ICT, Cyber Security Portfolio

Mohammed Nasser Alshukaili.

ICT, Fontys University of Applied Sciences.

Cyber Security, Semester 4.

2022

Contents

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.

Portfolio

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 managed to experience to hack secure websites in the pen testing group project. My group and I went to a local company called Beeyond. They have a secure website and we offered to try and find vulnerabilities to reduce the risk of them being hacked.

We learned so much in that experience. The guy responsible for our project there was happy to teach us new things and new ways to try to do against his own infrastructure.

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.

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

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 reduced by continuously pen testing the system.

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

In my pen testing group project, me and my group provided a complete guide for risk analysis for what we found against the client website.

Threat inventory and Risk Analysis method

List with descriptions of the threats for Beeyond in terms of possible attackers and their motivations

Portfolio

Threats	Attackers	Motivations
Lookup with Shodan	People who want to collect information	Get more information about the company/product
Lookup with RapidDNS	People who want to collect information	Get more information about the company/product
Lookup with SSLLabs	People who want to collect information	Get more information about the company/product
CMS Detection	People who want to collect information	Get more information about the company/product
Nmap Scanning	People who want to collect information	Get more information about the company/product
Hidden URLs	People who want to collect information	Get more information about the company/product
Lookup for documentation	People who want to collect information	Get more information about the company/product
Brute Force	People who want to get credentials	Try to login to the website
SQL Injection	People who want to gain access or information	Try to gain sensitive data from the database
Cross-site Scripting	People who want to gain access	Execute malicious scripts on victims' browsers
Reverse Shell	People who want to gain connection to the machine	Wait for the victim’s machine to initiate an outgoing connection
Lookup for the blueprints	People who want to get a better understanding of the data structure	Get information about the data structure
Lookup for data files	People who want to find some useful information	Find sensitive data
Downloading files without being logged in	People who want to gain information to which they shouldn't have access without providing the credentials needed.	Find sensitive data
Command Injection	People who	Execute arbitrary commands on the host OS
Cross-site Request Forgery	People who want to force users to perform actions against their will	Force a victim to execute unwanted actions
Performing actions as another user	People who want to gain the privileges of certain users	Impersonate that user/ make use of his privileges
User information and password hashes in the blueprint	People who want to gain access to the accounts of users	Find the password of that account

API Calls	People who want to collect information when they don't see anything	Get data from the API
Insecure Deserialization	People who want to perform malicious actions with encrypted data	Execute attacks with encrypted data
Iframe Configuration	People who want to crash the whole environment	Try to do malicious things on everyone's homepage

Risk Analysis method

In order to analyze the risks, we found we are going to make use of the risk matrix to calculate the impact level and probability as well as the corresponding risk level.
With this method it quickly becomes clear what risks exist and what the risk level of that risk is. At the same time, we will also include a conclusion and possible measures for each risk.

Risk Assessment, Management & Evaluation

Risk matrix

In this risk matrix we will describe the impact of each risk in various terms, which can be found in the matrix below. At the same time, we will also estimate the probability and calculate the resulting risk level.
Finally, we will also include an inclusion and advice on possible measures to mitigate the threat.

1. Threats/ Events	2. Impact Description	3. Impact Level (0-3)	4. Probability (0-3)	5. Resulting Risk Level	6. Conclusion and measures
Lookup with Shodan	No impact	1	2	2	Does not show important information
Lookup with RapidDNS	No impact	1	2	2	Does not show important information
Lookup with SSLLabs	No impact	1	2	2	Make sure your SSL webserver is configured correctly
CMS Detection	No impact	1	2	2	Free public information, no measures to stop this, you can make use of false version information
Nmap Scanning	No impact	1	2	2	Limit the amount of data you can get from Nmap scans. Only the TCP port was open.
Hidden URLs	Reputation damage	2	2	4	Whoami.x.com has all information about IP addresses of outgoing, local and from the Kubernetes cluster

Lookup for documentation	No impact	1	3	3	Don't leave vulnerable information in documentation. The roadmap from the website had mostly examples.
Brute Force	No impact	1	1	1	Does not work with the top 1000 most common passwords
SQL Injection	No impact	1	1	1	The application blocks any attempts to perform it
Cross-site Scripting	Customer damage	2	1	2	The application blocks any attempts to perform it. There is a possibility for a phishing attack though
Reverse Shell	No impact	1	1	1	No reverse shells possible
Lookup for the blueprints	Customer damage	1	3	3	Users should be limited in the amount of information they can see in a blueprint
Lookup for data files	Customer damage	1	3	3	Only front-end libraries found, and tokens are stored in cookies
Downloading files without being logged in	Financial damage	3	1	3	It should not be possible to download files when you are not logged in
Command Injection	No impact	1	1	1	No Command Injection possible
Cross-site Request Forgery	No impact	1	1	1	It is not possible to make requests as another user.
Performing actions as another user	No impact	1	1	1	When trying to forward with Burp Suite, the application always bounces back and returns to the old user.
User information and password hashes in the blueprint	Customer damage, Claims, Fines	2	4	8	User information can be used for targeted attacks on users. Having password hashes should never be included, especially not in an easily accessible location.
API Calls	No impact	1	1	1	We did not manage to find anything from the API
Insecure Deserialization	No impact	1	1	1	Deserialized data can't be decoded to editable string and there are no useful PHP files to build gadgets from.
IFrame Configuration	Downtime	4	1	4	Can block all the users from accessing the system if a GIF is used

I think this practical project brought me so much knowledge on how to deal with security threats.

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.

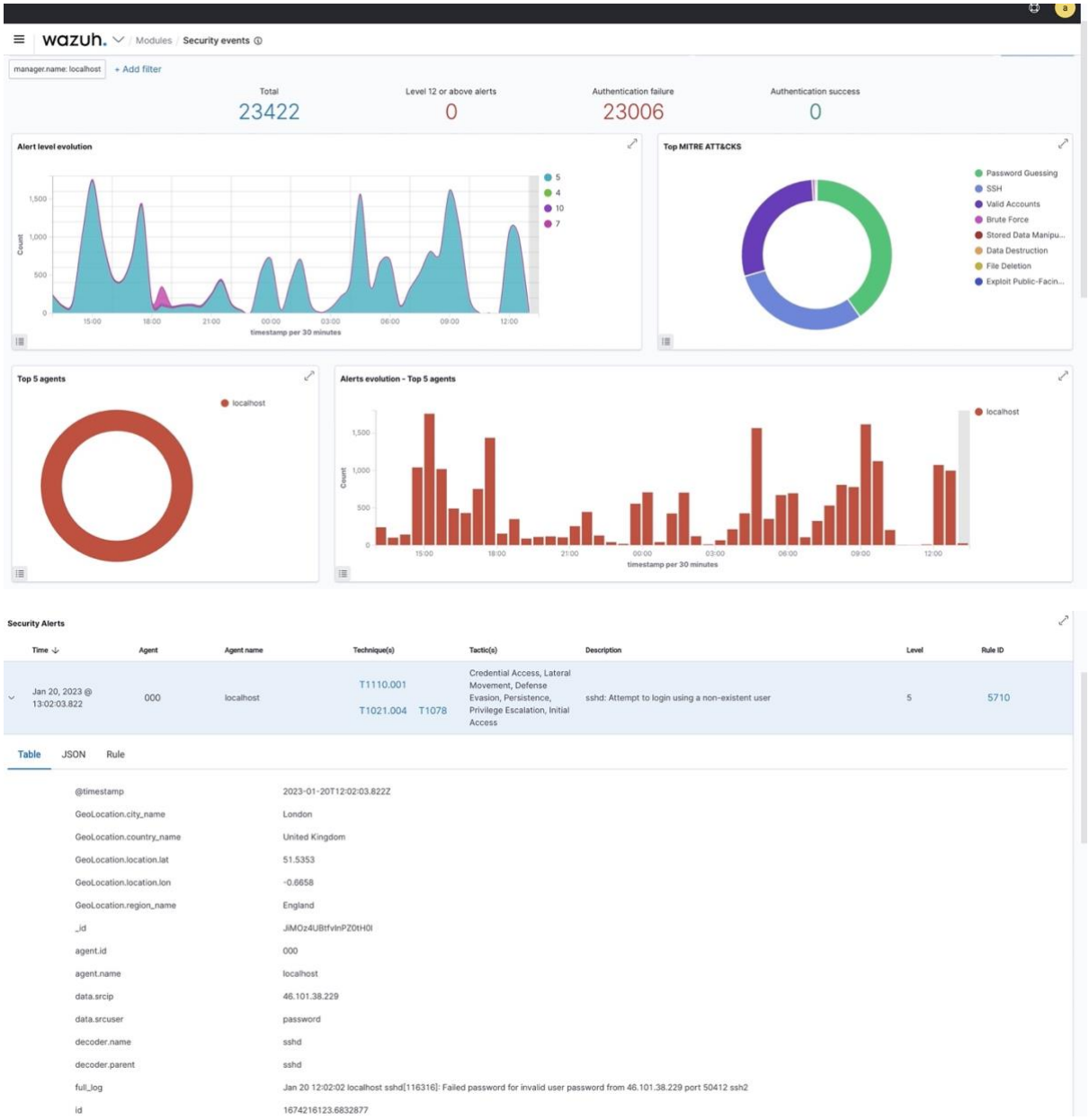
This tool uses thousands of lines to prevent hackers from exploiting most of the web application vulnerabilities.

I helped my group to use Wazuh to monitor our infrastructure in the Red vs Blue assignment.

Wazuh provided us with thousands of alerts happening against our infrastructure and helped us to quickly fix the infrastructure holes.

My internship company for next semester told me that I will be using Security Onion to monitor the infrastructure. Therefore, I invested my free time learning it. Teacher Stefan gave me the big picture for Security Onion and what it offers, he also helped me to deploy it on SecLab. I started playing and getting familiar with it.

In my free time. I decided to practice Wazuh on my personal website. I got an Ubuntu server from https://www.linode.com/ and deployed my personal website + Wazuh on it. I managed to receive a big number of alerts. I thought the number was not normal therefore I asked Raoul about it, and he said that is because I am exposing more ports than needed. He told me to only expose ports 80 and 443 for the website and use VPN to access the SSH and Wazuh.



I am proud of the Network Monitoring System solution that I provided for my own website. It would help me to stay engaged with it until the next semester starts. I am planning to keep monitoring my servers for a long time.

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 at vulnerabilities around the world.

I practiced Zeek, nagios, and many other monitoring systems that gave me a good foundation for how companies monitor their infrastructure.

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.

I managed to keep up with my group members on the 2 projects that I did with them.

Some of them were students from software background so they taught me some stuff about securing the backend and the database. I myself, am a media design and suggested for them to choose a JavaScript framework for the secure solution as it would saves us time to focus more on the monitoring system.

For the pen testing project, we worked together from 9 - 4 for 3 days to find vulnerabilities on our client website. We divided the work between each other equally and helped each other when needed.

I am grateful for everything my group mates taught me, and I am so happy that I got to also share my experience with other students.

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.

Portfolio

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.

After weeks of applying to multiple companies, some companies haven't responded, and most of them rejected my application. I talked with teacher Raoul about it, and he guided me to form my applications in more personal style. I started doing research on companies that I want to work for, and I sent them personal messages asking for good assignment for me.

I got accepted to have an interview by 2 companies, https://www.surf.nl/, and https://www.tue.nl .

I did the interview for both, and they both showed the interest for me.

I got to a point where I need to decide which company do I want to choose, I talked with teacher Raoul and Jeroen and they both agreed that the assignment at TU/E is better for me as they will allow me to work in a dedicated SOC for security students. The TU/E group is called ESH-SOC (Eindhoven Security Hub – Security Operation Center) and it is filled with passionate students that share the same interests as me.

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.

I followed 4 main sources to study networking.

1- ITPRO.TV – CCNA: it is a 20-hour course that brings good explanations and practices at the same time. It took me 30 hours to complete it as I needed to rewatch many lessons to finally get the idea. (https://www.itpro.tv/)
2- The official CCNA book: In addition to a digital course, I needed to get the book as well to balance my learning process.
3- CertBros YouTube channel: This guy has always simplified tech things for me since I started my bachelor. He explained networking subjects in details with clear examples. I spent approximately 7 hours watching YouTube courses. (https://www.youtube.com/@Certbros).

4- Cisco Packet Tracer: It is free application produced by Cisco to create and simulate virtual networks with the need to engage with cisco products command line. I spend 15 hours creating networks and simulate the.

Throughout this assignment I learned so many things related to networking, and I also got to practice these things in the packet tracer. I feel confident that I covered all the subjects that I need to build a strong foundation for my networking skills.

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 sources 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.

After that, I got to apply my hacking skills in a realistic environment with my group members, I am proud of the things that we found and advised the company to fix.

In last project, I developed my infrastructure skills by designing and building a production environment that consists of highly secured frontend, backend, and database.

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 encouraged me to spend too much time learning networking.

My next plans are to improve my personal website by adding all the projects I have done and making it more responsive. I will also setup a monitoring system for my webserver to practice what I learned in this semester in the upcoming weeks.

Personal website: https://mohammedx.tech