Portfolio of my work in semester 4

*By Aleksandar Garkov*

Contents

1. Introduction
2. Learning outcomes
3. Personal Learning Activities
4. Overall Conclusion and Reflection

Introduction

The decision to sign up for the Cyber Security specialization was something that I had been thinking about for a long time. Being a Software Engineering student and developing different projects in the early semesters gave me a good ground knowledge of how an application is constructed and developed, but I didn’t know much about security. Being in a class with people experienced in infrastructure, Linux, and networking, was a goal because I wanted to get knowledge as soon as possible.

The only prior knowledge I had about security and how to secure an application was about the different authentication and authorization methods. Going through the materials I learned about the different types of attacks, which can be done to a host and that if I wanted to make my application secure, I should’ve made several changes to my app.

I personally don’t have a preferred learning style because I think every topic can be reviewed with different methods. Most commonly my first step is to analyse the best practices, most common mistakes, different technologies and their pros and cons, then try to implement/avoid them.

Sometimes I face difficulties getting fast into new materials and their concepts. For example, the most recent thing that was a setback for me was setting up pfsense firewalls and even though I was studying along with my classmates, I struggled to grasp some of it, but I believe that anything can be learned if you put in enough work.

I believe a strength of mine is that I am eager to learn new things.

Learning outcomes

In my Body of Knowledge(BoK) document, I have documented most of my exercises, in-depth information on how I made the tasks, etc. The general feedback of my teachers is by far good with a few remarks concerning additional explanations and evidence of what I have done. The learning materials are divided into two categories – **offensive** and **defensive**.

For **both LOs**, I am proud that I managed to do all the exercises and tasks. The additional topics in my BoK file reflect on the learning outcomes. I managed to analyze and monitor the security of diverse IT environments using various tools according to a methodical approach for the **defensive side**. The IT monitoring, Host-based intrusion detection, and Web application firewalls, for example, relate to the learning outcome. The **network spoofing**, **password cracking**, **Wi-Fi-hacking**, etc, on the other hand, gave me a good understanding of the **offensive side**.

Furthermore, our group assignment, which is a **pentest** of a housing agency, aims to contribute to the objective of advising a client on security improvements on a technical level. We are currently due to start the pentest, so very soon the outcome will be a reality.

Further in the next phase, I will try to include all knowledge I have gained to attack my project environment as a hacker and then set up a secure environment and show how it can be protected.

That’s why I believe I did very well concerning those two learning outcomes and **I can say I have passed them successfully**.

I believe **professional standards** and **personal leadership** are two very important aspects of a successful specialist. **Both in the individual and group projects**, I believe everybody maintained professional behavior and that was justified in the peer review meeting and the several distinct conversations with our teacher and also in feedpulse. The most important thing that I have learned is that proactiveness is crucial when it comes to teamwork, and **I am proud that I am as active as the others on the team**.

Concerning the **Personal Learning Activities**, I think I have spent a bunch of time **researching and getting deeper into the learned materials**. The total expected hours are 60, but even though I didn’t track how many hours exactly I have covered, I think the more important fact was that I have a **big progress and interest** in the cyber security field. In the next phase, I would like to build on top of the current foundation of knowledge.

For both learning outcomes, **I believe that if everything is going like this, I will be proficient.**

Also, as my next semester is about an internship, I have spent a lot of time preparing documents and contacting numerous companies. I would like to further develop as a software engineer and through working with other people in an actual working environment to level up. The things that I am learning this semester are a strong addition to my palette of expertise and a fundamental part of developing software solutions, which I am extremely happy about.