ICT, Cyber Security Portfolio

Mohammed Nasser Alshukaili.

ICT, Fontys University of Applied Sciences.

Cyber Security, Semester 4.

2022

Contents

[INTRODUCTION 3](#_Toc120643274)

[Background 3](#_Toc120643275)

[LEARNING OUTCOMES 5](#_Toc120643276)

[Ethical Hacker 5](#_Toc120643277)

[Risk Consultant 5](#_Toc120643278)

[Security Engineer 5](#_Toc120643279)

[Security Analyst 6](#_Toc120643280)

[Security Professional 6](#_Toc120643281)

[PERSONAL PROJECTS 6](#_Toc120643282)

[PVI 6](#_Toc120643283)

[Internship 6](#_Toc120643284)

[PSP 7](#_Toc120643285)

[Overall Conclusion and Reflection 7](#_Toc120643286)

# INTRODUCTION

## Background

#### What was your relevant prior knowledge and experience on security, Linux and networking or what did you do to obtain this knowledge?

I only studied security in the first semester at Fontys ICT, there was a course called Infrastructure Engineering, it was super interesting for me, and I enjoyed it the most. However, I made the biggest mistake when I did not choose it for my profile. I chose media design for personal reasons.

I know that I made big mistake by not going to that path, but I did not let it stop me from learning that subject by myself. I asked some friends that studied Infrastructure about their course content, and I decided to self-study everything that is related to this side of IT. I subscribed to <https://tryhackme.com/> to learn about security, Linux, networking, and other cool stuff. I chose this path to learn because the website offers courses and exercises at the same time. I also got to learn good things throughout my media design journey as it introduced me to the web and how it works. I got so good at JavaScript which would definitely help me in my security journey.

#### What was your preferred learning style. Why?

I think it was always self-studying. Why? Because when you self-study something, there will be no pressure on you that slows you down from learning new things. I spent my holidays at home learning new things. When I had to leave home, I always wait until I go back to learning, this is how I know that I enjoy self-studying too much.

Also, this method works for me because there is no one is waiting for you to submit this assignment before the deadline, I was just going as the perfect pace for me.

I used to hate reading to learn, but this method helped me to love looking up new things and be patient to get better.

Nevertheless, school is as important as that. Because school gives me the real-life experience. In 6 months, I will be doing this stuff for a company as an intern, I would not be able to gain this experience only from the online courses.

#### What motivated you to join cyber security?

Curiosity.

For my profile (media design), it was about building websites and being creative to design and all this was repetitive. I did not find myself enjoying doing the same job for every assignment.

When I studied Cyber Security at home, I found out that it consists of endless information that I can obtain. Also, whenever I solved a problem, I found myself curious about how to solve the next problem, this was how I kept learning non-stop. Therefore, I chose Cyber Security as my specialisation.

#### What are your strengths and weaknesses? (Use these to develop your personal development goals.)

|  |  |
| --- | --- |
| **Strength** | **Weakness** |
| * Curiosity * Patience * Hard worker * Enthusiasm * Able to use the computer for so long without stopping | * Doing research * Referencing * Presenting * Lack of experience |

This semester, I will show the thing that I am good at. On the other hand, I will improve the weaknesses that I am struggling with.

# LEARNING OUTCOMES

## Ethical Hacker

This subject was new for me, and I was excited the most about it. I got familiar with this concept using online open-source website called DVWA. That website introduced me to the ethical hacking concept. I did good at it, I managed to complete most of the exercises.

I got to find vulnerabilities in many websites. Some of the vulnerabilities are SQL injections, Cross-Site scripting, file inclusion, Brute force, and many more.

I am proud of the successful hacks that I did against vulnerable websites. However, this is not enough to be a professional hacker. Next step is to extend my skills to more secure websites.

I thought ethical hacking was going to be the path that I want. However, I found something that is more suitable for me, which is blue teaming.

## Risk Consultant

As a cyber security specialist, I need to learn how to analyse the risk of most of the vulnerabilities to provide a secure system.

This subject introduced me to some of online threats and how to deal with them.

It also explained to me the CIA triad which is an integral part of any cyber security direction.

I did 2 research about this subject that helped me to gain a better view of the security of the internet.

However, I need to experience online threats in real life to help me more to analyse the risk and come up with solutions. This can be done by working at a tech company as an intern.

I believe that security threats can be avoided by continuously pen testing the system.

Try to reach the vulnerabilities of the system before the black hat hackers do.

## Security Engineer

I am enjoying this subject the most. I learned how firewalls work, and I learned how to secure networks by implementing everything I learned on my private network.

As I was learning firewalls, I also learned how to pass firewalls, this gets me closer to know how the hackers think.

I learned about VPN which is a great tool for working remotely. I always wondered how remote jobs can allow the employees to work from home and VPN was the answer.

I used an open-source package called OpenVPN to connect my private network with outsiders.

Intrusion detection and prevention system (IDS/IPS) is a great tool to implement beside the firewalls.

It helps to detect and block malicious data that the firewall did not know about. I got to implement IDS on both a network and a host, HIDS is important to work against frauds that are already passed the firewall and the NIDS.

I secured my web server using the ModSecurity tool that was made for web application firewall.

This tool uses thousands of lines to prevent hackers from exploiting most of the web application vulnerabilities.

I figured out that this is the path that I want to take as a cyber security student. I enjoyed implementing firewalls and VPN connections. I also liked coming up with new ways to stop the hackers from gaining access for my system.

## Security Analyst

This subject introduced me to monitoring the network and reading everything that is going in and out of my connected devices.

There is a big chance that I will become a security analyst in the future as it is popular in my country. It might seem boring, but it is an integral part of any successful company.

We also learned about the most common CVE’s to get a better look of vulnerabilities around the world.

## Security Professional

Running after experience only is not a professional thing. The cyber security specialist also needs to work on their team-work skills and improve ways to prove their points all the time.

Fontys always pays attention to working in groups as this concept has always been implemented since my first semester here. This opportunity gives me experience of how to deal with co-workers and how to persuade them with my results.

# PERSONAL PROJECTS

## PVI

For the Personal Vulnerability Investigation, I decided to choose router as a subject. I got a TP-Link router from the ISSD and started to dig deep into its vulnerabilities. I wrote a research paper for this and presented the results to my classmates and teachers.

## Internship

I started preparing for the internship by figuring out what I want to be specialized in.

In the beginning, I thought I would go for a red teaming internship assignment. However, after doing enough research, I chose to look for a networking internship.

My first steps were talking to people who were studying Cyber Security just like me. They both went for blue teaming and told me what they were expected to do. I talked to 2 friends. One of them did the internship at Signify company, and the other one did it at Surf.

I asked them for the contact information for these companies and I immediately sent them my resume and motivation letter asking them for an internship assignment that is related with networking.

After that, I looked for assignment in a website called indeed. (<https://nl.indeed.com/>).

I applied for some assignment that were suitable for me and now I am waiting for the best response.

## PSP

I chose to do research on Networking. I always regrated that I did not choose infrastructure engineering as a profile, and this is the time to learn what I missed.

To stay consistent, I chose to follow a training for the Cisco Certified Network Associate (CCNA) that covers intermediate- advanced topics for networking.

# Overall Conclusion and Reflection

I am grateful for everything I learned in this semester. Not just it introduced me to the security side, but also it offered me great resources to practice my ethical hacking skills. I started from a low point as I come from a media design profile. However, the first 10 weeks were enough to teach me all the basics for the cyber security. The dvwa and Juice shop helped me to build a strong foundation for the internet security. Then, the PVI introduced me the idea of investigating one thing which was the router in my case, I learned so much by doing for that assignment.

Finally, I think the best thing about this semester is the freedom of choosing the subject for the PSP. I thought they would force me to do research on a specific thing that I do not enjoy, and I would need to learn networking in my free time. However, teachers agreed for me doing research on what I am curious about which is super practical.