INTERNSHIP REPORT

Submitted by

RAHUL K
212221043006

In partial fulfilment for the award of the degree

Of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

SAVEETHA ENGINEERING COLLEGE

(AUTONOMOUS)ANNA UNIVERSITY: CHENNAI

600 025

APRIL/JUNE 2023

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Ethical Hacking

Ethical hacking, also known as, penetration testing or white-hat hacking, is the practice of testing computer systems, networks, and applications to identify vulnerabilities and weaknesses that might be exploited by malicious hackers. The objective of ethical hacking is to help organizations improve their security posture by identifying and remedying security issues before attackers can exploit them.

1.2 Types of Hackers

Hackers can be classified into three different categories:

1. Black Hat Hacker:

Black-hat Hackers are also known as an Unethical Hacker or a Security Cracker. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.

2. White Hat Hacker:

White hat Hackers are also known as Ethical Hackers or a Penetration Tester. White hat hackers are the good people of the hacker world. These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.

3. Grey Hat Hacker:

Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they do not have permission to test the security of the system but they will never steal money or damage the system. In most cases, they tell the administrator of that system. However, they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes.

1.3 Skills Required

An ethical hacker should have in-depth knowledge about all the systems, networks, program codes, security measures, etc. to perform hacking efficiently. Some of these skills include:

1. Knowledge of programming
2. Scripting Language
3. Networking Skills
4. Understanding of databases
5. Flexibility in using multiple platforms
6. Ability to use different tools available

1.4 Commonly Used Operating System (OS)

The most widely used operating system is Linux due to two primary reasons

1. Linux is open source
2. Linux can be easily modified or customized

Some widely used Linux Distros is the hacking community are:

1. Kali-Linux
2. Black-Arch Linux
3. Parrot-OS
4. Back-Box
5. Fedora Security Lab
6. ArchStrike

CHAPTER 2
INSTALLING AND SETTING-UP KALI LINUX

2.1 Downloading Virtual Box

To download Virtual Box, you will need to open up your Internet browser and go to the page (https:/www.virtualbox.org/wiki/Downloads). After entering into the page, choose the appropriate platform package. For the purpose of this demonstration, we will be downloading "Windows hosts" as highlighted in fig: 2.1.1.

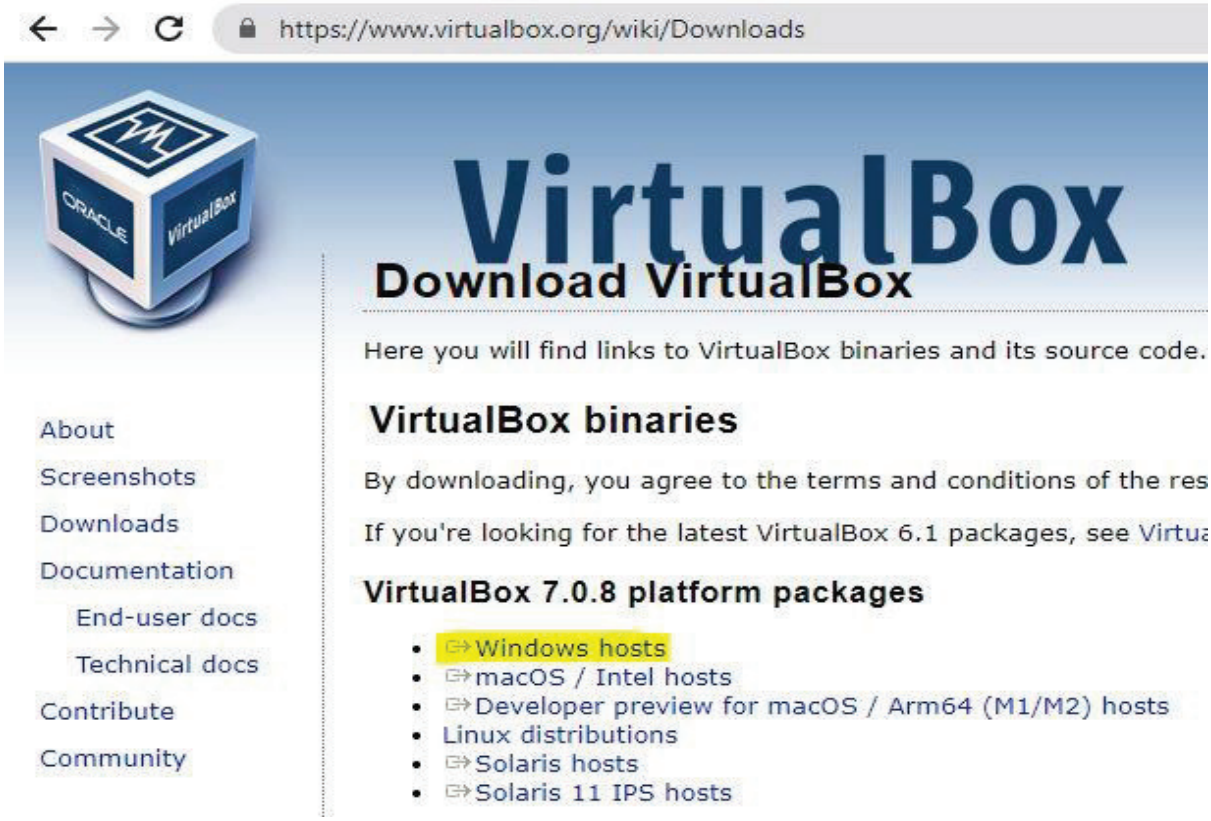

Fig: 2.1.1 VIRTUAL BOX DOWNLOAD LINK

Once you have clicked on that, the download process will start, it may take a few minutes to download. After downloading run the executable file and leave the all the settings at default and accept.

2.2 Downloading Kali Pre-Built Virtual Image

Go to the webpage (https://www.kali.org/get-kali/#kali-virtual-machines) to download the image. Choose the 64 or 32-bit option depending on your system specifications. Click on the Recommended VirtualBox image as shown in fig 2.2.1.

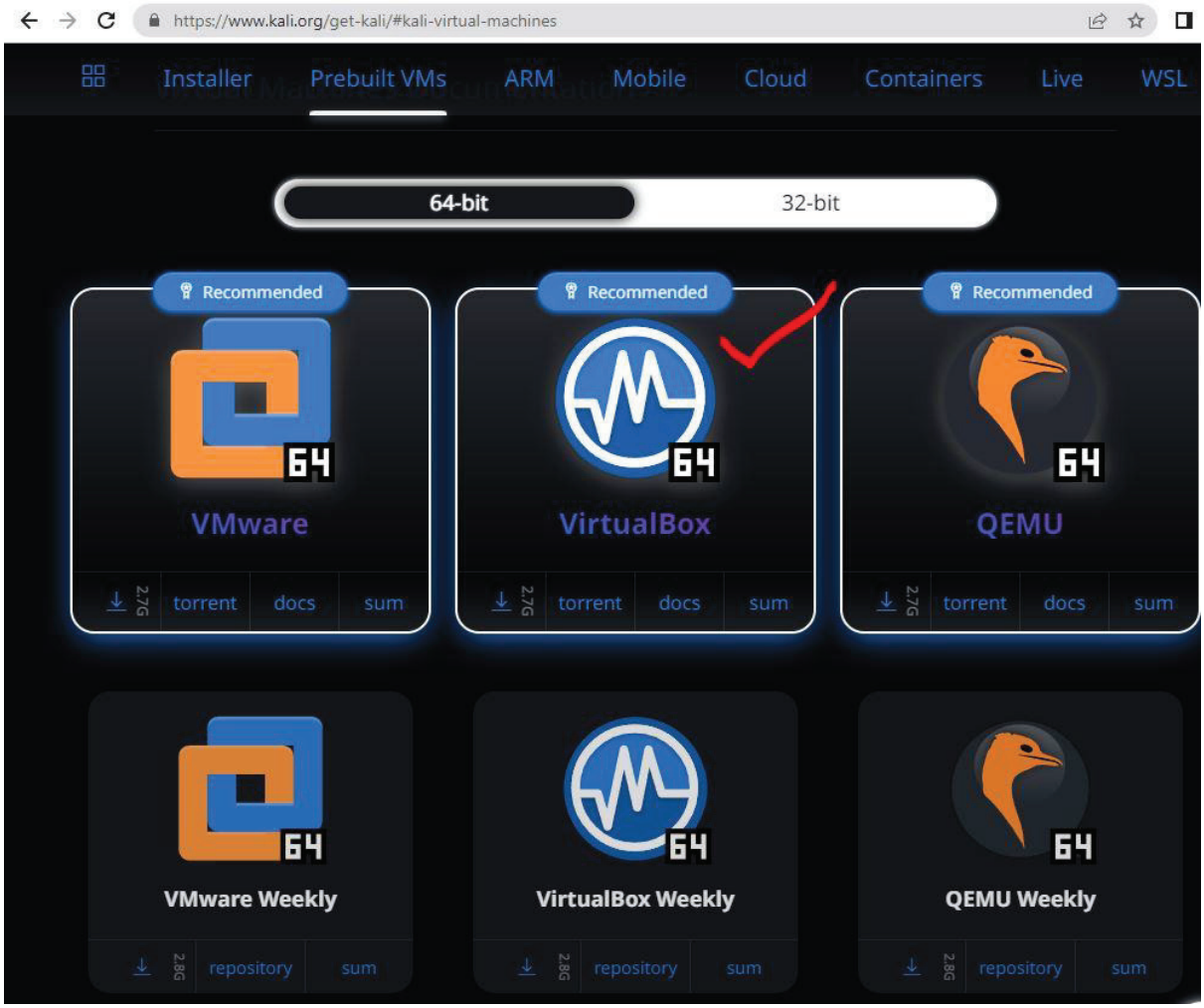

Fig: 2.2.1 KALI-LINUX DOWNLOAD LINK

Once clicked the download will start automatically, the download time may take anywhere from minutes to hours depending upon your internet speed due to size of file. Proceed to the next steps once download process is completed. After downloading extract, the contents from the zip file.

2.3 Setting-up Kali

After extracting there will be a folder created, in it there will be a pre-built image click on it and open it with virtual box as shown in fig 2.3.1.

Fig: 2.3.1 KALI-LINUX PREBUILT IMAGE

After successful installation kali-linux will appear in virtual box as shown in fig 2.3.2

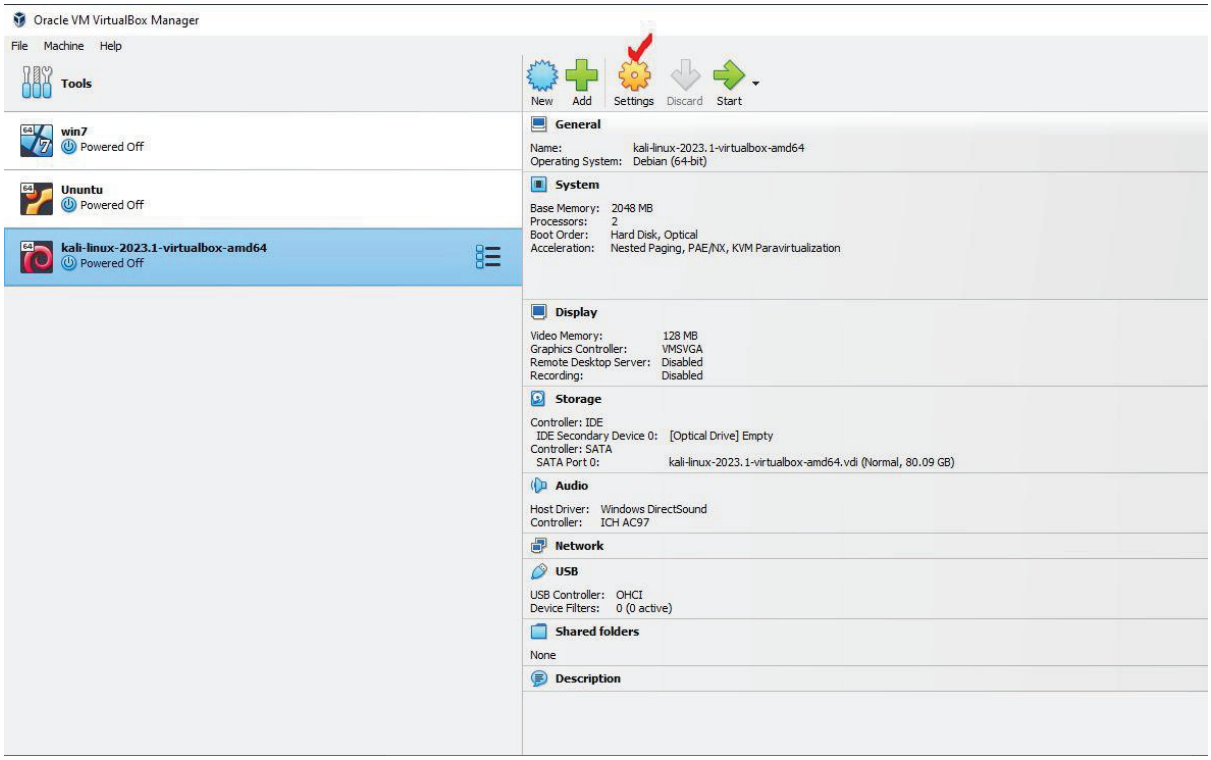

Fig: 2.3.2 VIRTUAL BOX SETTINGS

Now click on the settings option to configure the specifications of the virtual machine. Once clicked it will open a tab as shown in fig 2.3.3

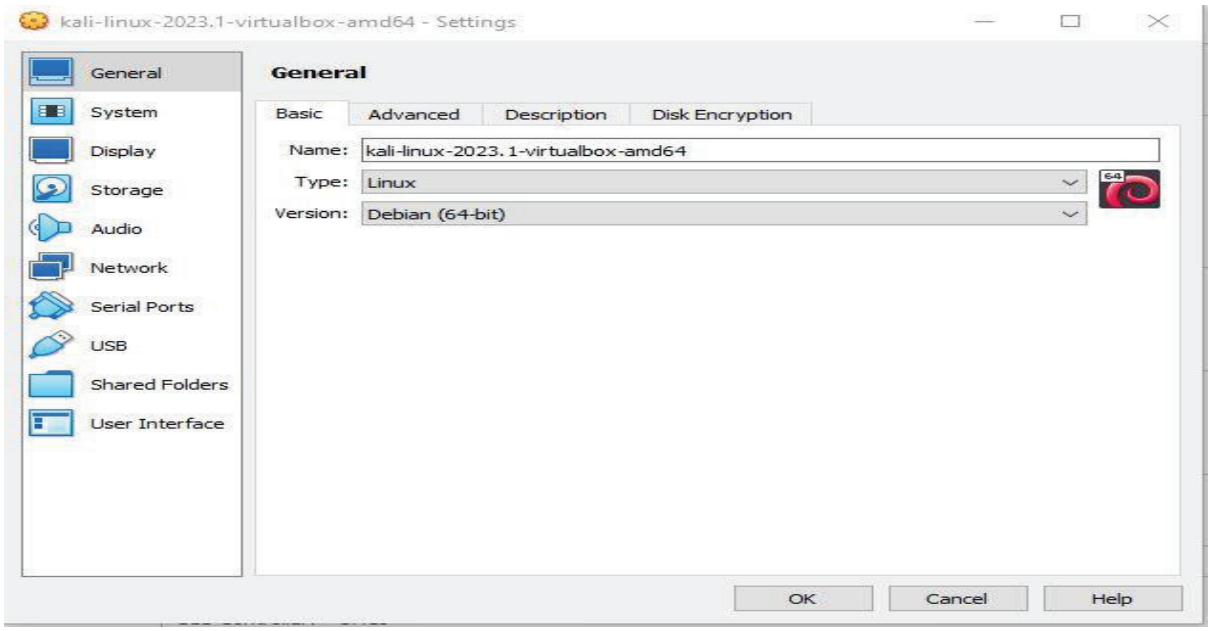

Fig: 2.3.3 GENERAL SETTINGS

Select the system settings and under motherboard settings set the base memory to a minimum of 4GB or higher if your system allows it as shown in fig 2.3.4.

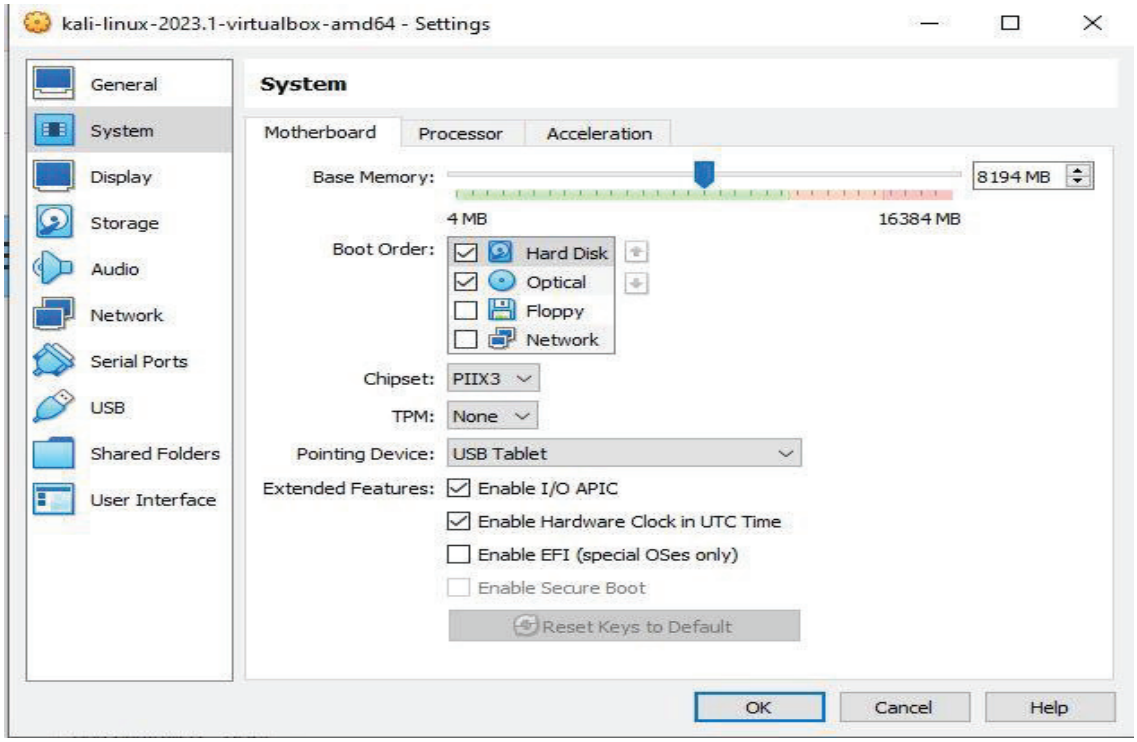

Fig: 2.3.4 SYSTEM SETTINGS

Under processor, settings select the number of CPUs allowed by your system higher number of CPUs improves performance as shown in fig 2.3.5.

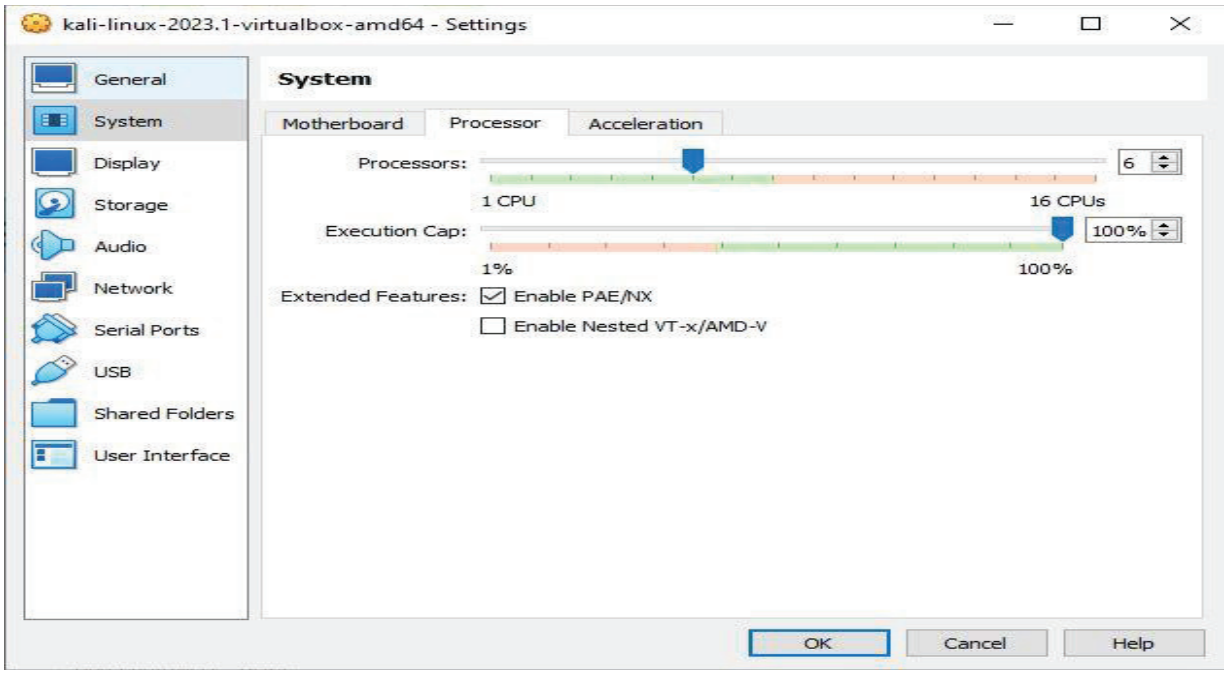

Fig: 2.3.5 PROCESSOR SETTINGS

Now move on to display settings and set video memory to the maximum allowed by your system and enable "3D Acceleration" feature if present as shown in fig 2.3.6 and keep the rest at default.

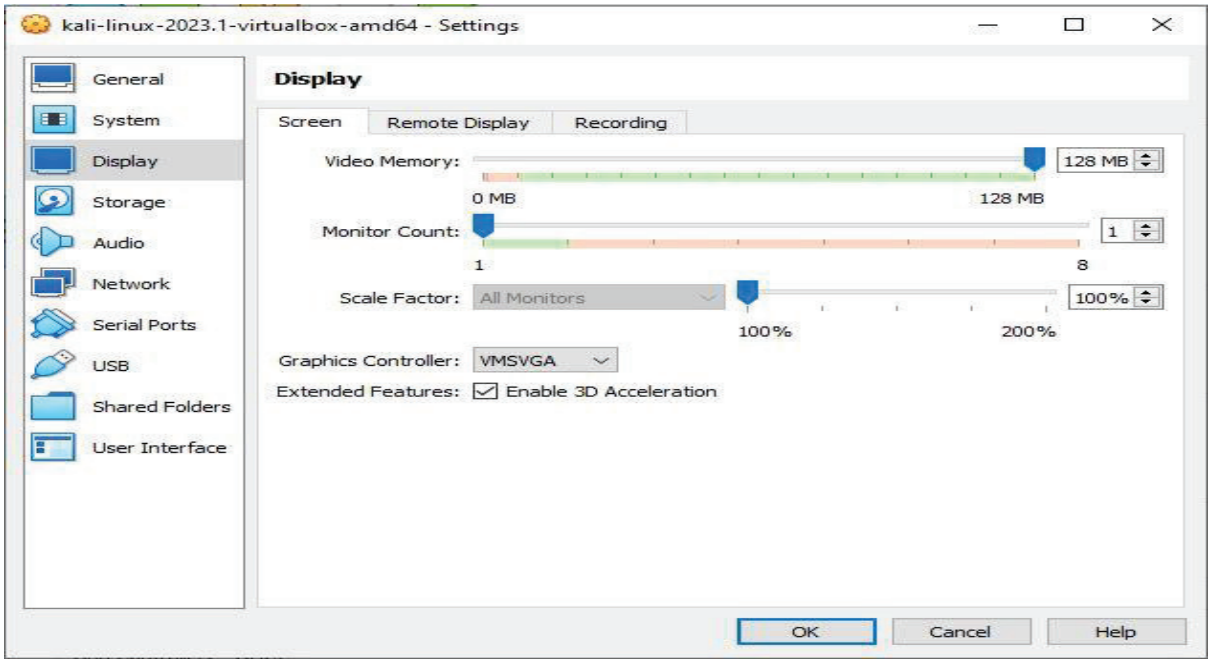

Fig: 2.3.6 DISPLAY SETTING

Next to the network settings set the network adapter to “NAT” or “Bridged Adapter” depending on your needs for security purposes, I will be choosing the “NAT” option as shown in fig 2.3.7.

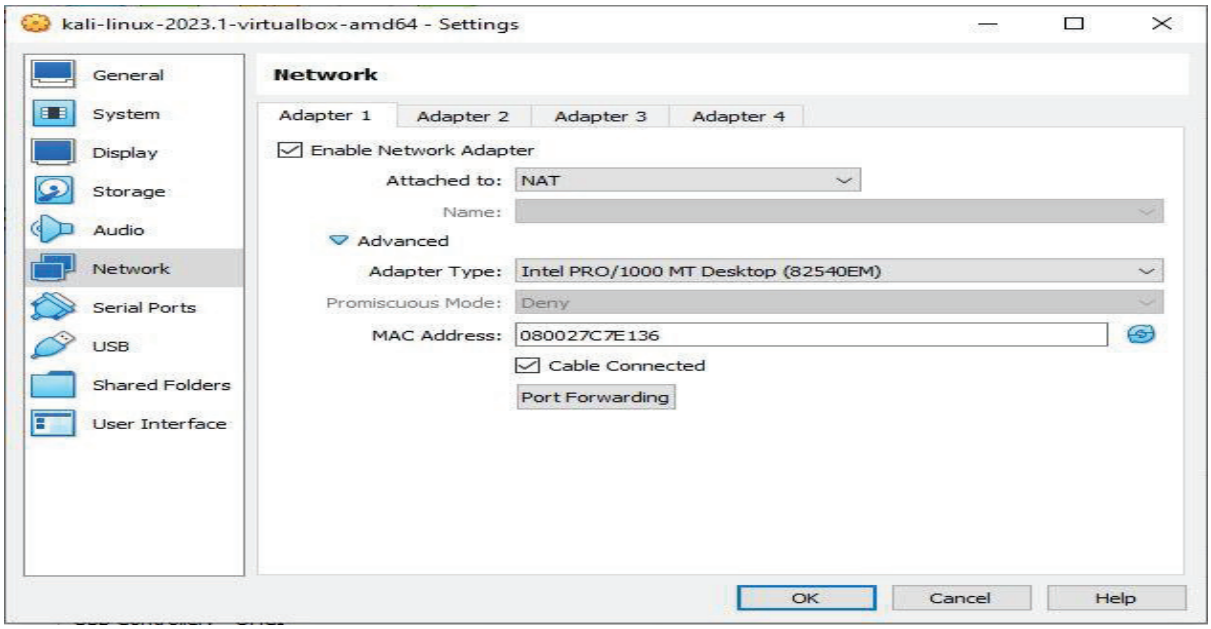

Fig: 2.3.7 NETWORK SETTINGS

After configuring your settings click ok and select the “start” button as shown in fig 2.3.8 to start the virtual machine.

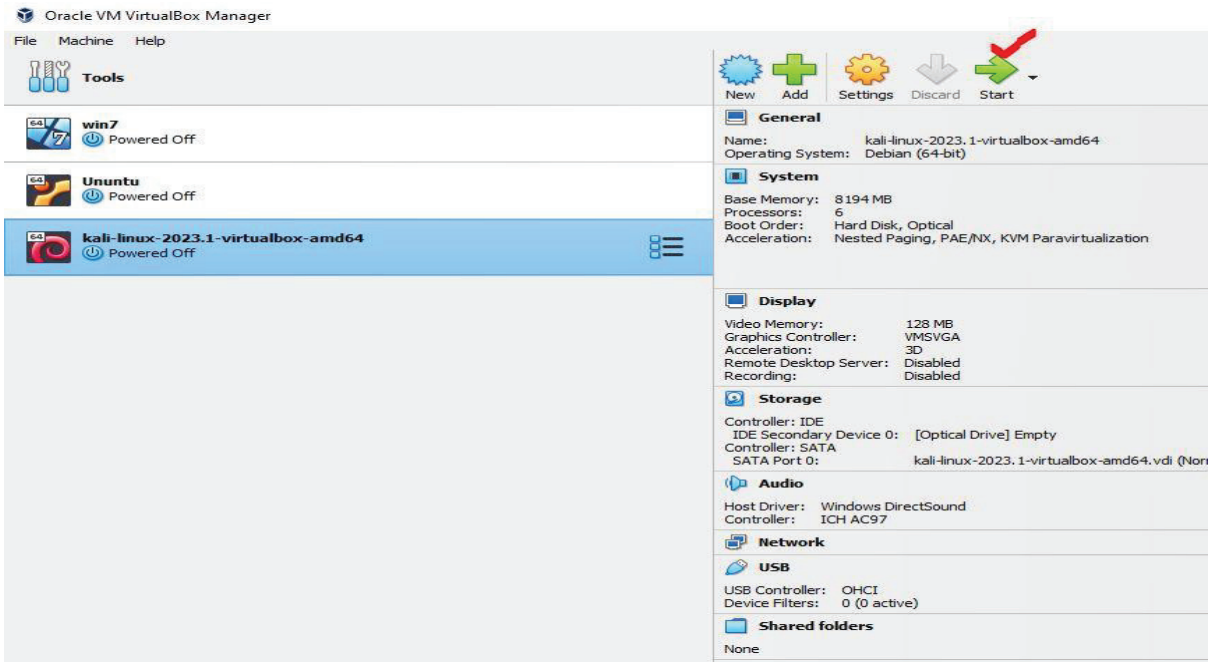

Fig: 2.3.8 STARTING KALI-LINUX

2.4 Booting Kali

After successfully completing the previous steps, a new window will open with kali linux running on it and we will get to the login page as shown in fig 2.4.1.

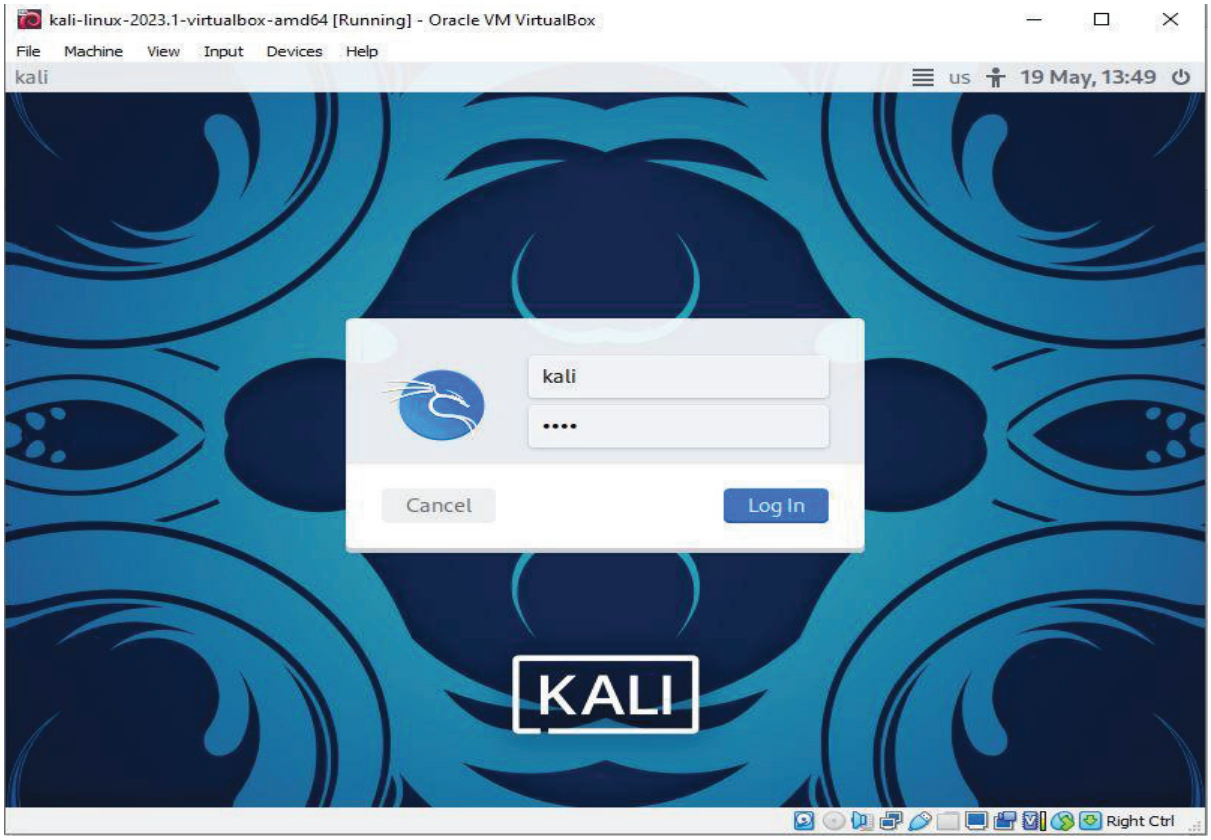

Fig: 2.4.1 KALI-LINUX LOGIN

The default username and password is "kali", use these credentials to login to the system after a successful login run the following command "sudo apt-get update && sudo apt-get dist-upgrade -y" in the terminal to update the OS to the latest version and features as shown in fig 2.4.2. The upgrade may take a few hours depending on your internet speed.

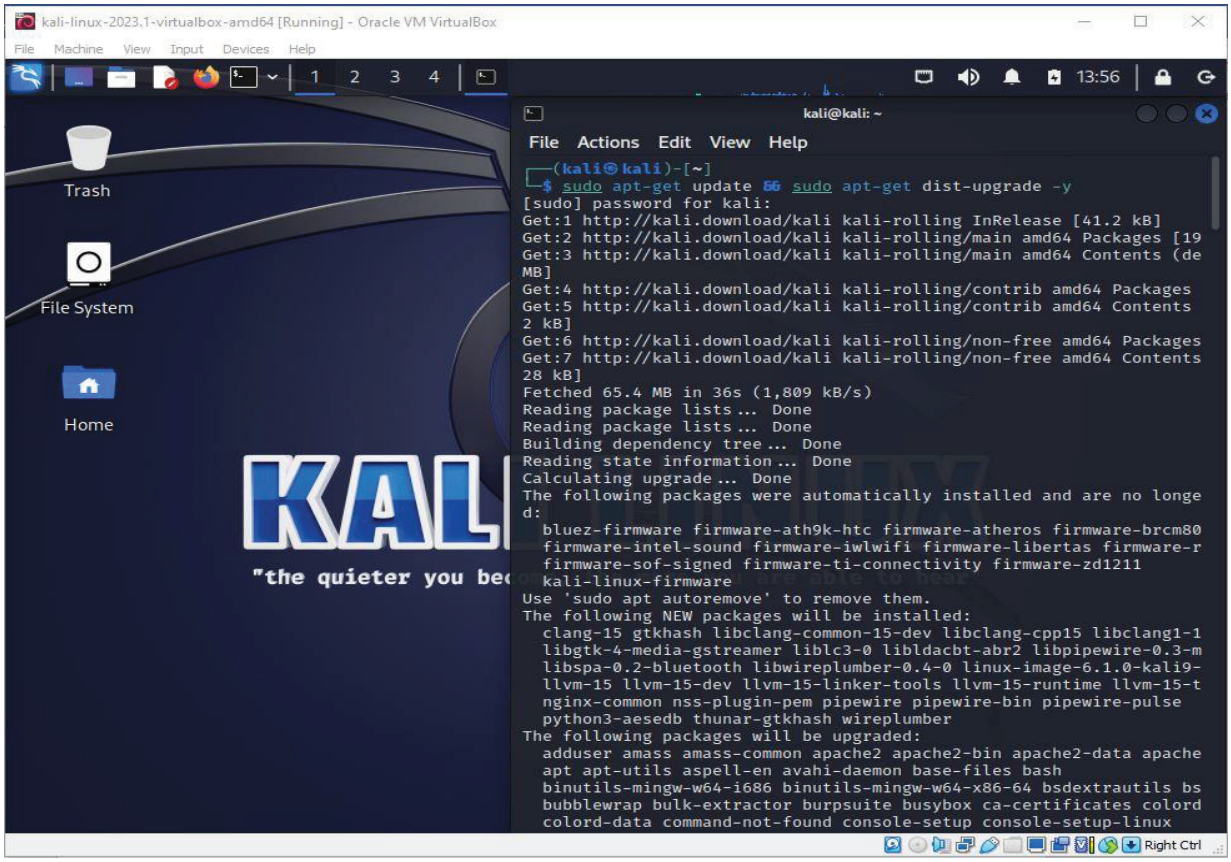

Fig: 2.4.2 SYSTEM AND DISTRO UPGRADE

After the upgrade process is completed, we can use the machine to for ethical hacking purposes

NOTE: If any errors or anomalies occur during the installation process at any step in chapter-2, please visit the "kali docs" for more information.

CHAPTER – 3
HACKING METHODOLOGIES

3.1.1 Introduction

Ethical Hacking is a repetitive and systematic process, which is followed continuously in order compromise systems or networks. The process are as follows:

1. Information Gathering
2. Vulnerability Assessment
3. Exploitation
4. Post-Exploitation

All phases of hacking use these four main process.

In this chapter, we will be looking through each of the process in details with some tools and examples.

3.2 Information Gathering

Information gathering is a crucial phase in ethical hacking. It involves gathering relevant data and intelligence about a target system, network, or organization in order to identify vulnerabilities and potential entry points that could be exploited.

The goal of information gathering is to obtain as much information as possible about the target, including its infrastructure, technologies, security controls, and potential weaknesses. This information helps ethical hackers understand the target's security posture and aids in the development of effective attack strategies.

Information gathering can be broadly categorized into two main types:

1. Passive reconnaissance
2. Active reconnaissance

3.2.1 Passive Reconnaissance

Passive reconnaissance involves gathering information without directly interacting with the target. It includes techniques such as browsing public websites, searching for publicly available information, analyzing social media profiles, and reviewing public documents. This approach aims to collect as much information as possible without alerting the target organization.

Some tools and techniques used are:

1. whois

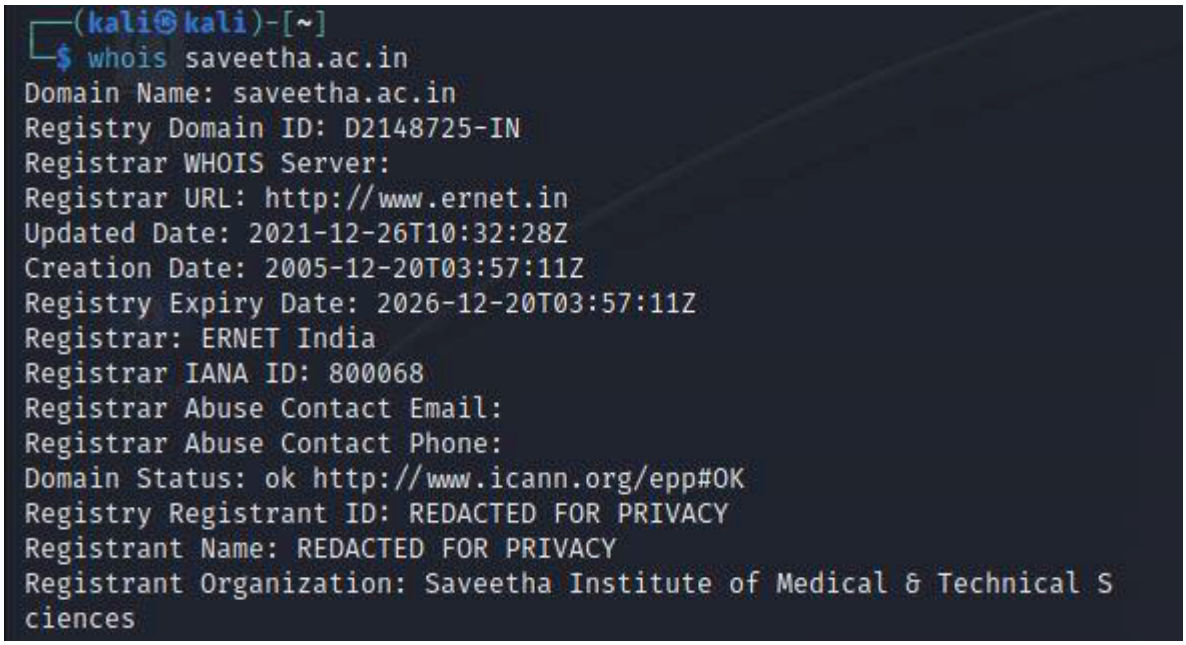

Fig: 3.2.1.1 WHOIS EXAMPLE

whois tool is used to find information regarding a particular website as shown in the fig 3.2.1.1 we get some information about our target website.

2. Wayback machine (https://archive.org/web)

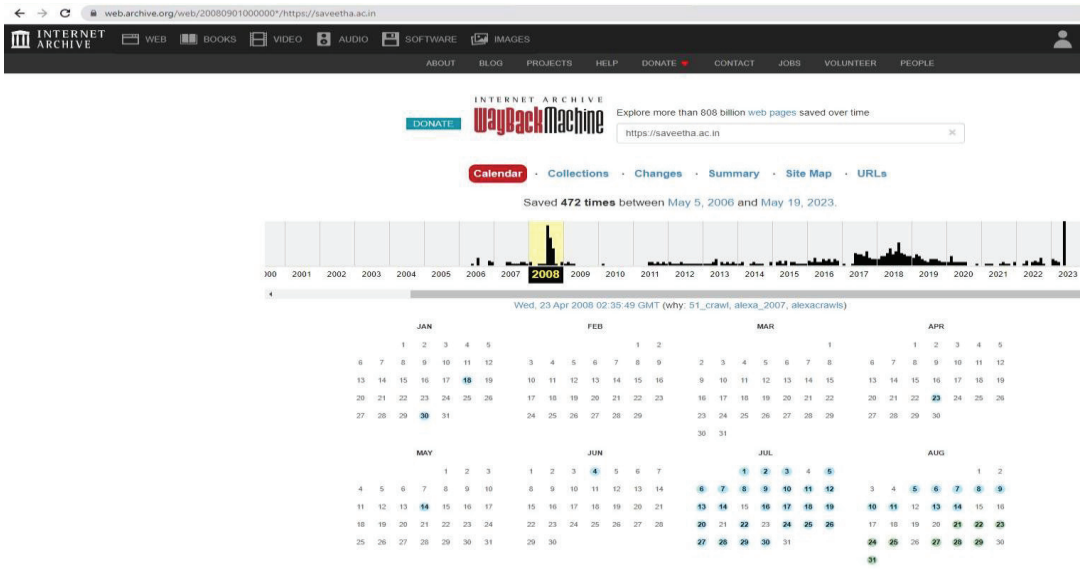

Fig: 3.2.1.2 WAYBACK MACHINE LINK

The wayback machine or the internet archive contains snapshots of the past and current activities of monitored websites as shown in fig 3.2.1.2 we get information from 2006 – 2023 information about a website.

3. Open Source Intelligence (Looking at Source Code)

```
┌──(kali㉿kali)-[~/test]
└─$ curl https://saveetha.ac.in > test.txt ; cat test.txt | tr " " "\n" | cut -d'"' -f2 | grep "https\|.php" | sort -u > test.txt | wc -l ; cat test.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 88095    0 88095    0     0   135k      0 --:--:-- --:--:-- --:--:--  135k
129
document,'script','https://connect.facebook.net/en_US/fbevents.js');
https://admissions.saveetha.ac.in/
https://api.whatsapp.com/send?phone=+918939902737
https://chatbot.in1.nopaperforms.com/en-gb/backend/bots/niaachtbtscpt.js/5075f35478c51e72/12e5eb13c5bf453fb1fb055b0cb9f33a
https://docs.google.com/forms/d/e/1FAIpQLSc9HIDGhvnteoOHJ6tRti6takm-xT4H846tz1Enw7D76Odb5A/viewform
https://docs.google.com/forms/d/e/1FAIpQLSeKs4u-P3kadjULnSE94_ybh6mWFEujm_UzUYCJmD_YjQ4-IQ/viewform?c=0&amp;w=1
https://forms.gle/18NMnHzV1od1LwRJA
https://in.pinterest.com/saveethaengineering/pins/
https://mail.saveetha.ac.in/
https://niaa.nopaperforms.com/npfchtbtscpt.js?t=
'https://saveetha.ac.in/';
https://saveetha.ac.in
https://saveetha.ac.in/
https://saveetha.ac.in/index.php/life-at-sec/academic-life/coe-blogs
```

Fig: 3.2.1.3 OSINT EXAMPLE

As shown in the fig 3.2.1.3, we were able to gather subdomains, directories, and other links of a website from their html page. We have also found that this website uses php.

3.2.2 Active Reconnaissance

Active reconnaissance, on the other hand, involves more direct interactions with the target. This includes techniques like network scanning, port scanning, fingerprinting services and applications, and conducting vulnerability scans. Active reconnaissance can provide more detailed information about the target's infrastructure, network topology, and potential vulnerabilities.

Some tools used are:

1. Waapalyzer

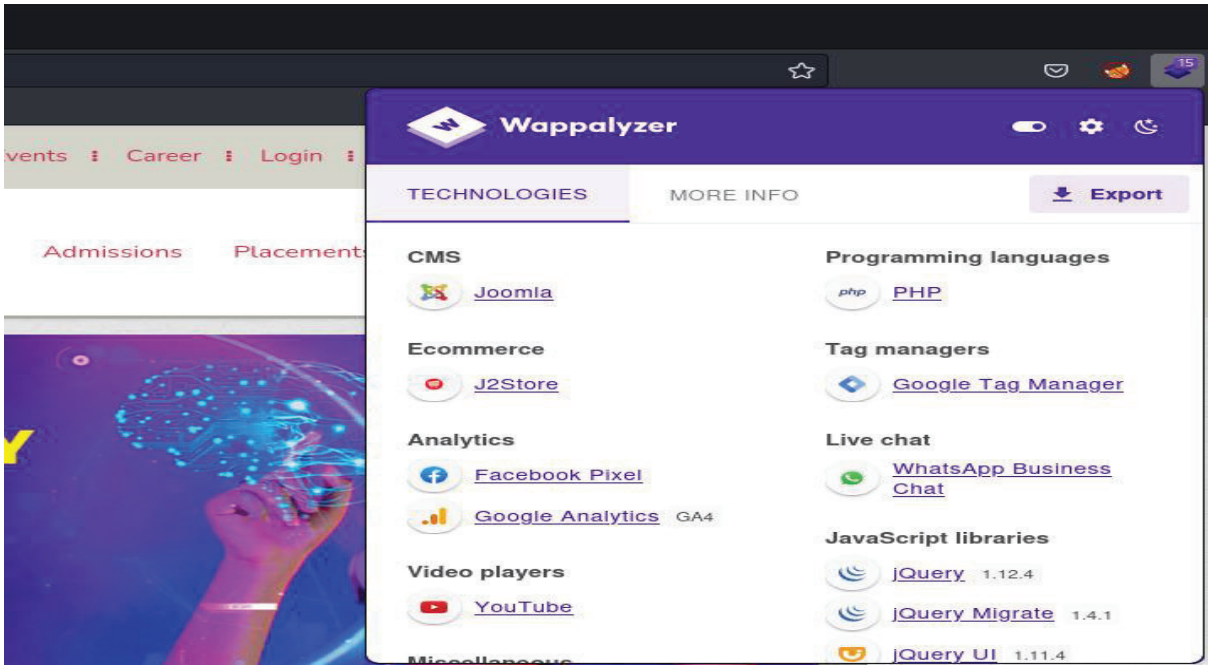

Fig: 3.2.2.1 WAPPALYZER EXAMPLE

From fig: 3.2.2.1 we are using the waapalyzer extension to search the website In addition, it has found Joomla a cms software, which means we can try to find its login page.

2. Netcraft

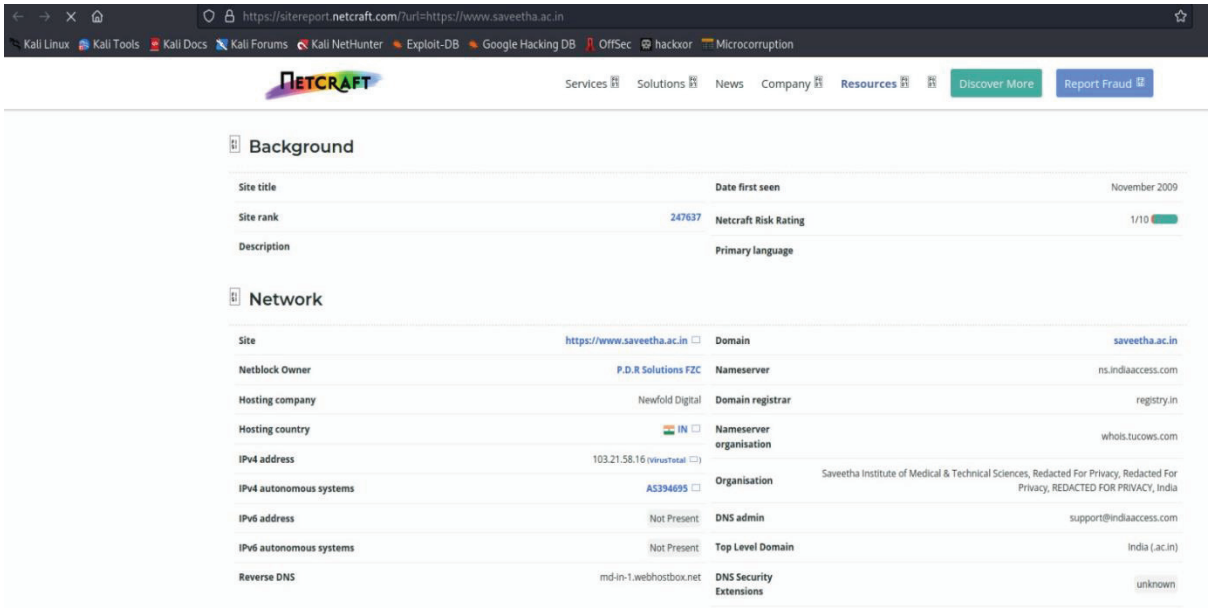

Fig: 3.2.2.2 NETCRAFT EXAMPLE

From the fig: 3.2.2.2 we can gather information like IPv4 address, domain name, location and other details, which are accurate. This information is used to further dig deeper and find more information about our target.

3.3 Vulnerability Analysis

Vulnerability assessment is a crucial aspect of ethical hacking that involves identifying and evaluating vulnerabilities within a target system, network, or application. It aims to provide organizations with insights into potential weaknesses that could be exploited by malicious actors.

The primary goal of vulnerability assessment is to systematically assess the security posture of the target and identify any vulnerabilities that may exist. This assessment helps organizations understand their exposure to potential threats and respond appropriately to mitigate risks.

3.3 Exploitation

Exploitation is a critical phase in ethical hacking that involves the deliberate and controlled use of identified vulnerabilities to gain unauthorized access or control over a target system, network, or application. It is an essential step to demonstrate the impact of the vulnerabilities and assist in the mitigation process.

The goal of exploitation in ethical hacking is to validate the existence and severity of identified vulnerabilities, understand their potential impact, and provide concrete evidence to support the need for remediation. This phase helps organizations realize the potential consequences of leaving vulnerabilities unaddressed and reinforces the importance of implementing appropriate security measures.

3.4 Post-Exploitation

Post-exploitation is a critical phase in ethical hacking that occurs after successfully gaining unauthorized access or control over a target system, network, or application. It involves further exploration and actions taken by ethical hackers to gather intelligence, escalate privileges, and maintain persistence within the compromised environment.

The goal of post-exploitation in ethical hacking is to maximize the impact of the initial exploit and understand the full extent of the compromised system or network. This phase helps ethical hackers assess the potential damage that could be caused by an attacker and provides valuable insights to assist in the remediation process.

During the post-exploitation phase, ethical hackers typically perform the following activities:

1. System Reconnaissance: Ethical hackers explore the compromised environment to gather additional information about the target system, network architecture, installed software, user accounts, and other relevant details.

2. Privilege Escalation: Ethical hackers attempt to elevate their privileges within the compromised environment. They search for vulnerabilities or misconfigurations that could allow them to gain higher levels of access, such as administrative privileges or system-level control.

3. Maintaining Access: Once ethical hackers have full control of the system they may run certain scripts in the target system to allow remote control access to the ethical hacker, so he does not have to repeat the exploitation steps again.

4. Lateral Movement: Once elevated privileges are obtained, ethical hackers may move laterally across the compromised environment. This involves exploring other systems, devices, or network segments within the organization to expand their control and gather additional information.

5. Data Exfiltration: In some cases, ethical hackers may extract sensitive data from the compromised system or network. This step helps organizations understand the potential impact of a successful attack and the types of information that could be at risk.

6. Reporting: Ethical hackers document their findings and prepare a detailed report that outlines the activities performed during post-exploitation, the compromised systems or network segments, the potential damage or exposure, and recommended remediation measures.

CHAPTER – 4
PRACTICAL DEMONSTRATION

4.1 Introduction

In this practical demonstration, we will see how ethical hackers use the above-explained hacking methodologies to compromise a system. We will be using "tryhackme" an online learning platform for aspiring ethical hackers where we can practice our skills using vulnerable boxes.

For this demonstration, we will use a box named Pickle Rick a very easy box themed around a children's cartoon named "Rick and Morty"

Note: The box is works in a capture the flag or ctf manner, where after finding and exploiting vulnerabilities we will obtain flags, which are secured or hidden. Our goal is to obtain such flags and submit it to gain points.

4.2 Tryhackme Box: Pickle Rick

Connecting to the lab network.

Ctf boxes are kept in virtual private networks, which cannot be accessed by the internet and can only be accessed through a vpn. So first, we will download and connect to the vpn config file and access the machine.

Once connected to the virtual network it will show a successful connected as shown in fig: 4.2.1

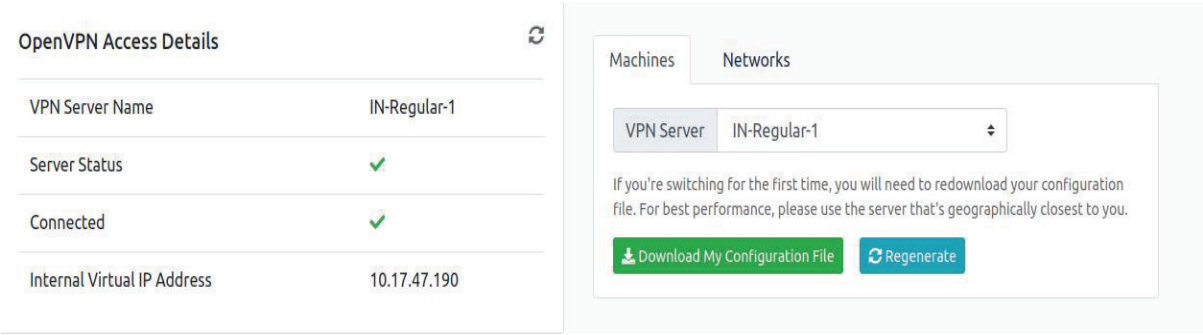

Fig: 4.2.1 VPN CONNECTION STATUS

Now the first step in hacking a box is the "**INFORMATION GATHERING**" step, let us see what type of information are provided for this challenge.

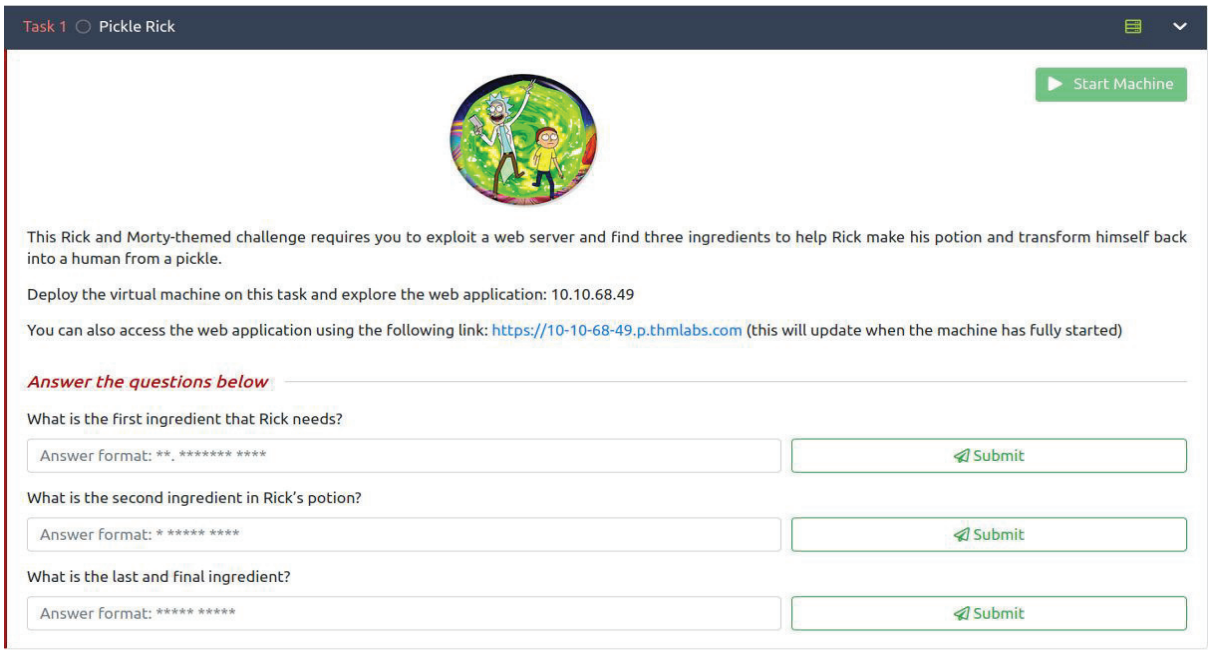

Fig: 4.2.2 TRYHACKME CHALLENGE

In fig: 4.2.2 we are given an ip address and a website link let us see what type of info we can gather using an nmap scan on the provided ip address.

```
└─$ sudo nmap -sV -sC  10.10.68.49
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-20 03:37 IST
Nmap scan report for 10.10.68.49
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 58a28bb38dc09ef82d81b520f7d87f25 (RSA)
|   256 d64e3441917135f8d4ad90d006eb6464 (ECDSA)
|_  256 ad83c8fea862d59f2d76648b3e5cdbef (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Rick is sup4r cool
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.77 seconds
```

Fig: 4.2.3 NMAP SCAN RESULTS

From fig 4.2.3 we can see that there are 2 open ports 22 and 80, which means ssh and an http service is running on the machine, additionally we also find the system running web server is a linux machine. Now we know that a web server is running lets visit the webpage.

Now let us go to the target's webpage. It looks like fig 4.2.4.

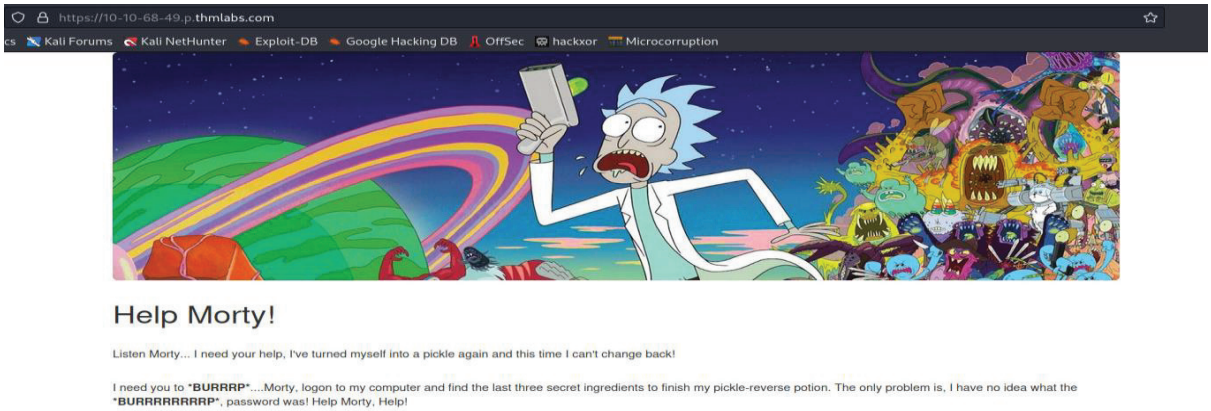

Fig: 4.2.4 TARGET WEBPAGE

After analyzing the website there really is not much, there are no hyperlinks or login pages nothing. At times like this, it is always important to go through the source code, because sometimes developers might leave some sensitive information during the development process.

```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
  <style>
  .jumbotron {
    background-image: url("assets/rickandmorty.jpeg");
    background-size: cover;
    height: 340px;
  }
  </style>
</head>
<body>

  <div class="container">
    <div class="jumbotron"></div>
    <h1>Help Morty!</h1></br>
    <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></br>
    <p>I need you to <b>*BURRRP*</b>....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion.
    I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Help!</p></br>
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRu13s

  -->

</body>
</html>

```

Fig: 4.2.5 WEBPAGE SOURCE CODE

From fig 4.2.5 we see that a username of "R1ckRu13s" in the source code. Now we have to find a login page where we can try to brute-force or try some passwords to login to the system.

Let us also look at Waapalyzer a web extension to see what the webpage run on as shown in fig 4.2.6.

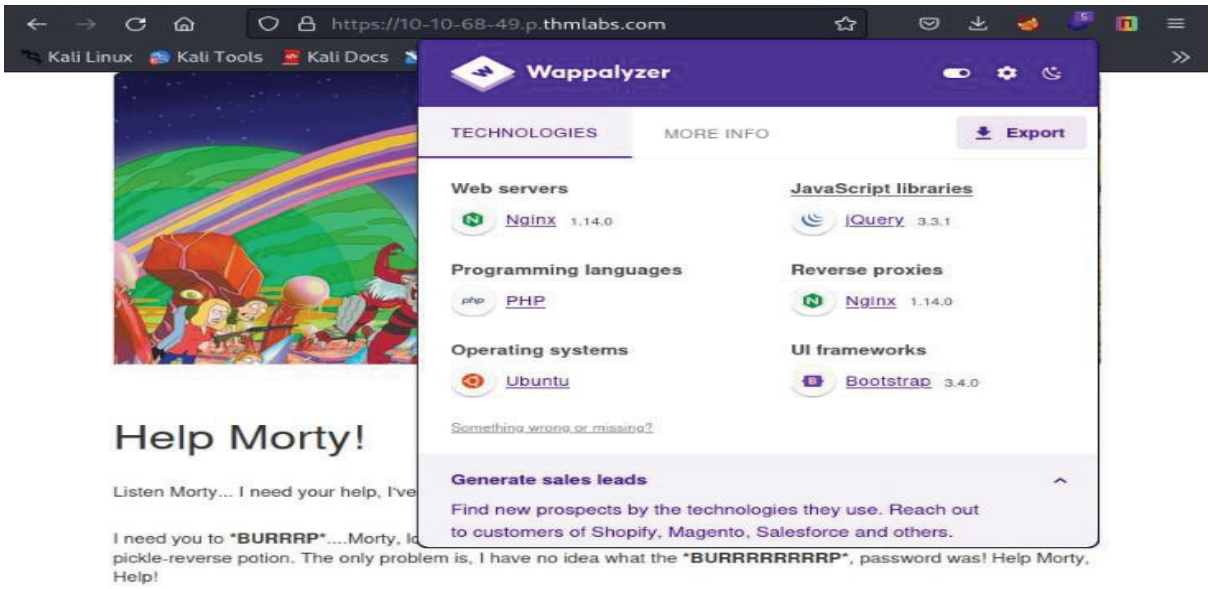

Fig: 4.2.6 WAPPALYZER RESULTS

From Waapalyzer we see that this website uses php. Now let us try the login and other hidden directories in the website.

To find hidden directories in a website we will be using a tool called gobuster, which can bust directories.

```
└─$ sudo gobuster dir -u https://10-10-68-49.p.thmlabs.com/ -w /usr/share/wordlists/seclists/Discovery/Web-Content
/big.txt -x php
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10-10-68-49.p.thmlabs.com/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2023/05/20 04:05:52 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 309]
/.htpasswd            (Status: 403) [Size: 309]
/.htaccess.php        (Status: 403) [Size: 313]
/.htpasswd.php        (Status: 403) [Size: 313]
/assets               (Status: 301) [Size: 339] [--> http://10-10-68-49.p.thmlabs.com/assets/]
/denied.php           (Status: 302) [Size: 0] [--> /login.php]
/login.php            (Status: 200) [Size: 882]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 313]
Progress: 40951 / 40954 (99.99%)
===============================================================
2023/05/20 04:22:37 Finished
===============================================================
```

Fig: 4.2.7 GOBUSTER RESULTS

From fig 4.2.7. we can see that gobuster has found 5 directories, 2 of which can be accessed by us that is the /login.php and /robots.txt, lets looks at robots.txt page and see what we can find.

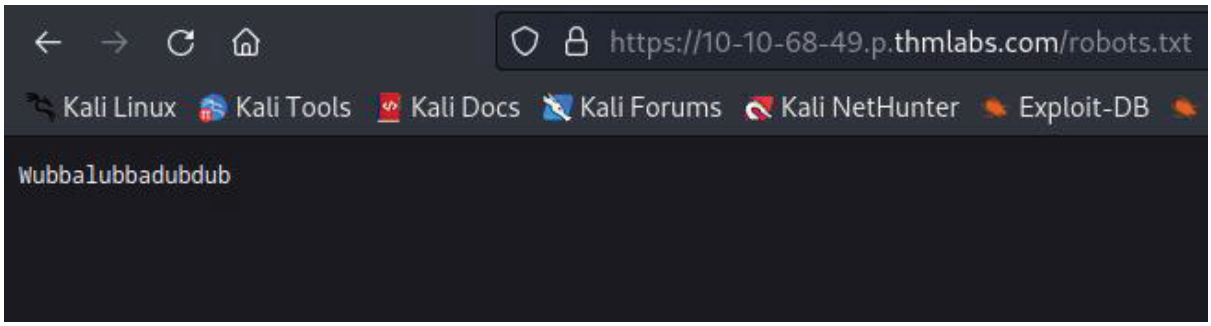

Fig: 4.2.8 ROBOTS TEXT FILE

From fig 4.2.8 in the robots.txt file, we can see a random word "Wubbalubbadubdub" which can be a potential password, for our login page

Now let us visit the login page at /login.php

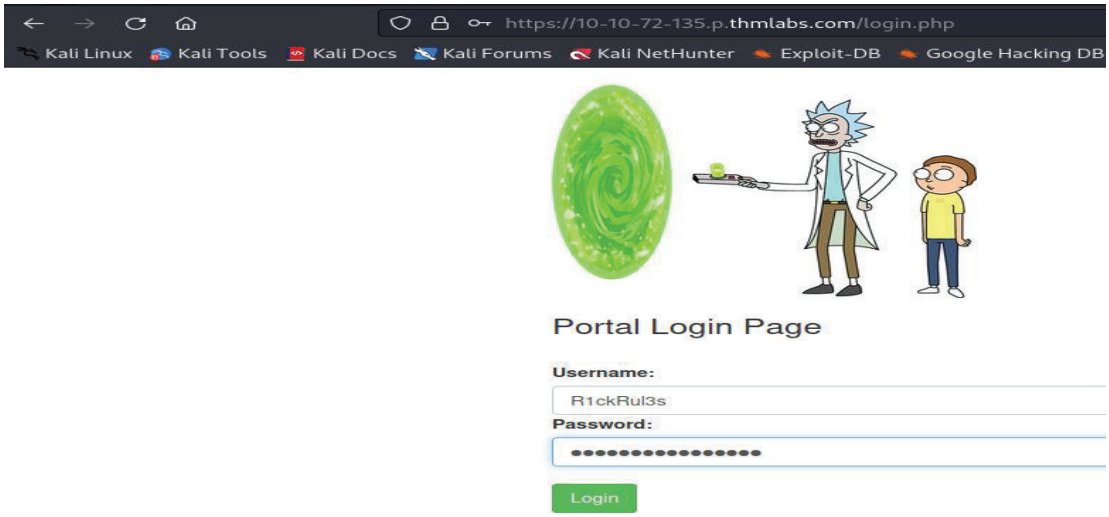

Fig: 4.2.9 TARGET LOGIN PAGE

As shown in fig: 4.2.9 lets provide the username as "R1ckRu13s" and password as "Wubbalubbadubdub" to login and login was successful. Just from using few information-gathering techniques, we were able to successfully login to a webpage.

After logging-in, we find a page showing "Command Panel" as shown in fig 4.2.10

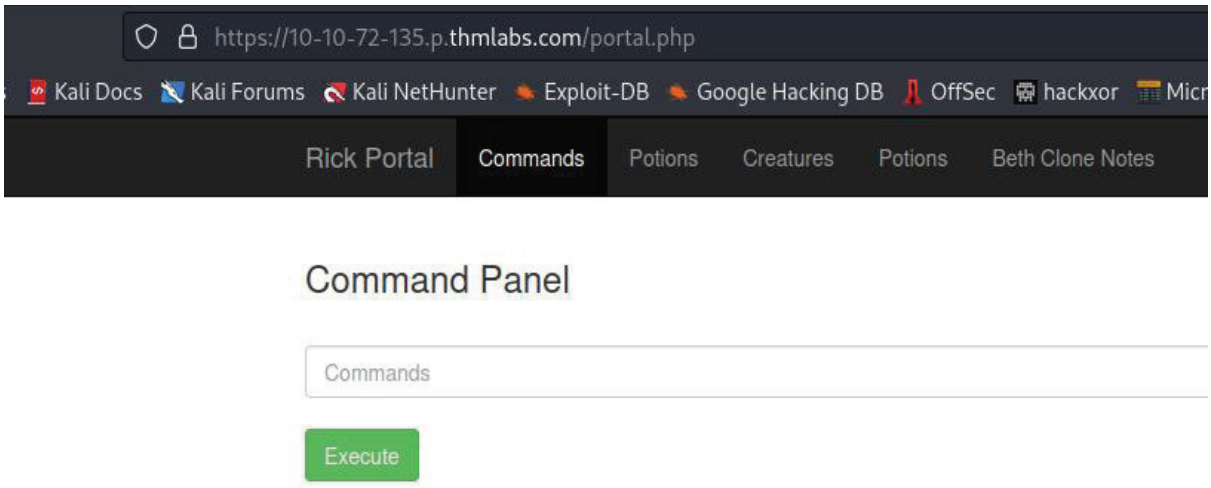

Fig: 4.2.10 COMMAND PANEL

Let's try some linux commands because cased on our information we have gathered this machine was a linux with Ubuntu distro running on it.

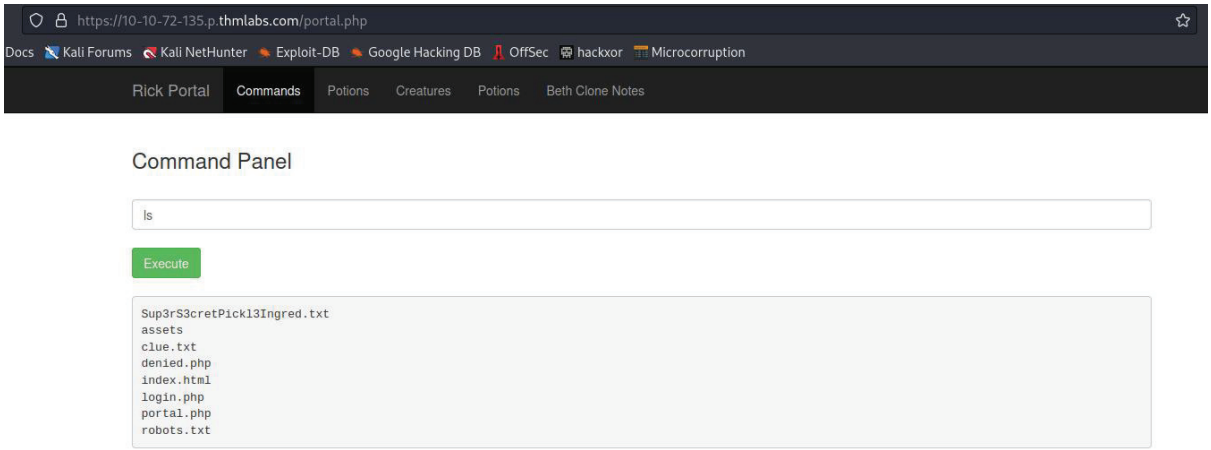

Fig: 4.2.11 COMMAND LINE INJECTION VULNERABILITY

From fig 4.2.11 we can see that the ls command does work that means we have **Command Line Injection vulnerability** on the webpage.

Now let us move on to the next phase of ethical hacking called "**VULNERABILITY ASSESSMENT**".

So far, we do know that the machine is a linux machine, it supports php and we have command line injection vulnerability present in the system. This is a high-risk vulnerability because we have access to the command line of the system, which means any threat-actors can use it run any commands.

The possible vulnerability we can use is running a php reverse shell to connect to our machine to gain shell access to the system.

Now that we have found a vulnerability let's move on to the "**EXPLOITATION**" phase of ethical hacking. In the exploitation phase, we try to exploit the vulnerability found in the previous phase.

Let us search in google for a php reverse shell command line injection vulnerability.

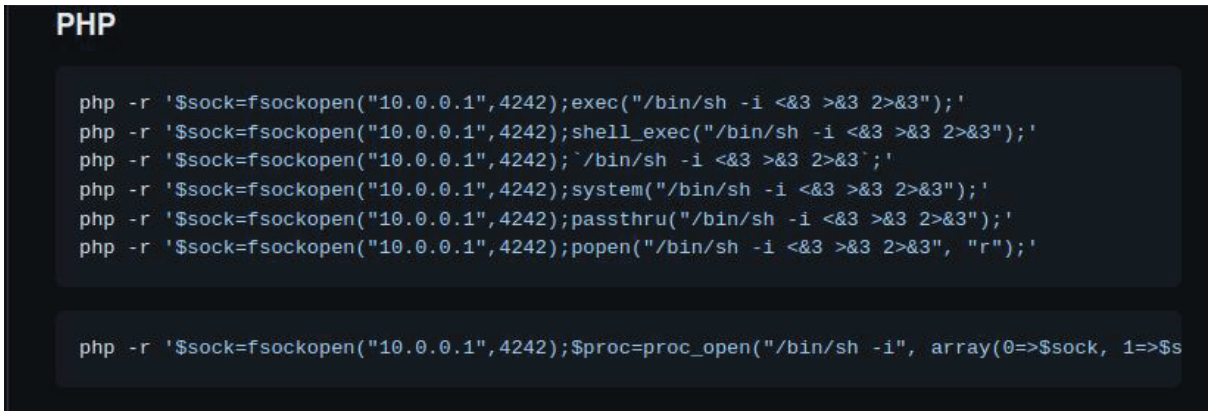

Fig: 4.2.12 PHP REVERSE SHELL

We find a list of possible php reverse shells in GitHub as shown in fig 4.2.12. Now let us try executing this php command in the website.

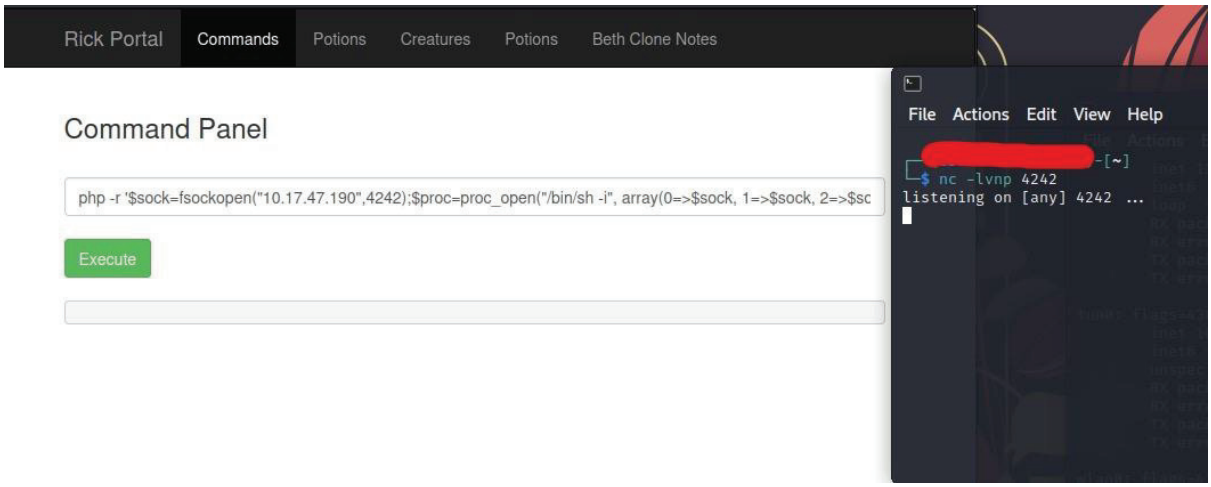

Fig: 4.2.13 EXECUTING PHP REVERSE SHELL AND NCAT

As shown in fig 4.2.13 entered in the php reverse-shell and opened our terminal to listen and capture the shell at port 4242.

Upon executing the command, we get the shell and have now obtained remote access to the target machine as shown in fig 4.2.14.

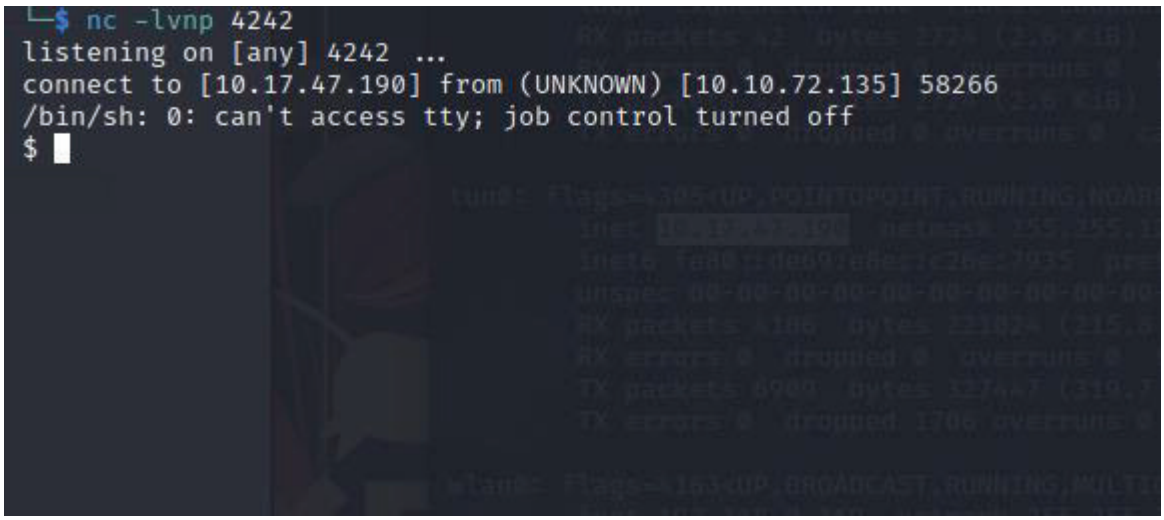

Fig: 4.2.14 REMOTE SHELL ACCESS

Now that we have completed the exploitation phase let's move onto the "**POST-EXPLOITATION**" phase.

In the post-exploitation phase, we try to escalate our privileges from a user to root user or admin privileges.

If we read our current directory, we see a "Sup3rS3cretPickl3Ingred.txt" if we open it, we get our first flag called "mr. meeseek hair" as shown in fig 4.2.15.

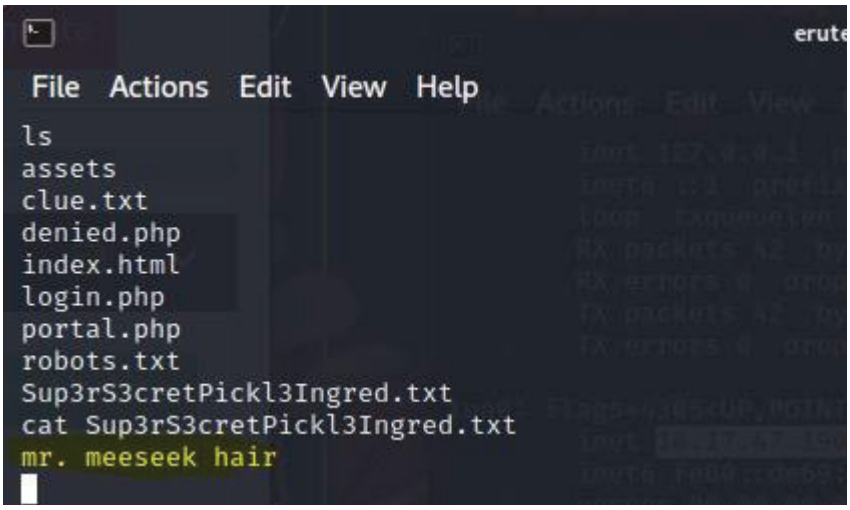

Fig: 4.2.15 FIRST FLAG OBTAINED

Now lets see if we are in sudoers group and check if we ca execute as root without sudo passwords.

To check if such misconfigurations are present we type in “sudo –l” command in the terminal.

As shown in fig 4.2.16 there is a major misconfiguration, which allows us to execute commands as root without requiring any kind of password.
We can now escalate our privilege from a normal user to a root user using the “sudo su” command.

Fig: 4.2.16 SUDO MISCONFIGURATION AND PRIV-ESCALATION

Now that we are the root user we have full access to the system, now let’s try to find the other two flags present in the system.

We found the second ingredient at the /home/rick directory as shown in fig 4.2.17

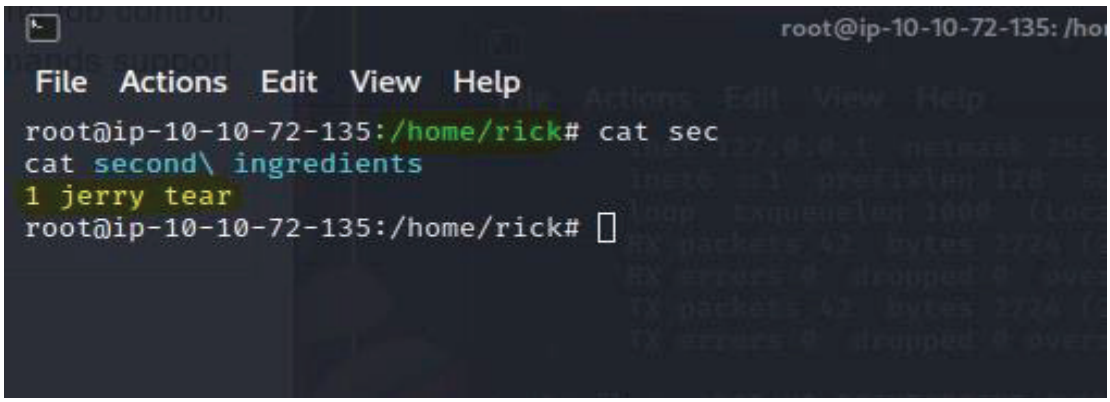

Fig: 4.2.17 SECOND FLAG OBTAINED

Finally, the third ingredient was in the root folder at /home/root/3rd.txt as shown in fig: 4.2.18

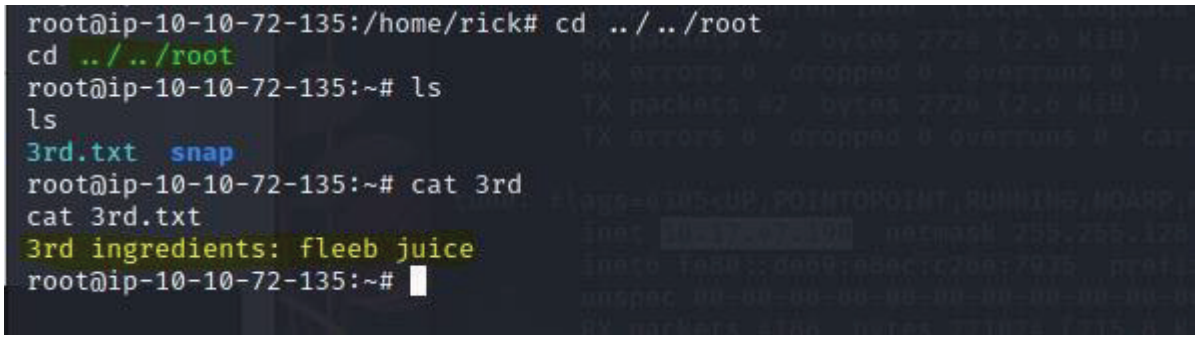

Fig: 4.2.18 THIRD FLAG OBTAINED

Finally, we have successfully pawned the box and obtained all three flags.
From this demonstration, we can see that each phase of hacking is vital to move to the next step. Failing to successfully clear any phase of hacking will stop our progress from moving to the next phases.

CHAPTER – 5
BENEFITS OF ETHICAL HACKING

Benefits of Ethical Hacking: Strengthening Cybersecurity through Proactive Vulnerability Assessment

Early Identification of Vulnerabilities:
Ethical hacking allows organizations to identify vulnerabilities in their systems, networks, and applications before malicious actors can exploit them. By conducting systematic and controlled assessments, ethical hackers simulate real-world attack scenarios, enabling organizations to patch vulnerabilities and prevent potential breaches.

Improved Security Posture:
Through ethical hacking engagements, organizations can enhance their overall security posture. By addressing identified vulnerabilities and strengthening defenses, they reduce the likelihood of successful attacks. This proactive approach ensures that systems and networks are better equipped to withstand potential threats.

Awareness of System Weaknesses:
Ethical hacking provides valuable insights into system weaknesses and potential entry points for attackers. By understanding these vulnerabilities, organizations can make informed decisions regarding security investments, policies, and procedures. This awareness helps in prioritizing resources and allocating efforts effectively.

Compliance with Industry Standards and Regulations:
Ethical hacking enables organizations to assess their compliance with industry standards, regulations, and cybersecurity frameworks. By conducting regular assessments, organizations can identify gaps and ensure that their security measures align with required guidelines. This proactive approach helps avoid potential legal and regulatory penalties.

Increased Customer Trust and Brand Reputation:
Demonstrating a commitment to cybersecurity through ethical hacking practices can enhance customer trust and brand reputation. By actively assessing and mitigating vulnerabilities, organizations show their dedication to protecting customer data and maintaining privacy. This fosters a sense of trust among customers, leading to stronger brand loyalty.

Cost Savings and Risk Reduction:
Ethical hacking helps organizations minimize financial losses associated with data breaches and cyber-attacks. By identifying and addressing vulnerabilities proactively, organizations can prevent costly incidents that could result in reputational damage, legal liabilities, and financial repercussions. Ethical hacking provides a cost-effective approach to risk management.

Continuous Improvement and Resilience:
Ethical hacking promotes a culture of continuous improvement in cybersecurity. By regularly assessing and remediating vulnerabilities, organizations can adapt their security measures to evolving threats. This iterative process ensures that systems and networks remain resilient and up-to-date against emerging attack vectors.

Collaboration and Knowledge Sharing:
Ethical hacking encourages collaboration between ethical hackers, security teams, and organizational stakeholders. This collaboration fosters knowledge sharing, allowing organizations to leverage the expertise of ethical hackers and security professionals. By sharing insights, best practices, and emerging trends, the collective defense against cyber-threats is strengthened.

CHAPTER – 6
CONCLUSION

I believe this report has proven to us how easy it is to install and use offensive tools and gain access to the system and how important ethical hacking is to find vulnerabilities in a network and system.

In this report we have covered

- What is an ethical hacker and their types
- Installing and setting up kali-linux
- Hacking Methodologies
- Using hacking methodologies to compromise a system
- Benefits of ethical hacking

In conclusion, ethical hacking plays a vital role in ensuring the security and integrity of computer systems, networks, and digital assets. Through the systematic and controlled process of identifying vulnerabilities, ethical hackers help organizations strengthen their defenses against malicious attacks.