PORTFOLIO

Cyber security, Semester 4

Rik Leemans
[redacted]

Contents

Introduction

knowledge and experience on security

I am Rik Leemans, I started this training, after I had passed the havo. So I didn't have any MBO prior education. In recent years I have chosen software as a choice. Now I want to specialize myself in cyber security. In recent years I have done some research myself into networks, virtual machines and software programs. for this I have read studies and watched explanation / instruction videos. I myself have occasionally been busy testing this myself and seeing what it does and how far I get. I also have my own website where I practice and try to play different things in security and network.

What was your preferred learning style

I think my favorite learning style is coused based basis. I would like to be able to learn and practice freely without having to follow every hour to a class, I like to follow a workshop together on a subject where the basics are told and it is up to you to find assignments and other information. As a result, you are interactively engaged with the teaching material, which you can then apply in your own project. What I also really like is that with other students you teach each other things and help when you can't figure it out, so that you can figure out small things together.

What motivated you to join cyber security?

I wanted to follow a course in ICT from the age of 7. I've always been interested in computers and software and the security around them. Later on, my choice always remained for ICT. This is because you can find work in it and it always remains a challenge to carry out your work. In addition, I would like to remain a learner even when I start working, I want to continue to improve myself. Ict is therefore a good profession that suits me. You have to keep up with it, what every day it changes.

What are your strengths and weaknesses

My strengths are very clear to me! I have always been a go-getter, if I want something I always go for it. Furthermore, I am a team person I can get along well with others in a group or work. I am also someone who can take the lead, I like this and I can work clearly in insight points what needs to be done so that the planning runs smoothly and everything is clear. I have been a scrum and project leader at school several times and have been a manager at companies where I work for several years.

Furthermore, I also have a few weaknesses my English is not excellent, I can use basic English but my grammar is not always completely correct. Also a small point I could change is to arrive on time for the lessons and group. May still be a few minutes later. I have already changed this to a large extent, but there is always room for improvement.

Learning outcomes

Ethical Hacker

I liked the ethical hacker, I wanted to learn more about this in the previous semester. This semester, that has come into effect. I didn't have much experience in ethical hacking so many of these topics were new to me. But there were also subjects that I have already practiced at home once, which I have been able to improve. This is mainly about SQL and script injection. These were also my favorite throws. View my BOK document.

Mainly I got my knowledge from the workshops and from the course on the fhict website. I also watched additional videos to study an example and the operation of a topic. Furthermore, I have practiced my knowledge on exercises of DVWA application. This can be found in my BOK document.

I've learned a lot more about red teaming this semester. I have learned that much more is needed in preparation to be able to perform a PEN test ethically on a network. This happens in footprinting, reconnaissance and social engineering, Then you also have to try to find access with different scanning methods. These are subjects that you think less about in the beginning and yet are very important to learn about. Finally, I used many new tools to access a network or operating system. For example, xsser for script injection or ettercap for spoofing.

I am proud that I have been able to perform all the exercises in DVWA, I have learned a lot from this to understand the basics of the subject of tooling. I was then able to apply this to the PEN test.

I want to continue with red teaming, I would like to know more or the tools you use to enter a network. I also want to learn more about the different approaches to perform a pen test. I hope that I will learn more about this in the internship semester, because I am going to do an internship in red teaming.

Next time I might do more exercises at a higher level. I'm in it with these topics for most fairly new ones. I want to continue with my internship in this, so therefore try more different difficulties.

I would give myself a show, because I have worked out all the basic exercises in my buck. Furthermore, I have performed few advanced exercises. Well I show that I master the basic levels of all subjects, this can be seen in my BOK.

Risk Consultant

I think risk consultant is a less interesting topic in cyber security, but it is a topic that should be covered in this specialization. The interesting thing I covered during this section was about secure threats, because this also has something to do with ethical hacking that I would like to study further. For this it is also important that I know the threats of the cyber security profession.

I have applied my knowledge through information available on the canvas page of school. In addition, I have seen video and news articles on the topic of secure threats. Then I applied this in the assignments I made in my body or knowledge on the title page a link to the knowledge.

In this part of cyber security I learned what the threats are applications, networks or servers. That they can not only steal or delete data, but also carry out a real attack to demand money. This not only damages the server but also the staff and the company.

I am proud of my explanation of the top 5 cybercrimes that are described in my body of knowledge. In it I explain 5 different crimes that can be performed on a company on an individual. In it, it mainly explains what those risks are of the crimes and how you can best prevent them. Look in my body or knowledge if you are interested.

I would continue with that topic of cyber security to keep an eye on the news for future cybercrimes. I think it's important to stay on top of what's happening in the cyber security world.

Next time I would like to improve my tables in my body of knowledge. They do look good for knowledge document now, but it could have looked more professional.

I would give myself a show, because I have worked out all the basic exercises in my buck. Furthermore, I have performed few advanced exercises. Well I show that I master the basic levels of all subjects, this can be seen in my BOK.

Security Engineer

Security engineering was an interesting topic. Especially installing the firewalls on my network from netlab. I learned a lot about networks and infrastructure. I also learned about how to securely connect to your network through VPN. In addition, there was also an interesting workshop on detection and prevention, here you will learn about tools that can prevent a virus from spreading across the network. You could also get an overview of what is connected to your network.

I got my knowledge mainly from the canvas website and the workshops at school. In addition, there were also a number of instructions documents and videos to install tools on your pfsense. this can be found in my BOK. Finally, I worked with many other classmates to set up the firewalls on my netlab. Others have helped me and I have helped others, works well.

I learned how to safely think about setting up a network. It is not just about setting up, but also thinking about how to make a secure connection. Firewalls should not allow all requests to pass through if they can see dangerous. By means of detection and prevention you can prevent this.

I am most proud of setting up my network on netlab. I have been able to perform and install all the exercises on my network. This took a lot of time and effort, but it is nice if it has finally succeeded. This can be found on my netlab network or BOK document.

I would like to keep track of detection and prevention. They are interesting tools that stop many attempts at network intrusions. It is interesting to continue practicing these aspects, especially because I am interested in red teaming.

Next time I would immediately start with my netlab network. Now I had postponed it for a few weeks but it was more work that I had expected this I would plan better the next time.

I would give myself a show, because I have worked out all the basic exercises in my buck. Furthermore, I have performed few advanced exercises. Well I show that I master the basic levels of all subjects, this can be seen in my BOK.

Security Analyst

In security analyst I learned a lot about detecting security incidents. This means not only seeing but also analyzing what you are dealing with and reporting this. Eventually I started to discover patterns in different situations to assess how bad the situation is. Ultimately, you can use this to strengthen your application or network.

I have taken my knowledge from canvas and workshops that I have applied in my BOK. I have also extracted some information from sources from the internet, for these sources I refer you to my BOK source list.

I have learned how to monitor a network, with this I can keep an eye on everything that happens on it and which machines are connected to it. I also learned what tools I can use to manage and detect incidents on a program. Finally, of course, you will also learn about making a report and delineating the weaknesses and preventing it from happening again next time.

I am proud to set up nargos detection program on my netlab network. this allows me to monitor my network and get a notification in time when an incident occurs. Check out my BOK for more information.

I will certainly take into account how to deal with it when an incident occurs on your network. I myself am interested in penetration tester, so knowing what the other party does or does not get notification about what they do with it is important to know.

Next time I would try to get further with challenge in this part of cyber security. I only did the basic challenges because otherwise I would be short of some time. Next time I would like to follow some extra assignments or training, because it remains an interesting topic.

I would give myself a show, because I have worked out all the basic exercises in my buck. Furthermore, I have performed few advanced exercises. Well I show that I master the basic levels of all subjects, this can be seen in my BOK.

Security Professional

I mainly applied this topic in my group project. In my group project I applied how to work together in a group. But also how to manage a good and clear project. You also have to deal with cultural differences, because not everyone speaks Dutch, you have to get along in English. Finally, of course, you have done a lot of research for the information you have documented in your report. You present this in front of the class.

I have applied these skills with what I already know or have learned in previous semesters. Every semester you will of course learn something about how you can best work together in a group on a project. We also had a number of workshops on how best to do your research.

This semester I was able to practice my English again in the group project and the presentations. This is very nice because my English does not have the best pronunciation I have to keep practicing. I have also been able to apply better planning in our group, last semester we ran out of time. This semester, the group's planning was better organized and planned.

I am proud of my English accent which has gotten better in this semester. Every semester I see the weather improve not only me but also classmates. I hear from my group (Cas, Brit, Daan) that it is better than when the semester started. This is nice to hear.

My English will hopefully continue to improve next semester is a matter of continuing to talk. I would also like to continue to improve my presentative skills, because I think this is important. Usually that is the end of a project and that must of course be presented at its best.

Next time I will start looking for more internships. I had found an internship but it had been cancelled at the last minute, so I don't have an internship now. I would not only start earlier but also look for more internships.

I would give myself a show, because I have worked out all the basic exercises in my buck. Furthermore, I have performed few advanced exercises. Well I show that I master the basic levels of all subjects, this can be seen in my BOK.

Personal Projects

Personal Vulnerability Investigation

For my PVI I worked on it for about 18 to 20 hours. I think I worked on about three hours a day for six days. I first started researching my LSC camera, then I started testing it for its weaknesses. And finally, I have fathered this and written it out in the report.

Personal Specialization Project

For my PSP I worked on it for about two weeks. I worked on my PSP for 4 days every week. Have been busy for about 4 hours a day, which comes out to a total of 32 to 35 hours. I started by coming up with an idea to work out, which I then discussed with the teacher. After that I started researching the project, mainly on the website of OWASP. Then I started documenting and testing it on my application from last year. Finally, I have incorporated it into my report.

Internship Preparation

For my internship I already spent quite a lot of time in it. I already had an internship in the beginning, but it was cancelled at the last minute because the internship supervisor was no longer available. After this I started searching on LinkedIn, google ASAM and other vacancies. I've emailed about 25 different companies, but I still haven't found an internship. I have been working on it for 12 hours now, spread over several days. I keep looking for an internship.

Overall Conclusion and Reflection

I think I've done pretty well this semester. I have made and executed all the basic assignments, in addition I have covered all the underwork of my goat in my report. I have included feedback from my teacher and incorporated/improved in my BOK. I also created and completed both my projects through a presentation in class. Finally, I created my portfolio that I learned and did this semester.

I have also improved my learning process in this semester, not only individually but also in the group. I learned a lot about cyber security in this semester, this can all be found above in this document. As a member of a group, I have also been able to practice some teamwork qualities, this can also be found in the Security Professional section.

Finally, what I find most important in my personal development is passing the semester cyber security, because I would like to continue with ethical hacking. I am going to stay busy with this topic and also try to find an internship here. I have also been able to practice my English again, this is not yet optimal but I will continue to work on this in the coming years. This was a good semester.