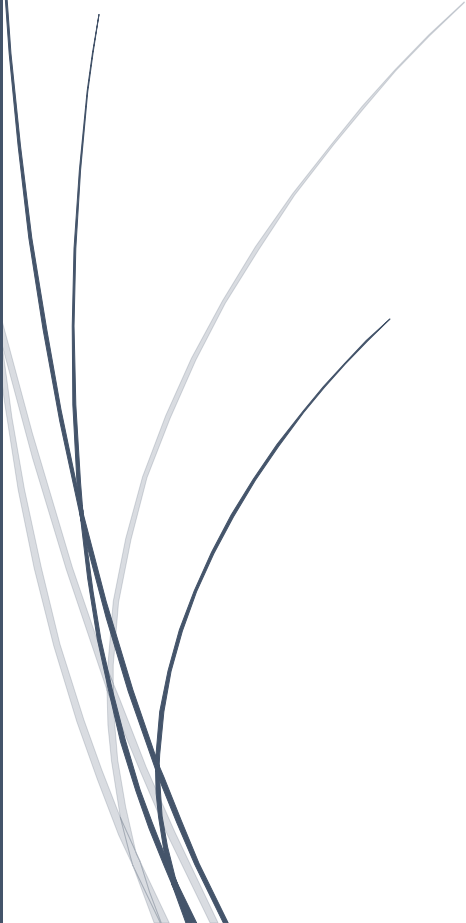


A dark blue vertical bar runs down the left side of the page. A blue arrow points to the right from this bar, containing the date.

6/11/2023

# Portfolio

Document Reflection CS4

Several thin, curved lines in dark blue and light grey originate from the bottom left and sweep upwards and to the right.

|                 |              |
|-----------------|--------------|
| Student Name:   | Hristo Kolev |
| Student Number: | 4110021      |
| Student Group:  | D            |
| Coach:          | Xuemei Pu    |

## **Table of Contents:**

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>INTRODUCTION .....</b>                      | <b>2</b>  |
| <b>2</b> | <b>LEARNING OUTCOMES .....</b>                 | <b>3</b>  |
| 2.1      | ETHICAL HACKER .....                           | 3         |
| 2.2      | RISK CONSULTANT .....                          | 4         |
| 2.3      | SECURITY ENGINEER .....                        | 4         |
| 2.4      | SECURITY ANALYST .....                         | 5         |
| 2.5      | SECURITY PROFESSIONAL .....                    | 6         |
| <b>3</b> | <b>PERSONAL PROJECTS.....</b>                  | <b>7</b>  |
| 3.1      | PERSONAL VULNERABILITY INVESTIGATION.....      | 7         |
| 3.2      | PERSONAL SPECIALIZATION PROJECT.....           | 7         |
| 3.3      | INTERNSHIP PREPARATION.....                    | 8         |
| <b>4</b> | <b>OVERALL CONCLUSION AND REFLECTION .....</b> | <b>8</b>  |
| <b>5</b> | <b>REFERENCES .....</b>                        | <b>10</b> |

# 1 Introduction

This document is about a personal reflection for the first specialization course – Cyber Security that I am following in Fontys University of Applied Science. I will give my evaluation and reflection on all learning outcomes that I have completed through the semester.

Before starting the semester, I did not have quite big knowledge with Linux OS and networking. My previous experience was in semester 1 where I have several workshops about installing Ubuntu Linux on a virtual machine and some exercises using some simple commands and tools like “Wireshark”. On the start of the semester, I knew that it will be a challenge not knowing anything about networking and Linux, but I was determined to learn. Over time I learned some basic knowledge in both areas and a lot of hard work to read and understand the material, of course with the help of my groupmates.

My decision to follow Cyber Security was an interesting choice. I had a friend that was in this specialization and when we saw each other, he was telling me about his projects and how he was exploiting routers and for me this was the way to go. From then I start watching videos about this IT area. The individuals that uncover vulnerabilities and exploits them, continue to amaze me still till this day.

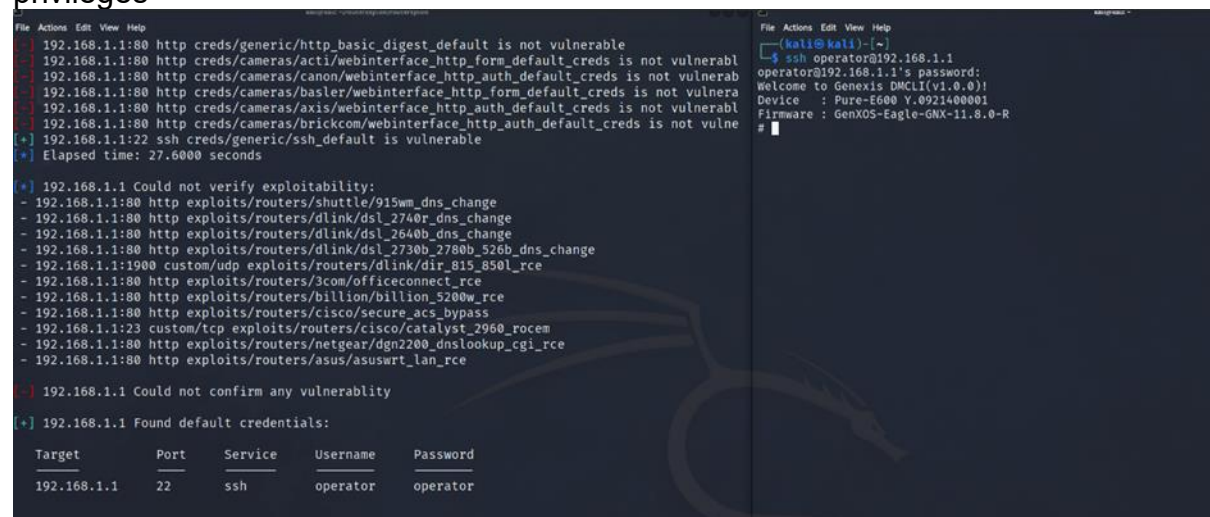
## 2 Learning outcomes

During this semester I had to proof that I am capable of acquiring new skills in the following learning outcomes. They were ordered into themes, that I covered in my Body of Knowledge document. Here is the reflection of each Learning outcome.

### 2.1 Ethical Hacker

This learning outcome was probably the most interesting of all for me. I actually studied penetration test techniques that allows me to access the IT systems, both software and hardware. I learned how actual hacker thinks, how to study potential target, how to identify vulnerabilities within the system.

In the [penetration test report](#), my group and I demonstrate the use of some techniques. I managed to run a routersploit on the tested device and I participated in the execution of the Phishing attack. The outcome of that exploit was one vulnerability about the router's users-Operator user's credentials. With this information I managed to enter in the router's settings and I can edit them. These credentials have admin rights and I managed to edit the root user credentials. The final result was: I had the root user privileges



```
File Actions Edit View Help
192.168.1.1:80 http creds/generic/http_basic_digest_default is not vulnerable
192.168.1.1:80 http creds/cameras/acti/webinterface_http_form_default_creds is not vulnerabl
192.168.1.1:80 http creds/cameras/canon/webinterface_http_auth_default_creds is not vulnerab
192.168.1.1:80 http creds/cameras/basler/webinterface_http_form_default_creds is not vulnera
192.168.1.1:80 http creds/axis/webinterface_http_auth_default_creds is not vulnerabl
192.168.1.1:80 http creds/cameras/brickcom/webinterface_http_auth_default_creds is not vulne
[*] 192.168.1.1:22 ssh creds/generic/ssh_default is vulnerable
[*] Elapsed time: 27.6000 seconds

[*] 192.168.1.1 Could not verify exploitability:
- 192.168.1.1:80 http exploits/routers/shuttle/915mm_dns_change
- 192.168.1.1:80 http exploits/routers/dlink/dsl_2740r_dns_change
- 192.168.1.1:80 http exploits/routers/dlink/dsl_2640b_dns_change
- 192.168.1.1:80 http exploits/routers/dlink/dsl_2730b_2780b_526b_dns_change
- 192.168.1.1:1900 custom/udp exploits/routers/dlink/dir_815_850l_rce
- 192.168.1.1:80 http exploits/routers/3com/officeconnect_rce
- 192.168.1.1:80 http exploits/routers/billion/billion_5200w_rce
- 192.168.1.1:80 http exploits/routers/cisco/secure_acs_bypass
- 192.168.1.1:22 custom/tcp exploits/routers/cisco/catalyst_2960_rocem
- 192.168.1.1:80 http exploits/routers/netgear/dgn2200_dnslookup CGI_rce
- 192.168.1.1:80 http exploits/routers/asus/asuswrt_lan_rce

[-] 192.168.1.1 Could not confirm any vulnerability
[*] 192.168.1.1 Found default credentials:

Target      Port  Service  Username  Password
192.168.1.1 22    ssh      operator  operator
```

In my opinion the main topics that were covered were to understand the Ethical Hacker and the technical part of the Ethical Hacker. The first topic involves learning about the legality of the ethical hacking, this was made in the very beginning of the course by the teachers. Also, I had to familiarize myself with the mains steps of making the penetration test successful. I watched some videos from Cyber Security specialist that explained how by following these steps they conduct pen tests.

The second aspect covers learning how hackers exploit vulnerabilities in the system and identifying these weaknesses. This includes the use if various techniques, tools and hacks for detection and analysis. All of this was covered in different workshops where the teachers show and explain everything needed about the today's technique. For example, I show a bigger interest in XSS, CSRF and SQL Injection. I was very surprised when I found out that with several symbols, I can get to the whole database or with the use of a specific tool I can edit the information of a specific request. The execution of the exercises given by the teachers and their result is documented in my

[Body of Knowledge](#), Chapter 1. I suppose I show bigger interest in these techniques because of my Software background and I probably did these mistakes that allows the hacker to mess with the web- application.

To be honest, I learned new techniques that every is a must have and every IT engineer must know. I understood every topic and manage to complete all the tasks that the teachers gave us successfully.

## 2.2 Risk Consultant

This learning outcome is about my abilities about to analyse security threats, using risk analysing methods to provide business analysis and advising clients what security steps they should take after the made analyse.

Same as Ethical Hacker, it is very important to know the security threats and their impact on the business, how to find and analyse these threats and how to consult your clients.

Of course, the important thing is to know the business model that you researching, because how to analyse the IT environment if you don't know the context.

I covered all the topics connected with this learning outcome in my [Body of Knowledge](#) where I documented my acquired new skills about analysing various types of cyber threats and attacks, analysing different CVEs and assign them a CVSS score. I was analysing an vulnerability that I found in this [website](#). There were XSS vulnerabilities discovered and reported in the Dispatch application, affecting name and description parameters of Incident Priority, Incident Type, Tag Type, and Incident Filter. This vulnerability can be exploited by an authenticated user.

The screenshot shows a CVSS Base Score calculator interface. At the top right, a yellow box displays the 'Base Score' as 3.5 (Low). The interface is divided into two columns of settings. The left column includes: Attack Vector (AV) with 'Network (N)' selected; Attack Complexity (AC) with 'Low (L)' selected; Privileges Required (PR) with 'Low (L)' selected; and User Interaction (UI) with 'Required (R)' selected. The right column includes: Scope (S) with 'Unchanged (U)' selected; Confidentiality (C) with 'None (N)' selected; Integrity (I) with 'Low (L)' selected; and Availability (A) with 'None (N)' selected. Each setting is represented by a button with its selected value highlighted in green.

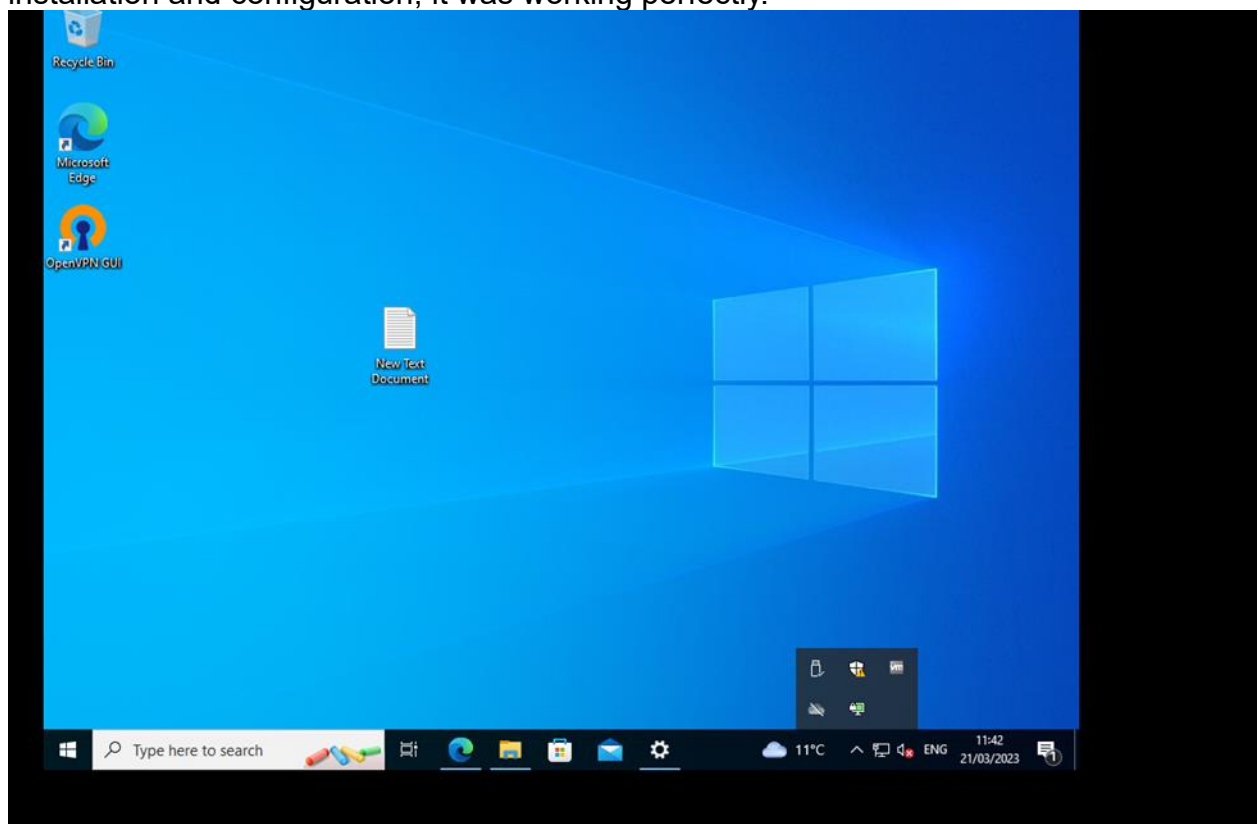
I think this learning outcome is as important as the previous one, to become an Ethical Hacker and it require a lot of thinking of the current situation of the client. I think I have managed to cover and get the basic knowledge of the topics because I am sure that it is way different in the real environment and there are more things that I did not even consider.

## 2.3 Security Engineer

This learning outcome is part of the Blue Team area of the Cyber Security. It includes designing IT structure and securing them with software tools.

This topic is closely related to the infrastructure and most of the topics covered in the workshops, were about designing networks, setting up connections, routers and virtual machines, creating firewalls and etc. This was completely new material for me and was more difficult than my colleagues, but with their help I managed to learn and understand all topics. I learnt how to add monitoring tool like NIDS and HIDS, how to create VPN, SSH certificate and apply them in the network system that we have to design and create. Every topic is described in details in my [Body of Knowledge](#) document.

I think that I managed to understand the topics associated with Security Engineer learning outcome and I will practice and study infrastructure in the near future because in these workshops I learnt its importance, despite the fact I chose to pursue Software Engineer career. For example, I decided to make myself a VPN so I will not be tracked that easily. I managed to create one in Fontys's netlab using OpenVPN. After the installation and configuration, it was working perfectly.



## 2.4 Security Analyst

Same as the Security Engineer, this topic is also part of the Blue Team area. I would say also this topic has some similarities with the Risk Consultant – understanding the security incidents.

One of the main aspects is to work with monitoring tools. This way you can see what time the incident happened, how it happened. This way you can have an approach to handle the incident. By learning how to install and work with the monitoring tools, I acquired this knowledge, which is very important these days, because if not a hacker easily can do harmful things on my computer and I will not even know because I give him the opportunity to delete his footsteps.

Another important aspect is the skill to properly react and fix the incident. Accident happens all the time even when you are responsible, so it is your job to prevent them. I think managed to understand the topics associated with Security Analyst. I think the hardest part here is to apply the knowledge in real life situation and I hope I will be able to deal with these situations.

## 2.5 Security Professional

This learning outcome I confidently say that I demonstrate the whole semester. I always kept my head down to work on the given assignments and projects. I completed all the exercises within the given deadline and I am happy with that, despite the last-minute problems. While writing the [Body of Knowledge](#) I had a lot of problems, for example the structure of the document, Afterthoughts section, some of the exercises that requires more Infrastructure knowledge and others, but the key of my success was the hard work and reading and watching tutorials that are outside of the given material and of course a lot of help from my group members.

The group that I entered is with very high work ethic and always down to learn new techniques and always gives 100% and I am happy that I entered in that group. We communicate easily and the work flow is very positive.

During this semester I developed new skills and upgraded others. While writhing the Body of Knowledge, personal and group projects I managed to understand all the material (offensive, defensive security and the hardware and networking in general) needed to complete this semester successfully. I definitely think that I improved my communicational skills, become more consistent and learned to structure my work.

## 3 Personal Projects

### 3.1 Personal Vulnerability Investigation

My [Personal Vulnerability Investigation](#) project was about hacking wireless router. I was very interested about entering in a device unauthorized. The expected hours for this project were about 20h, but I am pretty sure that I spend more than that. I manage to recreate 3 different types of attacks. The first was wireless password cracking which is entering in the router's network without having the password. The second attack was running a routersploit. This is a tool that will find exploits and vulnerabilities on the router and to my dismay I found one exploit called "The moon warm", but still only one for an old router. This exploit was common for Linksys models but not for mine. And the last attack was Phishing attack. It is basically creating a network exactly the same as the original one but will not allow you to enter in the original and will force you to enter in the fake one. This way the hacker can capture the password of the network. Overall, it was enjoyable writing about this topic. I believe that my project was on a good level with different types of attacks. I was very interested in doing this kind of project, where I had my responsibility to choose the device, then research for it and do different attacks. I believe with I was developed my research skills even more.

### 3.2 Personal Specialization Project

During the semester, I had to create a personal specialization project, regarding developing malware and password manager. The start of this project was around week 12 and it is not finished yet, due to final presentation of the demo occurring in the next days in front of my class. The initial activity was to research about best programming language for this exercise, how to establish connection with the victim machine and how to execute commands on it. The other part of the research was about best practices about password manager and how to secure all the passwords. All the research was completed with the use of Stackoverflow, youtube, w3schools and github.

For the creation of the malware script, I used the python programming language and it's packages. The basis of the code is socket which is a software structure that serves for sending and receiving data. The main functionalities of the script are uploading and downloading files, executing commands on the victim's machine, changing the directory and taking the screenshot of the machine.

```
Connection established with: 192.168.178.189 on port: 51370
[+] Handle connection

[1] Run Command on victim OS
[2] Upload files to the victim machine
[3] Download files from he victim machine
[4] Change Dir
[5] Capture Screenshot
[99] Exit
[+] Select your options
```



For the password manager the biggest problem that I had was the encryption and decryption of the file using the cryptography key. After numerous attempts and rewriting the code several times I manage to fix this problem and run the program without problems. The main functionalities are creating and loading the cryptography key, loading the password file, adding new password and displaying all the passwords.

```
C:\Users\hrist\OneDrive\Desktop\PassManager\venv\Scripts>
What do you want to do?
    1 Create a new key
    2 Load an existing key
    3 Load a Password file
    4 Add a new password
    5 Show the passwords
    q Quit

Enter your choice: 2
Enter your choice: 2
[+] The key is loaded
b'aixfL3l0lM5IxIw6y9ydIwu5-m2D3eUBp40xRfPU2gY='
```

### 3.3 Internship Preparation

At the beginning of this semester, I was added to course about the internship next semester. I was a little bit prepared by my friends about the internship and its duration and documentation but still read all the available information. I started searching for internships in Fontys portal, LinkedIn, Indeed and other sites. I also went to an event organized by Fontys about companies that are searching for new interns. As you may know I have Software background, so I was looking for software internships. I talked with a lot of companies, but most of them did not want to meet and have an interview. Eventually I had an email from one company that they want to meet me and decide if they have the right internship for me. We had 2 meetings and agreed on the terms of the proposed internship, but week later they decided to go with another student. I started to look for internship again and after several weeks I managed to find another international company that wanted to work with me, so I proposed that internship offer to Fontys and they agreed on my journey next semester.

## 4 Overall Conclusion and Reflection

During this whole semester, I learnt a lot about the cyber security and its topics. Every workshop was very useful and helpful to me. The teachers explained and demonstrated something from every topic. For me it was challenging this semester because I have software background and most of my groupmates have infrastructure background and for them is a little bit easier, but with hard work and with a lot of help from their side, I thing I managed to keep up with them and manage to finish this BOK and acquire the given knowledge during the lectures. I am happy from the outcome

that I am right now. I think I will continue my studies in the security profile that Fontys provides in their curriculum and I am planning to continue to acquire new knowledge in this field.

## 5 References

H, & Kolev, H. (2023). *Personal Vulnerability Investigation*.

Source: [File](#)

Kolev, H. (2023). *Body of Knowledge*.

Source: [File](#)

Vinken, J., Kolev, H., Georgiev, L., & Popov, Y.-A. (2023). *Penetration Test Report*.

Source: [File](#)

*CVE-2020-9299 : There were XSS vulnerabilities discovered and reported in the*

*Dispatch application, affecting name and description param. (n.d.).*

<https://www.cvedetails.com/cve/CVE-2020-9299/>