

Forum:[Hack Forums](#)

Thread: [Capture user credentials \(NOTE: Requires JailBreak\)](#)

Pirni - September 29, 2015, 4:02 am

Requirements: Pirni.

Jailbroken device.

* Xsellize repo

-

First off, this is not a tutorial that will make you a l33t hacker in a day. This is just a simple thing you can do to monitor public networks or your own & see if you can obtain any credentials.

You could use it if you suspect someone is using your internet, or if you just want to try and get a friends password (Although this will require you to stay outside their house and wait).

-

First step: Installing the REPO & Pirni

Cydia > Manage > Sources > +

Repo: <http://cydia.xsellize.com>

Wait for it to install, then go to the search and search for "Pirni".

Download either the terminal one or the GUI.

I recommend the GUI as it's easier.

Second step:

Connect to either a public wifi network, or someone who you want to spy on. You can use iWeb Pro to get a router password or try to get it your self.

Open up Pirni, and everything should be already set up.

It will log everything to /tmp/log.pcap which I will explain later.

Try to start the sniffer, and if it says something like "Could not parse PBF filter" then just remove anything in the third column so remove tcp usd whatever 80 and leave it blank.

Third step: Basic stuff

Deciding whether you want to capture user:pass, or just random crap.

If you want to capture user:pass/email:pass go to the "Regex" thing and select them all or create your own.

If someone logs in, it should give you something like this in the log

Post:

Headers:

Referrer:

etc, and the user:pass/email:pass.

It will also show in the live packet sniffing thing.

Fourth step: Finding the log.

You can choose to pay for iFile or get it from xsellize. Just search iFile and download it.

All you need to do is locate the /tmp folder, and go to /log.pcap

NOTE: It will be removed on phone restart so you can choose somewhere else to log the information.

Fifth step: Yolo.

Camp out at McDonalds free wifi and watch all the skiddies log in, while they unknowingly give you their info.

Thanks for reading this quick and simple tutorial, and if you found it helpful please leave a thanks in the thread :)

YungTrigz - September 29, 2015, 4:35 am

So It's a MITM attack that you can do from an iPhone? Seems pretty cool.

Mr. Robot - September 29, 2015, 4:39 am

Android - download Droidsheep/fing/piik/zANTI/.

You don't need this big long tutorial but cheers OP - hope I helped you instead.

Also - you can install android on an old iphone if your bored. :D

Best investment you can make though is rooting an android and putting getting pixiewps running on it - easy wifi password

Droidsheep and zANTI allow you to not only capture passwords but sslstrip and also inject javascript into each page visited - change all images the victim will see

Also you can just log in with their session ID without their password and view everything they look at with a tool like Driftnet

Pirni - September 29, 2015, 4:42 am

I want to buy an android, no money right now.

Got a family members old one but I'm not too good with androids.

Besides now that my iPhone is broken, might need to use it.

Pirni - September 29, 2015, 5:02 am

Well, I guess I'll be downloading a few of those soon :p
thanks lol

Pirni - October 3, 2015, 4:21 am

Still available if anyone's interested in a simple mitm attack on an iPhone.