

Forum:[Hack Forums](#)

Thread: [\[TUT\] \[Legends\] How to hijack a drone in the air!](#)

j1nx0 - May 14, 2016, 4:44 pm

DO NOT DO THIS FOR FUN, DO NOT BREAK SOMEONES DRONE, IM NOT RESPONSIBLE FOR ANYTHING YOU DO WITH THIS. - IF SOMEONE FUCKS WITH YOU FUCK THEM BACK.

"Others toil their entire lives to make a name for themselves, some are just born LEGENDS."

Hello everyone!

I will teach you guys how to hijack a WIFI drone while it's in the AIR, this tutorial will only teach you how to deauth the drone pilot and make the drone just stay in the air either you let the battery die in the air or you take over the control with the application FreeFlight 3. (This will deauth and malfunction every WIFI function in the drone. Which means that this would shutdown the camera on the DJI drones if I'm correct) I will link another tutorial at the end of this thread on how to take over the control and fly the hijacked drone with a raspberry pi

Requirements

- ROOTED Android device
- Someone with a drone
- Try not to do this so everyone sees you.

What do you mean with hijacking?

So, about 3-4 months ago a new shopping mall opened near me. It's really huge so they have a lot of new things there. One new thing was these drones that they were flying around with on a track they had made for drone usage. So I got an idea, I always knew that these wifi drones didn't have any security. When you connect to these you just simply tap their SSID on the application and you are connected there's no need to type in any kind of password in order to auth with the drone. This can break the drone, but in my case it did not, the drone crashed but survived it. So I thought I would try to deauth a pilot while he is flying his drone. So I pulled up my phone and connected to the wifi of the drone then I started the application called Wifi Kill (Download is below) meanwhile this guy flew his drone I saw the pilot on the Wifi Kill App. And I attached to the IPs and then I deauthed everyone who was on that network, and voila. He couldn't fly his drone anymore, the drone was just stuck in the air and he couldn't reach it. After 3-4 minutes the drone just crashed down. And no, it did not break so relax. If I was smart I could just auth with the drone by using the application for this drone. But I didn't.

Tutorial

Download Wifi kill app (REQUIRES ROOT): Spoiler ([Click to View](#))
<http://ybshare.com/download/wvc6ljk684#download>

Okay, so first off we need to install the application on our Android device. The usage of the application is really simple; You have to be connected to a Wifi network in order to use this application and deauth people. You start off by finding a wifi drone that someone is using, once that is done you go to your Wifi settings in your Android device and try to find it. Parrot drones are the most used wifi drones right now. I'll take the Bebop as an example. When you scan for networks in your Android device you should find an SSID called Bebop something. You will see that the network is open and you can connect to it. When you are connected you should start the WifiKill application. Press the "play" icon in the upper right corner and you will start to scan the network for connected devices. This is where you should find the pilot that is driving the drone. 2 IP addresses will appear in the list of WifiKill once the scan is done, it's you and the pilot. Instead of just trying to find the pilots IP you can simply just press "grab all" in the bottom left corner, this will attach you to all the devices connected to the network. This includes you and the pilot. Then press the magical button on the bottom right corner called "kill all" this will deauth everyone on the network. The pilot should not be able to move the drone anymore. This is where you connect to the drone via the application Bebop is using (FreeFlight 3)

Tutorials on how to fly the hijacked drone with scripts

https://www.youtube.com/watch?v=EHKV01YQX_w
<http://samy.pl/skyjack/>

SIM-2580909 - May 16, 2016, 3:31 am

My favorite part about this part about this tut was the very begining
"IF SOMEONE FUCKS WITH YOU FUCK THEM BACK" - j1nx0 2016

Infinite power - May 16, 2016, 3:35 am

Never thought about using wifikill like that. On the other hand I never even saw a drone so I didn't know they used wifi lmao.
Nice tutorial!

Edit: Link is broken.

esoteric? - May 16, 2016, 3:38 am

The download link is broken pls fix <3

Anarchist07 - May 16, 2016, 3:40 am

That's pretty awesome dude, maybe I should try this one day.

0x52-0x75-0x64-0x79 - May 16, 2016, 3:54 am

Could also be done with any unix OS and aireplay by the seems of it

j1nx0 - May 16, 2016, 4:35 am

(May 16, 2016 03:35 AM)Infinite power Wrote: [\[CITE\]](#) Never thought about using wifikill like that. On the other hand I never even saw a drone so I didn't know they used wifi lmao.
Nice tutorial!

Edit: Link is broken.

Thanks man! I fixed the link, if it gets broken again google wifikill apk and download it :)

(May 16, 2016 03:38 AM)HollowSquad Wrote: [\[CITE\]](#) The download link is broken pls fix <3It's fixed! :)

(May 16, 2016 03:54 AM)0x52-0x75-0x64-0x79 Wrote: [\[CITE\]](#) Could also be done with any unix OS and aireplay by the seems of it

Yeah but I believe this is the easiest way to do it unless you want to bring your whole workstation with you.

I added a RPI tutorial at the end of the tutorial.

Infinite power - May 16, 2016, 4:58 am

Just a heads-up according to avast the apk is a virus.

Although this doesn't prove much.

Probably because it needs root xD

0x52-0x75-0x64-0x79 - May 16, 2016, 4:58 am

(May 16, 2016 04:35 AM)j1nx0 Wrote: [\[CITE\]](#) Yeah but I believe this is the easiest way to do it unless you want to bring your whole workstation with you.

I added a RPI tutorial at the end of the tutorial.

Sorry didn't mean to sound like a dick. Good tutorial man :)

If you have a rooted phone and that, it's definitely the convenient method

Yeah RPI with Airplay should work also, comes down to choice and tools available

THEMANSF - May 16, 2016, 10:14 am

Cool tut, Well I guess I'm going to New York and hijacking Casey Neistat's drones. :D

regime - May 18, 2016, 3:42 am

Nice tutorial . GOnna try it LOL

Two-Ton 21 - May 20, 2016, 7:23 am

At first I was expecting this tutorial to be hard. I couldn't believe how easy it is to hack someone's drone. Now all you have to do is learn how to hack military drones. ?

j1nx0 - May 21, 2016, 12:39 pm

(May 20, 2016 07:23 AM)L3X LUTH0R Wrote: [\[CITE\]](#) At first I was expecting this tutorial to be hard. I couldn't believe how easy it is to hack someone's drone. Now all you have to do is learn how to hack military drones. ?

Yeah, I didn't think it was so easy either. It was first when I tried it I realized how easy it actually was.

L33tness - May 21, 2016, 1:04 pm

WOW. This has to be one of the GREATEST tuts i have seen on here. It is a very simple tutorial. But at the same time it is very well written and anyone could follow it without getting their d.ick stuck in a fan. LMAO. Great tutorial man! Will deff give it a test if i see any drones buzzing around.

Fatboy Slim - May 22, 2016, 10:33 am

unable to start service, do you have root?

j1nx0 - May 22, 2016, 10:39 am

(May 22, 2016 10:33 AM)Fatboy Slim Wrote: [\[CITE\]](#) unable to start service, do you have root?Hmm, not sure what you are trying to say but I guess you are asking if you require root.

You need to give the applications SU access so yes you have to root your device for this to work.

Fatboy Slim - May 22, 2016, 10:40 am

(May 22, 2016 10:39 AM)j1nx0 Wrote: [\[CITE\]](#) Hmm, not sure what you are trying to say but I guess you are asking if you require root.

You need to give the applications SU access so yes you have to root your device for this to work. I have, it still returns this error.

j1nx0 - May 22, 2016, 10:48 am

(May 22, 2016 10:40 AM)Fatboy Slim Wrote: [\[CITE\]](#) I have, it still returns this error. "service error - unable to start service, do you have rooted?" Error message is because the application has not been granted SU access. What phone do you have? Custom ROM? Do you have Supersu or superuser installed? You can provide me Logcat and I can have a look at it.

The problem seems to happen with people with an older phone because it doesn't have time to request SU access before the application start.

Fatboy Slim - May 22, 2016, 10:55 am

(May 22, 2016 10:48 AM)j1nx0 Wrote: [\[CITE\]](#) "service error - unable to start service, do you have rooted?" Error message is because the application has not been granted SU access. What phone do you have? Custom ROM? Do you have Supersu or superuser installed? You can provide me Logcat and I can have a look at it.

The problem seems to happen with people with an older phone because it doesn't have time to request SU access before the application start.

Hi, here you go <http://www.filedropper.com/log2016-05-2219-52-24>

I have a nexus 5 (hammerhead) and it has been granted superSU access already. It's on the stock rom with TWRP as recovery.

j1nx0 - May 22, 2016, 11:07 am

(May 22, 2016 10:55 AM)Fatboy Slim Wrote: [\[CITE\]](#) Hi, here you go <http://www.filedropper.com/log2016-05-2219-52-24>

I have a nexus 5 (hammerhead) and it has been granted superSU access already. It's on the stock rom with TWRP as recovery.

Really weird, log looks okay. You can see Wifkill in the list of granted applications aswell I guess.

Sorry man, I don't think I can help you it works on my two phones and I have 1+1 and SGS6 works on both. I know this is a common problem with Wifkill but try googling it and see what other people have done.

Fatboy Slim - May 22, 2016, 11:09 am

(May 22, 2016 11:07 AM)j1nx0 Wrote: [\[CITE\]](#) Really weird, log looks okay. You can see Wifkill in the list of granted applications aswell I guess.

Sorry man, I don't think I can help you it works on my two phones and I have 1+1 and SGS6 works on both. I know this is a common problem with Wifkill but try googling it and see what other people have done.

Ok, not a problem. Thanks for looking into it regardless.

Nice tutorial as well, shame it doesn't work for me.

j1nx0 - May 22, 2016, 11:21 am

(May 22, 2016 11:09 AM)Fatboy Slim Wrote: [\[CITE\]](#) Ok, not a problem. Thanks for looking into it regardless.

Nice tutorial as well, shame it doesn't work for me.

Thanks man, I'm sorry that it's not working for you.

There could also be a problem with the Wifikill application since this is modified.

Check this original free version;

<http://forum.xda-developers.com/showthread.php?t=1282900>

Let me know if that one works.

Fatboy Slim - May 22, 2016, 11:26 am

(May 22, 2016 11:21 AM)j1nx0 Wrote: [\[CITE\]](#) Thanks man, I'm sorry that it's not working for you.

There could also be a problem with the Wifikill application since this is modified.

Check this original free version;

<http://forum.xda-developers.com/showthread.php?t=1282900>

Let me know if that one works.

Sadly that did not work either. Do you reckon there is an alternative to this app?

j1nx0 - May 22, 2016, 11:37 am

(May 22, 2016 11:26 AM)Fatboy Slim Wrote: [\[CITE\]](#) Sadly that did not work either. Do you reckon there is an alternative to this app?

Not that I know, I've searched around a bit but I didn't manage to find any application that is similar.

What you can do though is to use "Linux deploy" deploy kali and deauth with terminal commands:

<http://www.aircrack-ng.org/doku.php?id=deauthentication>

But this is a complicated way of doing it, this takes time etc. You could do it with a laptop aswell.

Rubixa - May 22, 2016, 11:56 am

HQ Tutorial my friend, Great contribution.

AristoCrack - May 24, 2016, 10:03 am

Thank you bro i will try it lol seems funny ! but link is not valid more, i have downloaded from another site, upgrade your link for other peoples ;)

j1nx0 - May 26, 2016, 4:37 am

(May 24, 2016 10:03 AM)AristoCrack Wrote: [\[CITE\]](#) Thank you bro i will try it lol seems funny ! but link is not valid more, i have downloaded from another site, upgrade your link for other peoples ;)

Link is valid.

Hermenaut - May 26, 2016, 4:53 am

There's another app, NetCut. Since WiFiKill doesn't work for everybody, this helps. There is even a Widows application for it, so you can kill someone's connection right from your laptop too. It works by ARP flush, so if the victim has some kind of protection against that, it won't work. But most don't.

j1nx0 - May 26, 2016, 6:10 am

(May 26, 2016 04:53 AM)Hermenaut Wrote: [\[CITE\]](#) There's another app, NetCut. Since WiFiKill doesn't work for everybody, this helps. There is even a Widows application for it, so you can kill

someone's connection right from your laptop too. It works by ARP flush, so if the victim has some kind of protection against that, it won't work. But most don't. Thank you for this!

AAA+ - May 27, 2016, 8:11 am

OP saw this on Defcon and decided to write about it. LOL!

But hey a written tut is better then a video

j1nx0 - May 27, 2016, 8:18 am

(May 27, 2016 08:11 AM)AAA+ Wrote: [\[CITE\]](#) OP saw this on Defcon and decided to write about it. LOL!

But hey a written tut is better then a video

No I actually saw Samy's video and used my brain to know that WifiKill also deauths.

santeez - May 28, 2016, 5:59 am

Dope guide. I'll check this in shop next to me xD

j1nx0 - June 29, 2016, 12:34 pm

(May 28, 2016 05:59 AM)santeez Wrote: [\[CITE\]](#) Dope guide. I'll check this in shop next to me xD
Just be careful when doing it, don't break someones drone.