Portfolio

Cyber Security Specialization

May 30th, 2023

Aleksandar Penev

a.penev@student.fontys.nl

Contents

Introduction

This is a personal reflection document for the Cyber Security Specialization course that I'm following at Fontys UAS. In this document, I will be evaluating and reflecting on all the learning outcomes I have completed throughout the semester.

Before starting this semester I already had knowledge about the Linux operating system and Networking. During my High-School years, I used many Linux distributions, primarily for playing with the Gnome customization options which Windows didn't offer, but while using it I've gotten comfortable with bash as well. As for networking, when I was 15 my sister got me a job to help the network administrator at her office, although it was more of a watching him work than actually helping him. Over time, I have acquired a lot more knowledge in these areas, yet I recognized that there were still gaps in my understanding before starting on this semester.

My decision to follow this specialization was a natural choice for me. Throughout my school days, I became the go-to person for console hacking among my peers. Since then, I have been actively following the new console hacking and homebrew scenes. The individuals who uncover vulnerabilities and develop intricate exploits continue to amaze me to this day. Their work has always appeared incredibly complex and has this sense of craftsmanship to it. This Cyber Security specialization presented the perfect opportunity for me to see if it could be the right thing for me and my future career.

Learning Outcomes

During the semester I had to show the following learning outcomes. They have been mixed into the themes I have covered and shown my progress in my Body of Knowledge. The following is a reflection of each Learning Outcome:

Ethical Hacker

The Ethical Hacker outcome of my studies focuses on my ability to assess the security of IT systems in various environments using penetration testing techniques, providing valid vulnerability assessments that cover each layer of an IT infrastructure.

There are two fundamental aspects to this learning outcome. Firstly, it requires a deep understanding of the importance and potential capabilities of a hacker. To have that understanding you have to fully comprehend how hackers thinks, select their targets, and identify vulnerabilities within systems.

To address the first aspect, the initial portion of my Body of Knowledge centered around gaining a comprehensive understanding of Ethical Hacking. This involved learning about the legality of ethical hacking, as well as familiarizing myself with the main steps involved in the CKC kill-chain, which hackers must navigate. I also explored how specialists can follow these steps to conduct effective penetration tests.

The second aspect involved acquiring knowledge about how hackers exploit vulnerabilities in systems, both in terms of software and hardware, and proactively identifying these weaknesses. The topics I covered in Ethical Hacking focused on various types of hacks and techniques for detection and analysis. These topics included File Traversal, File Inclusion, Command Injections, XSS, CSRF, SQL Injections, Sniffing, Spoofing, Network Scanning, Password Cracking, Identity Management and more.

Many of the web and application topics were already familiar to me due to my background in Software Engineering. I have encountered and created many of them in the past semesters. To learn and cover these subjects, I attended university lectures, extensively read popular blogs that delve into these subjects, and watched YouTube videos featuring CTF solutions that incorporated similar topics.

To be honest, I cannot say I have a preference for any specific topic as each one is crucial to master. They are a must-know for every IT worker and if I want to be a qualified Engineer in the future, I must keep learning and building on top of my current knowledge on the subjects. I understood every topic and successfully completed all the assigned tasks that were asked of me this semester so I would give myself a good grade.

Risk Consultant

This learning outcome and the Ethical Hacker outcome both tie into Offensive Security. Risk Consultant refers to my ability to analyze security threats and provide business analysis using risk analysis methods and in turn advise clients on the steps they should undertake after that analysis.

This outcome also has two aspects. First one is the same as the one from Ethical Hacker, a thorough understanding of security threats and their impact, how can you analyze and consult someone if you have no understanding of it yourself. Second aspect is less technical and requires a business mindset. To consult you need to understand the business model of the IT environment you're inspecting. Again how could you understand the importance of something that you don't know the context of.

The themes referring to this Learning Outcome that I've covered in my BoK are analyzing the different types of security threats, the different types of cyber attackers, analyzing risks using the CIA triad, analyzing different CVEs and their CVSS scores. I gained that knowledge by listening the lectures and reading about the subjects online.

I personally think this is the next step of becoming an Ethical Hacker. A real Security Analyst that can think in the place of the client is required in every offensive Cyber Security team. I think I did well covering the subjects and hope I will get to learn even more on the subject and even get to be a Risk Consultant someday. I know there's a lot more to the topics and in a real-world environment there would be way more things to consider. I would give myself a good grade.

Security Engineer

This learning outcome is placed on the defensive side of Cyber Security. Security Engineer refers to my ability to design IT structures and securing them with detection and prevention softwares while considering their context and security risks.

This topic was mainly setting up infrastructure, i.e. designing secure networks and setting up routers, machines, connections, vlans and firewalls. Although I mostly knew the material I have never actually gotten the opportunity to practically setup networks. Combining those networks that I have created with encryption, tls, ssh mfa and vpn tunnels and adding monitoring tools like nids and hids was an amazing practice to realize my designs.

I have understood every subject related to the Security Engineer learning outcome, I want and I definitely will continue studying infrastructure due to it's importance in the IT world. Even if I decide to follow a software engineering career, it will be of great importance, due to work with the cloud, Kubernetes and docker. Also even though it is more related to defensive security, it is very important for any offensive(red teaming) security professional. I would give myself a good grade.

Security Analyst

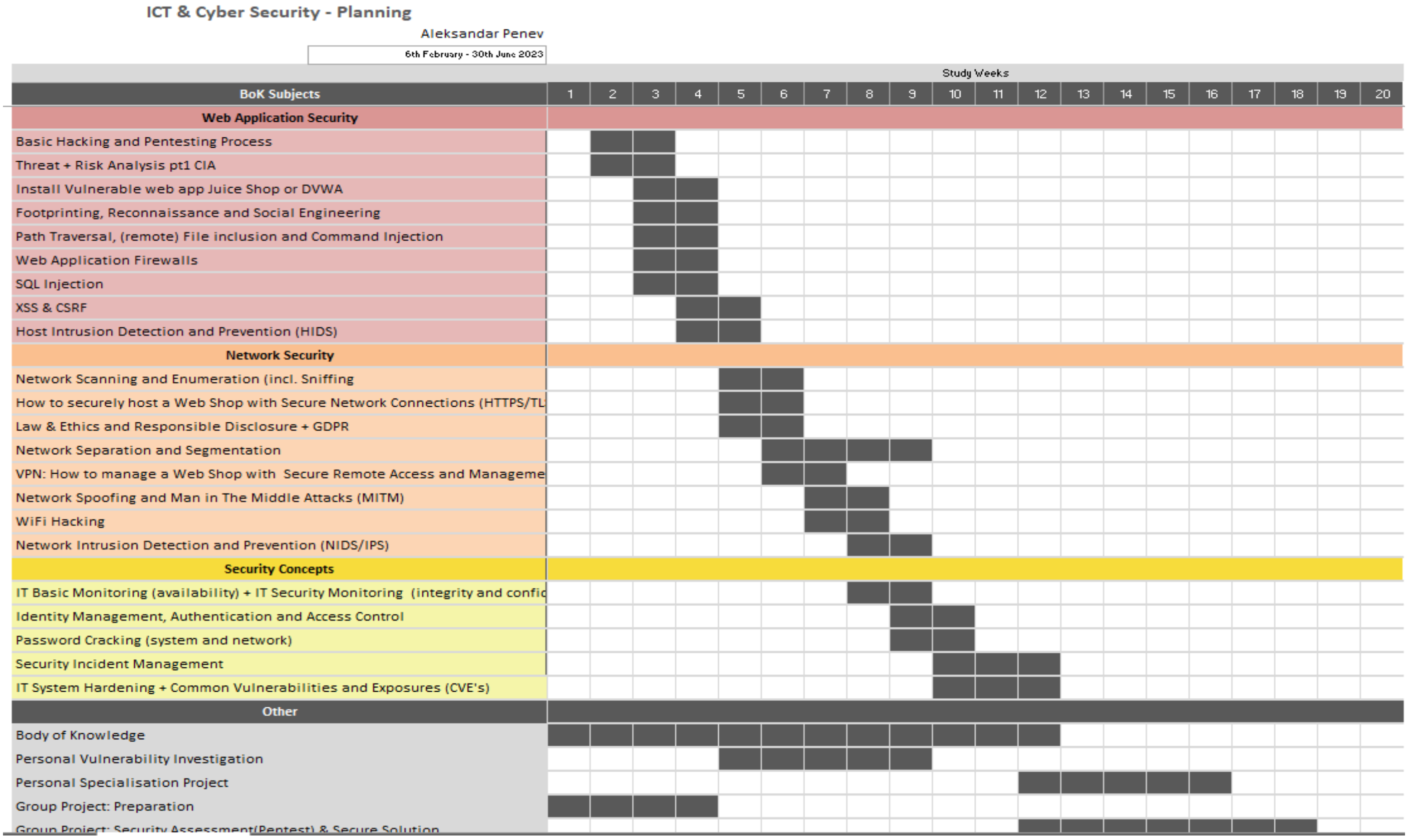
This is again part of the Defensive Security learning outcome. It is the other side of the Security Engineer outcome. Security Analyst refers to comprehending and responding to security incidents in an efficient and methodical manner.

The outcome has two aspects, one is actually having the tools(monitoring) so you can see what at the time of the incident and the second aspect is having a systematic approach to handle incidents. The first aspect is the knowledge on how to install and work with monitoring tools. Those are really important especially nowadays, because if not setup a skillful hacker would just erase all his footsteps.

The second aspect is the skill of reacting properly, responsibly, and actually getting incidents/problems fixed especially in stressful situation is the most important one as security administrator/analyst in my opinion. You can't always foresee or prevent the issues that arise, but it is your job to fix them and get things done. Accidents, especially ones that are related to cyber security occur very often and a lot of the times out of nowhere. Even when, someone else is responsible. Writing the topics was easy, the hard part is actually applying that knowledge in critical moments, and I hope one day I will be adaptable enough to deal with situations like that. If I would grade myself, I would give myself a good grade.

Security Professional

This learning outcome is different than the others. I have not demonstrated it through the subjects in my BoK, but through the writing of the BoK itself. At the beginning of this semester I crafted a thorough planning of how the semester would go. Here is it:



ICT & Cyber Security - Planning

Aleksandar Penev

6th February - 30th June 2023

	Study Weeks																			
BoK Subjects	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Web Application Security																				
Basic Hacking and Pentesting Process		■	■																	
Threat + Risk Analysis pt1 CIA		■	■																	
Install Vulnerable web app Juice Shop or DVWA			■	■																
Footprinting, Reconnaissance and Social Engineering			■	■																
Path Traversal, (remote) File inclusion and Command Injection			■	■																
Web Application Firewalls			■	■																
SQL Injection			■	■																
XSS & CSRF				■	■															
Host Intrusion Detection and Prevention (HIDS)				■	■															
Network Security																				
Network Scanning and Enumeration (incl. Sniffing					■	■														
How to securely host a Web Shop with Secure Network Connections (HTTPS/TL					■	■														
Law & Ethics and Responsible Disclosure + GDPR					■	■														
Network Separation and Segmentation						■	■	■	■											
VPN: How to manage a Web Shop with Secure Remote Access and Manageme						■	■													
Network Spoofing and Man in The Middle Attacks (MITM)							■	■												
WiFi Hacking							■	■												
Network Intrusion Detection and Prevention (NIDS/IPS)								■	■											
Security Concepts																				
IT Basic Monitoring (availability) + IT Security Monitoring (integrity and confic								■	■											
Identity Management, Authentication and Access Control									■	■										
Password Cracking (system and network)									■	■										
Security Incident Management										■	■	■								
IT System Hardening + Common Vulnerabilities and Exposures (CVE's)										■	■	■								
Other																				
Body of Knowledge	■	■	■	■	■	■	■	■	■	■	■	■								
Personal Vulnerability Investigation					■	■	■	■	■											
Personal Specialisation Project												■	■	■	■	■				
Group Project: Preparation	■	■	■	■																
Group Project: Security Assessment(Pentest) & Secure Solution												■	■	■	■	■	■	■		

I can confidently say that I adhered to it throughout the entire semester, although with an exception. While I completed all the exercises within the given time frame, there was a considerable time lapse between finishing them and writing them into the BoK. Nevertheless, I am pleased with how things turned out as I managed to finish all the topics within the deadlines.

While writing the BoK I had to solve many different problems but , I kept working and reading and I think I understood all the topics to be able to finish this semester successfully. While writing, I found certain topics to be particularly interesting, and I came to realize that to be a well-rounded IT specialist, it is imperative to have a comprehensive understanding of offensive and defensive security, and hardware/networking in general. As for this Learning Outcome, I can confidently say I showcased my professional development and my ability to take responsibility and structure my work. I would give myself a good grade.

Personal Projects

Personal Vulnerability Investigation

My Vulnerability Investigation was on High-Frequency RFID Tags and their security. My idea initial idea was to get a fundamental understanding of the technology and then get into exploitation. This is how I usually learn new things, first going into the basics and then build from there, that is especially valid in the Cyber Security field. How could you be trying to break the security of something that you don’t understand. But this is where my downfall was, I had 20 hours to invest in this investigation and I underestimated the RFID field. I was calling the smart cards, RFID tags, which is true, but is like calling submarine a vehicle. Although I probably invested even more than 20 hours, I can’t say I gave the topic justice. I didn’t fully dive into how the encryption specifically works. But I learned the “map” of the RFID field, understood how the technology works, found many exploits for the Mifare 1k Classic, managed to exploit my own cards and finally gave a good presentation on my investigation. Overall I think I did well, I liked the subject that I chose, but I didn’t get enough time to fully cover the topic.

Personal Specialization Project

Not Finished yet

Overall Conclusion

I am glad I chose to do this Cyber Security Specialization. Before doing it I never considered that I could be working in the Cyber Security field. I've always been hearing about massive companies that have been hacked, and watched hacking competitions like the google ones, and it has always seemed far fetched for me to do it in my future, although it seemed very interesting. The stigma that Media portraits didn't really help either. Now after doing this specialization I am still seeing the field as incredibly hard; I've started doing some CTFs and some of them can be so peculiar (like how could I even imagine to look over there for a vulnerability). But I want to see where I can get, I've looked at some of the most-widely recognized certifications, mainly (CCNA and Pentest+) and want to take them someday. I intend to do the advanced Cyber Security Specialization in the upcoming semester, and I want to see where I can get, but there is a very big difference between want and will. In conclusion I feel that I have just scratched the surface, but I truly want to learn everything and I will keep going to see where I can get.