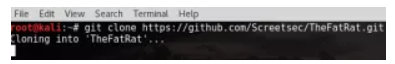
**Penetration Testing for Android Applications Using Kali Linux.**

This report is a process required to perform pen testing on Android Applications. This process is done in two simple steps It requires two libraries i.e. Fat rat and Metasploit. The whole and sole purpose of this application is for education use regarding Ethical Hacking.

**STEP 1:**

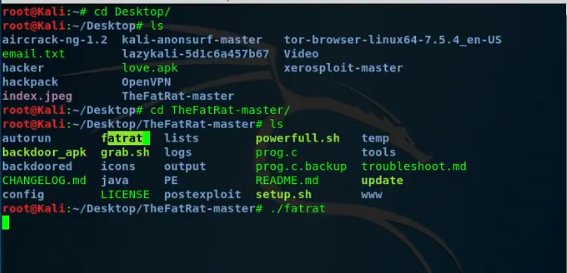
To pen test android applications, we first need to create an APK file and create a payload on that file to get all the information from the targets phone.

Install Fat Rat with the following command on image 1 in the terminal.

****

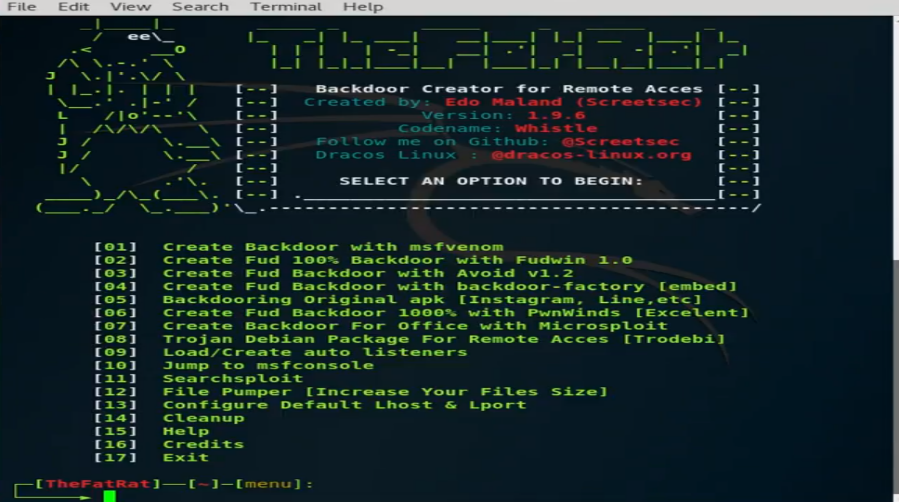
**Image 1**

Navigate to Fat Rat via terminal shown on Image 2:



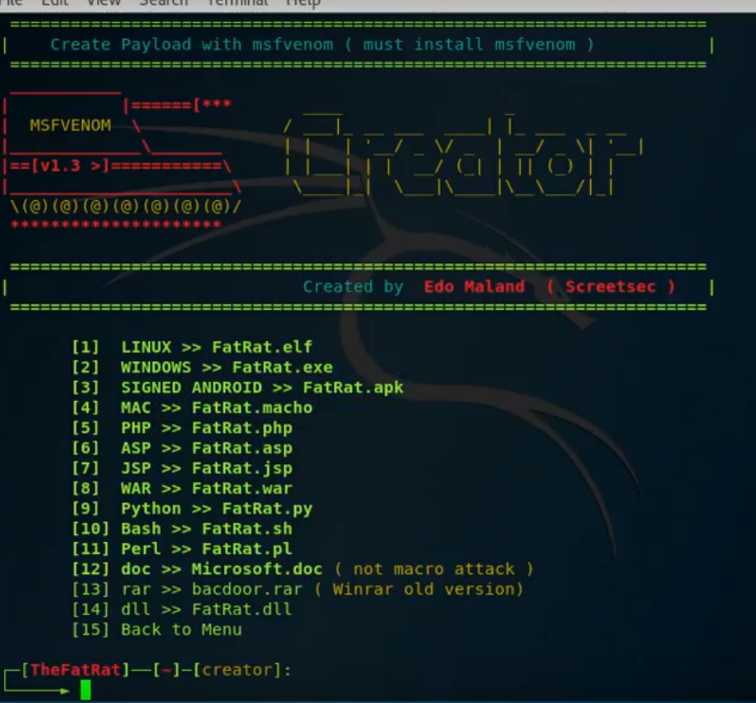
**Image 2**

The after a few steps the application will open as in Image 3:



**Image 3**

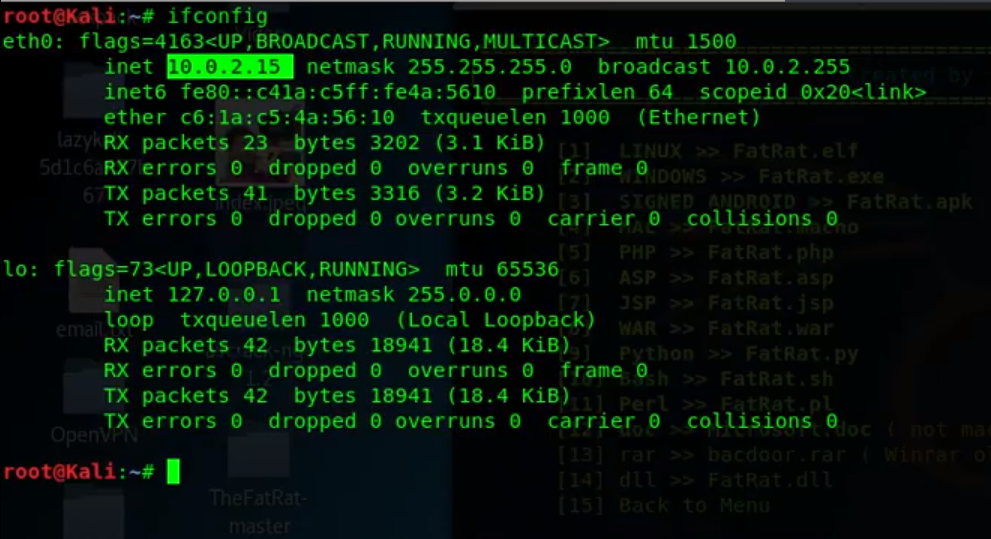
Select option 1: Create backdoor with MSF venom and it will navigate to as shown in image 4.

****

**Image 4**

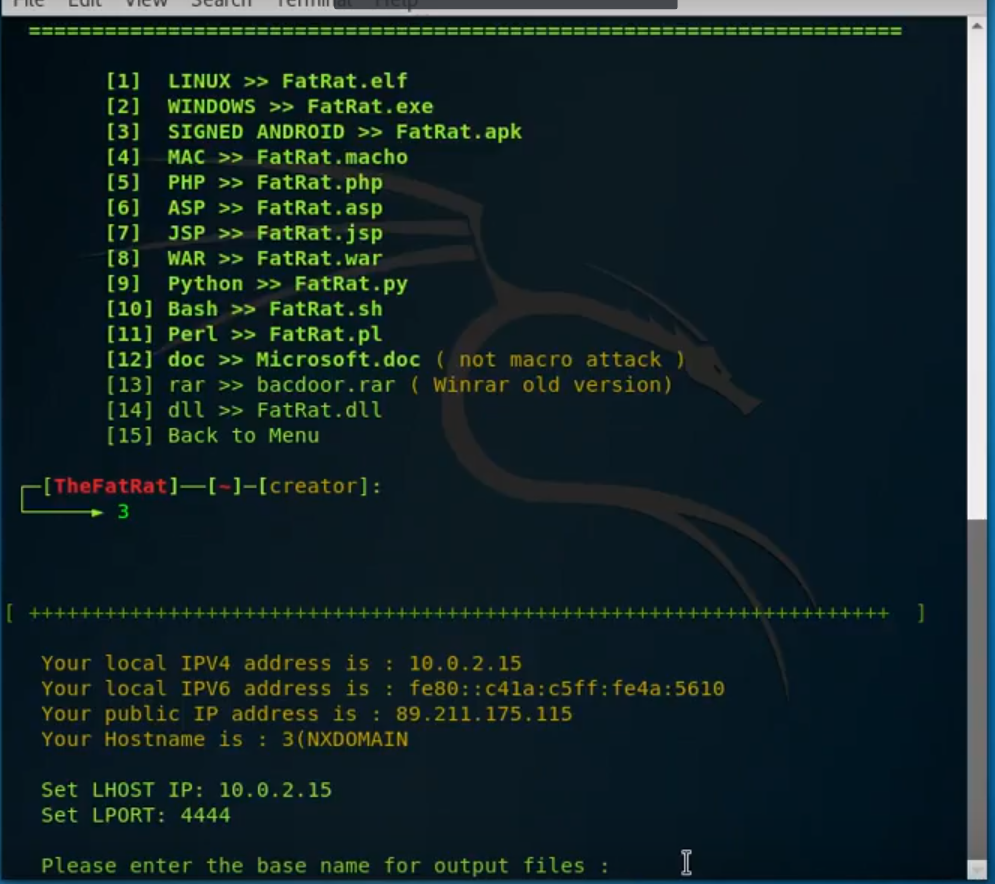
This section is to select the type of payload format you need. There are options like Linux, Windows, Android, MAC, Python and may more. But we are targeting on android so select 3.

Fat Rat will as for LHOST IP. To get the IP open a new terminal and type ifconfig. It will display as image 5.

****

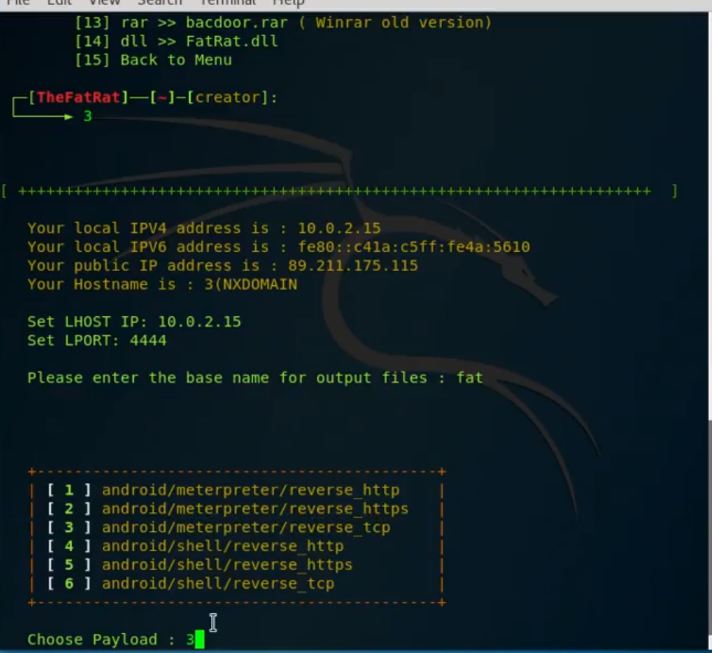
**Image 5**

Select the highlighted portion selected in image 4. Paste it in LHOST IP and set LPORT as 4444 as shown in image 6.

****

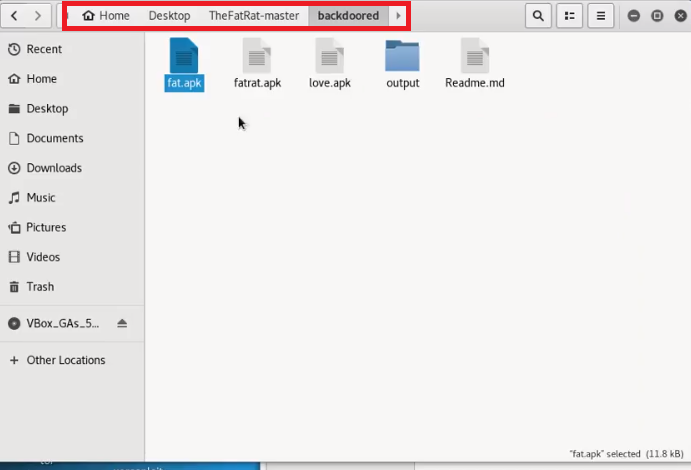
**Image 6**

It will then ask for a base name for output files. Any name can be selected on your choice. It will then ask for choose payload. Just select option 3 as shown in image 7.

****

**Image 7**

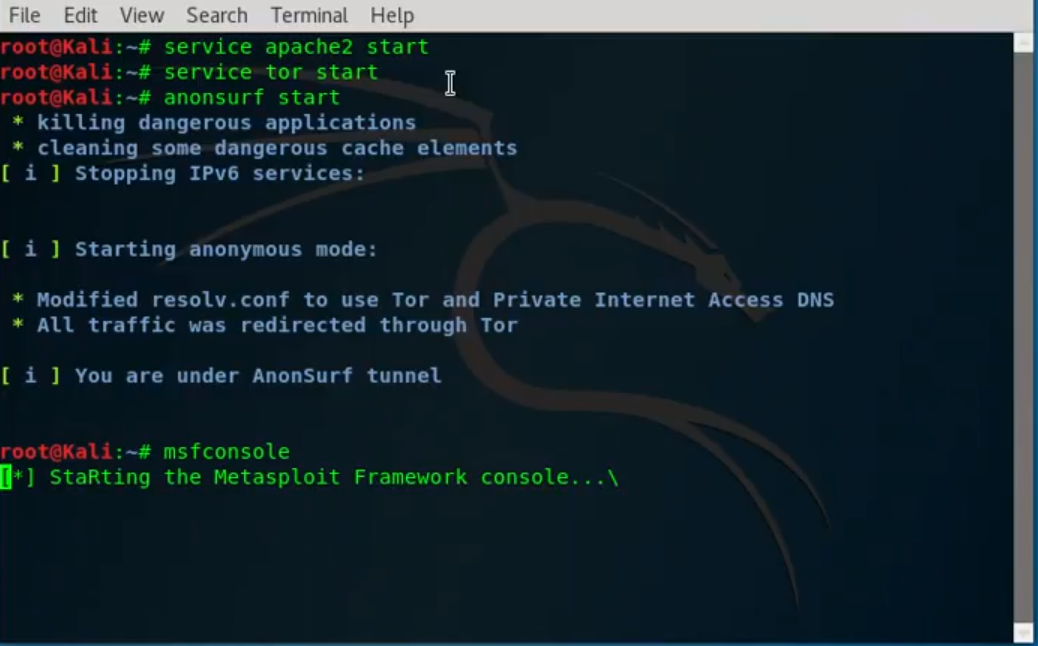
After selecting payload, it will ask to create a listener for this configuration. Press option y. IT will then as for name of this config. Type name of any choice. The process of creating payload on an Android APK is done. To get the APK file navigate to Fat Rat folder via Explorer as shown in image 8. Send this payload APK to the target device.

****

**Image 8**

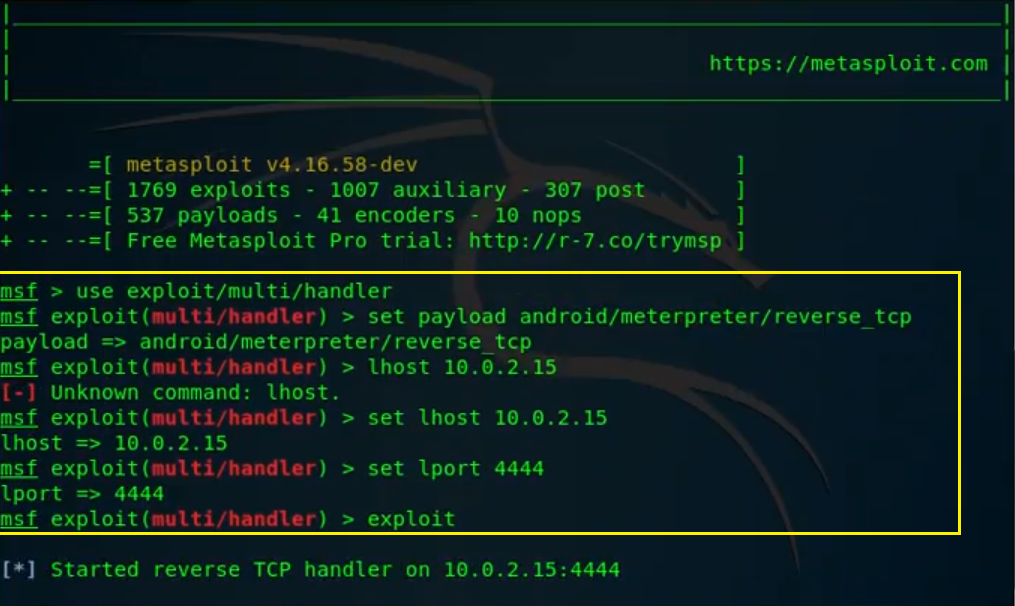
**Step 2:**

The step two is to gather information form target device. For this process Metasploit is used. Close all old terminal after creating APK file. Open a new terminal. Type the following commands as shown in image 9.

****

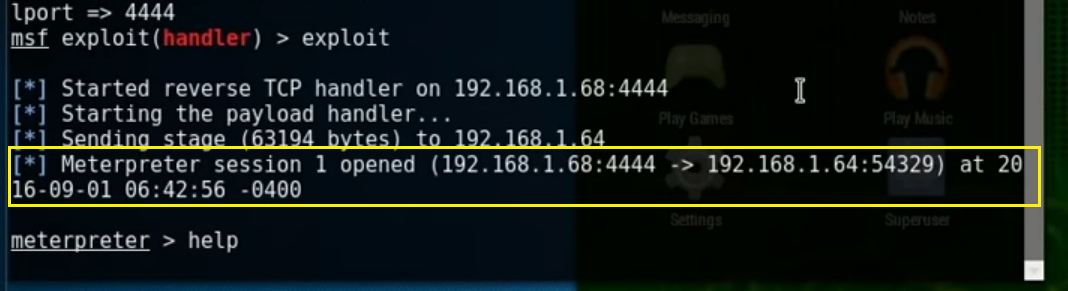
**Image 9**

Metasploit will then open MSF console and type the following commands according to your computers LHOST, LPORT set earlier in image 6. The guide for this step is on image 10 in yellow box.

****

**Image 10**

These commands it will start working. The moment you send the APK file that we create fat.apk to any mobile the target must install it and the app will start working and you will get the connection here on terminal. As the target will open the app session will start on Metasploit as shown in image 11 in yellow mark. Then you can type help and choose the option you want to exploit the device.

****

**Image 11**