axis cameras allow the owner to choose whether to set a new

user password or stop at the usual pass. As a result, lazy owners and administrators of video surveillance systems put their information at great risk.

Dahua generally offers the well-known combination “admin/admin”, and in some models of DVRs, including the latest generation equipment, there is no way to change this login and password. Not to mention that their IP cameras have two accounts (one of them with administrator rights) that cannot be deleted (these are 666666/666666 and 888888/888888).

The inattentive attitude of many manufacturers to the process of persuading users to change login data is, in principle, understandable. After all, if a person decides to install a video surveillance system to protect his property and life, then does he not take care of the security of the system itself?

Some network resources specifically publish complete lists of default logins and passwords for all popular brands of equipment [14]. This is an unobtrusive reminder to those who have not yet bothered to think about protecting their information.

The search for vulnerable IP video systems can be divided into two categories: manual and automatic. In the first case, the user searches for the IP address, login, and password himself, and this search should not go to random addresses, but only to those that have cameras.

In the second case, the user enters certain or random ranges of IP addresses into specialized software and hopes to find the address of CCTV cameras with a login and password there. This method practically does not require active user actions and can be performed in parallel with other processes. However, many of the IP addresses found will be inappropriate, or with a changed username or password.

The first method is more expedient but requires much more time. The user needs to find devices himself and, in some cases, use software vulnerabilities to find authorization data.

To implement the first method, a specialized search engine Shodan was used.

Shodan is a search engine that allows users to search for various types of network devices connected to the global Internet. Shodan is also described as a service banner search engine containing a set of metadata that the server sends back to its client. The metadata may contain information about the server software, the options supported by the service, and other information that the client must find out before interacting with the server (Figs. 1 and 2).

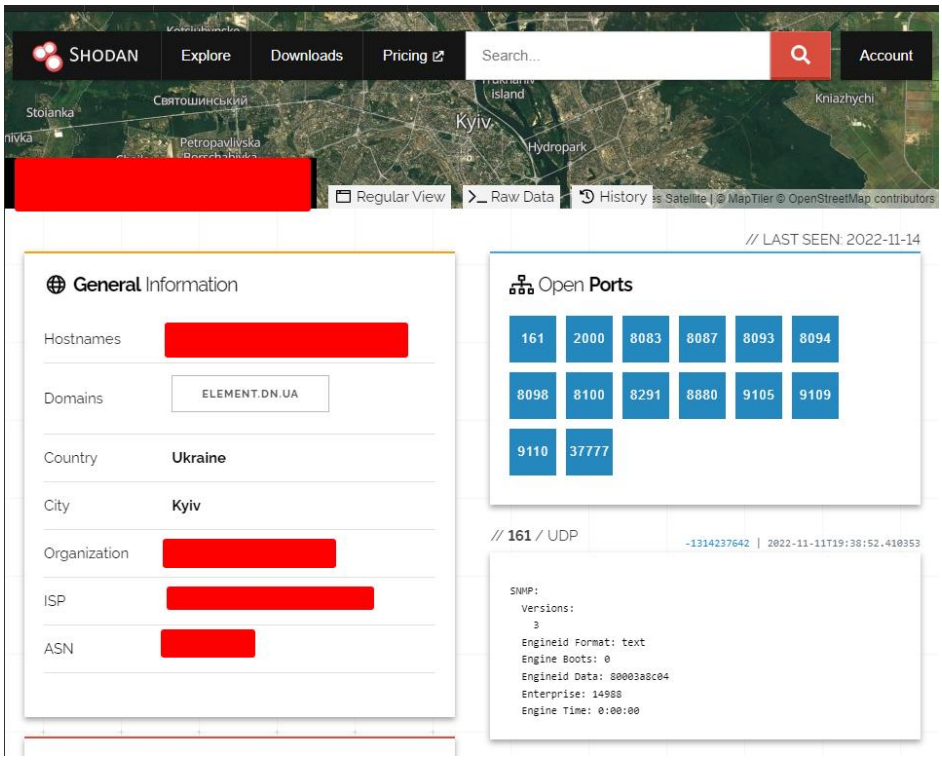

Figure 1: General view of the initial Shodan window

By building the right query, the search engine can find cameras with standard login and password, with specified vulnerabilities, etc. By entering a simple query to search for Hikvision IP cameras, Shodan found 3,095,840 devices worldwide (Fig. 3).

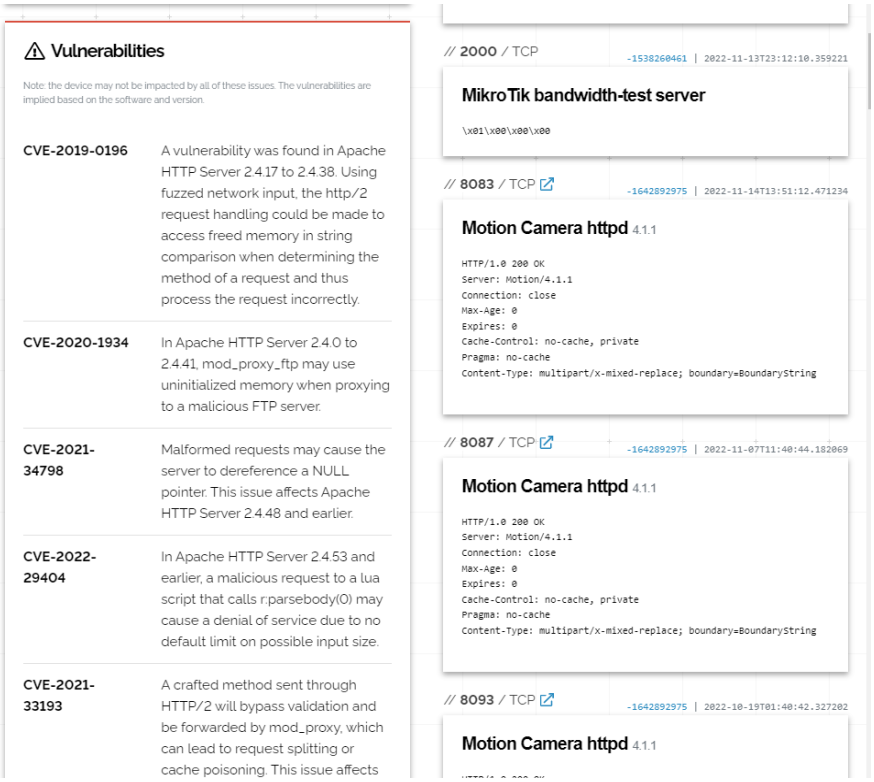

Figure 2: The list of data to be scanned

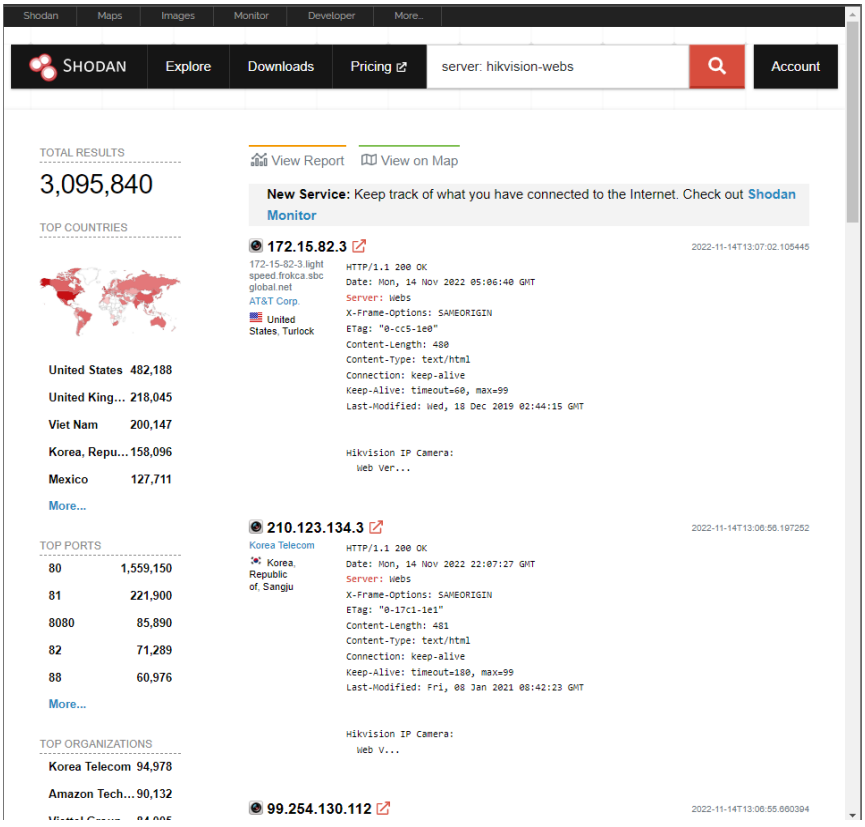

Figure 3: Hikvision Brand IP Camera Search Result

On the results page, you can see the directly found IP addresses, each of which you can click on and view the specific metadata of that device, the response from a specific device to a Shodan server request, and additional operators that help filter responses into the following categories: ports (Fig. 4), providers, operating systems, products, countries (Fig. 5).

The results show that for the selected query, port 80 ranks first, and Hikvision found the most in the US.

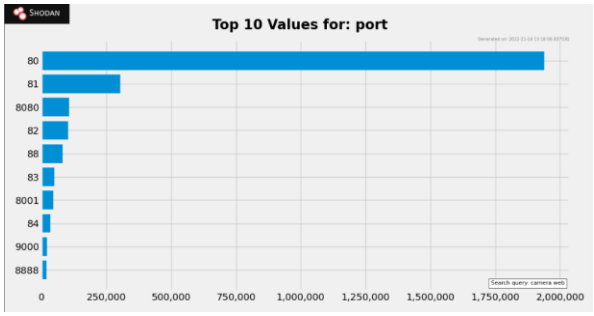

Figure 4: Result of filtering by ports

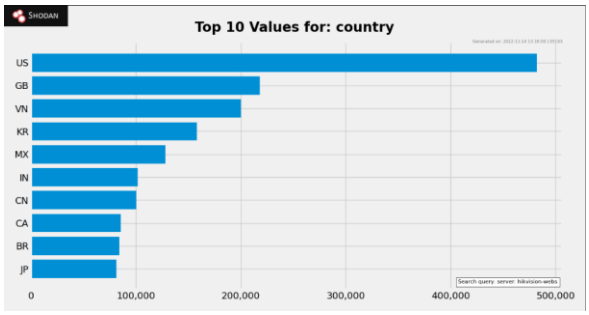

Figure 5: Result of filtering by countries

To implement unauthorized access to video systems by an automatic method, the following software was used:

- KPortScan—Software for scanning open ports by a range of IP addresses.
- RouterScan—Software for scanning, identifying, and connecting sorted IP addresses.
- IVMS-4200—Software for connecting to video systems.

To access IP video surveillance systems, you need to know the addresses and to get them, you can use available web resources, for example, https://4it.me/getlistip, where you only need to enter the search city. As a result, we get a part of the range of IP addresses of the city (Fig. 6).

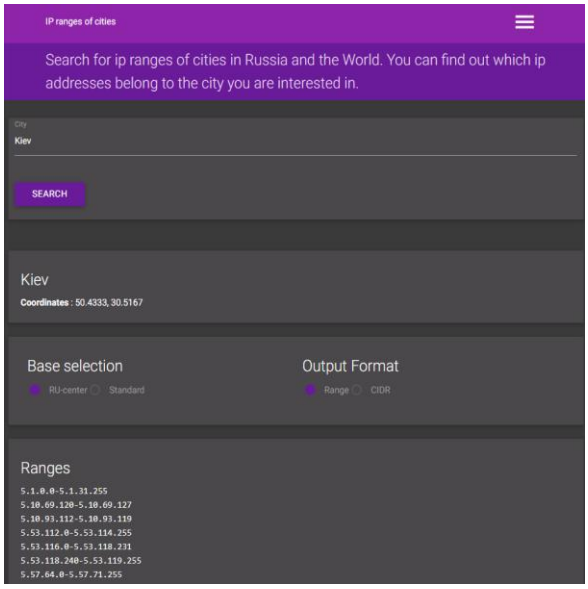

Figure 6: The result of the search for addresses in Kyiv

The next step is to copy the resulting range of addresses and add them to KPortScan by selecting the number of streams and port 8000 (Fig. 7).

After the scanning of addresses is completed, you can see the number of selected IPs and delete them from the created “result.txt” file, which is located next to the program. (Fig. 8).

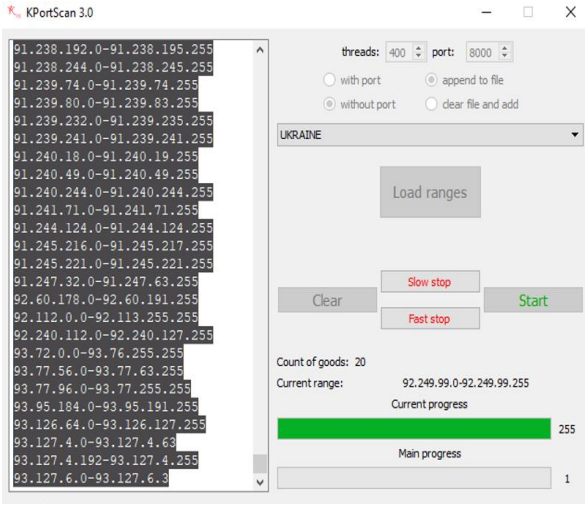

Figure 7: Search for specific IP addresses from specified ranges

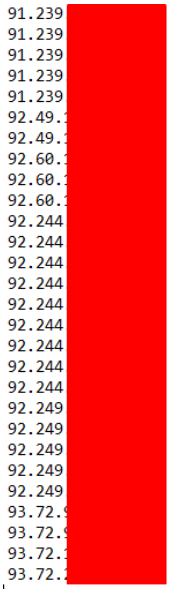

Figure 8: Found IP addresses

Having received a list of addresses, we add it to the Router Scan software, and scan through the corresponding ports, if necessary, changing the number of streams and the dictionary for selection (Fig. 9).

After scanning a small range of addresses, quite a lot of Hvision brand IP cameras were found, and even one with a weak login and password.

After a more detailed analysis and search of IP video surveillance systems in a part of the Kyiv address range, more than 1,500 thousand weakly protected and unprotected devices from various manufacturers were found, of which more than 300 were with standard and weak logins and passwords. Including the vulnerability factor of video surveillance software, we can conclude that the vast majority of cameras found are vulnerable due to outdated firmware updates (Hikvision CVE-2021-36260, Dahua CVE-2022-30563, etc.).

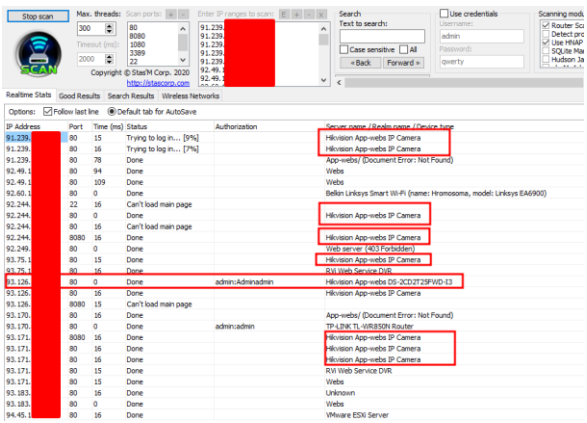

Figure 9: The result of scanning specific addresses with Router Scan

3. Conclusions

As a result of manual and automatic searches of IP video systems, many were found to have vulnerabilities that can be accessed in an unauthorized way. Knowing the IP address, port, login, and password, an attacker can connect to the video surveillance system using the IVMS-4200 software or a regular web browser. Without knowing the specified parameters, access to IP video systems can be obtained using other software, including those used for the study, but only if the default value has not been changed. Therefore, to avoid the threat of unauthorized access, it is necessary to change the login and password to complex ones and constantly update the firmware of your camera.

We see a deeper analysis of the vulnerabilities of video surveillance systems and the development of effective methods of protection against them as prospects for further research.

4. References

[1] B. Cusack, Z. Tian, Evaluating IP Surveillance Camera Vulnerabilities. Valli, 15th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, December 2017, 25–32.

[2] N. Kalbo, et. al., The Security of IP-based Video Surveillance Systems, Sensors, 20(17) (2020) 4806.

[3] P. Vennam, et. al., Attacks and Preventive Measures on Video Surveillance Systems: Review. Appl. Sci. 11 (2021) 5571.

[4] N. Topchii, O. Bilevska, Analysis of the Security of IP Surveillance Cameras, Scientific Journal "Scientific notes of TNU Named After V.I. Vernadskyi. Series: Technical Sciences", 32(71) 3 (2021) 157–161.

[5] A. Costin, Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations, 6th International Workshop on Trustworthy Embedded Devices. October 2016, 45–54.

[6] J. Obermaier, M. Hutle, Analyzing the Security and Privacy of Cloud-based Video Surveillance Systems, 2nd ACM International Workshop on IoT Privacy, Trust, and Security, May 2016, 22–28.

[7] D. Nagothu, et. al., A Study on Smart Online Frame Forging Attacks Against

Video Surveillance System, Sensors and Systems for Space Applications XII, 11017, 2019, 176–188.
[8] B. Muthusenthil, H. Kim, CCTV Surveillance System, Attacks and Design Goals. International Journal of Electrical and Computer Engineering, 8(4) (2018) 2072-2082.
[9] H. Kim, et. al., A Study on the Security Threats and Privacy Policy of Intelligent Video Surveillance System Considering 5G Network Architecture, 2020 International Conference on Electronics, Information, and Communication (ICEIC), January 2020, 1–4.
[10] Z. Hu, et al., Bandwidth Research of Wireless IoT Switches. In 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (2020). doi: 10.1109/tcset49122.2020.2354922
[11] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 222–233.
[12] S. Obushnyi, et al., Ensuring Data Security in the Peer-to-Peer Economic System of the DAO, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3187 (2021) 284–292.
[13] E. Bertino, N. Islam, Botnets and Internet of Things Security. Computer, 50 (2017) 76–79.
[14] Ethan Ace. IP Cameras Default Passwords Directory. IPVM. URL: https://ipvm.com/reports/ip-cameras-default-passwords-directory