

Forum:[Hack Forums](#)

Thread: [\[Tut\] Pirni Pro- How to Sniff packets with your iDevice](#)

Bot Seller-Crypting Shop™ - September 11, 2011, 8:32 pm

Packet Sniffing with Pirni Pro

Ever wanted a portable packet sniffer for easy, quick access on the go? Well, you're in luck! Pirni Pro is the iPhone's first GUI Packet Sniffer. What it does is simple. It connects to the local router and intercepts all outgoing traffic from the users on that network where it is recorded, then forwarded back to the router.

Now, This may seem intimidating but let me assure you it is very easy to get the hang of.

How to download

The app is hosted by BigBoss and Cydia store for \$1.99. There are alternative sources (xSellize.com and h7v.org) that offer the app for free, but it's always good to support the developer.

Sniffer

The GUI makes this app very easy to use without sacrificing power. The home page should look something like this

[img=450x600]http://i1103.photobucket.com/albums/g463/roflkitties/IMG_0412.png[/img]

Now allow me to explain these functions.

- 1) Source IP: By default, 192.168.1.1 This is the default address for connecting to your router. Meaning, it will grab the packets of the router your currently connected to.
- 2) Destination IP: This is the IP you will grab packets from. By default, it is 255.255.255.255, meaning it will grab packets from all devices on that network. For more specific results, enter the IP of the device here.
- 3) BPF Filter: A BPF (or Berkly Packet Filter) is applied to filter out useless packets. In most cases, this should be left as default.
- 4) Save to File: To toggle whether or not to save the dump file. Should always leave "On" because the dump file can have information not gathered by Pirni.
- 5) Dump File: Location of dump file.
- 6) Regex Option: Possibly the most useful function this app has to offer. Chooses what the packet will grab and displays in the live feed (I.e. Emails, logins, credit card numbers, ect.) This will be explained in greater detail later on in the tutorial.

Live Feed

The app is pretty straight forward, just choose Start and it will begin the sniffing process and display results in the live feed:

[img=450x600]http://i1103.photobucket.com/albums/g463/roflkitties/IMG_0415.png[/img]

Settings

This is where you configure your Regex options. It comes with 3, basic codes but those won't get you very far. The "+" button at the top corner of the screen is where we will add our new Regex:

[img=450x600]http://i1103.photobucket.com/albums/g463/roflkitties/IMG_0414.png[/img]

A simple Google search will find you more Regex than you'll ever need, but here are some I find useful:

Code Title: Email Address

Regex: \b[A-Z0-9._%~+@][A-Z0-9.-]+\.[A-Z]{2,4}\b

Description: Regex to grab email address's

Code Title: General SQL Queries

Regex: (SELECT\s[\w*])\s([\s]+\sFROM\s[\w]+)| (UPDATE\s[\w]+\sSET\s[\w\,\'\=]+)|

(INSERT\sINTO\s[\d\w]+\s[\s\w\d])\s([\s]*\sVALUES\s([\d\w\'\,\,])+\s)| (DELETE\sFROM\s[\d\w\'\=]+)

Description: This will match the following SQL Queries (SELECT, UPDATE, INSERT and DELETE)

Code Title: Website URLs

Regex: (http://|)(www\.)?([^\.\+]\.){2}((com|net|org|edu|int|mil|gov|arpa|biz|aero|name|coop|info|pro|museum))\$

Description: This will find websites that users are viewing

Code Title: Phone Number Capture

Regex: ^(\(?+?[0-9]*\)?)[0-9_-\ \(\)]*\$

Description: This Regex can be used display any Phone Numbers that are Captured

Dump File

In many cases, the live feed will display less information than actually gathered. In these cases, we revert to the dump file. By default, it is located in "/var/tmp/log.pcap". With this file you can later get information from it using other packet analyzers, such as Wireshark. You can even get some information (such as website URLs and rarely logins) with a text editor and iFile.

LACHLAN227 - September 12, 2011, 3:26 am

there is already more than 5 tuts for this in the sub forum alone.

Bot Seller-Crypting Shop™ - September 12, 2011, 11:13 am

Really. I did a search for Pirni and nothing came up... besides the non GUI version

Today - September 12, 2011, 4:58 pm

So Can I use this to packet sniff server side games FOR my iphone?

Bot Seller-Crypting Shop™ - September 12, 2011, 6:03 pm

(Sep 12, 2011 04:58 PM)Today Wrote: [\[CITE\]](#) So Can I use this to packet sniff server side games FOR my iphone?

If you mean sniffing packets sent between your iphone and the server, then no. This app is a type of Man in the Middle attack. However, if it was another device on the same network, then it should work fine.

Grin - September 12, 2011, 10:28 pm

Sir, this is a great tutorial and all, but I prefer to use pirni thru terminal. Main reason, Pirni Pro has given me shitloads of problems.

Døñ - September 12, 2011, 10:56 pm

I agree with Grin, it's good and all; but the terminal is always more reliable.

Glitched - September 13, 2011, 4:31 am

If you use the terminal app, check out pirni-derv

Bot Seller-Crypting Shop™ - September 13, 2011, 5:44 am

I made this tutorial mostly because i saw someone in another thread requesting it (a video tutorial, but i figured this would be just as good). Also keep in mind that this is my first Tutorial, so any suggestions im up for :P