Individual Assessment Coversheet

To be attached to the front of the assessment.

Campus: Pretoria

Faculty: Information Technology

Module Code: ITSPA0-B33

Group: Group 1

Lecturer's Name: Ms. Montwedi. B.

Student Full Name: Kelebogile Nanikie Mathebula

Student Number: [redacted]

Indicate	Yes	No
Plagiarism report attached	×	

Declaration:

I declare that this assessment is my own original work except for source material explicitly acknowledged. I also declare that this assessment or any other of my original work related to it has not been previously, or is not being simultaneously, submitted for this or any other course. I am aware of the AI policy and acknowledge that I have not used any AI technology to generate or manipulate data, other than as permitted by the assessment instructions. I also declare that I am aware of the Institution's policy and regulations on honesty in academic work as set out in the Conditions of Enrolment, and of the disciplinary guidelines applicable to breaches of such policy and regulations.

Signature: KNP.	**Date: 28 August 2025**

Lecturer's Comments:

Marks Awarded:	**%**

Signature	**Date**

Table of Contents

NB: ZOOM FOR CLEAR VIEW!!

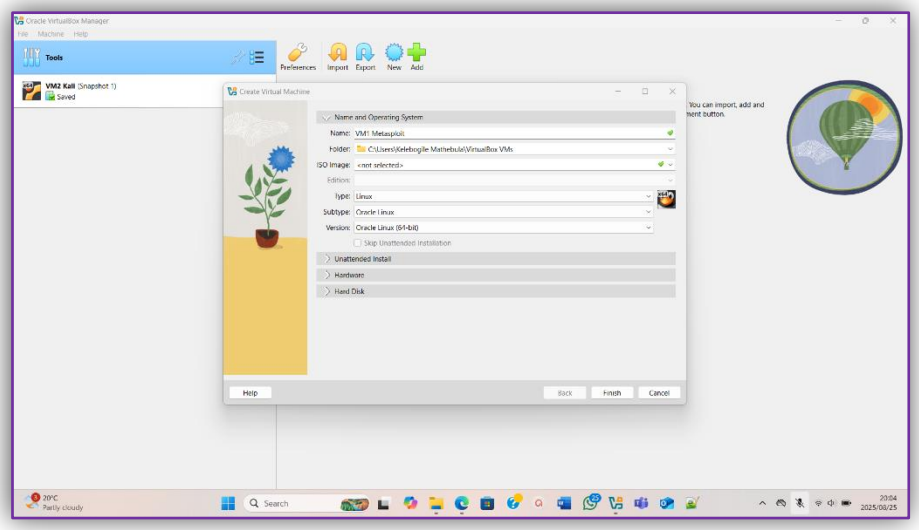
1.1. Install two virtualisation machines (VM1 and VM2) on your host computer and configure 80GB and 1024MB of RAM for each machine.

On VM1 Metasploit 2 partition: (HackHunt, 2023)

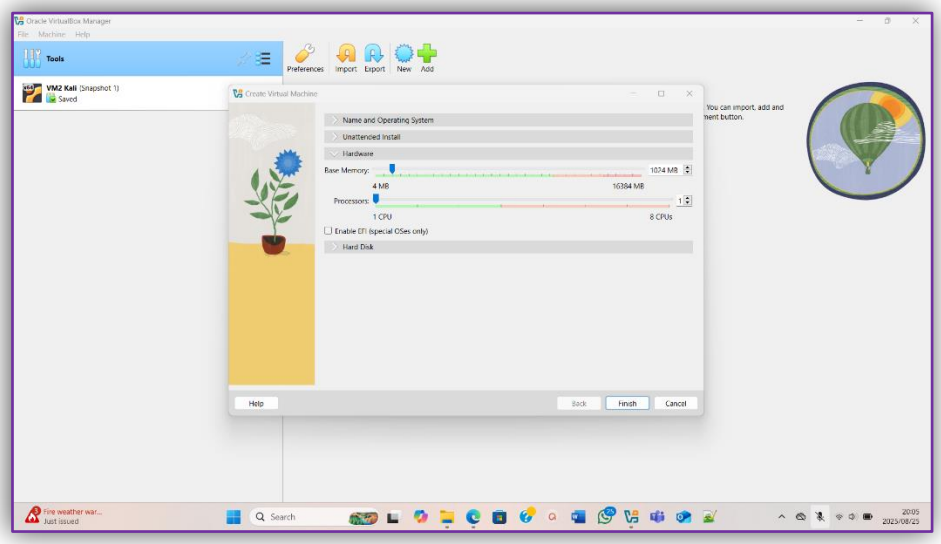
- Name the computer DC1

The first thing I did was create the VM using Oracle Virtual box.

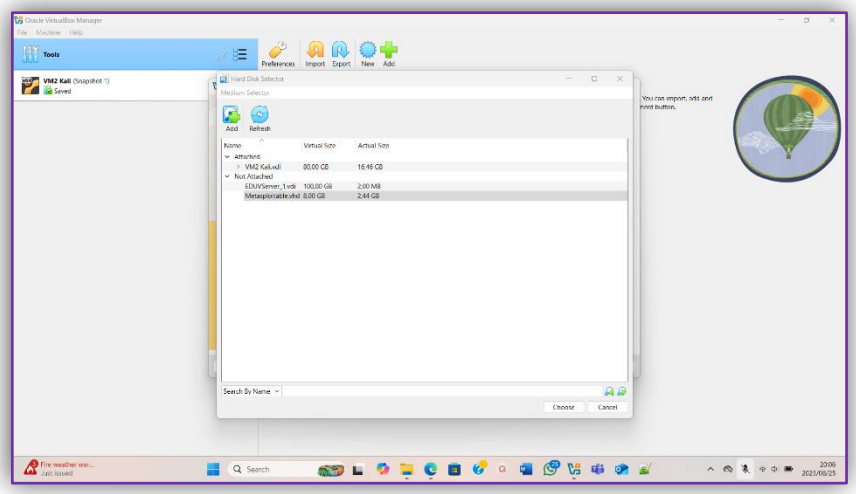
When creating the VM I changed the type from Windows to Linux since the Metasploit VHD is based on Ubuntu and I need to tell VirtualBox what type of operating system that's inside the VHD. The following images show the creation of the VM.

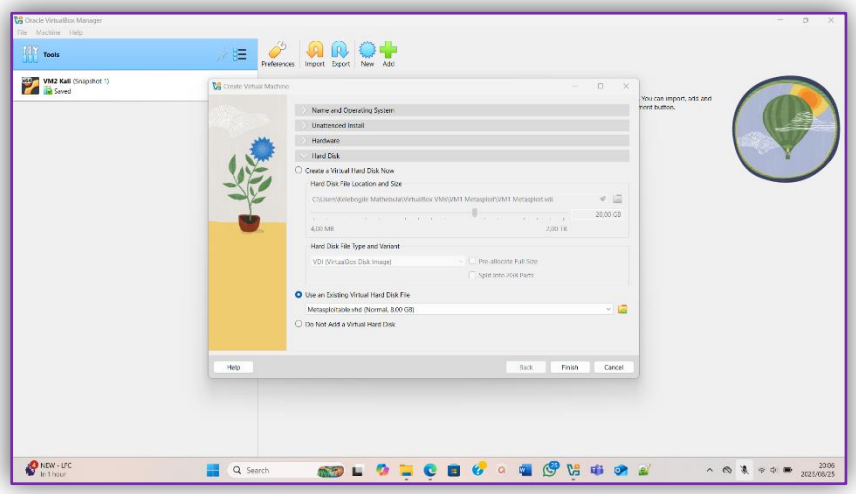


The following shows where I assigned the base memory of the VM.

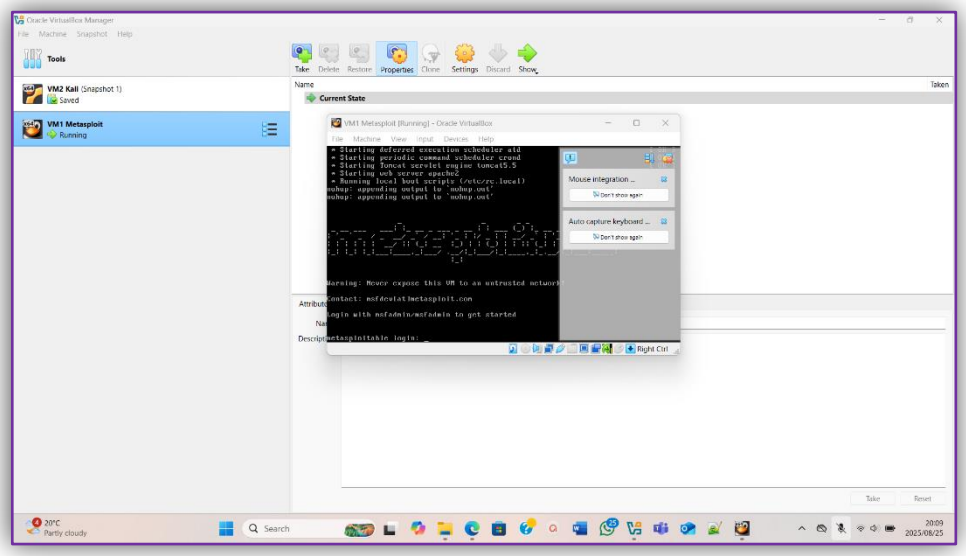


The following image shows when I added the Metasploit .vhd file.

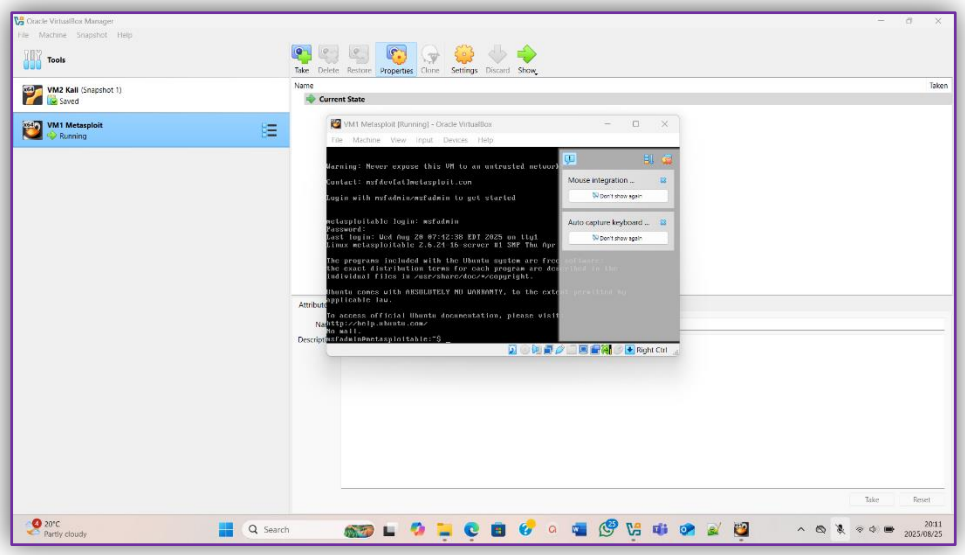




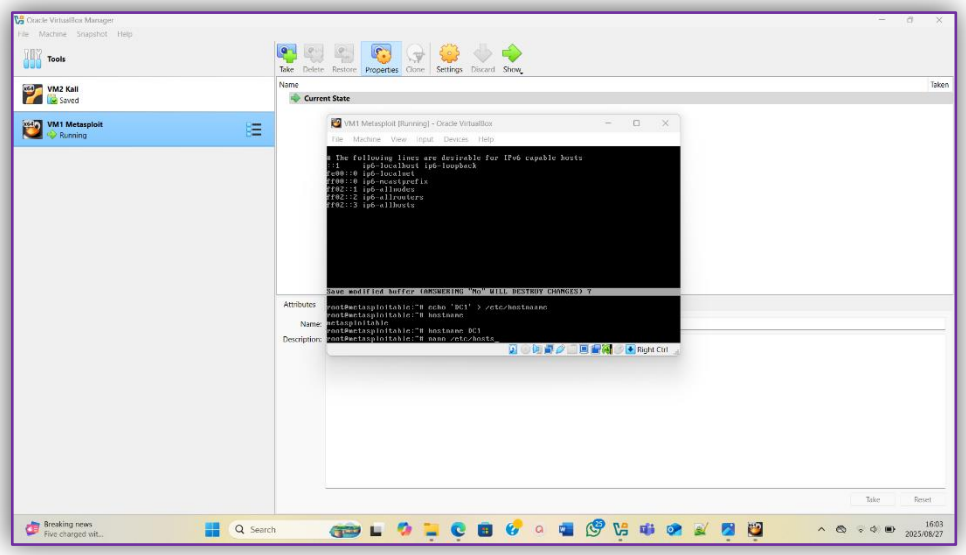
Once the creation was complete, I then started the machine, the following image shows the sign in stage before I changed the computer name/hostname to DC1.

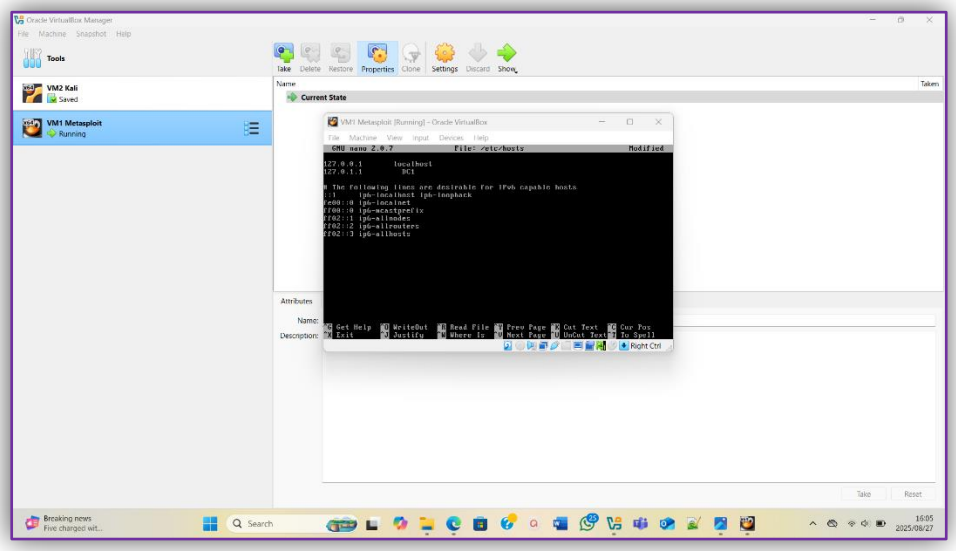


The following image shows what you supposed to see once you successfully sign in.

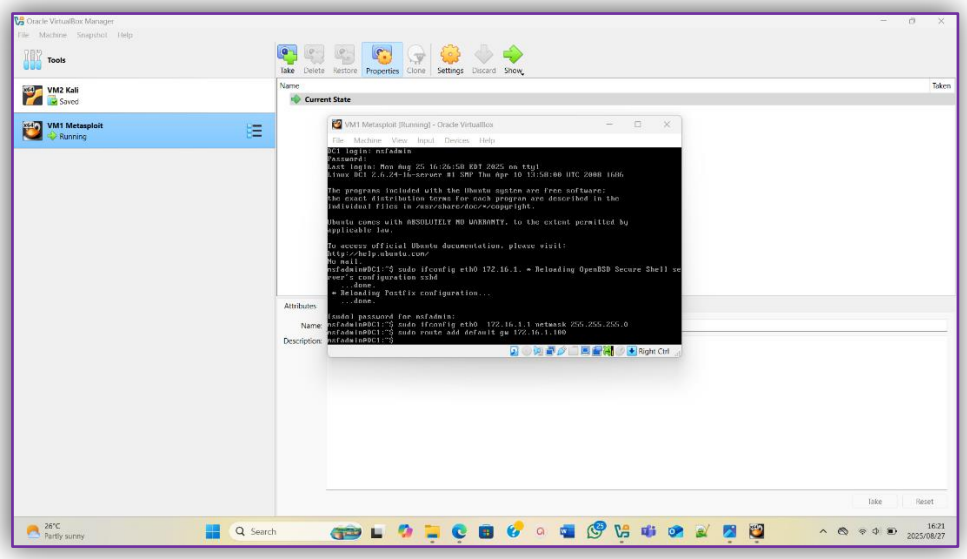


I then started the process of changing the computer name/hostname, the commands at the bottom of the first image are the ones I used when changing the computer name to DC1.



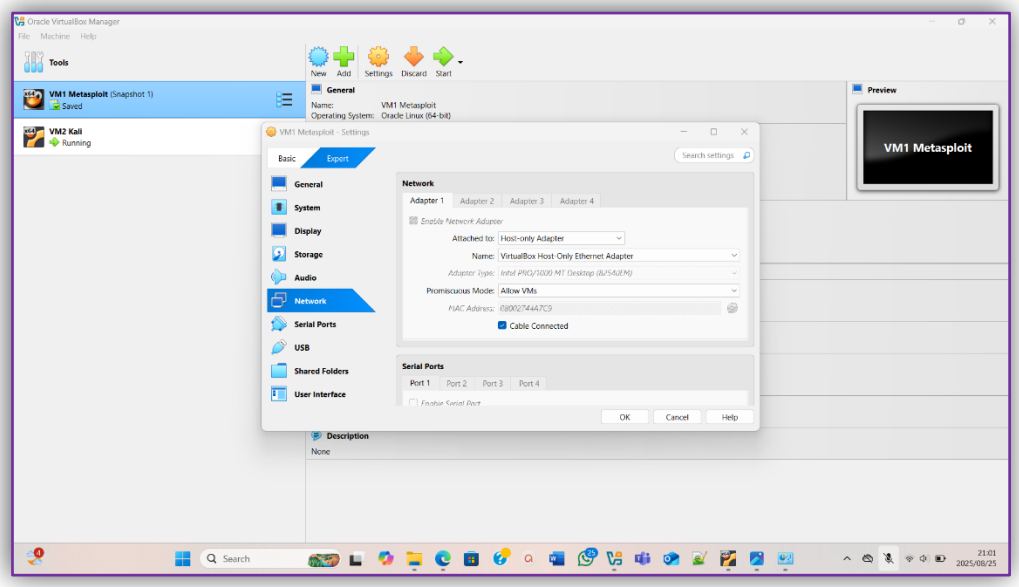


I then rebooted the machine once I saved the changes I made to the host name. The hostname/ computer name was then successfully changed. The following image shows the sign in step after the reboot, which shows that the hostname was successfully changed.

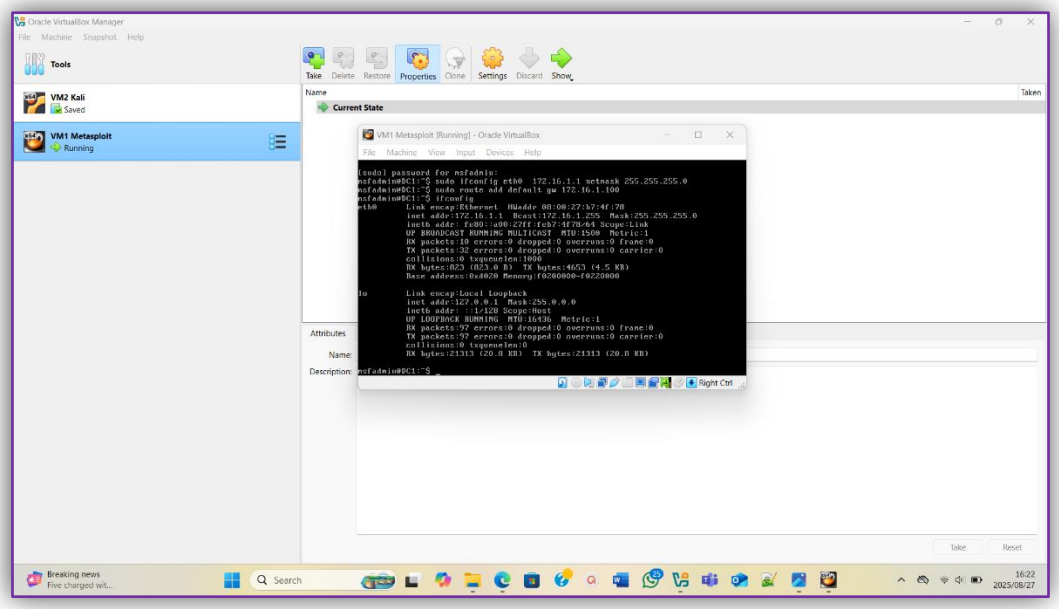


- Assign an IP 172.16.1.1 (SecDive, 2019)

Before changing its IP address, I connected it to the virtual switch which I connected to the Kali machine, just so that both the machines are on the same network.

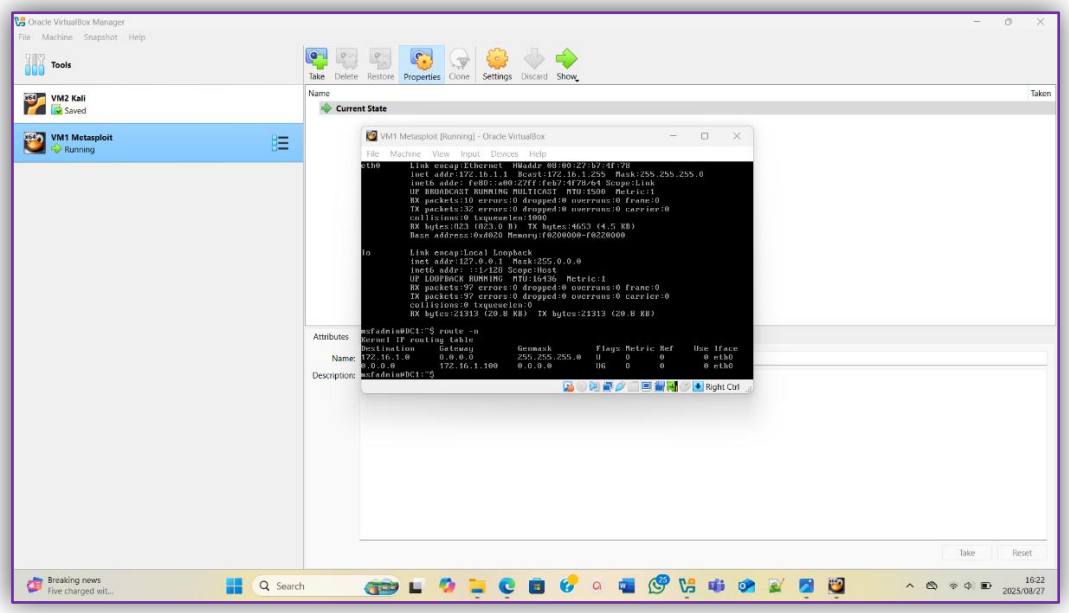


The following images shows that the command I used to set the IP address as well as the default gateway and the results of the result from setting the IP.



- Gateway 172.16.1.100

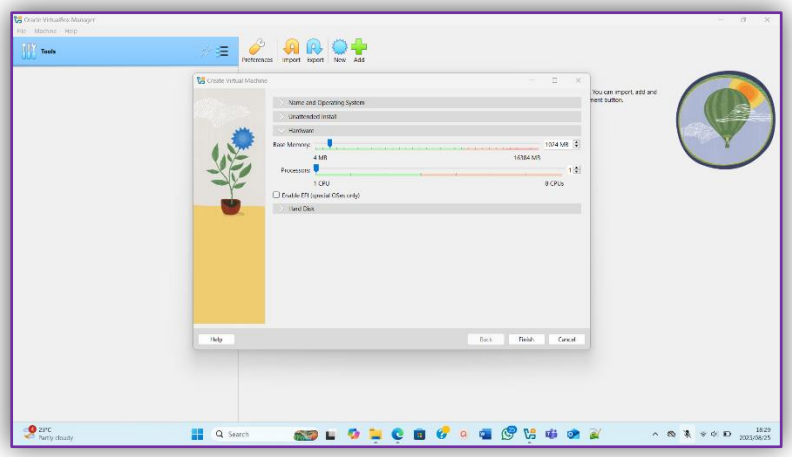
This image shows the results from the command "**route -n**" which shows us the gateway.



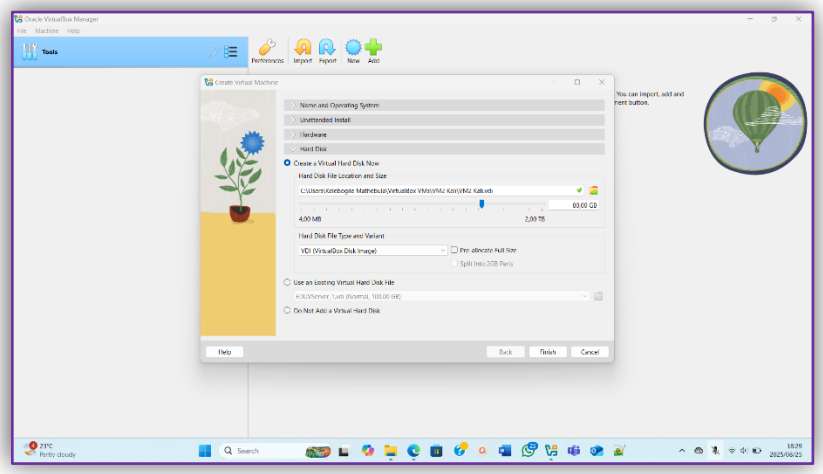
On VM2:

- ❖ Install Kali Linux on 50GB Partition

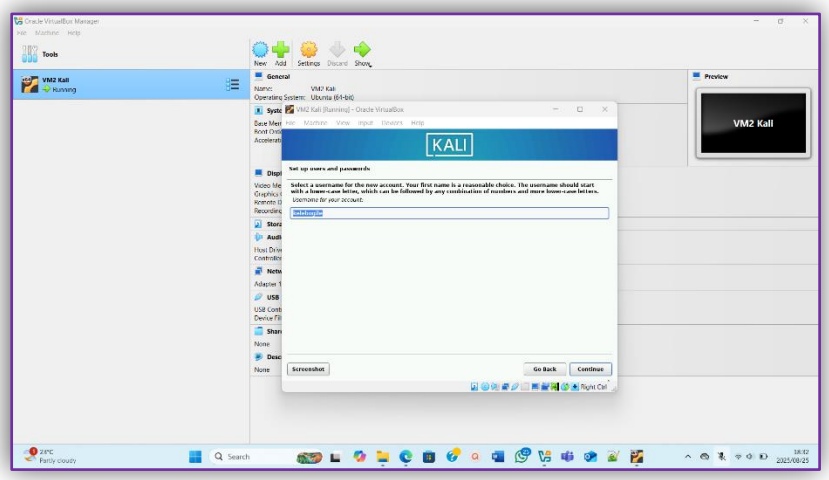
The following images show the creation of the VM. The following image shows the size I allocated to the base memory.

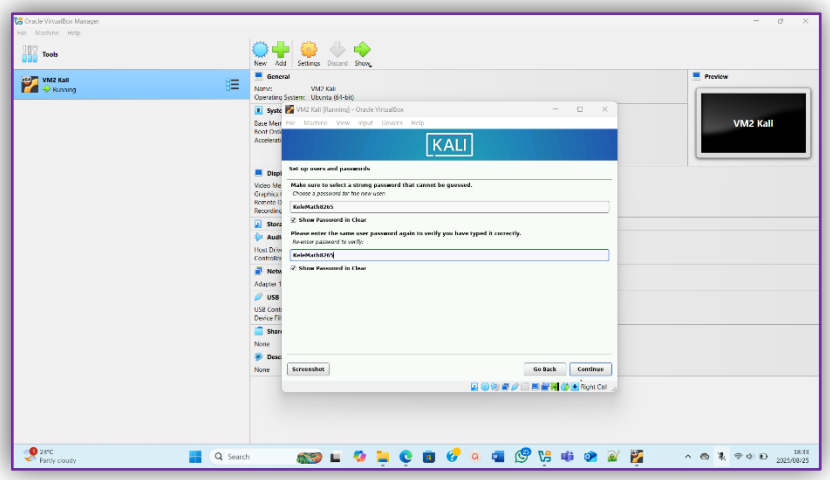


The following image shows the VHD size allocation.

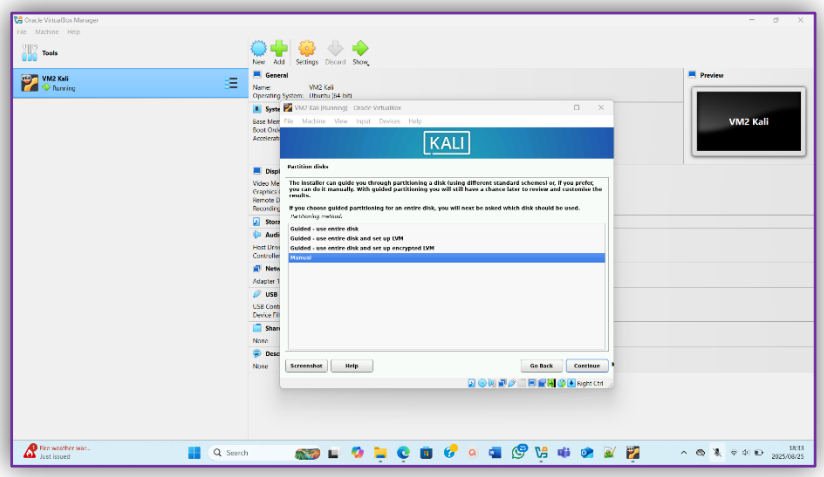


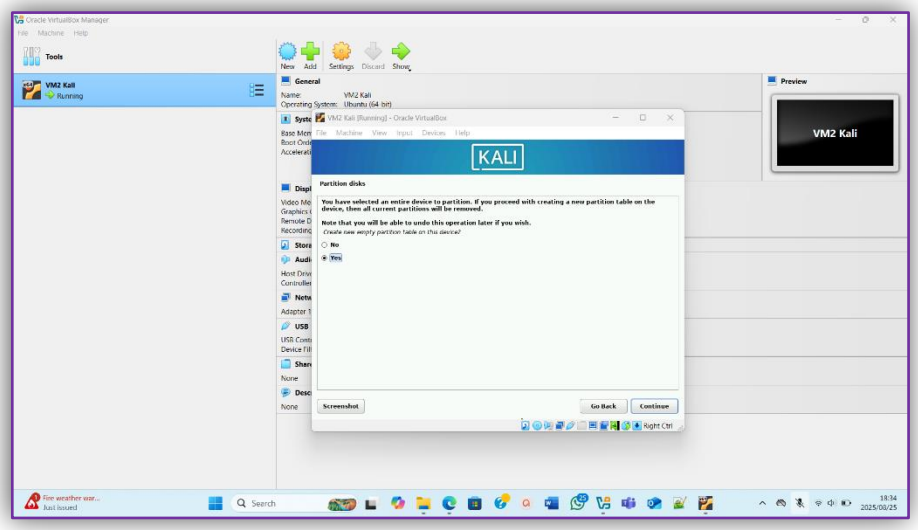
Once the creation was finished, I then started the setup of the machine. The first thing I did was select the “Graphical Install” then the language which is “English”, after selecting the language I then choose the country which is “South Africa” I also choose the keymap for the configuration of the keyboard which is “American English”. Once that was done, I had to give the hostname a name, once I assigned the hostname I went ahead and named the domain “kali”. The following images show the steps after naming the domain, which starts from assigning my user’s name.

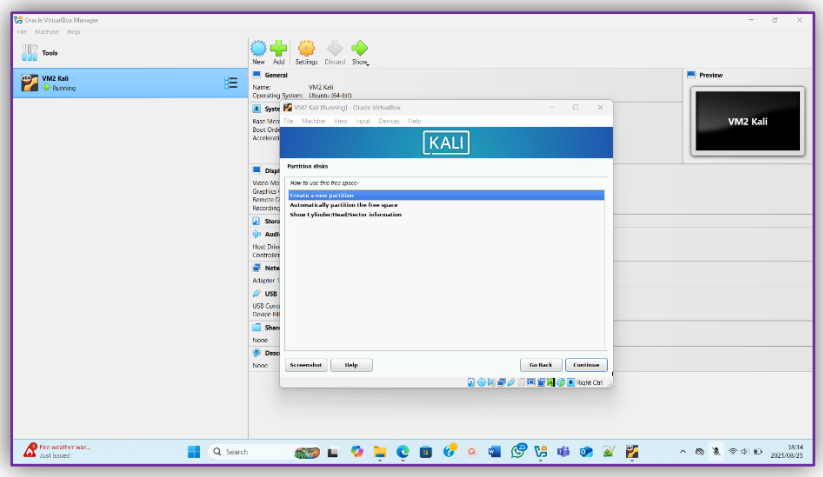




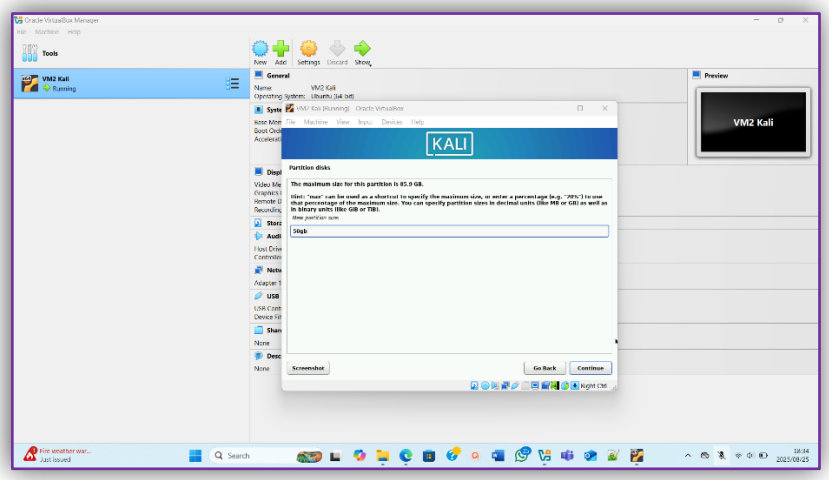
I then started the partitioning of the hard disk drive. I choose to manually partition the hard disk drive.



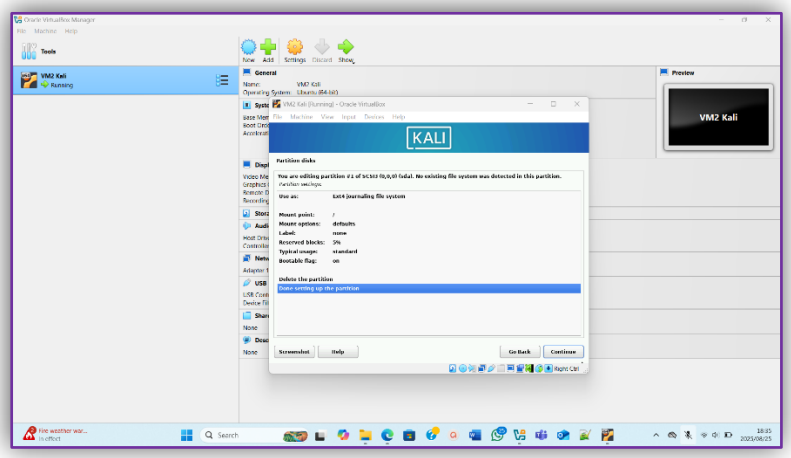




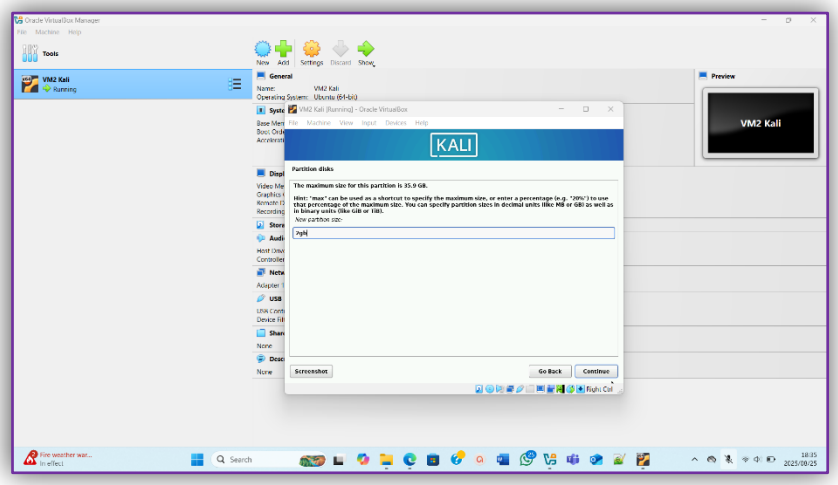
The following image shows when I choose the size I wanted to partition, I also made the bootable flag on.



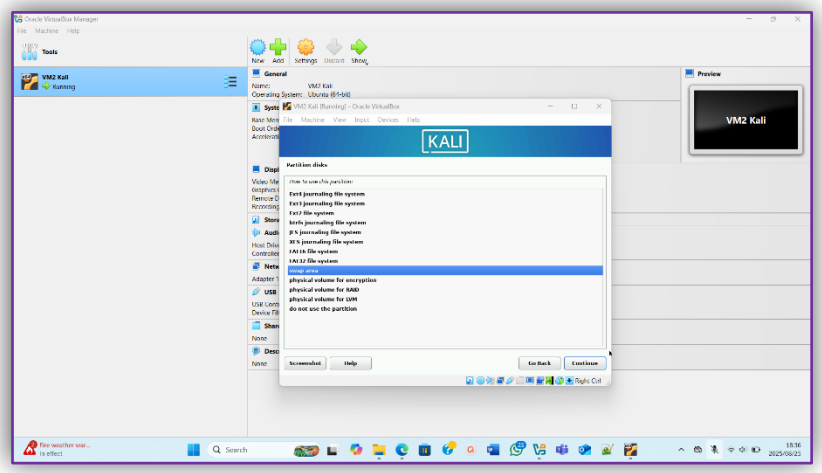
I made the type of partition “Primary”, and I set the location of the partition to be at the “Beginning”. The following image shows the partition properties and the mount point is a “/root mount point”.



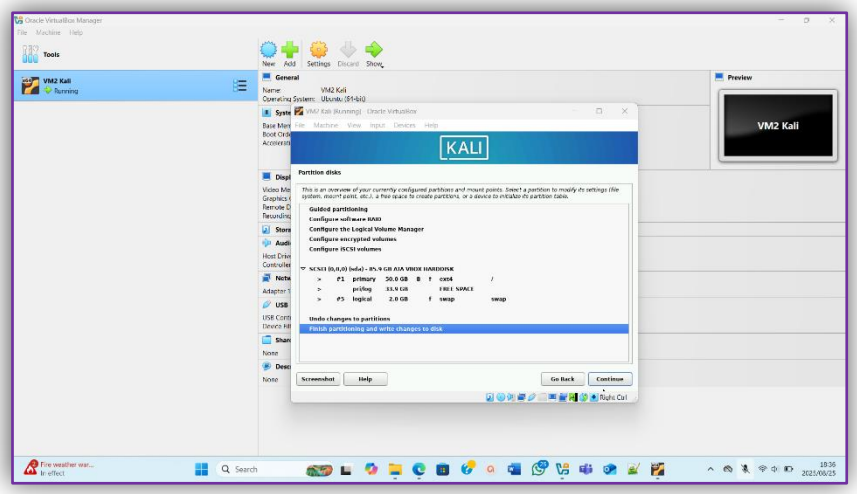
I then created a new partition that I was going to use as a swap which is the backup memory space on the hard drive that Linux uses when RAM is full or for hibernation. The steps are the exact same as for the 50GB partition. I made the type of partition “Logical” and the location was set to “End”. The following image shows the size I wanted to partition.

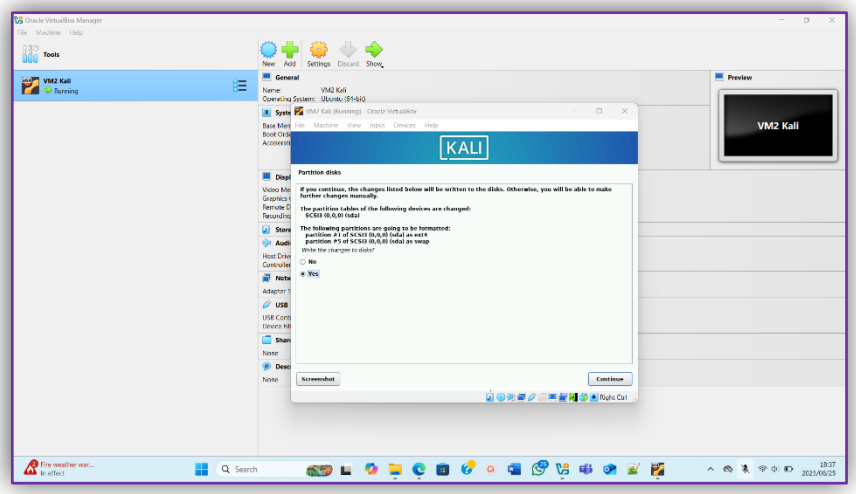


I used the partition as a swap.

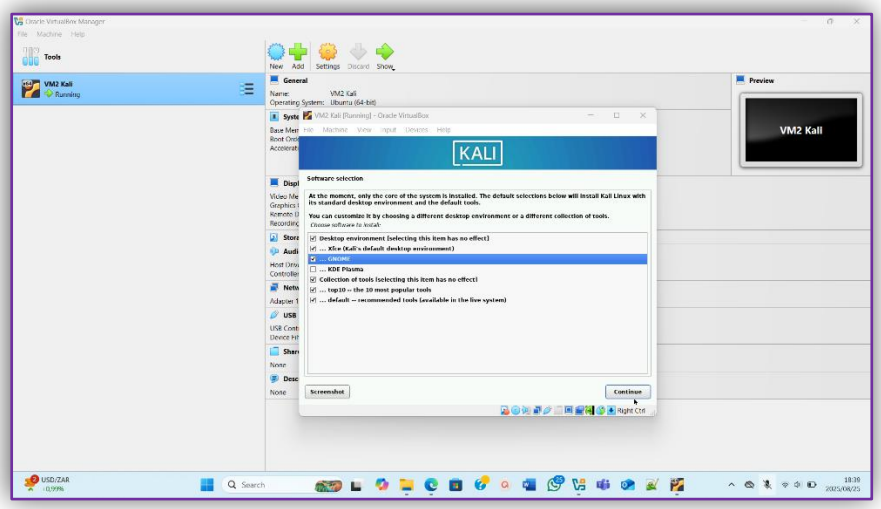


The images below show the steps from writing the partitioning to the disk.

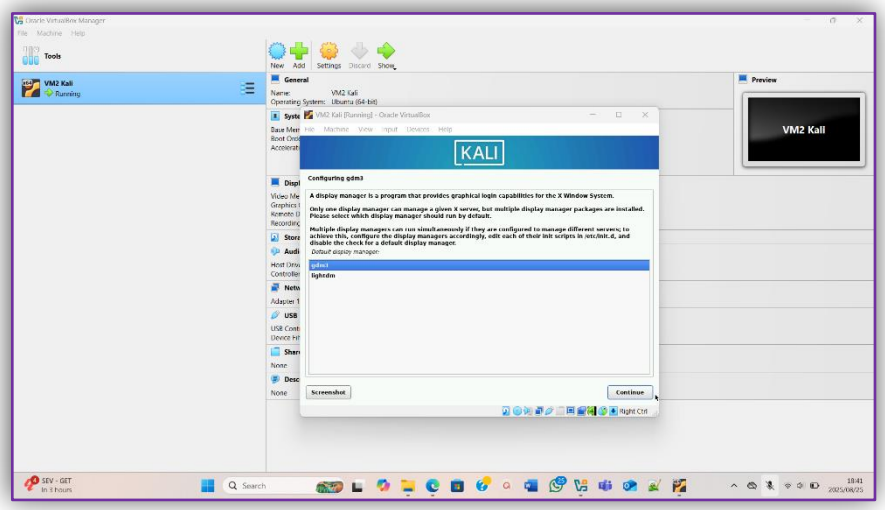




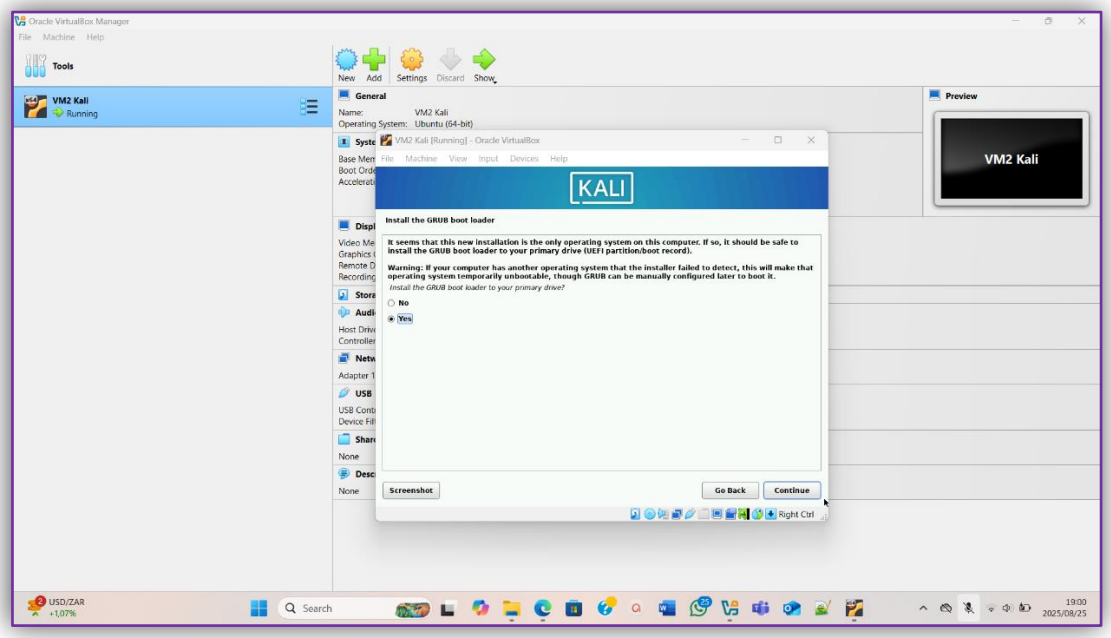
Once that was done, I then had to select the software that I wanted to install. I left the default as they where and added “GNOME” and that is because it gives a more modern look to the desktop and also I added the “Xfce” which is the default software for the desktop environment for kali Linux.

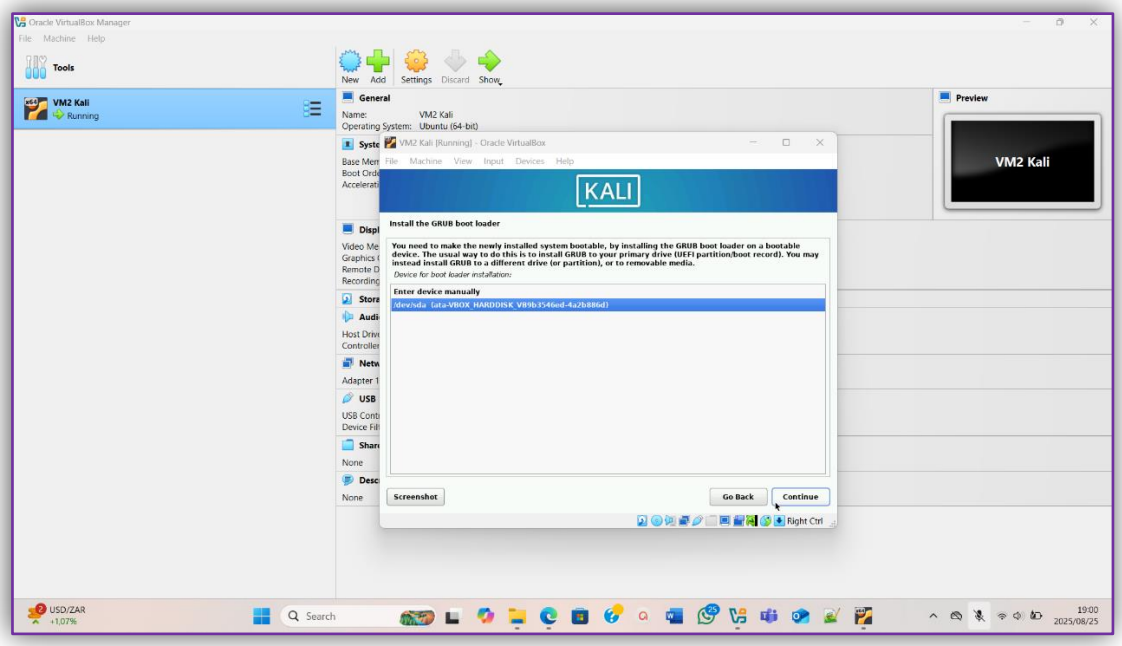


I then choose the display manager that I wanted.



I then installed the GRUB Boot loader which is loads the OS, and it is like the menu that you see when you start your computer and it decides which operating system or kernel to boot.

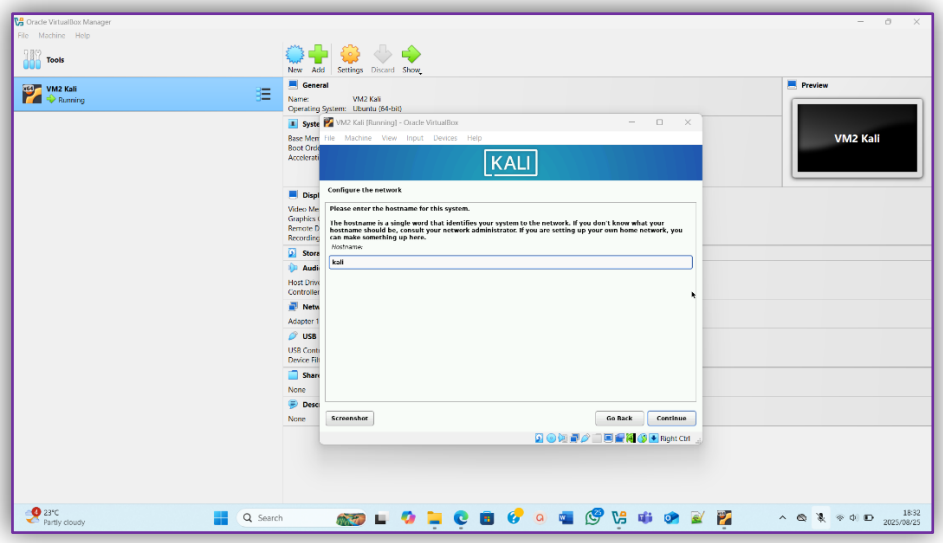




Once the installation was finished the sign in page is what appeared. Kali Linux was installed with a 50GB partition.

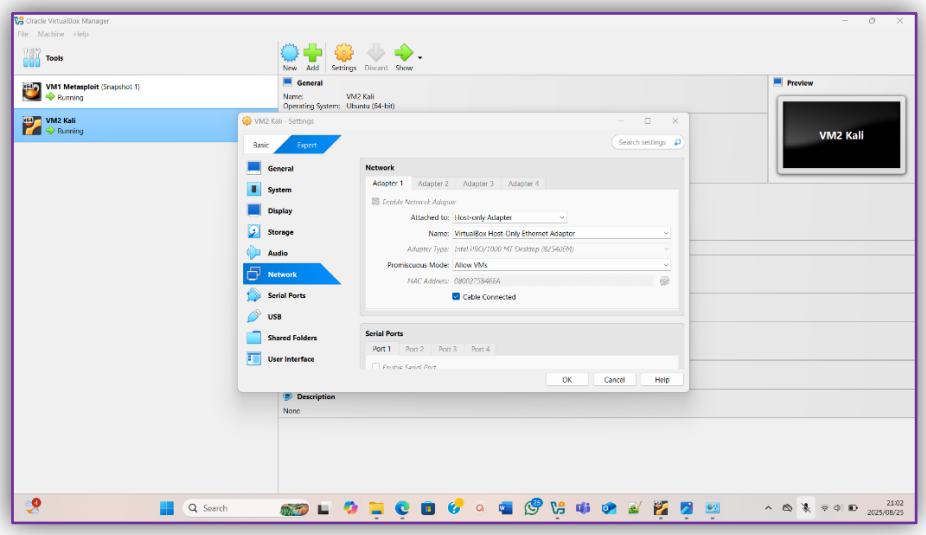
- ❖ Name the computer Kali

As I mentioned above, I named the hostname “kali” which was the fifth step of the VM setup. I named the VM itself “VM2 Kali”.

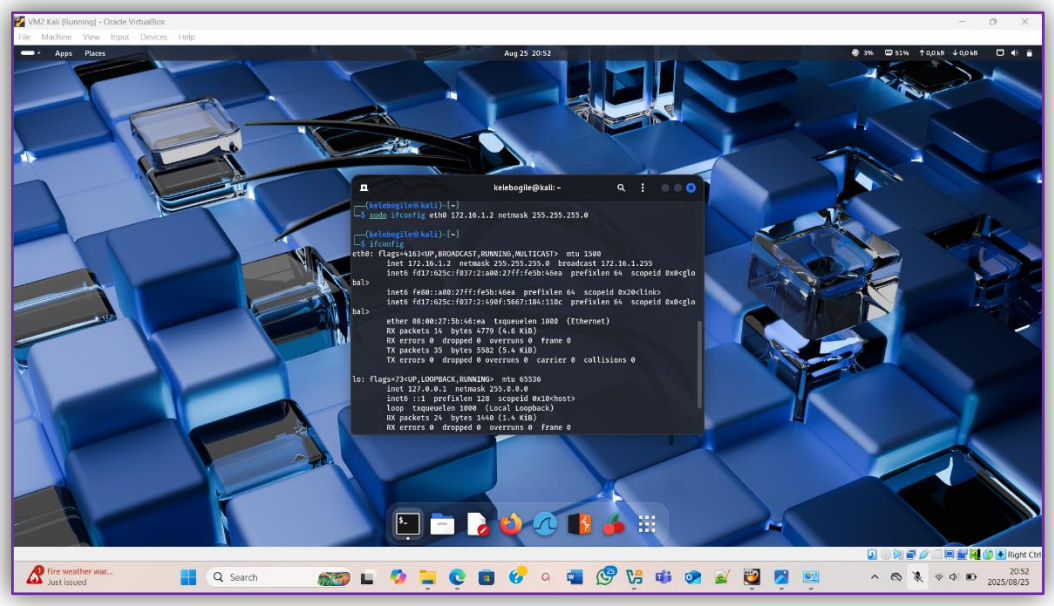


- Ensure an IP of 172.16.1.2 is assigned on the Kali machine (Tips, 2025)

The first thing I did was connect both the DC1 and Kali to the same virtual switch just so that they are on the same network. The following image shows when I connected the VM to the virtual switch.



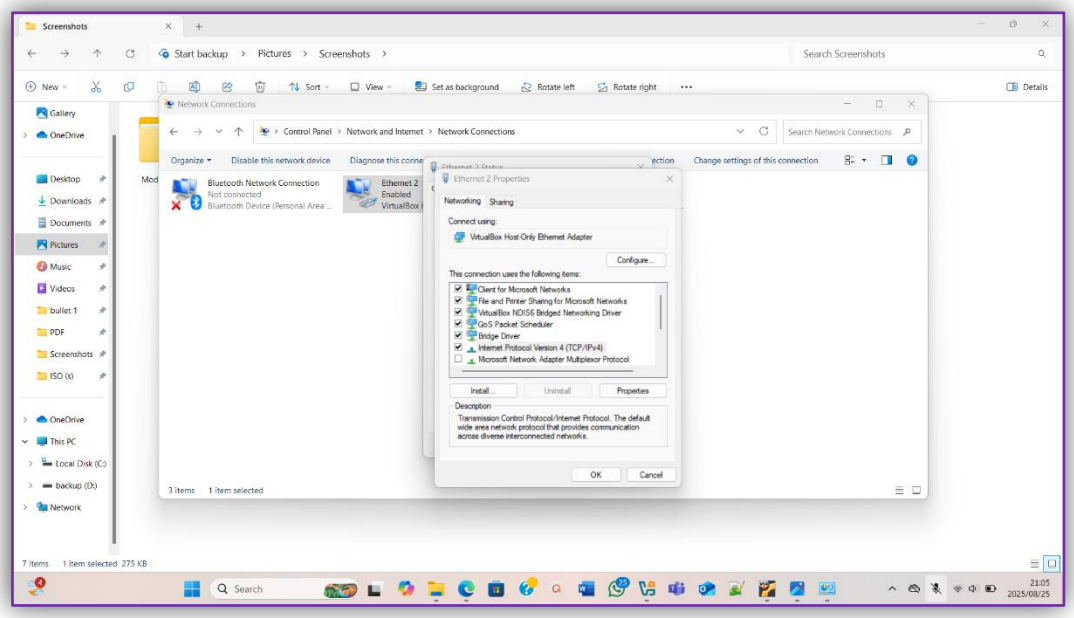
The second thing I did was sign in; after signing in I opened the terminal. I then ran the code that is used for setting the IP address and the subnet mask which is "**sudo ifconfig eth0 172.16.1.2 netmask 255.255.255.0**", sudo is used for running commands as the admin, ifconfig is used to configure network interfaces, eth0 is for the name of the network card/interface you're configuring and the netmask is what tells the computer what subnet it belongs to. I then ran "ifconfig" to see if the code was successful and that I actually assigned the new IP address.

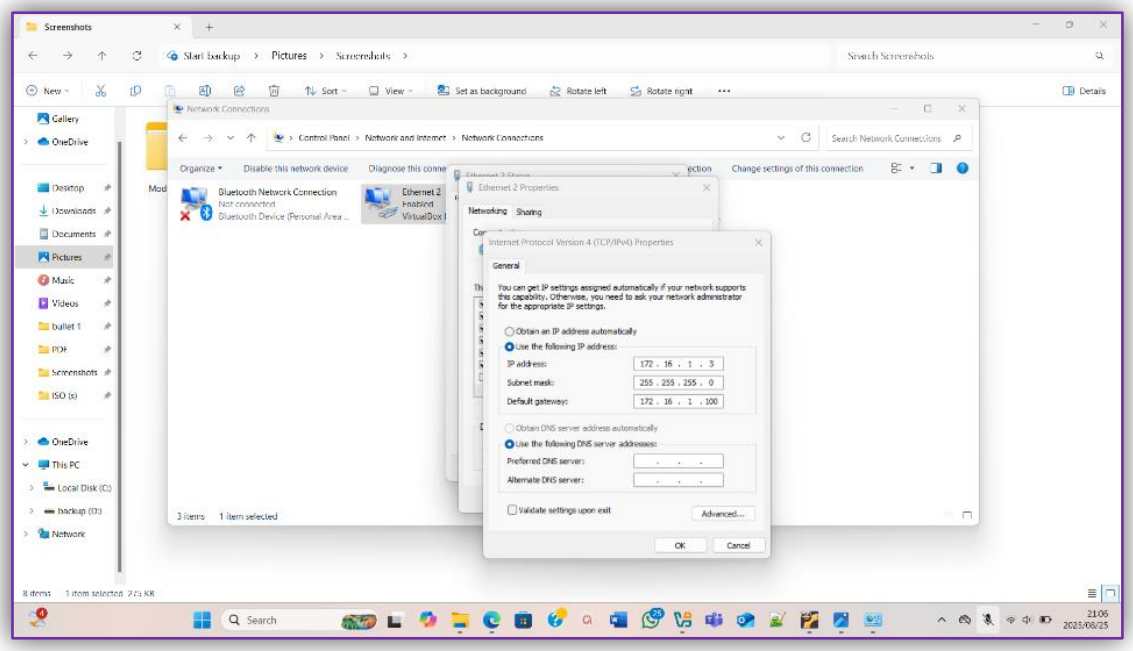


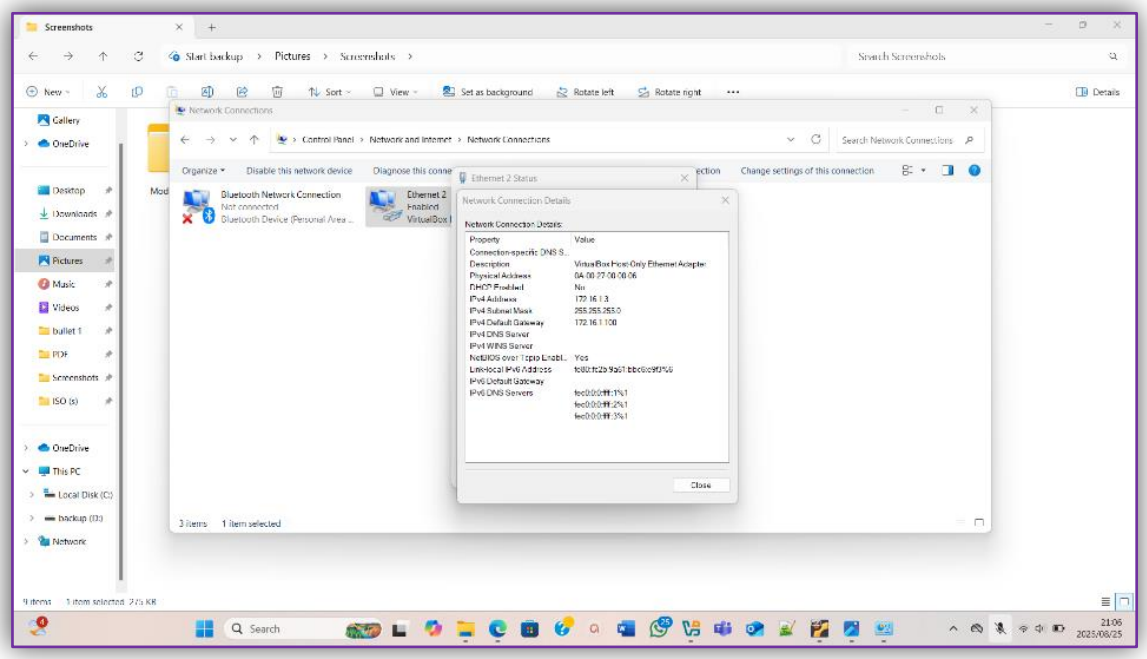
❖ Ensure the Windows 10 Host machine has an IP address 172.16.1.3

Before I set the IP address of both DC1 which I named “VM1 Metasploit” and Kali, I made sure that I changed the IP of the host and once I did that, I then connected them to the same virtual switch and then assigned their IP addresses.

So, when the changing the hosts IP I started by going to Control Pannel then I went to “Network and Internet” and clicked on it and by the search bar I looked for “Network Connections” and double clicked “Ethernet 2” and the started changing the IP address by going to “properties” and from properties I choose “Internet Protocol Version 4 (TCP/IP)” and went to its properties. The following images show the steps from there.

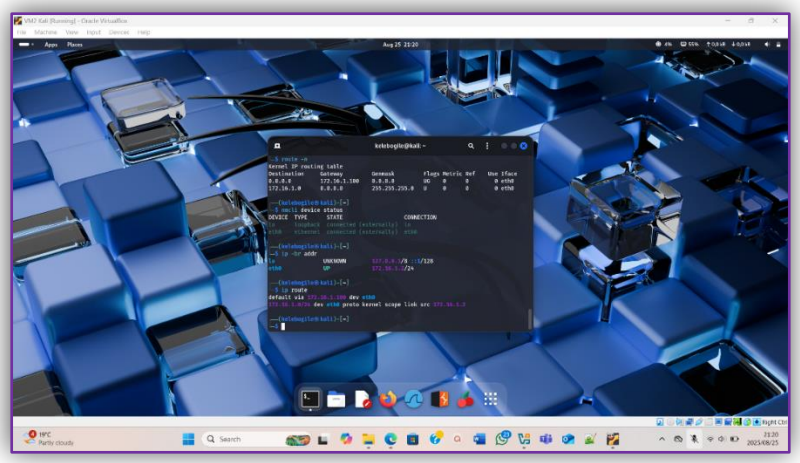






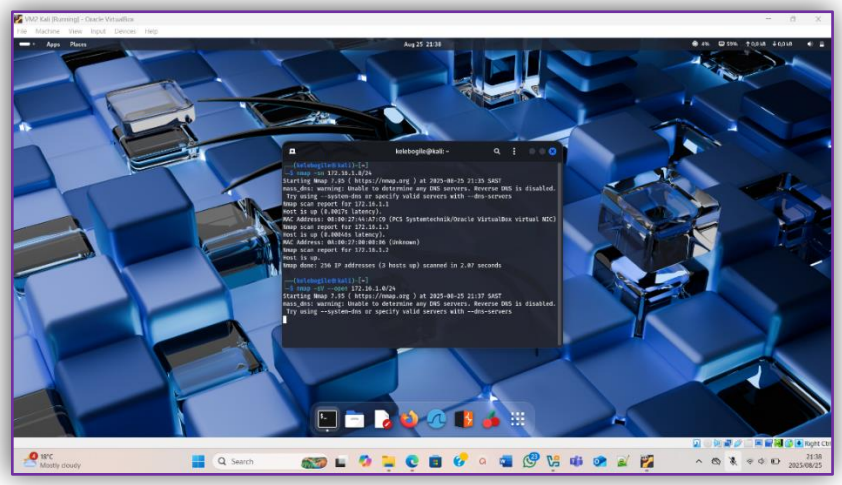
1.2. A) Check the devices connected to the Kali computer and display the default gateway.

The first code I ran was "**route -n**" which shows the routing table, I then ran the second code which is "**nmcli device status**", nmcli is the command-line tool that is used to manage Network Manager and device status is used to list all network devices and their current state and the code is for listing the network devices and which ones are connected. The third code I ran was "**ip -br addr**" which gives a short and cleaner summary of all network interfaces, and the last code I used was "**ip route**" to seem the default route and the local traffic.

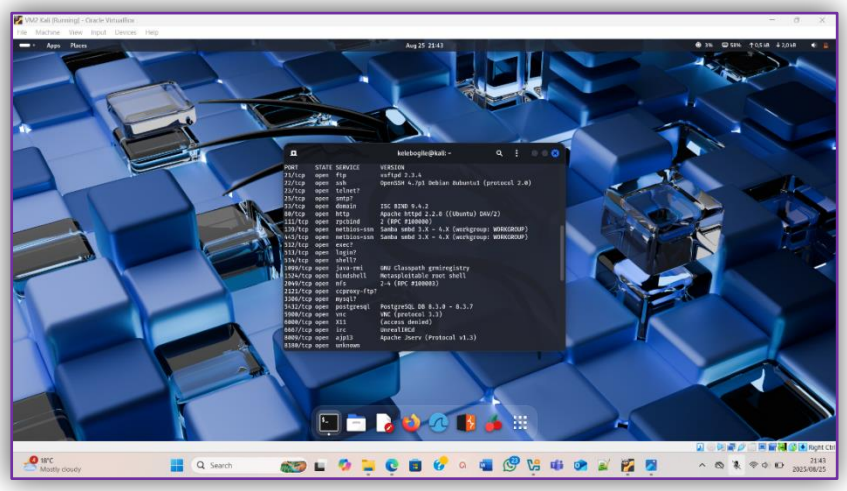


B) Scan the IP subnets on the network and confirm the number of hosts and open ports discovered.

The first code I ran was to find all live hosts on the network. The second code I ran was to scan for open ports on the hosts that I looked for. (TechyNoob, 2023)

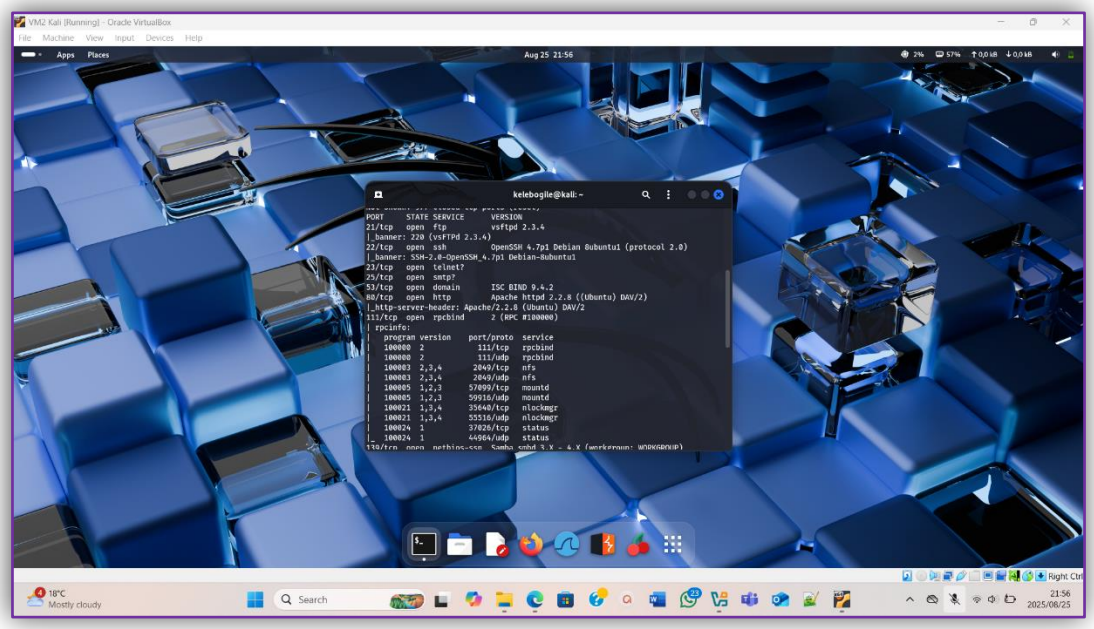


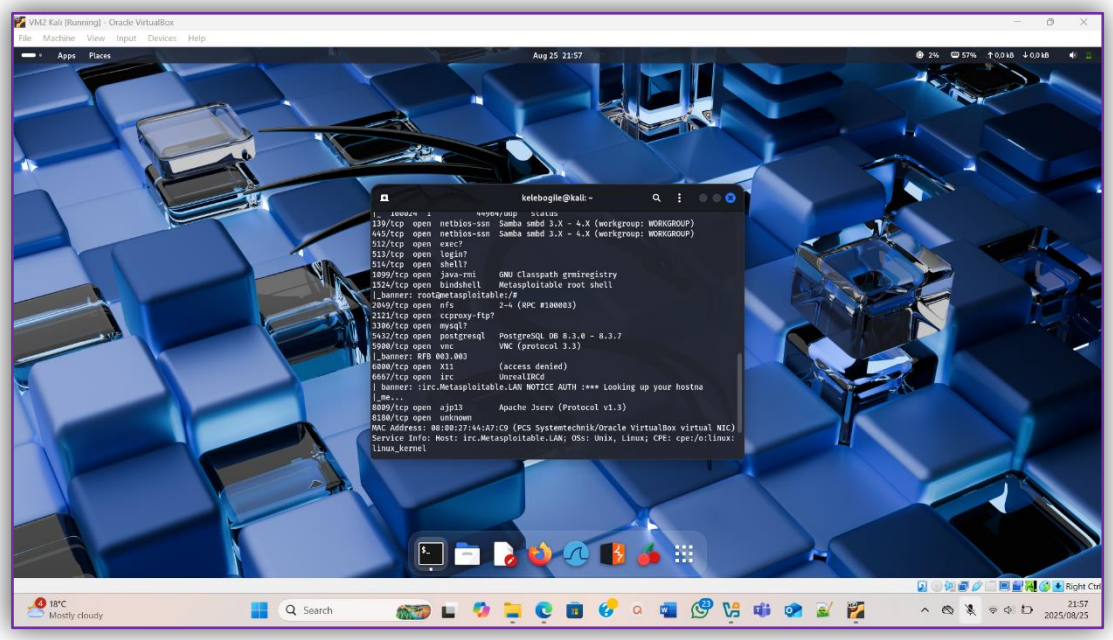
The following images are for the open ports I found on the hosts.



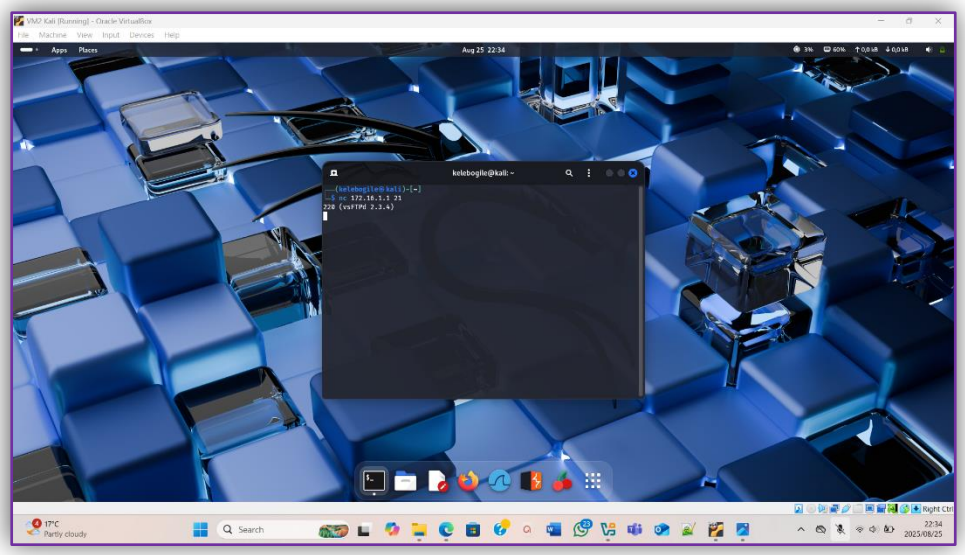
C) Perform a banner grab to check for potentially vulnerable machines on the network

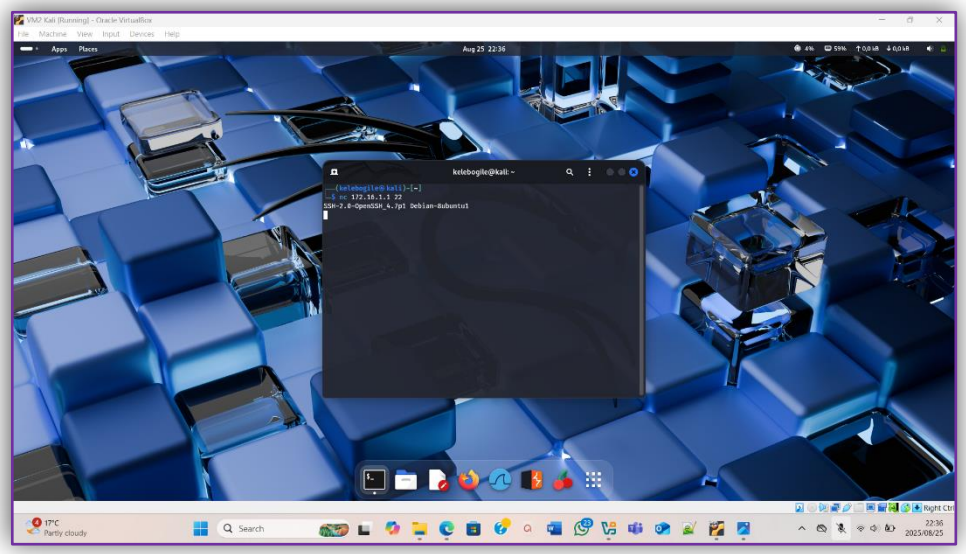
The first code I ran was "**nmap -sV - -script=banner - -open -n 172.16.1.1 -oN banners_quick.txt**", the -sV is for detecting versions (It grabs banners), the - -script=banner is for extra banner grabbing, the - -open shows open ports only, the -n is there to skip or remove the DNS warning and the -oN banners_quick.txt is there to save proof for the report. The following image shows the result from this command.

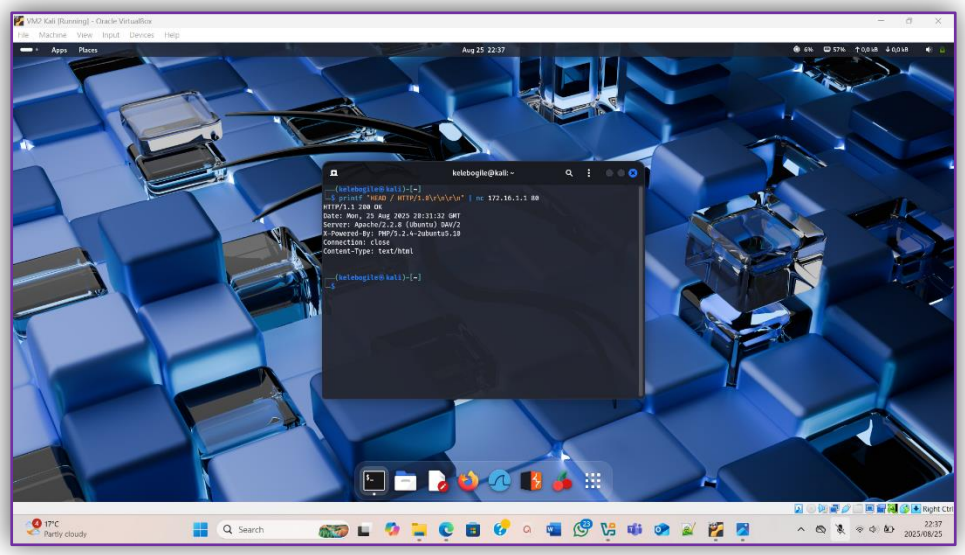




Once that was done, I then went ahead and ran "**nc 172.16.1.1 21**" which was for the manual banner grabbing, I also ran "**nc 172.16.1.1 22**", the last manual banner grab I did was with code **"printf "HEAD / HTTP/1.0\r\n\r\n" | nc -v 172.16.1.1 80**" which was for port 80. The number at the end shows the port number so I ran a manual banner grab for port 21, 22 and 80. The following images show the three banner grabs.


VM2 Kali [Running] - Oracle VirtualBox
Apps
Places
Aug 25 22:34
kelebogile@kali: ~
nc 172.16.1.1 21
220 (vsFTPd 2.3.4)
17°C
Partly cloudy
Search
22:34
2025/08/25

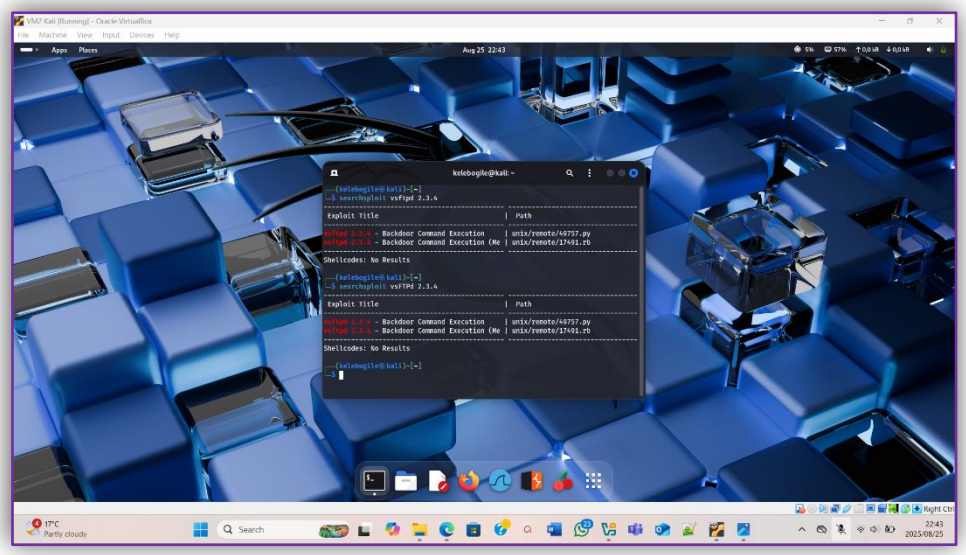

VM2 Kali [Running] - Oracle VirtualBox
Apps
Places
Aug 25 22:36
kelebogile@kali: ~
nc 172.16.1.1 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
17°C
Partly cloudy
Search
22:36
2025/08/25


VM2 Kali [Running] - Oracle VirtualBox
Apps
Places
Aug 25 22:37
kelebogile@kali: ~
printf "HEAD / HTTP/1.0\r\n\r\n" | nc 172.16.1.1 80
HTTP/1.1 200 OK
Date: Mon, 25 Aug 2025 20:31:32 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
17°C
Partly cloudy
Search
22:37
2025/08/25

I then started looking for the vulnerabilities which could possibly be present from the three manual banner grabs that I did by running the codes "**searchsploit vsftpd 2.3.4**" which was for port 21, "**searcgsploit OpenSSH 4.7p1**" which was for port 22 and "**searchsploit Apache 2.2.8**" which was for port 80.

The vulnerabilities that could possibly be present for port 21 according to the image are:

- It has a backdoor. A backdoor is a secret entrance left inside a program and that allows hackers to get inside with little to no permission.
- So, in this case if someone tries to log in using a username that contains a smiley face the program will secretly open a command shell.
- The command shell means that the attacker can type commands directly into the victim's computer as if they are the owner. This then gives the attacker complete control of the machine from anywhere.



The vulnerabilities that could possibly be present for port 22 according to the image are:

<u>Username Enumeration:</u>

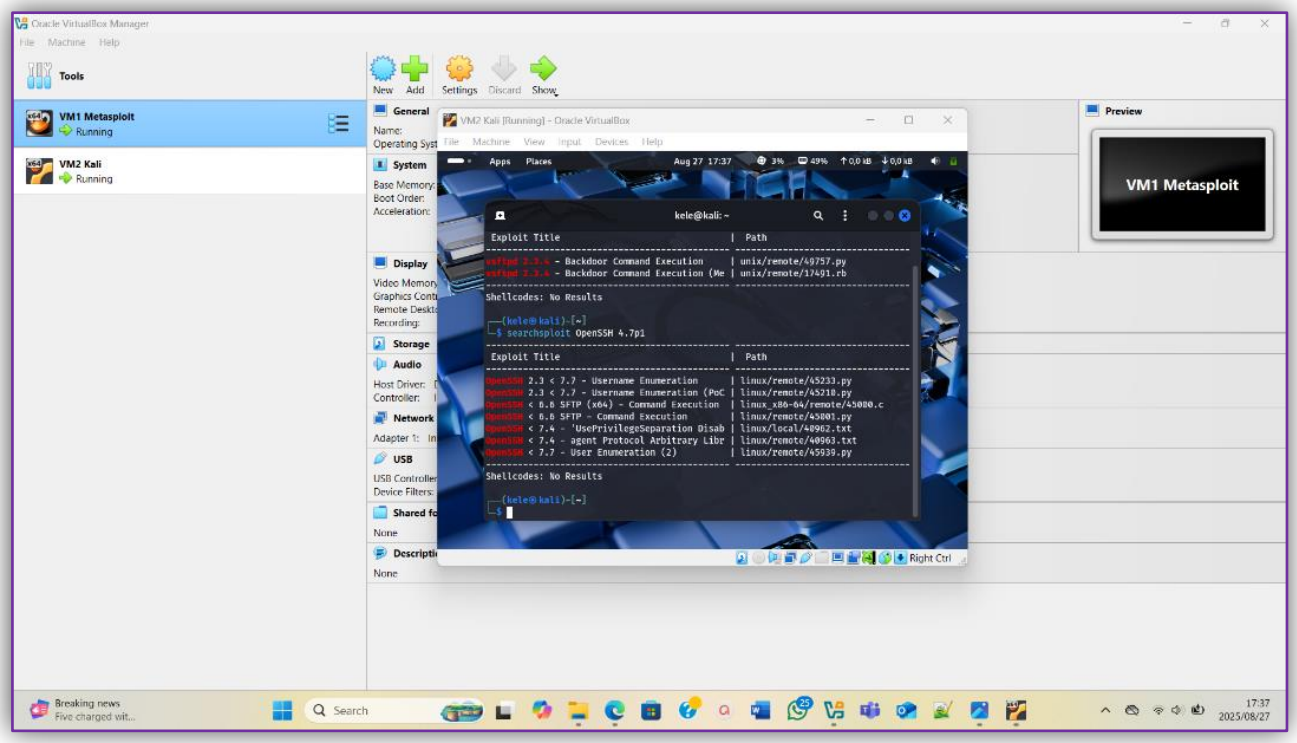
- If someone tries to log in with a wrong username, the system should not tell you whether the name exists and this version leaks that information which then means that an attacker can test many names and then finally figure out which accounts are real on the system and once the hacker knows real usernames his/her job becomes way easier.

<u>SFTP Command Execution:</u>

- SSH has an extra feature called SFTP which is used for transferring files and sometimes hackers can run actual system commands through SFTP. This can allow them to manipulate files or even take over parts of the system.

<u>Privilege Separation Bypass:</u>

- Normally, even if a hacker gets into SSH, the system tries to limit what they are able to do by putting them in a restricted zone. This bug allows them to escape that restricted zone and act like a more powerful user. This means attackers can discover accounts, and possibly upgrade their control once they are inside.



The vulnerabilities that could possibly be there for port 80 according to the image are:

Remote Code Execution through CGI/PHP:

- Some pages or scripts can be tricked into running malicious code. An attacker can place their own program on the server and run it, this then allows the attacker(s) to take full control of the website or even the whole server.

Denial of Service (DoS):

- Some weaknesses allow attackers to overload the server with requests; this makes the website crash or stop responding to real users.

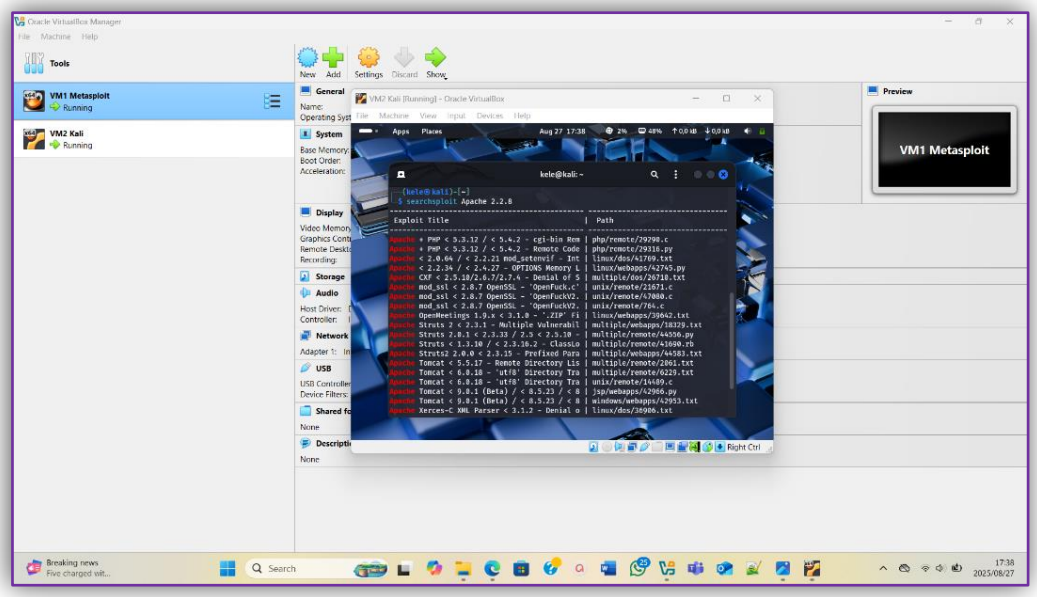
Directory Traversal:

- Normally, a website should only show the files inside its own folder, but with this bug, an attacker can move outside that folder and read sensitive files, such as /etc/password which contain system user details.

mod_ssl Exploits:

- If SSL (secure connection) is enabled, attackers can use flaws in the encryption system to run commands on the server.

Apache 2.2.8 can be abused to steal information, run malicious programs, or make the site go offline.



Therefore, Port 21 is very serious, because it gives instant remote access with a backdoor. Port 22 is medium to high risk, because attackers can gather usernames and possibly get stronger control, lastly but not least port 80 is very serious, because it can lead to data theft, denial of service, or even remote takeover of the web server.

1.3. What are at least three important factors that an attacker can use to compromise security?

Weak Passwords or Credentials:

Passwords and other authentication methods are the first line of defence in protecting systems and accounts. If users create weak or predictable passwords, attackers can gain access easily. Weak passwords aften include simple words, common phrases, or easily guessed patterns like “12345678” or “password”. Attackers exploit this through methods such as **brute force attacks,** where they systematically try all possible combinations, or **dictionary attacks**, which use lists of commonly used passwords. Beyond passwords, other credentials like security questions, PINs, or API keys can also be weak points. Many attacks succeed not because of sophisticated technology but because credentials are poorly managed, reused across multiple platforms, or never updated.

Once the attacker compromises credentials, they can access sensitive information, modify system settings, or impersonate users to launch further attacks, creating a chain of security breaches.

Software Vulnerabilities:

Every software application, operating system, or network device can have hidden flaws or weakness, known as vulnerabilities. Attackers actively search for these vulnerabilities to exploit them. These weaknesses can be caused by coding errors, outdated software, misconfigured systems, or failure to apply security patches. Examples include **buffer overflow, SQL injection**, and **cross-site scripting (XSS)**. Exploiting these vulnerabilities allows attackers to bypass normal security measures, install malware, gain administrative privileges, or steal sensitive data.

Vulnerabilities provide attackers with a direct pathway into systems without needing to trick users. The risk increases significantly when software is not updated regularly or when systems are exposed to the internet without proper protection. Attackers often use automated tools to scan for known vulnerabilities, meaning even less skilled attackers can take advantage of these weaknesses if they exist.

Human Error and Social Engineering:

Even the strongest technical security measures can fail if users are manipulated or make mistakes. Social engineering attacks exploit human psychology rather than technical flaws. Examples include **phishing emails**, where a user is tricked into providing login credentials, and **pretexting**, where an attacker poses as a trusted figure to gain sensitive information. Mistakes such as misconfiguring access permissions, clicking on malicious links, or accidentally sharing confidential data also create openings for attackers. Humans are often considered the "weakest link" in security because attackers can exploit trust, curiosity, or lack of awareness.

Social engineering can bypass technical defences entirely. An attacker who convinces an employee to reveal credentials or download malware can gain unrestricted access, making human error one of the most effective tools for compromising security.

Question 2

EDUVOS has recently implemented a new web application that handles sensitive customer data.

Describe the steps you would take to conduct a vulnerability assessment on this web application. Include specific tools and techniques you would use and explain how you would prioritise the vulnerabilities you identify.

Eduvos has created a new web application that stores and manages sensitive customer data. Since this information is private and vulnerable, it is important to test the application for weaknesses that hackers could use. This process is called a vulnerability assessment.

The first step in the assessment is to collect information about the application. This means finding out what the website is built on, such as the type of server and programming language, and looking at the pages where users put in information, like the login page or contact form. Tools like Nmap can check which services are running, while WhatWeb can show the technologies used. This step gives a clear picture of how the application works and where attackers might try to enter.

The second step is scanning the application for weaknesses. Automated tools like Nessus, OpenVas, and Nikto can look for problems such as outdated software or misconfigured servers. Other tools like OWASP ZAP and Burp Suite can test for issues in the application itself, for example weak login systems or unsafe input fields. This helps quickly find common problems,

After this, manual testing is done to look for more serious weaknesses that scanners may miss. Examples of these include SQL injection, where someone could access the database by entering malicious code in a form, and Cross-Site Scripting (XSS), where harmful scripts could run on a user's browser. Manual testing also checks if authentication (logins and sessions) can be bypassed. This ensures that all important risks are found.

The next step is to check security settings. This includes making sure the application uses HTTPS with proper certificates so that the information is encrypted, and checking that important security headers are in place to stop attacks like clickjacking. It also means ensuring that private files or admin pages are not open to the public. Tools like SSL Labs' SSL Test and SecurityHeaders.com are useful here.

Finally, the results must be prioritised. Not all problems are equally dangerous. High-risk issues, such as SQL Injection that can expose customer data, must be fixed immediately. Medium-risk problems, such as XSS, should be fixed soon after. Low-risk issues, such as missing headers, can be fixed later. This order makes sure that Eduvos has time to deal with the most serious threats first.

Inconclusion, a vulnerability assessment for Eduvos should follow a clear process: gather information, scan for weaknesses, do manual testing, check security settings, and prioritise the problems found. By doing this, Eduvos can protect sensitive customer data, reduce risks, and keep the trust of its customers.

AI Declaration

I carefully read the assignment instructions, and the extent to which AI may be used for the assignment.
I used the following AI system(s)/tool(s): I did not use any AI tool.
I used it for the following: I did not make use of any AI tool.
If I quoted or paraphrased an AI output, I have referenced the relevant tool, version, and the date I used the tool.
I still consider this work my own (i.e., I have not outsourced the final product, or significant portions of it, to AI tools/systems)
If required, I can defend my argument/perspective, explain my choices and approach, and can show that I am knowledgeable about the details of my work.

Bibliography

References

HackHunt. (2023, October 4). *How to Install METASPLOITABLE 2 in VirtualBox Kali Linux*. Retrieved from YouTube: https://youtu.be/l8v65ePR44k?si=fpvvzZlWNtCnWddt

SecDive. (2019, June 8). *How to assign an I.P. to Metasploitable-2 on VirtualBox (Windows 10)*. Retrieved from YouTube: https://youtu.be/kR_BiZZeXtw?si=T5G4YhrGPfQ7Xgt2

TechyNoob. (2023, October 30). *How to Use Nmap to Scan for Open Ports || Kali Linux Network Scanning*. Retrieved from YouTube: https://youtu.be/81gn-wEF_lQ?si=sOT88J8_30-RLOCW

Tips, I. T. (2025, June 1). *Configure Static IP Address and DNS on Kali Linux*. Retrieved from YouTube: https://youtu.be/hwrPQSPfDaA?si=t5oXst1M4Mc5XFxb