**Hacking Android Applications using Kali Linux tools**

**Naitik Rathod 1714108**

**Heet Sakaria 1714110**

We will implement and demonstrate how to hack mobile phones using Kali Linux. We can spy anybody’s mobile and get any kind of details like the applications installed in it, it's geo location, can dump the mobile contacts, get the mobile to behave mischievously like playing random music file, etc

So, here we are going to create a payload using kali linux terminal and we will send that payload to the victim’s mobile phone. After the installation of that app on the victim’s mobile, the app sends us all the data of the victim’s mobile phone. This is the main trick to hack any android phone through which we will be able to gain remote access to that android device.

**Installation**

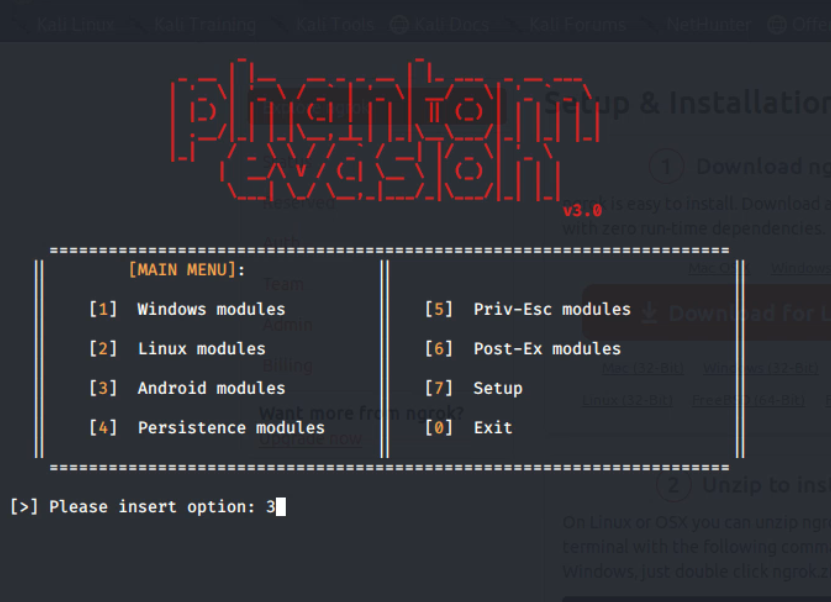
First we will install a pentesting tool named lPhantom Evasion by cloning from github link - <https://github.com/oddcod3/Phantom-Evasion> and runnin the setup through command python3 phantom-evasion.py --setup

We will use Ngrok which is a cloud service by which we will be able to run a program on your machine and provide it the port of a network service, usually a web server.

It automatically connects to the ngrok cloud service which accepts traffic on a public address and relays that traffic through to the ngrok process running on your machine and then on to the local address you specify

1. Launch phantom-evasion in interactive mode: using the command

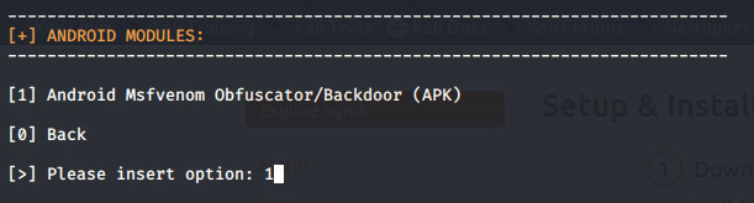
python3 phantom-evasion.py

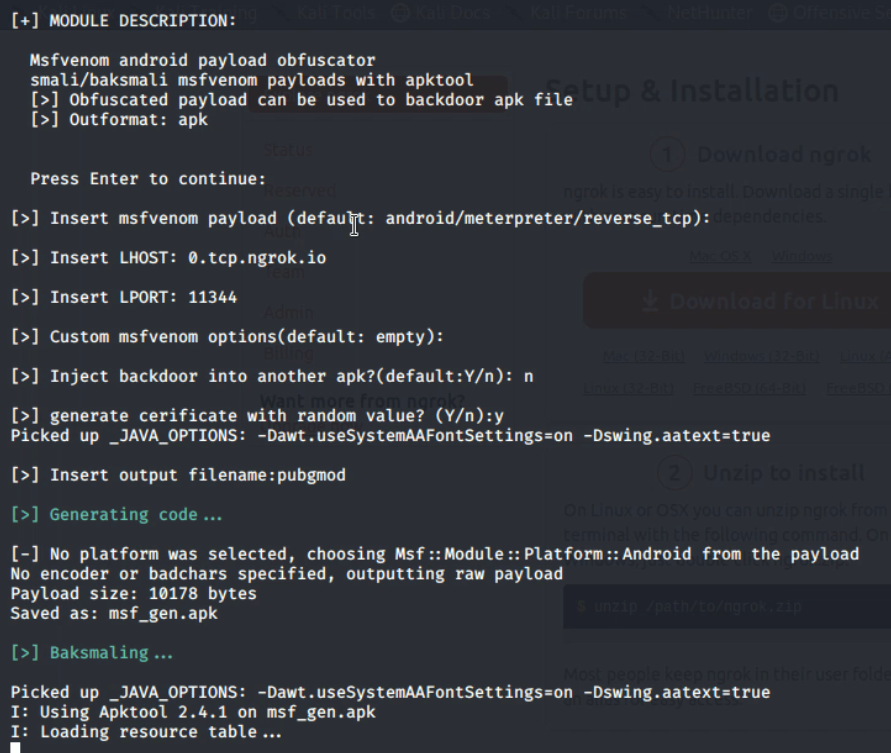


Since we want to create an android payload apk we choose the android modules .

Here, we will use MSFvenom for generating payload and save as an apk file and setup listener to Metasploit framework for Android tue default msfvenom is Android/meterpreter/reverse\_tcp

And then we insert the LHOST and Localport which will be established in the ngrok session which we have created.

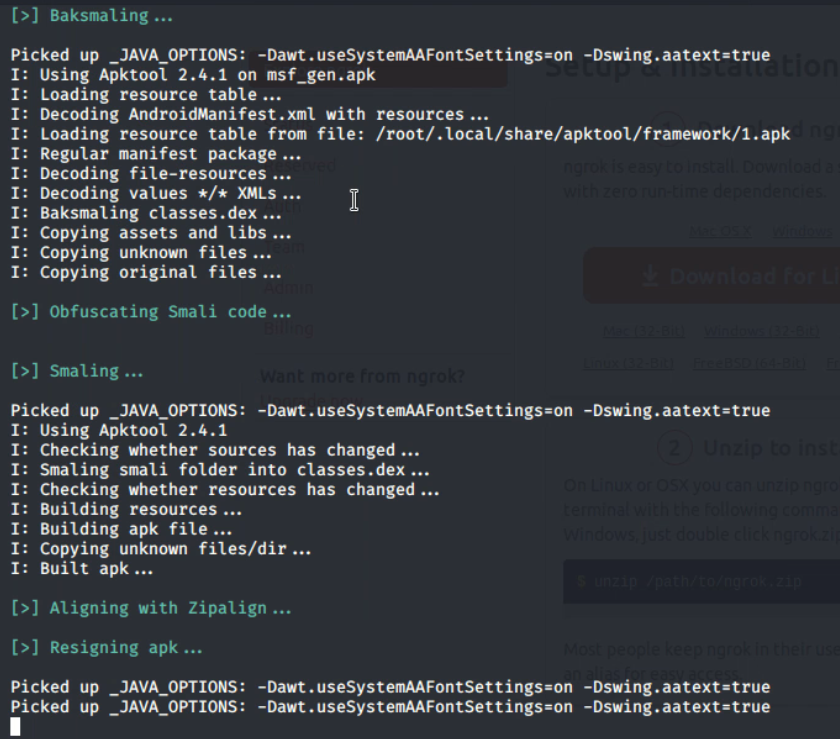


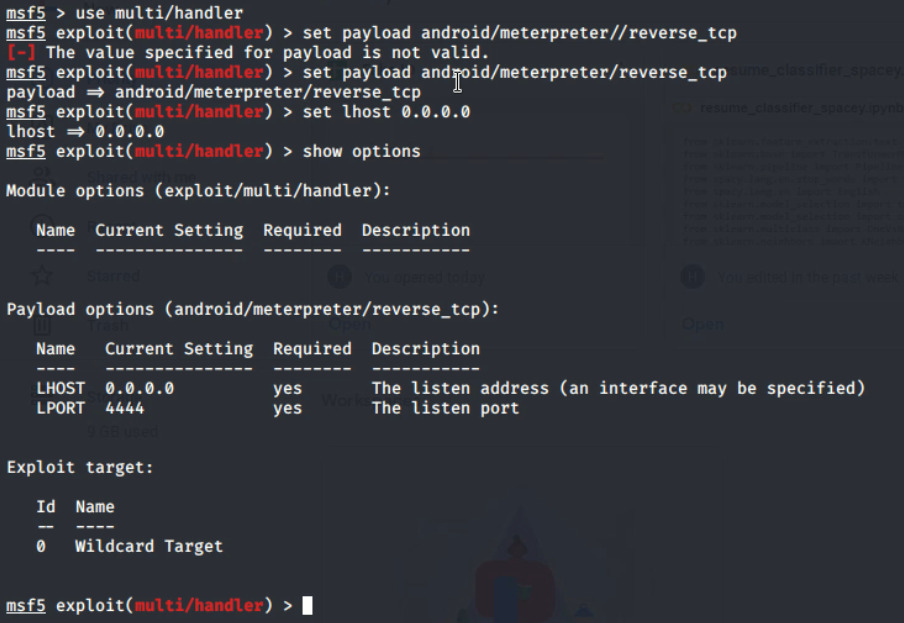


We need to have a sign certificate because Android mobile devices will not be allowing to installing apps without the signed certificate. Android devices only install the signed .apk files.

We need to sign the apk file manually in Kali Linux using:

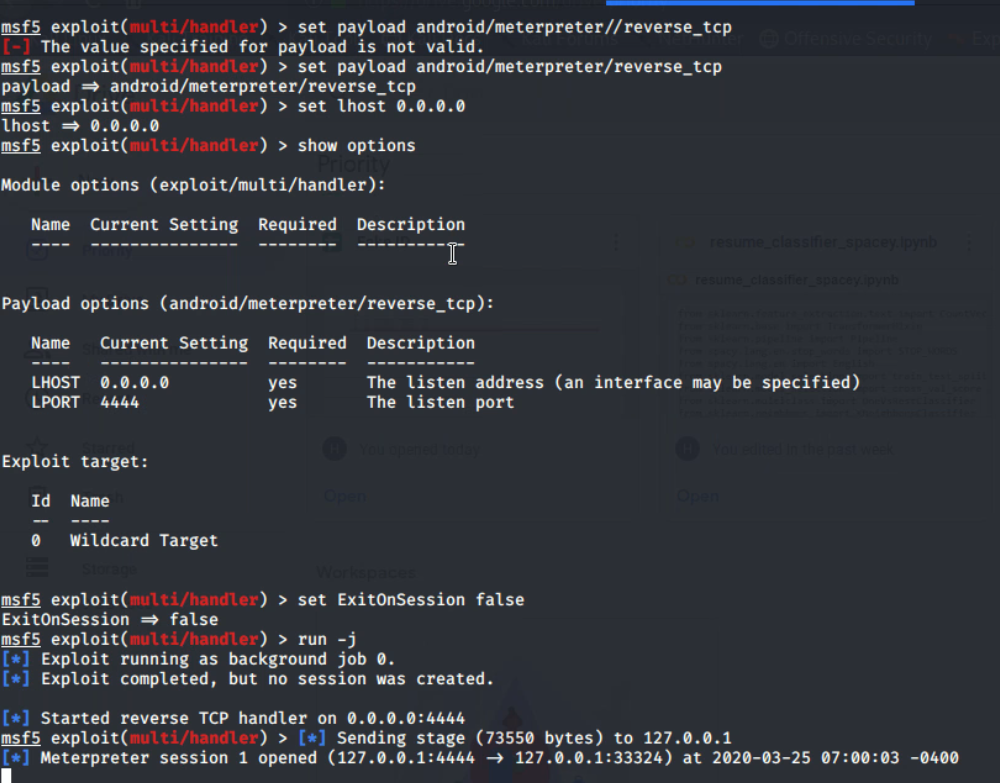
* Keytool (Preinstalled)
* jar signer (Preinstalled)
* zipalign (Need to Install)

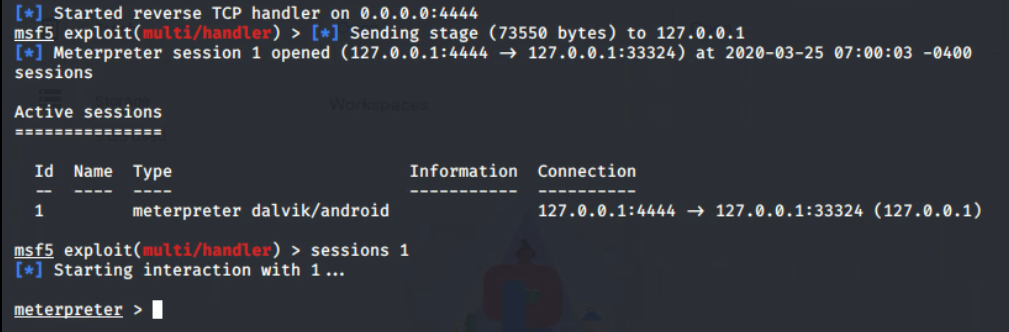
Phantom Evasion tool has Zipalign in itself so no need to install again Now we will set the name of the apk file which we will generate as pubgmod to increase the probability of the victim to install our app in their mobile applications. 

We will be using Kali linux tool called Metasploit by entering msfconsole command, we use multi/handler and set payload as android/meterpreter/reverse\_tcp which is the standard for android applications and then setting **LHOST** which is the ip address of pc used for hacking and **LPORT** is the port number generally set to **4444** by default also setting set ExitOnSession false which which eventually continue to search and create session with the apk and we don't need to start the hacking process from scratch.

LHOST – is a local host where you need to get session after payload execute

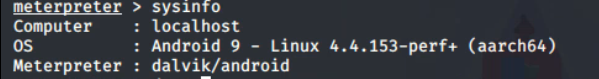
LPORT- Local port where you want session

Exploit – executing exploit

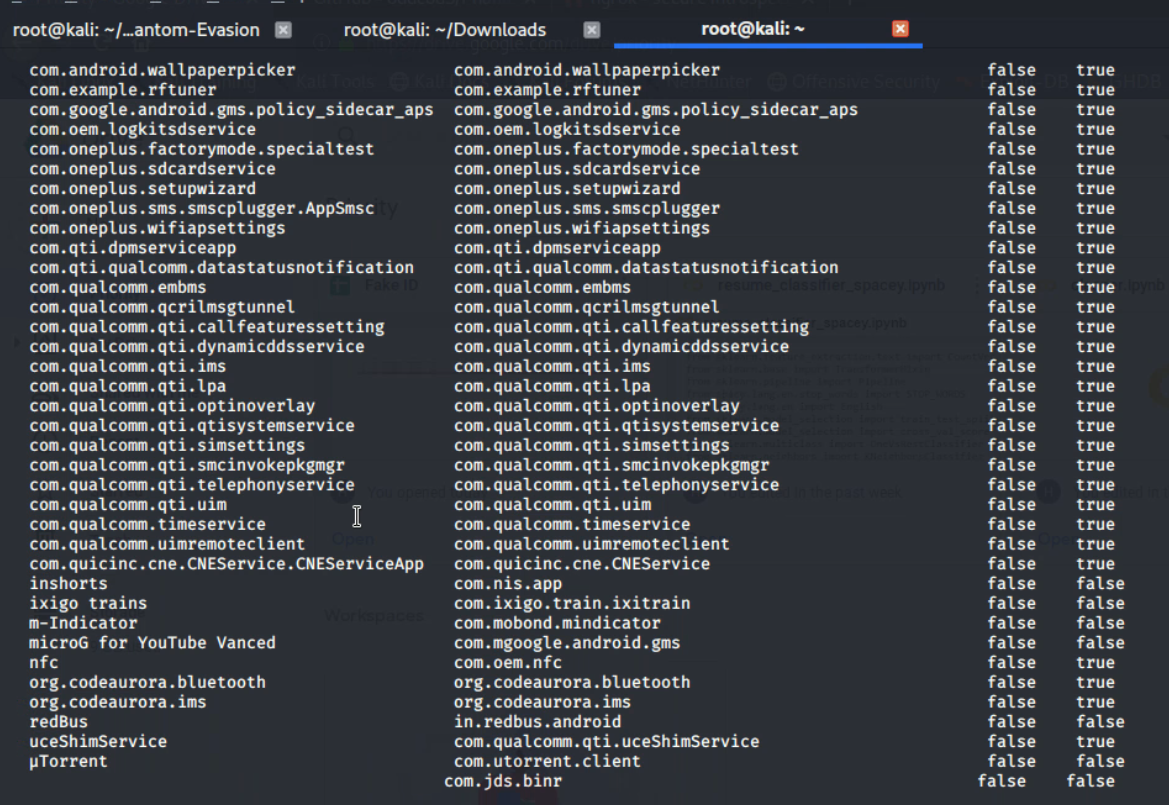


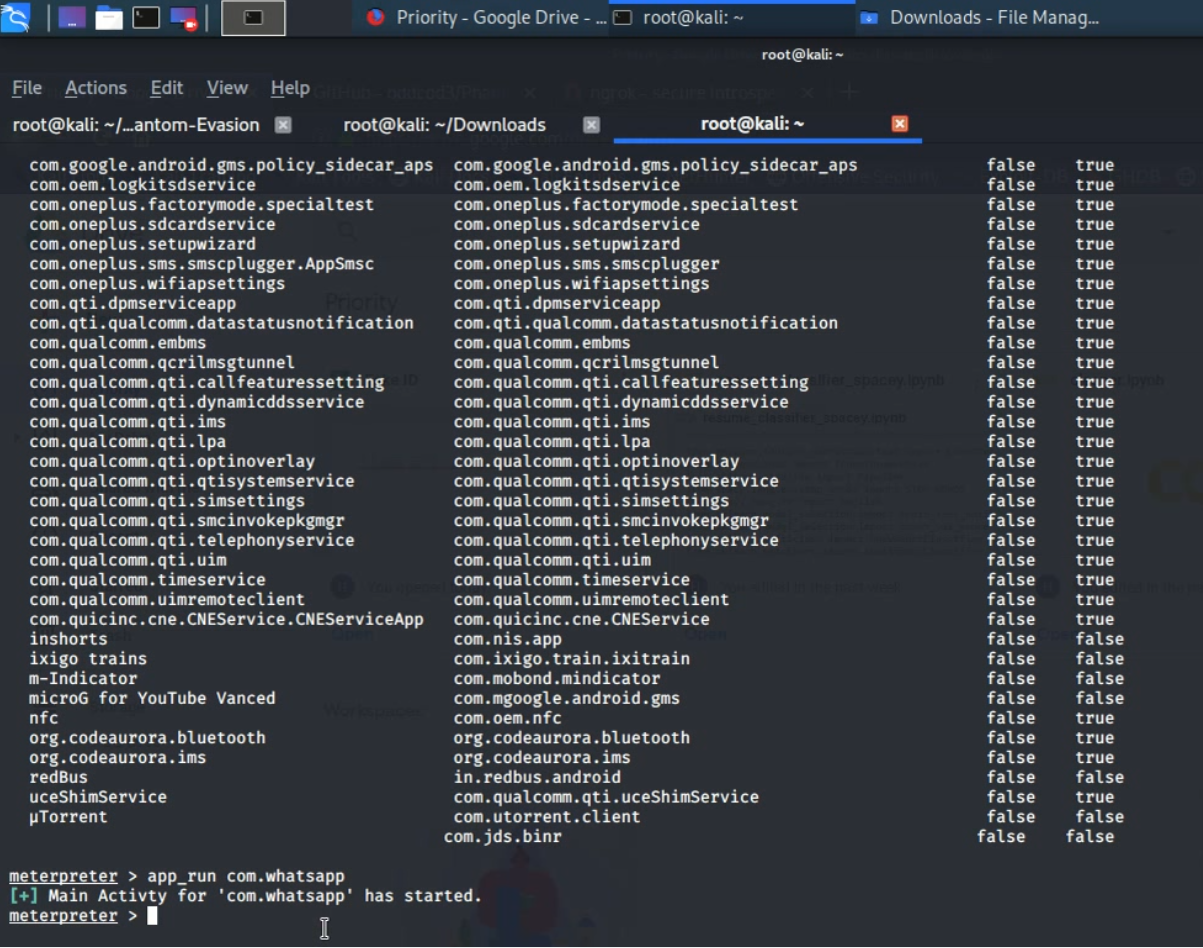
**Attacks**

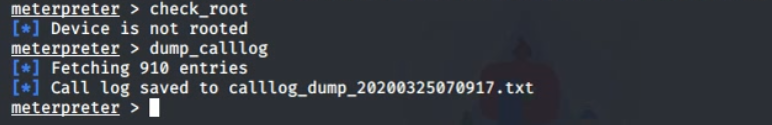
1 Getting the system information of the android device on which the payload apk is installed.As we can see the output that we come to know that the OS is Android 9



2 Getting details of the installed apps on the phone which will show a detail list of all the installed applications which are installed in the victims mobile

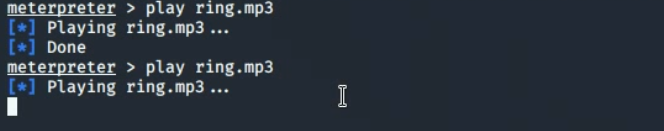


3 Getting any application in the victims mobile to run and open their mainActivity

4 Getting a detailed information about the call\_log of the victims mobile 

Below is the dumped call log output files which contains information like durations of the calls ,Date along with precise time



5 Maliciously playing Audio Files in the victim's android application

**Precautionaries**

Some ways to prevent these types of attack

* Don’t allow downloading any apps from cloud websites which asks for many unnecessary permissions required to run the app
* Don’t install apps with unknown resources enabled option.
* Use antivirus in a mobile device to keep an eye on every moment of mobile.
* Don’t click any random link
* Never download unwanted doc,pdf, apk file from unknown source
* Always confirm with source pertaining to file to double sure