## Metasploitable 2

## 1.1 Introduction

The Metasploitable 2 is an vulnerable machine based on Linux i.e. designed for testing security tools and demonstrating common vulnerabilities. This report demonstrates many of the security flaws in the Metasploitable 2 image. By this document we will show backdoor vulnerability that is present on this machine and we can exploit this machine due to this vulnerability. All necessary steps to attain privilege access will be mentioned in this report.

Name- Metasploitable 2

OS Type- Linux

Download Source: - Vulnhub

## 1.2 Objective

Metasploitable 2 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

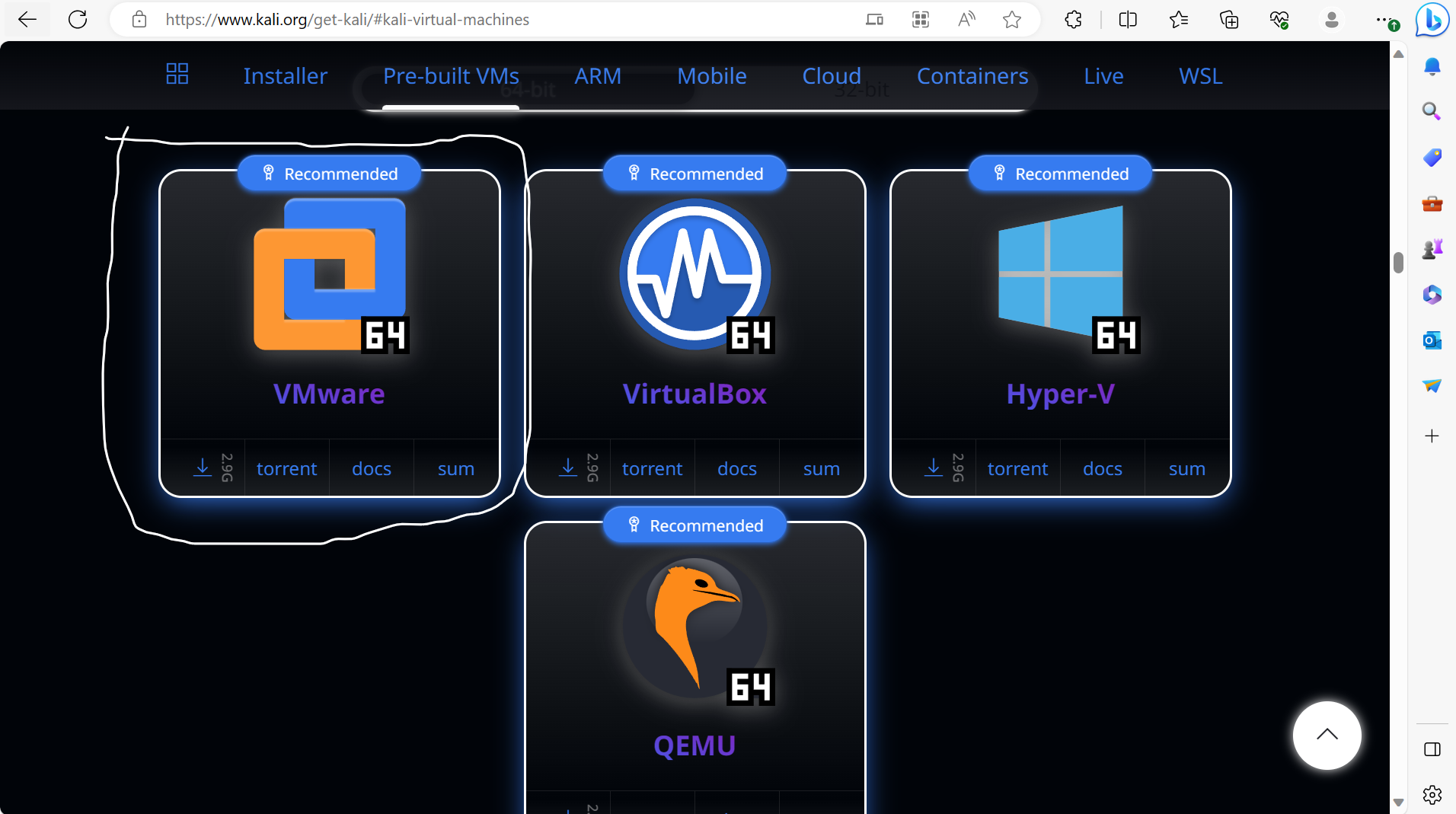
3. Metasploit

# 2.0 Prerequisite

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

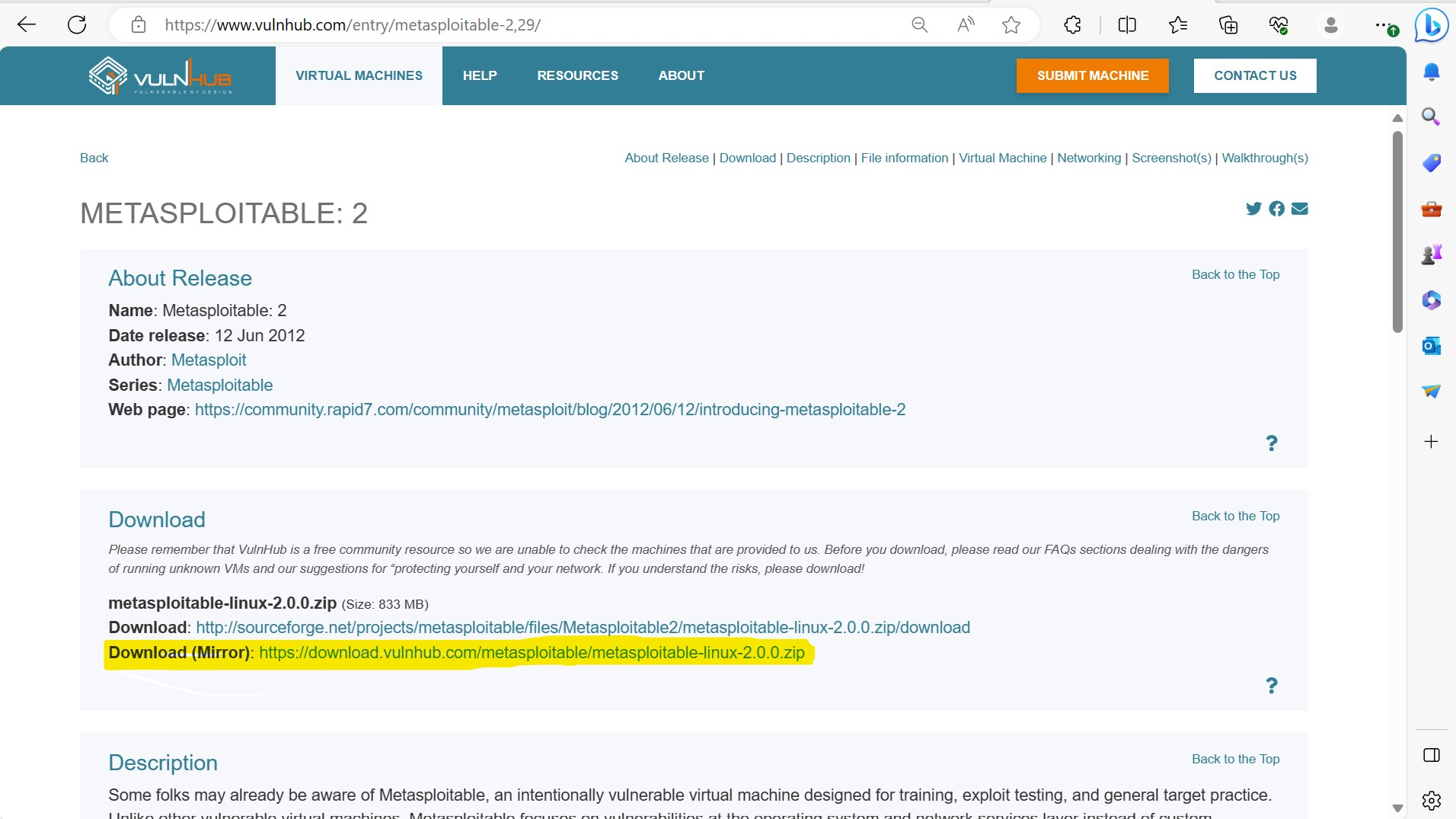
Download VMWare Workstation from mentioned url <https://www.vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html>

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.

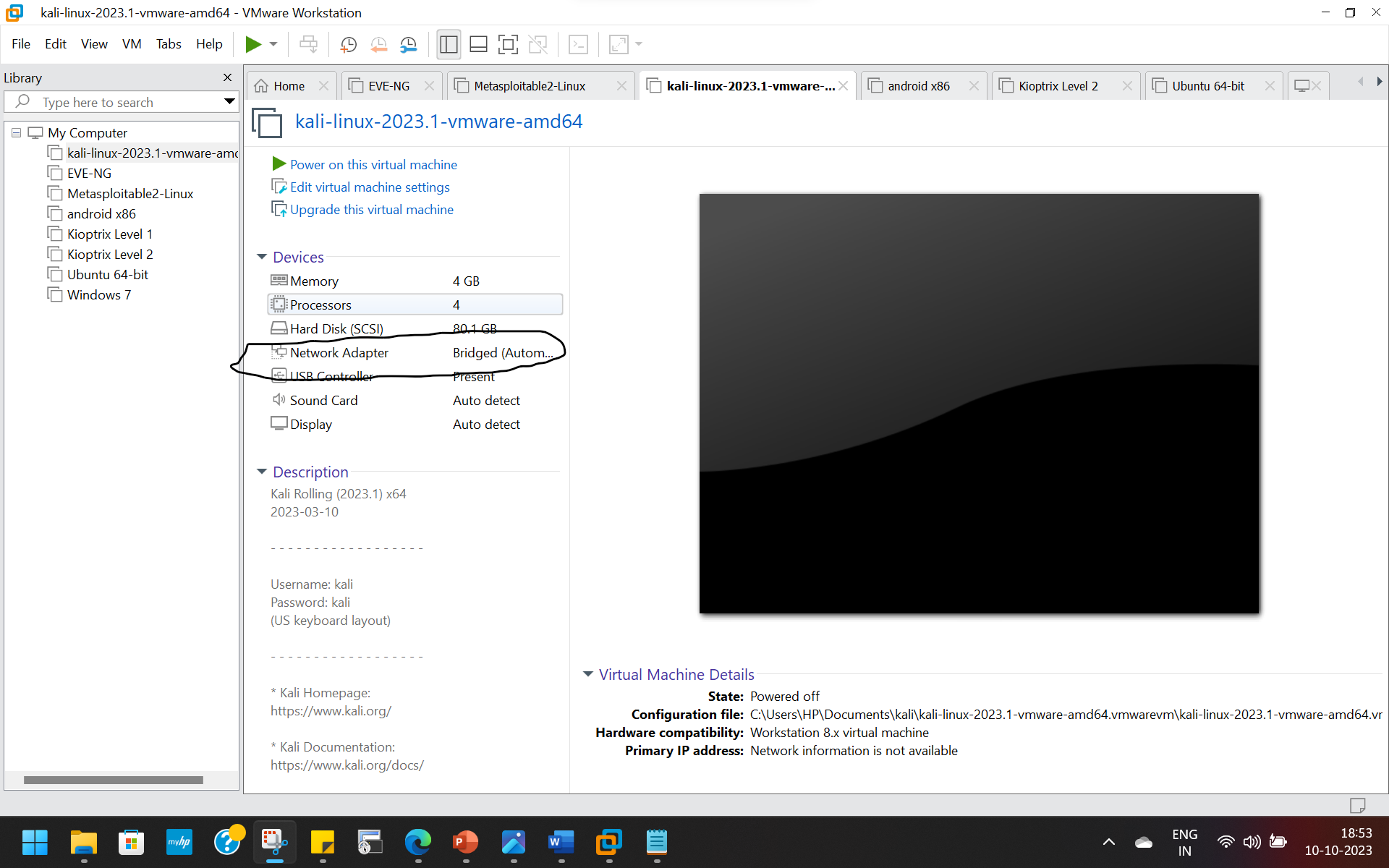
After installing Kali Linux on VMware Workstation next we need to install metasploitable 2 machine, to download Metasploitable 2 image from mentioned url <https://www.vulnhub.com/entry/metasploitable-2,29/>

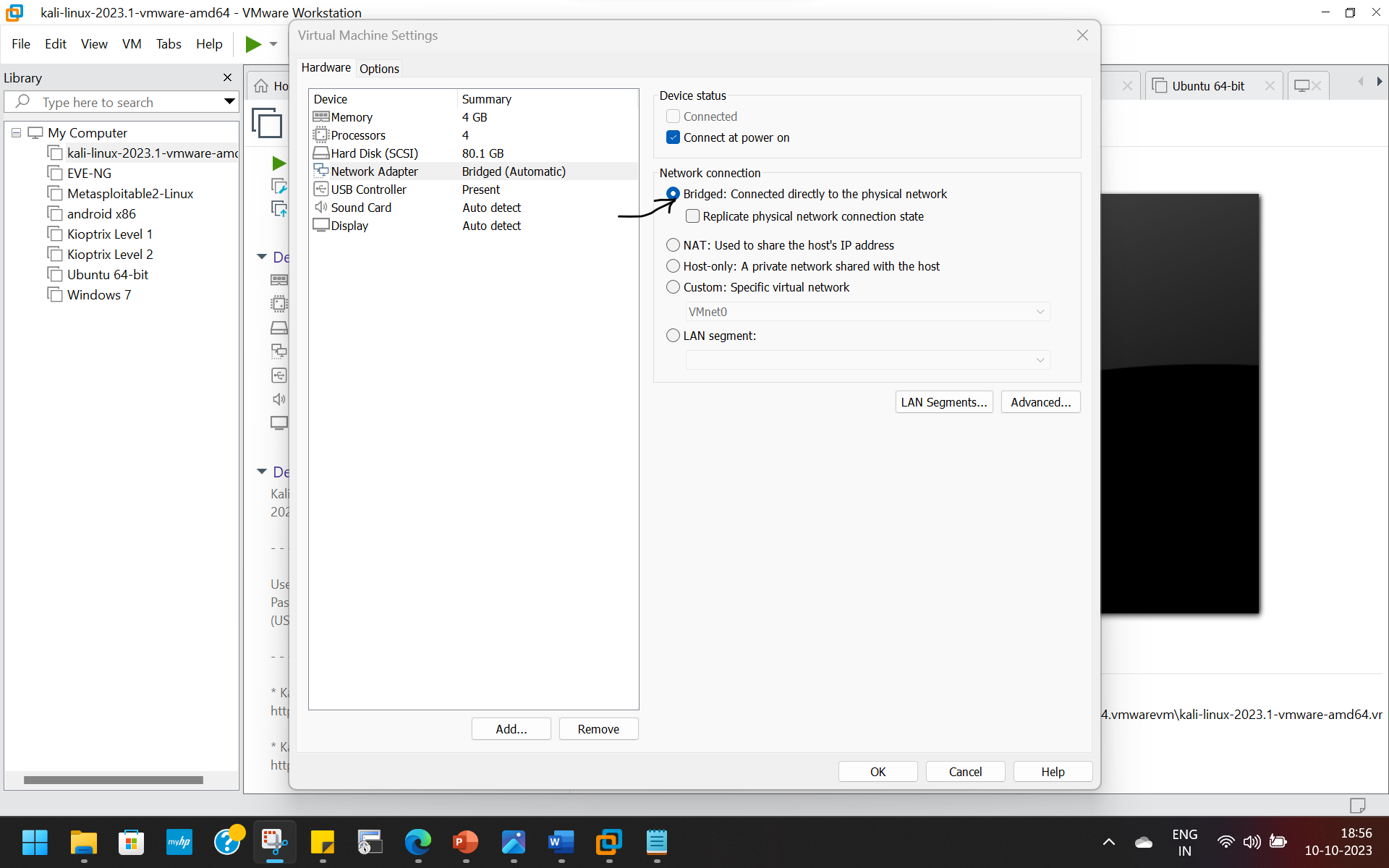


Click on yellow colour highlighted link to download image of metasploitable 2.

After downloading now we need to install the Metasploitable 2 image on VMware workstation.

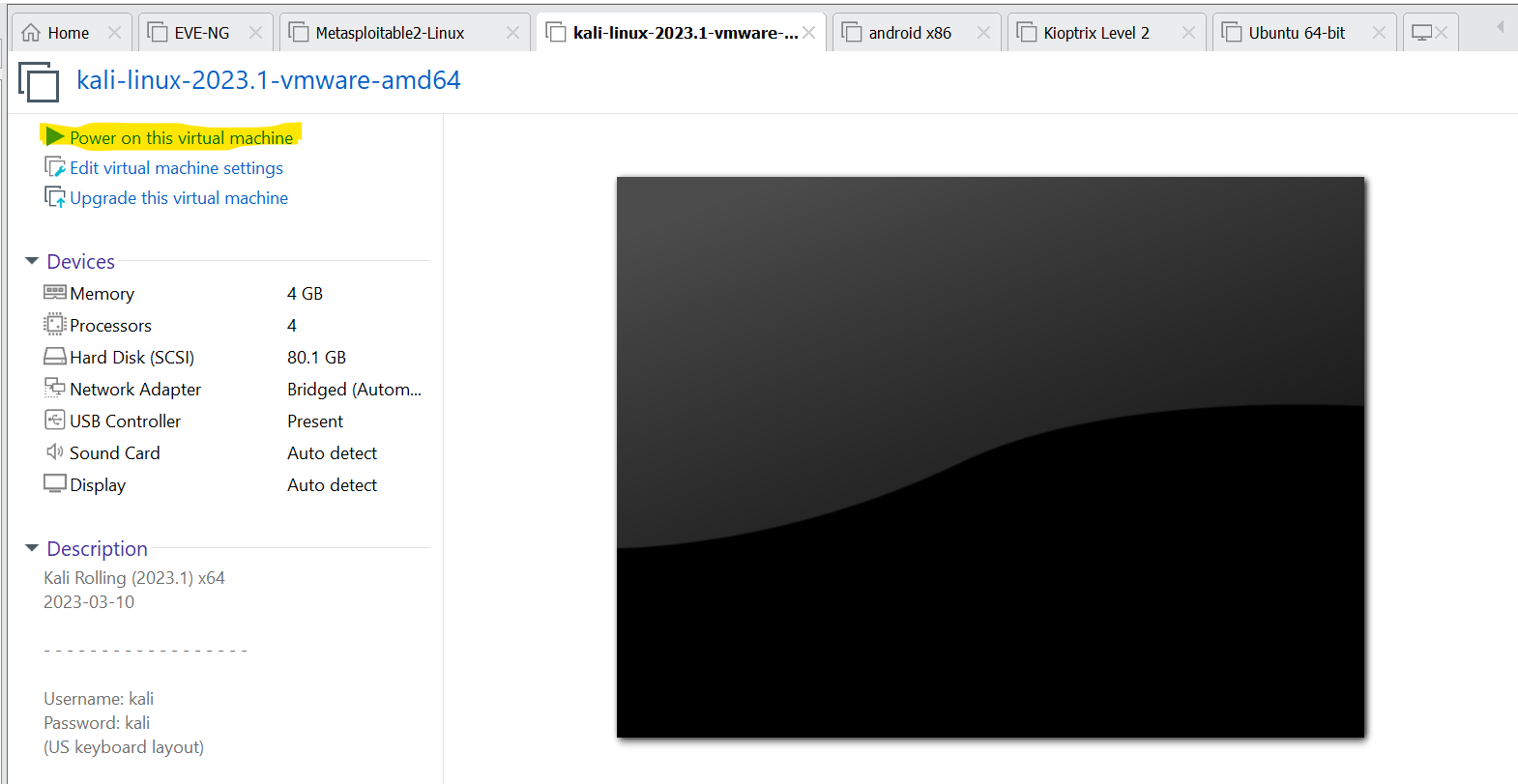
After completing installation next we need to put both Kali and Metasploitable 2 on same network, to perform that we will need to put the network adaptor to bridge of both the machines.





Click on Network Adaptor and select network connection type as Bridged, same task we need to do with Metasploitable 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 Metasploitable 2 Machine as well.

# 3.0 Metasploitable 2 – Short Summary

Target IP: 192.168.1.30

Target Machine: Metasploitable 2

Vulnerability Name: vsftpd 2.3.4

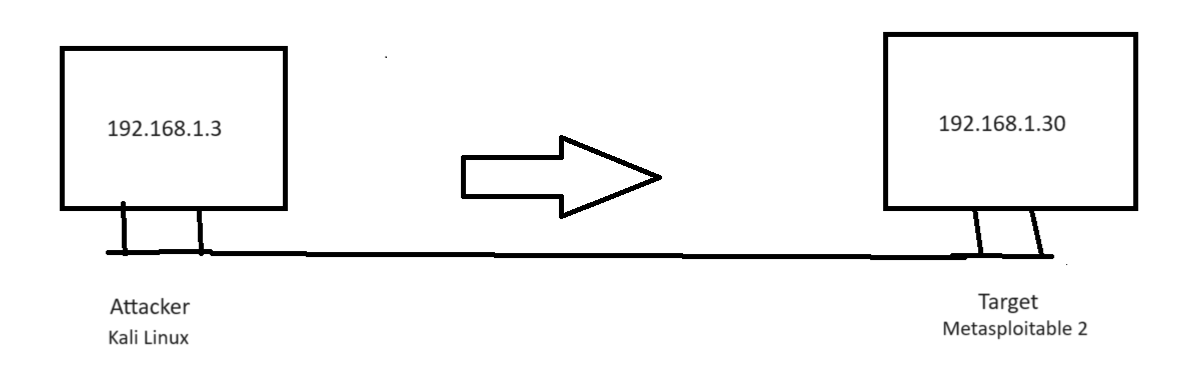
Vulnerability Exploited: unix/ftp/vsftpd\_234\_backdoor

Vulnerability Exploited With: Metasploit Framework

Payload Used: cmd/unix/interact

# 4.0 Metasploitable 2 – Methodology

Metasploitable 2 machine that runs on Linux based OS 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.

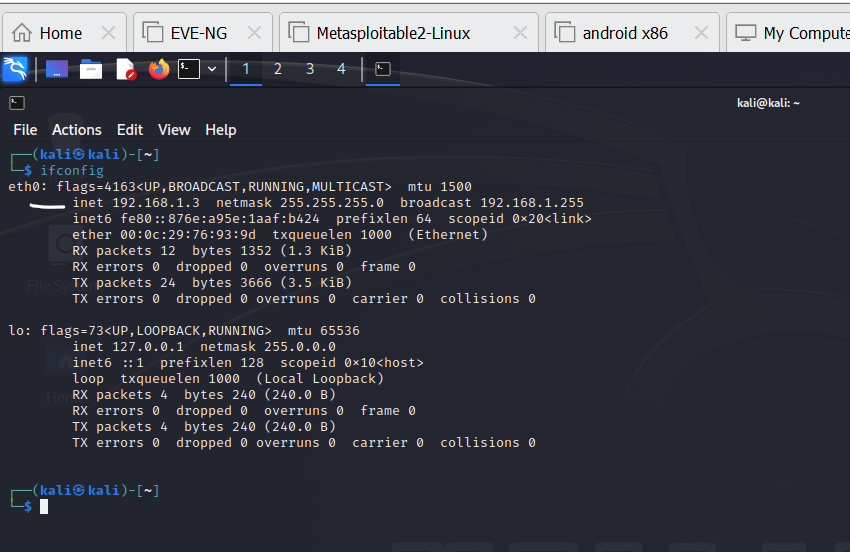


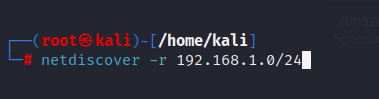
We will use Kali Linux as attacker machine and Metasploit framework as mode of exploit.

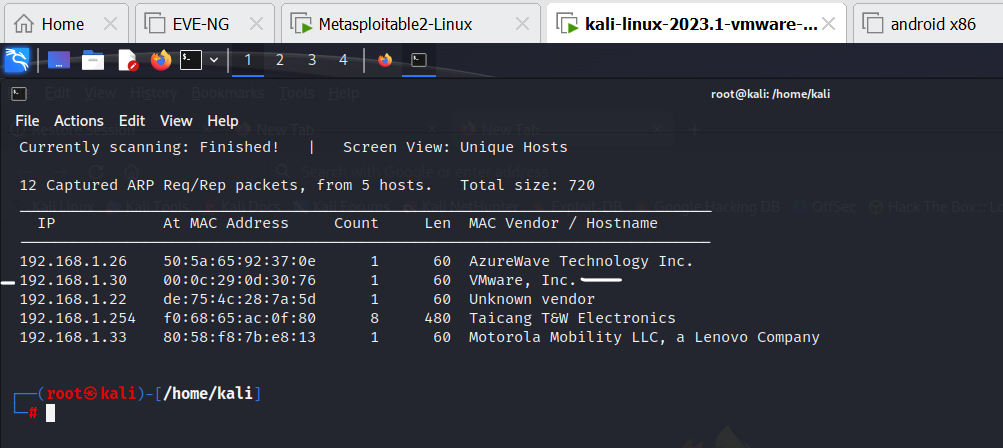
First step to proceed Pen testing is information gathering and scanning, so now just boot both the machines Kali Linux and Metasploitable 2 that are mounted on VMware.

## 4.1 Metasploitable 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.

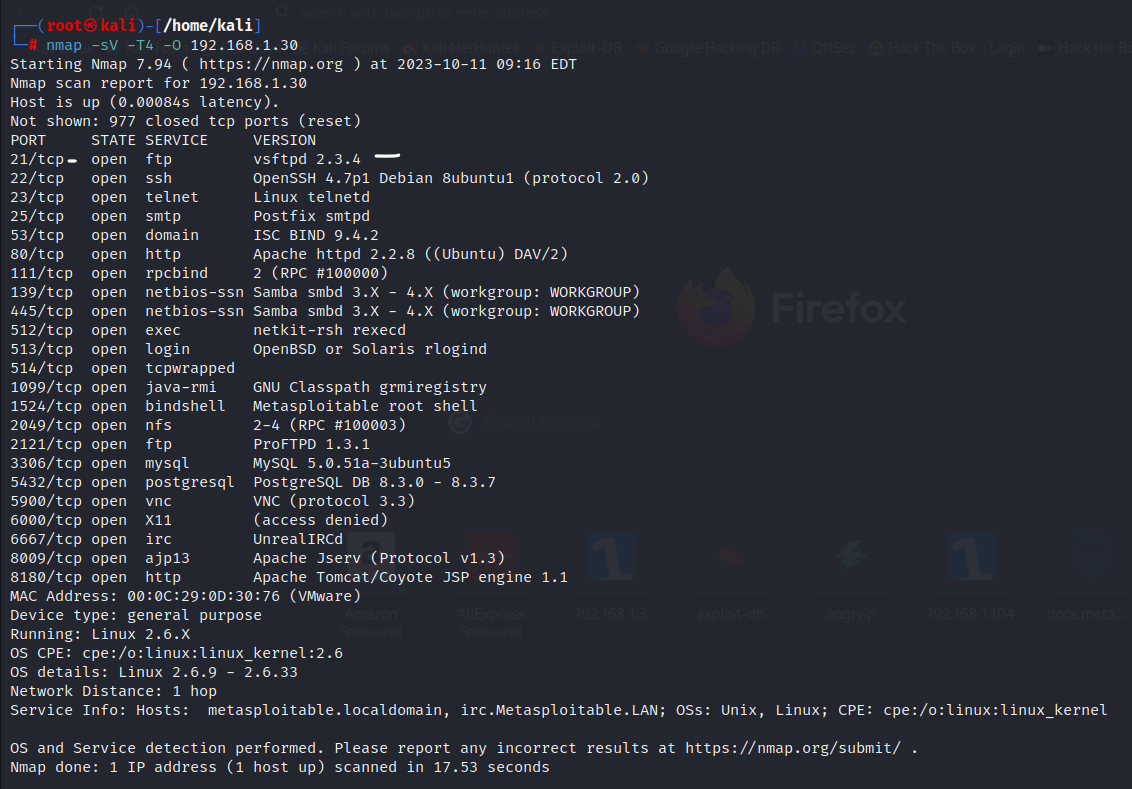


Now to check IP address of Metasploitable 2 we will need to use “**netdiscover**” command on Linux terminal to scan IP address in subnet range.



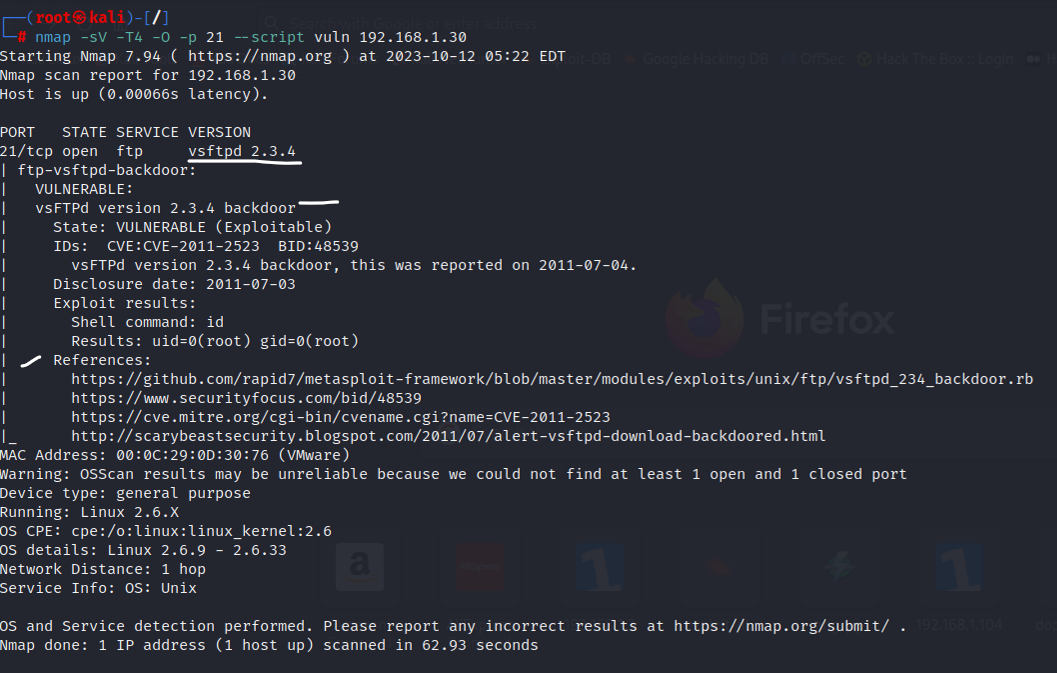
Since we have target machine mounted on VMware that’s why we can understand that IP address 192.168.1.30 is Metasploitable 2 Machine.

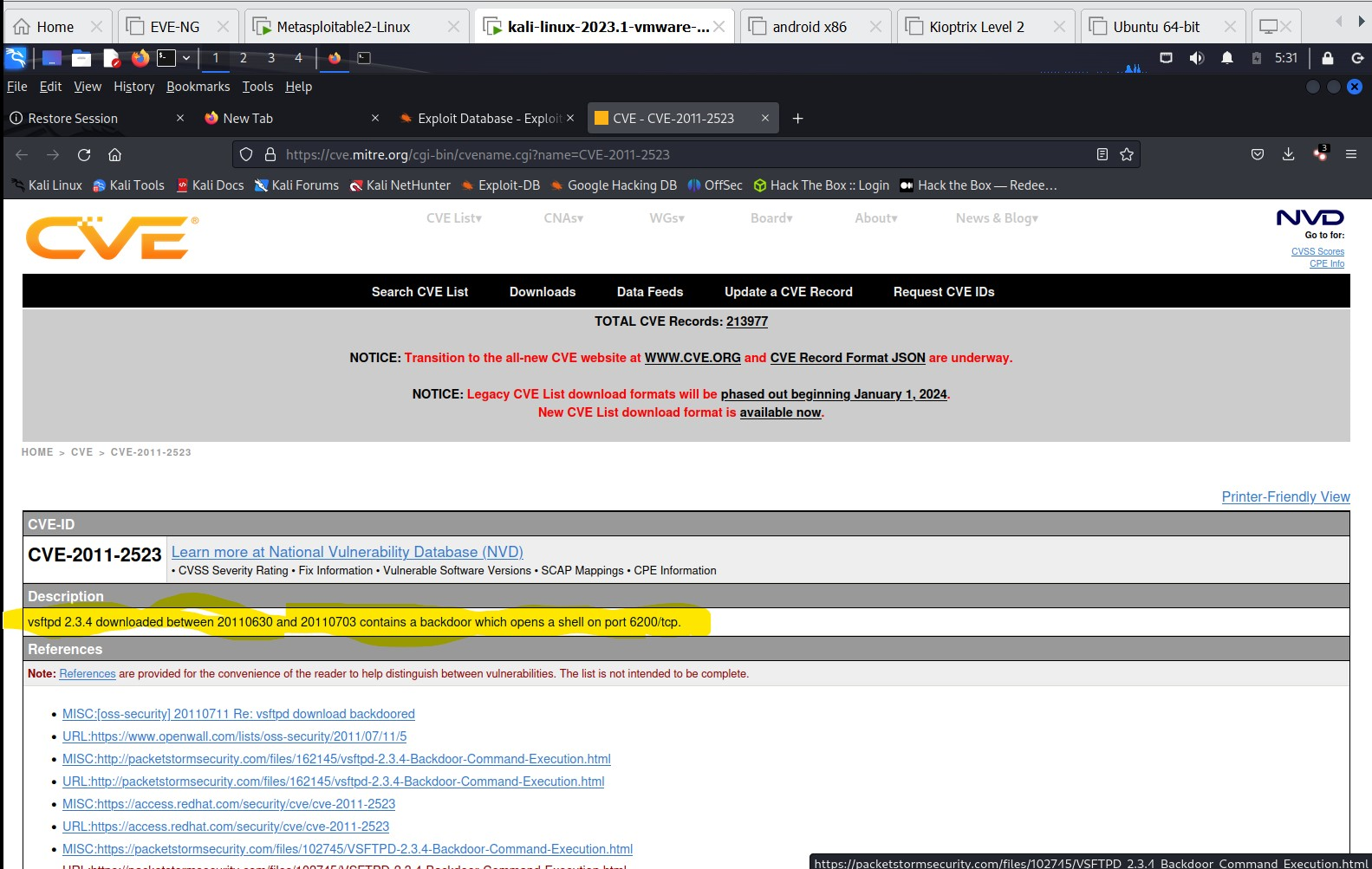
Next, we need to scan IP address 192.168.1.30 to check for open ports and Vulnerabilities, to perform this task we will need to run “**nmap**” on Terminal.

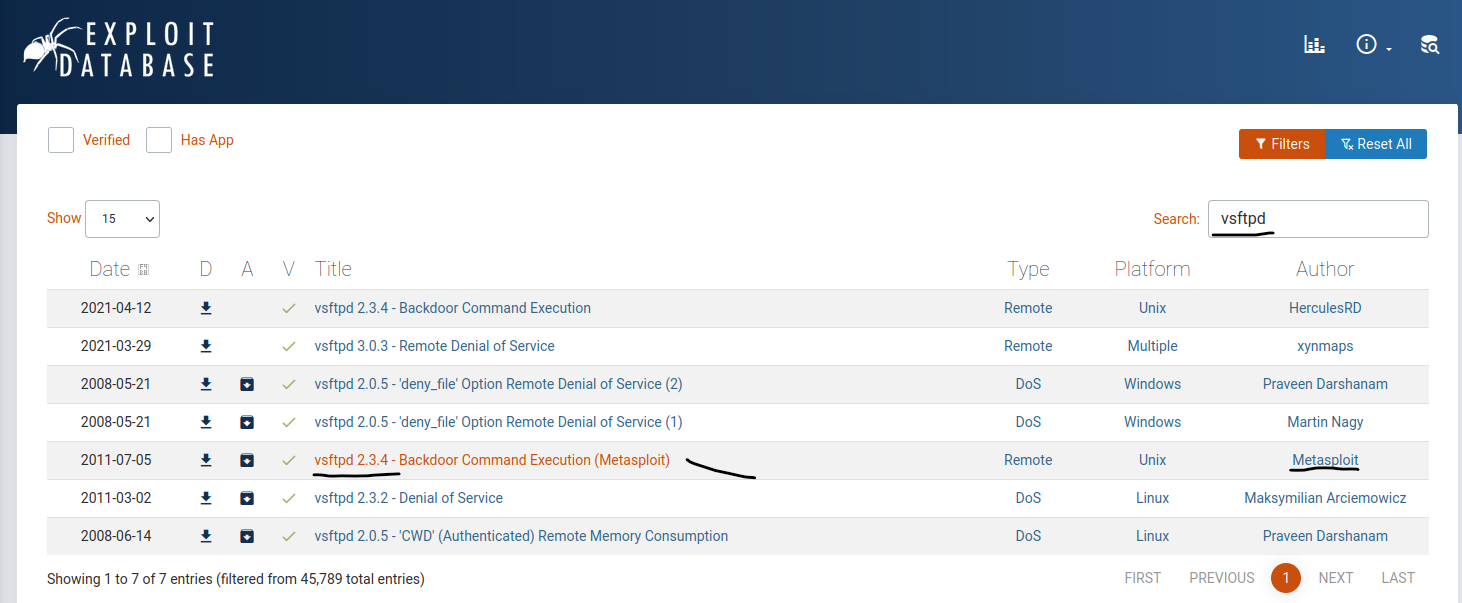


After scan we have identified that Port 21 is open and this port is used for ftp service and mentioned version vsftpd 2.3.4 is Vulnerable.

To check Vulnerability, we need to use nmap again for target IP with **-- script** **vuln** to confirm availability of exploit or we can also search for exploit manual on Exploit-db web site.





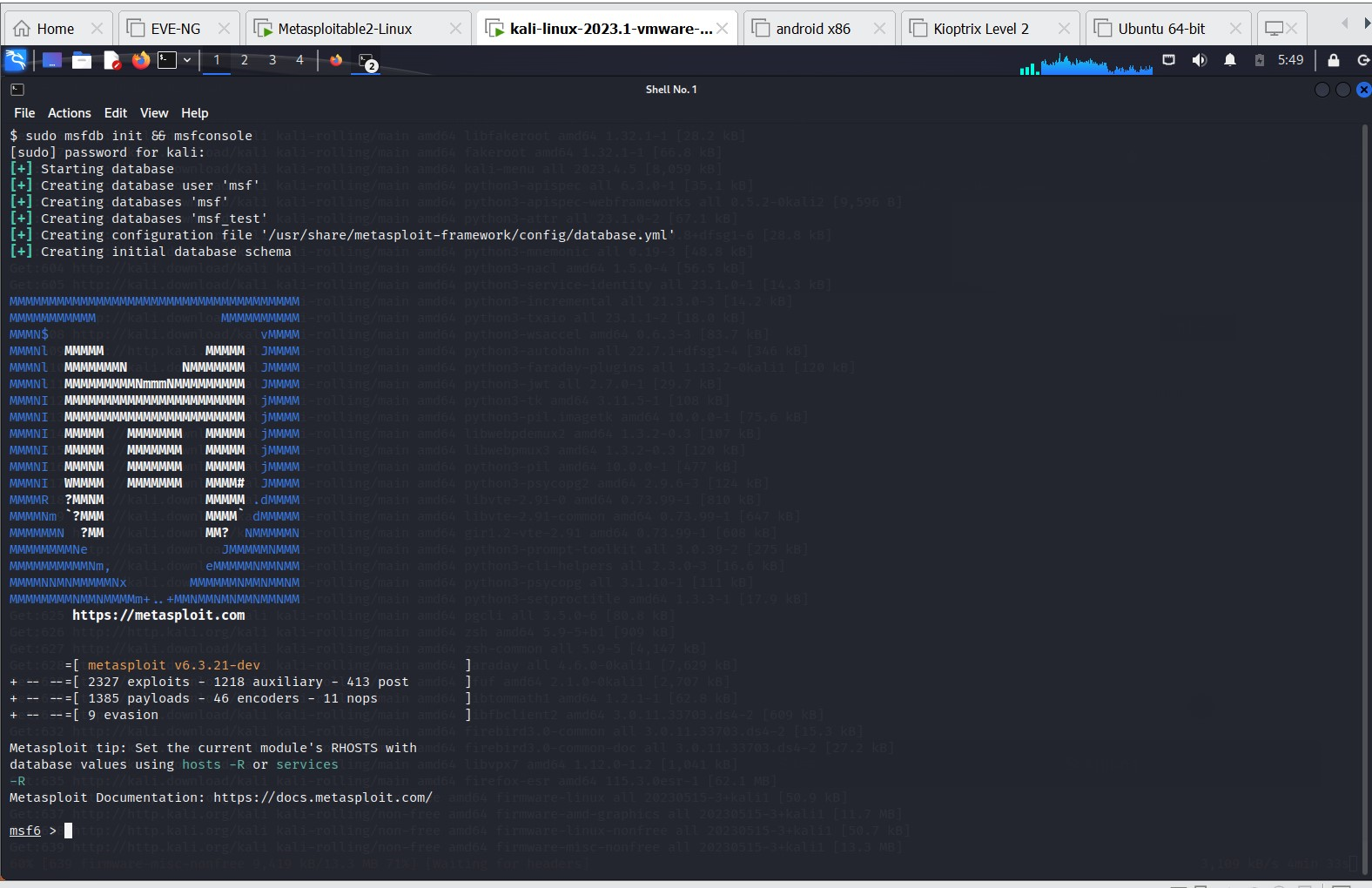


So, by checking on exploit it is clear that vsftpd-2.3.4 is a vulnerable version and can be exploited by Metasploit Framework.

## 4.2 Metasploitable 2 – Exploitation

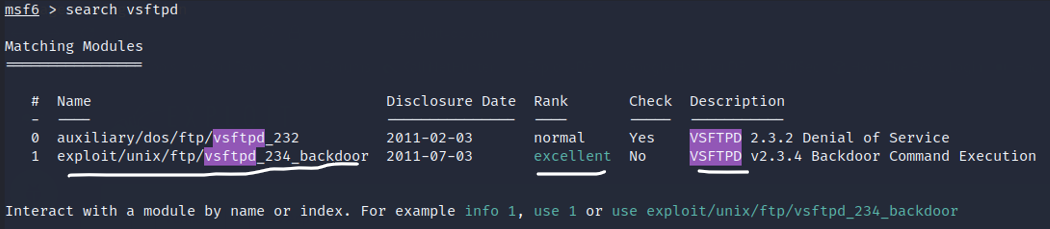
Now to run exploit we will first have to use Metasploit Framework i.e., already preinstalled on Kali Linux.

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 vsftpd-2.3.4 in Metasploit, we need to use command “**search vsftpd**” to check available exploit.

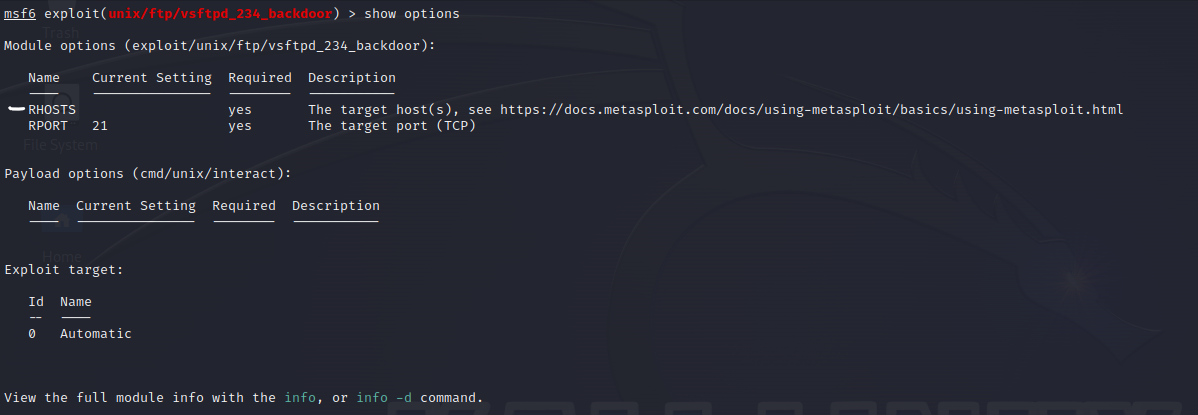


Now we need to select exploit, so we will use backdoor exploit, to confirm it we will use the command “**use exploit/unix/ftp/vsftpd\_234\_backdoor**”



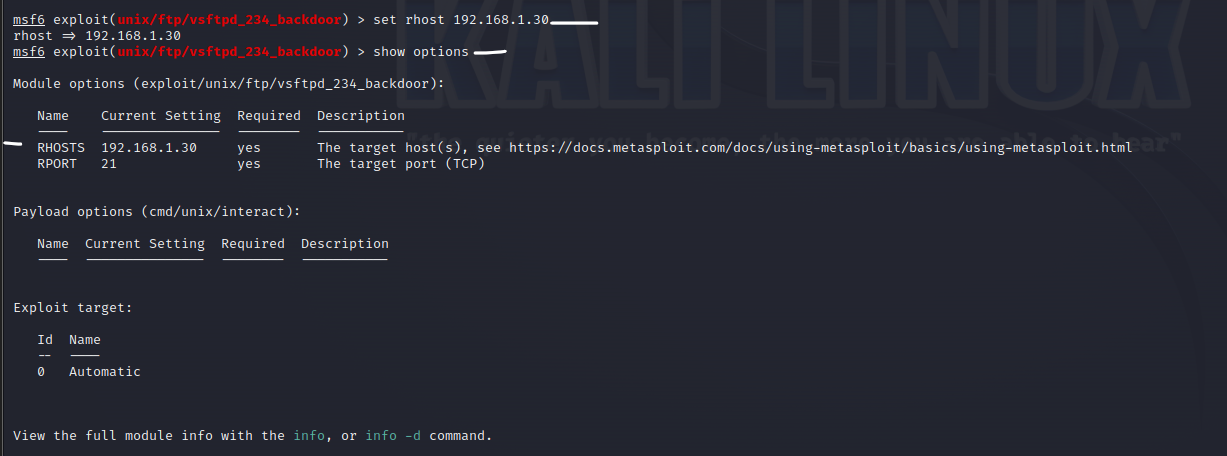
## 4.3 Metasploitable 2 – Gain Access to Root

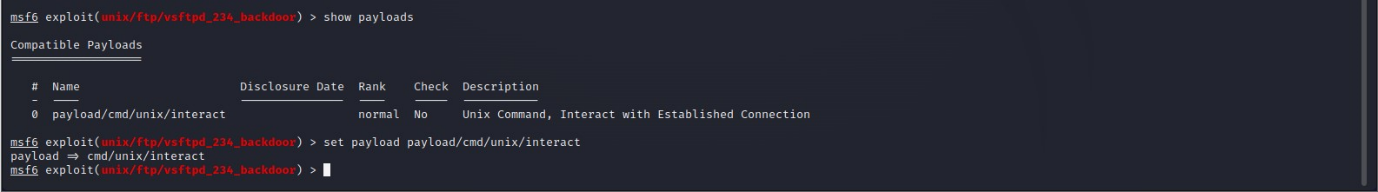
We need to check what parameters we need to set for target machine, to check that we need to run command “**show options**”



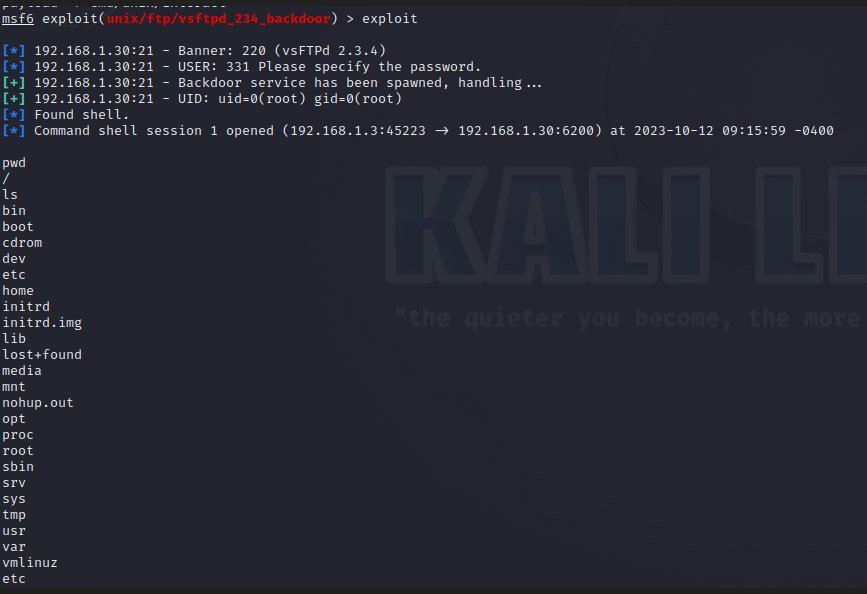
Here are two parameters, we need to set one only, as remote port no as 21, we need to set RHOST with target IP address.

To set this we need to use command “**set RHOST 192.168.1.30**”



So now we have set both options, only thing i.e., left is to set Payload. To check available Payload, we need to give command “**show payloads**” and then use command “**set payload payload/cmd/unix/interact**”

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 (Metasploitable 2).

For verification of access, I used the command “**pwd**” to check present working directory and the output is showing as “**/**” which indicates that we are in the root directory of the Target Machine. After this command I run command “ls” i.e., list command and all the directories that are present in root directory are visible to me. Hence, we are able to obtain **root access** of the Target Machine (Metasploitable 2).

# 5.0 Conclusion

We scanned port 21 and determined that a vulnerable version was running the FTP service on Metasploitable 2. By the help of Metasploit Framework we were able to gain root access of the target machine.