Astana IT University

**INDUSTRIAL INTERNSHIP REPORT**

6B06106 Cybersecurity

Yeldos Tazhenov

CS-2008

U-FUTURE LLP

Supervisor: Asem Temirbek

Nur-Sultan, 2022

Content

[**Introduction.** 3](#_Toc104473577)

[**Company.** 4](#_Toc104473578)

[**Goal.** 4](#_Toc104473579)

[**Main part.** 4](#_Toc104473580)

[**Process Explorer.** 5](#_Toc104473581)

[**SQL injection monitoring.** 8](#_Toc104473582)

[**Firewall rules and IDE signatures.** 10](#_Toc104473583)

[**OWASP ZAP.** 12](#_Toc104473584)

[**Conclusion.** 13](#_Toc104473585)

[**References.** 14](#_Toc104473586)

# **Introduction.**

Industrial practice is a necessary stage in the formation of students' required competencies. Its value lies in the acquisition of new and consolidation of already acquired knowledge. During the period of practical training, students should consolidate theoretical material, acquire practical skills.

Internship is a huge step for every student. During the practice, the student observes how a professional specialist works. Even if the practitioner does not perform the tasks set by the company, he is gaining experience, this experience can help in the future of a young specialist.

The main goal of any practice is experience. Experience should be accumulated so that after graduation a student can compete with former colleagues.

The internship gives the practitioner a chance to work at an unusual pace. This moral experience is very much in demand in any job. Stress resistance, competence are almost the main aspects that employers pay attention to.

The next goal is to help in the formation of useful relationships in the future. People who manage the internship process can act as assistants, providing useful information and providing good assistance in promotion. Since the company has seen the intern in action, the student can use it as a recommendation for a future job.

Practice is a step towards getting a job in the same company. In the process of studying, the student gets acquainted with people who work and teach him in this path. Mentors give their vision to the task received, and the practitioner can look at the problem from the other side, using the tips of a qualified employee (Vinay, 2021).

## **Company.**

The U-FUTURE LLP company is engaged in educational services. Headquarters in Nur-Sultan is located at st. Gaydar Aliyeva, 21. Subsidiaries such as Ustudy are involved in compiling and correcting tests for the Unified National Testing (UNT).

## **Goal.**

One of the goals of the cybersecurity specialists at U-FUTURE is to protect the data base, protecting the operating systems of office PCs, as they contain the confidential information of the entire company. Any information should be protected. The main goal of my internship was the protection of operating systems.

To prevent confidential information from leaking into the wrong hands, the company obliges everyone to sign a non-disclosure agreement.

Object of study: operating systems

Subject of study: structure, properties, security of operating systems.

The rapid development of information technology is engaged in the formation of a common environment, influencing all possible activities. However, with the advent of information technologies associated with their use, with consequences from the implementation of which did not happen before.

# **Main part.**

The main techniques for safeguarding computer processing are provided by operating systems. Operating system designers have been experimenting with ways to create "secure" operating systems since the 1960s. These are operating systems whose procedures safeguard the system from a motivated opponent. The importance of such security has recently become a mainstream problem for all operating systems. We look at historical research that describes the requirements for a secure operating system and research that implements sample systems that seek to meet those needs in this book. We observe that the complexity of software systems often resulted in implementation issues that we are still exploring to this day for system designs that attempted to satisfy these objectives.. (Jaeger T., 2008)

Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.  
OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised (Techopedia, 2022)

## **Process Explorer.**

Process Explorer is an application for monitoring processes in the system. Process Explorer is a program for real-time monitoring and control of the activities of various processes in the Windows operating system environment.

Изображение выглядит как стол

Автоматически созданное описание

Figure 1

Изображение выглядит как стол

Автоматически созданное описание

Figure 2

The program provides access to monitoring processes, and also allows you to kill them(Fig. 2).

Изображение выглядит как стол

Автоматически созданное описание

Figure 3

The Process Explorer program is able to analyze the process for viruses. This feature is useful for people who are not specialized in cyber security. This is an easy way to prevent (Fig. 3).

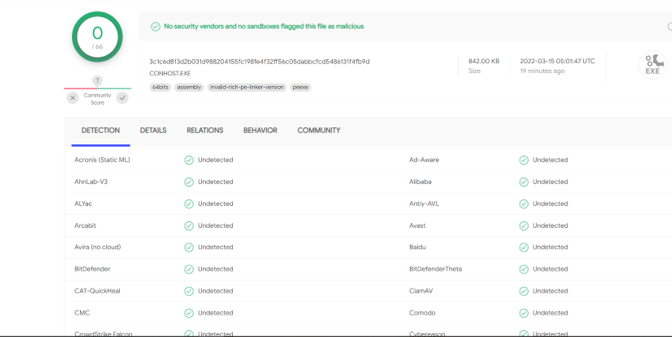


Figure 4

Information about the analysis is taken from the website offered by the program (Fig. 4).

## **SQL injection monitoring.**

Wireshark can be used for a variety of tasks, including diagnosing network performance issues. Wireshark is frequently used by cybersecurity professionals to trace connections, analyze the contents of dubious network transactions, and spot network traffic surges. It's an important aspect of any IT professional's toolset, and preferably, the IT expert knows how to use it.Изображение выглядит как стол

Автоматически созданное описание

Figure 5

Изображение выглядит как текст

Автоматически созданное описание

Figure 6

Изображение выглядит как текст

Автоматически созданное описание

Figure 7

In this case, it is presented that a SQL injection has been performed. With the help of the wireshark traffic analyzer program, it becomes possible to notice this.

## **Firewall rules and IDE signatures.**

In a secure production network, network alerts are generated by various types of devices such as security appliances, firewalls, IPS devices, routers, switches, servers, and more. The problem is that not all alerts are created equally. For example, alerts generated by a server and alerts generated by a firewall will be different and vary in content and format.

Изображение выглядит как текст

Автоматически созданное описание

Figure 8

Изображение выглядит как текст

Автоматически созданное описание

Figure 9

Изображение выглядит как текст

Автоматически созданное описание

Figure 10

Изображение выглядит как стол

Автоматически созданное описание

Figure 11

The packets pertaining to the traffic seen by the capturing NIC are stored in PCAP files. As a result, the PCAP is extremely valuable for retracing network activities like communication with malicious end points. PCAP analysis can be made easier with tools like Wireshark (Fig. 11)

## **OWASP ZAP.**

The OWASP ZAP web application security scanner is free and open source. It is intended for both novice application security testers and professional penetration testers..

Изображение выглядит как текст

Автоматически созданное описание

Figure 12

Изображение выглядит как текст

Автоматически созданное описание

Figure 13

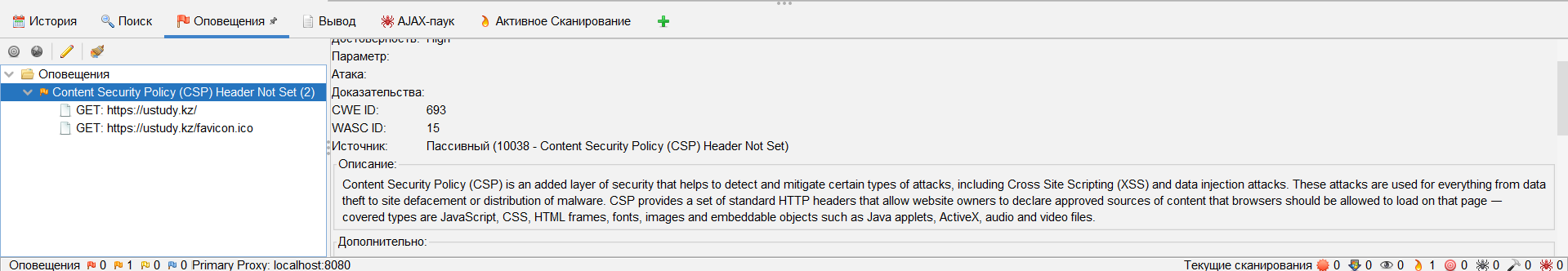


Figure 14

The history tab stores all analyzes of web applications. (Fig. 13)

The search tab helps you find the vulnerabilities you need.

The alerts tab stores all found vulnerabilities. (Fig. 14)

The output tab displays the comments of the action, works like a terminal.

OWASP ZAP encapsulates the program's functionalities (and more) in a single, intuitive, and efficient open source platform. ZAP is a sophisticated application security solution that has quickly become the industry standard for both manual and automated security scans. (we45, 2021).

# **Conclusion.**

Summing up, I can say that I learned a lot of new things in 2 months: I found new ways to protect my operating system, got information about snorts and firewall, got acquainted with tools such as wireshark and OWASP ZAP. Specialists working in the company instructed me, gave me additional knowledge. I upgraded my analytical and technical skills.

Also, I applied the acquired knowledge in practice. I am sure that this experience will help me in the future.

At the moment, I am still far from the professionals of my specialty, so I must often practice the acquired skills, adding new ones.

# **References.**

1)Vinay. (2021, November 15). *The importance of an internship*. Retrieved from Capital placement: https://capital-placement.com/blog/the-importance-of-an-internship-top-5-reasons-why-internships-are-critical/

2)Techopedia. (2022, March 31). *What is Operating System Security (OS security)? - definition from Techopedia*. Techopedia.com. Retrieved May 26, 2022, from https://www.techopedia.com/definition/24774/operating-system-security-os-security#:~:text=Operating%20system%20security%20(OS%20security)%20is%20the%20process%20of%20ensuring,malware%20or%20remote%20hacker%20intrusions.

*3)7 features that make Zap Great for Application Security Testing*. we45. (2021, June 4). Retrieved May 26, 2022, from https://we45.com/blog/7-features-that-make-zap-great-for-application-security-testing/

*4)What is wireshark and how to use it: Cybersecurity: Comptia*. Default. (n.d.). Retrieved May 26, 2022, from https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it

5) Jaeger, T. (2008). Operating system security. *Synthesis Lectures on Information Security, Privacy, and Trust*, *1*(1), 1–218. https://doi.org/10.2200/s00126ed1v01y200808spt001