

Forum:[Hack Forums](#)

Thread: [Sniff mobile data packets](#)

Tomsexitas5 - February 8, 2019, 12:40 pm

Hello. There it is: I need to sniff packets from an app, which only uses mobile data (as soon as it sees that I'm using Wi-Fi, it shuts off). Software: Android. Rooting is not an option (app doesn't work when rooted). I came up with few options on how I could approach this and with all of them I came to a dead end. So here are these options. Maybe someone will have a solution for at least one of them.

1. Somehow use some Wireshark alternative on Android. I highly doubt that it could work in any way as those apps need rooting. Also, I need to change routing tables, so probably these things will not work on-device.
2. Somehow spoof Wi-Fi connection as mobile. Again. Probably could work only on rooted phones. But I wonder if such spoofing could work in like a virtual android machine on PC?
3. Create an evil twin (fake AP).. Just not as Wi-Fi, but as LTE/3G (mobile data in general) router, so my phone would connect to like my pc (or other android phone, which is then connected to pc) via mobile data instead of WiFi. It's a stretch, but in my opinion it's the best option ;D

Also. I believe this application works on Windows, but I'm not very positive if my specific task would work, so before doing anything, I wonder if it is possible to change iptables (or whatever they're called in Windows environment) on Windows tablets that support SIM cards? And would those changes apply to mobile data? It's quite hard to get windows machines that support SIM cards, so I haven't thought heavily about this option.

So.. hopefully someone understood what I'm asking for and is willing to help a poor soul.

pasnger57 - February 8, 2019, 2:45 pm

IF you had a Cell repeater fem_to_cell you could perform your own MITM

<https://en.wikipedia.org/wiki/Femtocell>

Tomsexitas5 - February 9, 2019, 5:43 am

(Feb 8, 2019 03:45 PM)pasnger57 Wrote: [\[CITE\]](#) IF you had a Cell repeater fem_to_cell you could perform your own MITM

<https://en.wikipedia.org/wiki/Femtocell>

That's pretty interesting. But I was trying to avoid buying extra hardware for a one-time problem. On the other hand, I have extra android phone with which I can do whatever I want. I wonder if it would be possible to somehow fake such a device with phone's hardware? I mean.. It already has an antenna capable of transmitting cellular information.

Edit:

Apparently, Windows option is ruled out because my required settings are not compatible with Windows version of the application.

Also, emulator situation is ruled out as app disallows the use of it on emulator.

daizu - February 11, 2019, 9:41 pm

Can i know what app are you talking about you want to sniff?

Tomsexitas5 - February 12, 2019, 4:30 am

(Feb 11, 2019 10:41 PM)daizu Wrote: [\[CITE\]](#) Can i know what app are you talking about you want to sniff?

I doubt that it's going to help. But what the hell.. App: HTTP Injector. I have a payload that's locked and cannot see what's inside it. Payload is locked in all the ways possible. No wifi, no emulators, no root.. So there are two ways to read what's inside of it:

1. Try to decrypt the payload file (probably impossible).
2. Try doing man in the middle attack via mobile data.

daizu - February 12, 2019, 4:45 am

(Feb 12, 2019 05:30 AM)Tomsexitas5 Wrote: [\[CITE\]](#) I doubt that it's going to help. But what the hell.. App: HTTP Injector. I have a payload that's locked and cannot see what's inside it. Payload is locked in all the ways possible. No wifi, no emulators, no root.. So there are two ways to read what's inside of it:

1. Try to decrypt the payload file (probably impossible).
2. Try doing man in the middle attack via mobile data.

Lol haha i know that application

Your frm ph ?

Tomsexitas5 - February 12, 2019, 9:05 am

(Feb 12, 2019 05:45 AM)daizu Wrote: [\[CITE\]](#) Lol haha i know that application

Your frm ph ?

Nope.