Kioptrix Level 1

## 1.1 Introduction

Kioptrix Level 1 is a VM Image i.e., available on Vulnhub. It is an Entry level or beginner level 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 1.

Name- Kioptrix Level 1

OS Type- Linux

Download Source: - Vulnhub

Download Kioptrix L1 URL: - <https://download.vulnhub.com/kioptrix/Kioptrix_Level_1.rar>

## 1.2 Objective

Kioptrix Level 1 is a vulnerable linux machine that is developed for pentesters to practice penetration testing skills. It is a basic level or beginner 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

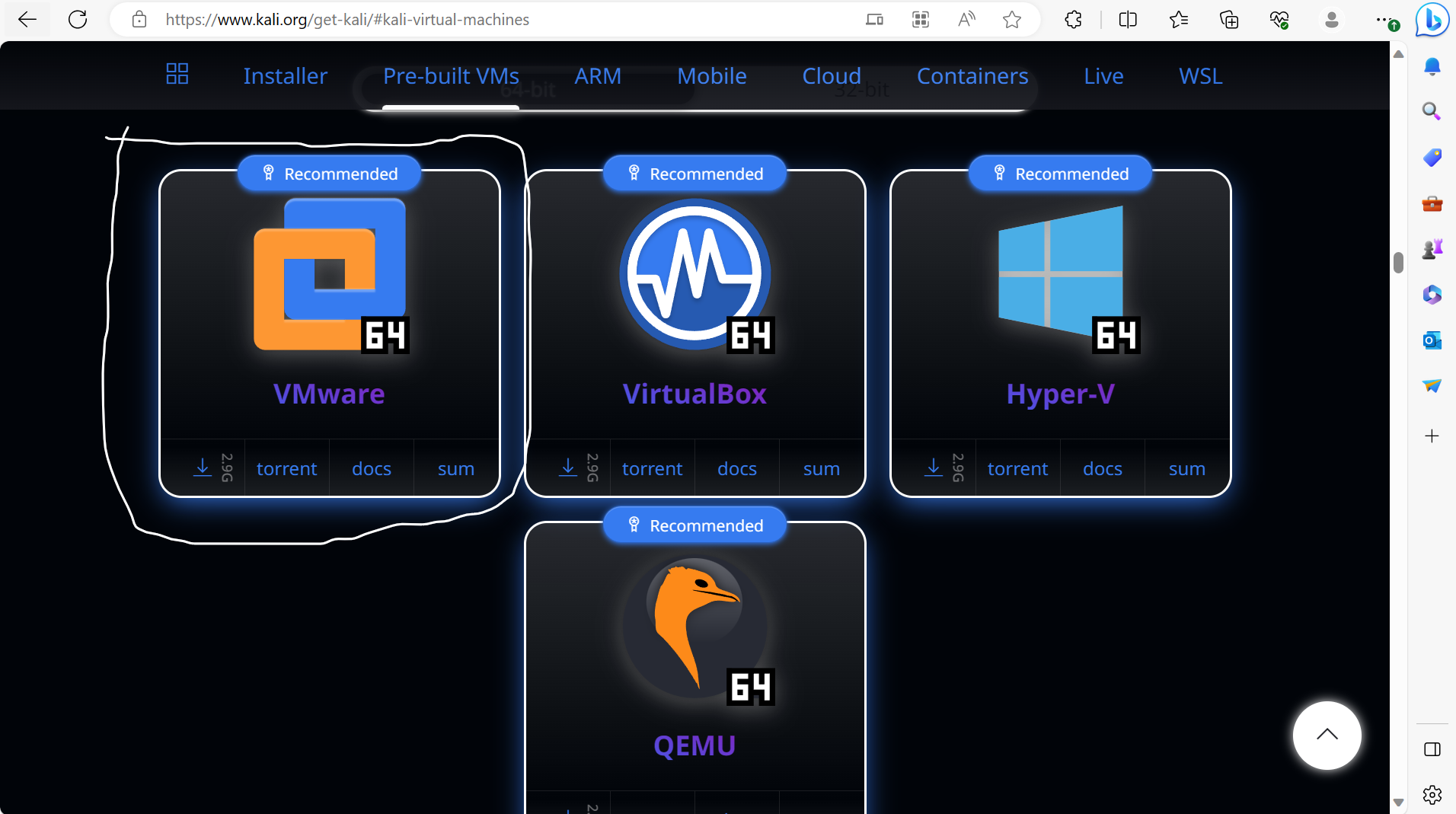
3. Metasploit

# 2.0 Prerequisite

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

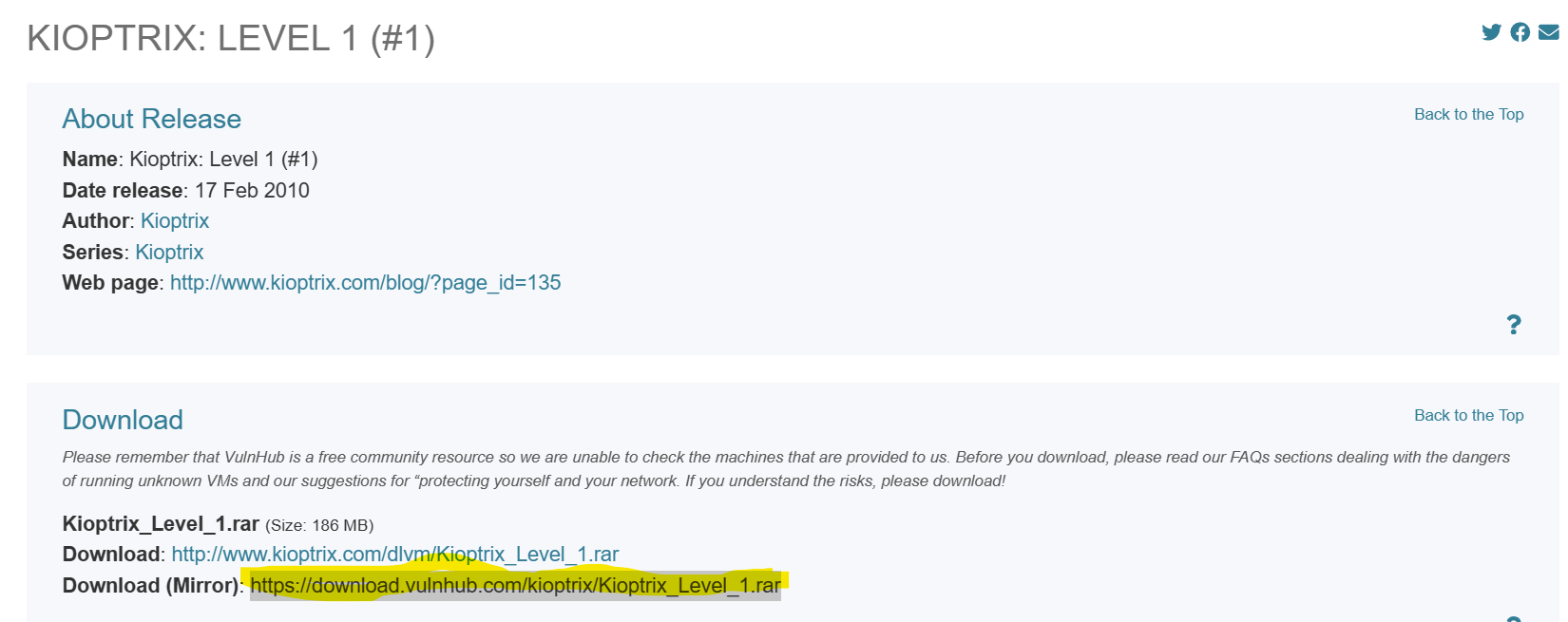
Download VMWare Workstation from mentioned url <https://www.vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html>

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.

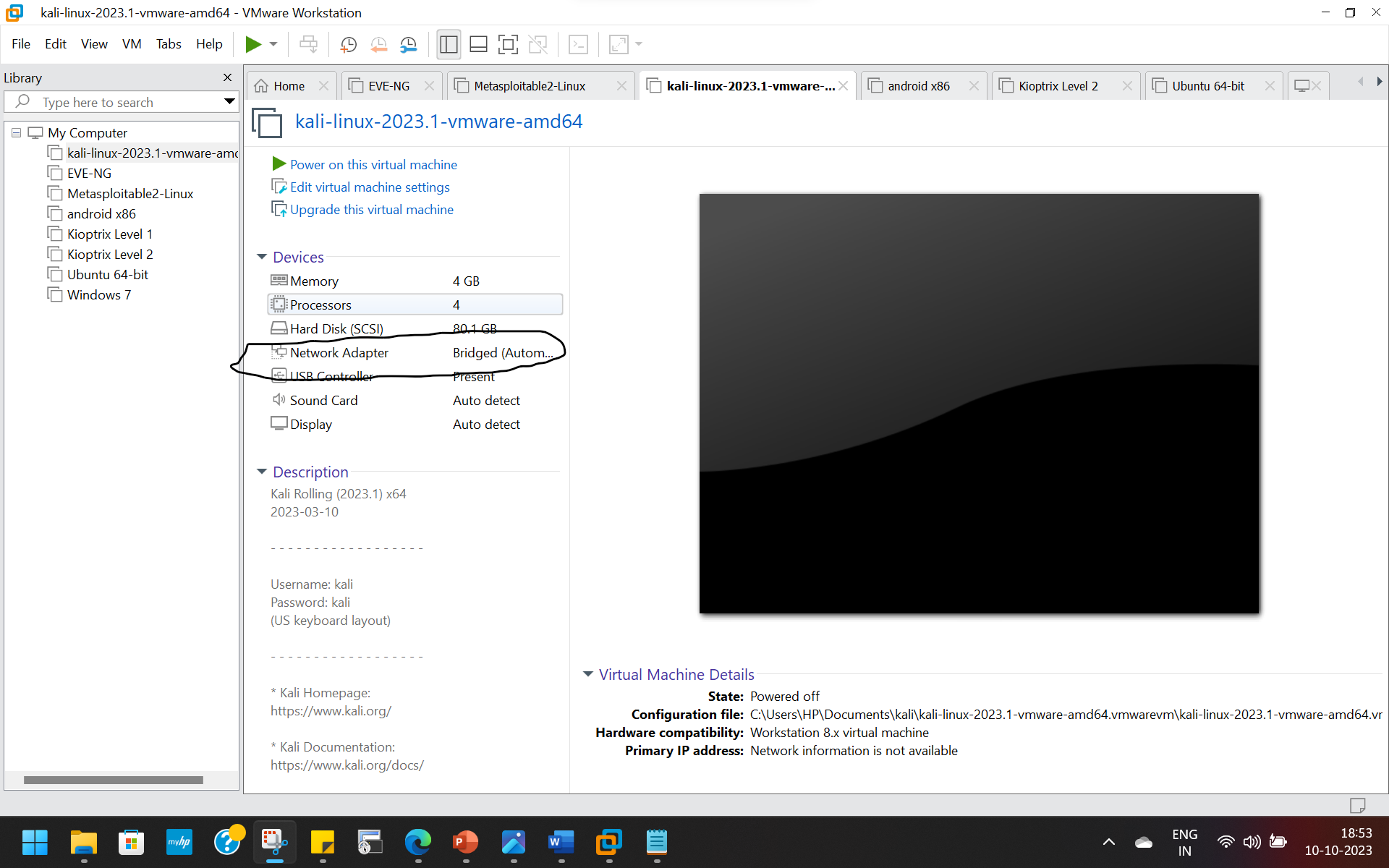
After installing Kali Linux on VMware Workstation next we need to install Kioptrix Level 1 machine, to download Kioptrix Level 1 image from mentioned url <https://download.vulnhub.com/kioptrix/Kioptrix_Level_1.rar>

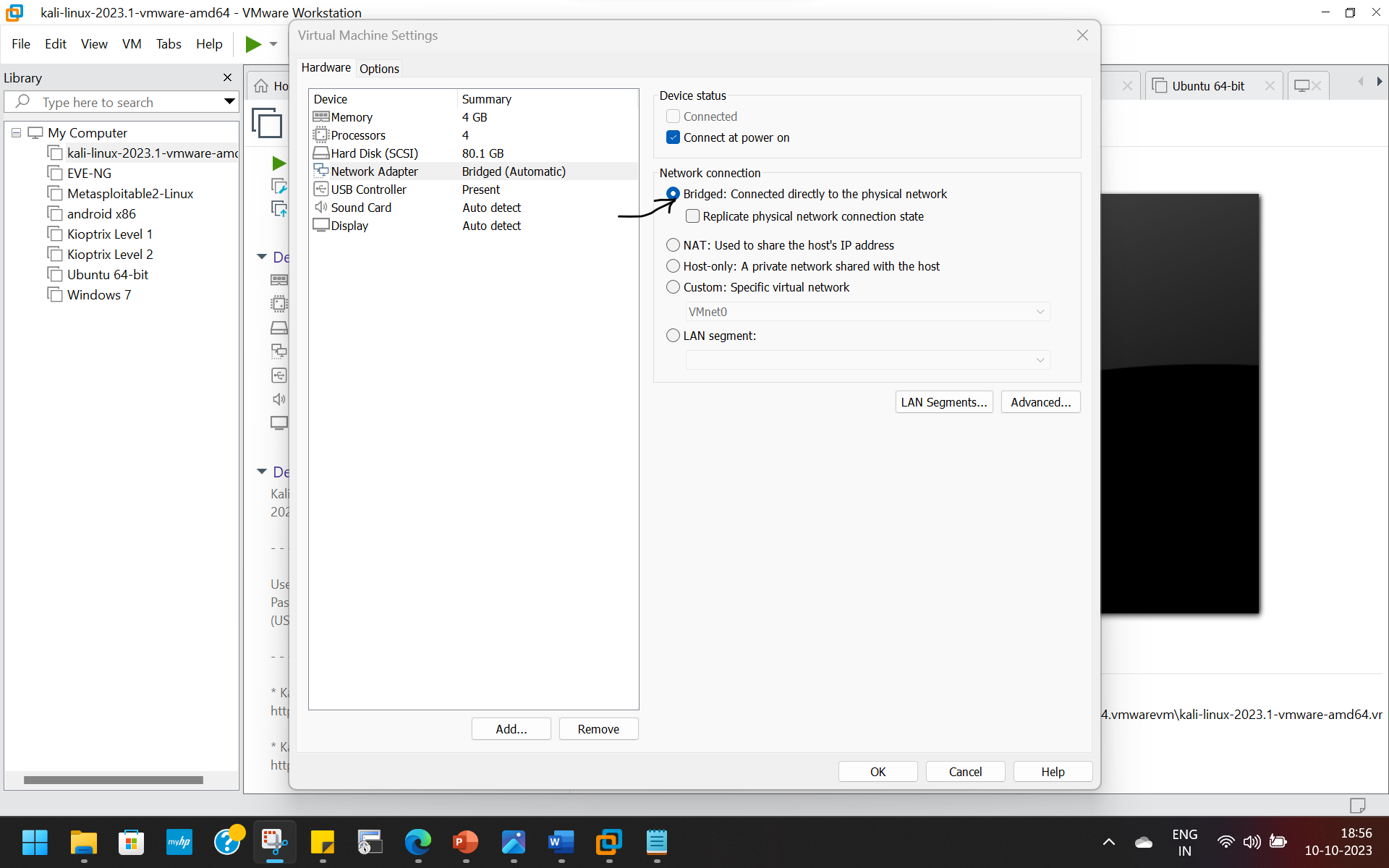


Click on yellow colour highlighted link to download image of Kioptrix Level 1.

After downloading we need to install the Kioptrix Level 1 image on VMware workstation.

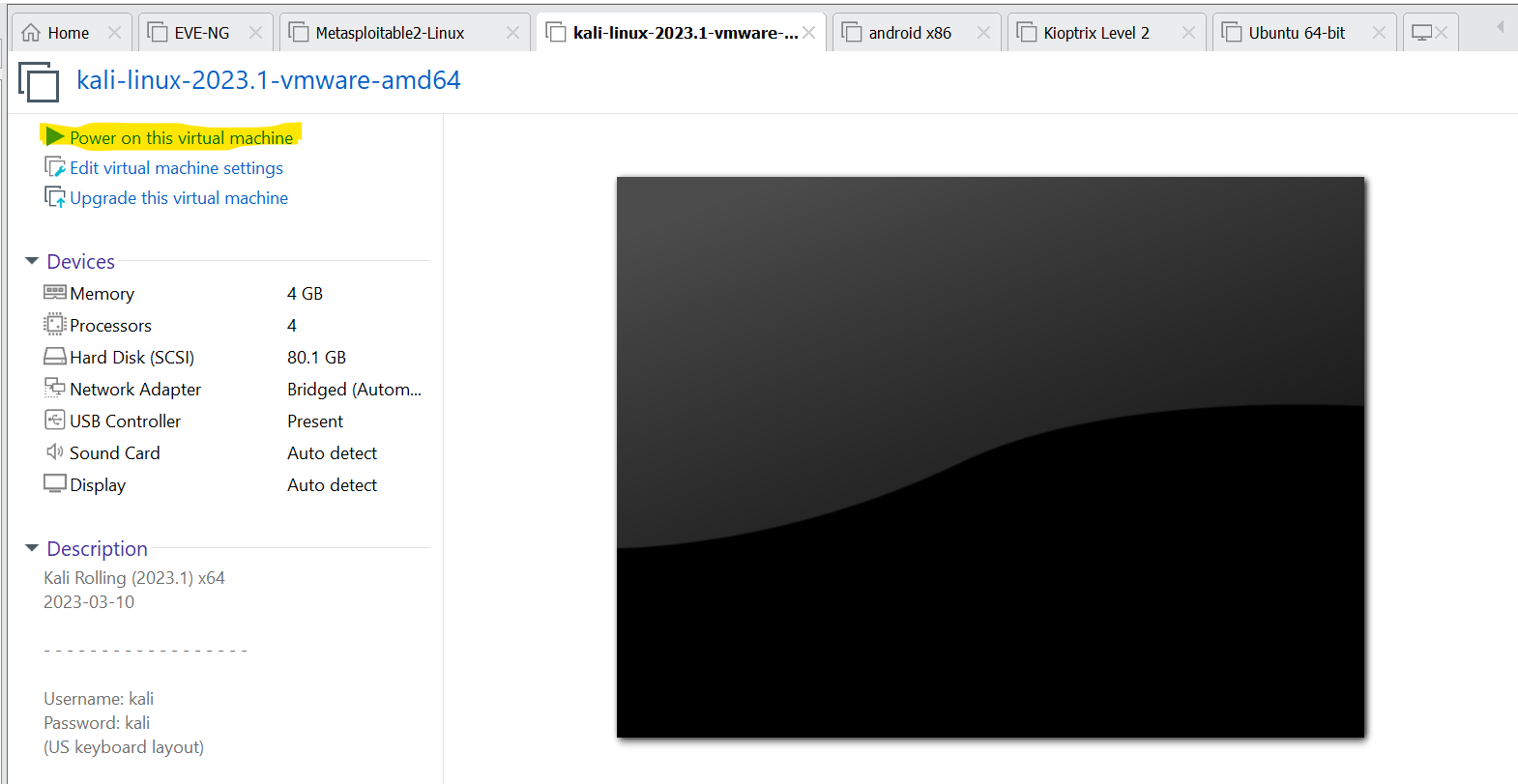
After completing installation next, we need to put both Kali and Kioptrix Level 1 on same network, to perform that we will need to put the network adaptor to bridge of both the machines.



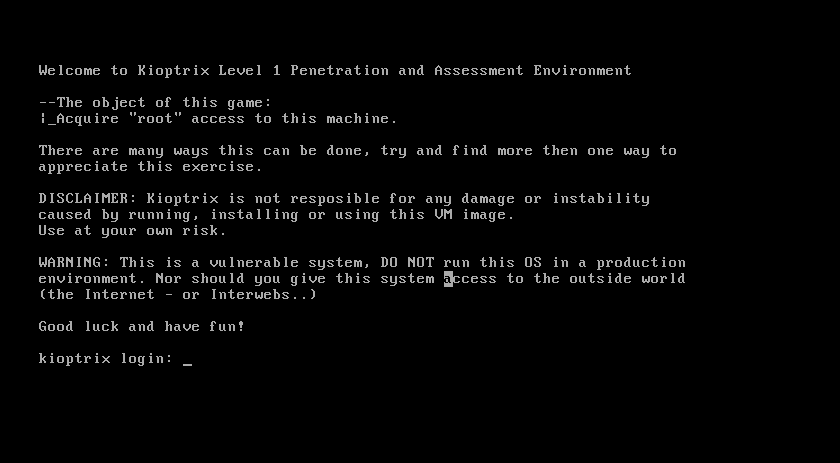


Click on Network Adaptor and select network connection type as Bridged, same task we need to do with Kioptrix Level 1 machine i.e., installed on VMware.

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 1 Machine as well.



Screenshot of Kioptrix Level 1 login screen.

# 3.0 Kioptrix Level 1 – Short Summary

Target IP: 192.168.1.104

Target Machine: Kioptrix Level 1

Vulnerability Name: samba/Trans2open

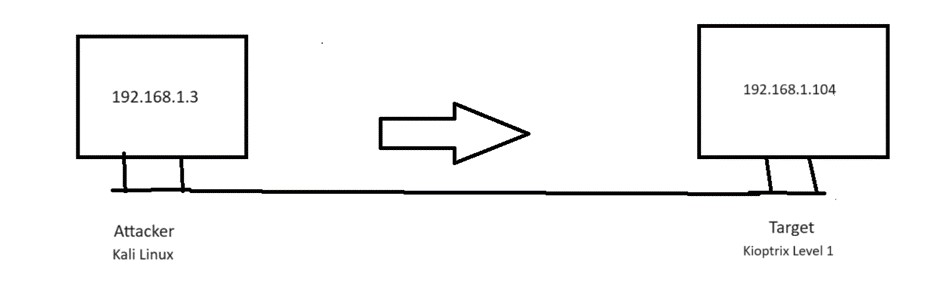
Vulnerability Exploited: linux/samba/trans2open

Vulnerability Exploited With: Metasploit Framework

Payload Used: linux/x86/shell\_reverse\_tcp

# 4.0 Kioptrix Level 1 – Methodology

Kioptrix Level 1 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.

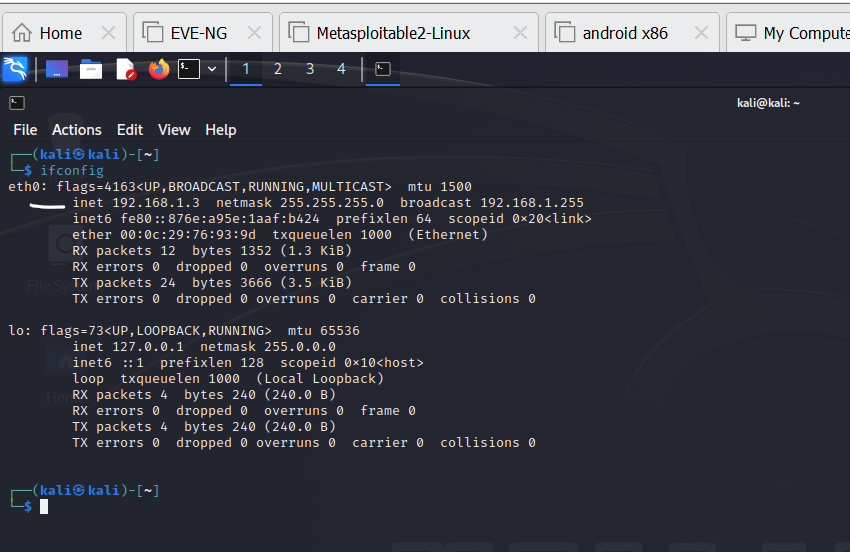


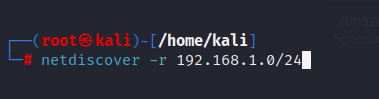
We will use Kali Linux as attacker machine and Metasploit framework as mode of exploit.

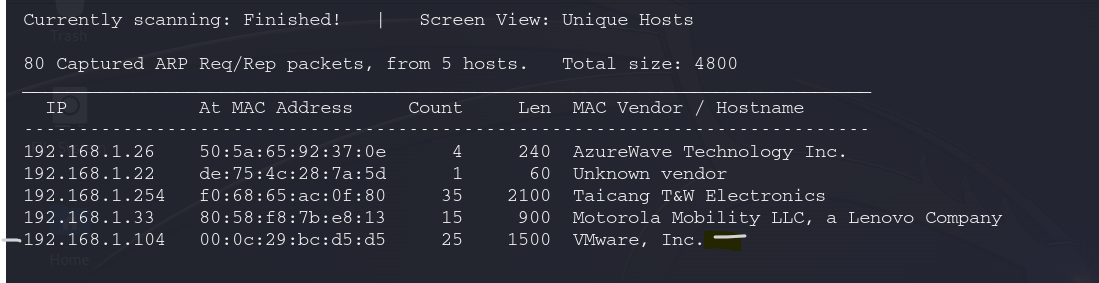
First step to proceed Pen testing is information gathering and scanning, so now just boot both the machines Kali Linux and Kioptrix Level 1 that are mounted on VMware.

## 4.1 Kioptrix Level 1 – 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.

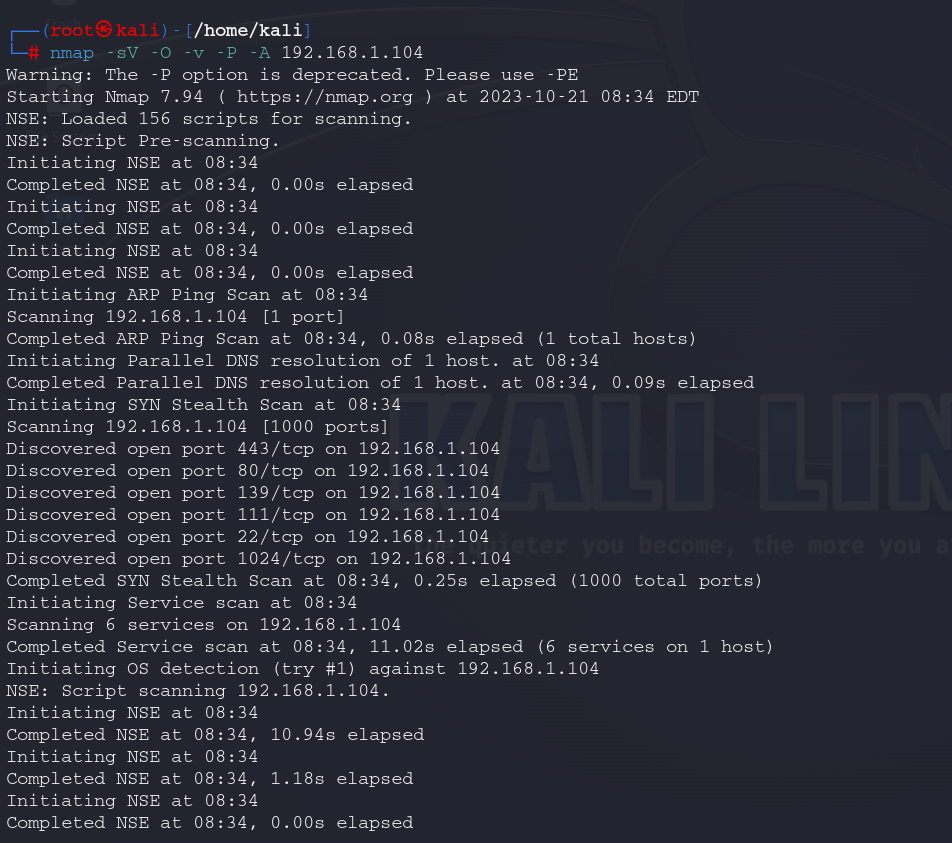


Now to check IP address of Kioptrix Level 1 we will need to use “**netdiscover**” command on Linux terminal to scan IP address in subnet range.



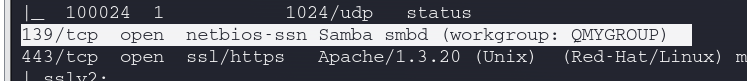
Since we have target machine mounted on VMware that’s why we can understand that IP address **192.168.1.104** is Kioptrix Level 1 Machine.

Next, we need to scan IP address **192.168.1.104** 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 192.168.1.104”**





After scan we have identified that **Port 139** is open and this port is used for

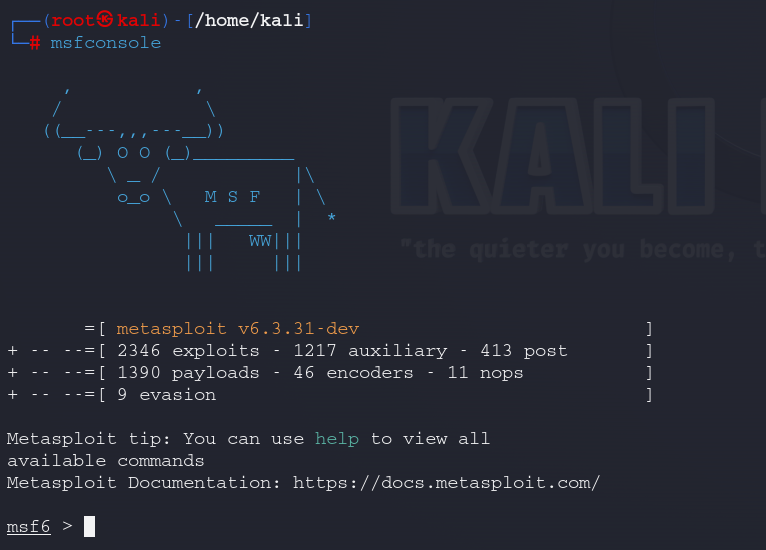


Hence, we will check for exploit for samba on Metasploit.

## 4.2 Kioptrix Level 1 – Exploitation

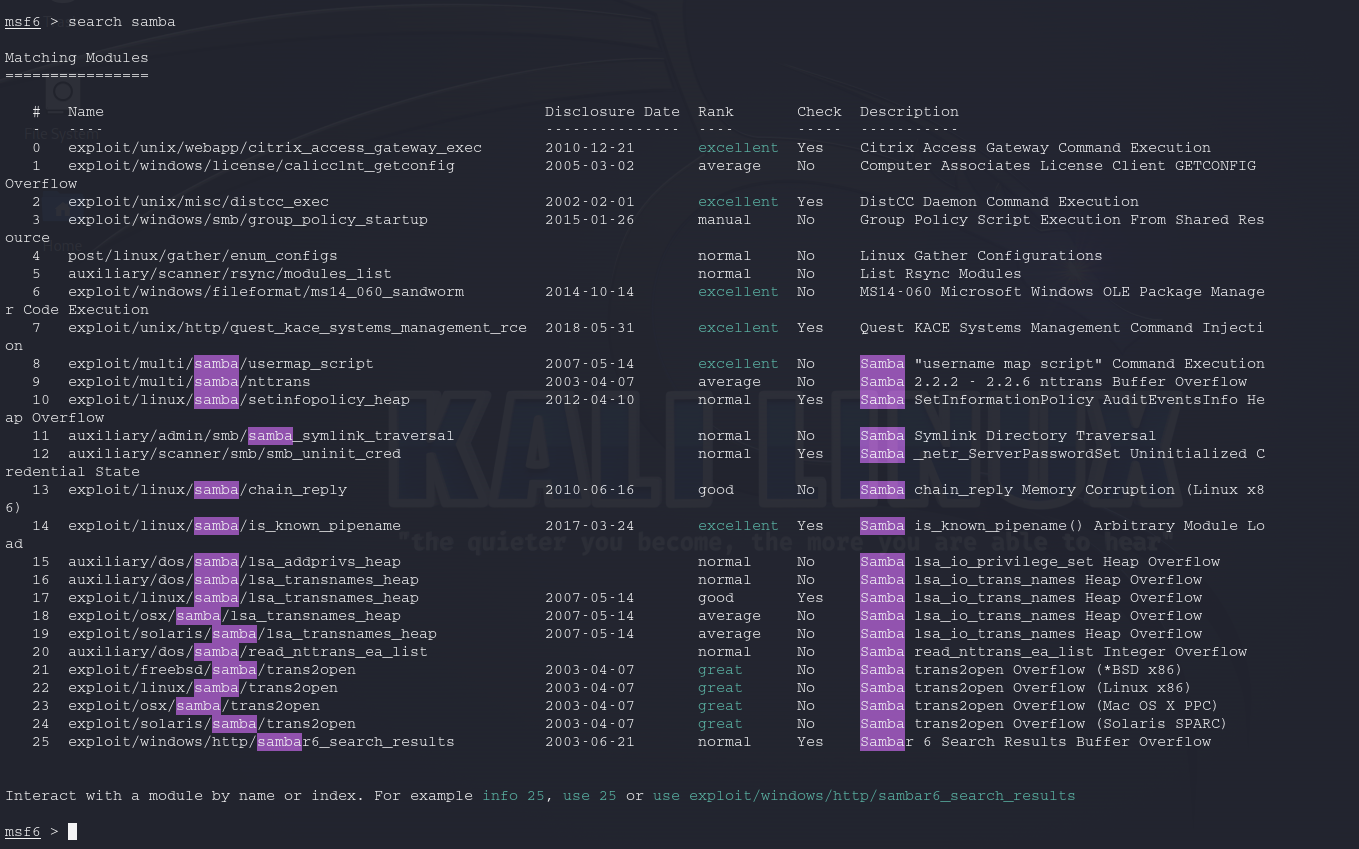
Now to run exploit we will first have to use Metasploit Framework i.e., already preinstalled on Kali Linux.

To run Metasploit Framework on Kali we will need to give a command on Terminal as “**msfconsole**” to start its operation.



“**msf6** **>**” will be shown once Metasploit is started completely.

Now, firstly we need to identify exploit availability for the vulnerable version samba in Metasploit, we need to use command “**search samba**” to check available exploit.



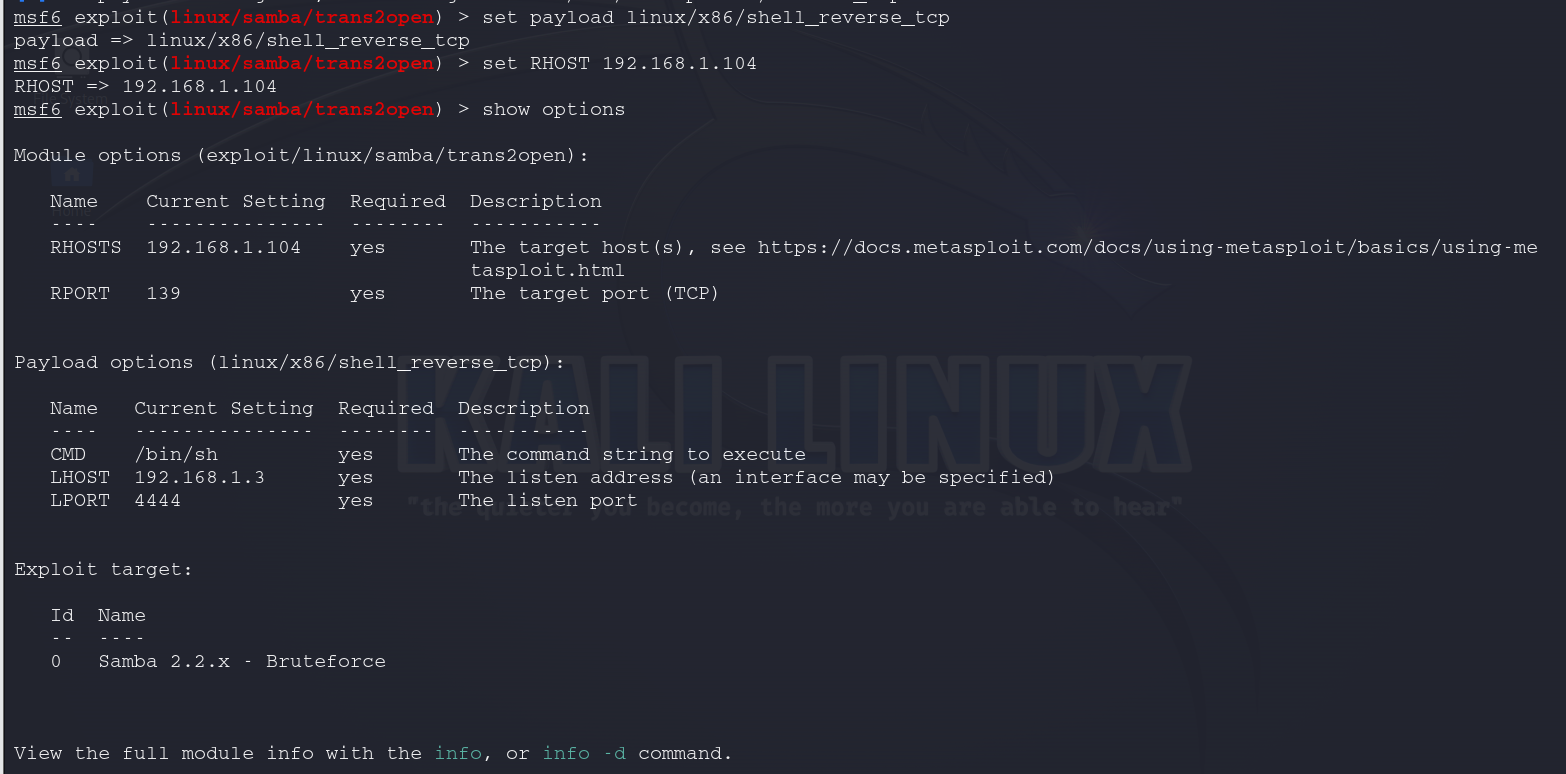
Now we will use trans2open exploit, since samba servers are vulnerable w.r.t to buffer overflow when used with trans2open function, to confirm it we will use the command “**use exploit/linux/samba/trans2open**”



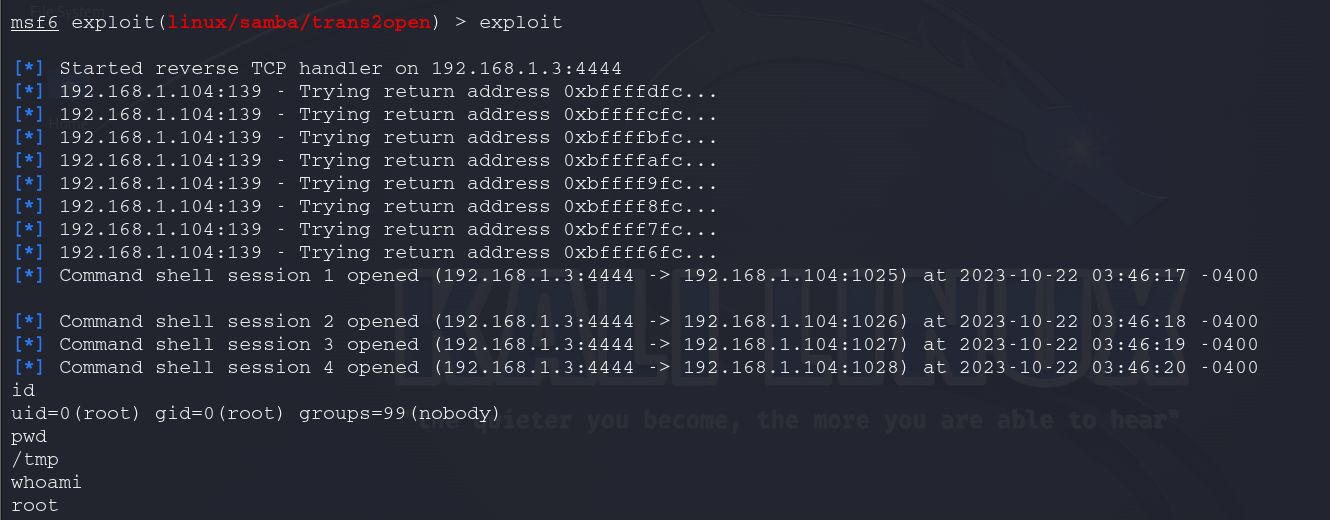
We had defined exploit for the vulnerability, next is to work to gain access and for that we need to define payload and RHOST, payload is already defined by Metasploit w.r.t. to exploit that we selected **linux/x86/shell\_reverse\_tcp**, lets proceed for gaining access.

## 4.3 Kioptrix Level 1 – Gain Access to Root

We have two parameters, RHOST as **192.168.1.104** and payload as **linux/x86/shell\_reverse\_tcp**



We are in the final step of penetration testing i.e., gaining access, in previous step we have prepared all the parameters that were required to run exploit successfully. Now next is to run exploit, hence use command “**exploit**”



After running this command, you can see that we have successfully established a shell connection with Target Machine (Kioptrix Level 1).

For verification of access, I used the command **“id”** and **“whoami”** to check access.

# 5.0 Conclusion

Kioptrix Level 1 has many open well-known ports in which port 139 is vulnerable to samba service w.r.t trans2open and by the help of Metasploit Framework it can be exploited.