Body of knowledge

Hristo Kolew

Table Of Contents

Version History:

11.02.2023	Basic Hacking and Pen testing Process
22.02.2023	Footprinting, Reconnaissance and Social Engineering
27.02.2023	Path Traversal, (remote) File inclusion and Command Injection
27.02.2023	WAF (Web Application Firewall)
28.02.2023	SQL Injection
06.03.2023	Host Intrusion Detection and Prevention (HIDS)
07-08.03.2023	XSS & CSRF
13.03.2023-15.03.2023	Network Scanning and Enumeration
14.03.2023	Law, Ethics and Responsible Disclosure
17.04.2023	Law, Standards & Compliance
20.03.2023	Secure Network Connections (HTTPS/TLS/SSH)
21.03.2023	Secure Remote Access and Management (VPN)
27.03.2023-29.03.2023	Network Sniffing and Spoofing
31..3.2023	Wireless Hacking
03.04.2023	Network Intrusion Detection and Preventions (NIDS-IPS)
18.04.2023	IT Basic Monitoring
26.04.2023	Identify and Access Management
17.04.2023	Password Cracking
17.04.2023	Network Separation and Segmentation (Firewall)
26.04.2023	Security Incident Management
02.05.2023	Common Vulnerabilities and Exposures (CVE's)
02.05.2023	IT System Hardening
03.05.2023	IT Security Monitoring

Ethical Hacker

Basic Hacking and Pen testing Process

What are the process steps of every pen test in general?

There are five penetration test phases: Reconnaissance, Scanning, Vulnerability assessment, Exploitation and Reporting.

Reconnaissance - In this phase tester gathers as much information about the system or network, such as IP addresses, domain names, open ports, user accounts and other relevant information. Reconnaissance can be divided on 2 methods: passive and active. While active reconnaissance includes directly interacting with the target system to gather information, passive reconnaissance draws information from sources that are already widely accessible.

Scanning - During this stage of penetration testing, the tester makes use of a variety of tools to find open ports and monitor network activity on the target system. Penetration testers must find as many open ports as they can in order to prepare for the upcoming penetration testing phase because open ports are potential entry points for attackers.

Vulnerability assessment - A vulnerability assessment is a thorough examination of an information system's security breaches. It determines whether the system is vulnerable to any known flaws, rates the seriousness of those flaws, and, where necessary, suggests prevention or correction.

Exploitation - In this phase, the tester attempts to access the target system and exploit vulnerabilities by using different tools to simulate real-world attacks. This is the most delicate phase of penetration testing due to the need to bypass security restrictions.

Reporting - In the final phase, the tester analyzes the result of the test and provide a detailed report of vulnerabilities found, the methods that he used for exploiting them and a recommendation for improving the security of the target system.

What are the minimal requirements for a good pen test contract and pen test report?

Both pen test contract and pen test report should be comprehensive, clear and provide actionable information that the organization can use to improve its security posture.

Pen test contract:

1. Indemnification clause – permission of the client that allows you to test and to address liability.

2. Confidential agreement
3. Scope of the test - should include the systems, applications, or networks to be tested, as well as the testing methodologies used.
4. Testing Timeline - defines the testing timeline, including when the testing will take place, the duration of the test.
5. Escalation procedure – in case of emergencies.

Pen test report

1. Scope and goals of the test
2. Explanation of your test approach
3. Test result
4. Conclusion

Reference:

E. (2022, August 1). *Understanding the Five Phases of the Penetration Testing Process*. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/

Richardson, L., Sillam, Y., Hasson, E., Hewitt, N., McKeever, G., McKeever, G., Rossi, E., & Hewitt, N. (2022, August 10). *What is Vulnerability Assessment | VA Tools and Best Practices | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/vulnerability-assessment/

Footprinting, Reconnaissance and Social Engineering

Explain why this is an important phase of the pen testing process

It allows a hacker to gain information about the target system or network. This information can be used to carry out attacks on the system. Footprinting is also used by ethical hackers and penetration testers to find security flaws and vulnerabilities.

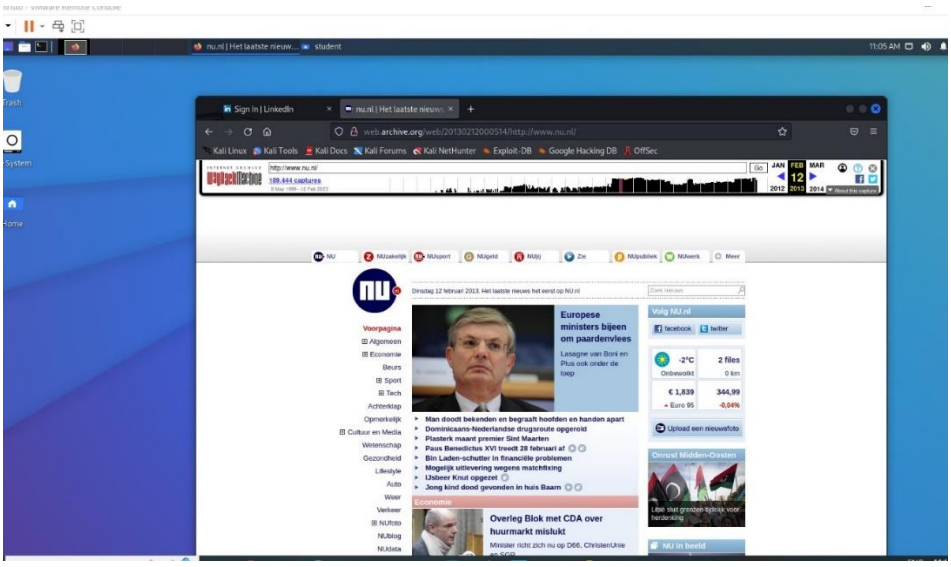
Make sure that you can show and explain at least 3 different techniques for searching useful information.

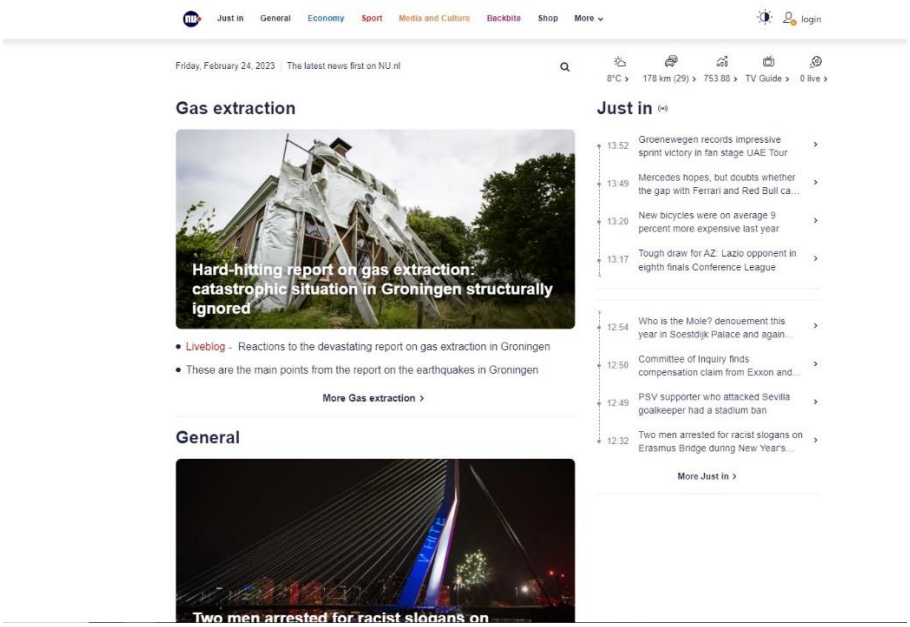
Find at least 3 people including email address (not management) that work within a large International Company, for example using social networks like LinkedIn.

The company that I researched was Architectural Digest and it is a vibrant monthly celebration of the international design talent, innovative homes and products, inspiring decoration ideas, culture, ad travel. I found 3 employees from LinkedIn with their emails.

1. Madeline O'Malley - Market Director, Email: madeline_omalley@condenast.com
2. Melissa Studach - Associate Editor, Email: m.studach@gmail.com, Facebook: https://www.facebook.com/melissa.studach
3. Allie Weiss - Deputy Editor, Email: sweiss303@gmail.com, Facebook: https://www.facebook.com/allie.s.weiss

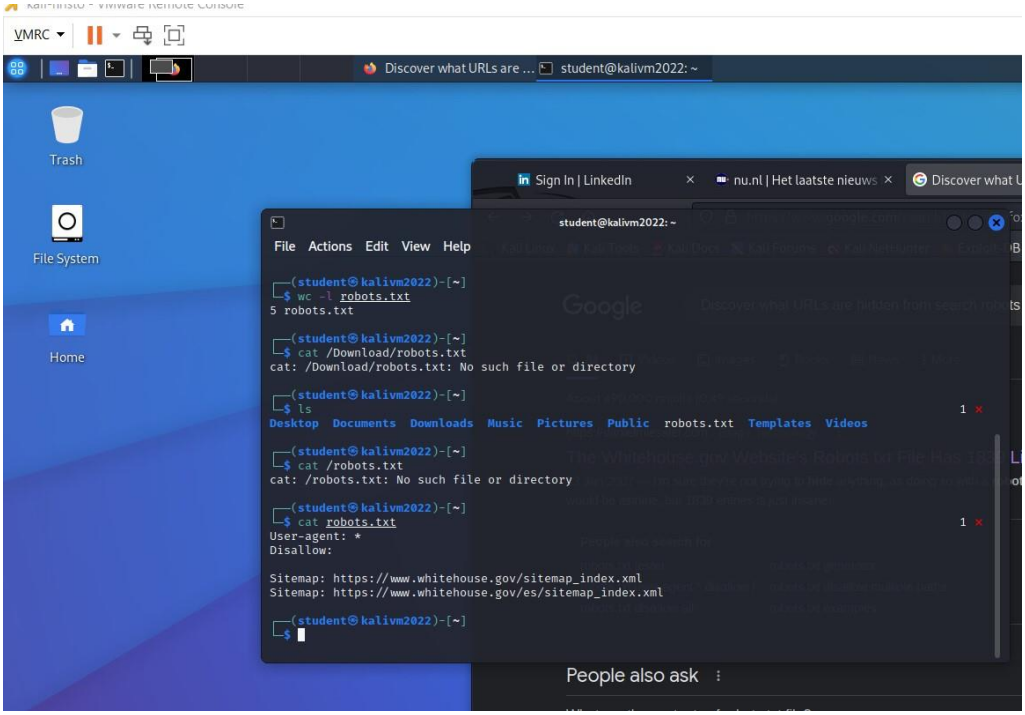
Find how frontpage of nu.nl looked like 10 years ago using waybackmachine.org





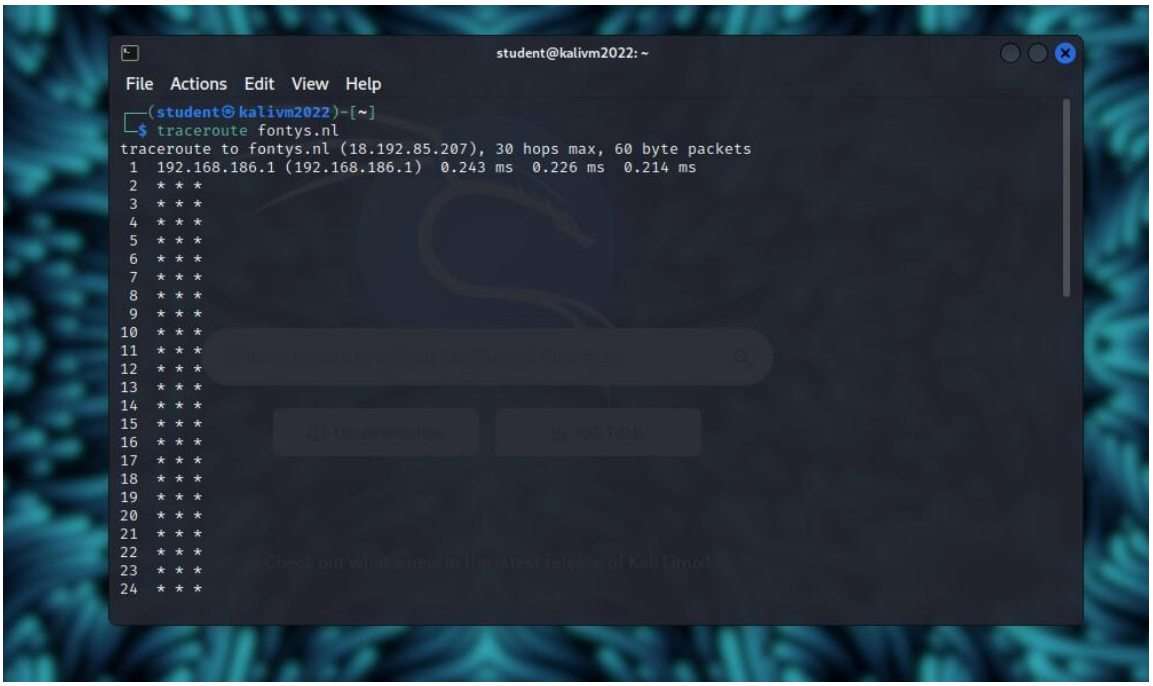
Here I present you the difference between nu.nl now and nu.nl 10 years ago. As you can see there are a lot of improvements in the design. Everything looks very structured and clean. I was surprised that they managed to made “Just in” section that is like a story board with the latest news. Very helpful is that they display live sports events, tv guide, stocks and traffic unlike before.

Discover what URLs are hidden from search robots in robots.txt files of Pentagon and Whitehouse.



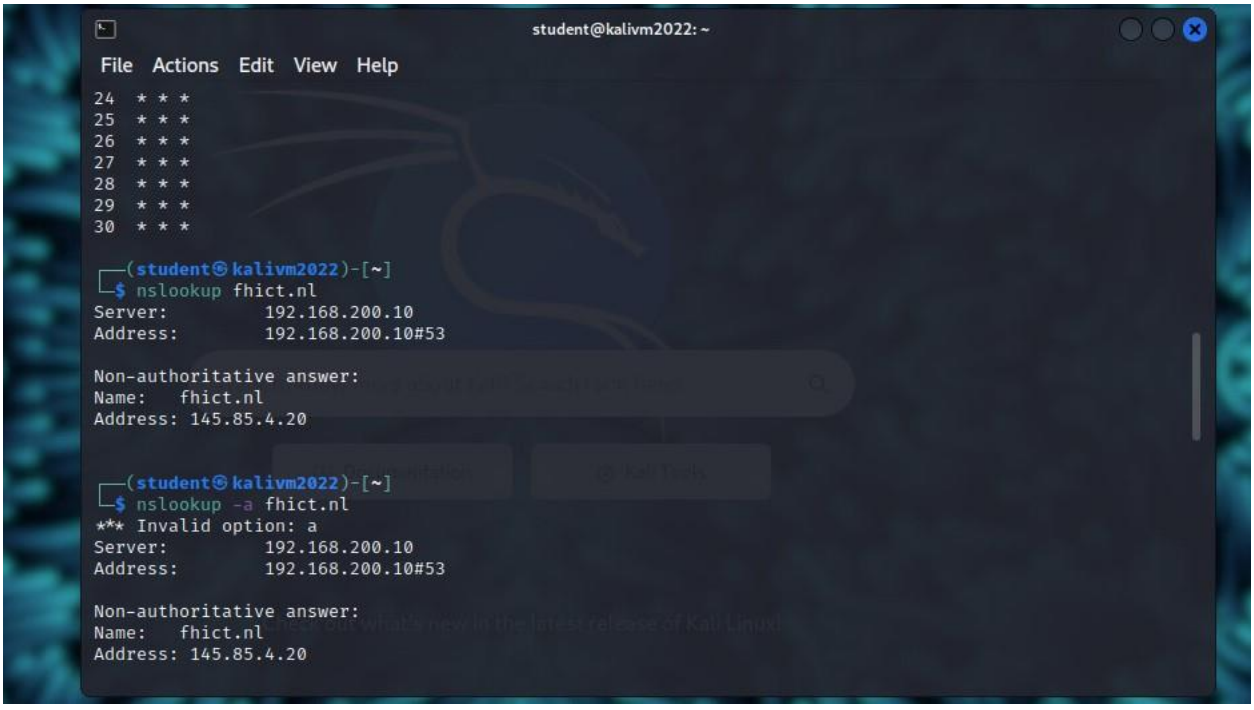
For this task I used several commands: ‘wget’, ‘wc’ and ‘cat’. With ‘wget’ command I download the file from www.whitehouse.gov/robots.txt. Then I user the ‘wc’ command to print how many lines this text file has. In the end I used ‘cat’ command to see the content of the file.

traceroute to determine path to fontys.nl, fhict.nl



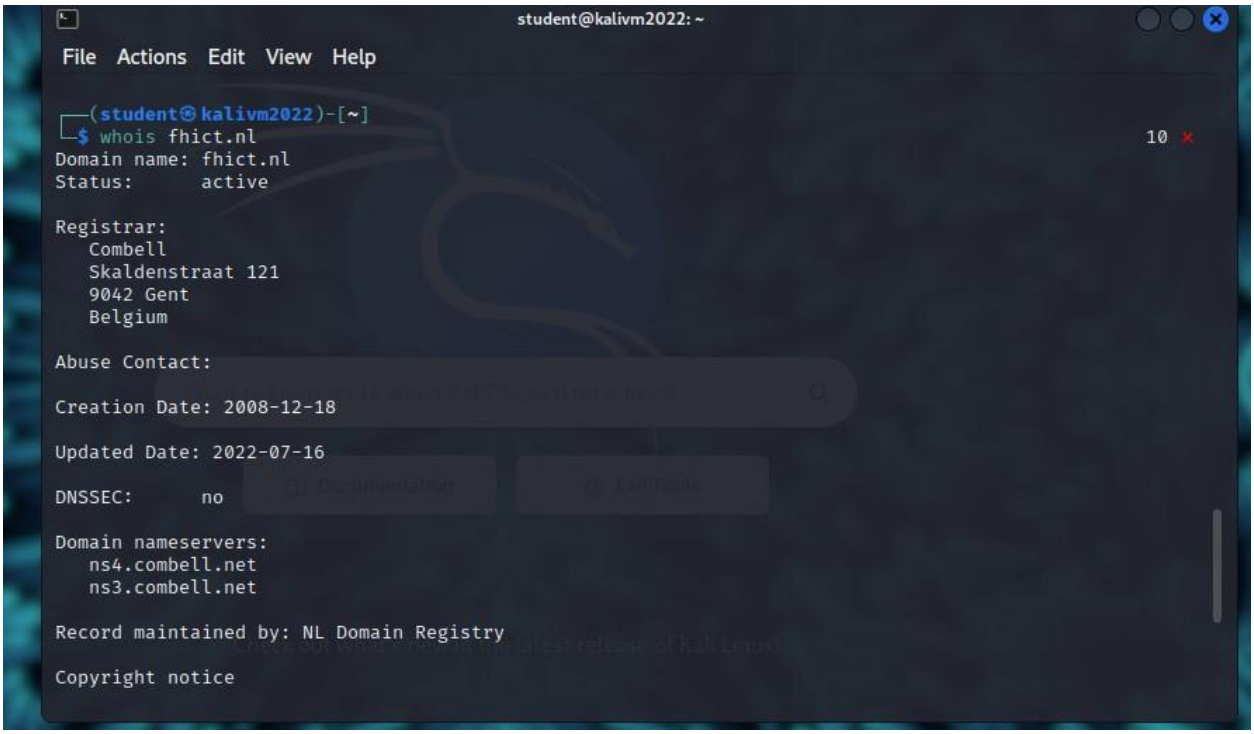
To complete this task, I used ‘traceroute’ command. Traceroute is a command-line tool for tracing the path an IP packet that takes across one or many networks. With this tool you can see how traffic flows and identify any irregular paths. It displays the time it takes to reach each “hop” between the source and destination, the length of the packet.

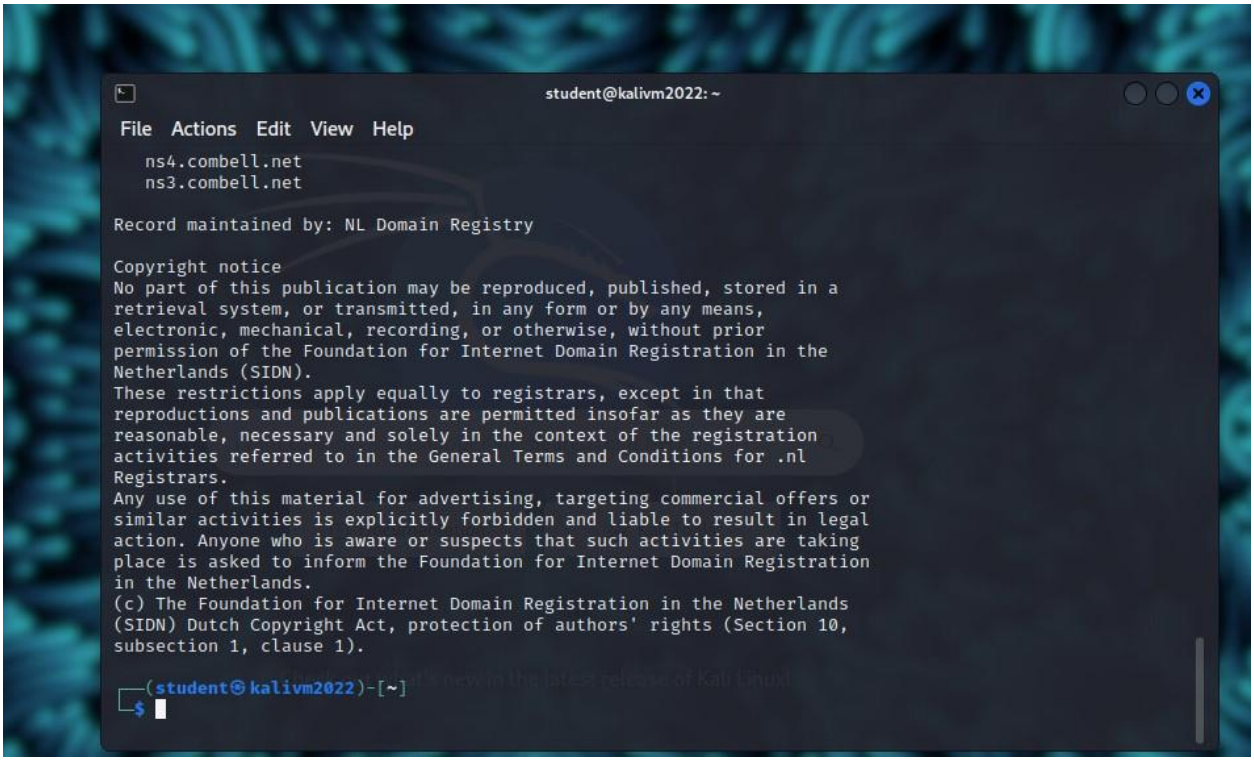
determine which DNS and email servers are used by fontys and fhict

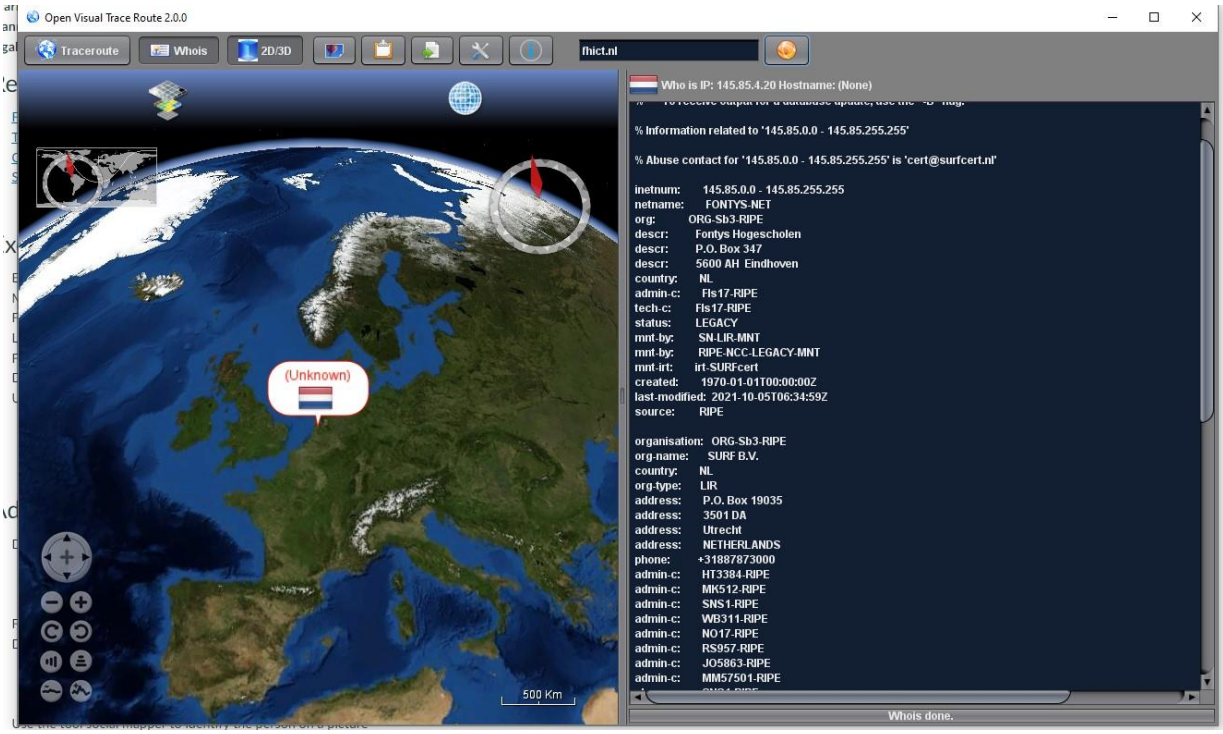


To determine which DNS and email servers are user by fontys, I used the command ‘nslookup’. In two different ways, the ‘nslookup’ command queries internet domain name servers. You can print a list of the hosts in a domain or query name servers for details about different hosts and domains while in interactive mode. For a given host or domain, the names and requested details are printed in noninteractive mode.

determine which ip-adressess are used by fhict by whois utility and non whois tool





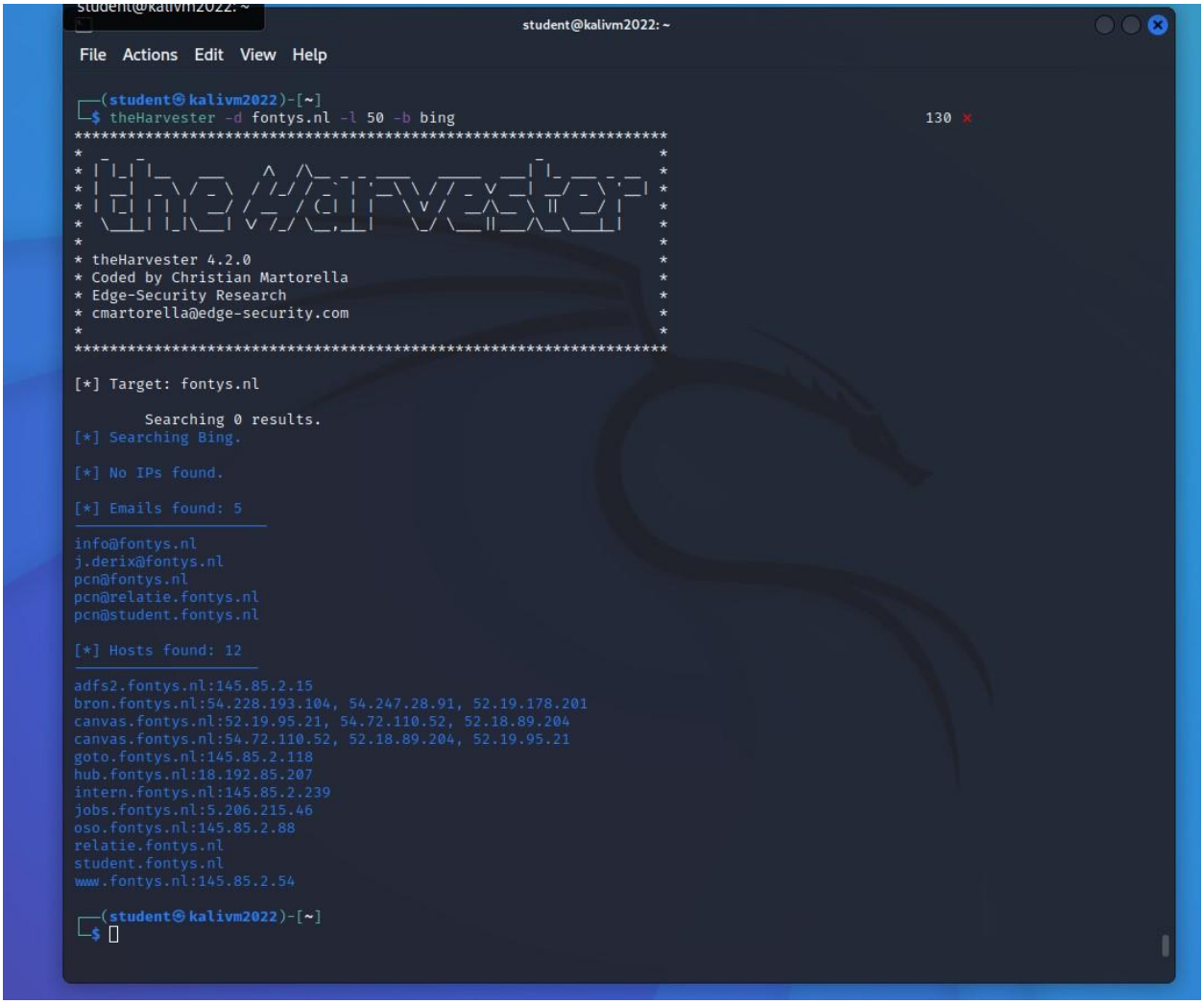


The whois system is a listing of records that contains details about both the ownership of domains and the owners. A whois record contains all the contact information associated with the person,

company, or other entity that registered the domain name. Some registrations contain more information than others, and some registries return differing amounts of information. (McKey, 2020)

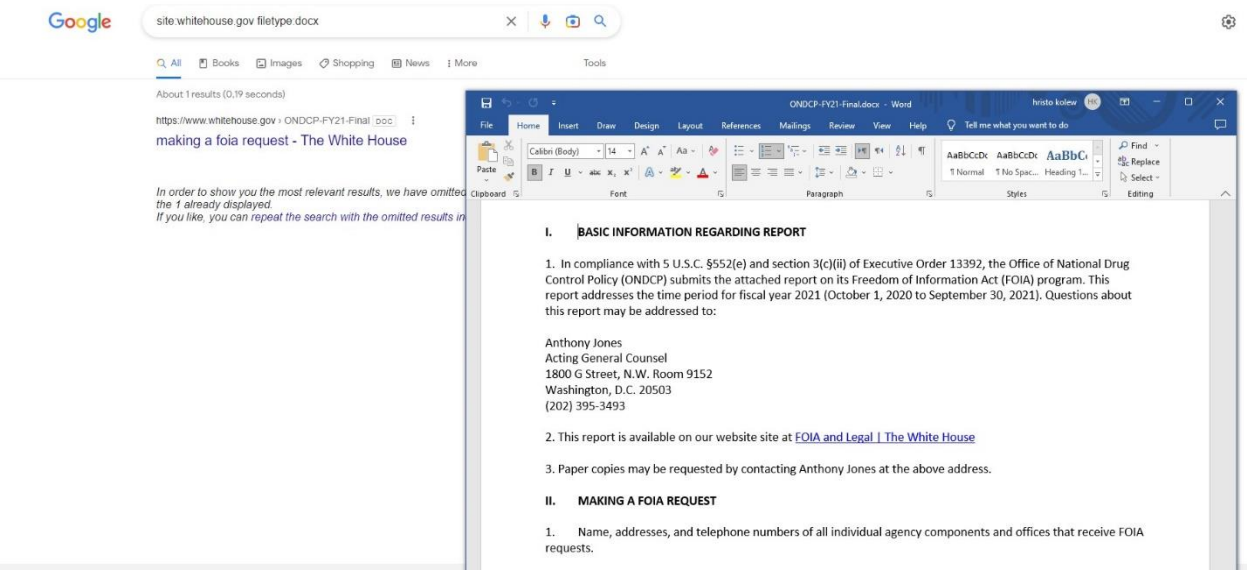
Open Visual Traceroute is networking toolkit which displays the path of your web traffic on 3D world map. Despite the "Traceroute" name, that's not all. Bonus features include a Whois tool, and a WinPcap-powered packet sniffer which shows exactly what your traffic contains.

run theHarvester utility for at least 3 domains of choice

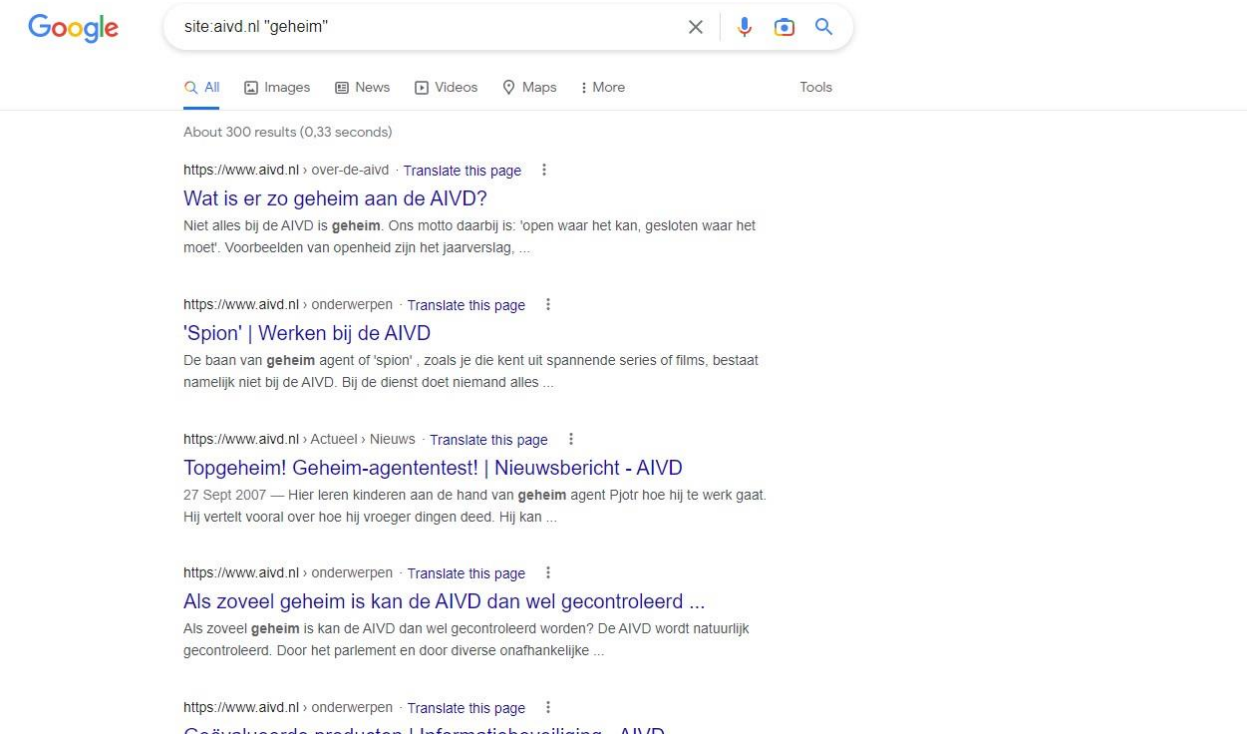


TheHarvester is a command-line tool included in Kali Linux that acts as a wrapper for a variety of search engines and is used to find email accounts, subdomain names, virtual hosts, open ports / banners, and employee names related to a domain from different public sources.

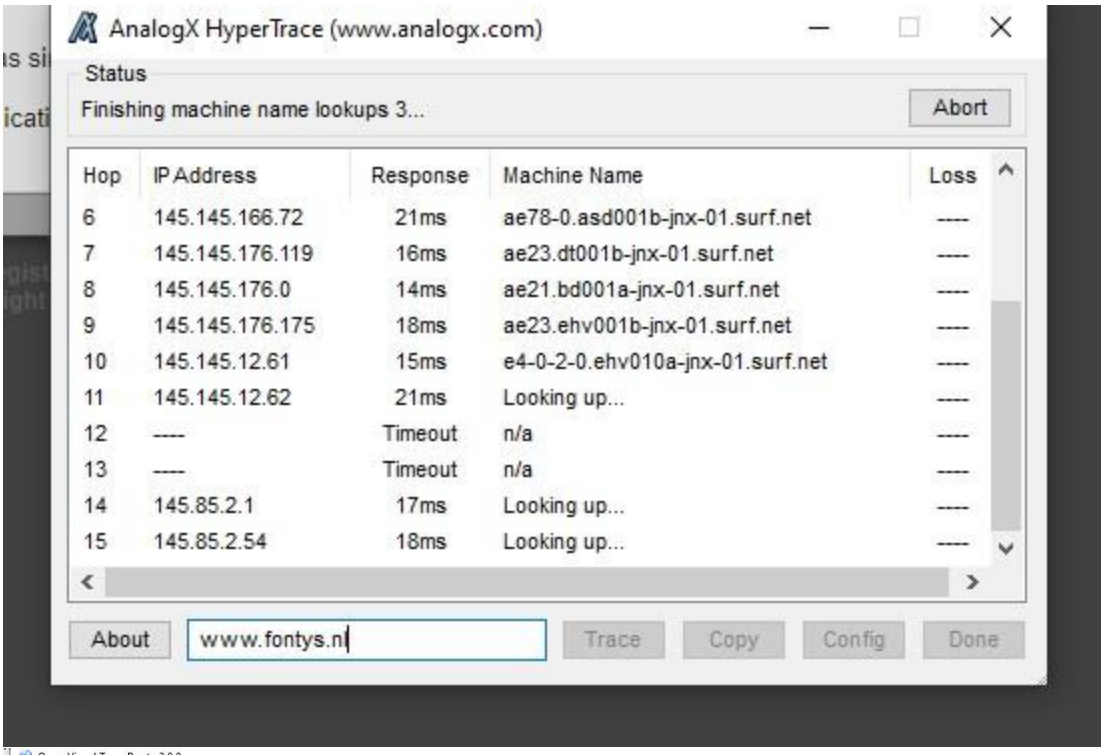
"filetype" - find all docx files on .gov domains containing phrase "top secret".

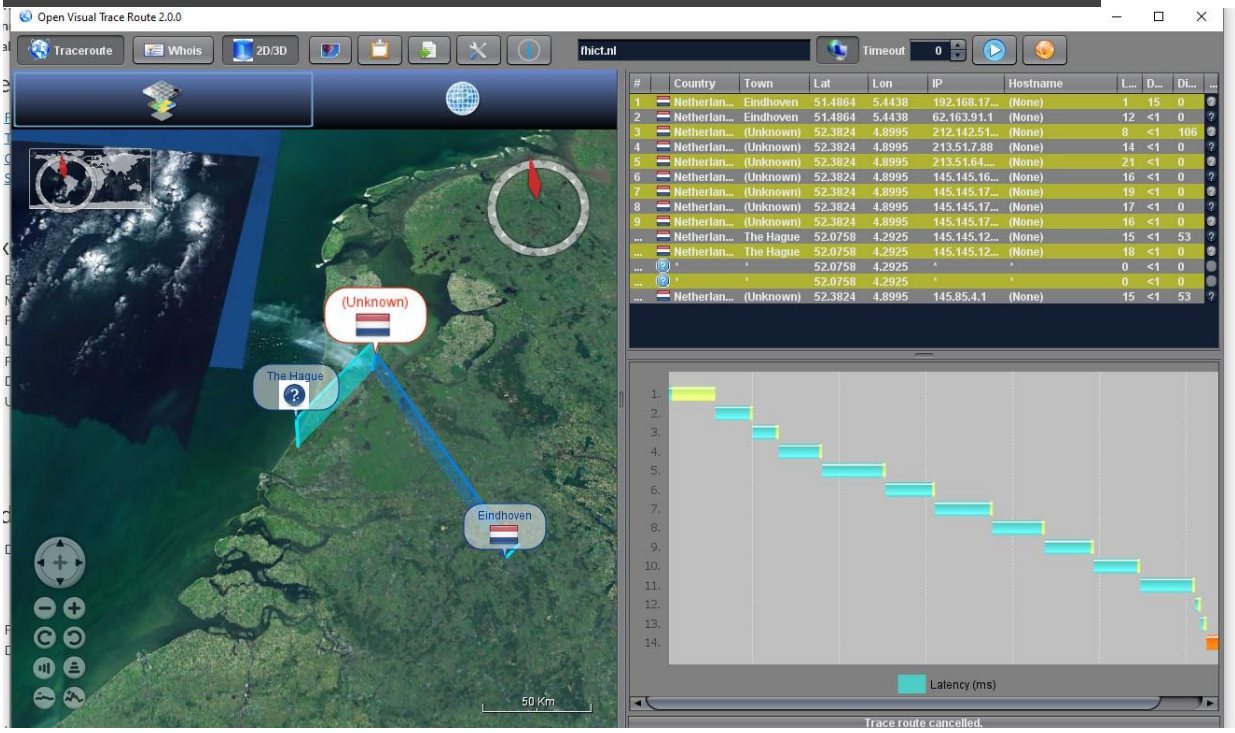


"" and "site" - find all pages containing phrase "geheim" on site defensie/aivd/mivd



Find 2 different visual trace route tools and discover why it's useful to use





I managed to find 2 visual trace route systems: First one is Open Visual Traceroute and the second one is AnalogX HyperTrace.

Open Visual Traceroute is networking toolkit which displays the path of your web traffic on 3D world map. Despite the "Traceroute" name, that's not all. Bonus features include a Whois tool, and a WinPcap-powered packet sniffer which shows exactly what your traffic contains.

AnalogX HyperTrace is a GUI version of traceroute, which shows you the route that information travels from your machine to another machine on the internet

Refences:

Grimmick, R. (2022, June 27). *What is Traceroute? How It Works and How to Read Results*. https://www.varonis.com/blog/what-is-traceroute

McKay, D. (2020, July 8). *How to Use the whois Command on Linux*. How-To Geek. https://www.howtogeek.com/680086/how-to-use-the-whois-command-on-linux/

Path Traversal, (remote) File inclusion and Command Injection

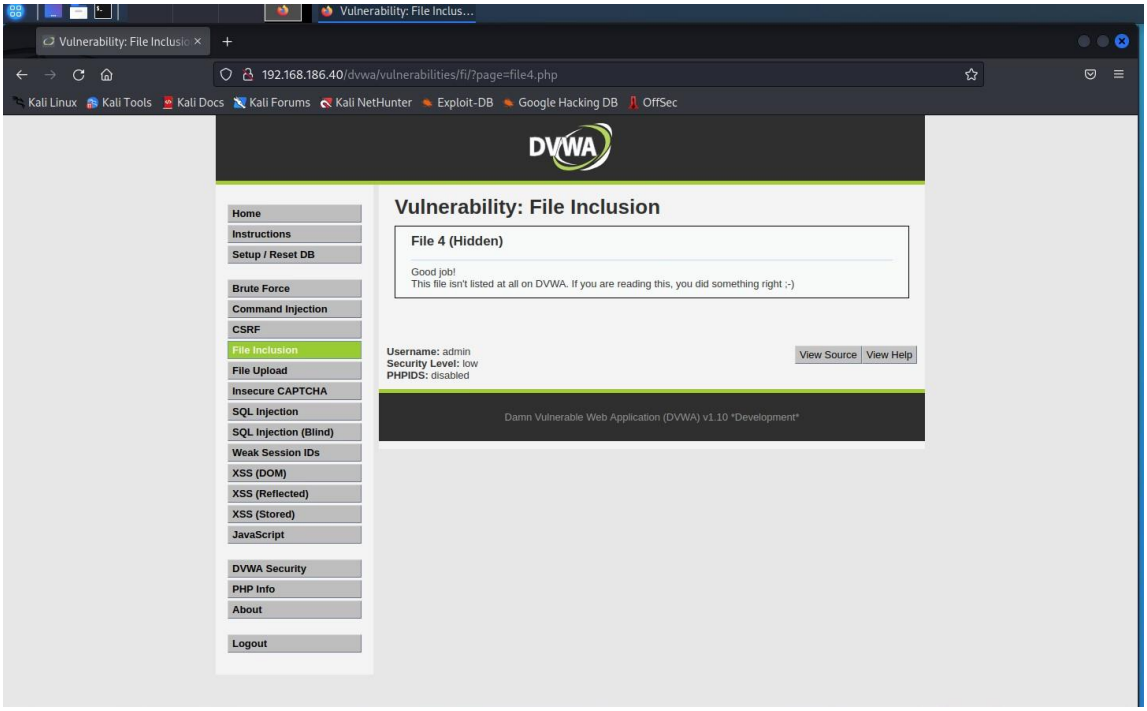
Explain what path traversal is and demonstrate how it works

A path traversal attack aims to access files that are stored outside of the web root folder. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. The attack is known as a dot dot slash attack(../).(*Path Traversal* | *OWASP Foundation*, n.d.)

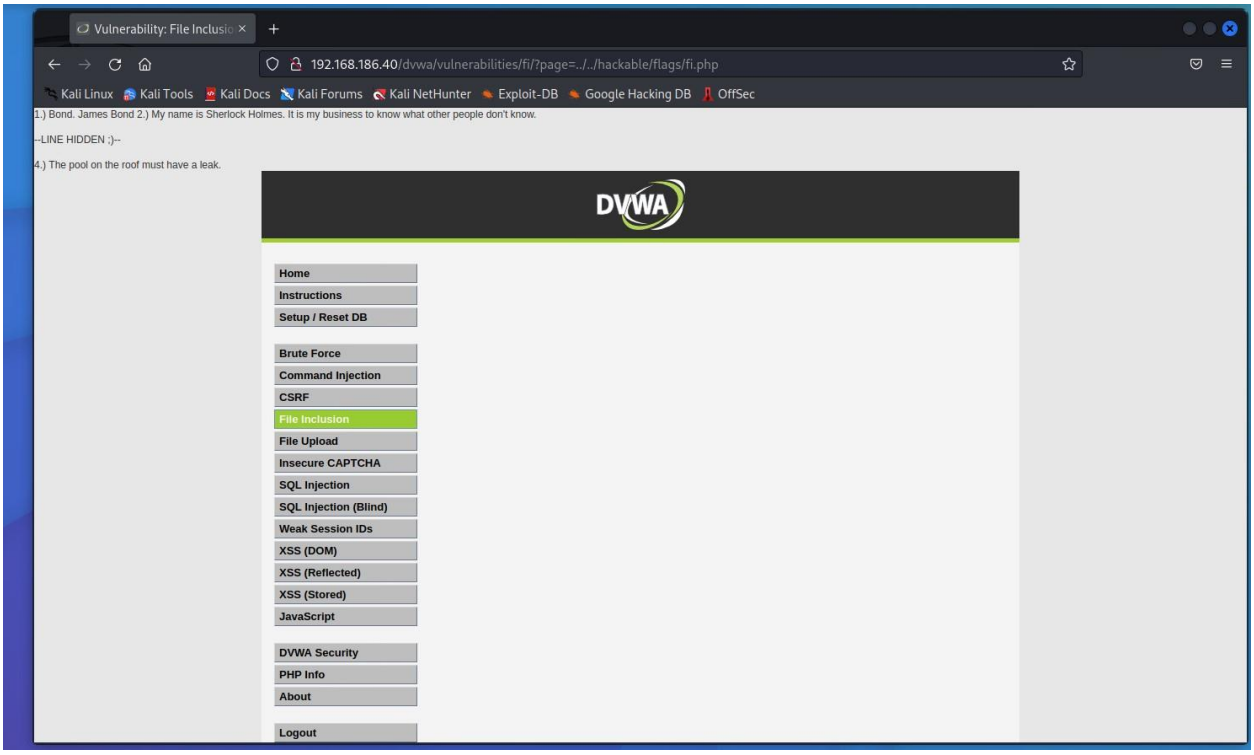
Explain what remote file inclusion is and demonstrate how it works

1. Low level:

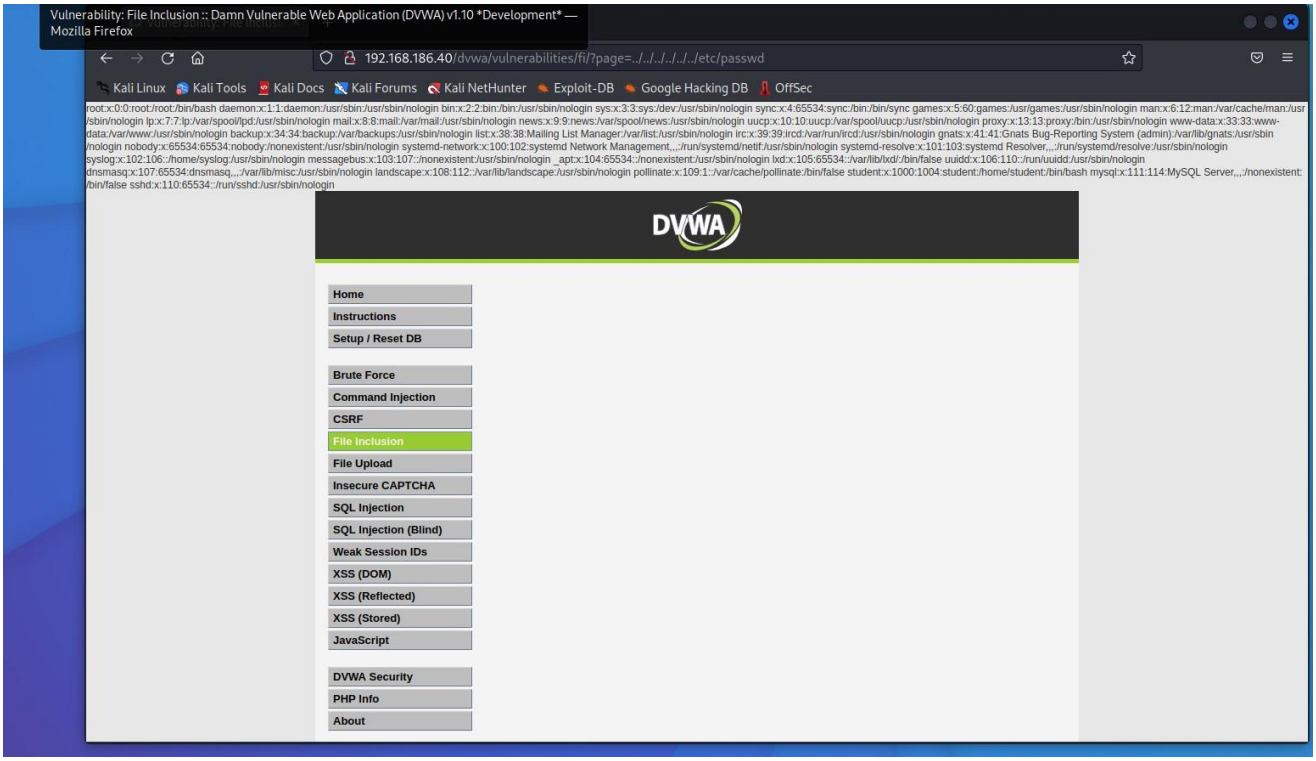
I managed to find the hidden file:



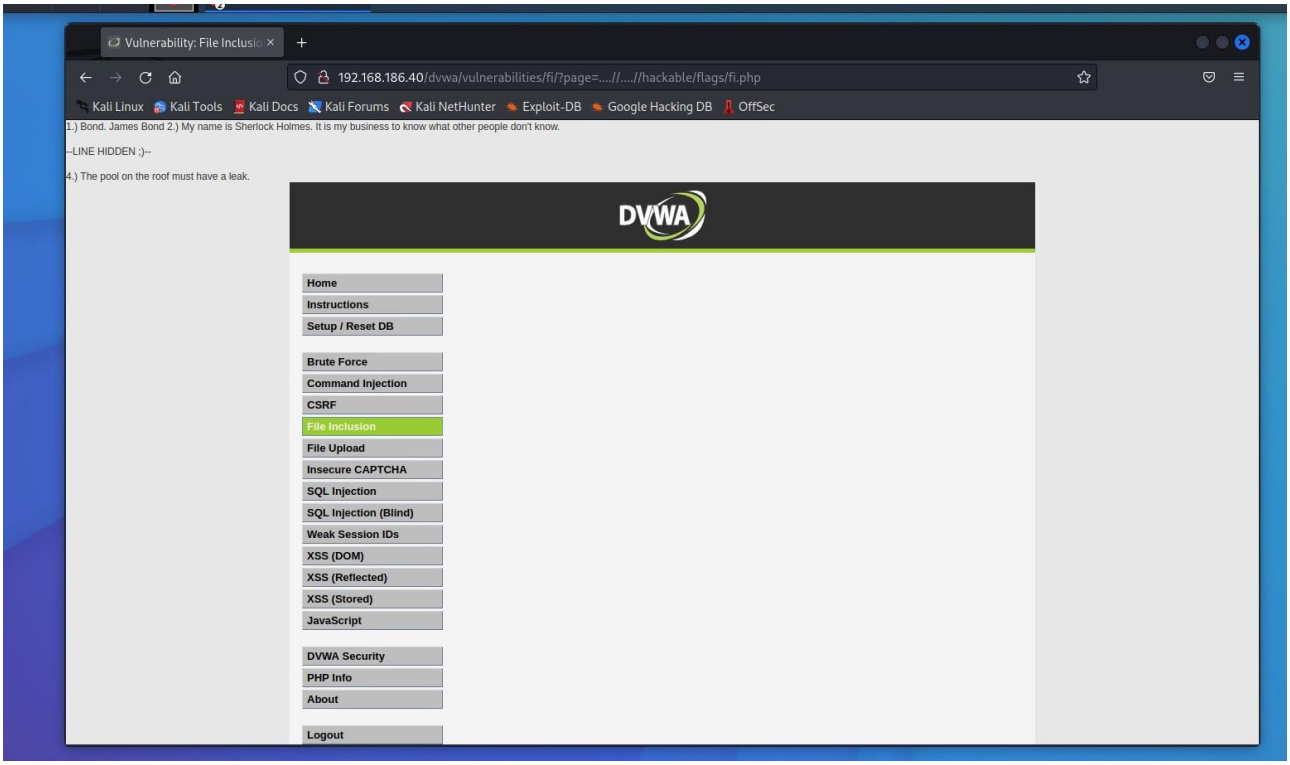
I also managed to find some hidden lines:



I also add several “../” to the URL and got this:



2. Medium level:
   I managed to display the hidden lines. This time instead of "../" I used "….//" and got this:

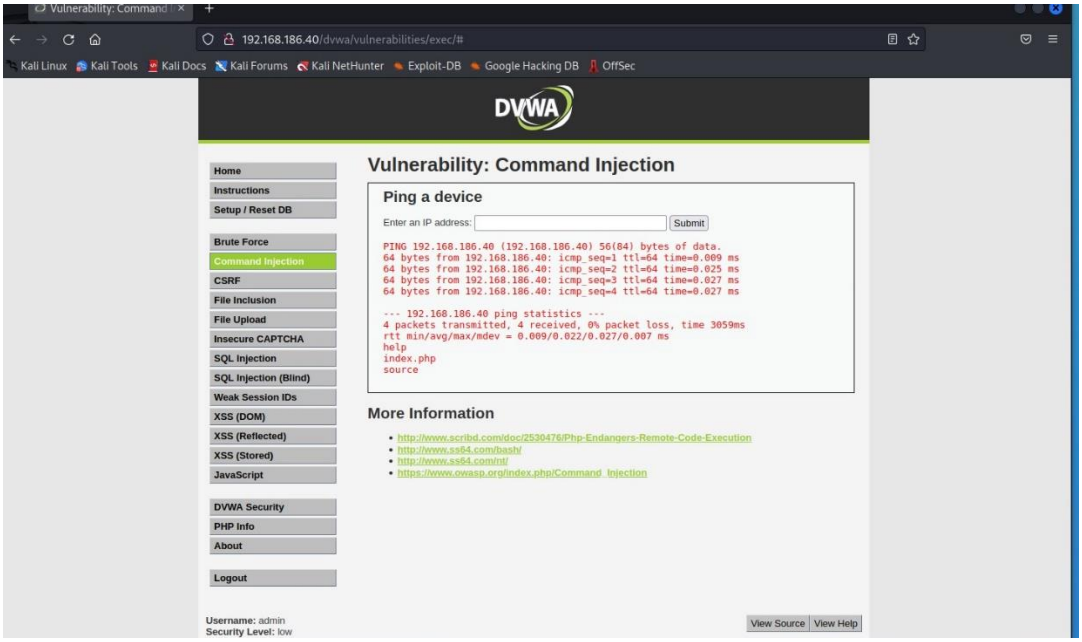


Explain what command injection is and demonstrate how it works

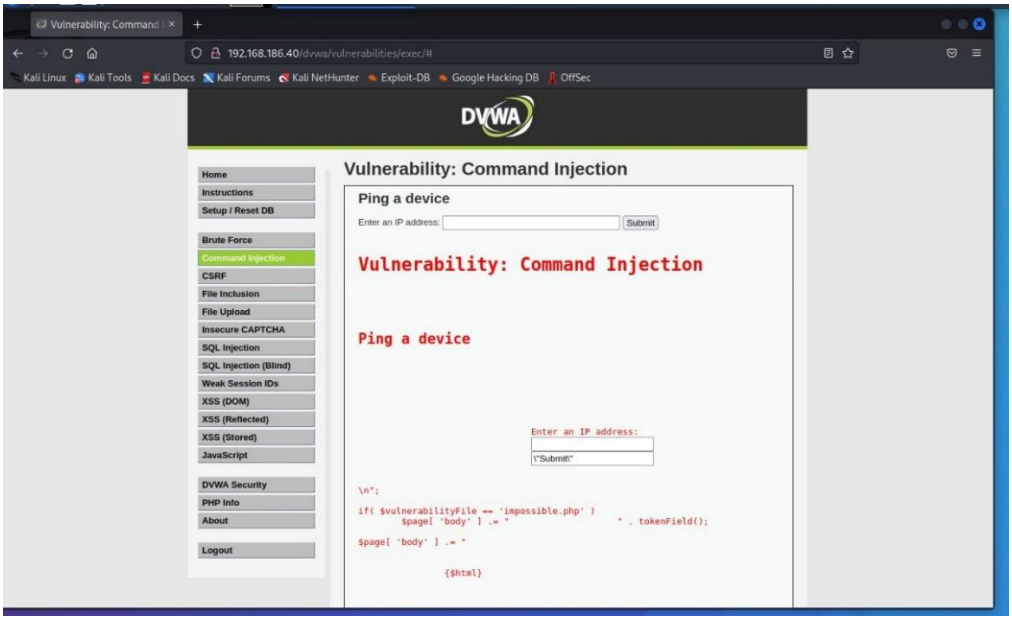
Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible largely due to insufficient input validation.

1. Low level:

I managed to put my Ip address and ‘ls’ command and received the ping and a list with all files in the directory.

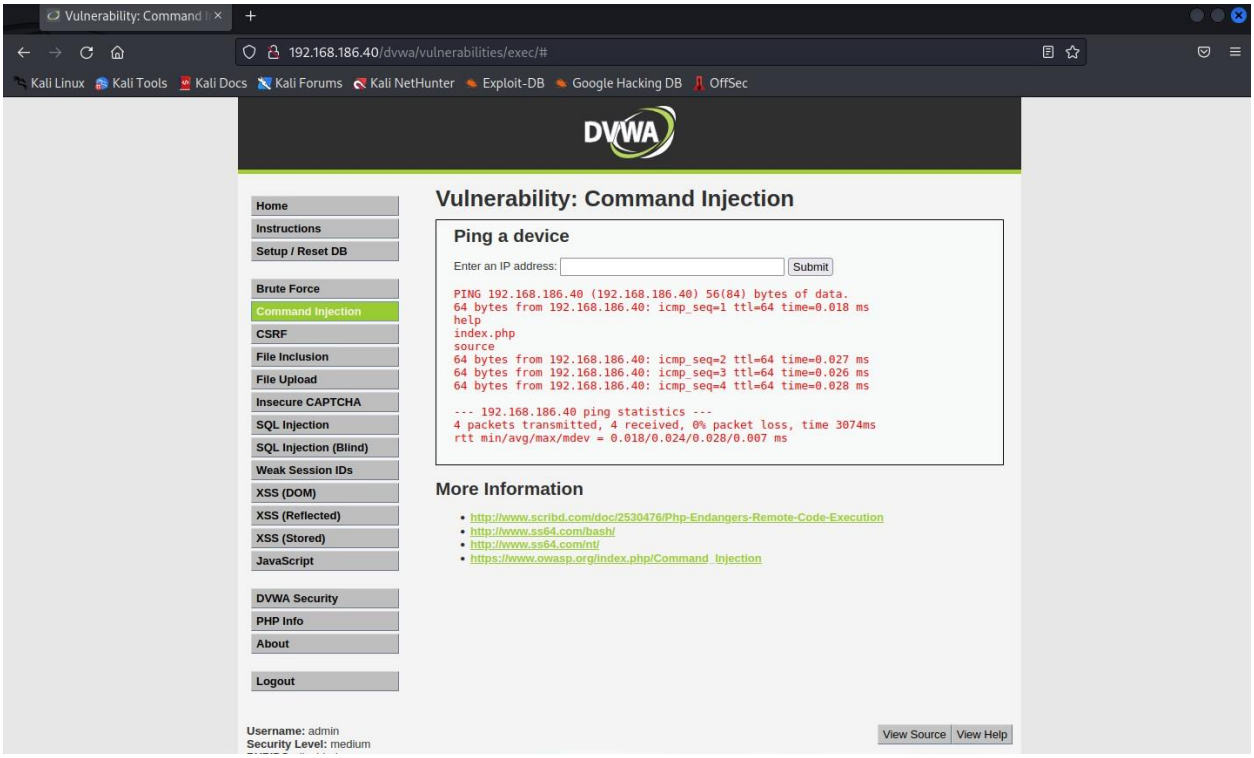


Then I put cat command and index.php and it printed again the same page.

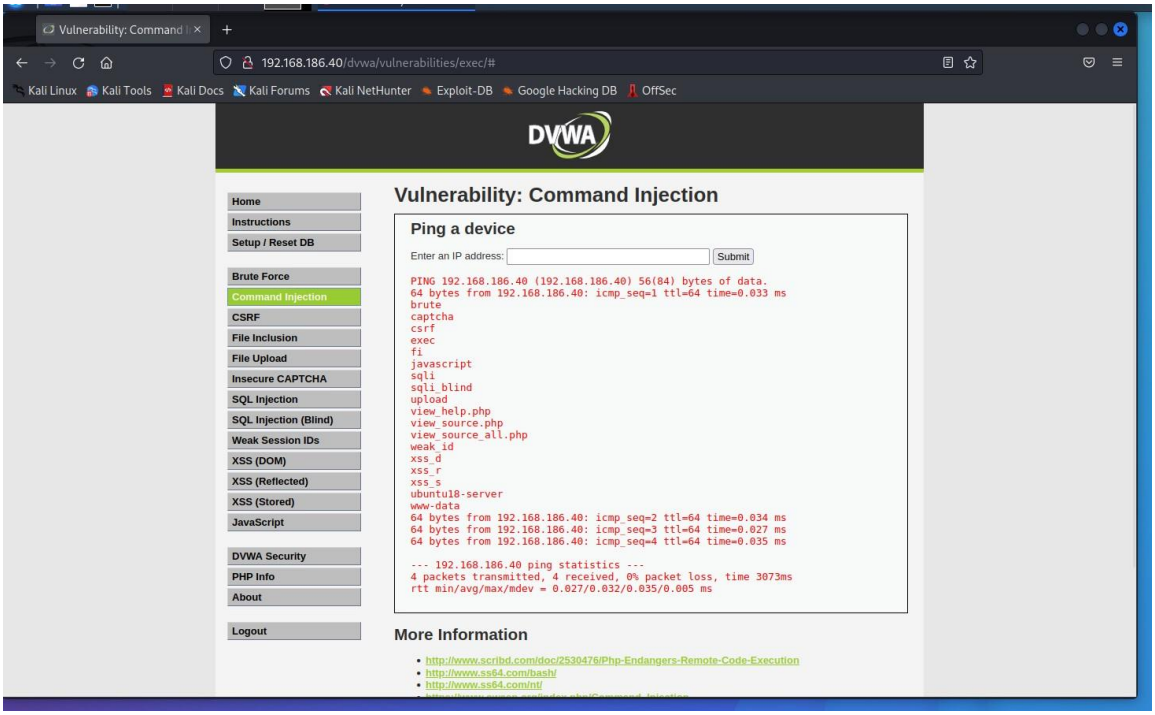


2. Medium level:

I typed my IP address and ‘ls’ command but with the difference that instead of using ‘&&’, I use only one ‘&’. This way it will run both commands simultaneously rather than sequentially.



After that I run the same command but with a few changes. I add ‘hostname’ and ‘whoami’ and change ‘ls’ to go back one directory.



Afterthoughts

Path Traversal is a type of web application vulnerability where an attacker can access files or directories outside the intended scope of the application. To prevent Path Traversal attacks, it is important to validate and sanitize all user input and implement proper access controls and permissions on the web server. Command Injection is a type of web application vulnerability where an attacker can execute commands on a server by injecting malicious code. To prevent Command Injection attacks, use parameterized queries or prepared statements to securely pass user input to commands and validate all user input to ensure it does not include any malicious code.

Both Path Reversal and Command Injection techniques can be used by attackers to gain unauthorized access to a system, execute arbitrary code, or escalate privileges. Regular security audits, code reviews, and penetration testing can also help identify and fix potential vulnerabilities in the early stages of a project to minimize the risk of these attacks.

Reference:

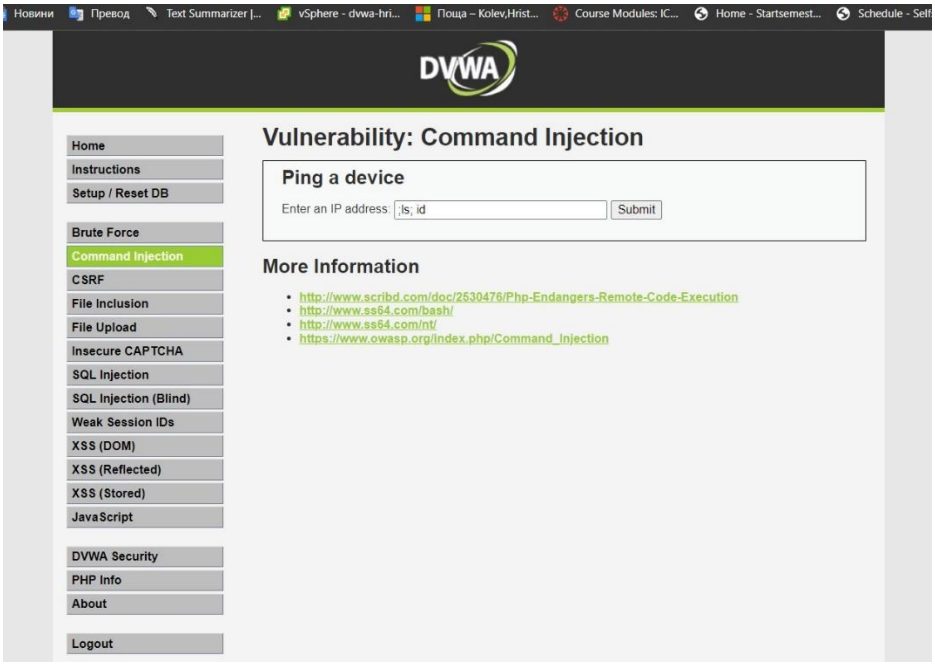
Path Traversal | OWASP Foundation. (n.d.). https://owasp.org/www-community/attacks/Path_Traversal

WAF (Web Application Firewall)

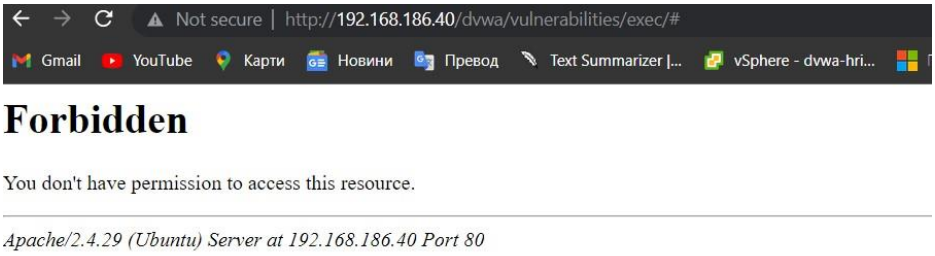
Perform one or more web application attacks. Deploy a web application firewall and repeat the attacks.

I managed to build a web application firewall using the instructions given in the files after the presentation. This is a system that detect and block the attacks on web applications such as SQL injection, Command injection, Cross-Site forgery, Cross-Site-Scripting, File Inclusion and many more.

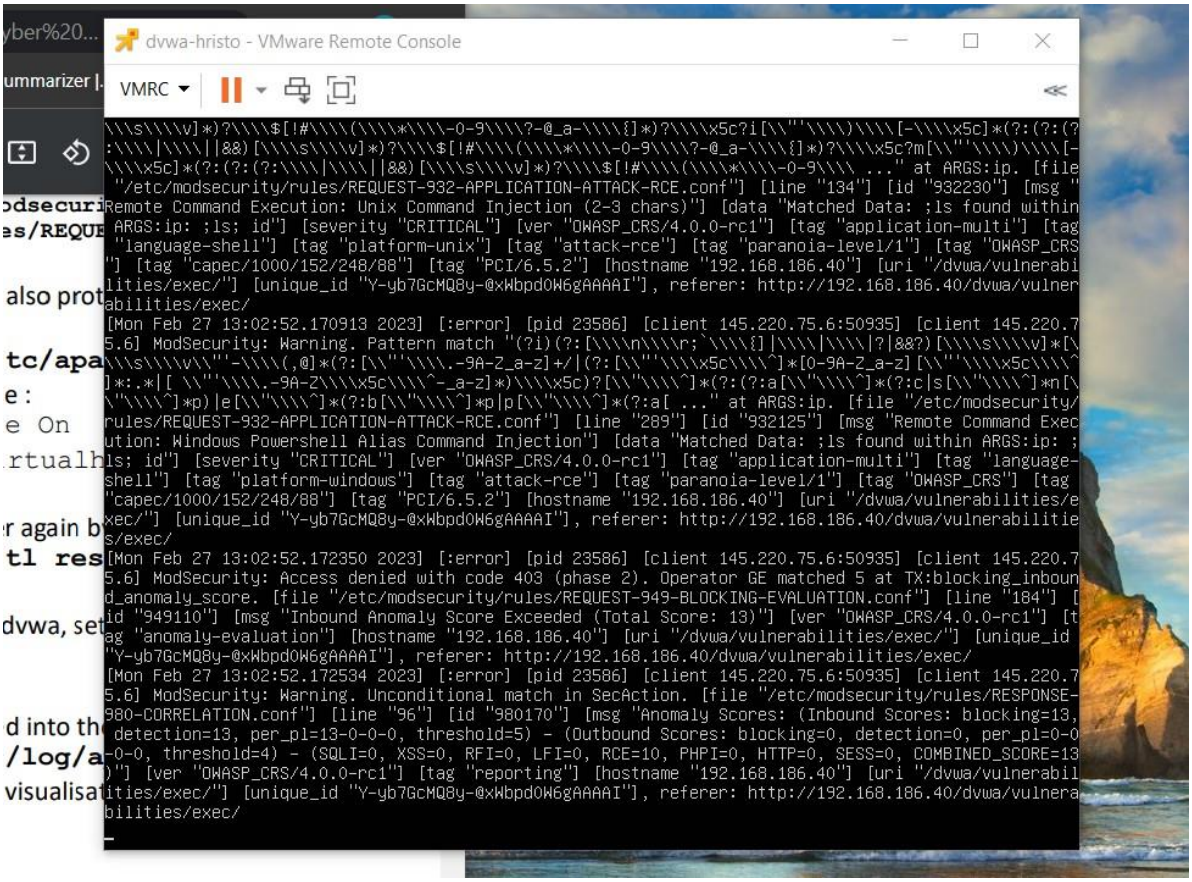
After I built the WAF, I tried to test it in Command Injection page on the lowest level of security.



After the execution of the command, I get a message that says that I don’t have permission.



On the server side the message that was displayed was this:



Afterthoughts

A Web Application Firewall (WAF) is a security solution that monitors incoming and outgoing traffic to detect and block malicious activities. It uses signature-based detection, behavior-based detection, and rule-based detection to prevent attacks. Signature-based detection involves matching incoming requests against known attack patterns, behavior-based detection looks for suspicious behavior, and rule-based detection blocks requests that match certain patterns.

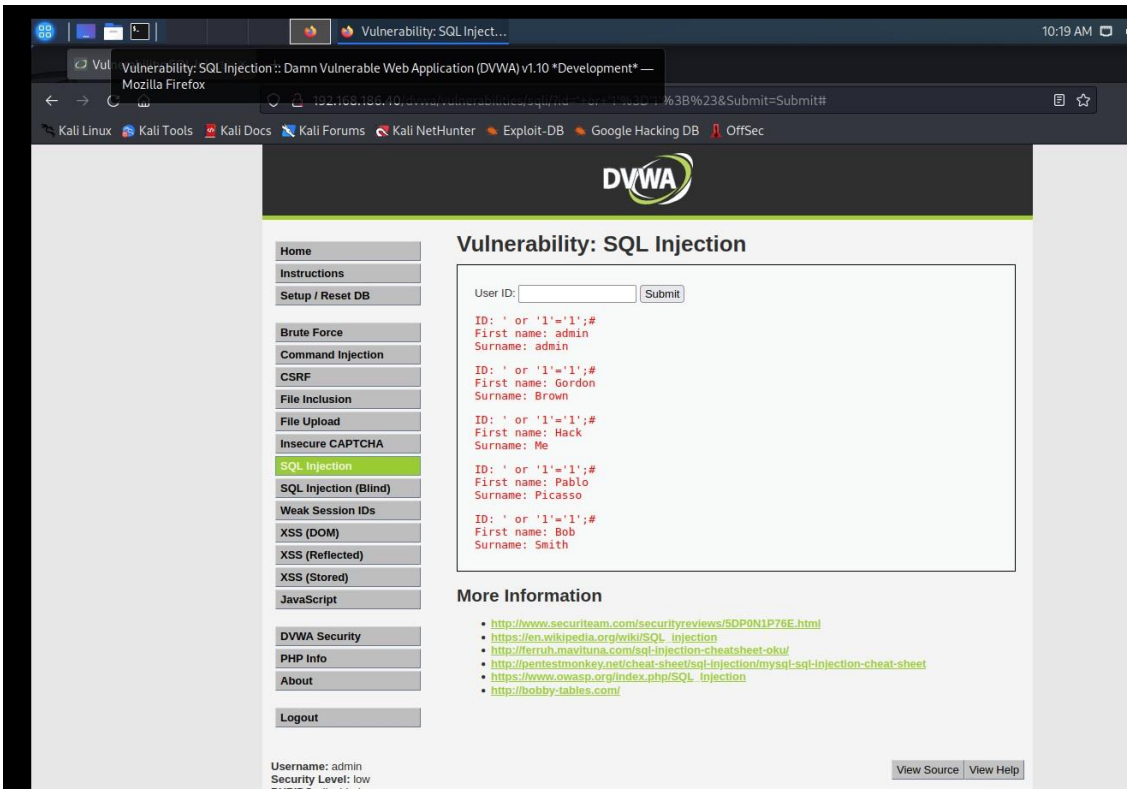
SQL Injection

Objective: There are 5 users in the database, with id's from 1 to 5. Your mission... to steal their passwords (hashes) via SQLi

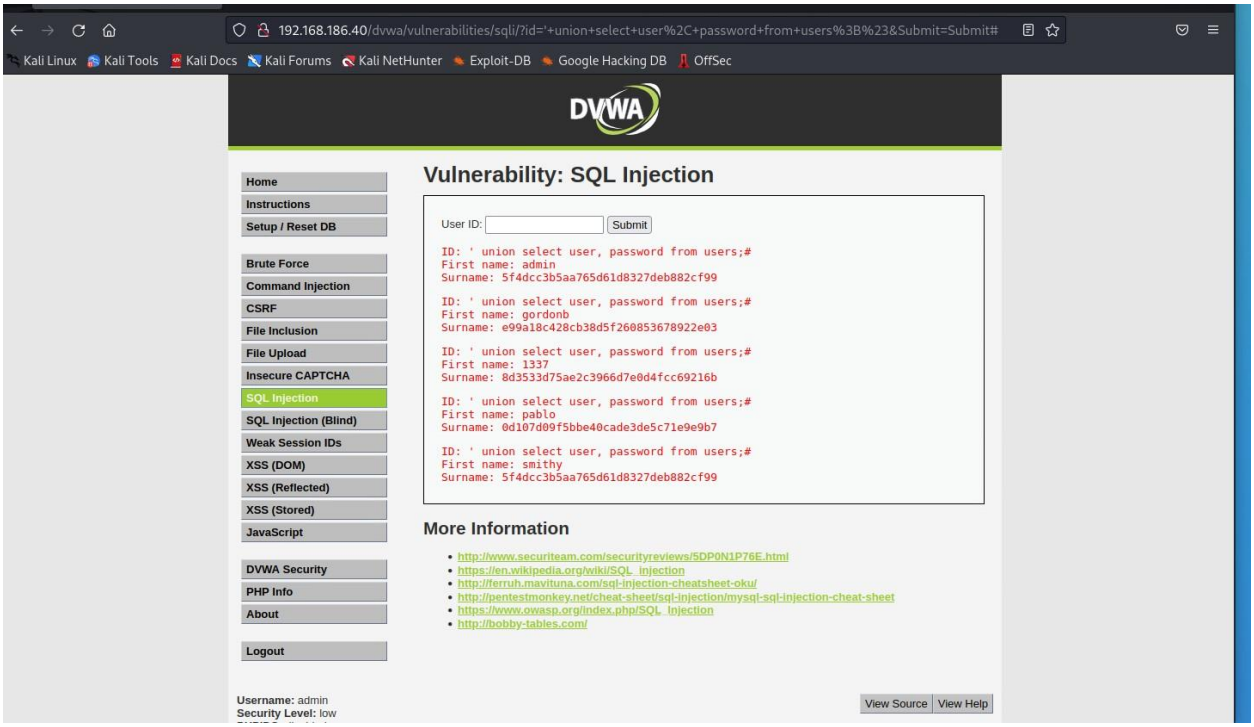
The operators “OR” and “==” are very handy in the SQL injection. It is a common way a hacker to receive information from the database because the statement will be always true.

1. Low level

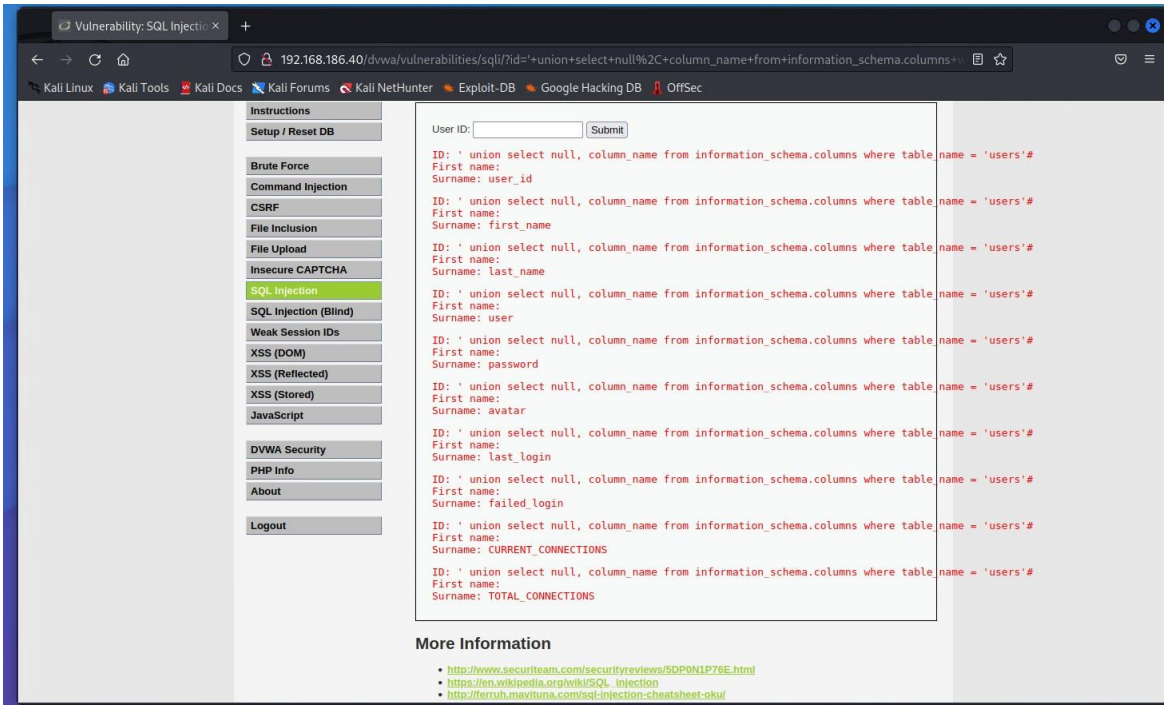
First, I user the statement: ‘or ‘1’==’1’; #. The first quote is to close the previous statement, the I am checking if 1 is equal to 1 and because it is true I will receive user’s information.



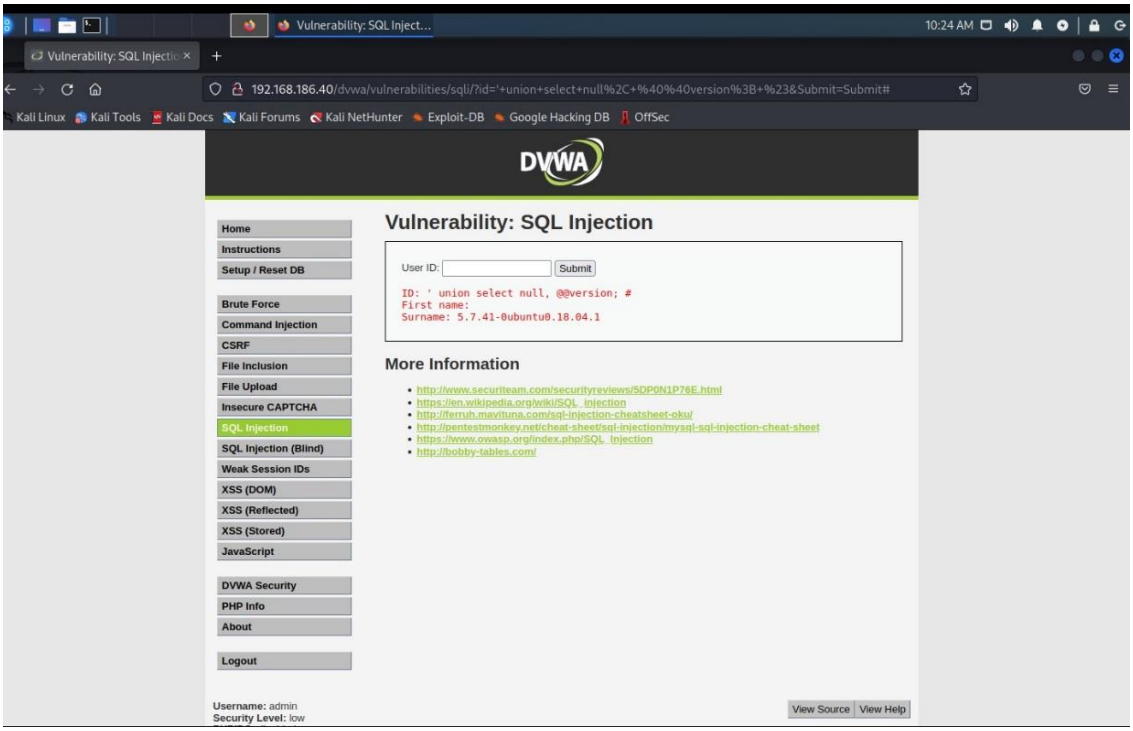
I used also the operator UNION, which is operator used to combine the result from 2 or more SELECT statements. Instead of using the operator OR like the previous example, this time I create a little query to display the user and the password from table ‘users’.



Then I decide to play a little bit with the SQL injection and manage to display all columns that exists in the table ‘users’ .

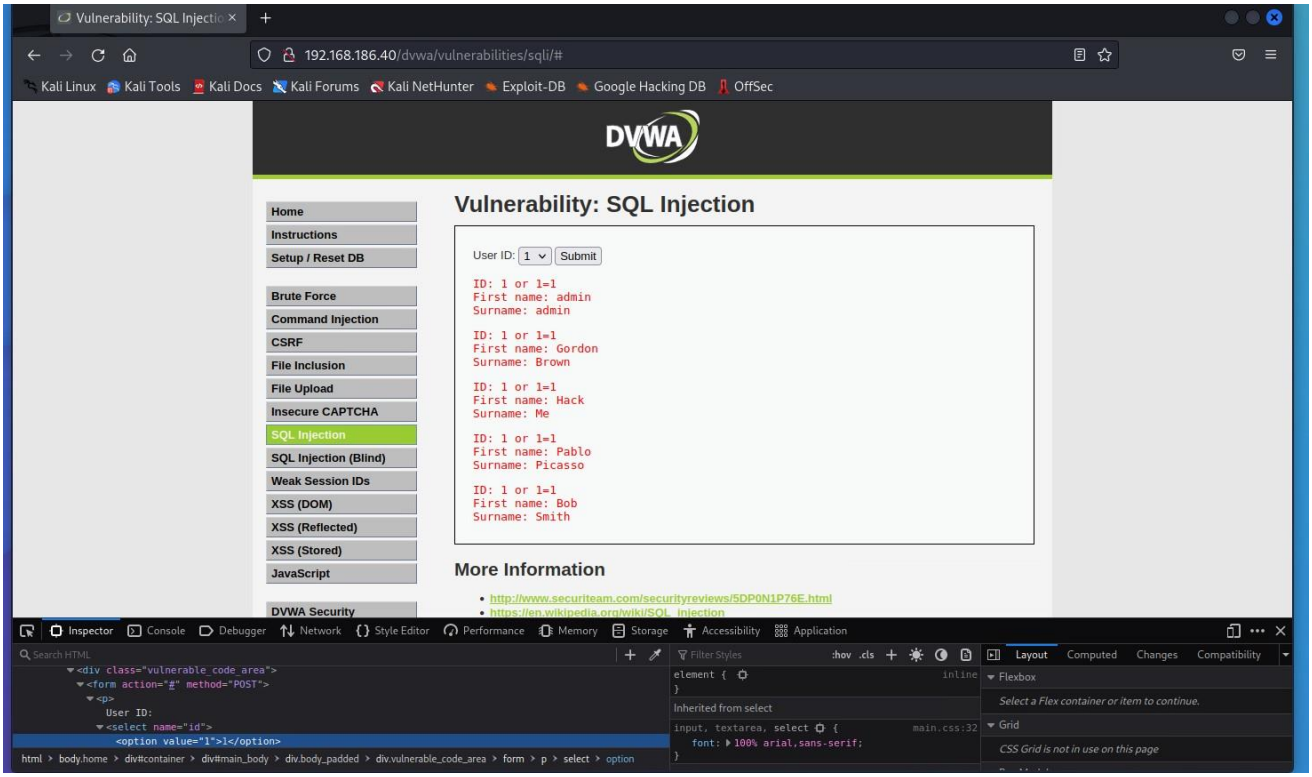


I also managed to display the version of the database.

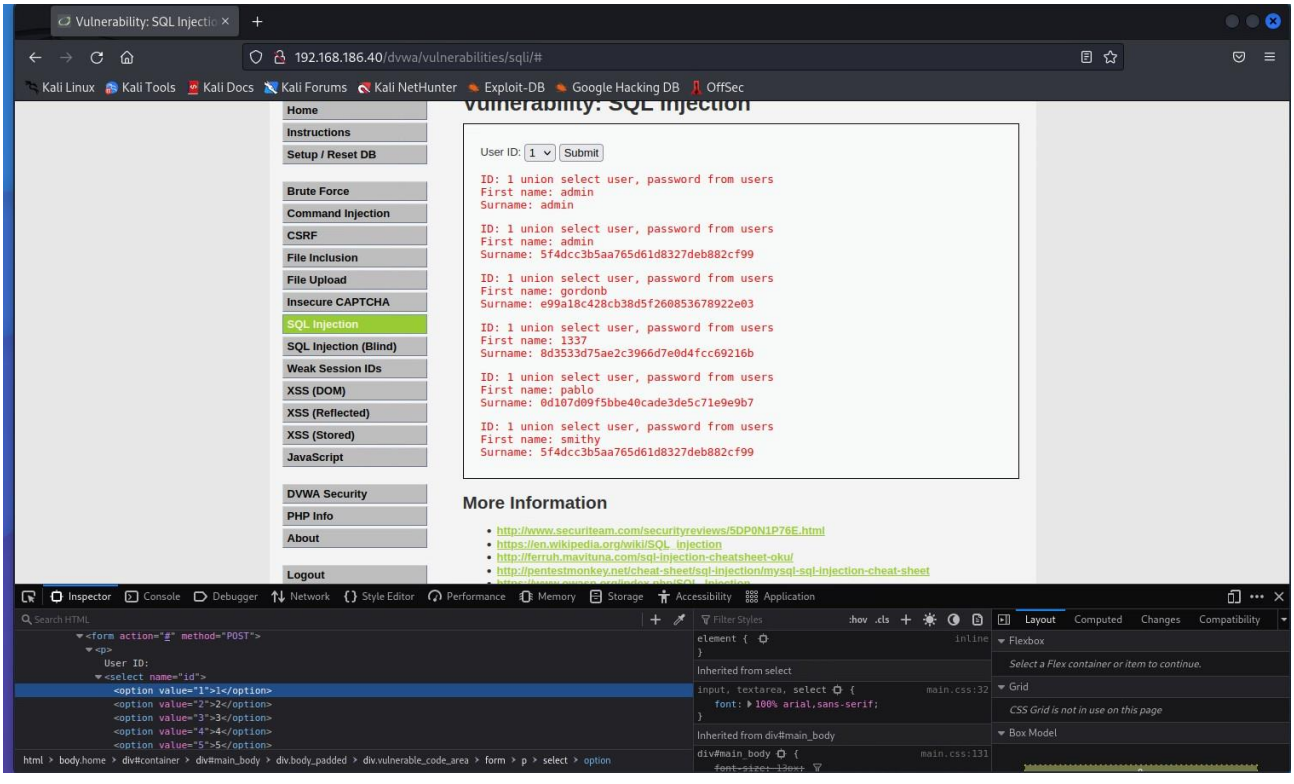


2. Medium level

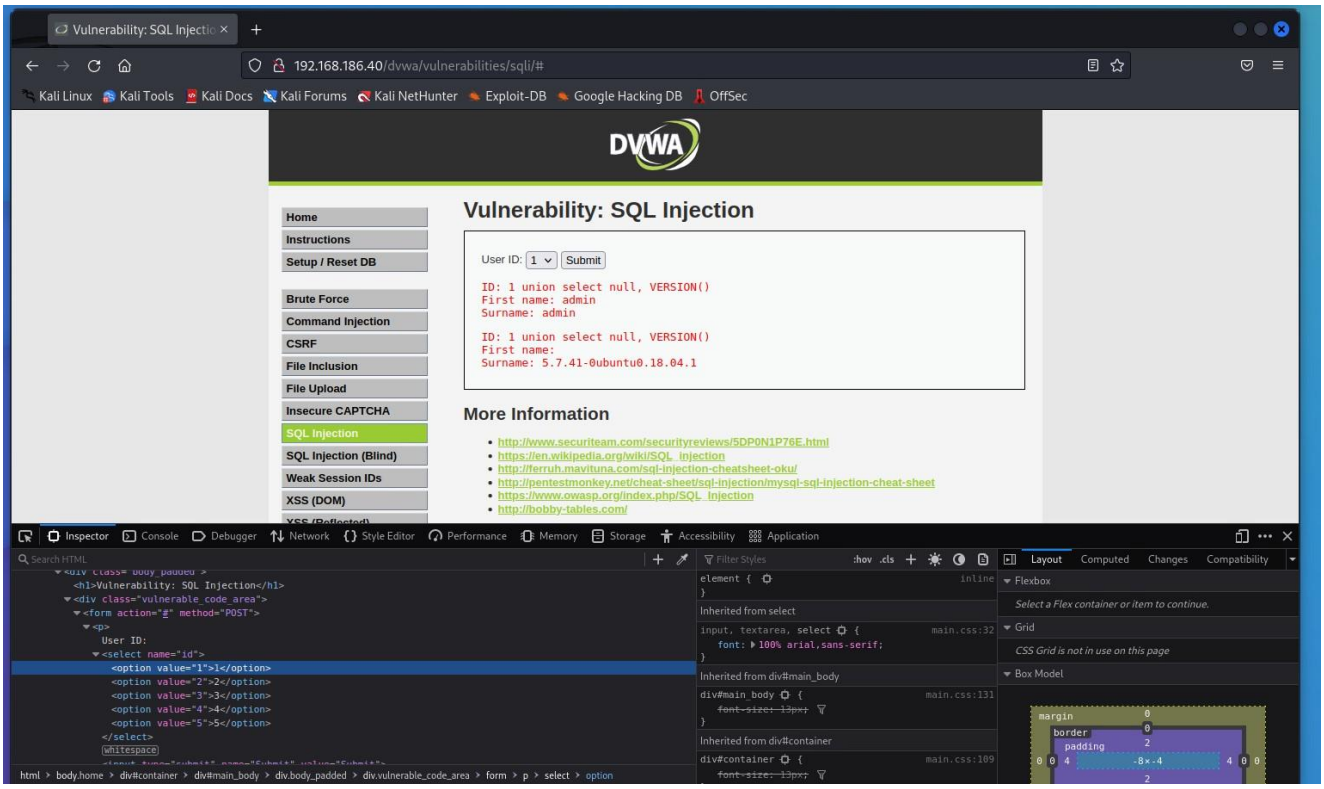
Here instead of using textboxes, I used the Inspector. From there I have to rewrite combobox to receive some information. To be successful the attack both values should be rewrite.



Then I managed to display the users and the password from the table ‘users’.

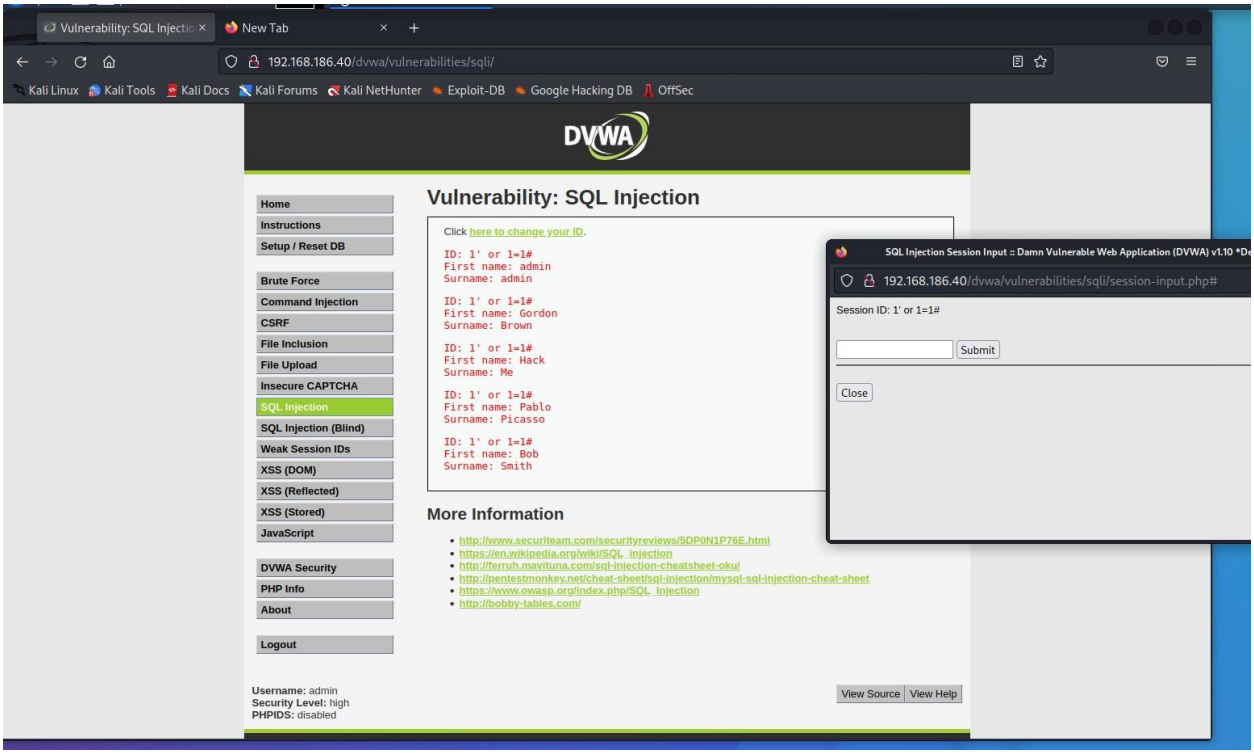


I also managed to display the version of the database.

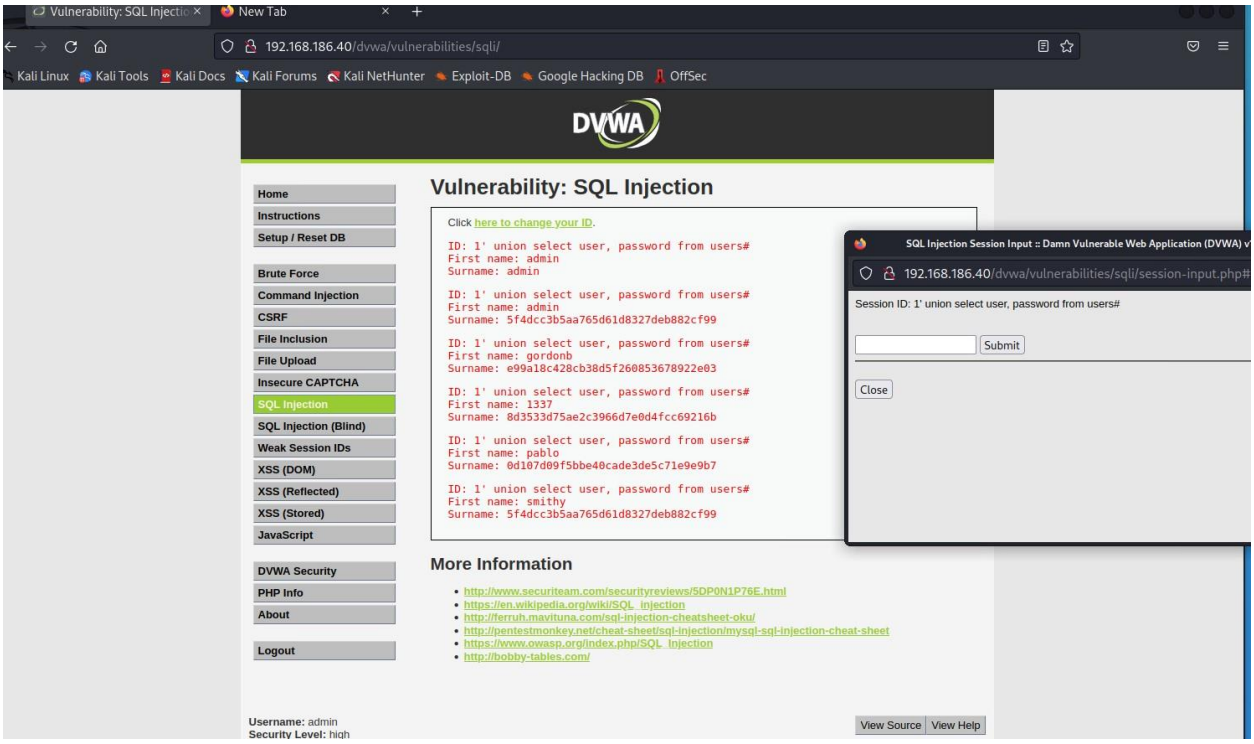


3. High level

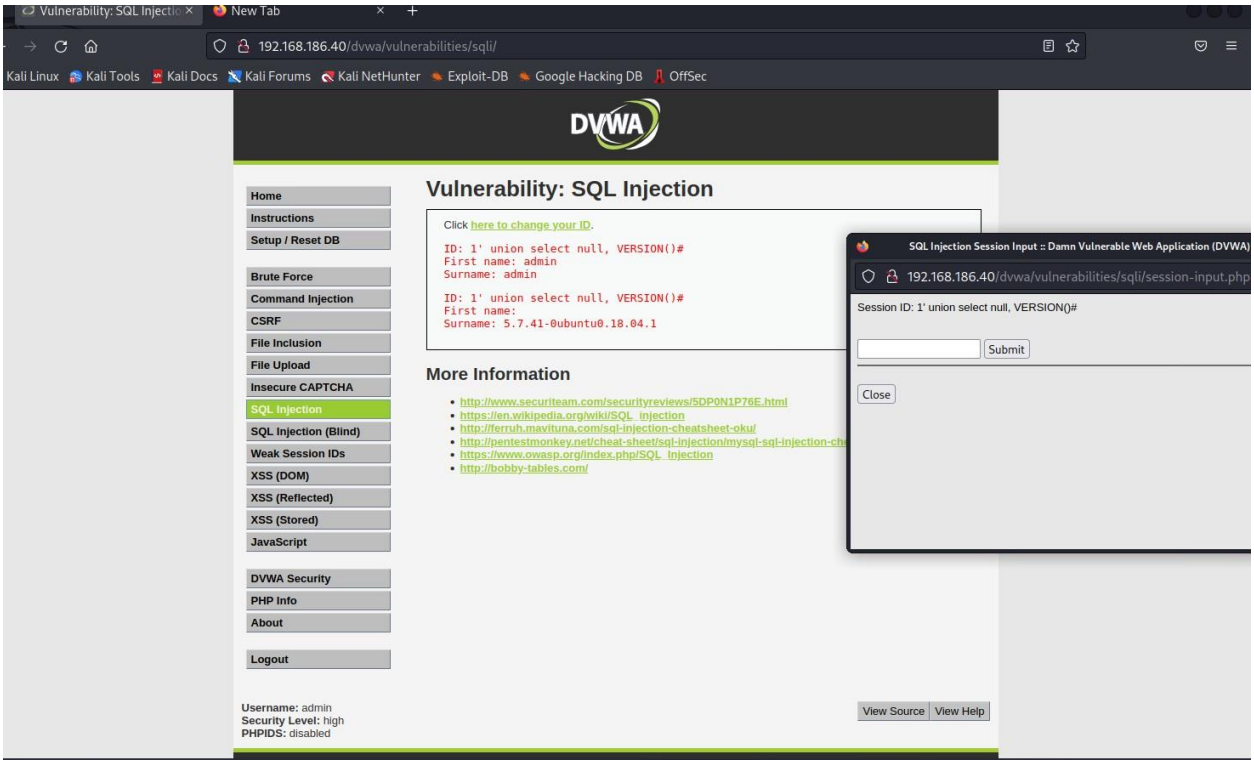
Here the application starts to use SESSION and another page for typing the user id. The trick here is to use number for the session and then to add another query.



I display the users again but with their passwords.



And again, I display the version of the database.



Afterthoughts

SQL Injection is a web application vulnerability where an attacker can manipulate SQL queries to execute arbitrary SQL commands. To prevent this, it is important to use parameterized queries or prepared statements instead of directly concatenating user input into SQL queries. Input validation and sanitization should also be applied to all user-supplied data that is used in SQL queries. SQL Injection can be used in a project by exploiting vulnerabilities in a web application's code that allow unsensitized user input to be directly concatenated into SQL queries, allowing for the execution of arbitrary SQL commands.

Host Intrusion Detection and Prevention (HIDS)

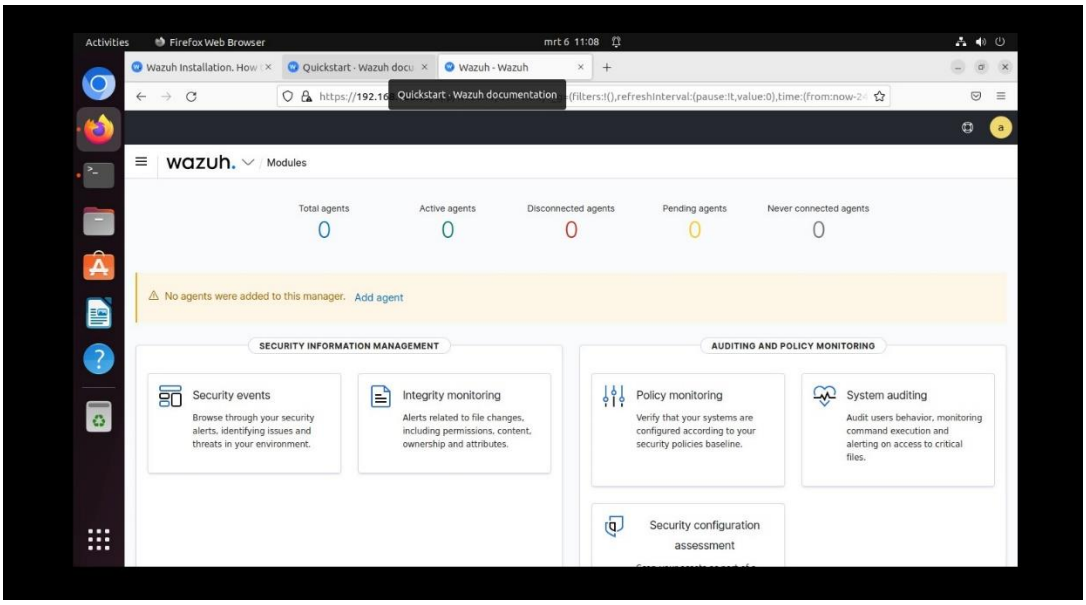
> Explain the difference between NIDS and HIDS and IDS and IPS, and the meaning and relevance for your company.

Intrusion detection system (**IDS**) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported to an administrator. The most common classifications are **Network intrusion detection systems** (**NIDS**) and **Host-based intrusion detection systems** (**HIDS**).

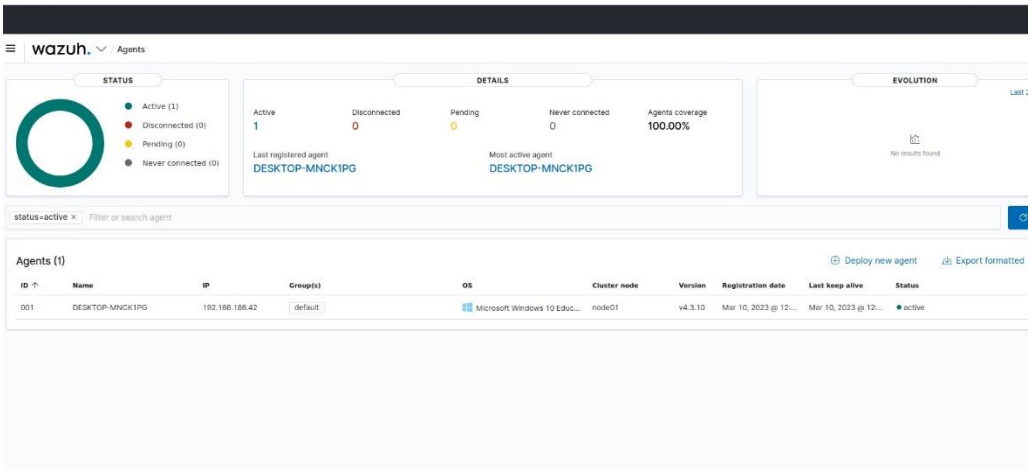
Network intrusion detection system (NIDS) is a security tool designed to monitor and detect suspicious activity on a network. NIDS works by analyzing network traffic and looking for patterns or behaviors that indicate an intrusion attempt, such as unusual network connections, traffic spikes, or patterns that match known attack signatures. It can detect a wide range of attacks including port scans, network probes, denial of service attacks, and malware infections.

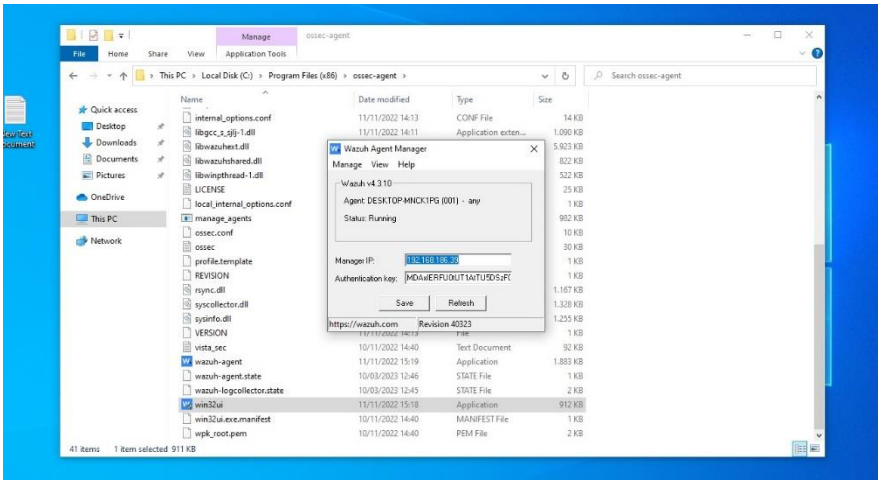
Host-based intrusion detection system (HIDS) is a security tool made to monitor over and detect inappropriate activity on a single host or computer system, like a server or endpoint. HIDS concentrates on the actions and conduct of the host on which it is installed. To identify signals of intrusion, it keeps an eye on the host's system logs, file integrity, and other forms of activity.

I install Wazuh integrated solution on the Ubuntu machine following the instructions after the presentation.

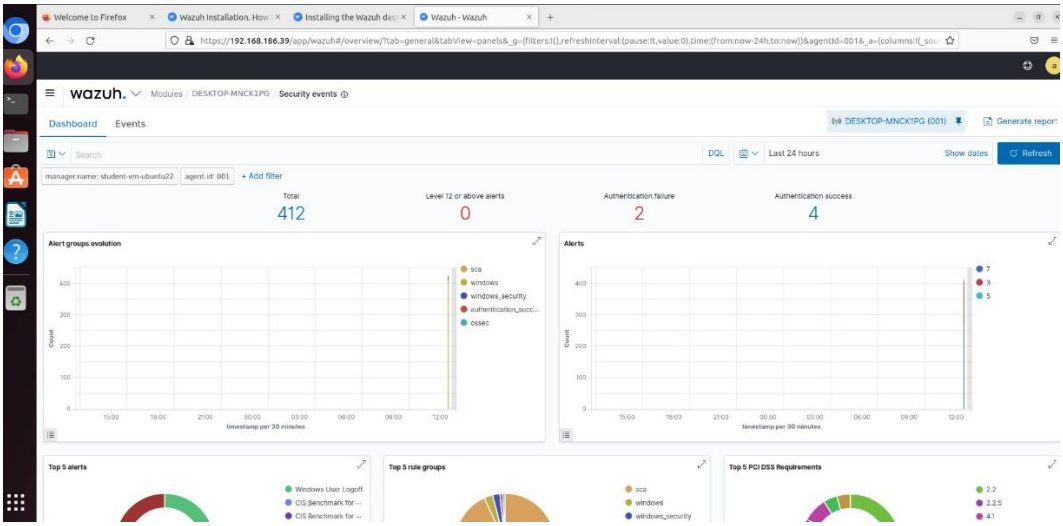


Then I connect it with my Windows 10 machine and configure it:





After everything I tried it if it is working correctly. I logged out and tried to log in with several wrong passwords. When I check the Ubuntu machine the result was this:



Afterthoughts

Host Intrusion Detection and Prevention (HIDP) is a security mechanism that focuses on detecting and preventing unauthorized activities and malicious behavior on individual host systems. Wazuh is an open-source security solution that provides HIDP capabilities for monitoring and protecting hosts against various types of attacks. It uses log analysis, anomaly detection, and rule-based detection to identify potential security breaches on hosts. Detected events can trigger alerts, notifications, or automated responses, such as blocking or quarantining the suspicious activity.

Reference

Wikipedia contributors. (2023a, February 7). *Intrusion detection system*. Wikipedia. https://en.wikipedia.org/wiki/Intrusion_detection_system

Wikipedia contributors. (2023a, February 7). *Host-based intrusion detection system*. Wikipedia. https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

XSS (Cross-Site Scripting)

Cross-Site Scripting (XSS) is a computer security vulnerability typically found in web applications. It enables the hackers to inject scripts into web pages viewed by the other user.

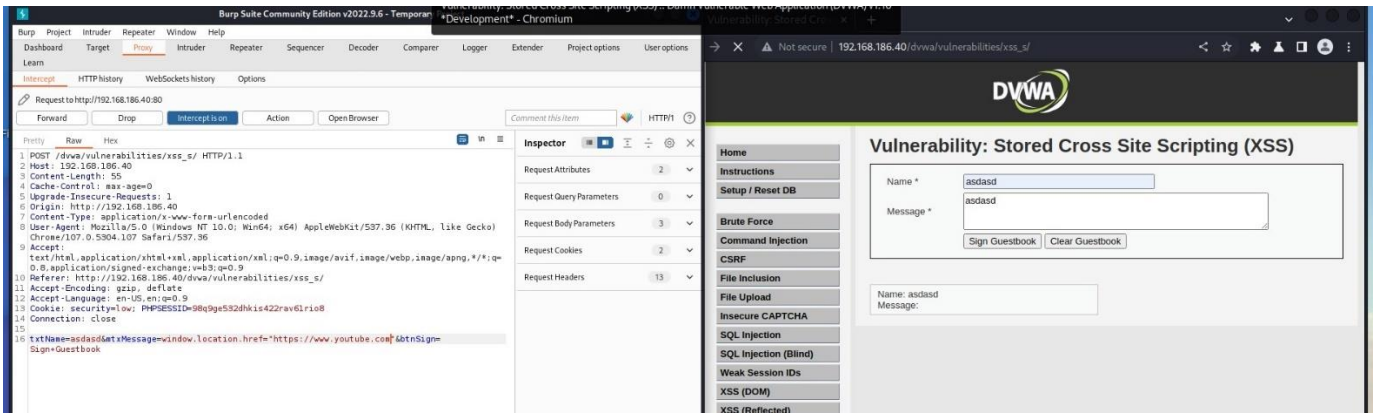
Use DVWA XSS reflected (low/medium for style 1) and DVWA XSS stored (low/medium for style 1) and explain

1. XSS stored

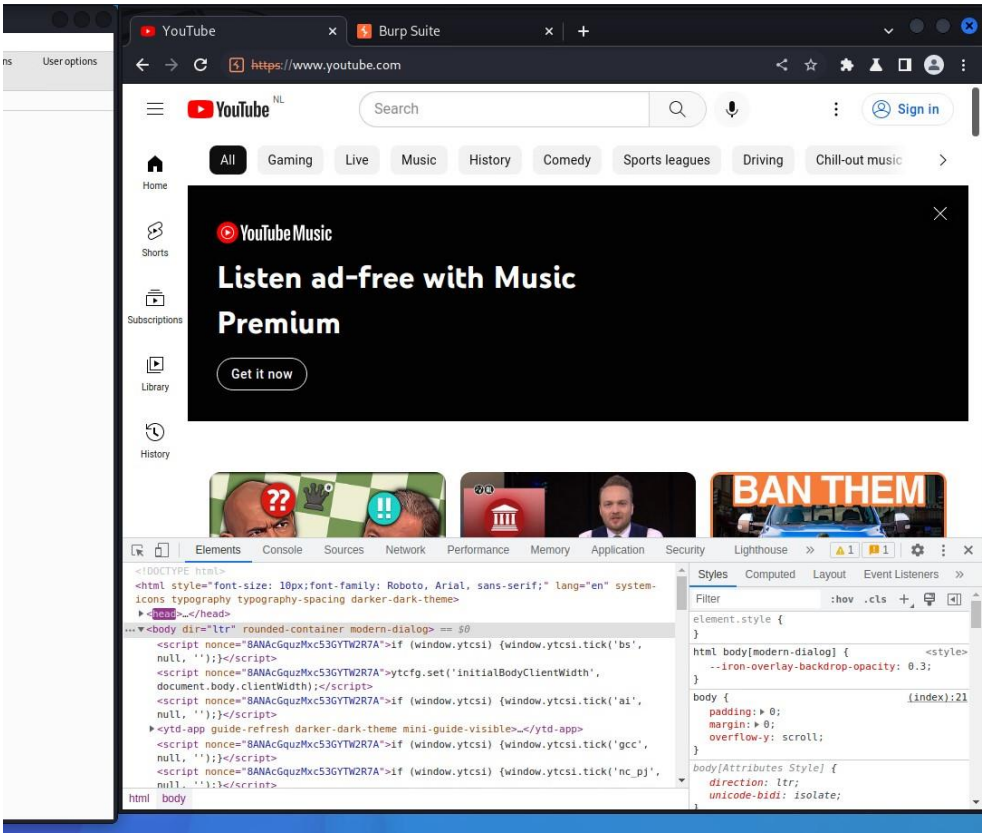
The persistent XSS vulnerability is a more devastating variant of a cross-site scripting flaw, where data provided by the attacker is saved by the server and displayed on "normal" pages returned to other users without proper HTML escaping.

1. Low

On this level the textboxes are not secured at all. I decided to type a script to redirect the user to the main page in YouTube. For this task I used Burp Suite. Burp Suite is popular web application security testing tool, used for testing the security of web application. Some of the key features of Burp Suite include its proxy server, which allows you to intercept and modify HTTP/S traffic; its web vulnerability scanner, which can automatically identify common vulnerabilities in web applications; and its repeater, which allows you to repeat requests to a web application and modify them in real-time.

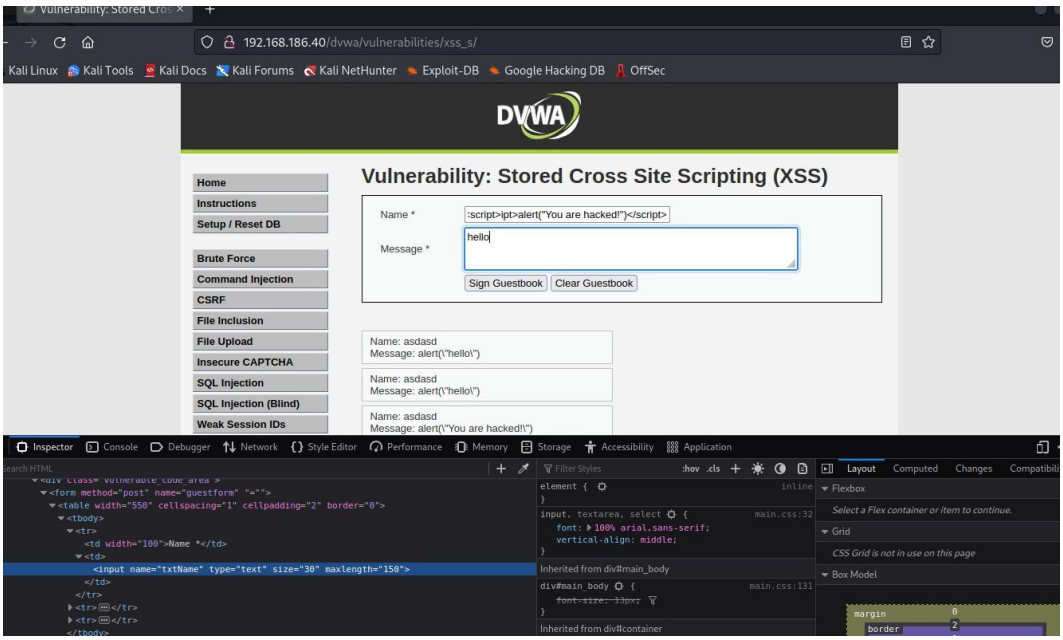


And the result was this:

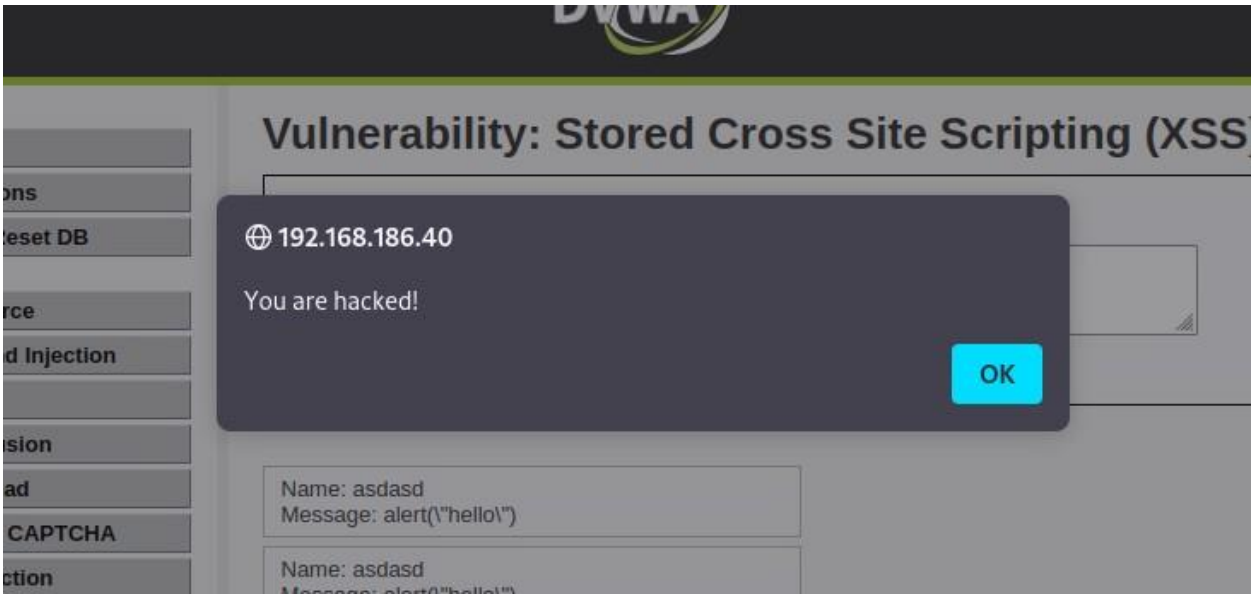


2. Medium

On this level the security of the message box is very good. I tried that commands: “<scr<script>ipt>alert(“You are hacked”)</script>” and it’s variation but nothing. Then I tried it on the first textbox.

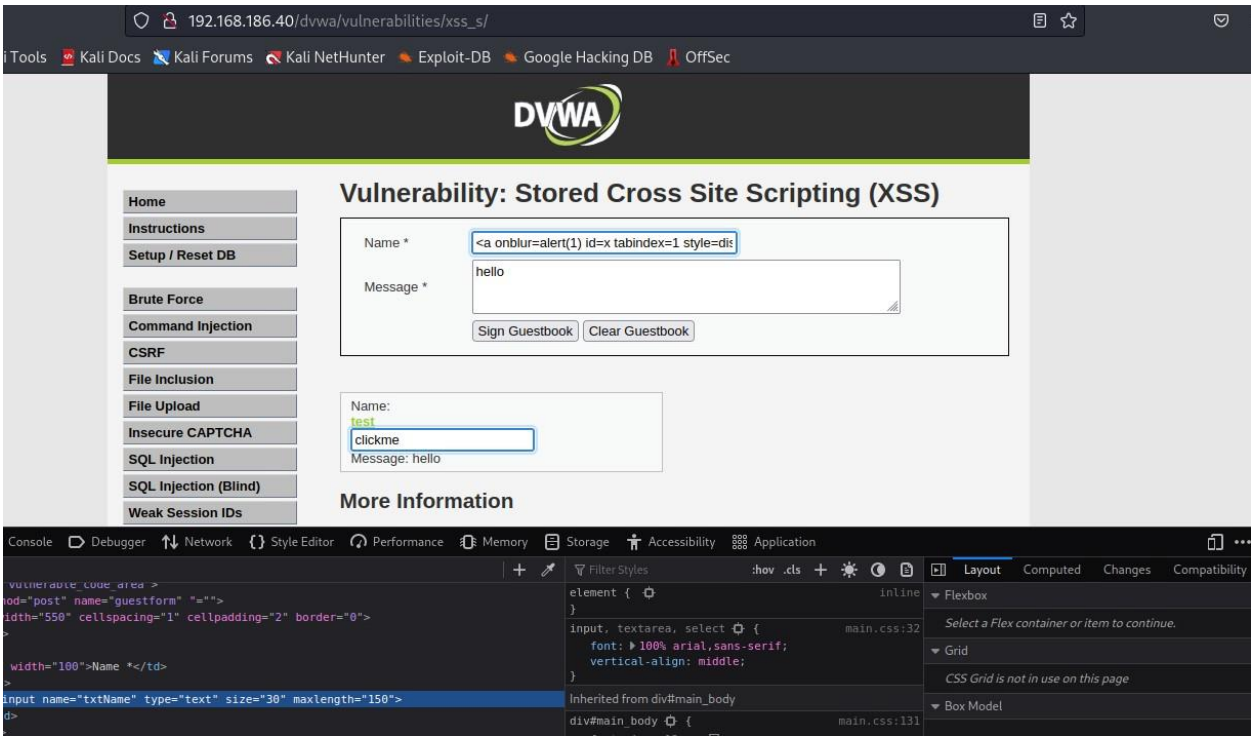


The result was this:



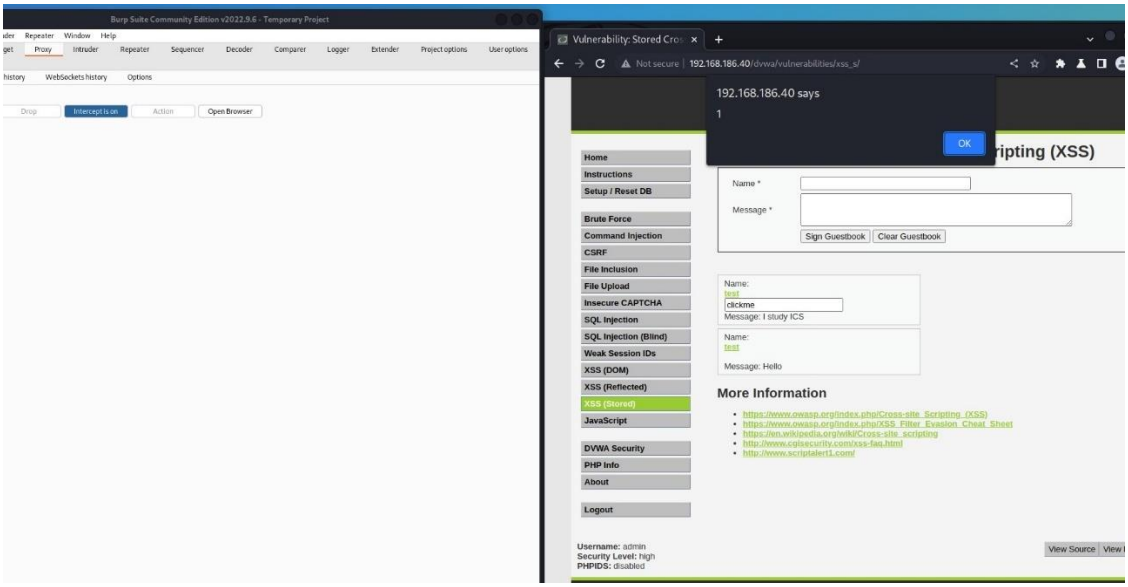
3.High

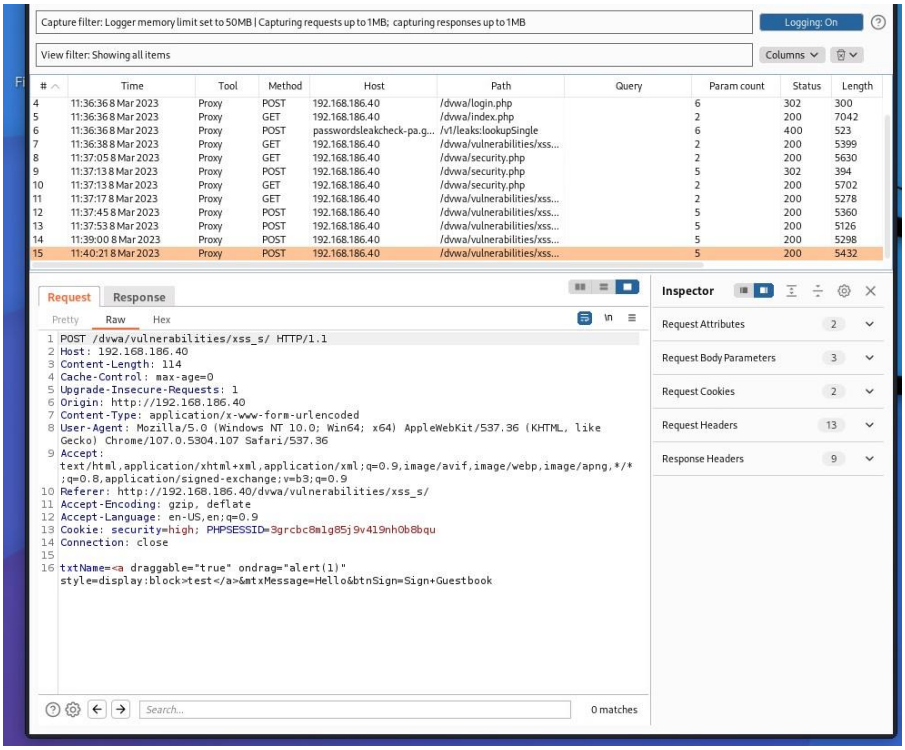
Here the “Message” and “Name” textboxes were also pretty good secured, but on the “Name” textbox there was no html limitation. With the help of a cheat sheet, I manage to write this:



The message will appear if you drag the word ‘test’:

I also tried that level in Burp Suite.



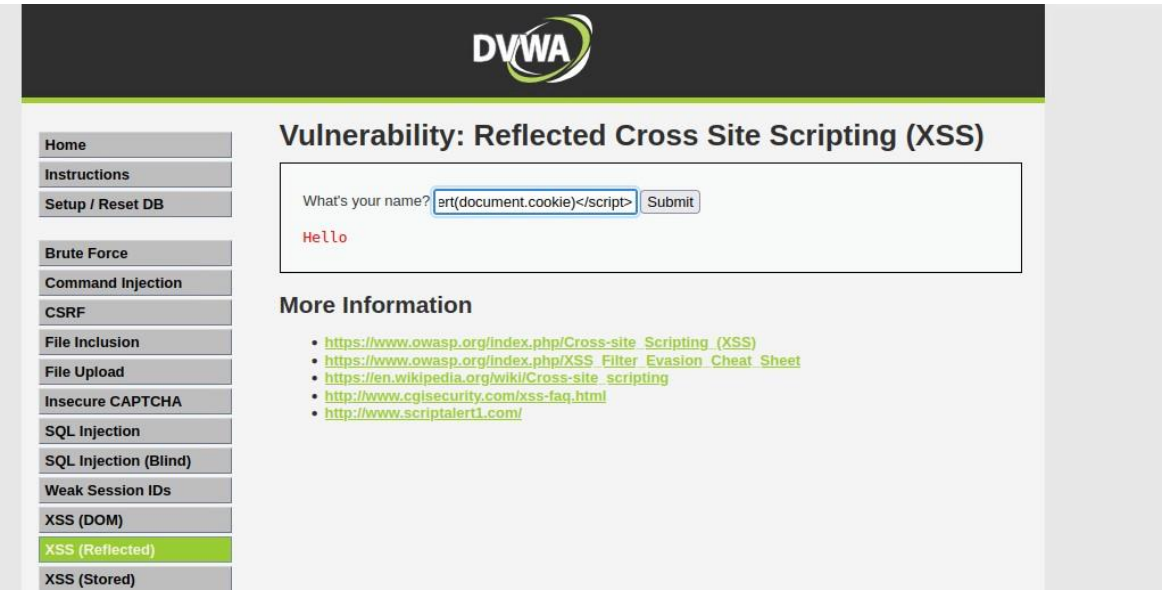


2. XSS reflected

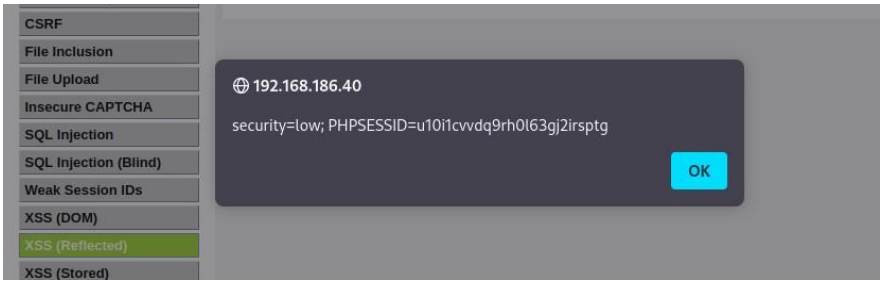
The non-persistent (or reflected) cross-site scripting vulnerability is by far the most basic type of web vulnerability. These holes show up when the data provided by a web client, most commonly in HTTP query parameters (e.g. HTML form submission), is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the content

1. Low

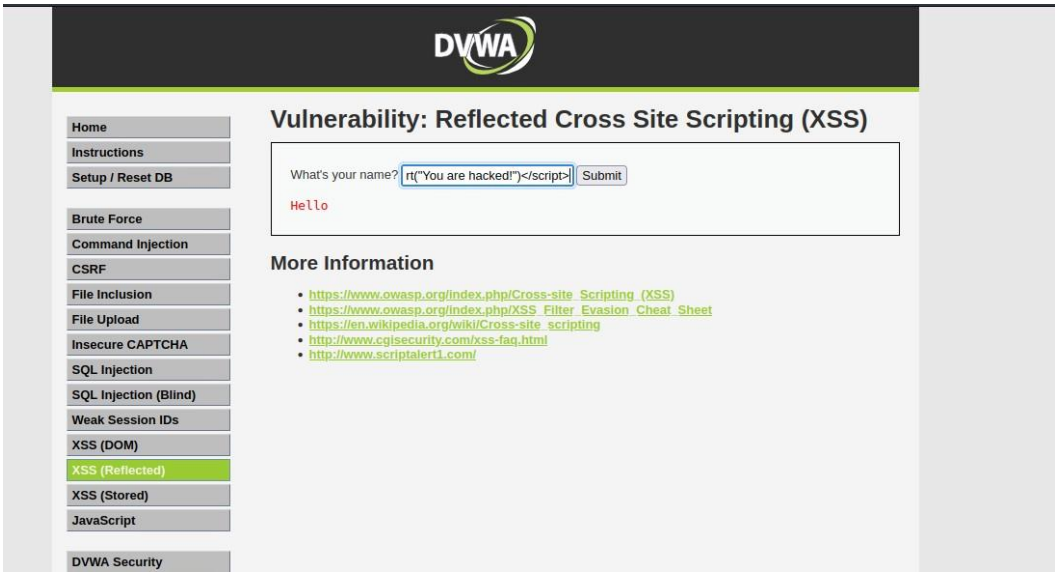
On this level there is no security. The typed text is displaying without any checks. I decided to try to show the session.



And the result was this:

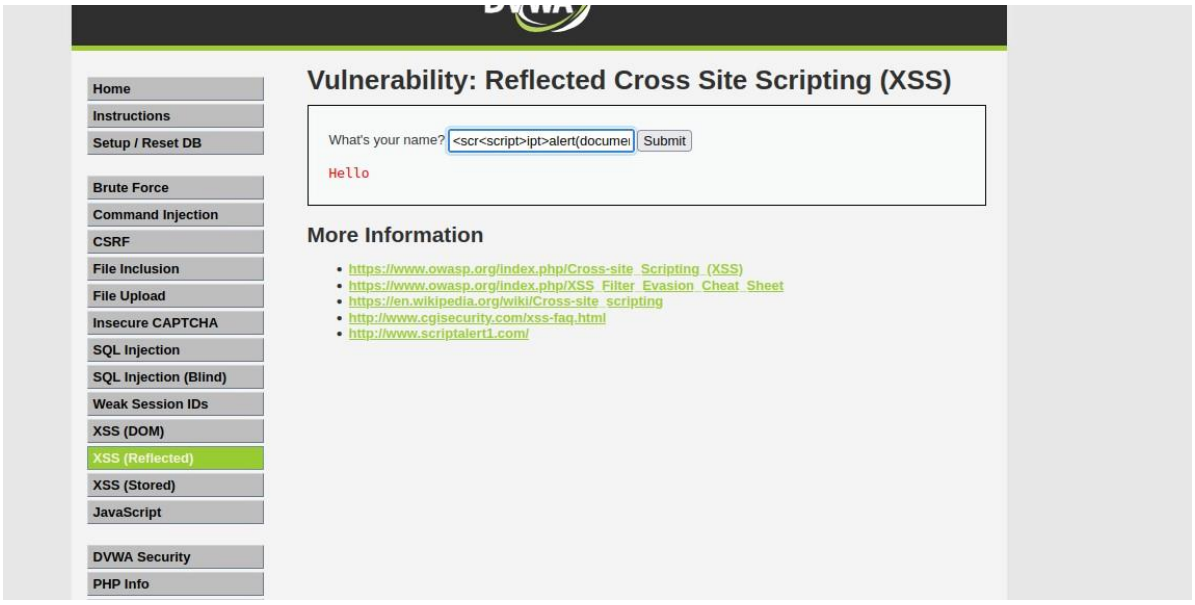


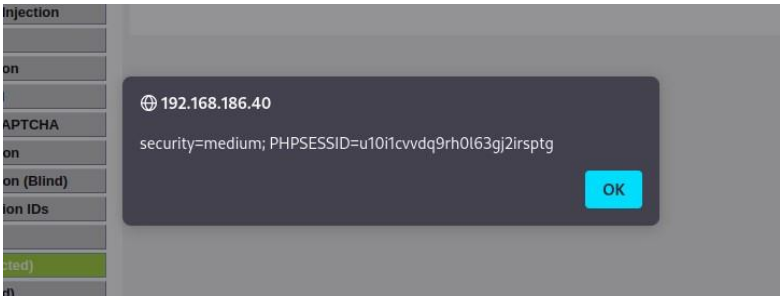
I also manage to display message:



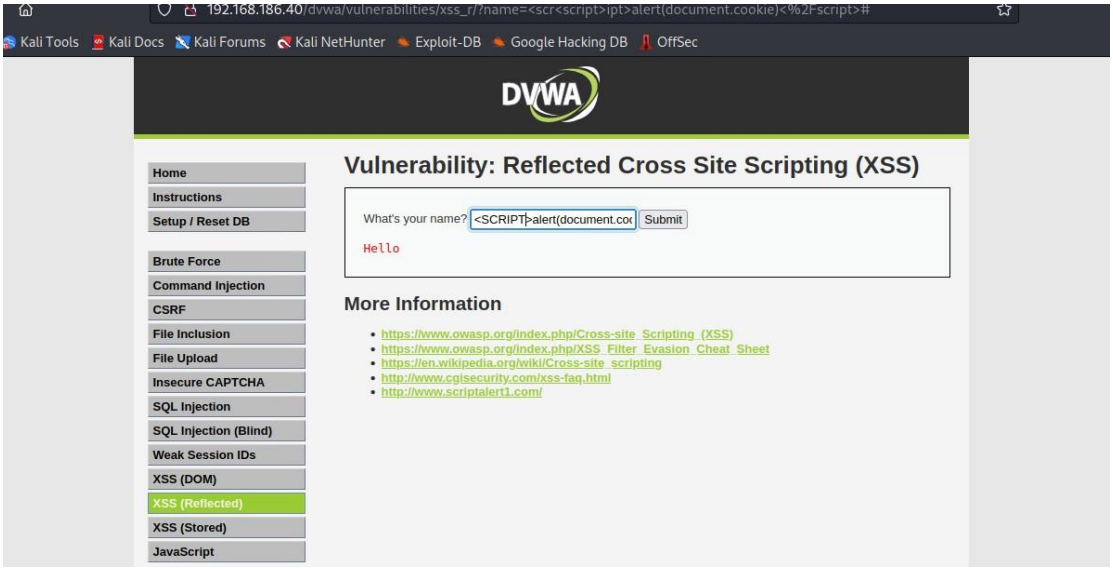
2. Medium

On this level there is a little protection that checks if there is any script tag. if it found one it will be removed. The gap here is that only check for the opening tag.



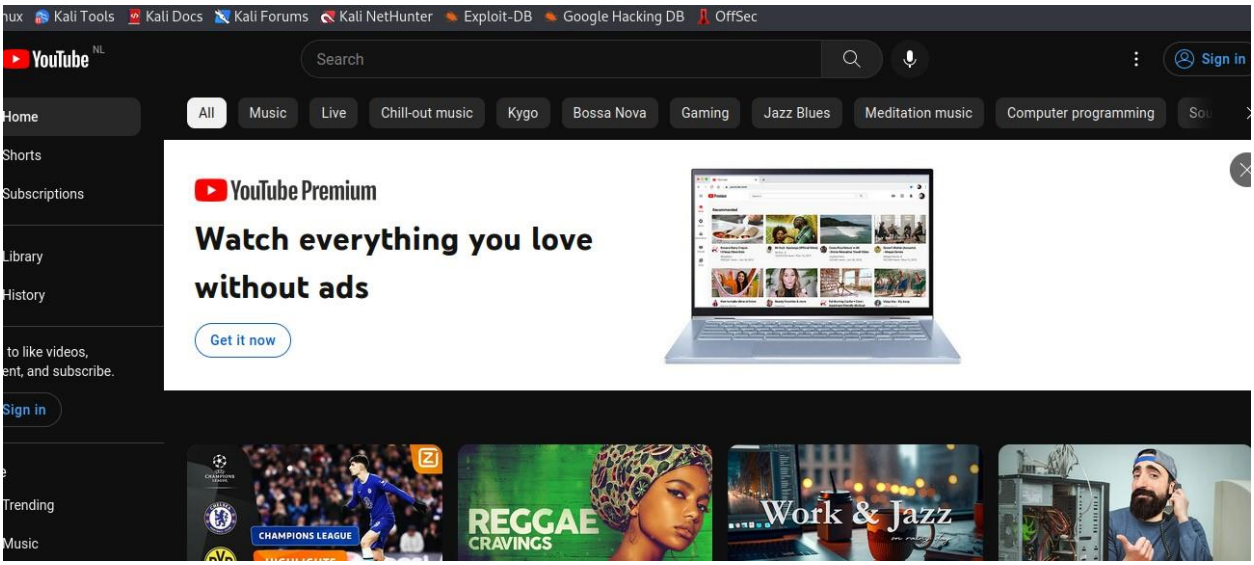


There is another way to pass the security check- using capital letters:



There result was the same as the previous example.

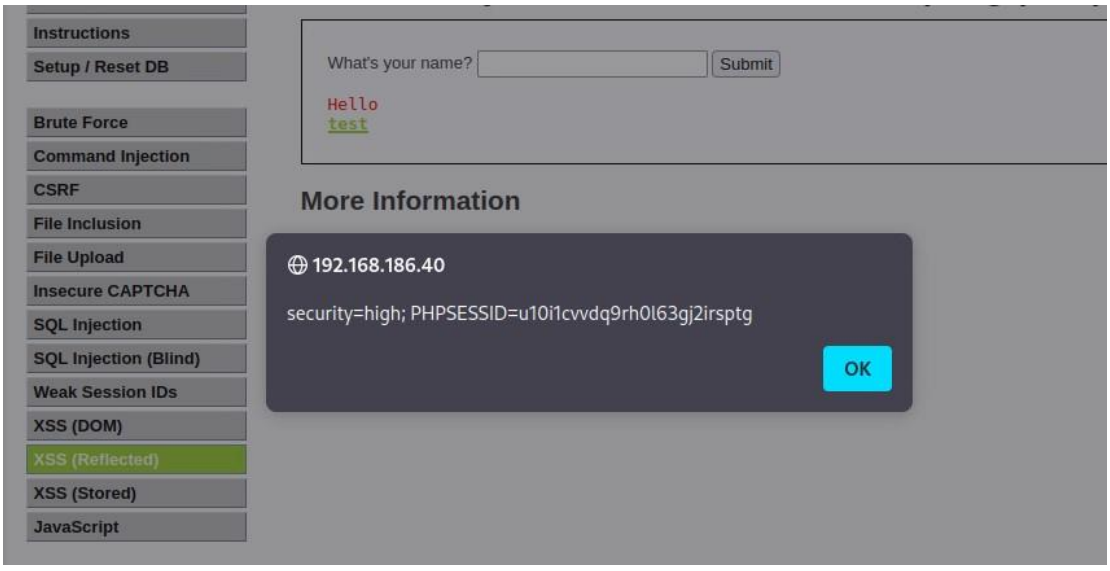
I decided to play a little bit and tried to redirect the page to YouTube- it was successfull.



3. High

Here the application is checking almost everything and it is removing everything when detect script tag in any form. But the hole for the HTML tag is still there.

When this command will be executed it will be showed as a link and in order to see the message you have to click on it.



Afterthoughts

Cross-Site Scripting (XSS) is a web application vulnerability that allows malicious actors to inject malicious scripts into web pages viewed by other users. Preventing XSS attacks requires careful coding practices and input validation in web applications. Secure coding practices, such as using output encoding and avoiding direct injection of user input into HTML, JavaScript, or other active content, can also mitigate XSS vulnerabilities. Web application firewalls (WAFs) can also play a role in preventing XSS attacks by blocking or sanitizing any malicious scripts before they reach the web application.

Reflections

Wikipedia contributors. (2023, March 5). *Cross-site scripting*. Wikipedia. https://en.wikipedia.org/wiki/Cross-site_scripting

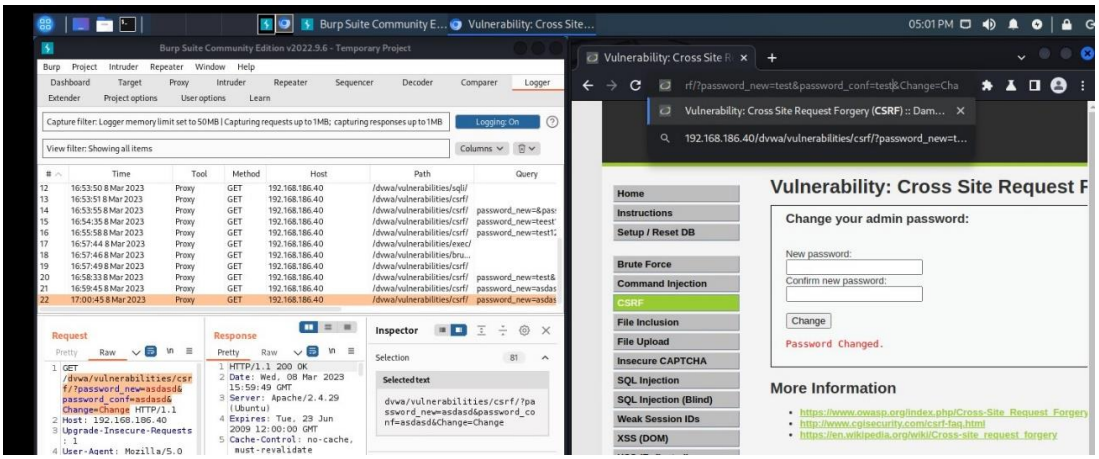
Wikipedia-bijdragers. (2023, January 3). *Burp Suite*. Wikipedia. https://nl.wikipedia.org/wiki/Burp_Suite

CSRF (Cross Site Request Forgery)

Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It allows an attacker to partly circumvent the same origin policy, which is designed to prevent different websites from interfering with each other.

1. Low

This level to be done I made several things. I created a new password which was ‘asdasd’. When the new password was set, I used Burp Suite to find the send request for this change.

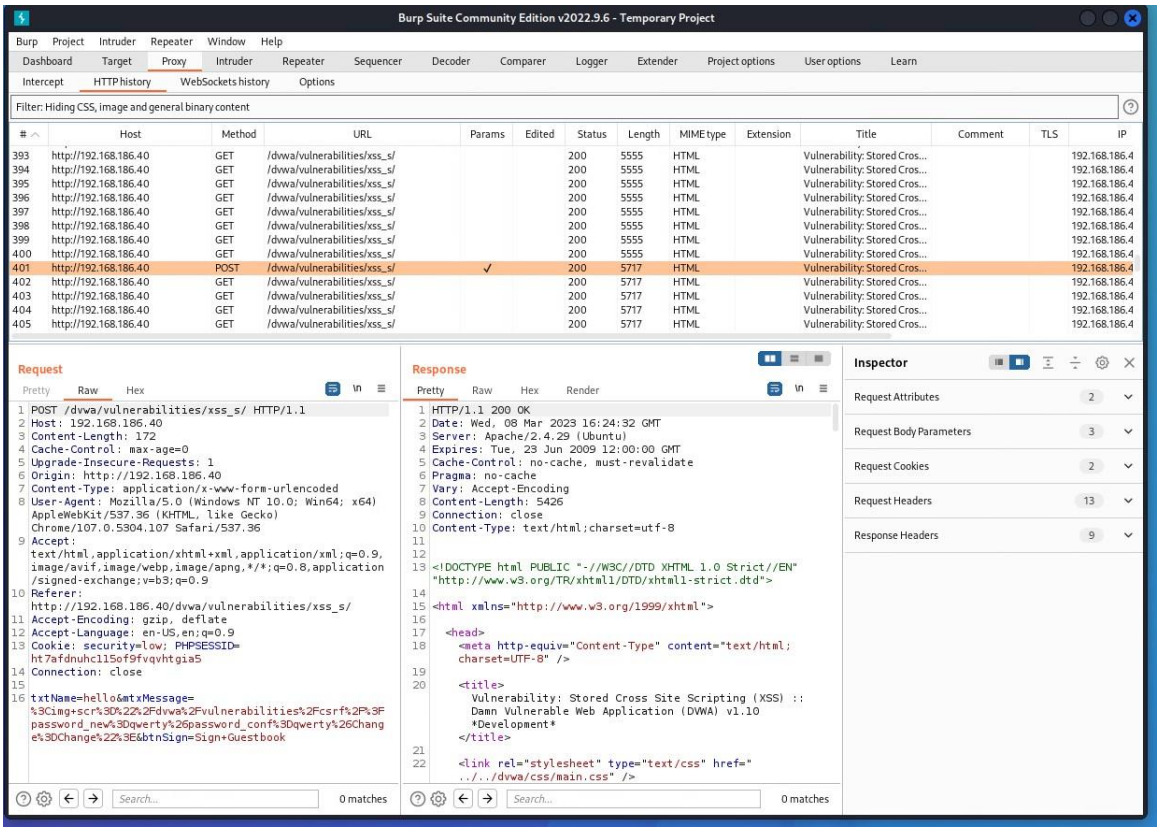


As you can see the get request contains the very new password. In order to change again the password without the knowledge of the user, I copy the request and paste in in the URL. Then I changed the password to ‘test123’. After the execution of the command, I checked if it worked in Brute Force tab. First, I tried with username ‘Admin’ and password ‘asdasd’ and the result Was this:

Then I tried with the new password and I succeeded.

2. Medium

This level was very hard to accomplish. I changed the password again to ‘test’. I tried again the same way as previous task but nothing – “That request didn’t look correct.”. Then I compare the requests of the Low and Medium level and I found that they are different. The Medium level request do not have the information that we used in the first task, also there are some changes in the ‘Refer’ section of the request. So to beat the system I have to change the ‘Referer’ header(a form of verification that the request is coming from the application’s own domain) to be a subdomain.I chose XSS (stored) tab and write a message that contains the requests from the Low level in image tag.



The password was changed to ‘qwerty’. It was executed correctly and I tried it in Brute Force tab. I tried the old password and then the freshly changed one.

Afterthoughts

Cross-Site Request Forgery (CSRF) is a type of web vulnerability that allows an attacker to perform unauthorized actions on behalf of a victim user on a different website. To prevent CSRF attacks, proper security measures must be implemented, such as using anti-CSRF tokens, regularly updating and patching web applications, frameworks, and libraries to the latest secure versions, and synchronizing token defenses built into many frameworks. It is recommended to research if the framework has an option to achieve CSRF protection by default before trying to build a custom token generating system. For example, .NET has built-in protection that adds a token to CSRF vulnerable resources. CSRF attacks can be used in a pen-test project by exploiting the vulnerability in the web application's design or implementation. A hypothetical scenario of how CSRF could be used in a project is when an attacker creates a malicious website or sends a malicious link to a victim user, enticing them to click on it. The victim's browser sends the unauthorized request to the vulnerable web application, which processes it as a legitimate request due to the lack of CSRF protection.

Reference

What is CSRF (Cross-site request forgery)? Tutorial & Examples | Web Security Academy. (n.d.). https://portswigger.net/web-security/csrf

Risk Consultant

Network Scanning and Enumeration

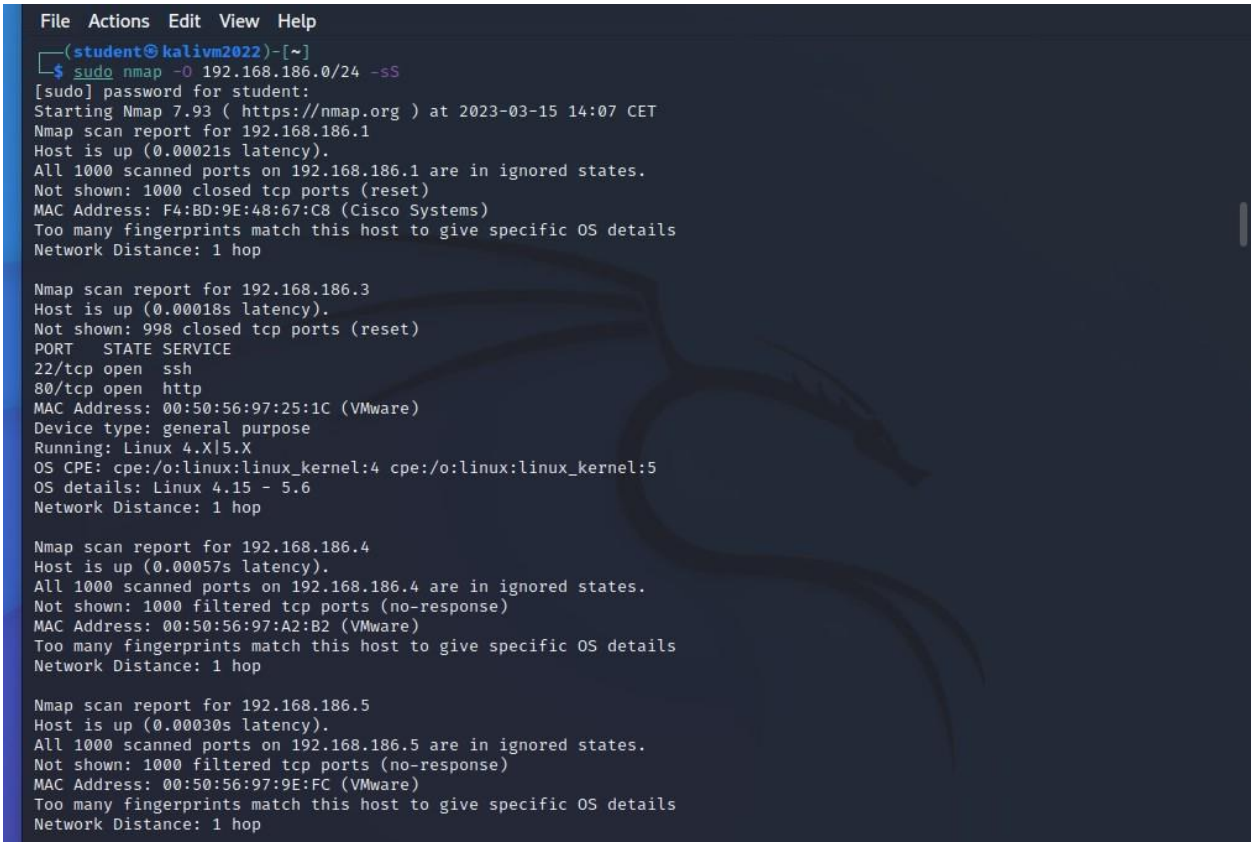
Nmap (Network Mapper) is a popular open-source tool used for network exploration, management, and security auditing. It can be used to discover hosts and services on a computer network, create a map of the network, and identify vulnerabilities and security weaknesses in a system.

Read, show and explain about the different type of **port scanning techniques**

The transmission control protocol (TCP) is defined as a connection-oriented communication protocol that allows computing devices and applications to send data via a network and verify its delivery.

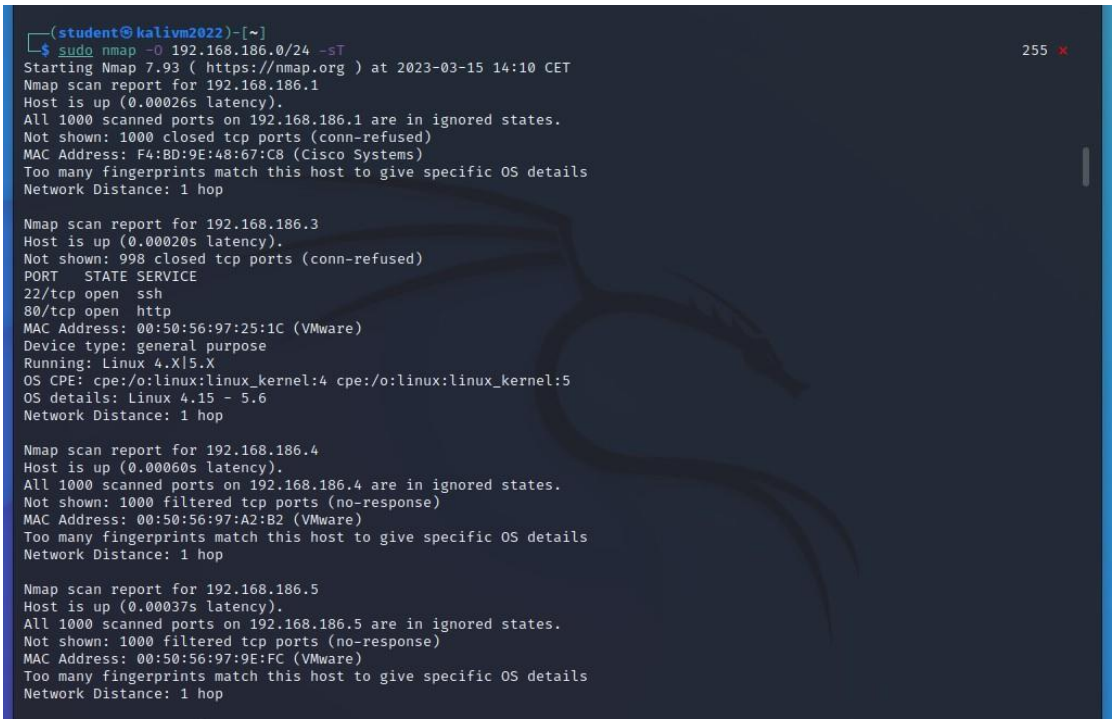
User datagram protocol (UDP) is a message-oriented communication protocol that allows computing devices and applications to send data via a network without verifying its delivery, which is best suited to real-time communication and broadcast systems.

There are several port scanning techniques in Nmap. The TCP SYN port scan is executed with the “-sS” switch and it is placed at the end of the line.

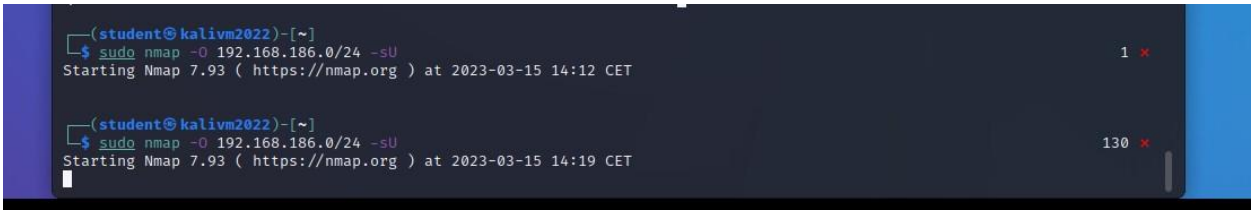


After the execution of the command, you will see all ports on the network.

If you change the switch to “-sT”, it will display only TCP connect ports.



To display only UDP ports the switch is “-sU”.



Read, show and explain about **service scans for enumeration**

To receive more information about the information that is running behind a certain port, the switch for the same Nmap command is “-sV”. The tool will try to guess the client software. The command should look like this: “nmap 192.168.186.0/24 -sV” and the result is this:

```
MAC Address: 00:50:56:97:A2:B2 (VMware)

Nmap scan report for 192.168.186.5
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.186.5 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:97:9E:FC (VMware)

Nmap scan report for 192.168.186.6
Host is up (0.0014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE  SERVICE VERSION
80/tcp closed http
MAC Address: 00:50:56:97:C8:07 (VMware)

Nmap scan report for 192.168.186.7
Host is up (0.000087s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 00:50:56:97:BB:90 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.186.8
Host is up (0.000092s latency).
All 1000 scanned ports on 192.168.186.8 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:50:56:97:A0:AA (VMware)

Nmap scan report for 192.168.186.9
Host is up (0.00071s latency).
All 1000 scanned ports on 192.168.186.9 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:97:38:0E (VMware)

Nmap scan report for 192.168.186.10
Host is up (0.00072s latency).
All 1000 scanned ports on 192.168.186.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:97:04:AF (VMware)

Nmap scan report for 192.168.186.12
Host is up (0.00046s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http     Apache httpd 2.4.29 ((Ubuntu))
443/tcp open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 00:50:56:97:CB:C5 (VMware)
```

Read, show and explain how you can **detect the operating system of a system**

To remote OS detection using TCP/IP stack fingerprinting the switch for that is “-O”.

```
┌──(student㉿kalivm2022)-[~]
└─$ sudo nmap -O 192.168.186.0/24                                                130 ×
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 14:25 CET
Nmap scan report for 192.168.186.1
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.186.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: F4:BD:9E:48:67:C8 (Cisco Systems)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.186.3
Host is up (0.0015s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:50:56:97:25:1C (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

Nmap scan report for 192.168.186.4
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.186.4 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:97:A2:B2 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.186.5
```

Reference:

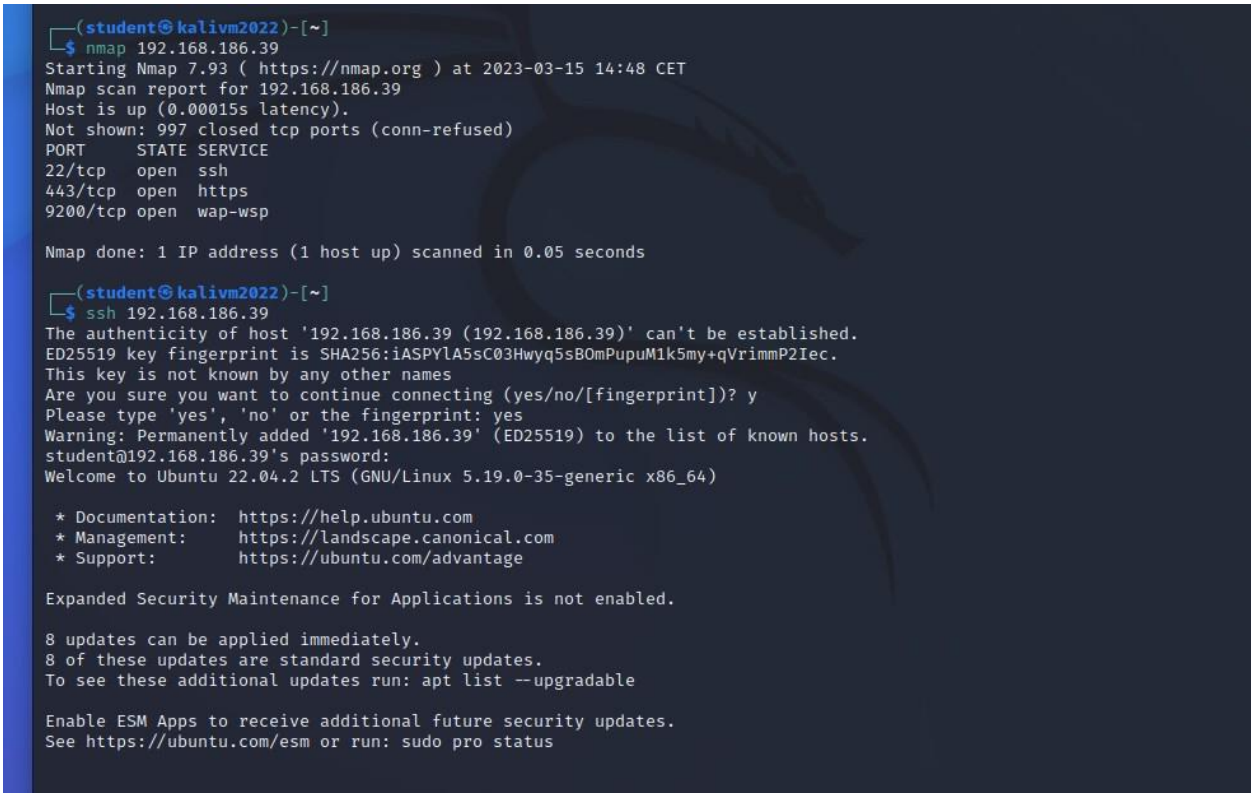
BasuMallick, C. (2022, April 18). *Differences Between TCP and UDP - Spiceworks*. Spiceworks. https://www.spiceworks.com/tech/networking/articles/tcp-vs-udp/#:~:text=Transmission%20control%20protocol%20(TCP)%20and,UDP%20prioritizes%20speed%20and%20efficiency.

House, N. (2023, March 6). *Nmap Cheat Sheet 2023: All the Commands, Flags & Switches*. StationX. https://www.stationx.net/nmap-cheat-sheet/

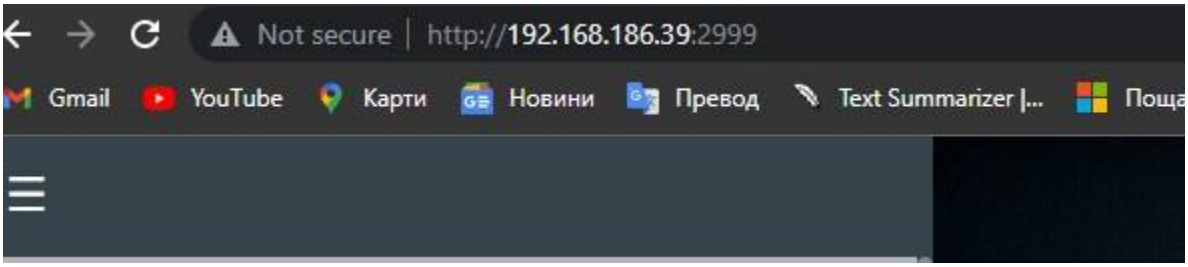
Secure Network Connections (HTTPS/TLS/SSH)

See "Exercise HTTPS and SSH" on the LMC

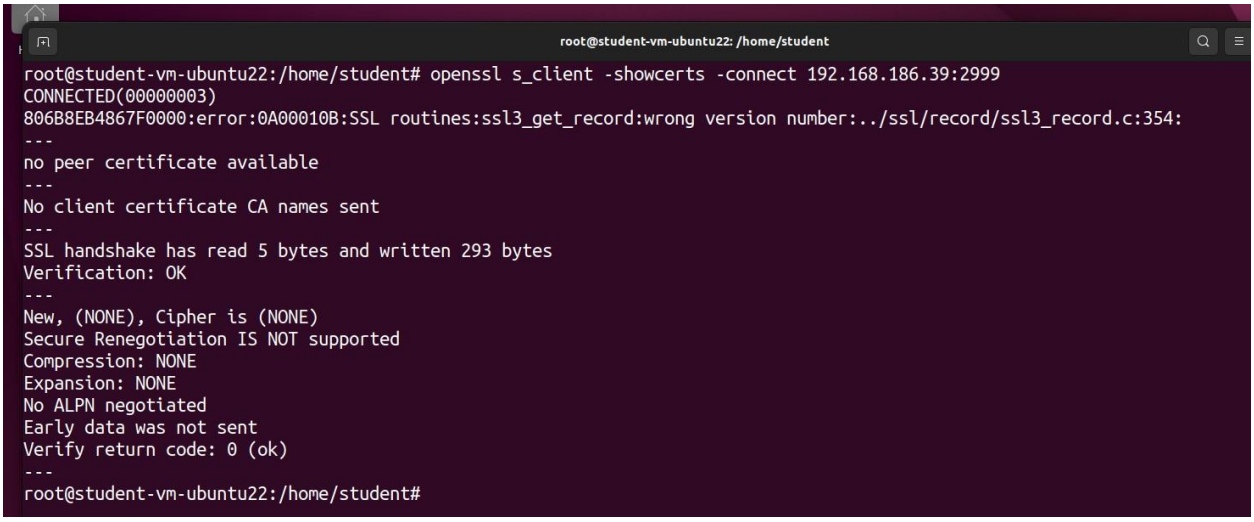
First task that I made was “Connecting with SSH to server”. For this task first I have to install “openssh- server” on the ubuntu server. Then I used the kali machine to identify my ubuntu machine using the “nmap” tool. Then I used the ‘ssh’ command to connect to my Ubuntu machine.



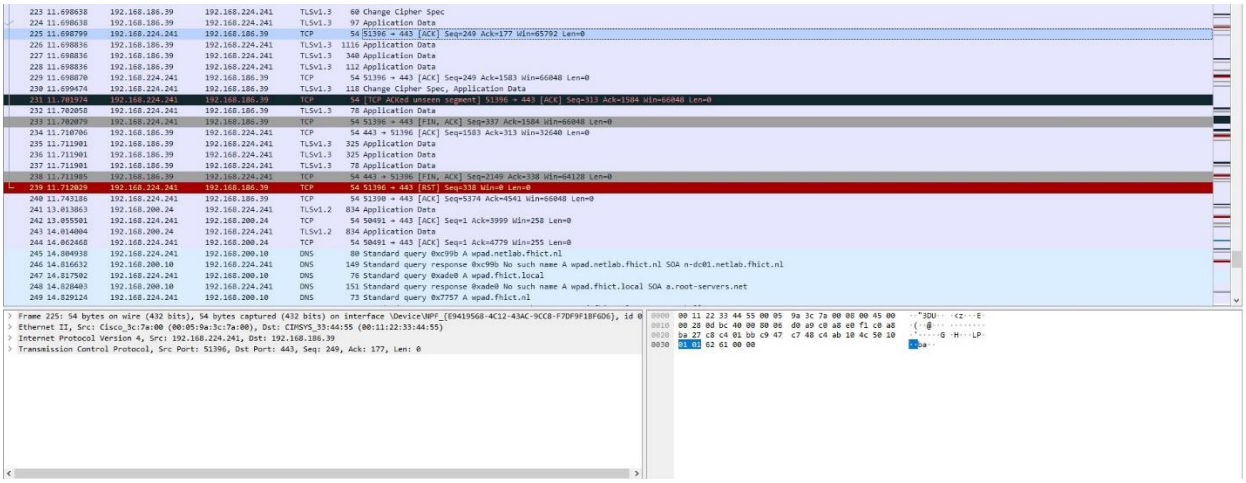
For the next task (Self-signed certificate web server), I have to use a localhost website. First, I check if it will have and certificate- it did not.



Another confirmation about that was from the Ubuntu machine:



I followed the guide from the document and the website www.digitalocean.com for the self-signed certificate and the result was this:



Afterthoughts

Implementing secure network connections using HTTPS, TLS, and SSH is essential for protecting data in transit and ensuring the confidentiality, integrity, and authenticity of information exchanged

over networks. Best practices such as using the latest protocols, properly configuring certificates, using strong cryptographic algorithms, and educating users can help enhance the security of network connections and mitigate potential security risks. HTTPS is the secure version of HTTP that uses SSL, TLS is a cryptographic protocol used to secure communication between clients and servers over a network, and SSH is a cryptographic network protocol used for secure remote access and management of servers and network devices.

Law, Ethics and Responsible Disclosure

> Find a few examples of cybercrime cases (sentences and penalties). If you are a student from abroad, find such example cases from your home country.

I found 2 cases of cybercrime that are made in Bulgaria.

The first case was made 4 years ago and the target was National Revenue Agency. The hackers were 2 - Christian Boykov and Ivan Todorov. In July 2019, the databases with personal data of the NRA were breached by hackers and the EGNs, names and addresses of 6 million Bulgarians were stolen. For a country with a population of just seven million people, the scale of the hacking attack meant that almost all working adults were affected.

I remember this case and it came from nowhere. I also remember that the “ГДБОП” (Main Directorate "Fighting Organized Crime") find the hackers really quickly. The sad news is that till this day they are not in jail.

The second case that I found was from several months ago and it is an attack on the websites of the presidency, power ministries and the Constitutional Court. It was done by the Russian hacking group “KillNet”. The website of the President's Administration has been the subject of a massive DDoS attack, associated with a delay or temporary restriction of access to the site. DDoS attacks block access to certain servers by sending an excessive number of requests through computer programs.

> Describe what you will do if you find a high-risk vulnerability, unexpected, in a website or IT-infrastructure. Take into consideration if you want to make money or make the world a safer place.

Last summer I had that situation. One of my friends showed me an app that can read NFC chip, can write it and can rewrite it again on the same device. I download the app on my phone and tried to read some information with it. Luckily from my work I had a bracelet for check-in, so I was playing with it. At some point I found that the app can read information from debit and credit cards. I tried it with my “Revolut” and “ING” card – nothing happened, but when I tried it in my Bulgarian card, it managed to take some information (encrypted of course). I tried with my parents’ cards and again managed to read some information. I talked with my parents and they advised me to

talk with the IT department of the bank. I talked with them for that problem and they fixed that problem immediately. The new card that I received did not have this problem.

Find two or three companies and explain the concept of responsible disclosure they have in place and compare those companies.

One of the companies I found is called “Vi company”. the practice of 'responsible disclosure' is the best way to safeguard the Internet. It allows individuals to notify companies like VI Company of any security threats before going public with the information. This gives us a fighting chance to resolve the problem before the criminally minded become aware of it.

The second company I found that practices “responsible disclosure” is called “nedap”. They encourage everybody to report potential security vulnerabilities and they have also given a scope for what to report and what not to.

What to report:

- Cross-site scripting (XSS) vulnerabilities
- SQL injection vulnerabilities
- Security misconfiguration
- Sensitive data exposure

What not to report:

- HTTP 404 codes, or any non-200 codes
- Fingerprinting on public services
- Public files, or files with harmless information (i.e. robots.txt)
- Clickjacking-related issues
- SPF, DKIM or DMARC issues
- Reports about old software versions without a POC for a working concept
- Issues related to the use of old browser versions

Reference:

Чобалигова, Б. (2022, September 12). *CNN за хакерската атака срещу НАП: Цяла нация току-що беше хакната*. Investor.bg. https://www.investor.bg/a/261-

novini/286105-cnn-za-hakerskata-ataka-sreshtu-nap-tsyala-natsiya-toku-shto-beshe-haknata

Dariknews.bg. (2023, March 6). *4 години по-късно: Отложиха делото за хакването на НАП*. dariknews.bg. https://dariknews.bg/novini/bylgariia/4-godini-po-kysno-otlozhiha-deloto-za-hakvaneto-na-nap-2340857

Европа, С. (2022, October 15). *Руска хакерска атака срещу сайтовете на президентството, силовите министерства и Конституционния съд*. Свободна Европа. https://www.svobodnaevropa.bg/a/32084652.html

Responsible disclosure | VI Company. (n.d.). https://www.vicompany.nl/en/responsible-disclosure/

Responsible Disclosure - Nedap Healthcare. (2020, September 25). Nedap Healthcare. https://nedap-healthcare.com/responsible-disclosure/

Law, Standards & Compliance

GDPR - legal instrument ensuring the protection of individuals regarding the processing of personal data and on the free movement of such data.

The main goal of GDPR is to protect user's personal identifiable information which can include every unique information about a person (Ip address, bank details, country of residence, car number plates, most visited websites).

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.

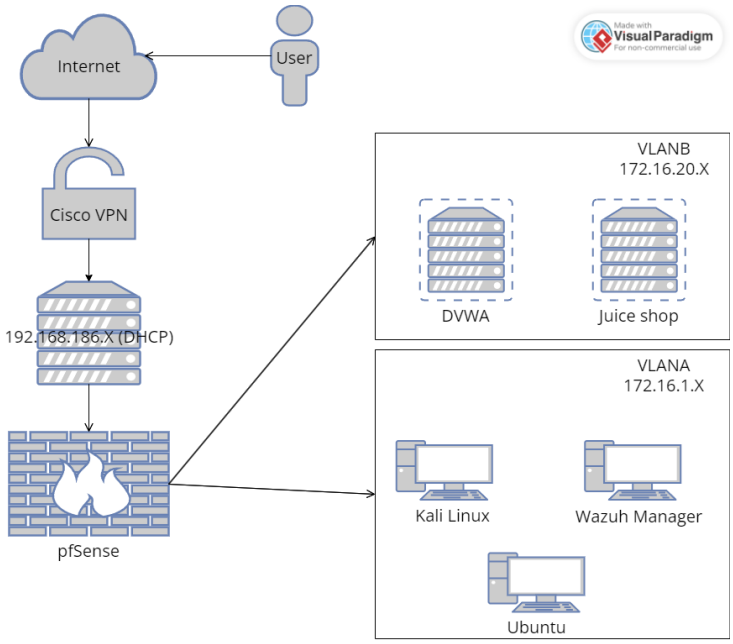
• The right to data portability - Individuals are allowed to get and reuse their individual information for their possess purposes over diverse administrations.
• The right to object - Individuals can protest to the preparing of individual information that's collected on the grounds of true blue interface 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.

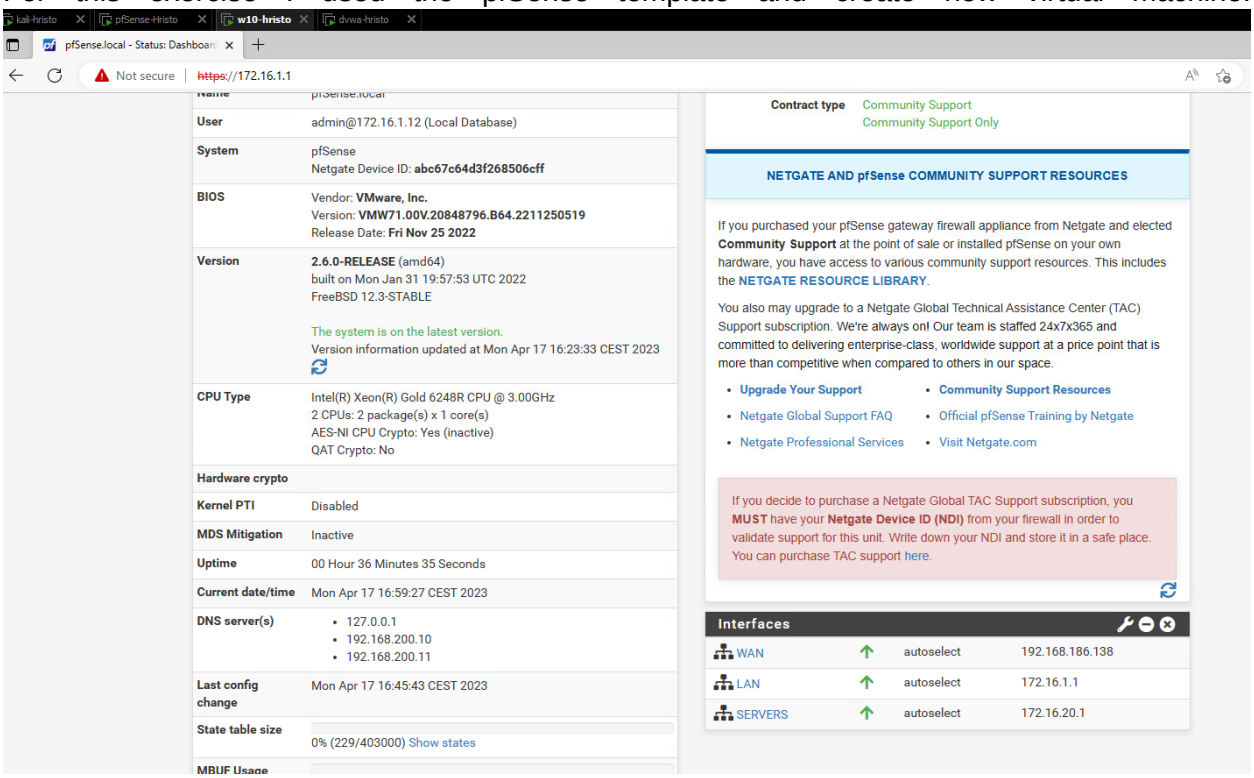
Purpose limitation requirements: personal data may only be used for specific, well-described and legitimate purposes;
Security requirements: organizational and technical measures must be taken to prevent the unlawful access to and processing of personal data;
Transparency requirements: the participant 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.

Network Separation and Segmentation (Firewalls)

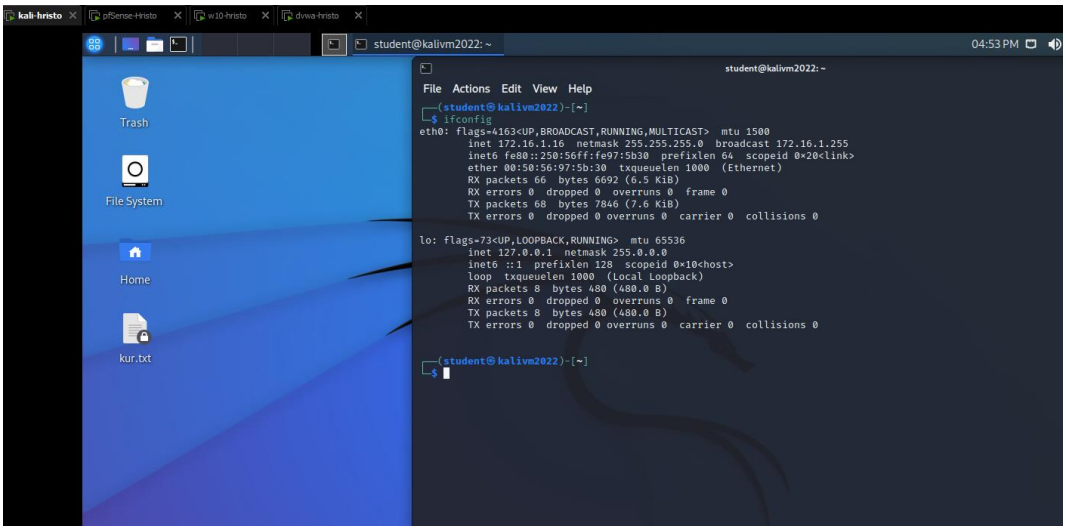
This is a network diagram of my seclab environment.



For this exercise I used the pfSense template and create new virtual machine.



After the configuration I added the kali and dvwa machines in it and test them. Everything was working correct.



Afterthoughts

Network segmentation and separation involve the use of firewalls and other network security devices to separate different parts of an organization's network and restrict access to sensitive information. It can help prevent the spread of malware and other cyberattacks, limit the impact of a security breach, and prevent attackers from accessing sensitive information. This includes regularly reviewing firewall rules and policies, implementing strong access controls, and monitoring network traffic for suspicious activity. To prevent attacks, it is important to properly configure and maintain firewalls and other network security devices. In a project, network segmentation and separation can be used to improve the overall security of the system by separating sensitive data and restricting access to it.

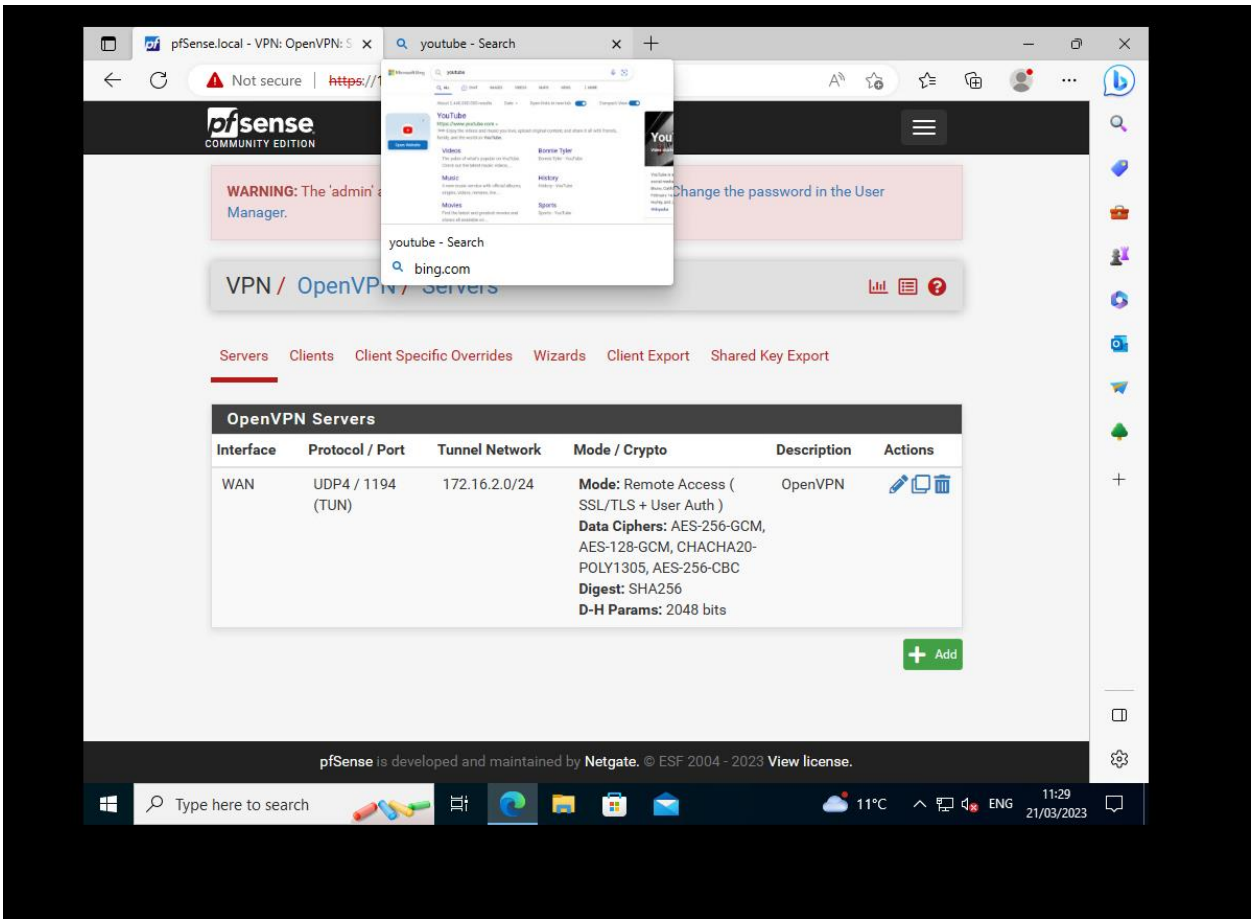
Secure Remote Access and Management (VPN)

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device, e.g., a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network.

A VPN is created by establishing a virtual point-to-point connection through the use of tunneling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN).

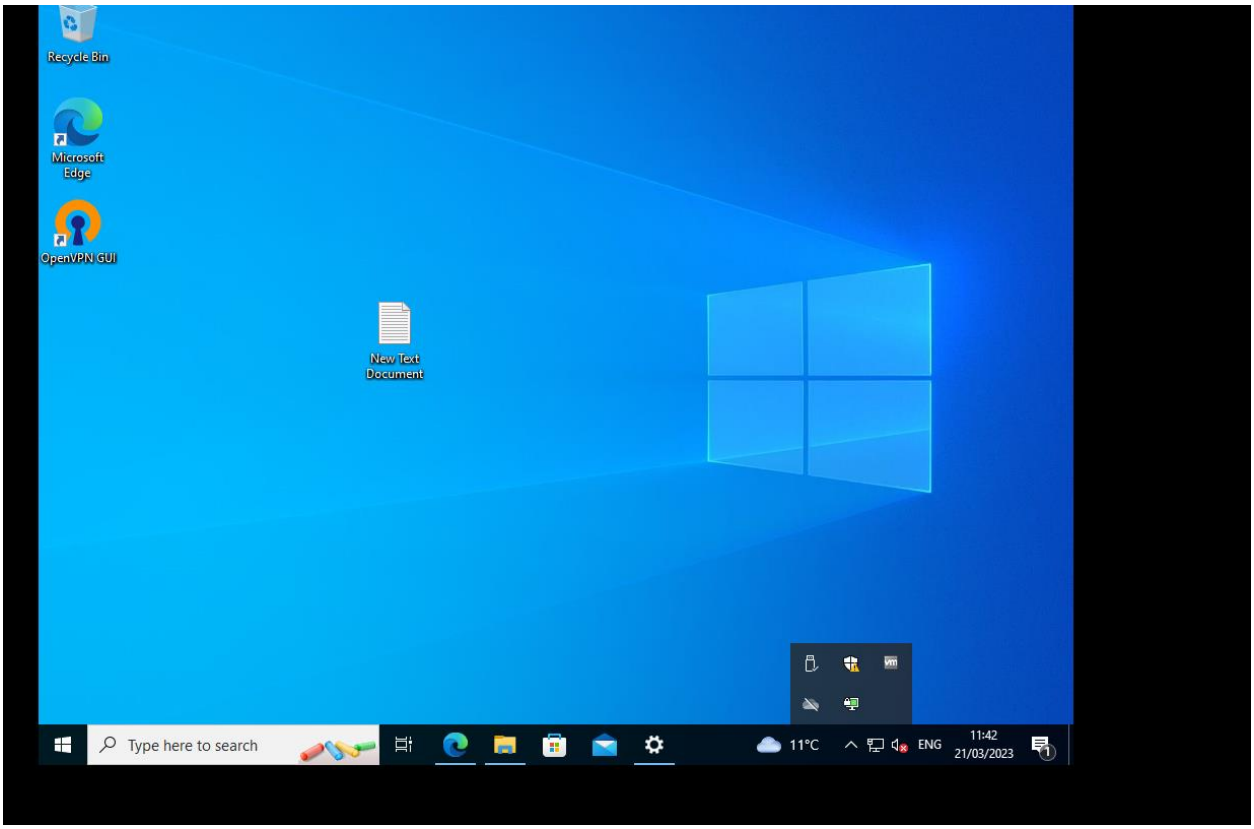
Create a VPN connection from a WAN-VLAN Windows 10 machine to your own Seclab demonetwork

I created a VPN connection in my Seclab using the OpenVPN. I connect to my pfSense and created the Certificate and set up the OpenVPN



I download it and I manage to connect to the VPN.

Service	Description	Status	Actions
dhcpd	DHCP Service	✓	
dpinger	Gateway Monitoring Daemon	✓	
openvpn	OpenVPN server: OpenVPN	✓	
syslogd	System Logger Daemon	✓	
unbound	DNS Resolver	✓	
vmware-guestd	VMware Guest Daemon	✓	
vmware-kmod	VMware Kernel Modules	✓	



The VPN starts automatically but you are connected to it when you open the app and fill your credentials. The icon will change to green when you are connected.

Afterthoughts

VPN technology is used to provide enhanced privacy, security, and anonymity for remote network connections. It creates a secure and encrypted connection over a public network, typically the internet, to establish a private network. It is important to understand the key aspects of VPN security, such as encryption, authentication, logging and privacy, server locations, software and configuration, trustworthiness of VPN service providers, and user awareness and education. In a project, VPN technology can be used to establish secure and encrypted connections for remote

access to internal networks, protect sensitive data transmitted over the network, enhance privacy and anonymity, and comply with security and regulatory requirements.

Reference

Wikipedia contributors. (2023d, March 14). *Virtual private network*. Wikipedia. https://en.wikipedia.org/wiki/Virtual_private_network

Network Sniffing and Spoofing

Sniffing will not disrupt the operation of the network operation. If the network is switched, it is impossible to sniff the entire network traffic because the switch will route the traffic from the sender to the destination. On a managed network sniffing can be done by defining one of the switch ports to mirror the traffic. Administrator permission is required. A common tool for sniffing is Wireshark.

Spoofing is the act of pretending to be another person or system.

• Sending an e-mail with a "from" address that isn't yours

• Sending a TCP/IP, ARP or DNS packet with a sender address that isn't yours

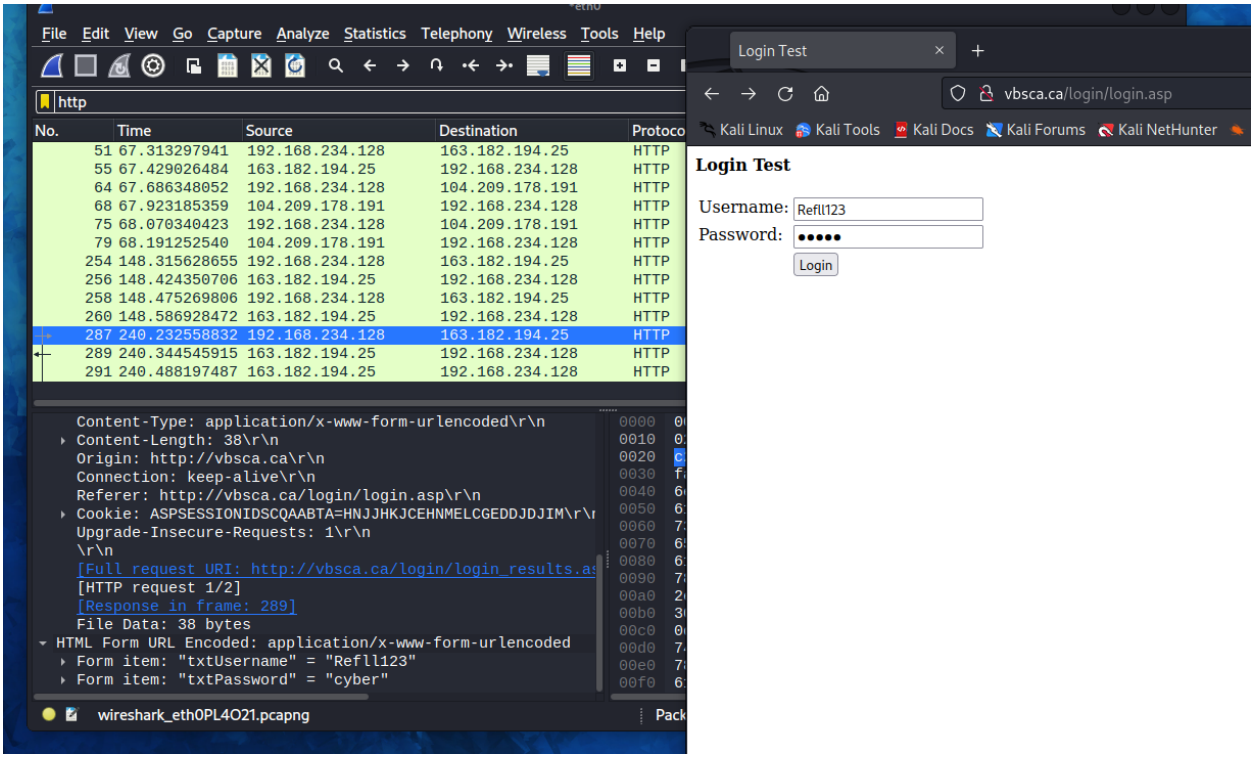
• Spoofing a website by cloning an existing website and using a similar but slightly different URL.

ARP spoofing uses a trick called “man in the middle” to pretend to be the router of the network. Therefore, all the traffic that comes to that router is first routed through the hacker’s machine then sent to the real router on the network. It enables devices to match IP addresses with corresponding MAC addresses. Each device keeps track of a list with cached replies. By fooling the switch, a hacker can become the "man-in-the-middle" between devices connected to the same network.

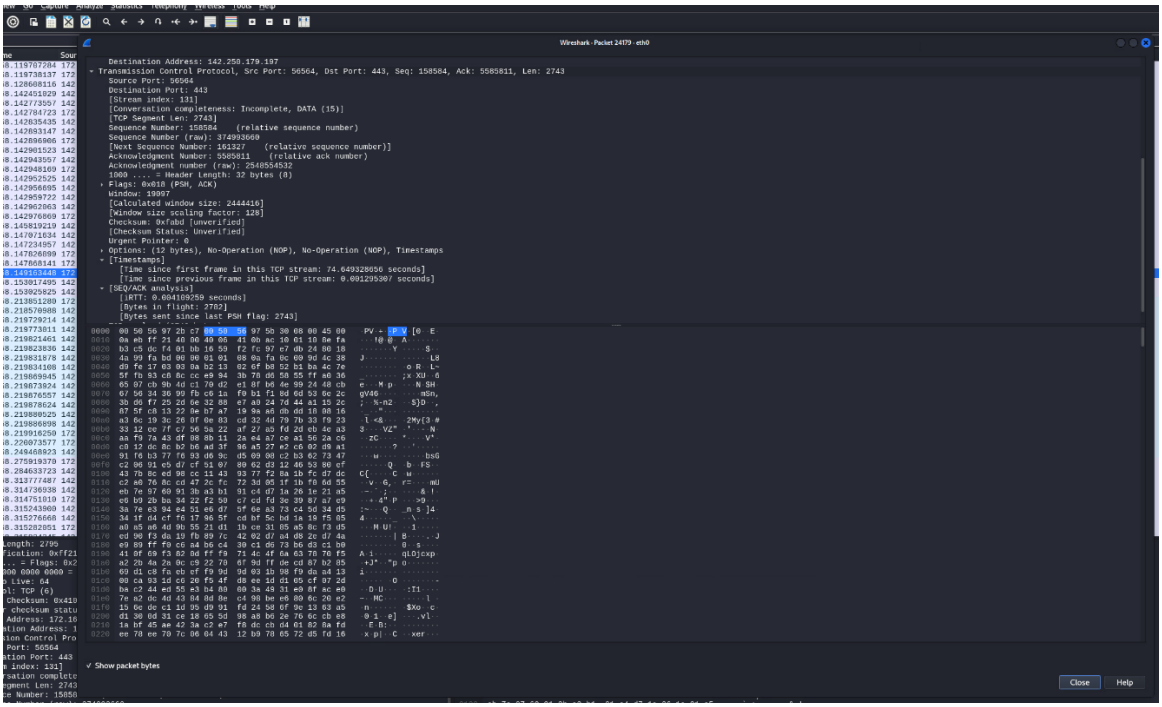
> Try to intercept a plain text password (HTTP or FTP) by capturing a login-name and password from
>
> 1) A non-secured connection

For this exercise I used Wireshark and this website: http://vbsca.ca/login/login.asp

I filled the credentials and submit. Then I used Wireshark to find this request and when I found it I saw everything.



2) password from secured connection

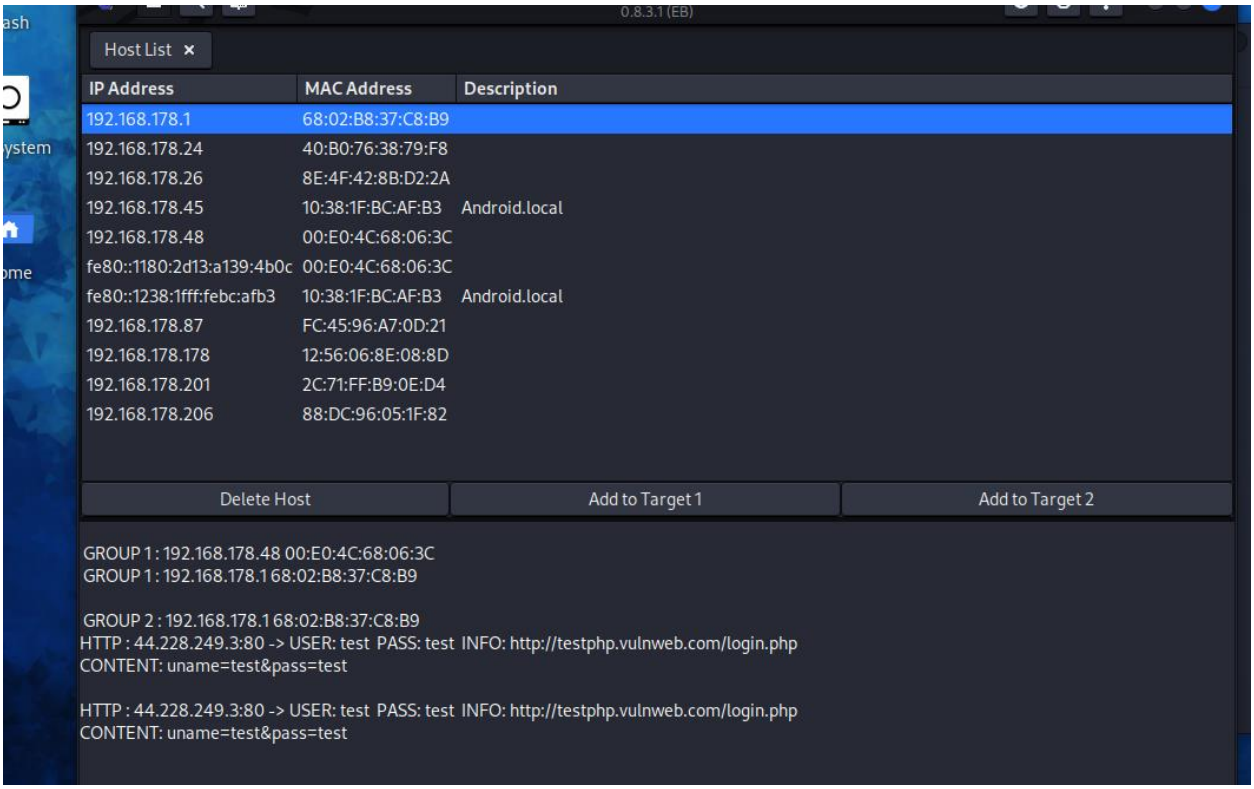


I tried the same thing but on a secured website- Gmail.com. The request was encrypted.

Demo and explain ARP spoofing

For this exercise I used the Ettercap tool. **Ettercap** is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

The first thing I did was to find all hosts. Then I select my Ip as a “Target 2” and the router Ip as a “Target 1” then I start the ARP poisoning. From other computer I entered a non-encrypted website(http://testphp.vulnweb.com/login.php) and I managed to get the login credentials:



As you can see the credentials was: Username: test and Password: test.

Explain what can be done to protect against ARP spoofing

• When connected to a public Wi-Fi network (e.g., McDonald’s) use VPN to encrypt the packets of information.

• Only open webpages starting with HTTPS, because the connection is secure.

• Do not click on dodgy links.

Afterthoughts

Network sniffing and spoofing, also known as man-in-the-middle (MITM) attacks, pose significant security risks to network communications. To prevent these attacks, it is important to implement strong encryption protocols, use strong authentication mechanisms, properly segment the network, monitor and analyze network traffic, and regularly monitor and analyze network traffic. These measures can help protect against network sniffing and spoofing attacks by encrypting data transmitted over the network, using strong authentication mechanisms, properly segmenting the network, monitoring and analyzing network traffic, and regularly monitoring and analyzing network traffic. In a project, network sniffing and spoofing attacks can be used to intercept sensitive data transmitted over the network, modify communication, or inject malicious content, leading to data breaches, unauthorized access, and other security incidents.

Reference

Ettercap Home Page. (n.d.). https://www.ettercap-project.org/index.html

Wireless Hacking

Crack WPA (2) with airmon-ng and aircrack-ng from Kali Linux

WPA2 (Wi-Fi Protected Access 2) is an encrypted security protocol that protects internet traffic on wireless networks. The second-generation of the Wi-Fi Protected Access security protocol, WPA2 addresses earlier flaws and offers more powerful encryption. In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2. The WPA3 standard also replaces the pre-shared key (PSK) exchange with Simultaneous Authentication of Equals (SAE) exchange, resulting in a more secure initial key exchange in personal mode and forward secrecy.

airmon-ng-This script can be used to enable monitor mode on wireless interfaces. It may also be used to kill network managers, or go back from monitor mode to managed mode. Entering the airmon-ng command without parameters will show the interfaces status.

Aircrack-ng is a complete suite of tools to assess WiFi network security.

It focuses on different areas of WiFi security:

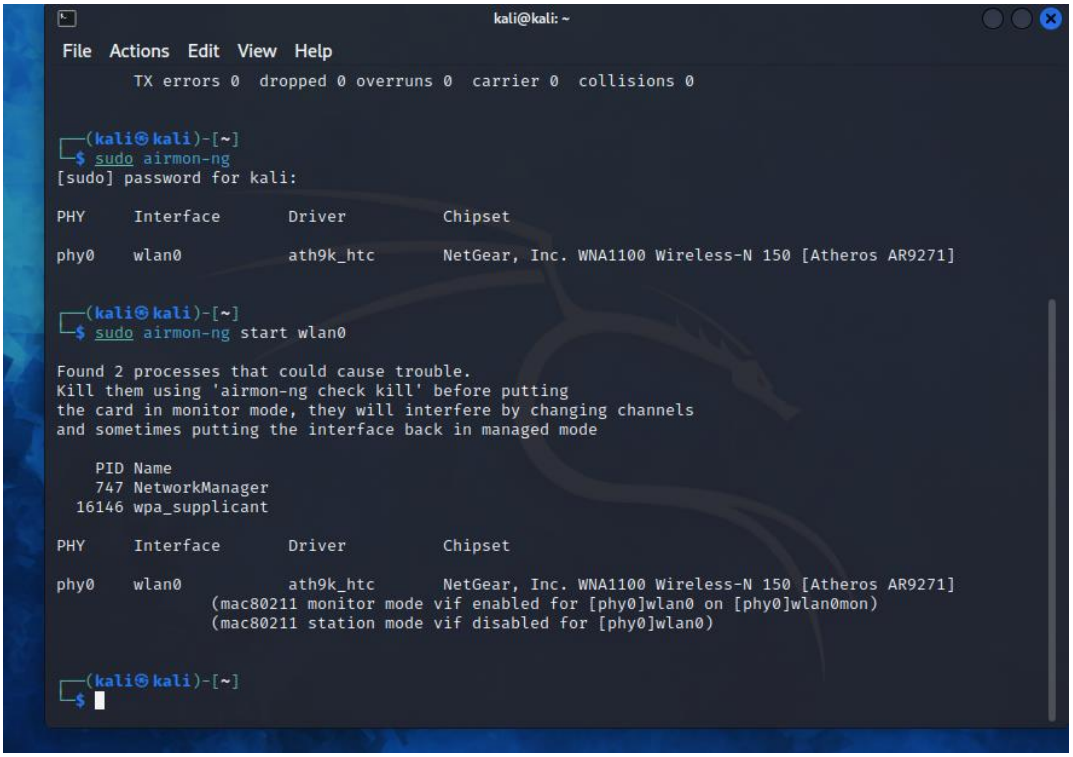
Monitoring: Packet capture and export of data to text files for further processing by third party tools

Attacking: Replay attacks, deauthentication, fake access points and others via packet injection

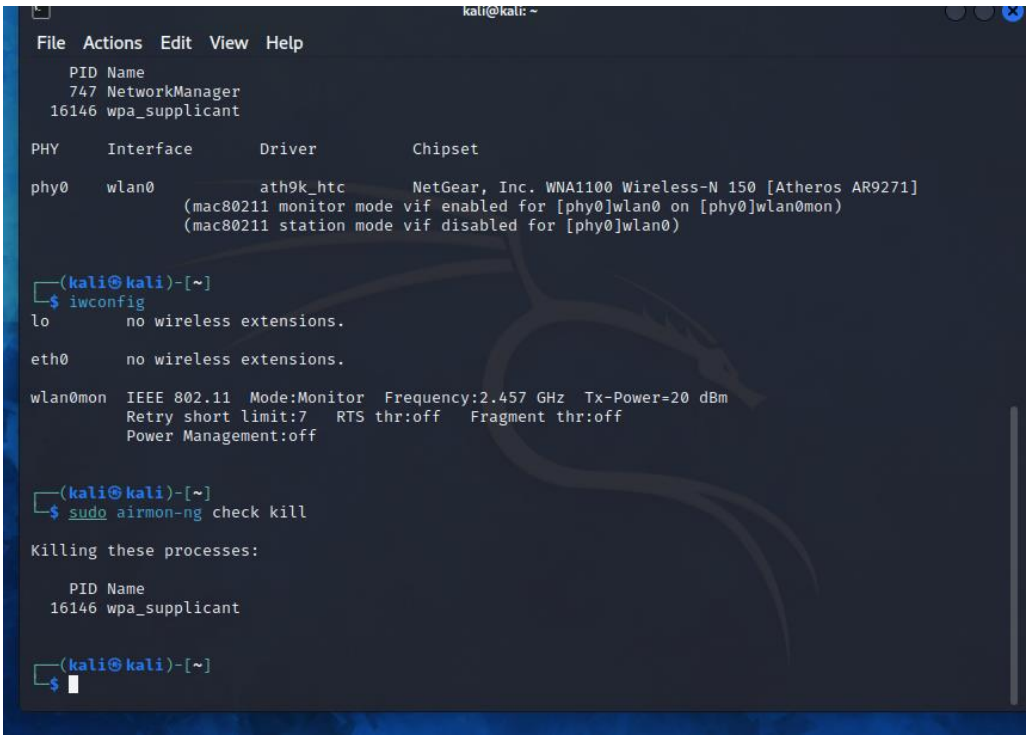
Testing: Checking WiFi cards and driver capabilities (capture and injection)

Cracking: WEP and WPA PSK (WPA 1 and 2)

For this exercise I also used NETGEAR tool (The NETGEAR N150 WiFi USB Adapter wirelessly connects to a Wireless-N network for applications such as surf, email, chat and a secure and reliable connection to the Internet.). The first thing to do is to put your WIFI card to monitor mode. It is important to run airmon-ng as an administrator.

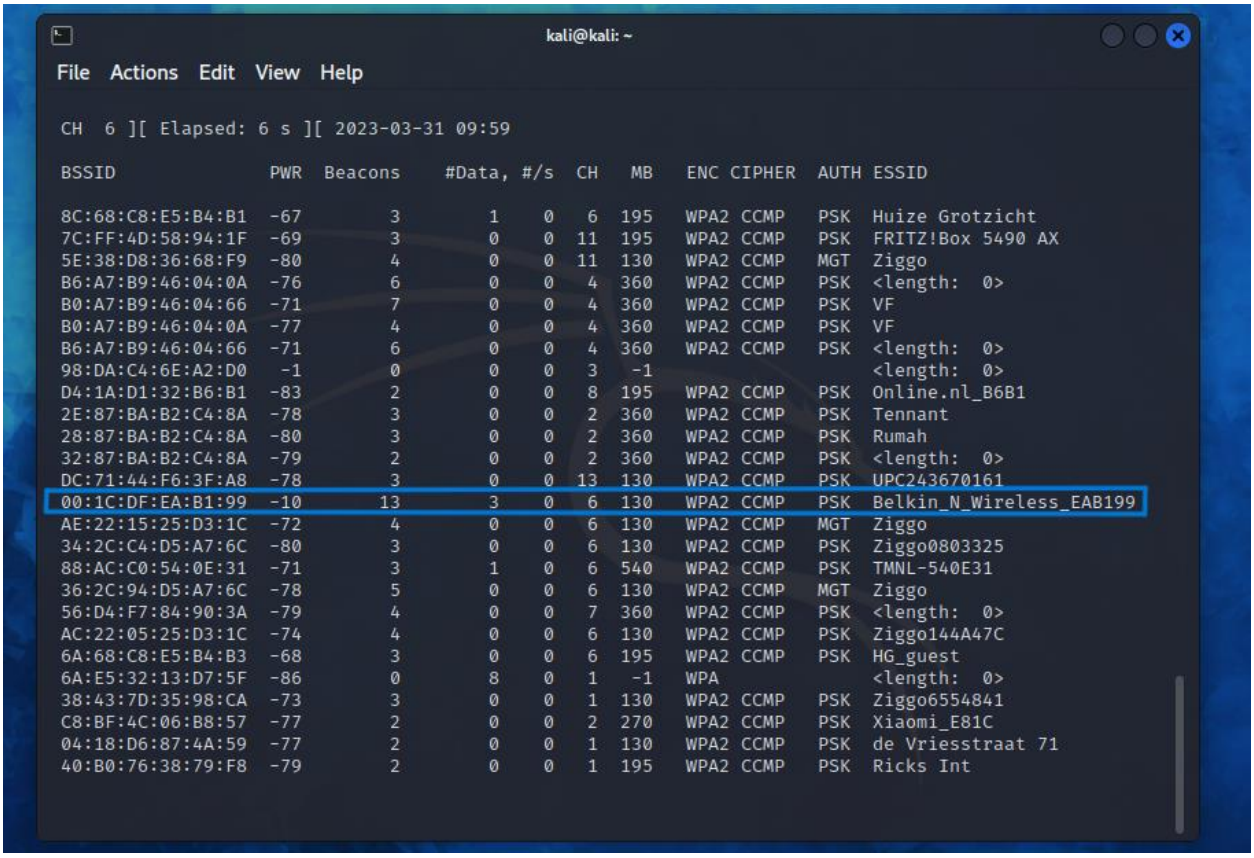


To be sure that the monitor mode is enabled I run the “iwconfig” command:

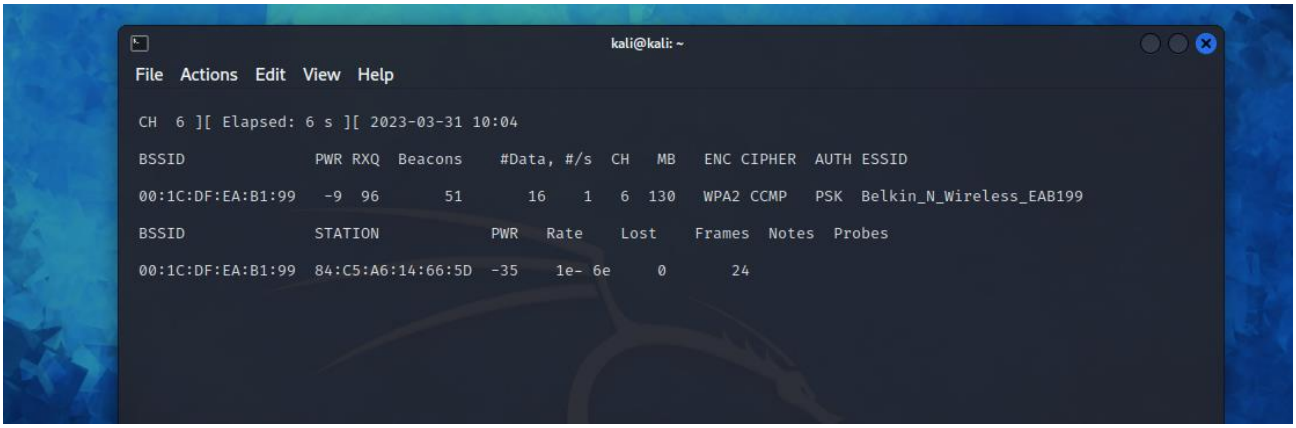


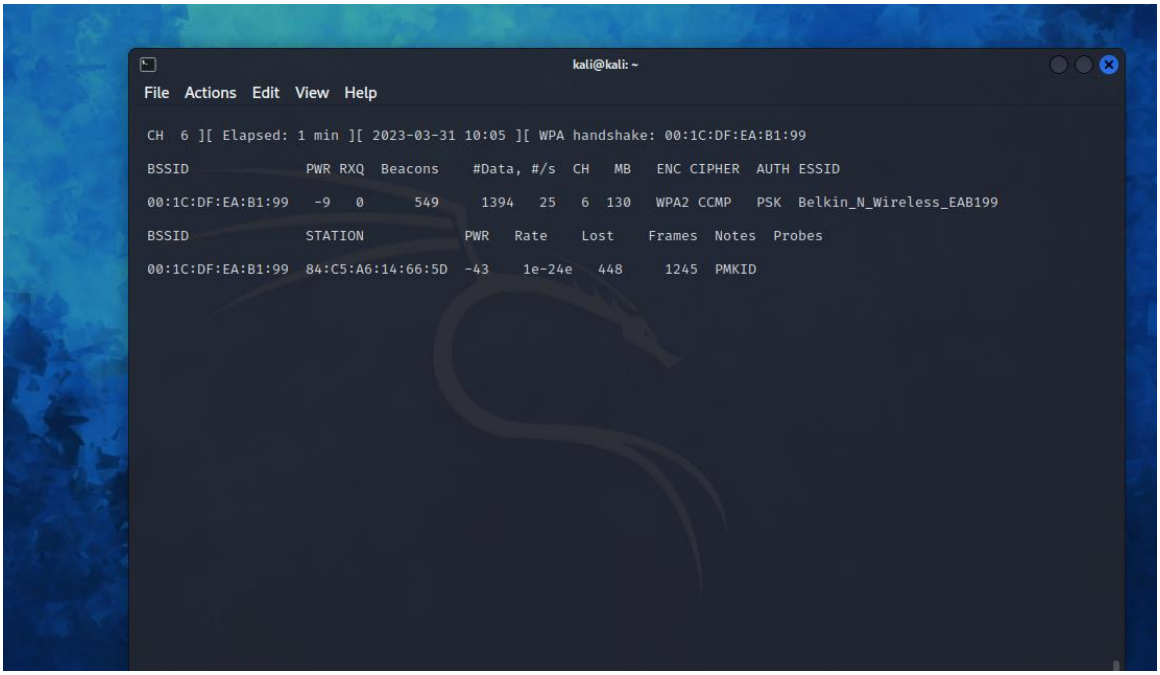
As you can see the WIFI card is on monitor mode and the name is modified from “wlan0” to “wlan0mon”. Before looking into the available WIFI connection I had to kill the processes that could interfere by changing the channels or putting the interface to managed mode. I do that with the command “airmon-ng check kill”

Then I used the command “airodump-ng [Network interface]” (in my case the interface will be “wlan0mon”). The airodump-ng command will display a list of detected access points near me, and also a list of connected clients (“stations”).



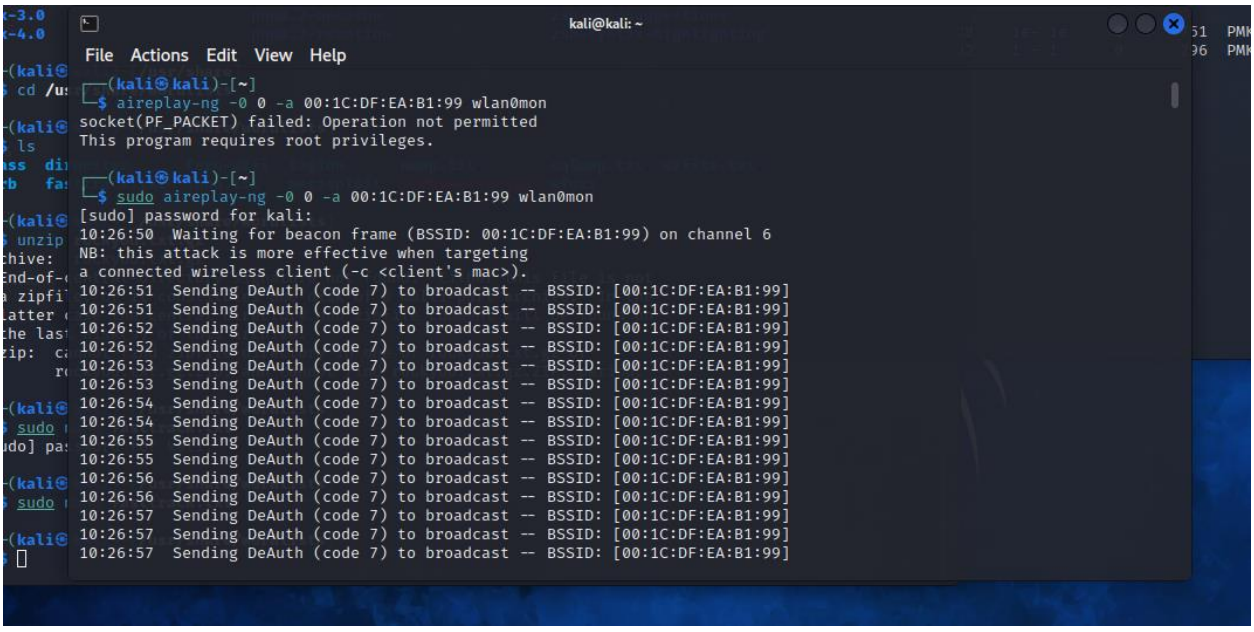
The selected target is “Belkin_N_Wireless_EAB199” and the important here is to remember the MAC address and the channel because I need them for the next command. Now I had to execute “airodump-ng -c [Channel of the network] –bssid [MAC address] -w [Directory where the file is going to be saved] [Network interface]”. In my case the command looks like this: “airodump-ng -c 6 –bssid 00:1C:DF:EA:B1:99 -w /home/ wlan0mon”.





The first picture shows no wireless client is connected. The second one shows when there is wireless client connected. On the top right corner there is “WPA handshake: 00:1C:DF:EA:B1:99”, this means that the airodump-ng has successfully captured the four-way handshake.

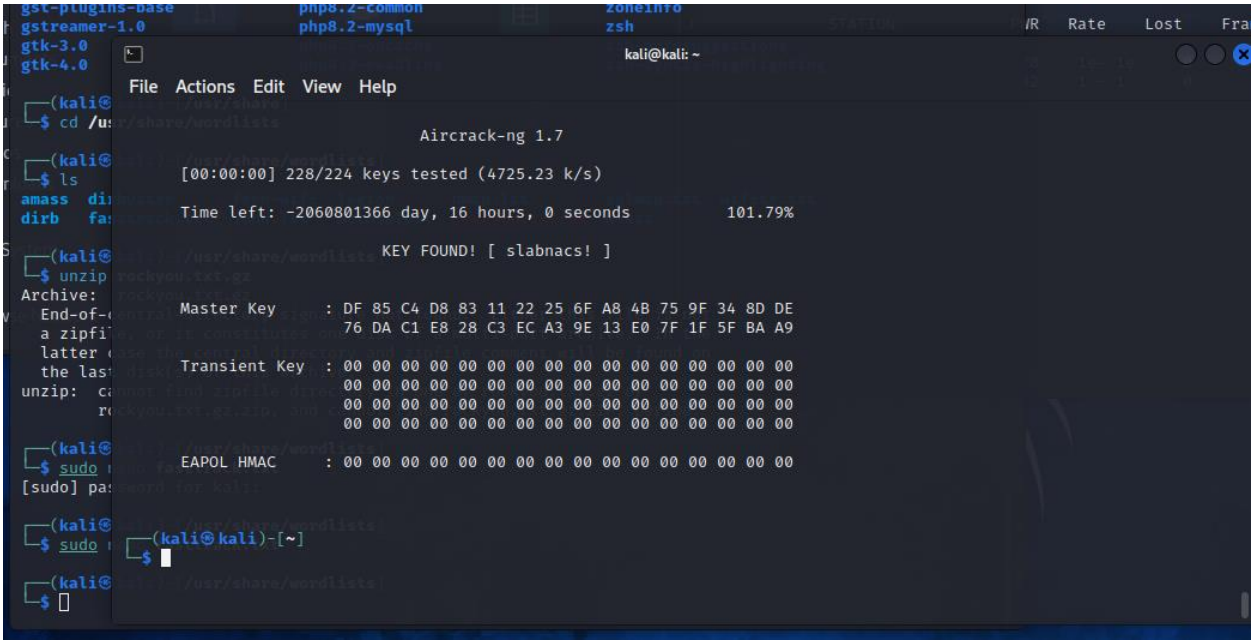
The next step is too deauthenticate the wireless client. The wireless client will then hopefully reauthenticate with the AP. The reauthentication is what generates the 4-way authentication handshake that I had to collect in order to break the WPA2 password. I used the command “airplay-ng -0 [Number of deauths to send] -a [MAC address] [Network interface]”.



After the deauthentication I had the file, which only needed to be cracked to see the password. The final step is to use aircrack-ng with a specific word file with a lot possible password.

```
┌──(kali㉿kali)-[~]
└─$ aircrack-ng -w /usr/share/wordlists/fasttrack.txt kali-01.cap
Reading packets, please wait...
Opening kali-01.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
```

After a little bit of waiting, I got the password:



Afterthoughts

Wireless hacking, also known as Wi-Fi hacking, is unauthorized access or manipulation of wireless networks. To prevent it, it is important to implement strong encryption, securing against rogue access points, addressing WPS vulnerabilities, preventing MAC address spoofing, educating users, monitoring for attacks, conducting regular security audits, and keeping all wireless devices and firmware up-to-date with the latest security patches are key considerations.

Reference:

Wikipedia contributors. (2023, April 7). *Wi-Fi Protected Access*. Wikipedia. https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

airmon-ng [Aircrack-ng]. (n.d.). https://www.aircrack-ng.org/doku.php?id=airmon-ng

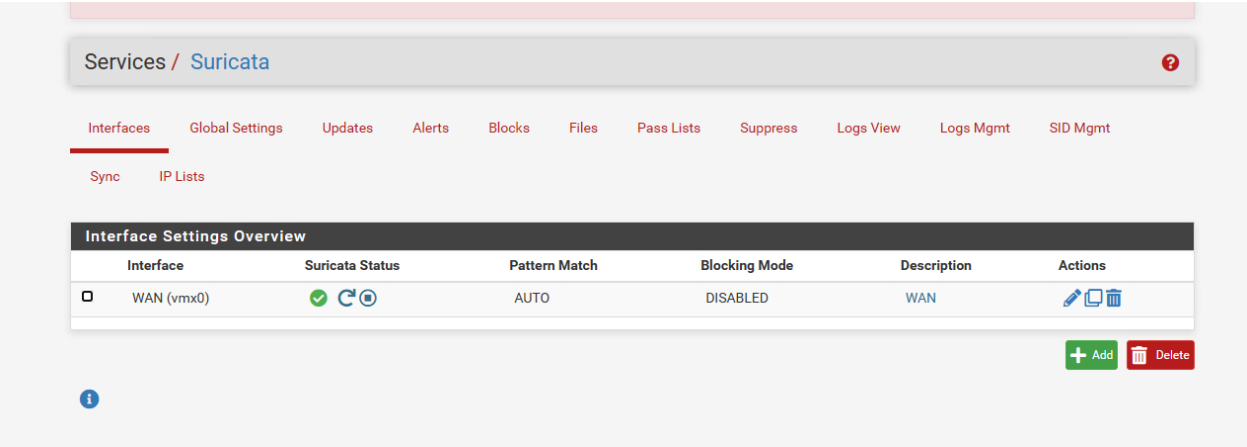
Aircrack-ng. (n.d.). https://www.aircrack-ng.org/

Network Intrusion Detection and Prevention (NIDS/IPS)

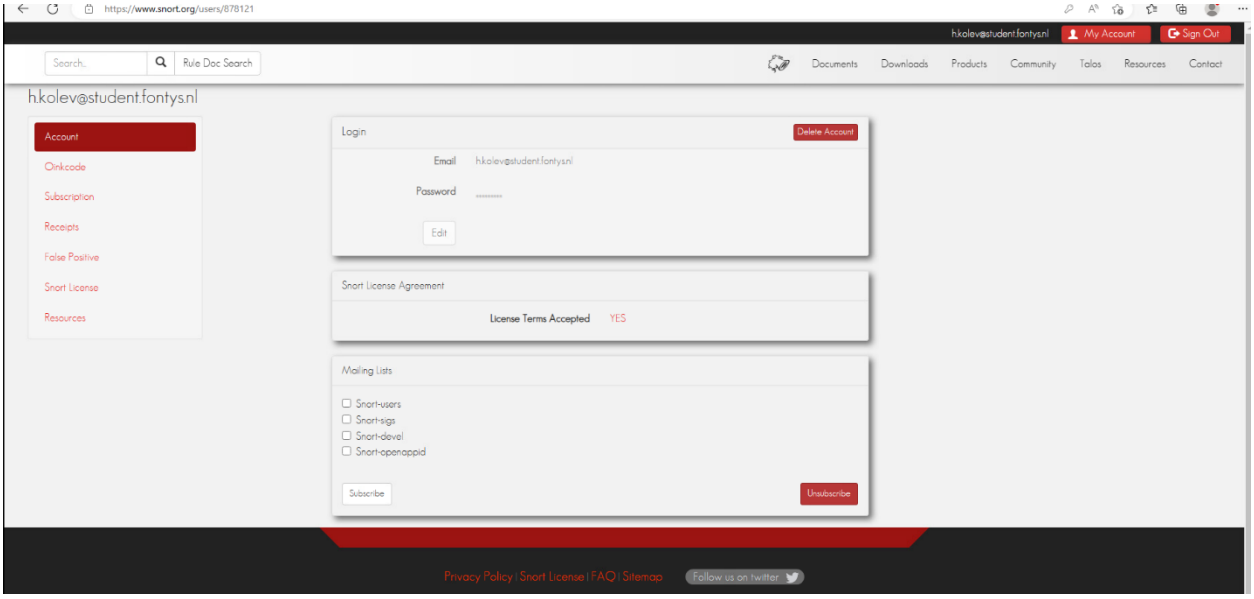
Network intrusion detection system (NIDS) is a security tool designed to monitor and detect suspicious activity on a network. NIDS works by analyzing network traffic and looking for patterns or behaviors that indicate an intrusion attempt, such as unusual network connections, traffic spikes, or patterns that match known attack signatures. It can detect a wide range of attacks including port scans, network probes, denial of service attacks, and malware infections.

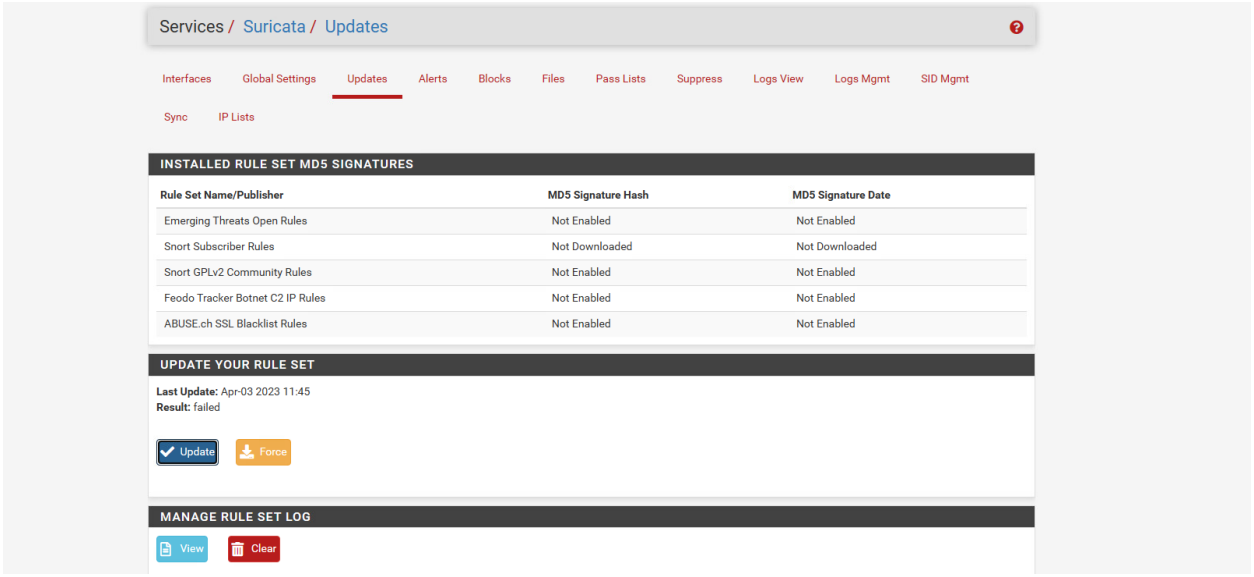
Add the Suricata IDS package

I have installed Suricata on my pfsense firewall. I made an account in snort and set up IDS interfaces

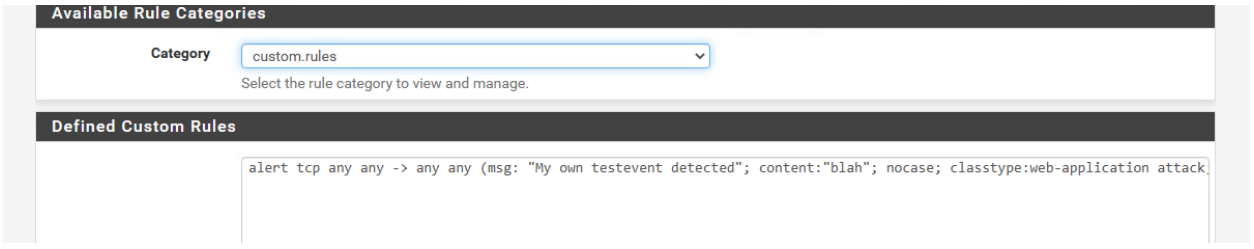


Adding SNORT:





And I add a custom rule:



It appears to be working.

the difference between ids and ips

IDS (Intrusion prevention system) flags upcoming attacks as potential threats and logs them.

IPS (intrusion prevention system) blocks upcoming malicious attacks

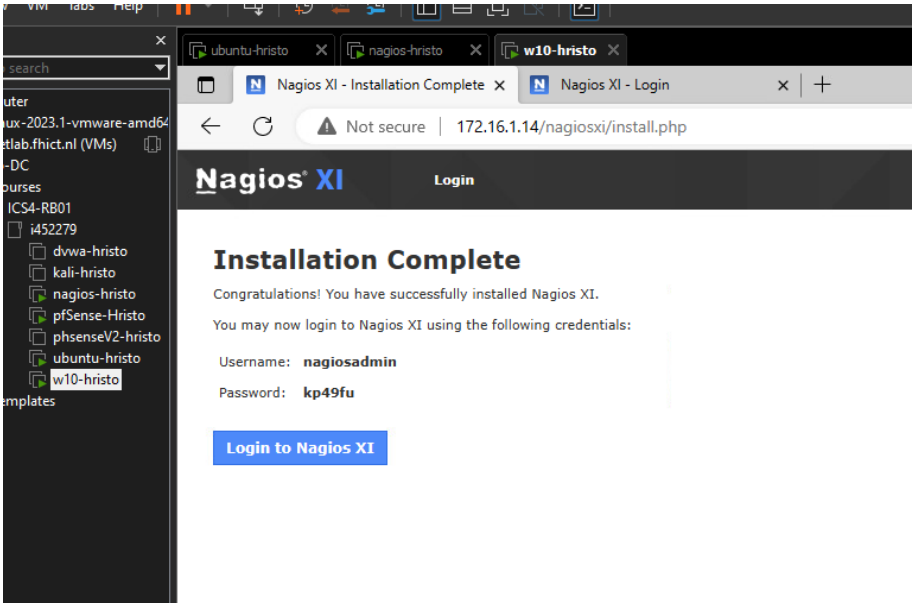
Afterthoughts

Network Intrusion Detection and Prevention Systems (NIDS/IPS) are critical components of a comprehensive network security strategy. They are designed to detect and prevent unauthorized access, malicious activities, and potential network-based attacks. Key considerations for NIDS/IPS security include deployment, signature-based detection, Behavioral/Anomaly-Based Detection, Real-Time Monitoring, Response and Prevention, Integration with Security Information and Event Management (SIEM). Proper deployment, configuration, tuning, real-time monitoring, response and prevention actions, integration with SIEM, regular updates and maintenance, and testing and validation are critical to ensuring the effectiveness of NIDS/IPS systems in protecting the network and project assets from network intrusions.

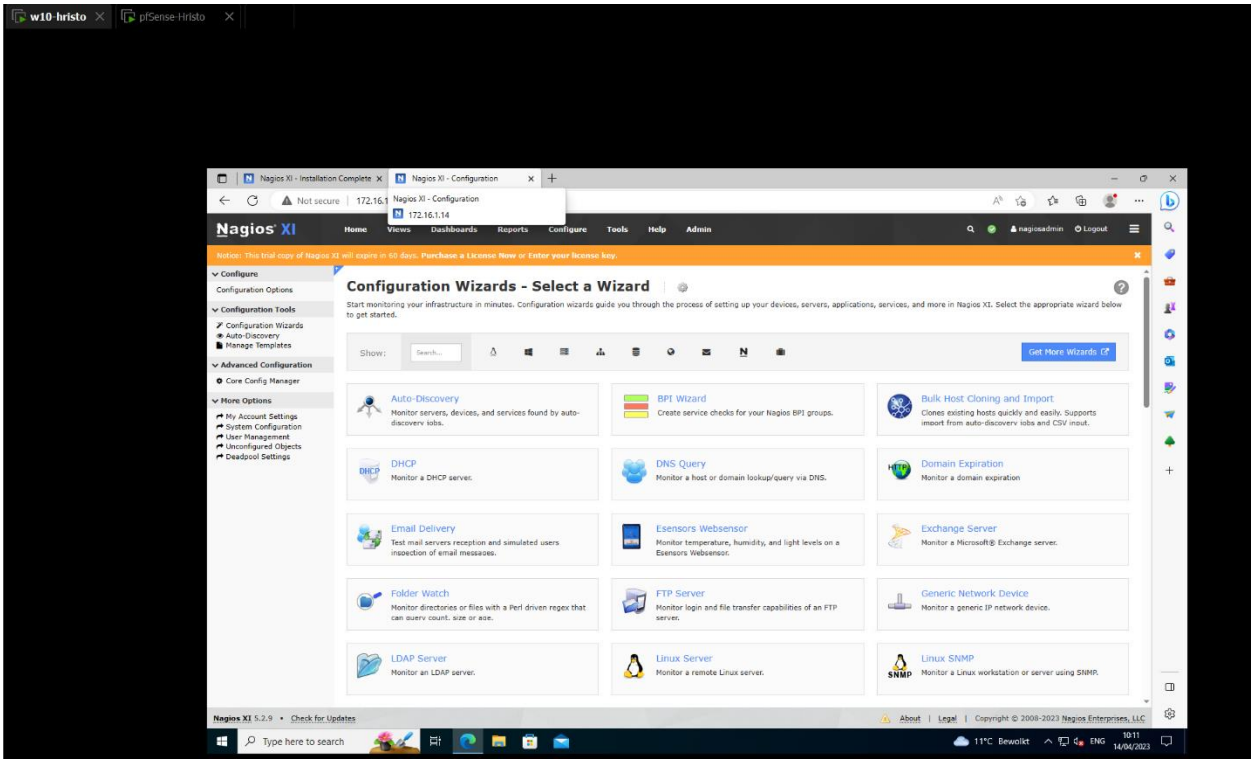
Security Concepts

IT Basic Monitoring

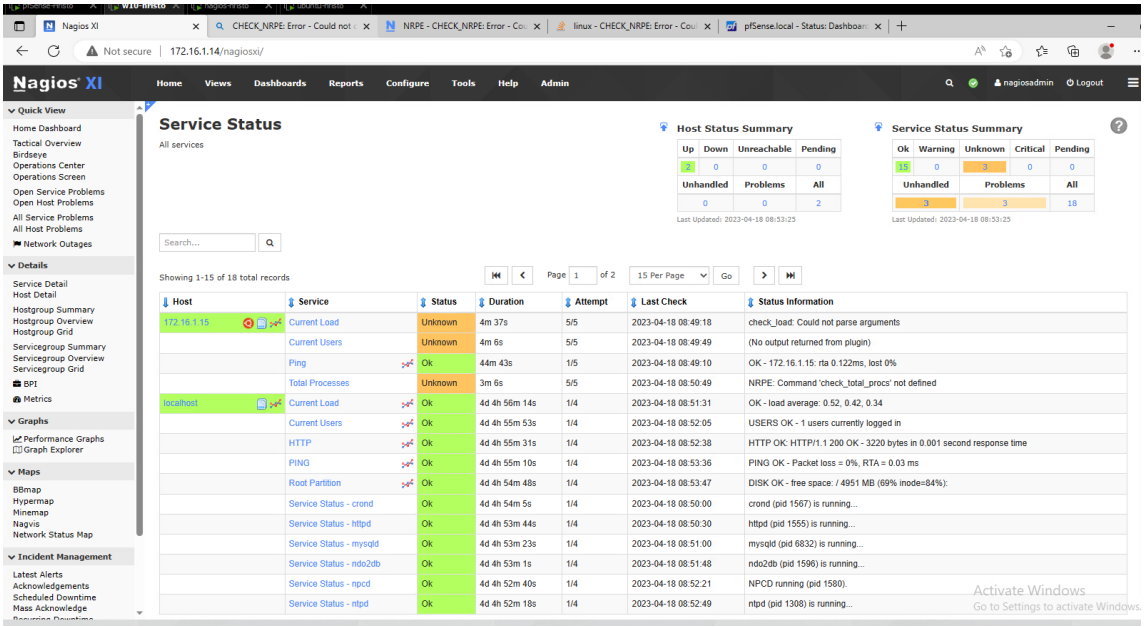
I installed the Nagios using the installation guide in Canvas. I installed it on PVLANA in my network.



When I logged in, I add the NRPE package.



I decided to monitor my Linux machine. When I install the Agent, I got this result:



Afterthoughts

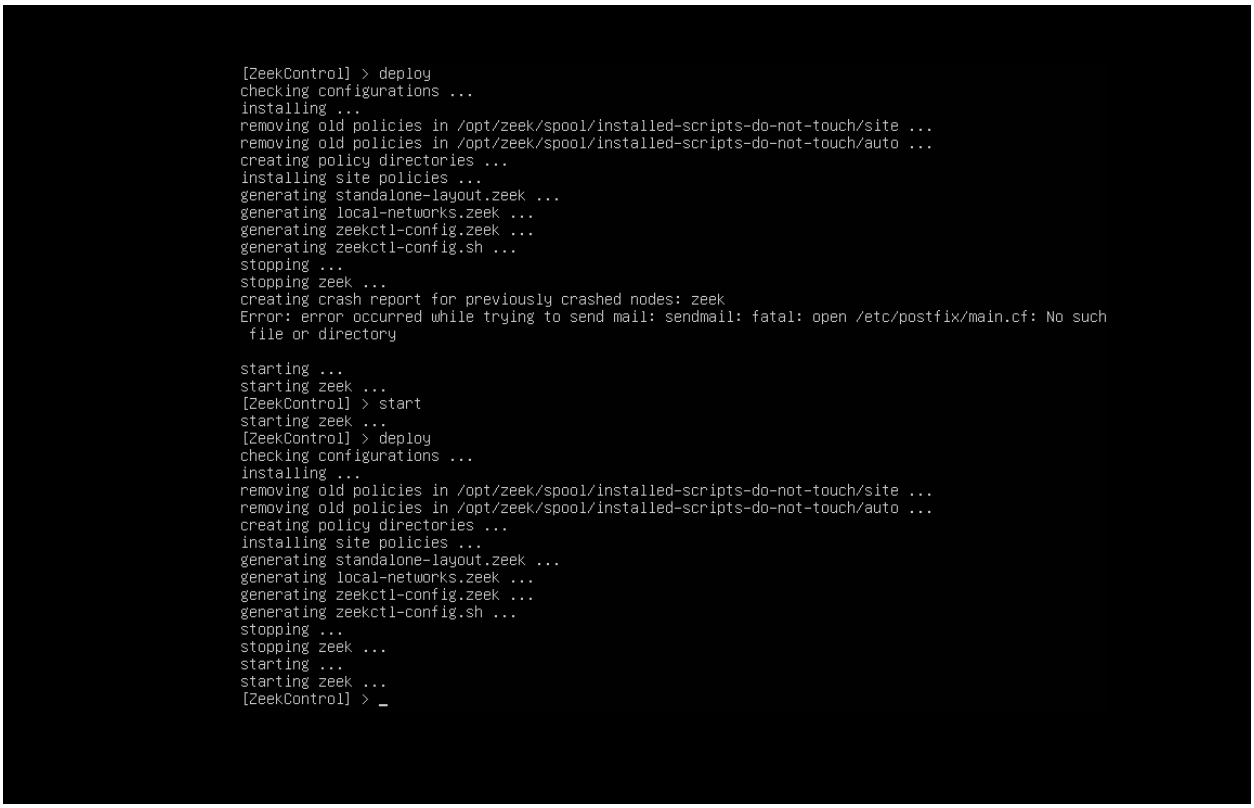
IT monitoring is an essential practice that involves the systematic collection, analysis, and interpretation of data related to the performance, availability, and security of IT systems and infrastructure. Key considerations for effective IT basic monitoring include system and network

health, SLA compliance, backup and disaster recovery monitoring, alerting and incident response, log monitoring, patch and vulnerability management, and documentation and reporting. Implementing an effective IT monitoring strategy can help identify and address IT issues proactively, minimize downtime, enhance security, and improve overall performance.

IT Security Monitoring

IT security monitoring refers to the process of constantly monitoring computer systems, networks.IT security monitoring typically involves collecting and analyzing data from various sources, such as security logs, network traffic, and system events. This data is then analyzed using security analytics tools and techniques to identify patterns, anomalies, and other indicators of a security threat.

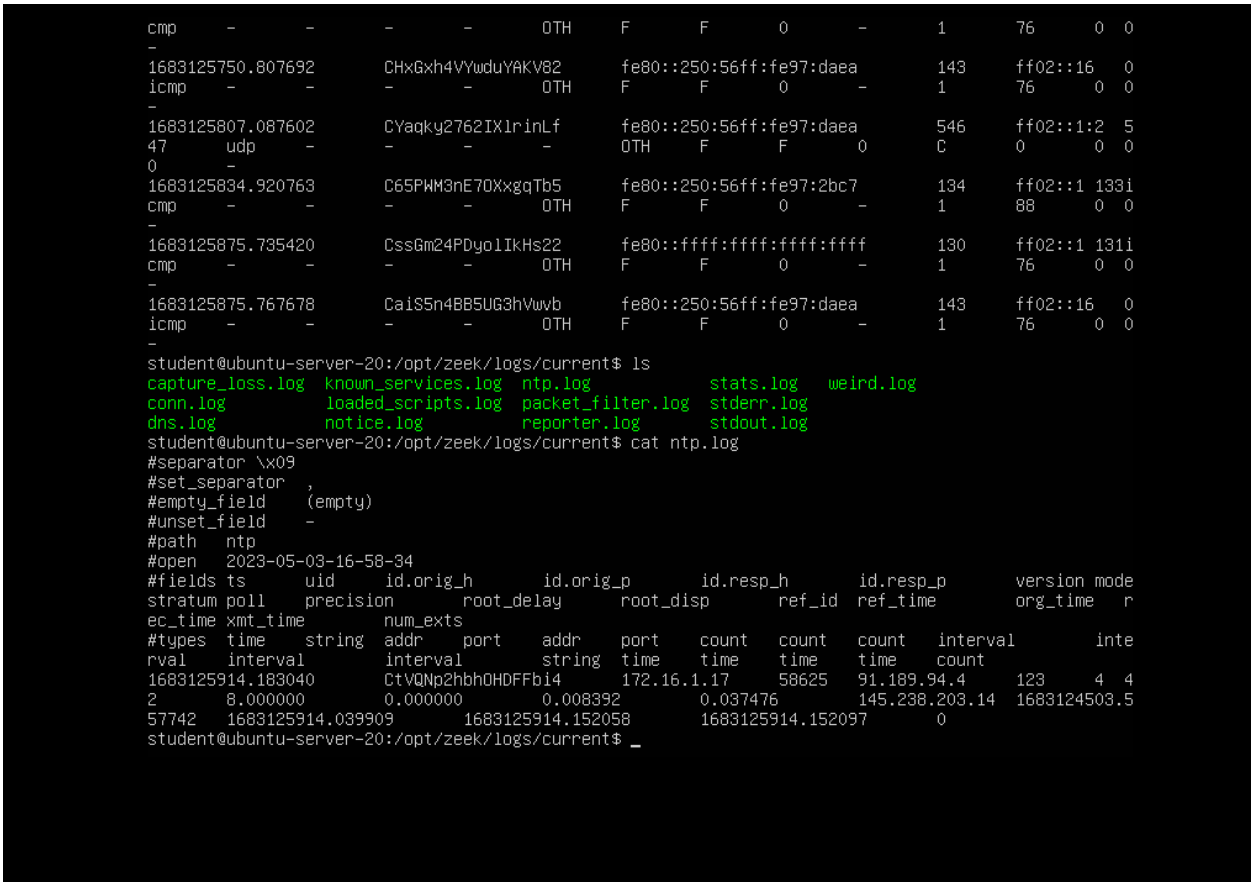
For this exercise I followed the Zeek instructions from the Canvas. After the installation I manage to start the tool.



When I started the tool I can access different log files to view the activity on the network in real time, allowing me to detect suspicious activity.

```
conn.log          loaded_scripts.log  packet_filter.log  stderr.log
dns.log           notice.log          reporter.log       stdout.log
student@ubuntu-server-20:/opt/zeek/logs/current$ cat conn.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2023-05-03-16-55-21
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   serv
ice     duration        orig_bytes      resp_bytes      conn_state      local_orig      local_resp m
issed_bytes     history orig_pkts       orig_ip_bytes   resp_pkts       resp_ip_bytes   tunnel_paren
ts
#types  time    string  addr    port    addr    port    enum    string  interval        count   coun
t       string  bool    bool    count   string  count   count   count   count   set[string]
1683125711.894145       CkOIP23cQ54FZ3Yxuk      172.16.1.17     45229   172.16.1.1      53      udpd
ns      0.000362        0       319     SHR     T       T       0       ^dC     0       0       2  3
75      -
1683125750.730778       CPPGnC2CfedOquQuu3      fe80::ffff:ffff:ffff:ffff       130     ff02::1 131i
cmp     -       -       -       -       OTH     F       F       0       -       1       76      0  0
-
1683125750.807692       CHxGxh4VYwduYAKV82      fe80::250:56ff:fe97:daea        143     ff02::16   0
icmp    -       -       -       -       OTH     F       F       0       -       1       76      0  0
-
1683125807.087602       CYaqky2762IX1rinLf      fe80::250:56ff:fe97:daea        546     ff02::1:2  5
47      udp     -       -       -       -       OTH     F       F       0       C       0       0  0
0       -
1683125834.920763       C65PWM3nE7OXxgqTb5      fe80::250:56ff:fe97:2bc7        134     ff02::1 133i
cmp     -       -       -       -       OTH     F       F       0       -       1       88      0  0
-
1683125875.735420       CssGm24PDyolIkHs22      fe80::ffff:ffff:ffff:ffff       130     ff02::1 131i
cmp     -       -       -       -       OTH     F       F       0       -       1       76      0  0
-
1683125875.767678       CaiS5n4BB5UG3hVuvb      fe80::250:56ff:fe97:daea        143     ff02::16   0
icmp    -       -       -       -       OTH     F       F       0       -       1       76      0  0
-
student@ubuntu-server-20:/opt/zeek/logs/current$ _
```

```
student@ubuntu-server-20:/opt/zeek/logs/current$ cat dns.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   dns
#open   2023-05-03-16-55-21
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   tran
s_id    rtt     query   qclass  qclass_name     qtype   qtype_name      rcode   rcode_name      AA T
C       RD      RA      Z       answers TTLs    rejected
#types  time    string  addr    port    addr    port    enum    count   interval        string  coun
t       string  count   string  count   string  bool    bool    bool    bool    count   vector[strin
g]      vector[interval]        bool
1683125711.894145       CkOIP23cQ54FZ3Yxuk      172.16.1.17     45229   172.16.1.1      53      udp6
2400    -       -       -       -       -       -       3       NXDOMAIN        F       F       F  F
0       -       -       F
1683125711.894507       CkOIP23cQ54FZ3Yxuk      172.16.1.17     45229   172.16.1.1      53      udp6
2400    -       -       -       -       -       -       3       NXDOMAIN        F       F       F  F
0       -       -       F
student@ubuntu-server-20:/opt/zeek/logs/current$ _
```



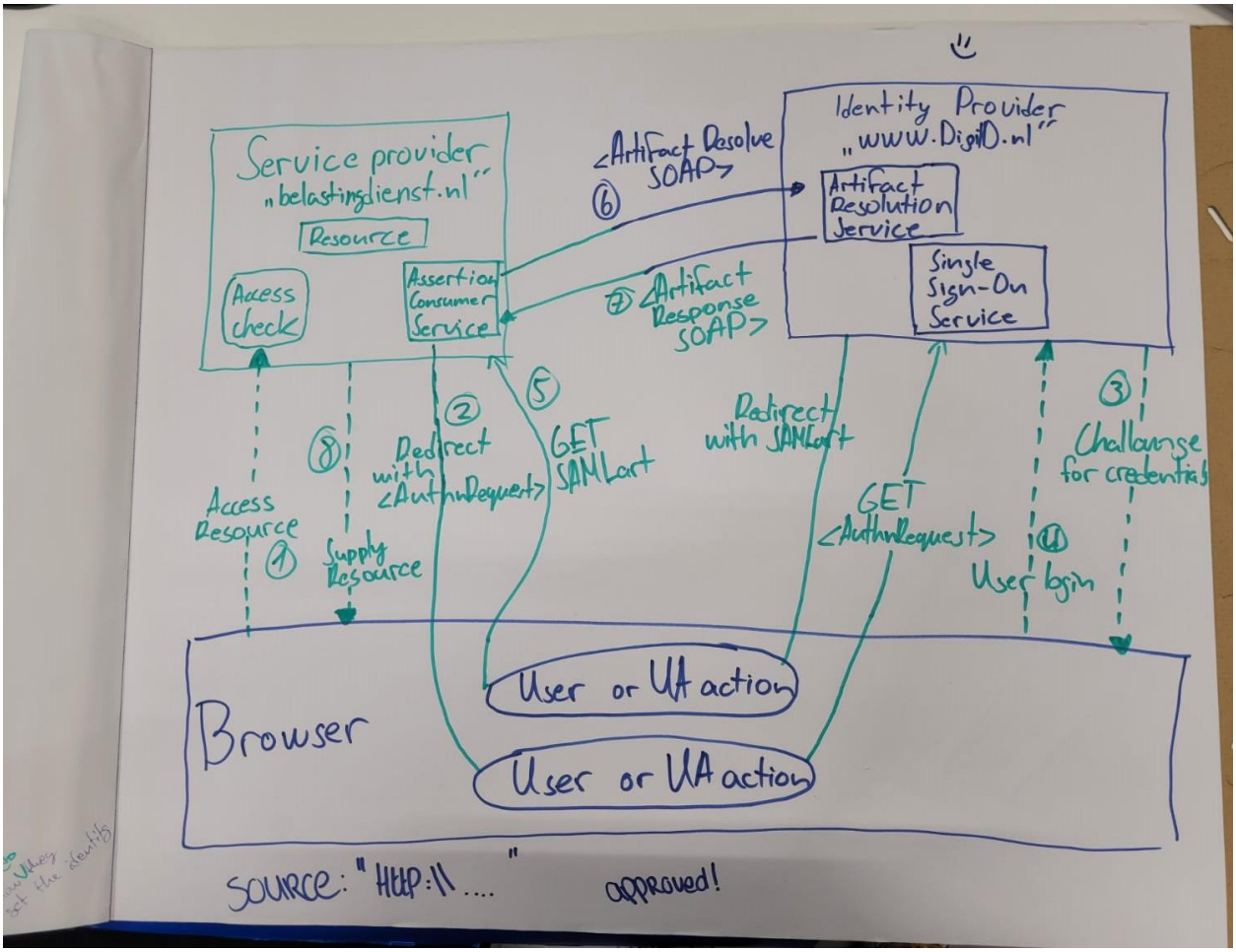
Afterthought

IT security monitoring involves actively monitoring and analyzing an organization's systems and network for potential security threats, vulnerabilities, and anomalies. To prevent attacks, it is important to ensure that the monitoring tools and systems are properly configured and up-to-date. This includes setting up alerts and notifications for potential security incidents and regularly reviewing logs and other security-related data. In a project, IT security monitoring can be used to improve the overall security of the system by identifying and addressing potential security threats in a timely manner.

Identity and Access Management

Design a role structure and policies for a small virtual company

We designed the DigiD Infrastructure. The diagram below contains the authentication steps that are made when an end user authenticates with a service provider.



Explanation of the steps in the figure:

Step 1: The end user with a browser as User Agent (UA) wants to use the service provider's web service.

Step 2: The service provider wants to establish the identity of the end user. The web service therefore forwards the end user to DigiD. The web service hereby asks for the minimum desired assurance level with which the end user must authenticate with DigiD.

Step 3 & 4: The end user is presented with the DigiD login screen and authenticates with one of the available logins means at the minimum desired assurance level.

Step 5: DigiD sends the end user back to the web service via a redirect. Here a meaningless Artifact generated by DigiD is sent along. This Artifact refers to the actual SAML message that is subsequently exchanged via the back channel in steps 6 and 7.

Step 6: The web service establishes a secure connection with DigiD via the back channel and sends an Artifact Resolve message containing the SAML Artifact.

Step 7: DigiD immediately replies with the Artifact Response message that belongs to the SAML Artifact. In this message, DigiD provides the Assertion, including the authentication result and, if authentication is successful, the BSN (sectoral number) of the end user.

Step 8: The service provider processes the Assertion from the DigiD authentication message, thus establishing the identity of the end user. Only with successful authentication will the end user gain access to the service provider's web service.

Reference:

Koppelvlakspecificatie DigiD SAML Authenticatie | Logius. (n.d.). https://www.logius.nl/domeinen/toegang/digid/documentatie/koppelvlakspecificatie-digid-saml-authenticatie

Password Cracking

The passwords are stored in a database or on a disk.

There are several ways companies to store passwords

1. Plain text
2. Encrypted
3. Hash

Plain text- This is the most dangerous way of storing passwords. If hackers breach the database, they can see the passwords of all users.

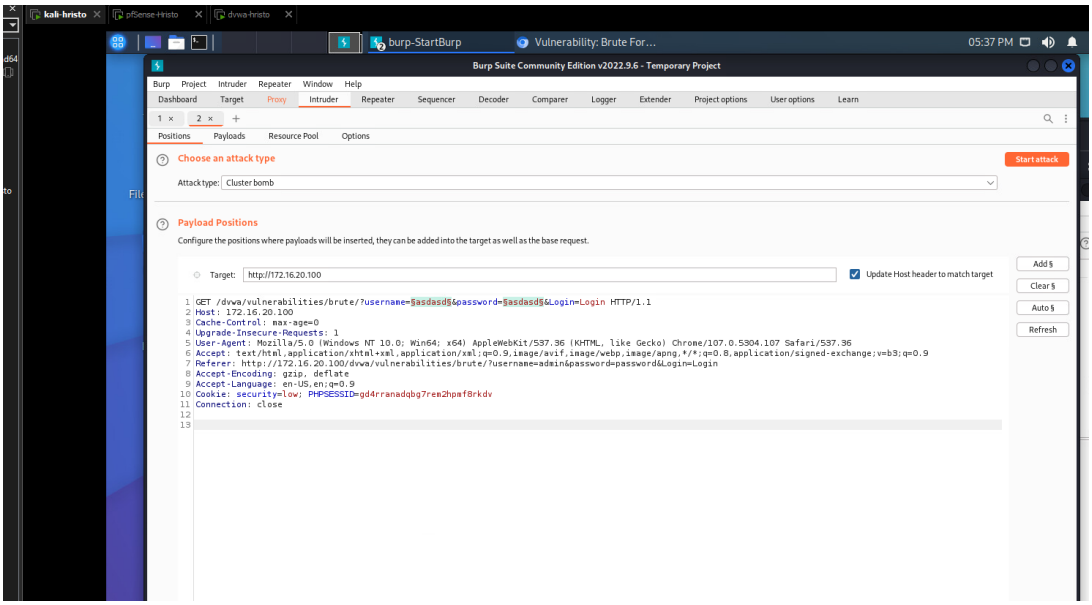
Encryption- Take the password from the user and before you store them encrypt them with an encryption key. This will prevent the hacker from obtaining the passwords. Underneath the encryption layer is still a plain text password, so if an attacker manages to steal the encryption key as well, he can unlock all passwords.

Hash- This is the process of transforming any given key or a string of characters into another value. This is usually represented by a shorter, fixed-length value or key that represents and makes it easier to find or employ the original string.

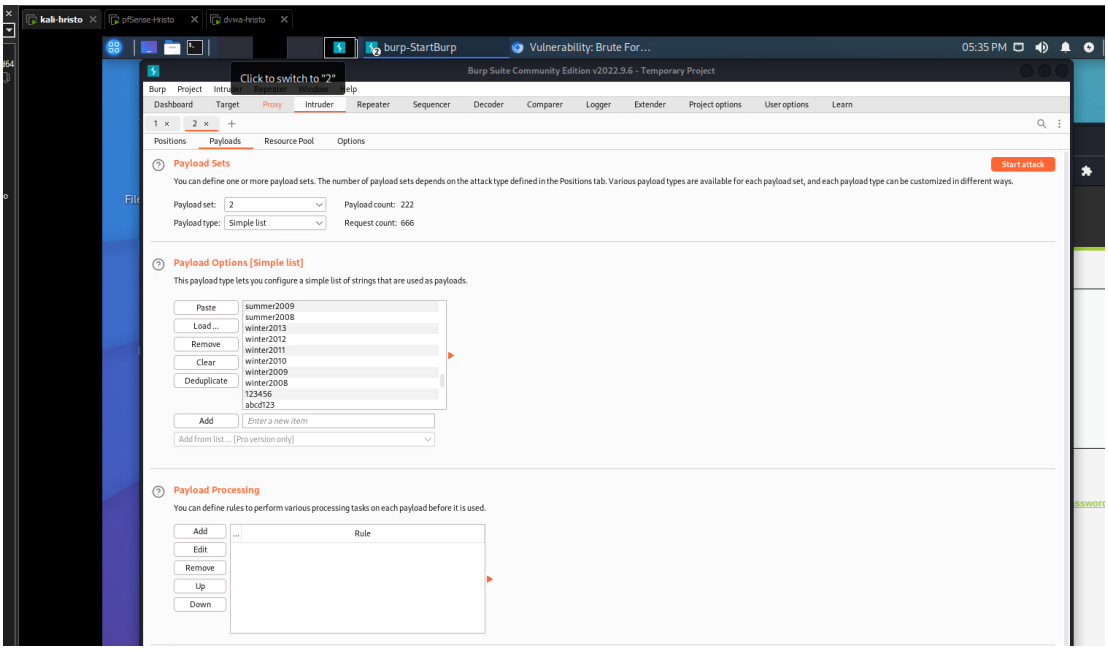
Salt- adding random characters to the data.

DVWA Brute force password hacking

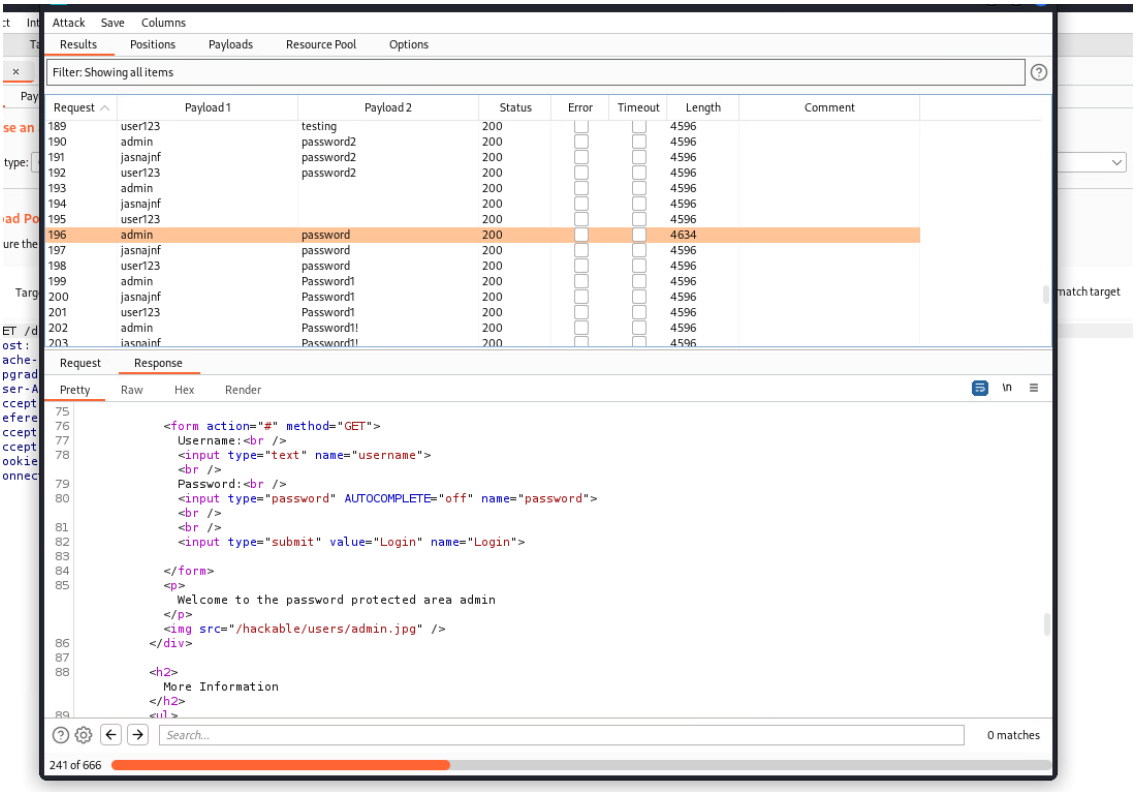
First thing to do is to intercept the “http-get-form” request using BurpSuite tool and send it to Intruder.



There I select the variables that I need for the payload. On the first payload set I added list with different username and on the second- list with passwords.



When done that I start the attack.



After several minutes of testing, I got the correct credentials. As you can see every status is the same, in my case in 200(OK) and the ‘Length’ is the same (4596). Only on the correct credentials the ‘Length’ is longer.

Afterthoughts

Brute force attacks, also known as password cracking attacks, are used by malicious actors to gain unauthorized access to user accounts or systems by systematically trying all possible combinations oof passwords until the correct one is found. To protect against these attacks, two-factor authentication (2FA), password complexity, monitoring and alerting (detect and alert on multiple failed logins attempts from the same IP address or user account) are key considerations.

Security Incident Management

The main goal of the incident management process is to restore a normal service operation as quickly as possible and to minimize the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

> Think about a security incident that could happen in your 'basic knowledge company'. Perform a triage and work out a complete response as it should be done in your company. Try to include realistic roles/employees from your company in the process where needed

The company name is NetTicket and they are one of the leading online sites for selling tickets for sports events. Through their website, user with personal account can see upcoming sport events and buy a ticket for them. The security incident is a brute force attack and the hacker gained access to some customer's accounts. He managed to access important personal information.

This type of attacks is very crucial and the impact can be big. This security incident requires urgent measures and the problem has to be solved as soon as possible. The main people, that are responsible, are the Cyber Security team and more specifically the people who are protecting the personal accounts. They have to go in details about the cyber-attack(from where this attack came from, IP addresses, check the failed attempts in log files, etc.). After the gathering and analyzing the needed information, the first thing to do is to inform the customer that his account was damaged and tell him the possible impact. After this the company should inform the police about the cybercrime.

The Cyber Security team has to improve the security of the accounts to avoid future attacks. Possible solutions for this scenario are:

1. Limit the login attempts – by limiting the data entry, you are preventing hacker attacks.
2. Usage of 2 Factor Authenticator – It uses 2 steps process to login. Most of the 2FA works with fingerprint, face recognition, SMS code, emails, Authenticator apps.
3. Use CAPTCHA – This helps distinguish between spam computers and real ones.

IT System Hardening

Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vectors and condensing the system's attack surface.

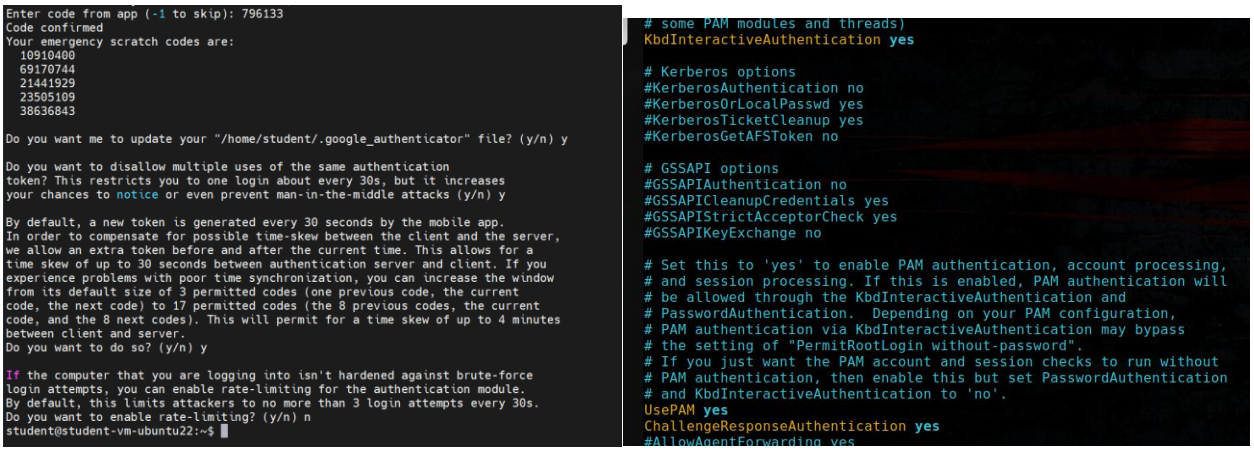
Is your laptop/PC hardened?

I am on a Windows 11 machine. I am installing every windows patch on the same day it comes out. Since it is a Windows machine it cannot be pinged on any network. I've installed anti-virus system that detects everything on internet and always asks me for permission and alerts me for phishing sites, ARP spoofing, and other cyber threats.

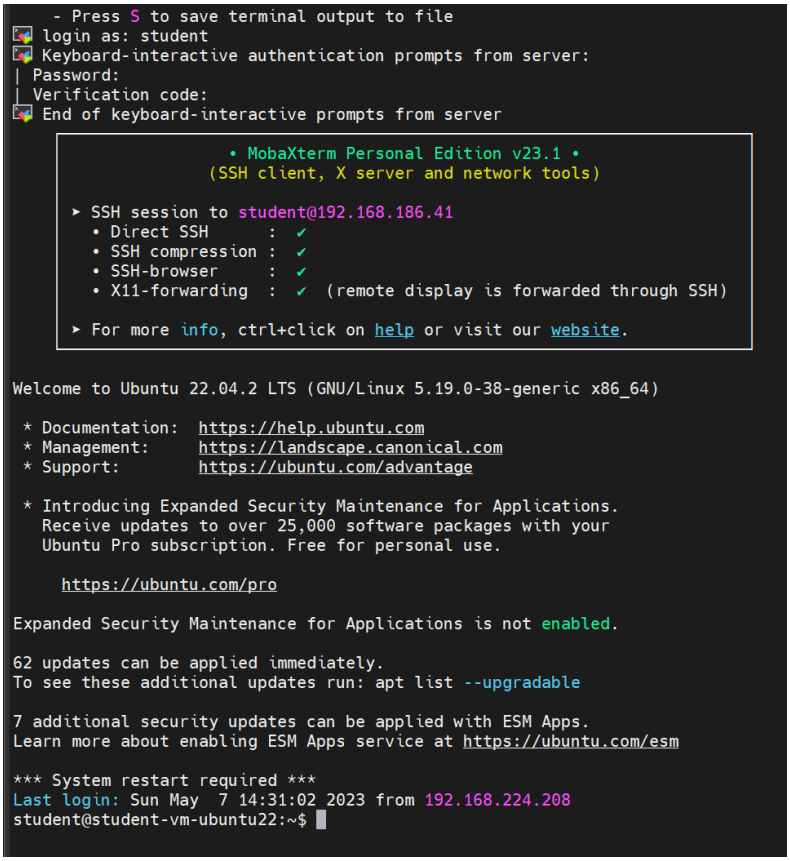
Configure two-factor authentication using the google authenticator

I decided to configure 2FA with Microsoft Authenticator app on my Ubuntu machine. First of all, I had to download and install the google authenticator on the machine. Then I connect Microsoft Authenticator application on my phone with the ubuntu server via QR code.

After the connection is made, I can start the application and configure it.



After changing several files, I was able to connect to the machine with two factor authentication.



Afterthoughts

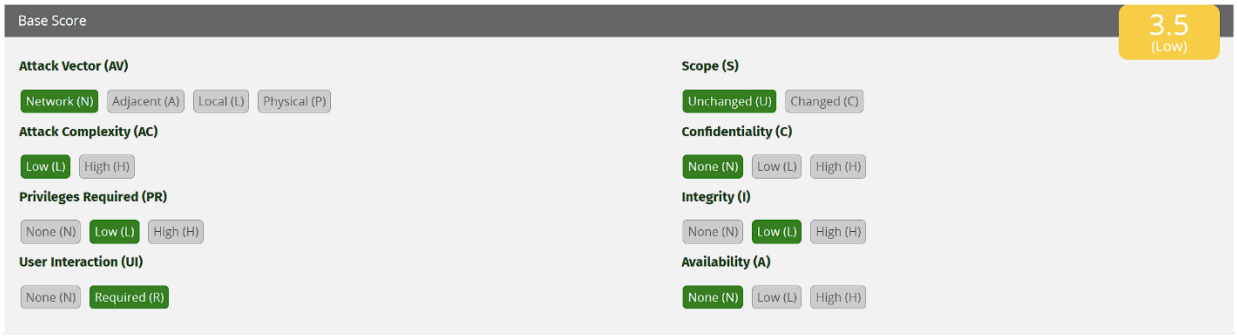
Two-factor authentication (2FA) is a security process that requires users to provide two different forms of authentication to access a system, account, or application. To prevent attacks on 2FA, it is important to ensure that the second form of authentication is not easily guessable or hackable. It is also important to regularly update and strengthen password policies, as well as to educate users on the importance of maintaining the security of their devices and accounts. In project, 2FA can be implemented to add an extra layer of security to user accounts, especially for those with access to sensitive information, preventing data breaches.

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.

Vulnerability: Netflix XSS vulnerability

There were XSS vulnerabilities discovered and reported in the Dispatch application, affecting name and description parameters of Incident Priority, Incident Type, Tag Type, and Incident Filter. This vulnerability can be exploited by an authenticated user.


Base Score
3.5
(Low)
Attack Vector (AV)
Network (N)
Adjacent (A)
Local (L)
Physical (P)
Attack Complexity (AC)
Low (L)
High (H)
Privileges Required (PR)
None (N)
Low (L)
High (H)
User Interaction (UI)
None (N)
Required (R)
Scope (S)
Unchanged (U)
Changed (C)
Confidentiality (C)
None (N)
Low (L)
High (H)
Integrity (I)
None (N)
Low (L)
High (H)
Availability (A)
None (N)
Low (L)
High (H)

Conclusion

During this whole semester, I learnt a lot about the cyber security and its topics. Every workshop was very useful and helpful to me. The teachers explained and demonstrated something from every topic. For me it was challenging this semester because I have software background and most of my groupmates have infrastructure background and for them is a little bit easier, but with hard work and with a lot of help from their side, I thing I managed to keep up with them and manage to finish this BOK and acquire the given knowledge during the lectures. I am happy from the outcome that I am right now. I think I will continue my studies in the security profile that Fontys provides in their curriculum and I ma planning to continue to acquire new knowledge in this field.