PERYTON

Your tiny WiFi passive handshakes sniffer

Thank You for buying Peryton, before we start playing with the device please remember this is only for testing your own devices and educational purposes.

I do not take responsibility for what you do with it.

havefun!

v1.4

What is it ?

Peryton is a tiny WiFi handshakes sniffer. It uses the wireless chip inside the board to listen for wifi frames and captures handshakes and beacons. The core idea of Peryton is to keep things super simple. Thanks to this, all you need is turn it on, and download captured handshakes for further processing.

Previously (with AttracThor) we worked to capture the WiFi password by phishing the victim devices to provide the credentials by doing an EvilTwin attack. This time with Peryton, we don't care. We sniff for authentication frames, which are later used for cracking.

This small device can be powered from pretty much anything (solar, power banks, usb) and with a small modification - you can even make it run on battery. Because this is based on ESP32 - feel free to hack / modify it - so it suits your needs.

How does it work?

Peryton on start gives you 3 minutes to play with the super simple status/config page.
It will host an AccessPoint called "PERYTON" for you to connect.

After 3 minutes, it goes into packet capture mode - hopping channels and listening for Beacons and EAPOL frames. All data is stored in Wireshark friendly format (PCAP).

It never stops doing that, meaning it continues in sniffer mode until rebooted.

In order to download and review the results, just reboot it (poweroff/poweron) and reconnect to Peryton Wifi for results. It's that easy.

When you obtain handshakes, you can easily download them by clicking on BSSIDS (Mac addresses) or get them all, by downloading the all in one pcap file.

After the files are downloaded, they are ready for further processing (Cracking).

Start

Ok, it's time to launch your Peryton - Let's do it.

Power on the device,
Peryton will start blinking, look for "PERYTON" WiFi access point and connect.

Head to: http://192.168.4.1/ to access main control panel and status page.

```
This is Peryton 8caab58bed98 version 1.4
(c) CodemasterPL 2020 - hack the planet

Space total: 1378241b
Space free.: 1377739b
Work mode..: passive
Channel....: hopping select
Hop Time...: 350ms
Broadcast..: 1
OLED.......: 1
-----------------------------------------------
-----------------------------------------------
[Delete All] [Update]
```

This is the page you will use to play with Peryton, it's almost empty - as we haven't yet captured any data. I will explain what particular links mean later, let's feed it with some data first.

Basic settings

You can tweak the way Peryton works a little bit (little - so it's not confusing).
The main things that you can modify are:

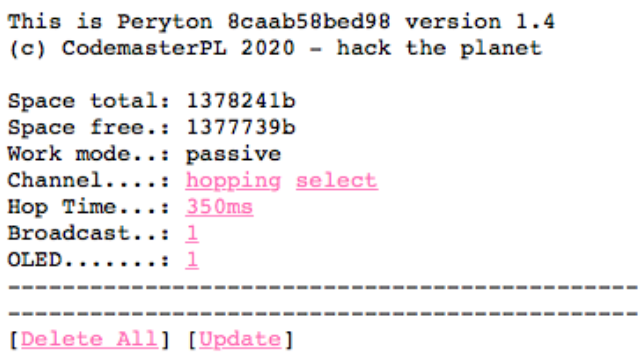
- **Channel**
  - Click on Hopping to:
    - Select specific channel for sniffing or choose hopping.
  - Click on select to:
    - Look for an access point around and use it for setting the channel

Hop Time
- Click to set channel hop time in milliseconds (500ms default)

Broadcast
- Enable/Disable status updates to ATTRACTHOR sister binary (for RaspberryPI)
1 = Enabled
0 = Disabled

OLED
- Available in firmware 1.4++, click to turn your OLED on
1 = Enabled
0 = Disabled

Strongly suggest to set as per below and head straight to sniffing:



Disconnect from Peryton WiFi but keep your Peryton powered on and leave it for a while, it will disable AP mode and go sniffing in a moment.

* The channel pinning is good if you are targeting specific channel / AccessPoint.
Peryton will stay on that channel without hopping increasing the rate of handshakes it captures for particular channel as there is no hopping around.

Work

After 3 minutes (180 seconds) of inactivity, Peryton will automatically switch mode to sniffing. The Access Point will be disabled, and you will no longer be able to connect to it - this is because it has to go promisc, hop channels, and listen instead of serving the data for you.

The blue led will stop blinking, Peryton is now looking for the handshakes and beacons around.

All data found will be stored on internal flash system, you can reboot Peryton at any point in time to access the status web page. For now, keep it going for a few minutes and lets return back after a short break.

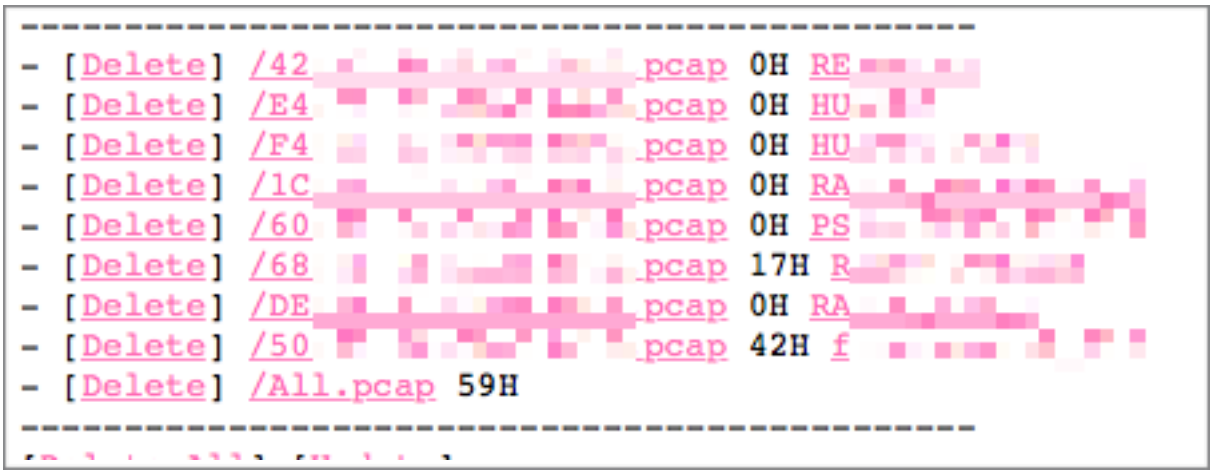
Even better, if you want to take a walk, take Peryton with yourself ;-)

Results

Had a break or a walk ?
Good, let's see what Peryton has for us.

Reboot it (power off, power on) and when you see Blue Led blinking, connect back to the PERYTON Access point.

Head to http://192.168.4.1/ and look at the results, here are mine;



All packets are captured PER BSSID :

/xx:yy:zz:ww:aa:bb.pcap 0H SSID
/aa:bb:cc:dd:ee:ff.pcap 0H SSID
/aa:cc:dd:ee:aa:bb.pcap 1H SSID

0H, 1H, 2H - This tells you the count of handshakes captured for the BSSID.

But also at the very bottom of the list, you can grab 'all in one' file called All.pcap.

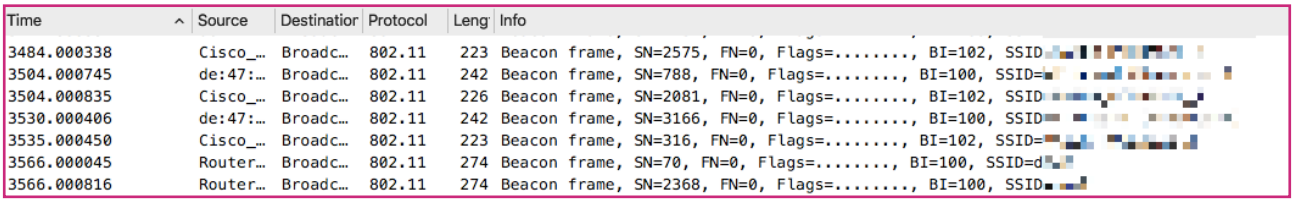
You can Delete any of the files if needed, but you can also Delete All if required.

Good job, we've got some data, we can start crunching.

Postprocessing

Ok, download All.pcap

Now open this file in WireShark - this is not needed btw. i'm just doing that to show you what i have captured.



Time	Source	Destination	Protocol	Leng	Info
3484.000338	Cisco_…	Broadc…	802.11	223	Beacon frame, SN=2575, FN=0, Flags=........, BI=102, SSID
3504.000745	de:47:…	Broadc…	802.11	242	Beacon frame, SN=788, FN=0, Flags=........, BI=100, SSID=
3504.000835	Cisco_…	Broadc…	802.11	226	Beacon frame, SN=2081, FN=0, Flags=........, BI=102, SSID
3530.000406	de:47:…	Broadc…	802.11	242	Beacon frame, SN=3166, FN=0, Flags=........, BI=100, SSID
3535.000450	Cisco_…	Broadc…	802.11	223	Beacon frame, SN=316, FN=0, Flags=........, BI=102, SSID=
3566.000045	Router…	Broadc…	802.11	274	Beacon frame, SN=70, FN=0, Flags=........, BI=100, SSID=d
3566.000816	Router…	Broadc…	802.11	274	Beacon frame, SN=2368, FN=0, Flags=........, BI=100, SSID

Immediately you see Beacon frames, that's good - let's check if we've found any Handshakes ;-) Scroll down a little bit, you should see EAPOL (Protocol) frames if there were any.

Time	Source	Destination	Protocol	Leng	Info
9953.000263	Ro	h…	EAPOL	159	Key (Message 1 of 4)
87605.000820	Ro	h…	EAPOL	159	Key (Message 1 of 4)
87662.000722	Ro	h…	EAPOL	159	Key (Message 1 of 4)
118103.000348	Tp	s…	EAPOL	137	Key (Message 1 of 4)
118118.000305	Tp	s…	EAPOL	241	Key (Message 3 of 4)
342602.000136	Ro	h…	EAPOL	159	Key (Message 1 of 4)
446936.000025	Ro	h…	EAPOL	159	Key (Message 1 of 4)
447004.000563	Ro	h…	EAPOL	159	Key (Message 1 of 4)
485030.000474	Ro	h…	EAPOL	159	Key (Message 1 of 4)
530254.000381	Ro	h…	EAPOL	159	Key (Message 1 of 4)
589150.999961	Ro	h…	EAPOL	159	Key (Message 1 of 4)
1142341.000451	Ro	h…	EAPOL	159	Key (Message 1 of 4)
1142355.000684	Ro	h…	EAPOL	159	Key (Message 1 of 4)
1246536.000170	Ro	h…	EAPOL	159	Key (Message 1 of 4)
1252780.000607	Ro	h…	EAPOL	159	Key (Message 1 of 4)
1285648.000365	Ro	h…	EAPOL	159	Key (Message 1 of 4)

Of course there are :)

You know what to do next right ?

Few things

- Peryton is not a toy, it's created to help you check if your WiFi setup is vulnerable for brute force /dictionary attacks. In order to check that, you need to sniff 4-WAY handshakes or PMKID and crack it.
- Peryton is not a cracker it will not crack any hash, it is a sniffer - it will capture required packets into a file for further processing.
  For cracking the sniffed handshakes, see hashcat tutorial.
- All firmware upgrades / news will be shared on Tindie product page.