Proceedings of IYSC, (2022), vol. 11

Journal homepage: http://journals.sdu.edu.kz/index.php/iysw

THE CONCEPT OF ANALYZING THE ARCHITECTURE OF THE SYSTEM AND MATHEMATICAL MODELS FOR ENSURING INTEGRATED SECURITY

N. Abdinurova[1], Y. Mukhamedkali[2], O. Baimuratov[3]

Suleyman Demirel University, Kaskelen, Kazakhstan

Proceedings of IYSC, (2022), vol. 11

Journal homepage: http://journals.sdu.edu.kz/index.php/iysw

2022 International Young Scholars' Conference

Abstract

Since the development of the Internet, humanity has stopped using real information data that is transmitted in a classical way, that is, printed or written on paper, which has increased the number of users, which, consequently, has increased the amount of data transmitted between users. Because of this, the number of both intentional and unintentional cyber-attacks has increased dramatically. With the development of technologies, people's privacy and confidentiality are increasingly vulnerable because of these cyber attacks. The article talks about the overall level of security and tries to define the general formula for organizations with Wi-Fi routers and network printers. The security level of each component is determined through penetration testing using open-source ethical hacking tools. Define math formula need to take into consideration several factors such as vulnerability, usage frequency, etc. This paper shows some ways to penetrate the organization's network and some recommendations are also given to improve the security of the local infrastructure of organizations.

Keywords: concept, security, structure, architecture, vulnerability

Introduction

With the development of technology, the number of users in the field of information technology and computer science has increased, which has caused a sharp increase in cyber threats and attacks on the Internet over the past few years. For the same reason, the topics of cybersecurity and protection have become more in demand and are relevant to this day. Data security of large and small companies has become vulnerable due to frequent cyber-attacks. Since the beginning of Covid 19, there have been more Internet users as a consequence of quarantine, as people at home were online more often and longer than ever before in history, as well as people who worked and communicated only on the basis of offline meetings switched to the remote option. Because of this fact, there are more potential victims for attackers. Organizations may have vulnerable points from different sides, such as being hacked from checkpoints (hardware components) or from software parts like Wi-Fi routers disabled or packets captured via Wireshark. All these attacks may lead to huge monetary losses. Therefore companies need a concept solution to these problems. This article discovers the architecture of one environment, scans all connected devices, and tries to find out vulnerabilities in order to construct a system for ensuring security.

Literature review

Learning-related works [1] showed that firewalls are leaky for attacks. Network Admission Control is an industry initiative that combines endpoint security technology, authentication, and network security and Network Access Protection is a Microsoft technology designed to control access to an enterprise network based on information about the system state of a connecting computer. However, as currently specified, they both assume that users are not malicious.

The report [2] of the National Institute of Standards and Technology discusses attack graph computation tools as a tool for organizing network security analysis. With the help of the attack graph, the security metrics of the system are more accurately calculated. The presented method of security analysis using an attack graph allows to minimize the risk of weakness and systematizes the approach of security analysis.

One more related article [3] discussed the integration of Enterprise Architecture

Management with Information System Security Risk Management based on The Open Group Architecture Framework (further TOGAF) tool. First, they analyzed key concepts and relations (structural and semantic correspondences) between TOGAF and International Symposium on Society and Resource Management (further ISSRM). After performing analysis and concepts with relations are summarised, the based ISSRM domain model added Enterprise asset management (EAM) concepts, and an integrated conceptual model EAM-ISSRM was created.

The main model of protecting the information reflects the processes of its protection in the form of interaction of a complex of destabilizing factors that directly affect information and its means of protection, and obstacles to their action. As a result of the application of this given model is the presence of a certain level of information security.

From the general model, a generalized model of the information security system follows as a continuation, which displays the main processes for rationalizing information security processes in the form of processes for the distribution and use of resources used in information protection.

Information structure of university system

The work started from learning enterprise networks architecture as a guest without being authorized somehow since the task was to check all vulnerabilities which can be compromised by third parties. The structure of the enterprise is shown in Fig.1.

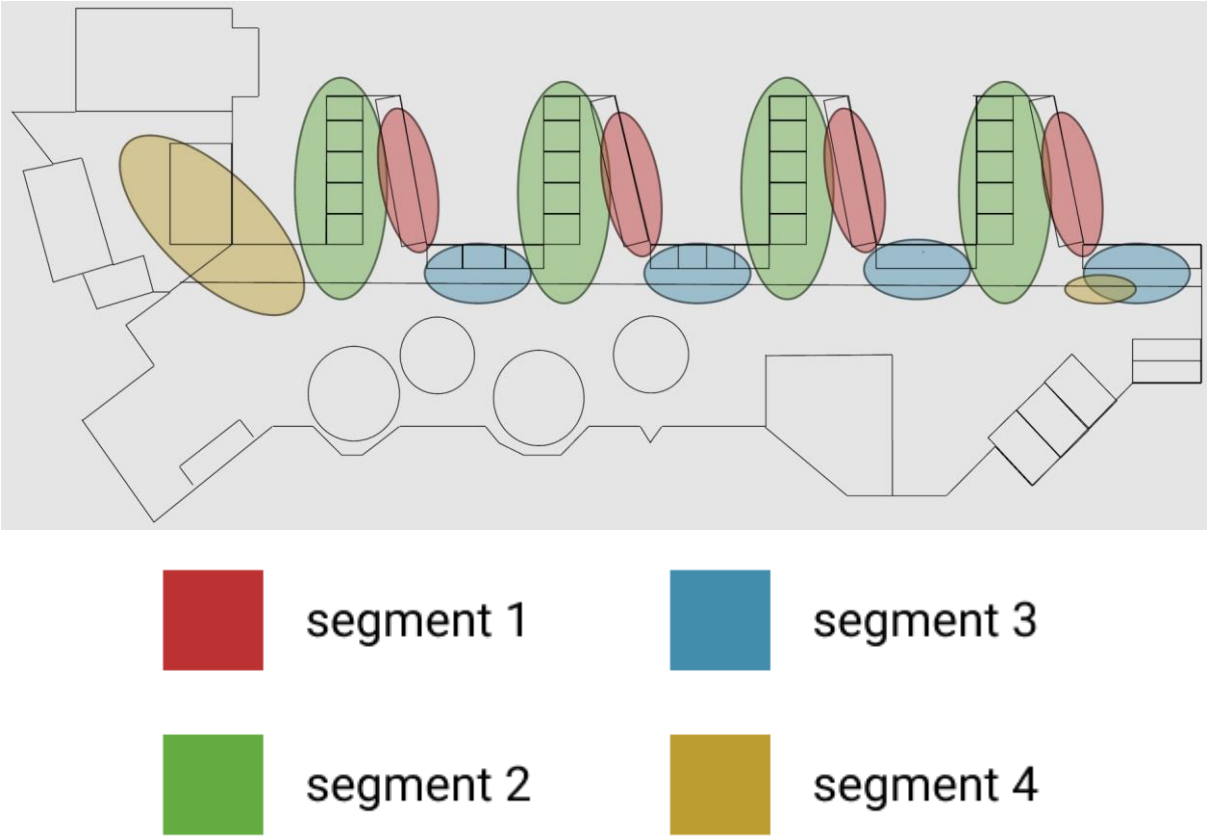


Fig.1. University Map

Visualization of the technological process

Nmap tool has been used to scan all devices connected to the internet. Nmap ("Network Mapper") is a free and open-source utility for network exploration and security auditing which was designed for fast scanning of large networks, although it does fine for single targets. Nmap uses raw IP packets in an ingenious way to determine which hosts are available on the network, what services (application name and version) they offer, what operating systems (and OS versions) they use, what types of packet filters/firewalls are in use, and many more. other characteristics. While Nmap is commonly used for security checks, many system administrators find it useful for common tasks such as monitoring network structure, managing service startup schedules and keeping track of host or service uptime.

Operating cycle of production

The task was to check the network organized within the walls of the university for vulnerabilities. To scan the local network, the Nmap utility was selected, in the Zenmap shell.

Before starting the scan, the device must be connected to the local network of the

university. This task was accomplished by borrowing an Ethernet cable installed on computers in regular classrooms. To set up a local connection, we needed data from the settings of the previously connected computer, which were protected by an "empty password". After a successful connection, we started working with Zenmap. As a result of scanning, 6 switches, 81 VLANs, and 132 devices were found. The number of devices may vary depending on the time of day. The most vulnerable among the devices were printers and faxes. Most of the most secure printers have been accessed through popular passwords such as "admin".

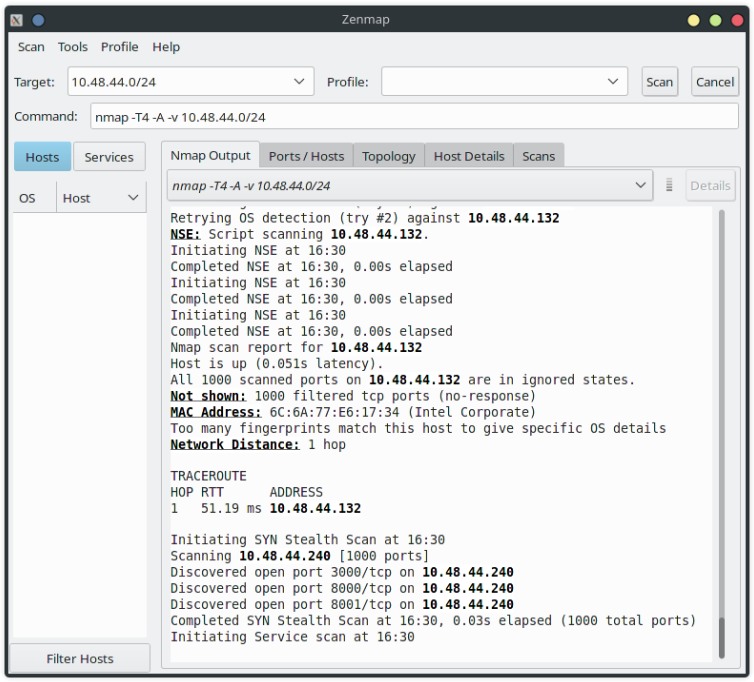


Fig.2. Zenmap tool

Scanned devices

Type of devices	*Number of devices*
Router	74
PC	39
Printer	15
Unknown	4

Table 1

Mathematical model of production

Mathematical models of the information security system act as an integral part of it in the form of a complex technical system. In order to fully solve the tasks of analyzing and synthesizing the information system, it is necessary to take into account a number of features that arise in this case, namely:

- the presence of a complex indirect relationship between the quality indicators of the information security system and the quality indicators of the information system;
- the need to take into account a number of indicators of information security tools when evaluating and choosing the most optimal protection option;
- significant interrelation and interdependence of these indicators, which are contradictory.

The presence of these features makes it almost impossible to use traditional mathematical methods, including methods of probability theory and mathematical statistics, optimization methods for solving applied problems of analysis, and synthesis of a complex information security system in modern data processing systems.

Methods and materials

Top vulnerabilities devices checked for

A - Brute Force - Remote print on found printer

Among the found printers were two types of printers: Konica Minolta, HP, and ImageRunner (Canon). After clicking on the IP address, we got to the authorization page.

Remote access was protected by default passwords, so it was easy to get into the settings. Among the settings, there were configurations that allow the printer to fail, including the function of printing one or another information about the printer, after which the printer also fails.

With the help of the Printer Exploitation Toolkit (PRET) malware, we can connect to the printer and launch the logger, as well as launch the physical damage script.

In the settings of ImageRunner, Canon, were found whole logs of the printing or printed queue. There were data such

Scanned devices

Section	*Number of devices*
Segment 1	42

Segment 2	50
Segment 3	22
Segment 4	18

Table 2

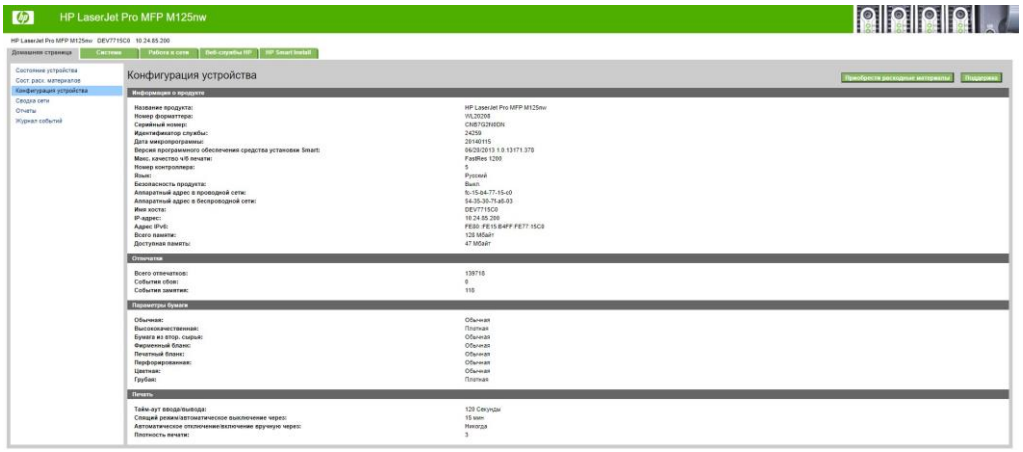


Fig. 3. HP printer settings

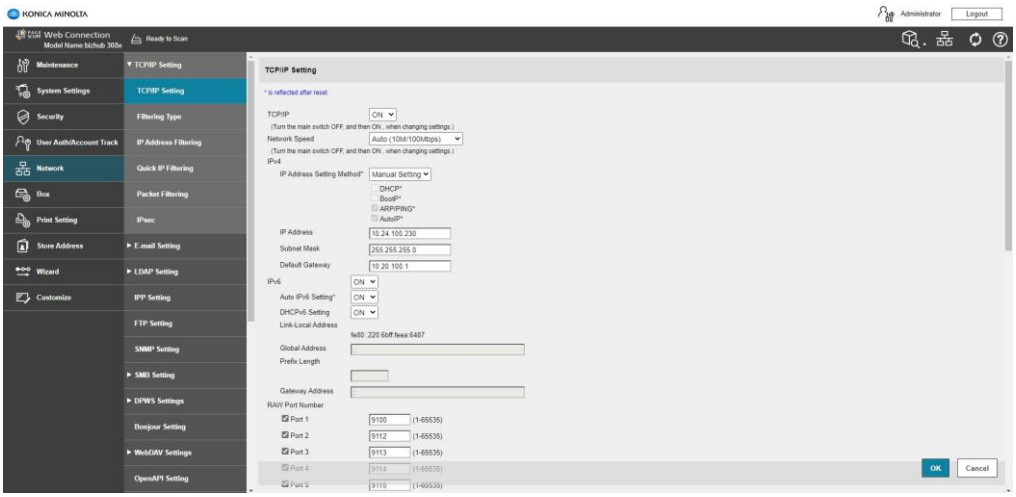
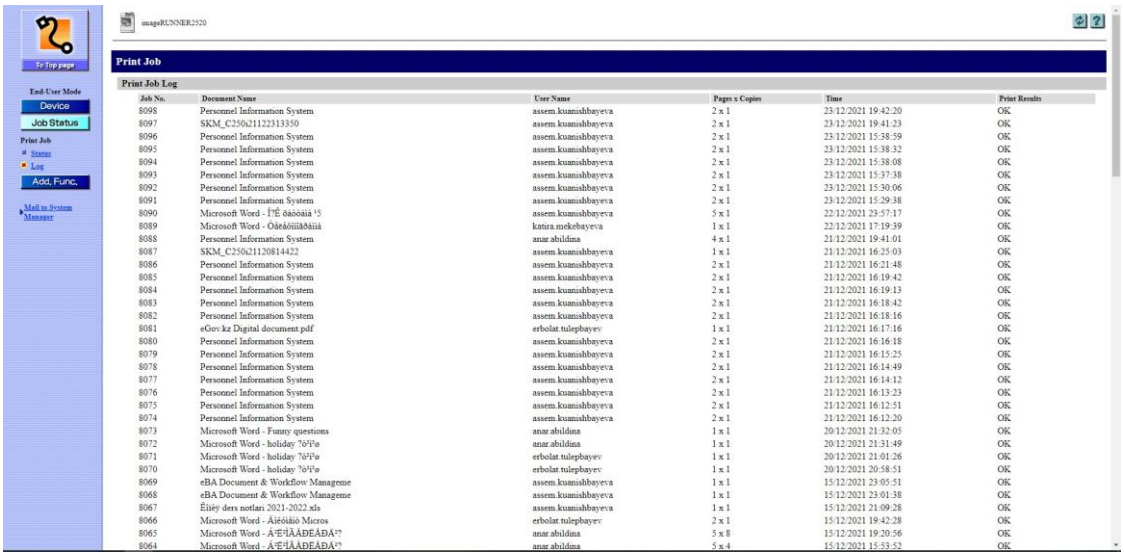


Fig. 4. Fatal settings

as document name, the user name (who sent the document to print), and time. Since the names of the document are input and general data, this component can be attributed to a data leak.



Print Job

Print Job Log

Job No.	Document Name	User Name	Pages x Copies	Time	Print Results
8098	Personnel Information System	assem.kuanishbayeva	2 x 1	23/12/2021 19:42:20	OK
8097	SKM_C250i21122313350	assem.kuanishbayeva	2 x 1	23/12/2021 19:41:23	OK
8096	Personnel Information System	assem.kuanishbayeva	2 x 1	23/12/2021 15:38:59	OK
8095	Personnel Information System	assem.kuanishbayeva	2 x 1	23/12/2021 15:38:32	OK
8094	Personnel Information System	assem.kuanishbayeva	2 x 1	23/12/2021 15:38:08	OK
8093	Personnel Information System	assem.kuanishbayeva	2 x 1	23/12/2021 15:37:38	OK
8092	Personnel Information System	assem.kuanishbayeva	2 x 1	23/12/2021 15:30:06	OK
8091	Personnel Information System	assem.kuanishbayeva	2 x 1	23/12/2021 15:29:38	OK
8090	Microsoft Word - Ï?Ë ðàòóâà ¹5	assem.kuanishbayeva	5 x 1	22/12/2021 23:57:17	OK
8089	Microsoft Word - Óâèäîìëåíèå	katira.mekebayeva	1 x 1	22/12/2021 17:19:39	OK
8088	Personnel Information System	anar.abildina	4 x 1	21/12/2021 19:41:01	OK
8087	SKM_C250i21120814422	assem.kuanishbayeva	1 x 1	21/12/2021 16:25:03	OK
8086	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:21:48	OK
8085	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:19:42	OK
8084	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:19:13	OK
8083	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:18:42	OK
8082	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:18:16	OK
8081	eGov.kz Digital document.pdf	erbolat.tulepbayev	1 x 1	21/12/2021 16:17:16	OK
8080	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:16:18	OK
8079	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:15:25	OK
8078	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:14:49	OK
8077	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:14:12	OK
8076	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:13:23	OK
8075	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:12:51	OK
8074	Personnel Information System	assem.kuanishbayeva	2 x 1	21/12/2021 16:12:20	OK
8073	Microsoft Word - Funny questions	anar.abildina	1 x 1	20/12/2021 21:32:05	OK
8072	Microsoft Word - holiday ?ò?í?o	anar.abildina	1 x 1	20/12/2021 21:31:49	OK
8071	Microsoft Word - holiday ?ò?í?o	erbolat.tulepbayev	1 x 1	20/12/2021 21:01:26	OK
8070	Microsoft Word - holiday ?ò?í?o	erbolat.tulepbayev	1 x 1	20/12/2021 20:58:51	OK
8069	eBA Document & Workflow Manageme	assem.kuanishbayeva	1 x 1	15/12/2021 23:05:51	OK
8068	eBA Document & Workflow Manageme	assem.kuanishbayeva	1 x 1	15/12/2021 23:01:38	OK
8067	Ëiíèý ders notlari 2021-2022.xls	assem.kuanishbayeva	1 x 1	15/12/2021 21:09:28	OK
8066	Microsoft Word - Áiéóíàio Micros	erbolat.tulepbayev	2 x 1	15/12/2021 19:42:28	OK
8065	Microsoft Word - Á'Ê¹ÍÅÅÐÉÅÐÁ*?	anar.abildina	5 x 8	15/12/2021 19:20:56	OK
8064	Microsoft Word - Á'Ê¹ÍÅÅÐÉÅÐÁ*?	anar.abildina	5 x 4	15/12/2021 15:53:52	OK

Fig. 5. Printer logs

B - Denial of Service - Disabling university routers

Using the aircrack-ng utilities, we tried to spam the authorization of university routers, thereby disabling one of the routers, so other devices were not able to connect to the router. When spamming the router, we were faced with the fact that it did not fail, which is due to the excellent protection of the router. However, we have bypassed this protection by increasing the amount of spam using different spam devices. Thus, by spamming through three devices, the router was incapacitated for a while.

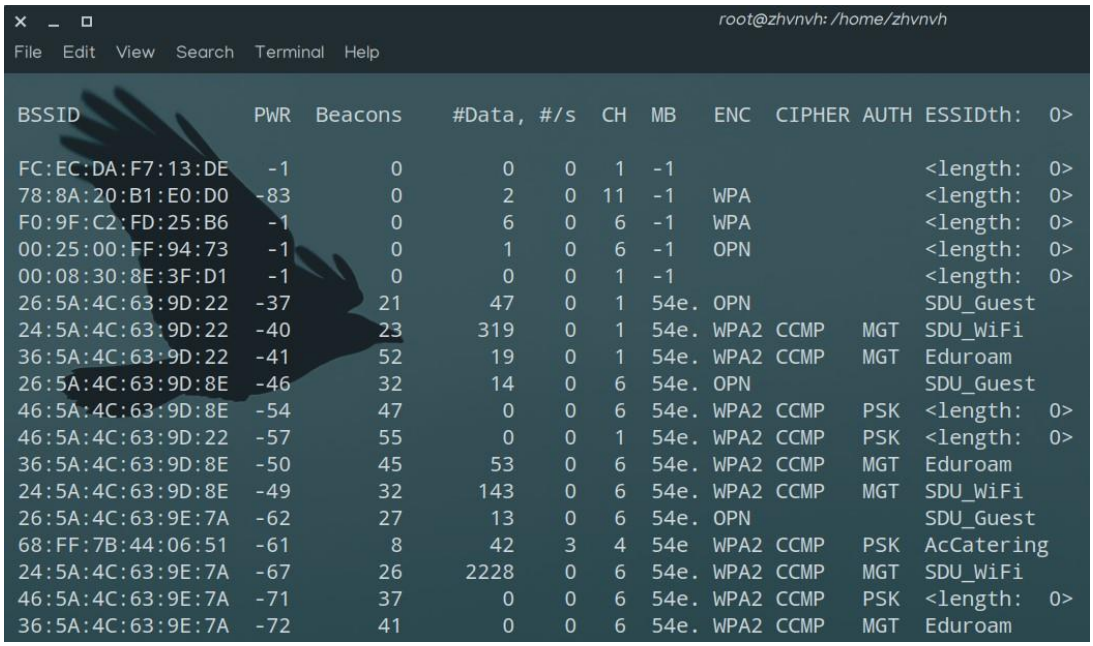


Fig. 6. Zenmap tool

Fig.7. Zenmap tool

Results

After quantitative research and scanning of all the found devices on the campus according to Fig.8 out of 100% the percentage of the devices as given: routers – 56.06%, personal computers – 29.55%, printers - 11.36%, and unknown devices - 3.03%. From the given information it can be concluded that routers of the university have a good level of protection against spam and cyber-attacks, even with success the situation is not so critical in general, since even if one router is overloaded (one router is equal to 1.75% out of 100%), the protection mode will work and the rest of the routers will continue working. But the situation is not the same with the printers. The printers on the campus are the most vulnerable devices because they are easy to be penetrated (it does not take a lot of effort to do this), and there can be leaks of information. Also, it can be added that losing one printer is losing 8.67% out of 100%, which is more critical.

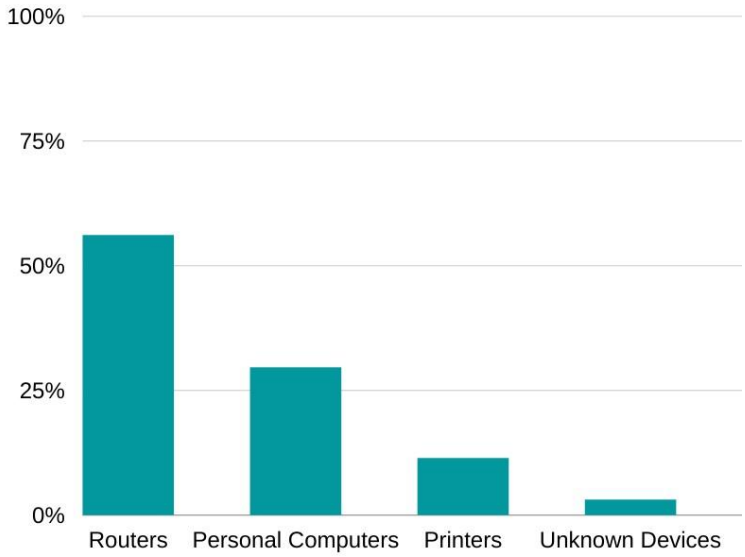


Fig. 8. Percentage of devices

Conclusion

All devices connected to the local network and having access to the internet have been scanned and analyzed. They have been divided according to their type, segment, and level of safety.

Information security is, first of all, a mechanism to ensure the state of protection of society and the state from the illegal and unauthorized use of information resources, thereby violating the information rights and freedoms of a citizen and a person.

The main goal of creating a comprehensive information security system is to achieve the maximum degree of effectiveness of its protection by simultaneously using the necessary resource base, models, and mechanisms that will prevent unauthorized access to protected information resources and ensure the physical safety of its material carriers.

References

1. Xia, H., Kanchana, J., & Brustoloni, J. C. (2005, May). Using secure coprocessors toprotect access to enterprise networks. In International Conference on Research in Networking (pp. 154-165). Springer, Berlin, Heidelberg.
2. Singhal, A., & Ou, X. (2017). Security risk analysis of enterprise networks usingprobabilistic attack graphs. In Network Security Metrics (pp. 53-73). Springer, Cham.
3. Mayer, N., Aubert, J., Grandry, E., & Feltus, C. (2016, November). An integrated conceptual model for information system security risk management and enterprise architecture management based on TOGAF. In Ifip working conference on the practice of enterprise modeling (pp. 353-361). Springer, Cham.
4. Yorozu, T., Hirano, M., Oka, K., & Tagawa, Y. (1987). Electron spectroscopy studies onmagneto-optical media and plastic substrate interface. IEEE translation journal on magnetics in Japan, 2(8), 740-741.
5. Young, M., & Howard, J. N. (1989). The technical writer's handbook: Writing with styleand clarity. Applied Optics, 28(22), 4952.