Acquire Body of Knowledge

Dimitar Lalev | ICS-CS4 | 27.02.2021

# How to become an Ethical Hacker

An ethical hacker is a hacker that works with ethical mindset. So this type of hacker can hack everything, but he can do it only with permission given by the other side and if it is allowed to do so. Ethical hacker can also test and report in a methodical way for a client. So far I understood that ethical hacker means:

* Being ethical

To be ethical hacker we need to research the typical ethical norms for a hacker. Maybe we should compare them to our own norms and if there is some difference we should follow the ethical norms, because otherwise we can easily break the laws.

* We can hack ‘everything’

To be able to hack everything we should learn how to hack websites, servers, networks, humans and lower level hardware systems. It is impossible for a beginner to learn everything, but they want us to learn at least 3 of these categories, so we can perform the typical hacking techniques.

* Knowing your tools

A hacker is not ‘a fool with a tool’, but we should know the tools that we are using and how to use them.

* Working for a client in a structured way

Pen testing methodologies such as OSSTM, PTES are used to structure the process of a pen-test for a client.

## What I learned and how

Learned what is the difference between a hacker and an ethical hacker. And that it is important to work with an ethical mindset. Ethical hacker can hack everything, but only will do if it is allowed or can be handled in a responsible way. This subject is relevant, because it is important to understand that the difference between a hacker and an ethical hacker is bigger than we thought. It is important, because otherwise we can break the laws easily and get into danger.

At this point I understand the subject, but so far I haven’t learned that much theory. I will practice more with the workshops and the tools provided in canvas. First I will begin with Wireshark and Linux and then I will continue with other

practical stuff. I started learning more about Linux and it seems interesting and in the same time probably a little bit difficult. I will follow this challenges:

1. **Law, Ethics and responsible Disclosure**

From this chapter we understood the laws and difference between ethical and non-ethical hacker. I did the exercises and found out that there is almost none information about a big hacker attack in my home country – Bulgaria, where 5 million Bulgarians have their personal data stolen. We only know that the hacker was 20 year old computer programmer. The fun part is that the hacker emailed the national tax agency saying that “The state of your cybersecurity is a parody”. The hacker used SQL injection to collect data from the servers. The 20-year-old hacker was arrested and was charged with breach and theft of personal data. According to police, the released data also contained a lock file with information about the attacker's computer and username, which matched the one Boykov used in social media. The lock file, however, was dated before the supposed time of the attack. Boykov was released on 18 July, on the grounds that his attack had not affected critical NRA databases.

I made research in some websites and checked out the resources we were given in Canvas. For the research about the National Tax Agency in Bulgaria I used Bulgarian resources, because the case was the most popular hack in Bulgaria, because 5 out of 7 million Bulgarians were affected. I also participated in a lecture about the laws and ethics and there we just talked about some cases in the Netherlands and other countries. We compared the cases and also looked at the charges of the hackers.

1. **Tooling**

In the beginning of week 3 I could say that I learned a lot about the Seclab, because we had to make accounts and connect to the VPN in order to use the VM. I created virtual machine with Kali template and started watching tutorial about Linux and Kali to be more specific. I set up the network and static IP. Started exercising with linux commands and navigating through the linux files and directories. Started watching Wireshark tutorial. Watched all the tutorials given in Canvas and did all the challenges, except of the expert ones. Now I know how to view packets and how to use display filters to find and see what I want to see in the capture. Also learned what is the capture settings. It is used to limit what I need to capture. Next thing I tried is to follow stream or more specific TCP stream. I received a lot of dots on the stream I tried to follow, which means there were a lot of non-printable characters. The traffic from the client was colored red and the traffic from the server was colored blue.

Next thing I made is to extract image from a PCAP file. I followed the steps, given in canvas and downloaded PCAP file. Then I opened the file and forwarded to Export object -> HTTP. Then I opened file called “owned” and it was a flag, saying the flag is Apple Sauce.

I already learned that it takes a lot of time and effort to make the thing work the way you want them to work. Or in other words – I don’t want to be “a fool with a tool”. Started watching tutorials and took a look at the reference in Canvas for the introduction to Linux, where I found a lot of useful commands, but need to follow some tutorial or to practice them to understand what they do and how do I use them. After the workshop for Linux this Friday I think I am more confident and learned a lot of new commands.

1. **Basic Hacking and Pentesting Process**
2. **Footprinting, Reconnaissance and Social Engineering**

I understood why this phase is so important in the pentesting process. This is basically the first stage, in which direct actions against the target are taken. It is really important to know as much as possible about the targeted organization.

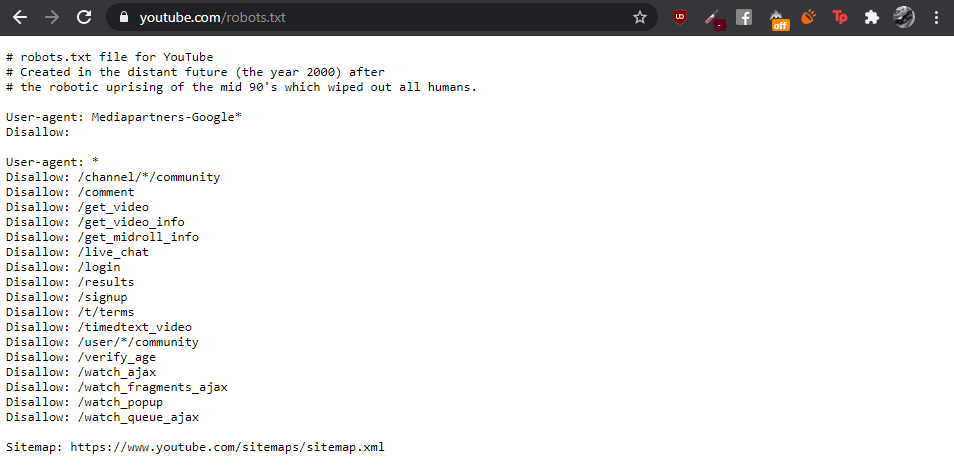
The technique used for gathering information is called “Footprinting” and to get the information a hacker can use various tools and technologies. Open-source Intelligence or in other words – OSINT is intelligence collected from public available sources. This could be everything from internet to the TV. I also learned that we can collect data with:

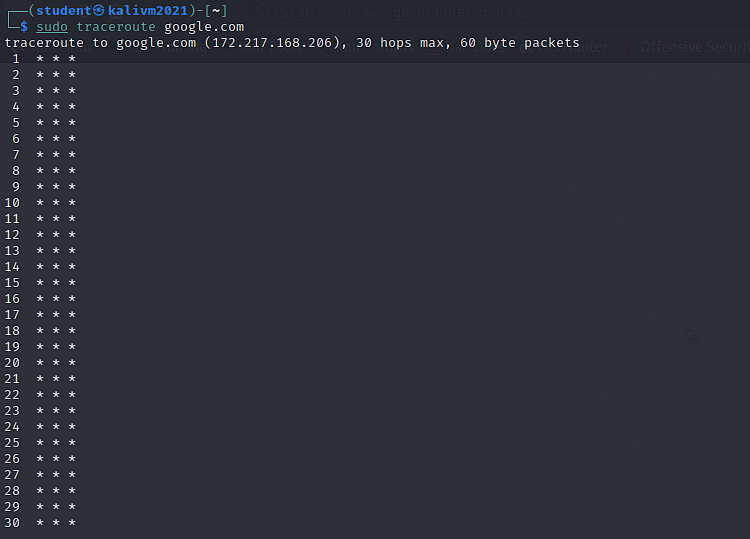
* Google searching
* Network information discovery
* Social network analysis

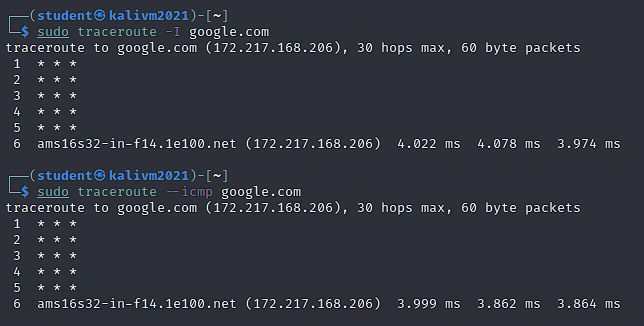
I did the challenges and tried the wayback machine. I checked nu.nl’s front page from 10 years ago, which I found pretty cool. This wayback machine let us see the previous versions of the sites.

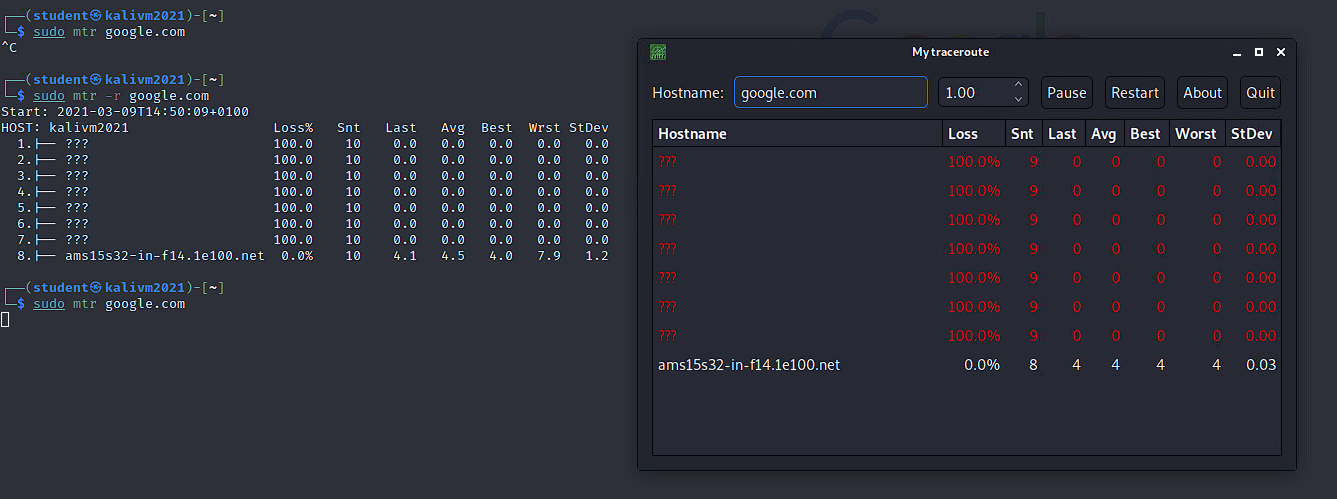


Then I continued to the next challenge, which was to discover what URL’s are hidden from search robots in robots.txt files of Pentagon and Whitehouse. I just did this with adding /robots.txt in the end of the homepage or the root directory. And I found this for the White House  

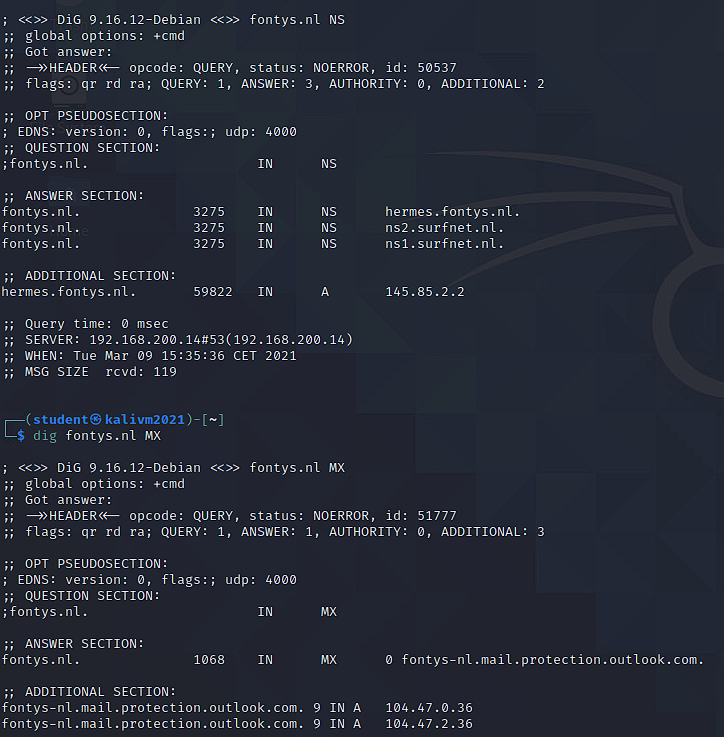

I also tried that on YouTube and found something pretty funny and interesting. The robots.txt file has a comment in the beginning saying: “Created in the distant future(the year 2000) after the robotic uprising of the mid 90’s which wiped out all humans”. I’m not sure if it’s funny or scary, but it looked interesting for me.  


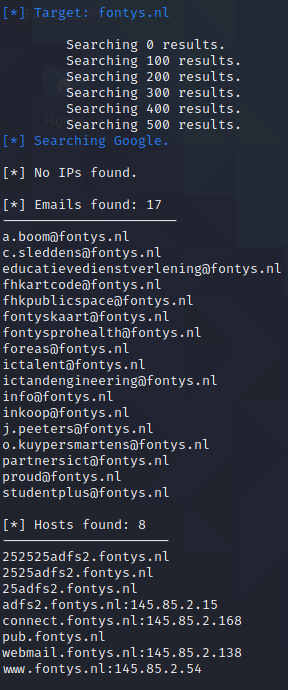
Next I used tooling for **traceroute** to determine path to google.com, but I received only stars  


Then I tried different command, which use ICMP echo packets, which are blocked less frequently and gives faster results. The first command was **traceroute -I** and later I found out that it was the same as **traceroute –-icmp. **

Then I found out myself about other command like **mtr,** which combines the functionality of ping and traceroute. The output is being constantly updated. Also it is being open In another window and not in the terminal, but there is this command **mtr -r** , which allows us to keep it in the terminal.   


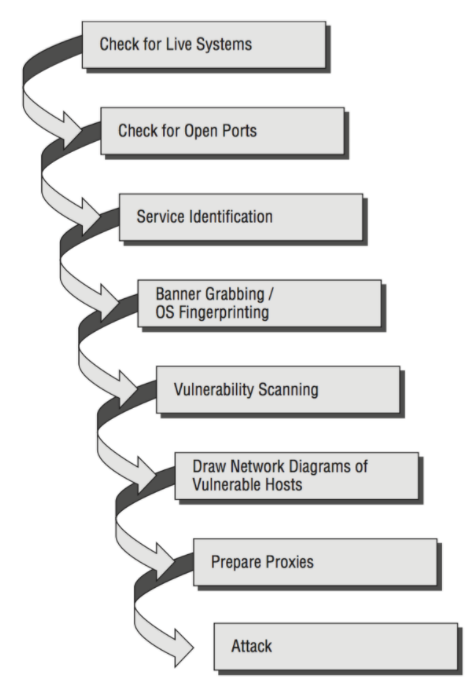
Next thing was to determine which DNS and email servers are used by fontys. I found this through the **dig** command.



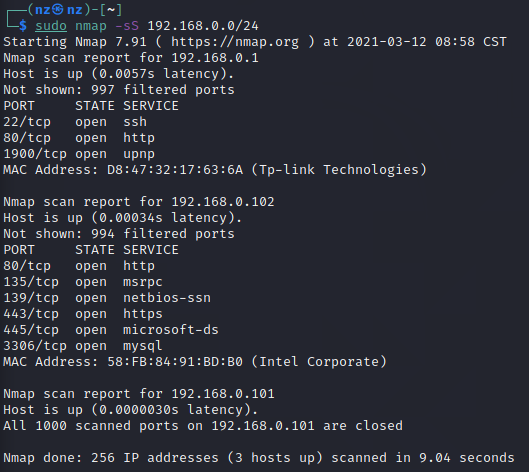
Finally for this basic challenges I ran theHarvester utility for domain fontys.nl and I found 17 emails and 8 hosts, but no IPs.   


This was the end of the challenges and now I feel way more into Footprinting, Reconnaissance and Social Engineering and I will proceed with the additional challenges for advanced level later, when I finish all the basic challenges.

1. **Network scanning and Enumeration**

In this chapter I learned how to scan a network and two different types of scanning – **nmap** and **metasploit.** The most commonly used is nmap and Metasploit is usually used if we really want to attack any system, but Metasploit is not considered as ethical and is not part of the pentest. I also learned that we need to be carefull when we are performing a network scan, because it often generates a lot of data on the network. The scanning process is as described.   


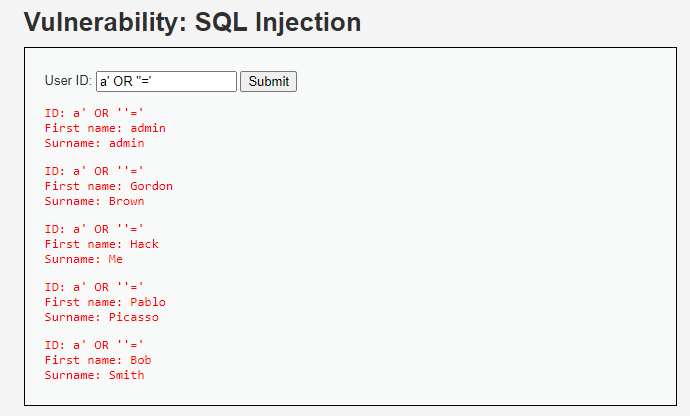
And now I am experimenting with nmap. There is a lot of different port scanning techniques and now I am trying some of them to understand the difference between them. For example this is SYN scan and is the most popular scan option. For example **-sS** performs quick scan of thousands of ports. It is also known as half-open scanning, because we don’t open a full TCP connection.



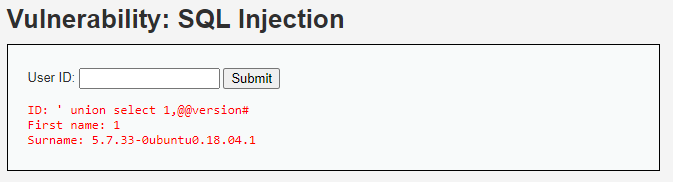
Now it says that all my ports are closed, but I am not sure if this is possible. I will investigate that and probably I will watch a tutorial about nmap, because I want to learn more about it.

1. **Web hacking: SQL Injection**

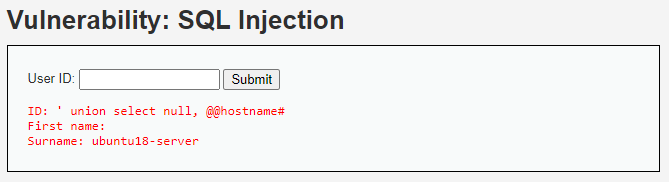
We had a workshop about the SQL Injection and I understood what is SQL injection and I am doing the SQL injection in DVWA. First I tried the low level and tried to list all the users first and last name with a query, which is always true.



Next step was to identify what is the kind of database they are using on the back-end so we can construct the queries accordingly and to extract the info that we want. We are doing this, because if we do not know the type of database we will not be able to exploit successfully the SQL Injection vulnerability. We can easily identify the database type when we are in a non-bind situation. If we try the query **‘ union select version()**  or ‘ **union select @@version,** but we received error, saying:

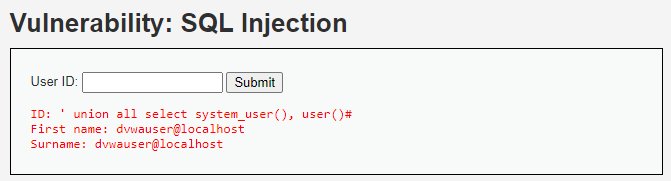
  
As I understood this error indicates that the two select statements have not the same number if columns. That’s why we cannot receive the version. In order to bypass this error I tried to increase the number of columns by 1, so this way we received the version.  


As we can see the query was executed sucessfully and now we know the exact version of the MySQL.

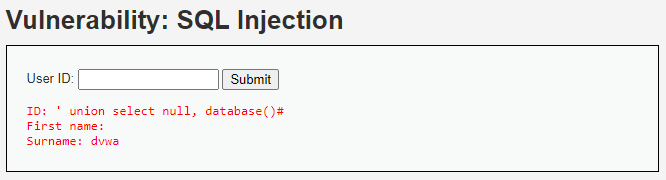
We can also see the hostname of the target with **@@hostname**:   


As we identified the database version and the hostname it’s time to look into the number of columns. I tried to do it with query **order by** and increase by 1 every time. Until it gives the error saying:

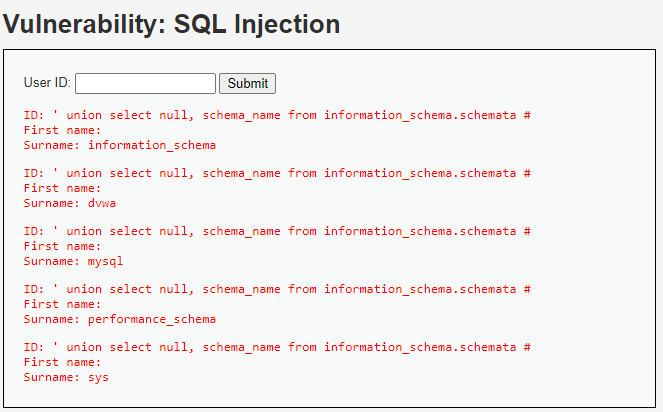


This means there are only 2 columns returned when the query is executed. Next I cheched who is the current user logged in with **‘ union all select system\_user(), user()#**

After that I tried to find the database name:



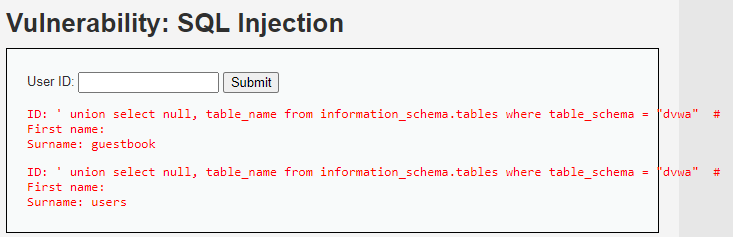
We can list all the available databases on the MySQL database with command select schema\_name from information\_schema.schemata which allows us to extract that kind of information regardless if we have administrator level privileges. So in this case I used **‘ union select null, schema\_name from information\_schema.schemata**



After I executed the query we can see that there are databases named: dvwa, mysql, performance\_schema and sys. The next thing I did is to try to discover the table names from information\_schema:



It showed many more tables than I expected, but this is because the information\_schema is the database that contains information for all other databases tjat MySQL maintains. But for example we can retrieve the tables from any database we want. For exapmle I chose database called dvwa and I found out that there were 2 tables there.



I also used String

1. **Web Hacking: XSS & CSRF**
2. **Web hacking Path Traversal, File inclusion and Command Injection**
3. **Network Hacking: Sniffing and Spoofing**
4. **Password Cracking**
5. **Specialist: System Hacking: Buffer Overflows**
6. **Specialist: WiFi Security Basics**
7. **Specialist: Other Wireless Hacking**

# How to become a Risk Consultant

Risk consultant is someone who has a broad overview of different security concepts. For this it is important to imagine that we are running a company with all the revenues and stakeholders. We should keep track of security threads, vulnerabilities, calculating risk based on objective observations and estimates. It is also really important to make good decisions on defensive security in order to make a good analysis.

* Having technical knowledge

To be a risk consultant it is important to have technical knowledge of all threats from physical security and awareness to specific threats in hardware or software code.

* We can categorise and prioritise

It is important to be able to categorise and prioritise threats and risks as they exist for a specific organization.

* We can advice and design

This means we can advice and design solutions to risk that matter to your client.

In order to become a Risk Consultant we should complete different challenges. We can gain skills by working on self created tasks.

## What i learned

So far I haven’t learned that much about being a risk consultant, because I don’t think we have any workshops about the security threats.

## How i learned it

I am still not competent in this subject, but soon I hope I will be more competent, because I will gain more knowledge in the course and will do my best to catch up. One lesson I learned so far is that the cyber security needs perseverance to learn.

# How to become a Security Engineer

Being a security engineer means that we can build a secure infrastructure or systems and grant end-user access to the system or infrastructure. A Security Engineer is equal to someone, who:

* Understand Networking and Infrastructure

We should master infrastructure and networking fundamentals.

* Can build a secure IT infrastructure and provide secure access

We can translate a business need into a logical network separation and segmentation and control secure access to the system or infrastructure.

* Can detect security threats and manage your environment

Intrusion needs to be detected and prevented. Incidents need to be monitored.

* Work in a structured way based on functional and technical requirements

This means we should be able to translate functional requirements to a technical design in a structured way and build accordingly to our design.

In order to become a Security Engineer we should complete different challenges. We can gain skills by working on self created tasks.

## What i learned

So far I haven’t learned that much about being a Security engineer, but we’ve got one workshop about networking and it seems really interesting and in the same time really difficult, because I’ve got networking only 6 weeks in the first semester, but they were even more basic stuff than what they showed us at the workshop. I will start with the first challenge as soon as I finish the first challenges in the Ethical hacker.

## How i learned it

I am still not competent in this subject, but soon I hope I will be more competent, because I will gain more knowledge in the course and will do my best to catch up. From the workshop about the networking we learned most of the things about the networking and the teachers answered some really interesting questions.

# How to become a Security Analyst

Being a security analyst means that he works in a Cyber Security Incident Response Team and can react adequately to imminent security threats. The analyst and his team can investigate hacks and other incidents, which are connected to security and can quickly process data from multiple sources, draw conclusions and initiate action. Being a security analyst means:

* We can detect, analyse and report security incidents

To be able to do this, we should obtain knowledge of SIEM systems and other monitoring systems. We also need to investigate the role of a CSIRT team within an organization. We are also responsible for the technical representation of the security incidents, working and impact.

* We can identify patterns in incidents

Incidents often appear in multiple sources and may be related. It is our job to understand relations and judge upon severity.

* We can evaluate security incidents and define improvements.

Based on the incident we should define security improvement.

In order to become a Security Analyst we should complete different challenges. We can gain skills by working on self created tasks.

## What i learned

So far I only read the first challenge and the reference in the toolboxes about the security Incident management.

## How i learned it

I read it in Canvas and waiting for the teachers to say something more about being security analyst.

# How to become a Security Professional

To become a security professional we should be technically skilled and we should be able to communicate with other security specialists, also with clients and stakeholders and with the customers. We should be able to explain to people with no IT knowledge how the technical stuff works or in other words to translate the hacking techniques or other security aspects to normal words so people can understand it, without any need of IT knowledge.

For this we need skills like interviewing, writing, presenting, collaboration with stakeholders, other experts and team members. Since in IT in general but also in cyber security these people could very well also include international colleagues, some intercultural training and training English skills are welcome. A security professional can:

* Interview clients, stakeholders, customers on security aspects, wishes, problems, issues.
* Diverse presentation skills to explain security findings to a client, issues and incidents to customers or stakeholders, advice to client, employees, consumers, etc.
* Write understandable reports, that can explain technical findings and solutions to a non-technical audience.
* Work with security colleagues, team members clients, stakeholders, target groups, experts from other disciplines.

In order to become a Security Professional we should complete different challenges. We can gain skills by working on self created tasks.

## What i learned

So far I understood that to become a security professional we need to be good in all the others body of knowledge skills. As soon as I understand how to handle everything I think I will be ready to become security professional.

## How i learned it

I am still not competent in this subject, but soon I hope I will be more competent, because I will gain more knowledge in the course and will do my best to catch up. Everything else was in Canvas or was said by our teachers.