**Body of Knowledge (BOK)**

Mohammed Nasser Alshukaili.

ICT, Fontys University of Applied Sciences.

Cyber Security, Semester 4.

September 2022

Table of Content

[INTRODUCTION 3](#_Toc114154854)

[IT Background 3](#_Toc114154855)

[(BOK) Web Application Security (week 1-4) 4](#_Toc114154856)

[Exercises & Challenges 5](#_Toc114154857)

[Lesson 1.3 5](#_Toc114154858)

[Ransomware 5](#_Toc114154859)

[Phishing 6](#_Toc114154860)

[Lesson 2.2 7](#_Toc114154861)

[Host Intrusion Detection and Prevention System (HIDS) 7](#_Toc114154862)

[DVWA (Damn Vulnerable Web Application) 13](#_Toc114154863)

[Path Traversal 13](#_Toc114154864)

[Brute Force 13](#_Toc114154865)

[SQL injection 18](#_Toc114154866)

[Command Injection 24](#_Toc114154867)

[(BOK) Network Security (week 5-8) 28](#_Toc114154868)

[(BOK) Security Concepts (week 9-10) 28](#_Toc114154869)

[References 29](#_Toc114154870)

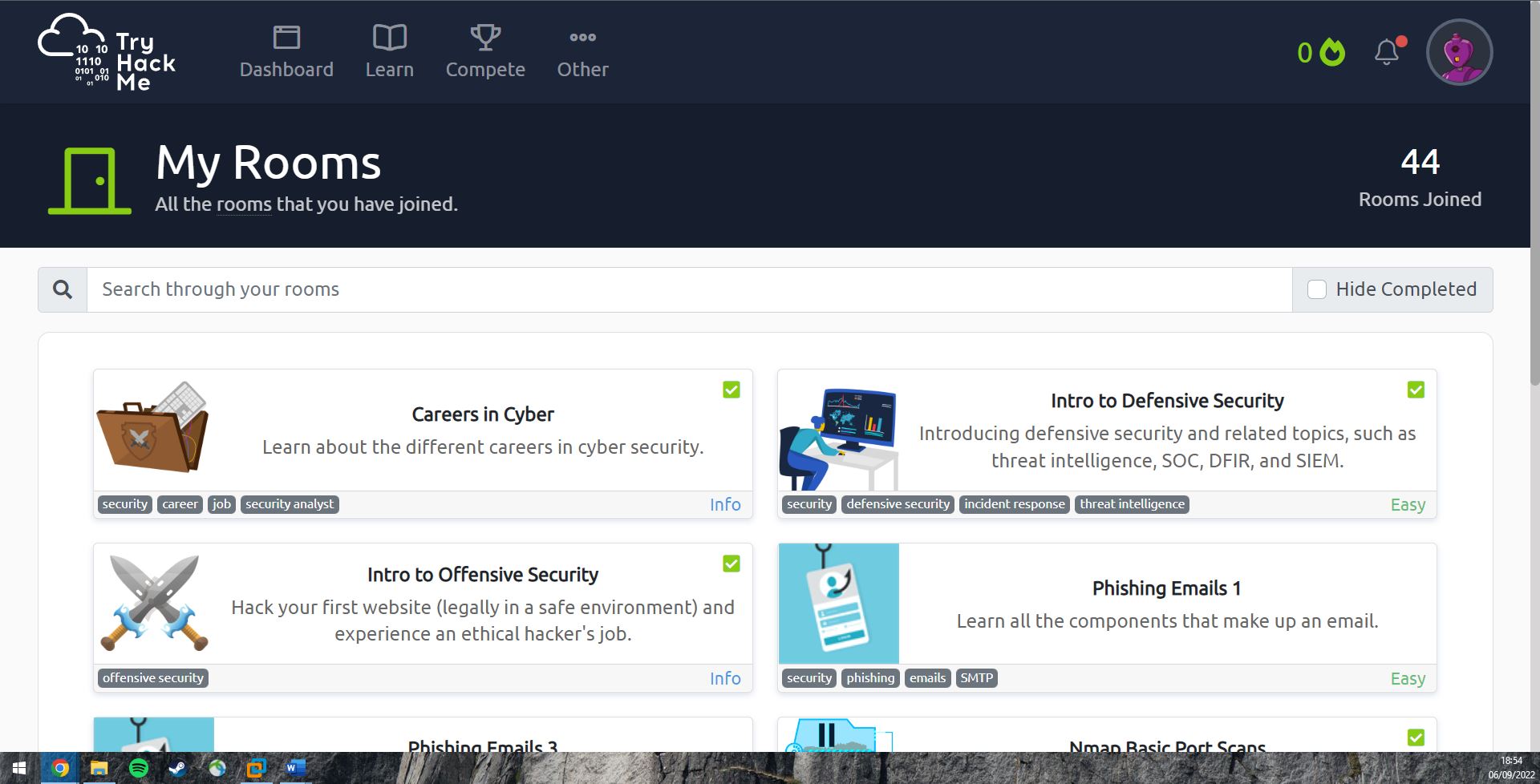
# INTRODUCTION

This report will take you through my learning process and semester progress for the Fontys, ICT, Cyber Security (S4) course.

My name is Mohammed Alshukaili. Although I come from media design background, my passion is to study cyber security. I consider myself an absolute beginner in this field. I will do whatever it takes to become a good student throughout the whole semester.

# IT Background

I only studied infrastructure engineering for 10 weeks in my first semester at Fontys. I felt like this was not going to be enough to become at a high-level student. Therefore, I decided to invest all my summer breaks studying new things that are related to infrastructure.

For instance, I subscribed to [www.tryhackme.com](http://www.tryhackme.com), a website that provides a huge amount of IT courses. I finished all the fundamentals for Linux, windows, and online databases. 

This picture shows some of the rooms that I enrolled for. I finished most of them with so much information gained.

I also like to learn by watching sometimes. I am subscribed to so many IT YouTube channels that provide basics for the IT industry. Some of my favorite YouTube channels are

* <https://www.youtube.com/c/PowerCertAnimatedVideos>
* <https://www.youtube.com/c/H>

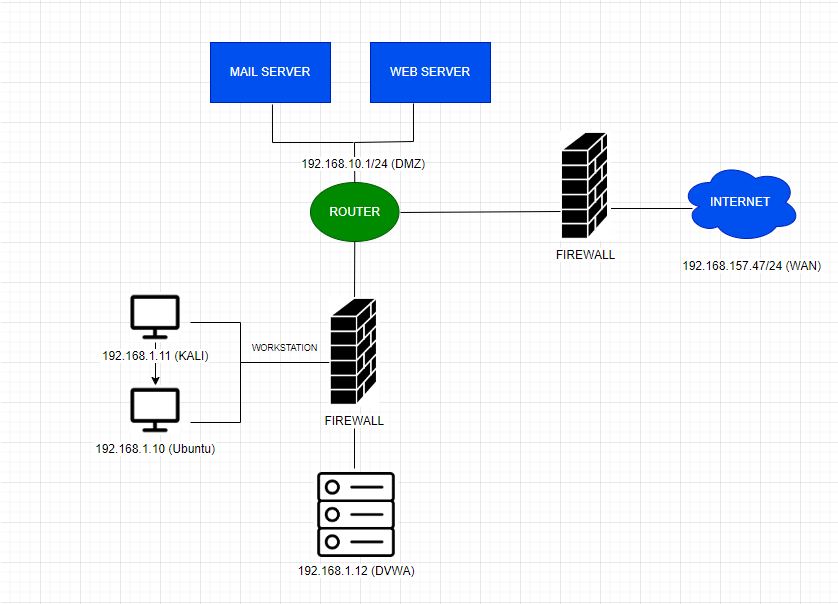
What I realized after all the tutorials that I have been to is that I prefer reading rather than watching tutorials. As the visual tutorials usually do not give me the chance to do things myself. On the other side, services like TryHackMe, Fontys are more practical that I found myself enjoy it more.

# (BOK) Web Application Security (week 1-4)

First day was a refresher to warm up ourselves. We made groups and competed by getting more points. The website name was picoCTF that gives you points by solving technical problems. The more you solve the more your group gets.

The second day, I attended the networking refresh. We learned about vSphere and how to set up a local virtual network. I thought that we would need to borrow some routers and devices to set up local network. However, the VLAN concept really changed the way I see internet. I managed to design a local network that includes 2 firewalls, workstation, DMZ, and the WAN to access the internet.

Here is a picture of my simple design:



I had to learn pfSense to set up this network and some of Docker basics.

Last class of the week, we had a theory about security and the different types of attacks.

## Exercises & Challenges

### Lesson 1.3

Task: To get a better understanding of these threats and attacks find articles on internet about any malware.

### Ransomware

Ransomware is one of the most popular cyber-attacks around the world. It is used to damage as many systems as possible. It encrypts the data in the infected system, this encourages the attacker to ask for money to decrypt the data. This malware spreads rapidly by itself without needing an attacker to manage it. Nobody can expect how fast it would spread to other systems.

#### WannaCry Attack

On May 12, 2017, the UK detected a ransomware called Wanacrypt0r. It affected the hospitals in the UK. After that, it went across the globe, infecting thousands of systems in at least 150 countries.

What did the attacker want?

The attacker promised to decrypt the data after receiving 300$ in Bitcoin. The hackers usually tend to use Bitcoin to get the money, to prevent the banks and governments to trace the money transfers.

What did the attacker damage?

The attack spread rapidly. It infected so many sectors. These included:

* Healthcare
* Emergency
* Security
* Telecom
* Gas
* Petrol
* Automotive
* Education
* Advertising

Who was responsible for WannaCry?

The United States officially blames North Korea for this attack.

### Phishing

Phishing is one of the social engineering methods to conduct an attack.

Social engineering is a term used to describe the attacks that take place by tricking the human to do something that leads to a vulnerability. It is when the attacker aims to trick the user to click on a malicious link.

Phishing types:

* **General Phishing** is a simple attack where the target can be anybody that uses popular services like PayPal, Amazon, Steam, etc.
* **Spearphishing** targets small group. However, that group might have security experience because they know that they can be targeted anytime.
* **Whaling** is so specific that it only targets the big names in a company. Well designed and crafted emails are being used for in this type.

Let us take a deep look at the general phishing type which is the most popular.

1. The attacker sends out an email that contains a malicious code.
2. The user (victim) sees the email and thinks that they should log in and do something about it.
3. The website retrieves the user credentials and forward them to the attacker.
4. The attacker receives the credentials and access the site, thus taking over the victims’ accounts.

How to identify phishing emails?

* The users’ names are replaced with something like “Dear customer”
* The link in the email looks almost exactly like a trusted website but one letter was changed for example.
* When hovering on the link in the email, something suspicious appears on the left bottom instead of the trusted website.

Now that we know how the hacker might get to our system, how can we prevent this from happening? Here are some good steps to stay safe:

* Delete every suspicious email that you detect.
* Report any email that looks harmful.
* Do not open attachments from untrusted emails.
* Do not click on any image in the email as it might be a hidden button that sends you to the attacker’s website.
* If you work from home, make sure to set up a save network and pay attention to all the emails received.

### Lesson 2.2

### Host Intrusion Detection and Prevention System (HIDS)

1. Explain the difference between NIDS and HIDS and IDS and IPS, and the meaning and relevance for your company.
2. Select (open source) HIDS software and deploy it in your network. Show that it triggers on (simulated) malicious activity.
3. Intrusion Detection System (IDS) is a method that strengthen the security against cyber crimes. It detects malicious activities entering/leaving the network and start sending alerts to do something about it.

Intrusion Preventing System (IPS) could do both, alerting and blocking the intruder from getting what they came for.

Host Intrusion Detection System (HIDS)

HIDS only monitors one device in a network. It keeps waiting for any malicious activity on a specific device, then sending alerts.

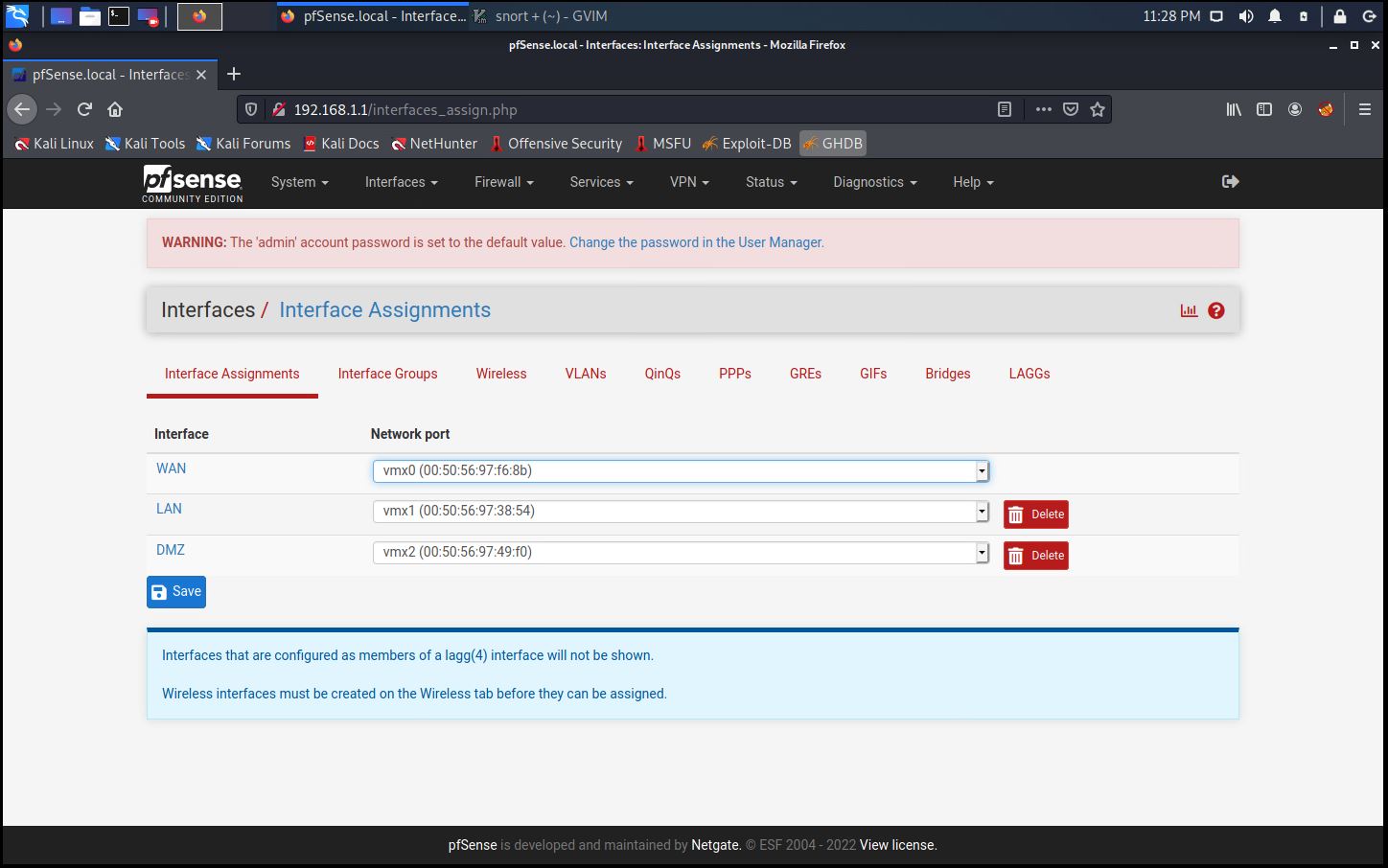
NIDS monitors a network segment. It keeps track of all the data entering and leaving a specific network.

Why would you need to use HIDS when you can just use NIDS to monitor all the devices in the network?

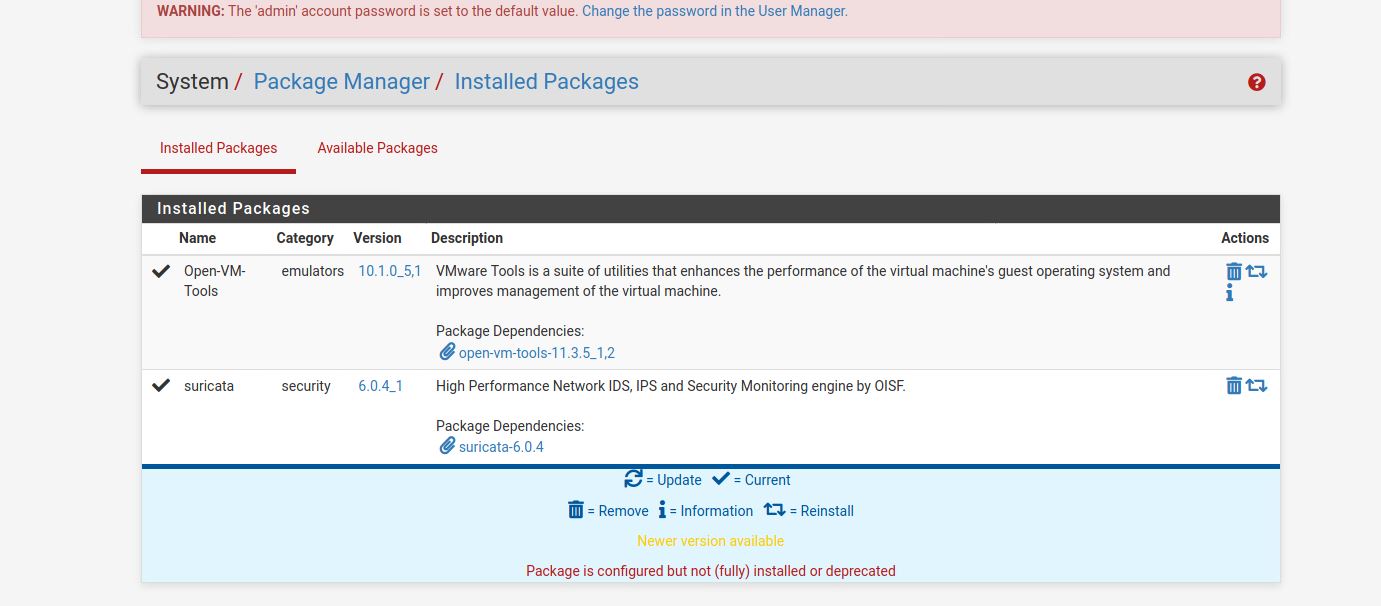
-Well, the intruder might find another path to a specific device and use that path to send malicious packets. Therefore, when having a very private device, HIDS is a better option.

1. Suricata

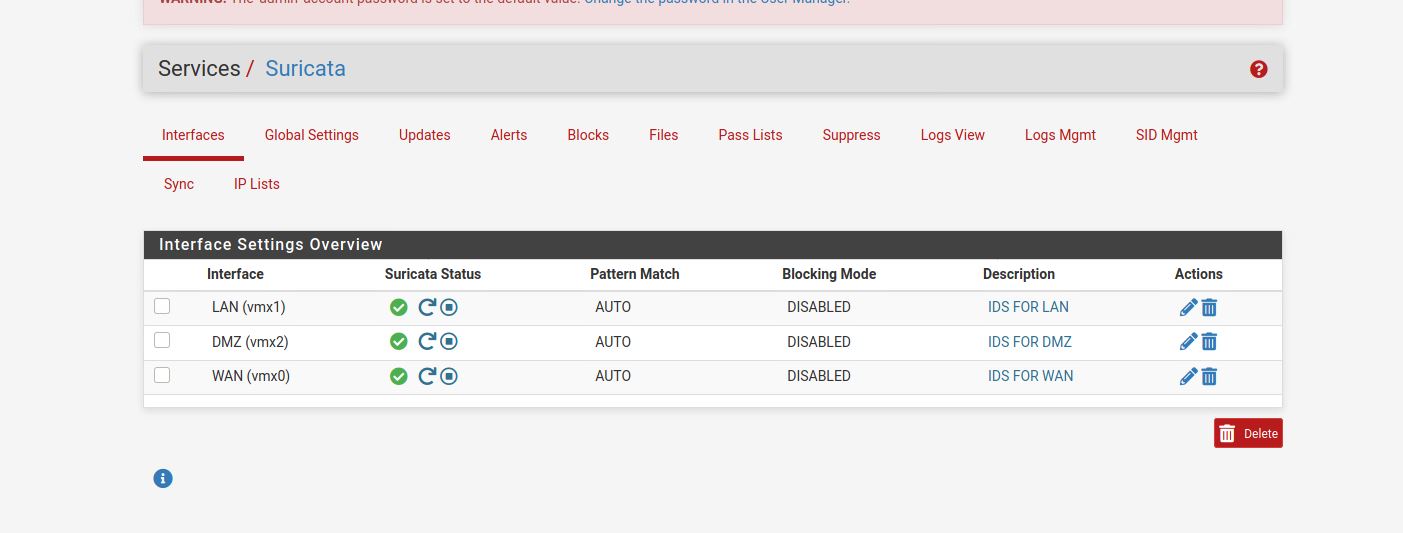
For network-IDS I decided to use Suricata package as it is available in pfSense and free to install.



In my pfSense, I set up 3 interfaces for my local network. I also set up 2 wirefalls. The next step is setting up IDS. I could find the Suricata package in pfSense-System-Package Manager- Available Packages. Then I searched for Suricata and I installed it.

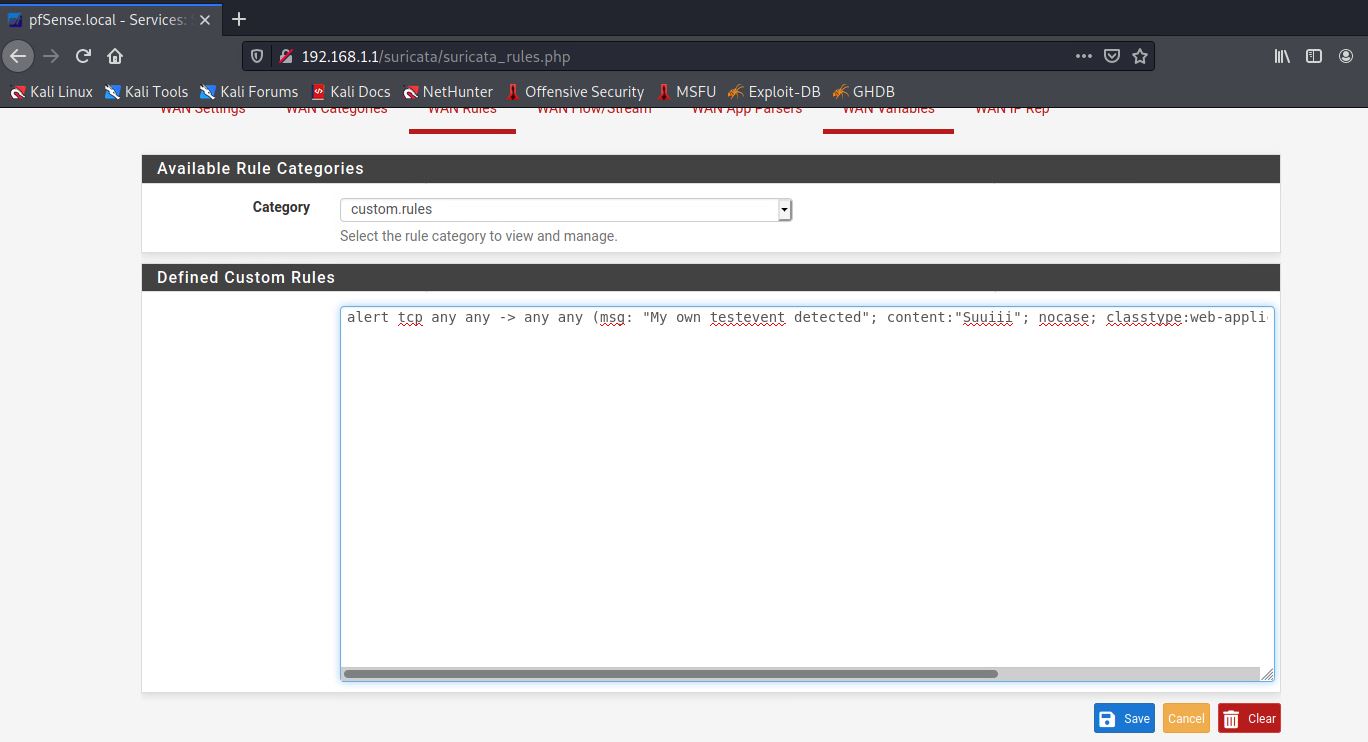


I setup 3 IDS for every interface. However, It says disabled so I still need to enable it.

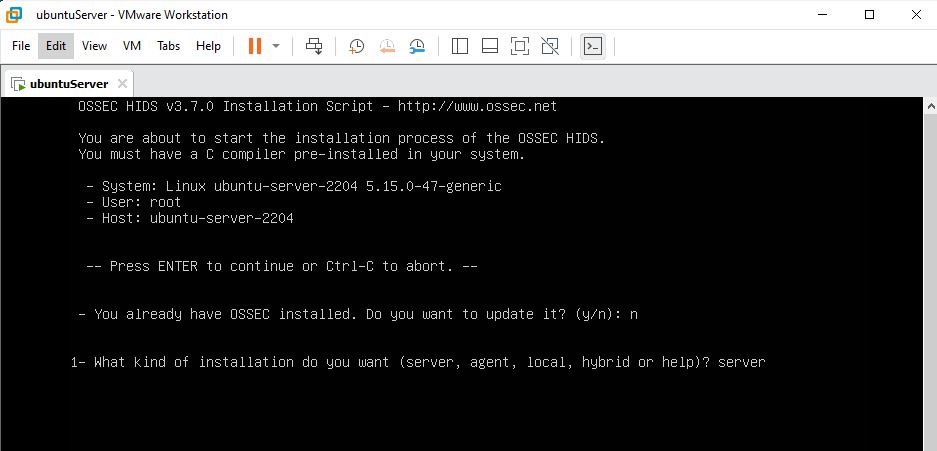


To set rules for the WAN IDS for example, we need to go to Services / Suricata / WAN Interface Settings / WAN – Categories. Then we can check all the rules that we want for the interface’s IDS.

We also can set up custom rules in WAN Rules section



* Setting up OSSEC:

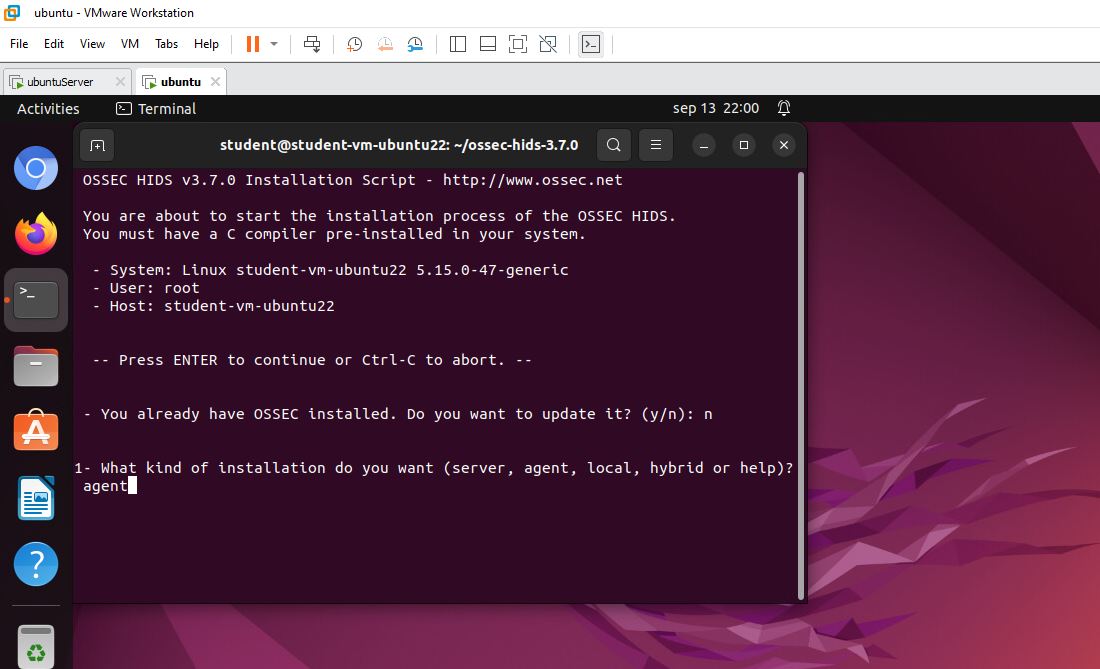


First, I git cloned the latest version of OSSEC from <https://github.com/ossec/ossec-hids>

Then, I unzip the file then I executed the file named install.sh using sudo.

The picture above shows that I am installing the server version because that is my server interface.

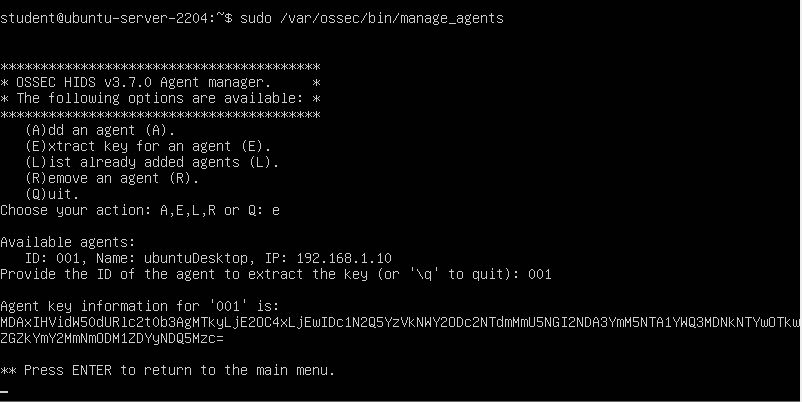
This server will need agents. Therefore, I will redo the same steps on my Ubuntu interface. However, when installing, I should install the agent version of ossec.



Now that I have set up OSSEC on server and agent. I could monitor all the requests that any agent sends.

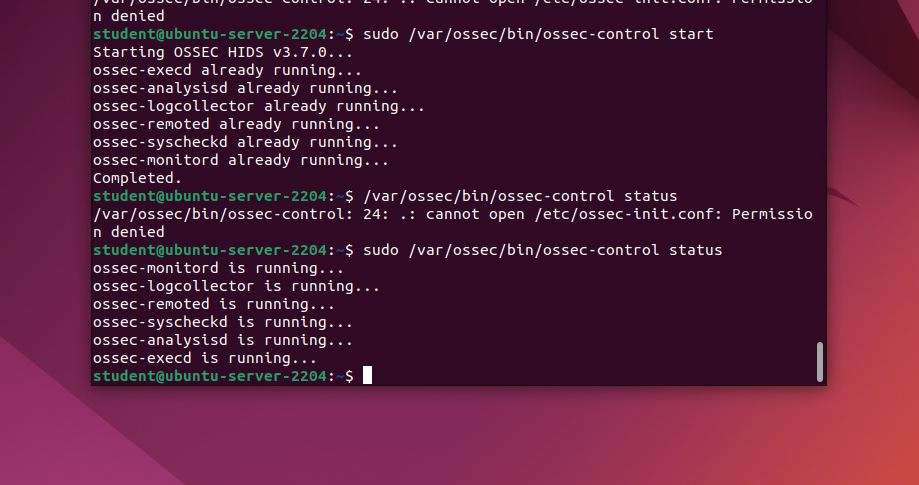
After setting up server OSSEC in the server, and agent OSSEC in Ubuntu. We need to link the agent to the server.

In the server, if we go to /var/ossec/bin/manage\_agents, we can add an agent. Let us add our Ubuntu client:



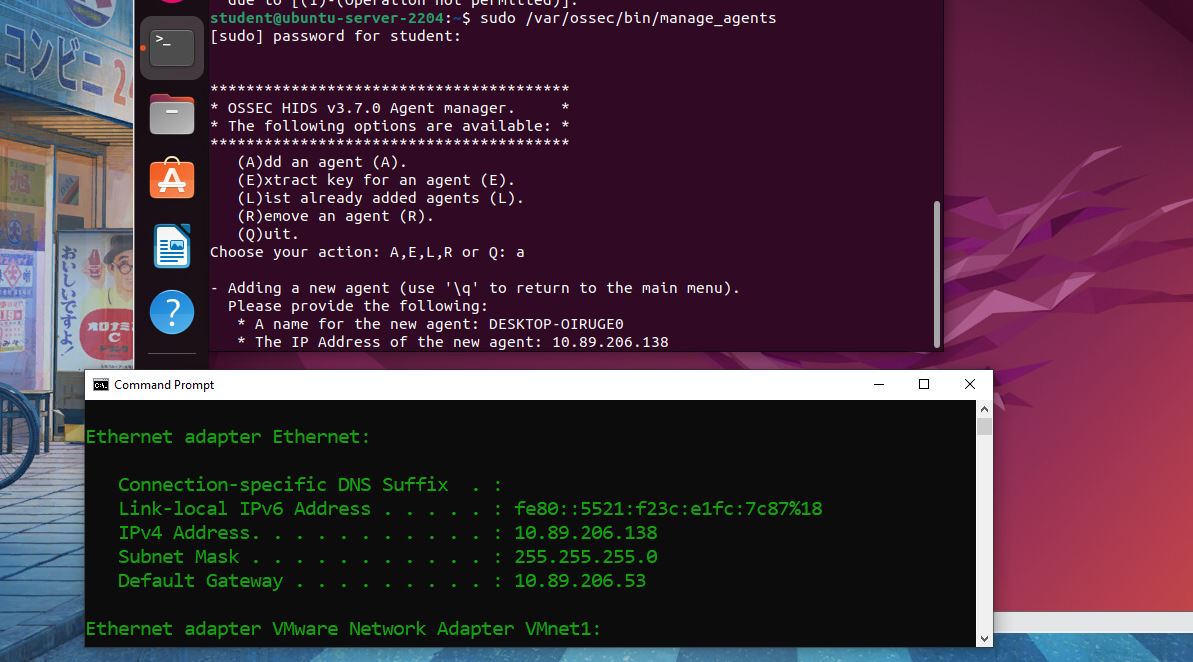
I added the Ubuntu agent and got the key that is unique for it.

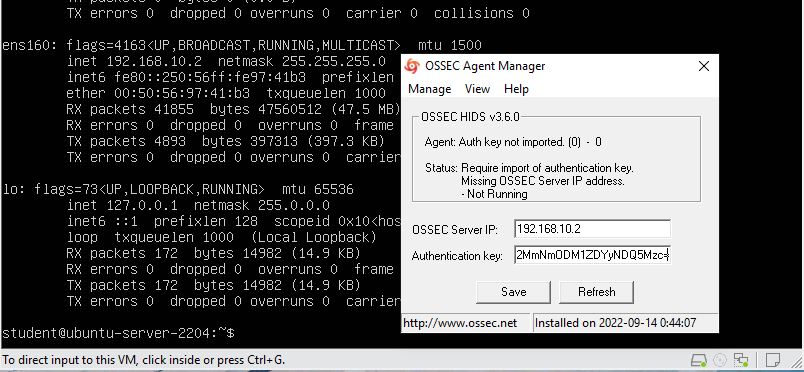
Now let us stop and start OSSEC



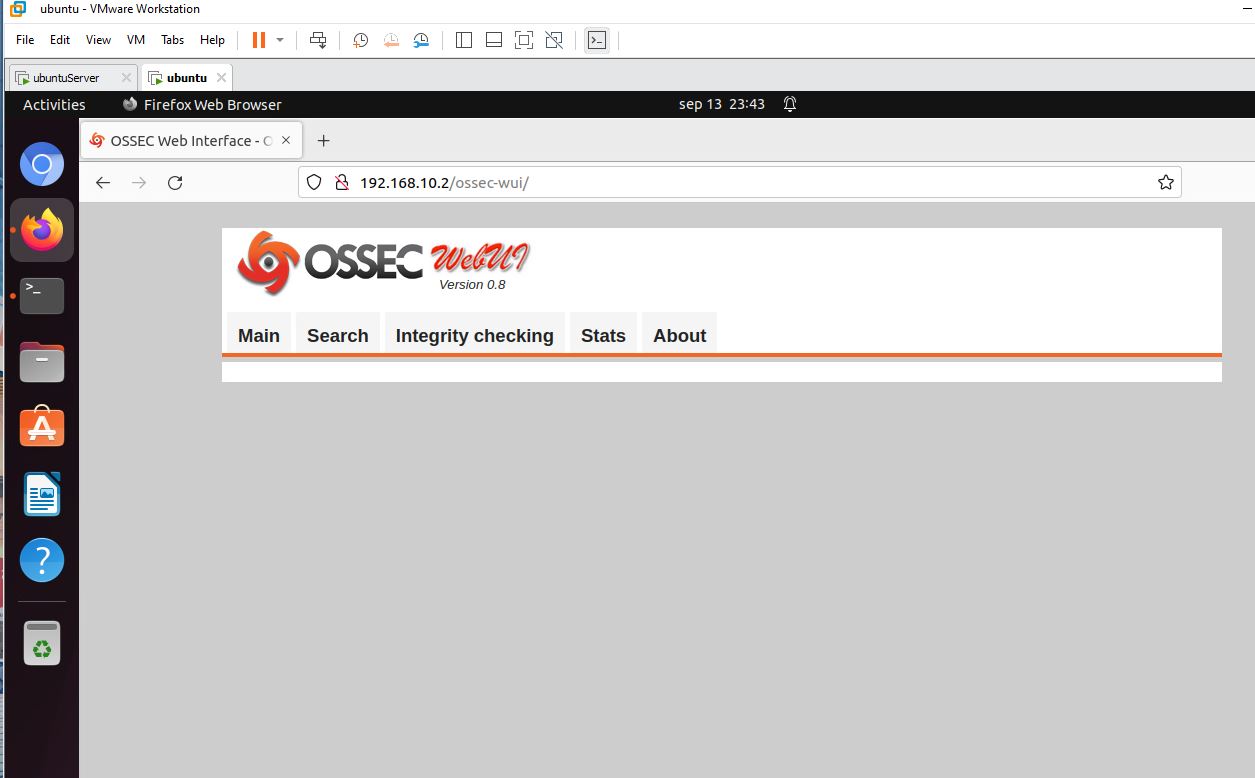
Now we can go to <http://192.168.10.2/ossec-wui> and see the dashboard for OSSEC.

I will do something optional which is installing OSSEC in windows. I could add agent like I did for Ubuntu. Then I enter the windows name and ip. I should get a key that is unique for windows. Install ossec and add the server ip and unique key in the interface.





The problem that I could not fix is that the OSSEC dashboard is empty. I spent hours trying to fix it and I looked for many websites, but nothing worked. However, I managed to make it work in the terminal only.



## DVWA (Damn Vulnerable Web Application)

### Path Traversal

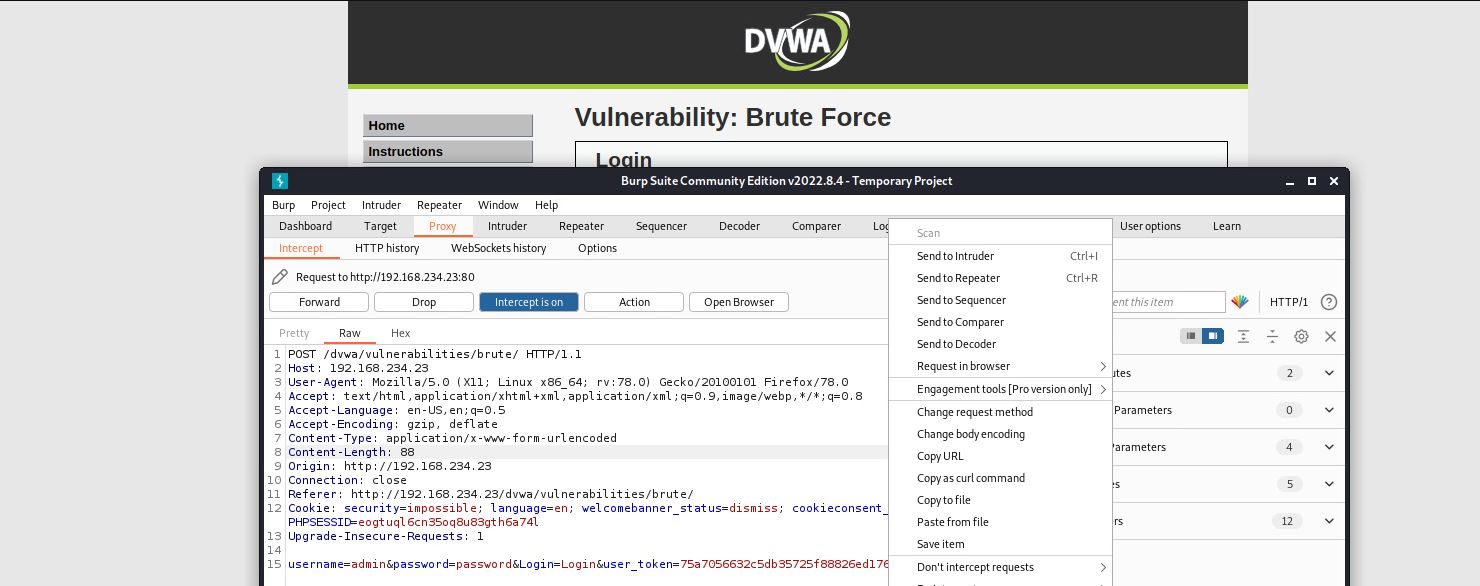
Moving to the real pen testing, we started the second week with a class for path traversal. It is when you study what is a specific system and then be able to know the file names and where sensitive data might be stored, you can navigate to the system files until you reach some private data.

Also, you could get to trick the terminal that you are someone else and execute commands on behalf of them.

### Brute Force

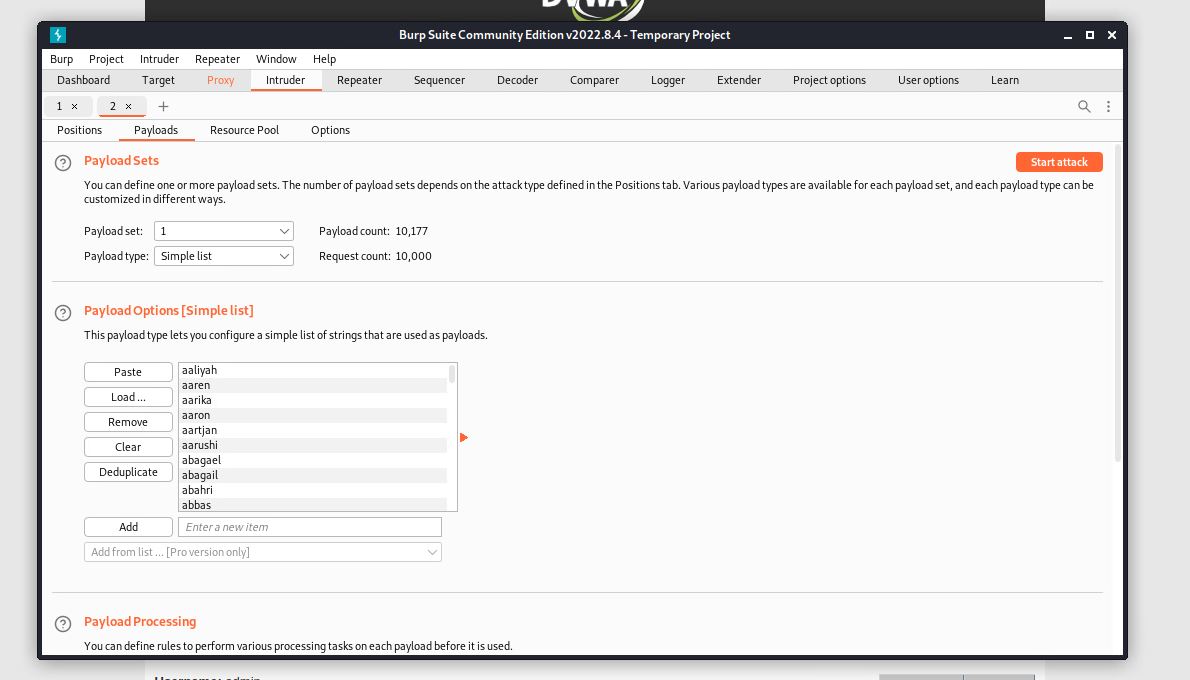
Brute force is when the attacker guesses the username/password to log into places they do not have access for. The way I would do this is by sending the POST request to Burp Suite to adjust the inputs as I desire. Burp Suite has many methods that have several purposes. For instance, Intruder is to specify a payload that you want to try so many inputs in that payload, and when burp suite returns a 200 status for the input (what the attacker guessed), means that the input was successful. Other way to know that the input is successful is by looking at the length as the correct input differs from the others.

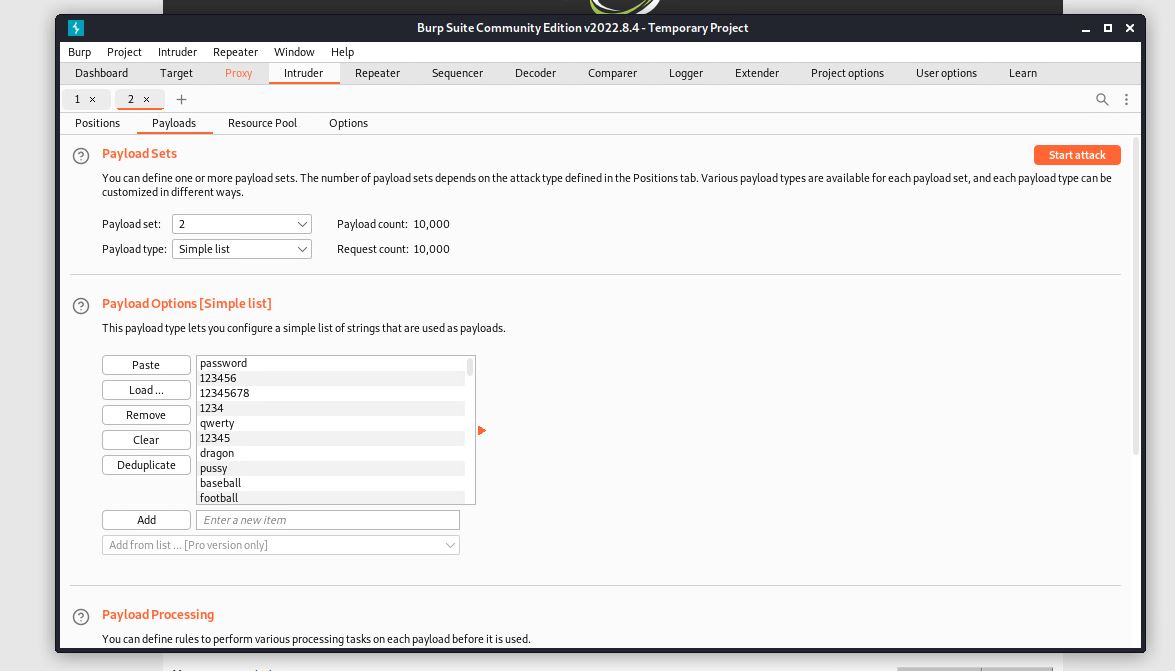
There are hundreds of username/password files that are available to make it easier for the pen tester to use instead of having to type the common username/passwords, you can just use these wordlists(/usr/share/secLists/), or you can find many other files on the internet.

Let’s get back to brute forcing, when capturing the request on Burp Suite, we should right-click and “Send to Intruder”. 

Then navigate to Intruder tab to specify the payloads that you want to test. For example, $username$(payload 1) and $password$(payload 2).

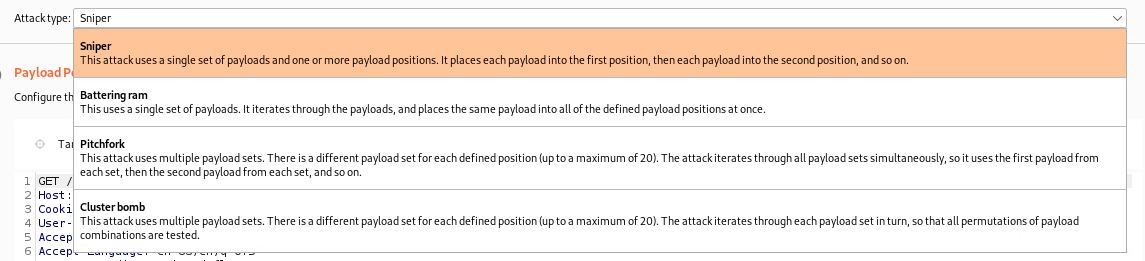
Start the attack and when there is a correct payload you would know by comparing to other inputs.





There are many Intruder methods. Such as, Sniper, Battering ram, Pitchfork, Cluster bomb.

You can choose one of them considering you situation.



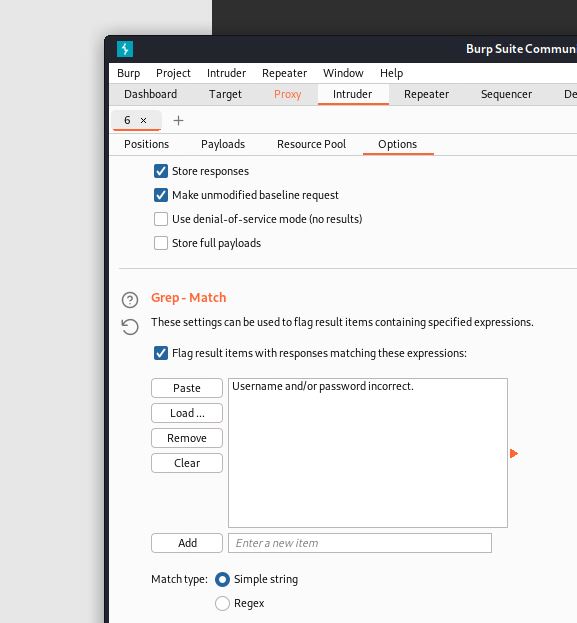
DVWA Exercise

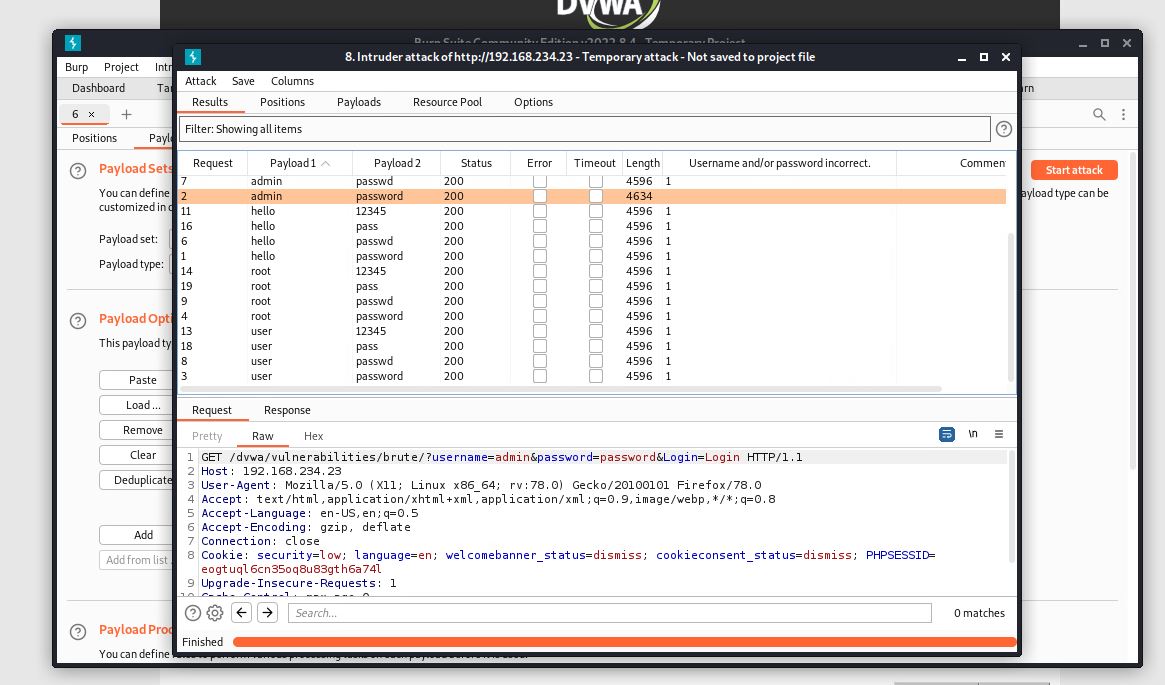
#### Brute Forcce – Low level

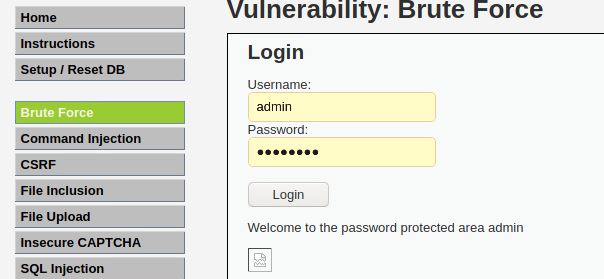
The correct answer is:

Username: admin

Password: password

You can notice it is the one that differs from others. I decided to filter the outputs as if they cause error and the correct answer is the only option that does not. 



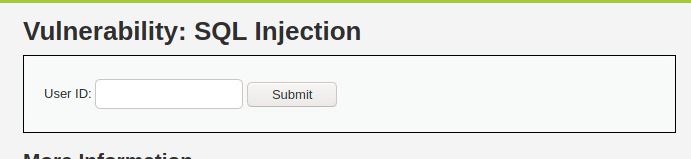


### SQL injection

This method attacks the database by tricking them to returning sensitive data. Websites have become more interactive than before. Therefore, the user is expected to manipulate the programming language code. For example, when the user is typing something in a web input, the website is ready to take that value to execute it to the website. This is a chance for the attacker to input malicious code that might affect the website in a bad way. One of the SQLi tricks is to force the database to return all the information by putting “1=1” in the sql query. 1=1 means that the query is always true, so it returns all the data.

DVWA Exercise:

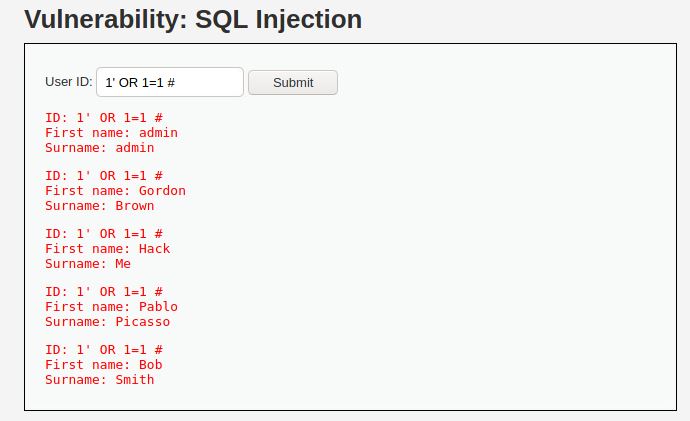
#### SQLi – Low level



The website here expects a number as input to return data that are true to that specific number. However, we can manipulate the query but first we need to understand it.

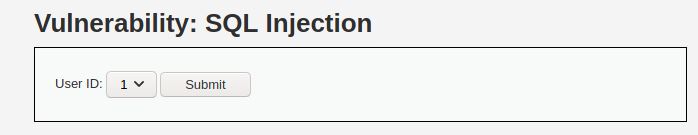


Simple query that we can easily adjust by entering a number as it asks, then close the quotation mark then type “OR 1=1” as it would return everything as true. Then finish the query with # to comment anything comes after.



Indeed the database returned all the data because of the 1=1 logic.

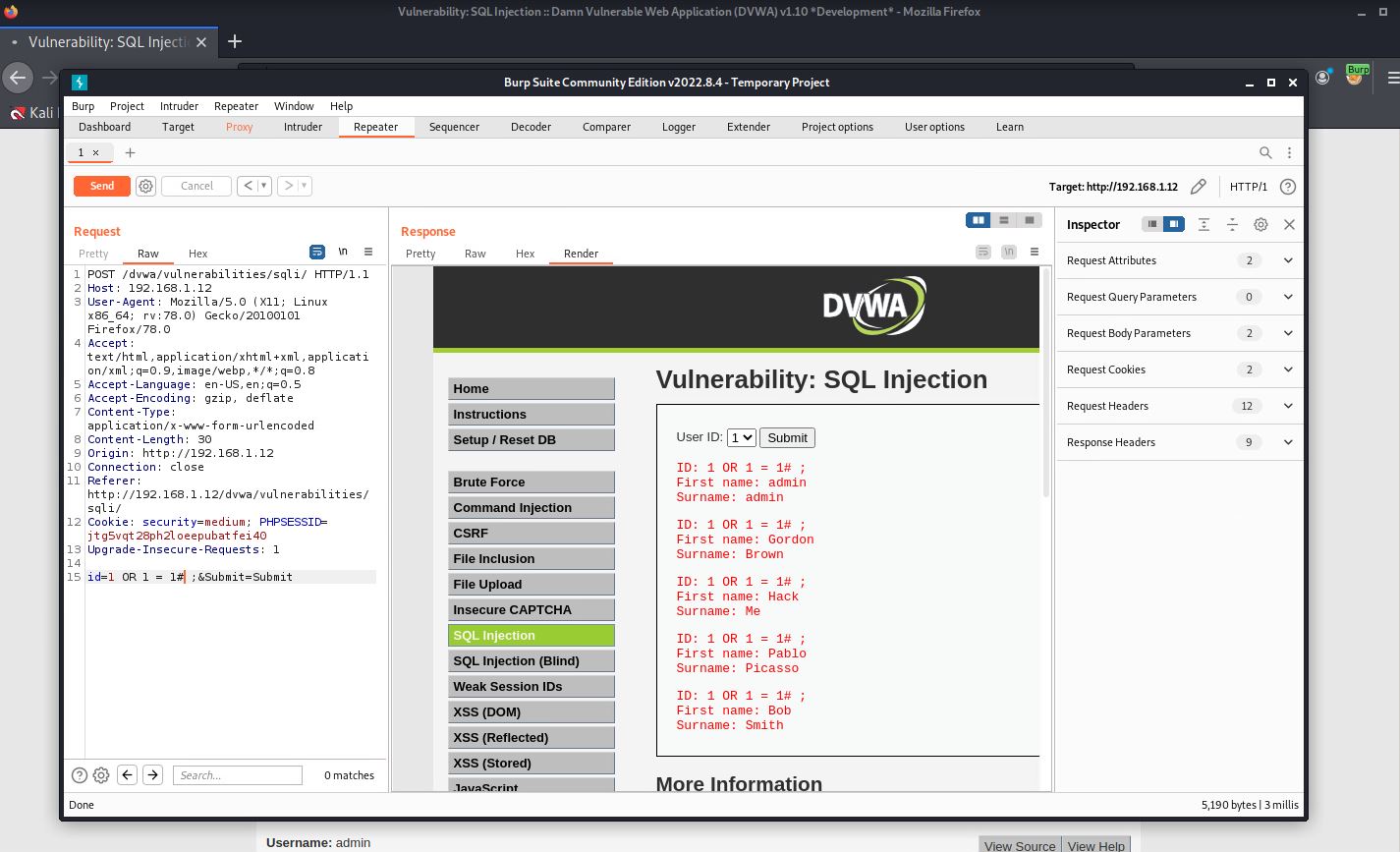
#### SQLi – Medium level



The difference here is that we are not given input to enter true logic with the input. We are just asked to select the number from a drop down. The idea for how to do this is still exactly like the old one. However, we just need to find a different way to put the logic onto the database.

For this I would choose Burp Suite to help me manipulate the POST request.

I just need to send the POST request to Burp Suite then send it to repeater to execute my logic there.



As you can see it is like the previous one, we only had to find a way to manipulate the POST request.

#### SQLi – Online Challenges

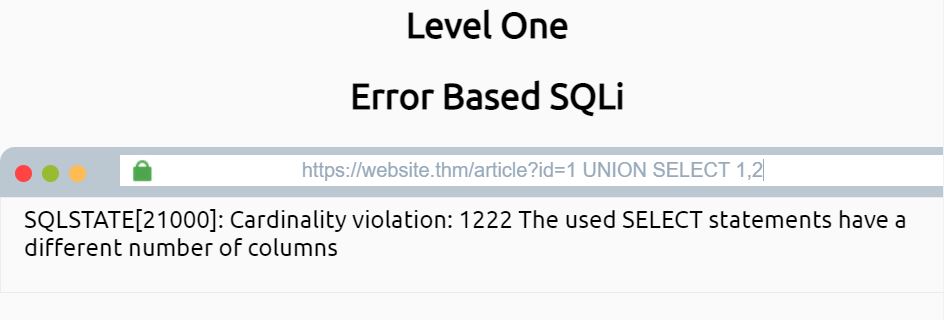
We can easily retrieve data from the database by just entering an expected number to the database. We can retrieve more data using the key word UNION.

How UNION works?

Union lets you trick the database by entering a number as expected, then after the number you type UNION to tell the database that you are not finished, and you demand more data.



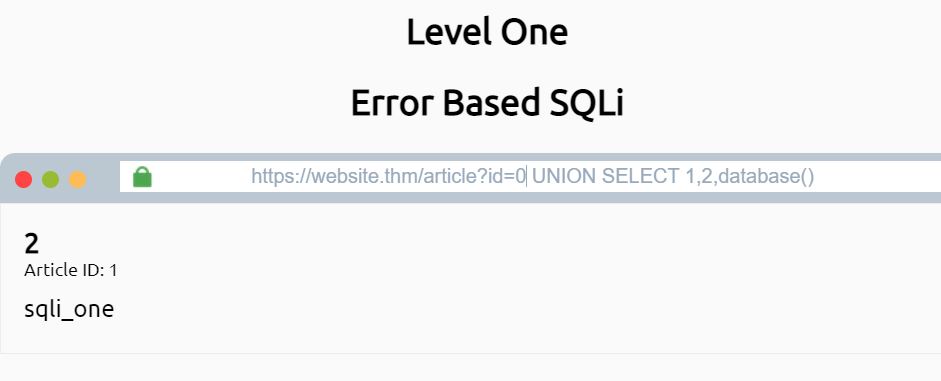
Getting error in SQLi is the first step towards breaking the database. The attacker should aim for getting error before trying to exploit. This error tells us that the second database has different columns than we entered. Therefore, let us try adding one column:



We still get the same error. Let us add one more column:

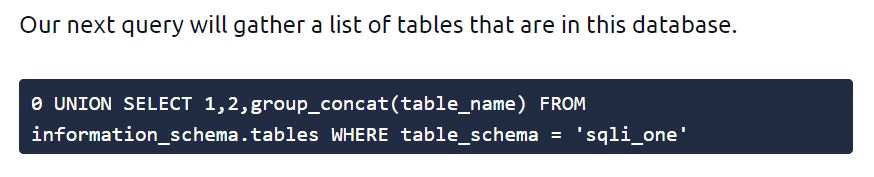


It worked. The second table has 3 columns. Let us now get the name of the database:



We replaced a column with “database()” to get the name of the database. Also you can notice that we changed the id value from 1 to 0, this is because we do not care about the return of the first part of the query, we care about the return of the UNUION SELECT statement.

Now we can ask for all the tables in that database.



And it returns:



This tells us that we have 2 tables: article and staff\_users, and we can access them using group\_concat().

admin123' UNION SELECT 1,2,3 where database() like 'D%';--

This query helps us to guess the database name. We keep entering values in the LIKE statement, as long as we get true as a respond, that means that the input letter/number is true. We keep guessing every letter until we get the whole name.

What is step 2?

admin123' UNION SELECT 1,2,3 FROM information\_schema.tables WHERE table\_schema = 'DATABASE\_NAME' and table\_name like 'u%';--

We repeat the same thing but for the table name this time.

Step 3:

admin123' UNION SELECT 1,2,3 FROM information\_schema.COLUMNS WHERE TABLE\_SCHEMA='DATABASE\_NAME' and TABLE\_NAME='users' and COLUMN\_NAME like 'a%';

We keep guessing the column name. After getting all the column names, we can retrieve the data inside that column using:

admin123' UNION SELECT 1,2,3 from users where username like 'a%

admin123' UNION SELECT 1,2,3 from users where password like '123%

OR

admin123' UNION SELECT 1,2,3 from users where username='admin' and password like '123%

With this technique, we can get to the username and the password then log in.

#### SQLi - TIME BASED

It has the same idea as the previous method. When the entered statement is true, the response should be delayed for some seconds.

admin123' UNION SELECT SLEEP(5),2;--

If the database has 2 columns(TRUE STATEMENT) the response should be delayed 5 seconds.

Then we can proceed:

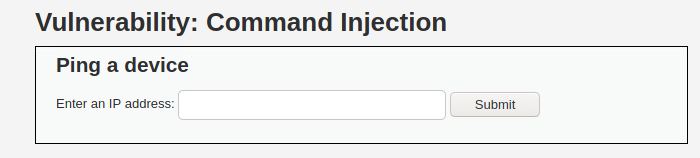
=admin123' UNION SELECT SLEEP(5),2 where database() like 'u%';--

(WE CAN USE BurpSuite to save time)

### Command Injection

#### Command Injection – Low level

We are presented with an input to enter any ip address to PING.

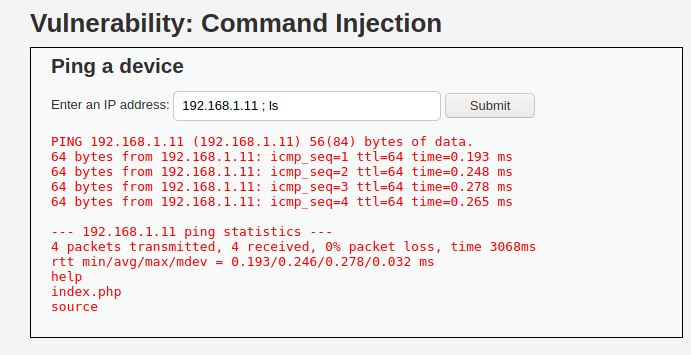


Let us see the code behind this function:



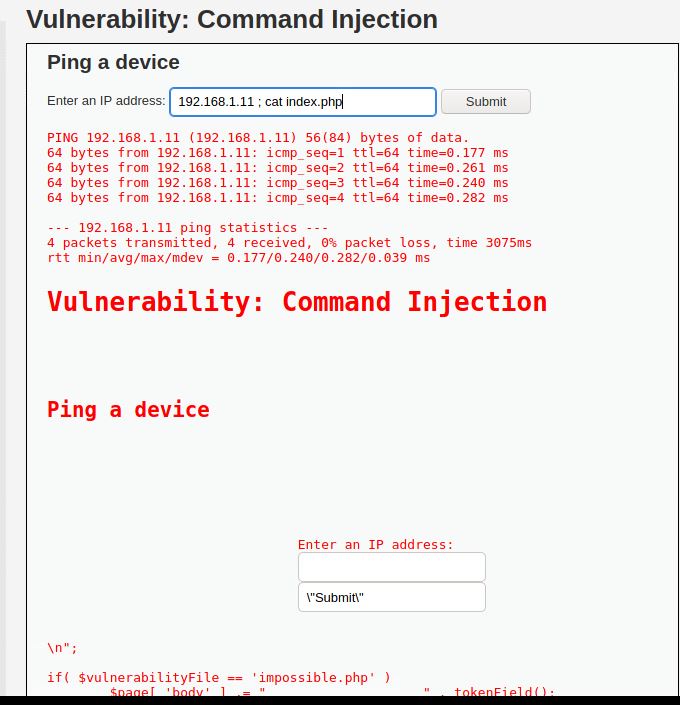
This function basically tells the program to go to the cmd and ping the target (entered ip).

It should be too easy to tell the input to do more commands. For example, we can enter any ip normally then we can finish the command by putting ; in the end. After that, we can enter more commands to get more details like (ls, pwd, etc).



As we ping the ip, we also managed to execute ls command which outputs files and folders in the system (help, index.php, source)

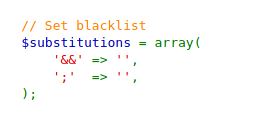
Let us see the content of index.php for example:



#### Command Injection – Medium level

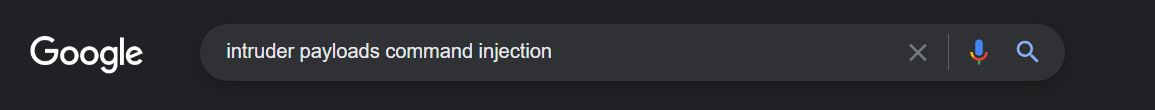
When trying to do the previous method here you would not get any response.

Why? Looking at the code:



We see that some symbols are not allowed anymore. Good but not good enough as the attacker can easily to adjust the POST request in Burp Suite to look for the allowed symbols.

First I went to google.com and looked up:

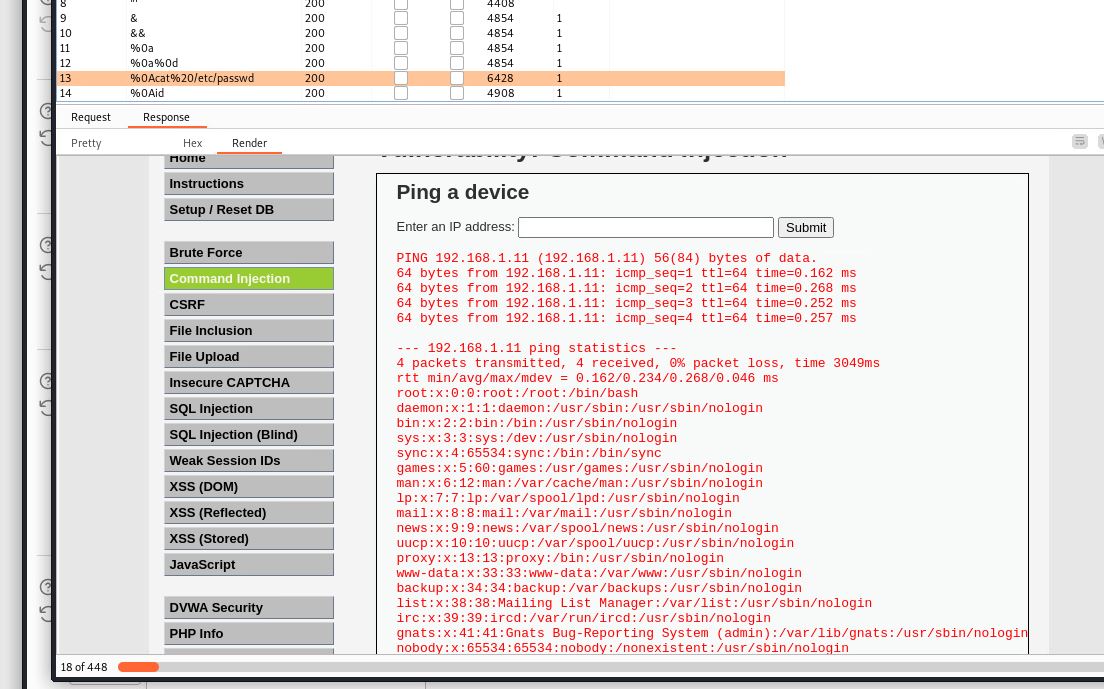


I found this page

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Command%20Injection/Intruder/command_exec.txt>

This github page has so many command injection payloads that I can try for the exercise.

I sent the request to Intruder. Sniper method helped me to load the words list and I filtered the output to packet loss as I would know the right answer If the packet loss check box was checked.



Eventually, I got to output the passwords file.

# (BOK) Network Security (week 5-8)

# (BOK) Security Concepts (week 9-10)

# References

* Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007, October). Social phishing. *Communications of the ACM*, *50*(10), 94–100. <https://doi.org/10.1145/1290958.1290968>
* Wallen, D. (2020, March 3). *Intrusion Detection Systems: A Deep Dive Into NIDS & HIDS*. Security Boulevard. Retrieved September 9, 2022, from <https://securityboulevard.com/2020/03/intrusion-detection-systems-a-deep-dive-into-nids-hids/>
* Tudor, D. (2021, August 27). *What Is a Host Intrusion Detection System (HIDS) and How It Works*. Heimdal Security Blog. Retrieved September 9, 2022, from <https://heimdalsecurity.com/blog/host-intrusion-detection-system-hids/>