



PVI_WIFIPINEAPPLE-TETRA

By Dave

Contents

Introduction	2
Research questions	2
Setup	3
Initial Setup with Windows.....	3
Here is the Initial Setup with VirtualBox (optional).....	5
Settings.....	7
Portability	8
How can the Wi-Fi pineapple be used with a android device?	8
Effectiveness in Hacking	13
In what ways does the Wi-Fi Pineapple Tetra effectively create real-world security threats?	13
What modules are used for the most common hacks?	16
Social Engineering with NFC tags	18
Possibilities of the Tetra in conjunction with NFC tags.....	18
References	21

Introduction

For this **Personal Vulnerability Investigation (PVI)** project I decided to go with the **Wifi Pineapple Tetra device (HaK5)**. Why? because I find it very interesting and I wanted to take a look at its capabilities.

Wi-Fi networks have become an essential component of our everyday lives in the rapidly changing environment of wireless communication. As people's reliance on wireless communication grows, so does the concern for the security of these networks. the Wi-Fi Pineapple Tetra stands out as a noteworthy device, offering unique capabilities that both security professionals and malicious actors find intriguing.

Research questions

Main Question:

- How does the Wi-Fi Pineapple Tetra, when used with Android devices, enhance portability for hacking, especially when paired with NFC-based social engineering?

Sub-questions:

Portability:

- How can it be used with a android device?

Effectiveness in Hacking:

- In what ways does the Wi-Fi Pineapple Tetra effectively create real-world security threats?
- what modules are used to do some common hacks?

Social Engineering with nfc tags:

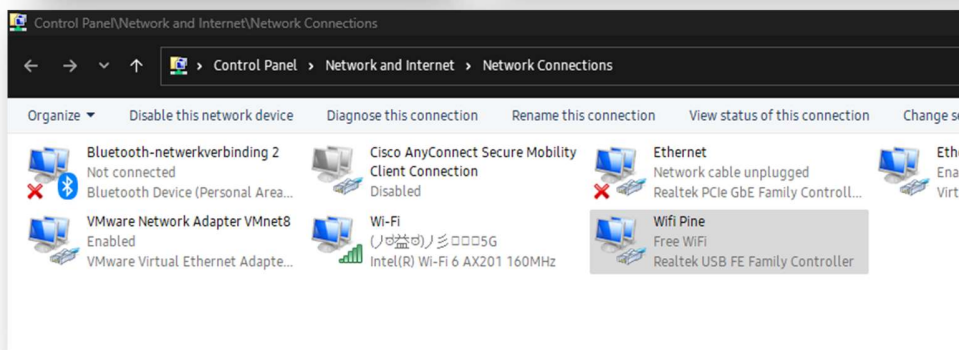
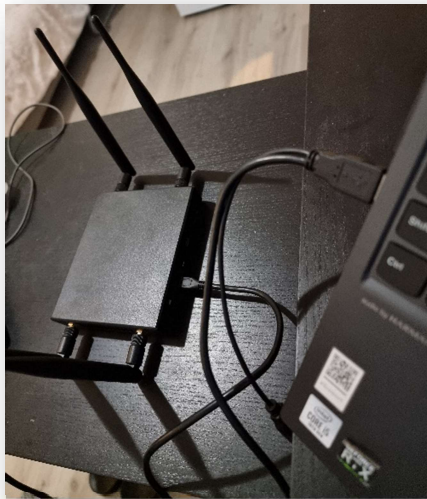
- Possibilities of using the Pineapple device in conjunction with nfc tags.

Setup

Initial Setup with Windows

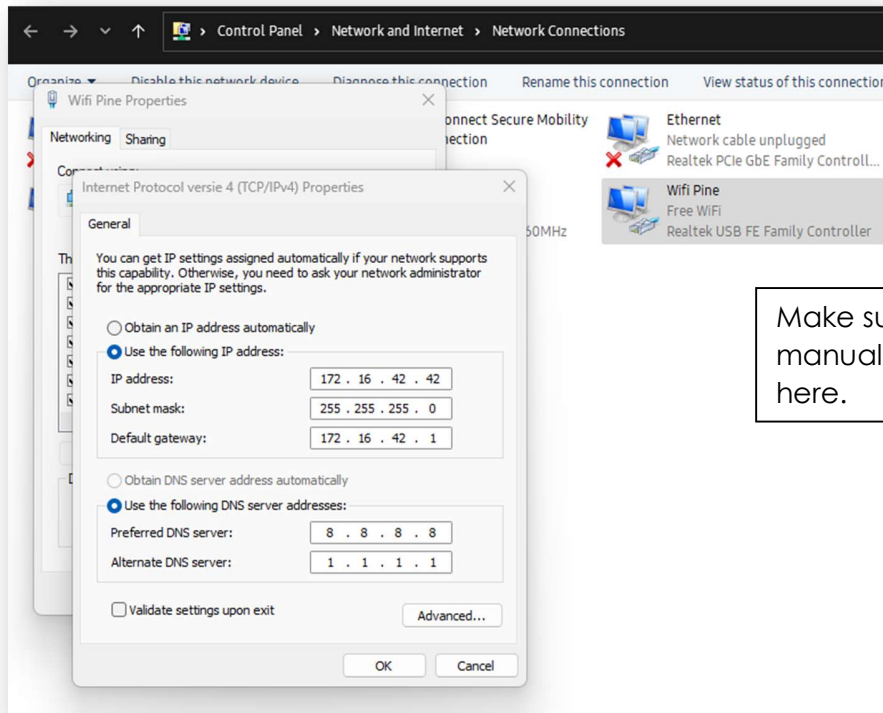
The setting up part of the Wi-Fi pineapple Tetra is easy. I am going to plug it in my windows laptop and change the network adapter settings in the control panel. (you will lose internet access if you are using Wi-Fi)

This part is **mandatory** for the setup. Later on we wont need to plug it to our laptop anymore.

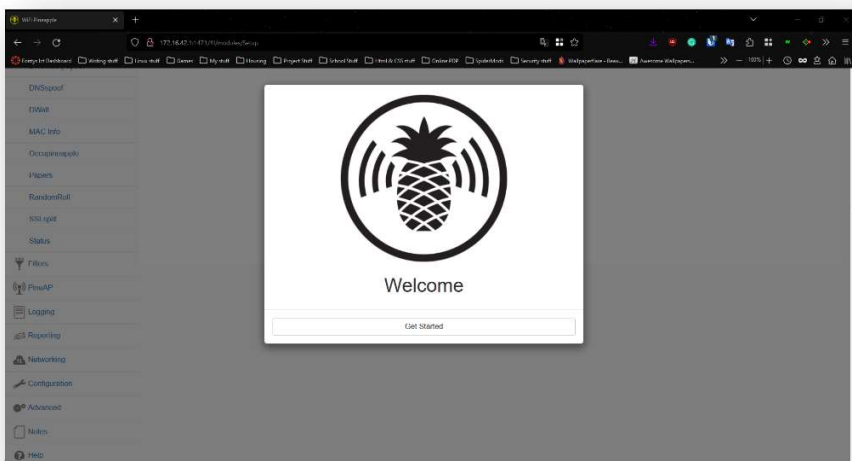


Here is the control panel network connections page. When you first connect the device it will be recognized as "Ethernet 4" or any other number and the built-in device name is "Realtek USB FE Family Controller".

I renamed the ethernet 4 to "Wifi Pine" for easier management.

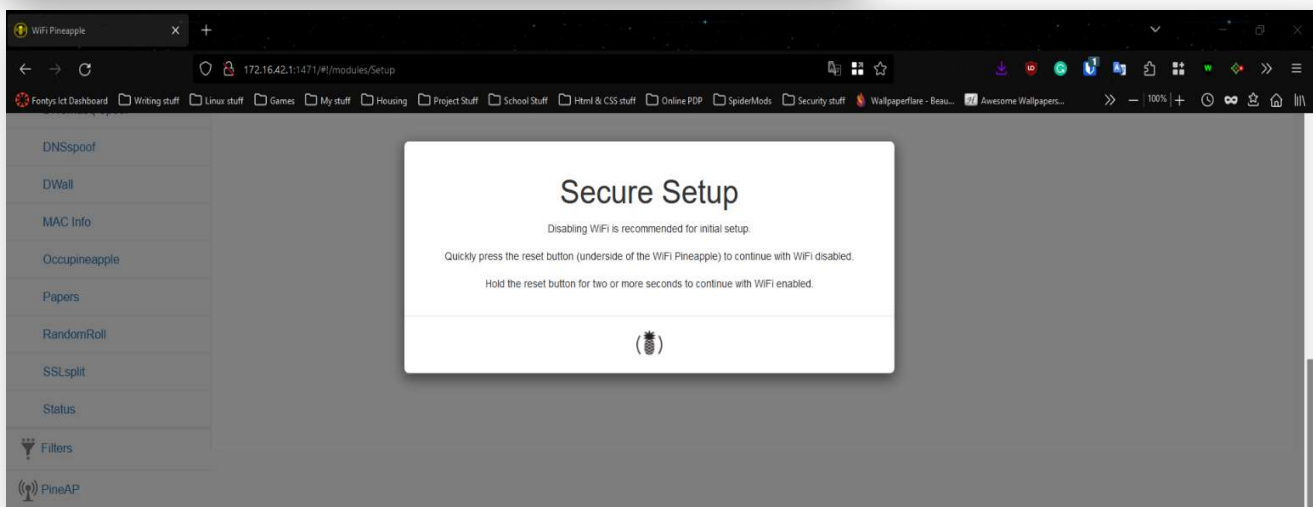


Make sure you have the manual Ip address settings here.



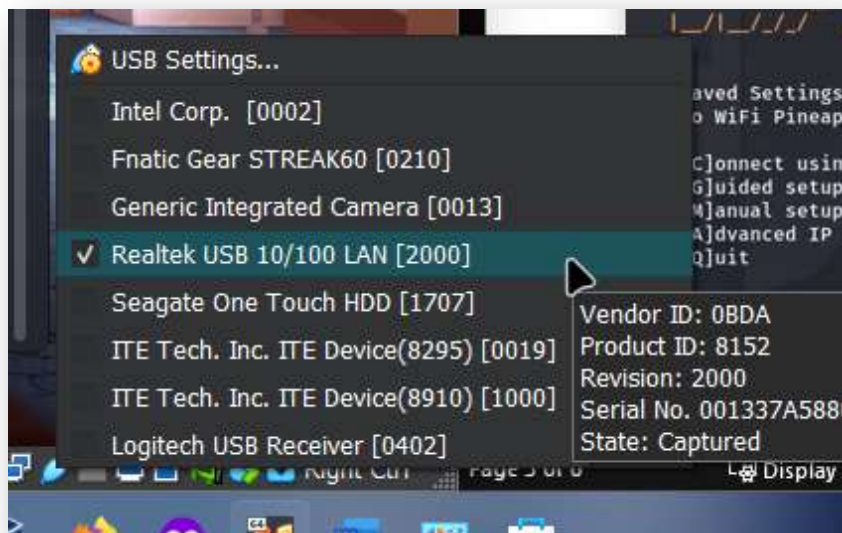
Now navigate to your preferred browser and go to the default Ip address of the Wi-Fi pineapple **172.16.42.1:1471**

And if everything goes well, you should see the Wi-Fi pineapple **web interface**.



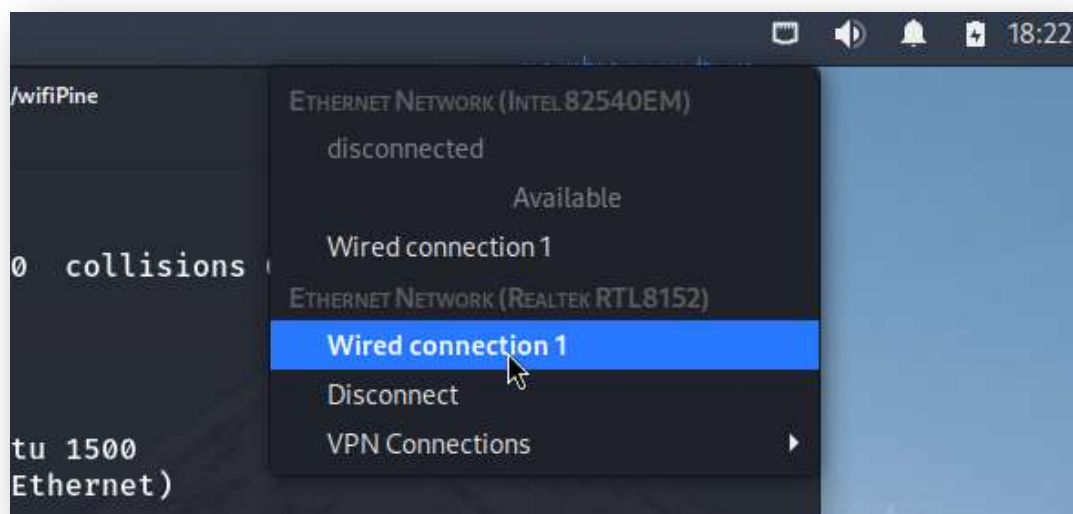
Here is the Initial Setup with VirtualBox (optional)

I have a virtual machine with Kali Linux installed. I will go to my VirtualBox USB settings and add my Wi-Fi pine device (Realtek USB).



Now that it is connected to VirtualBox, go to the Wi-Fi settings (top right on desktop) and make sure it is connected on **Ethernet Network (RealtekRTL8152)**

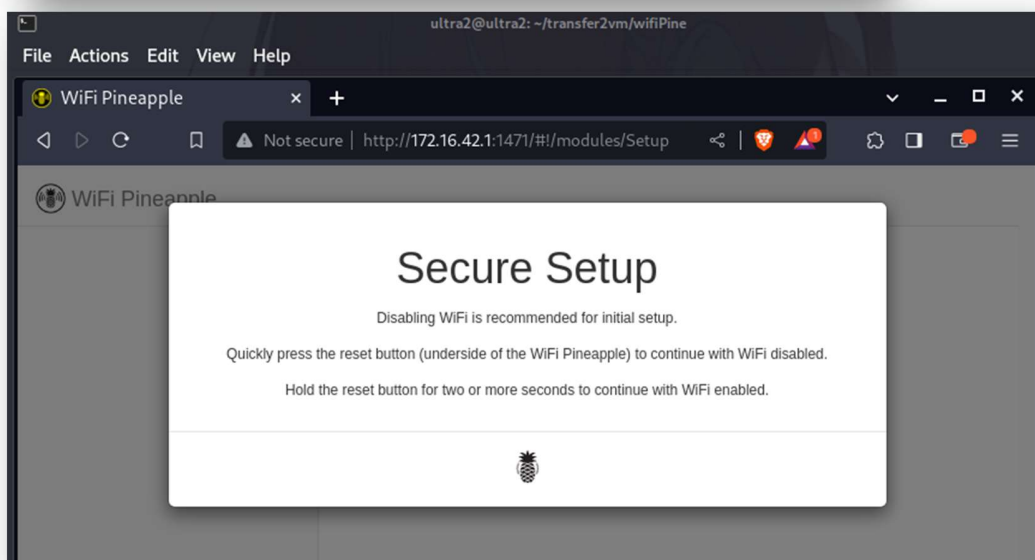
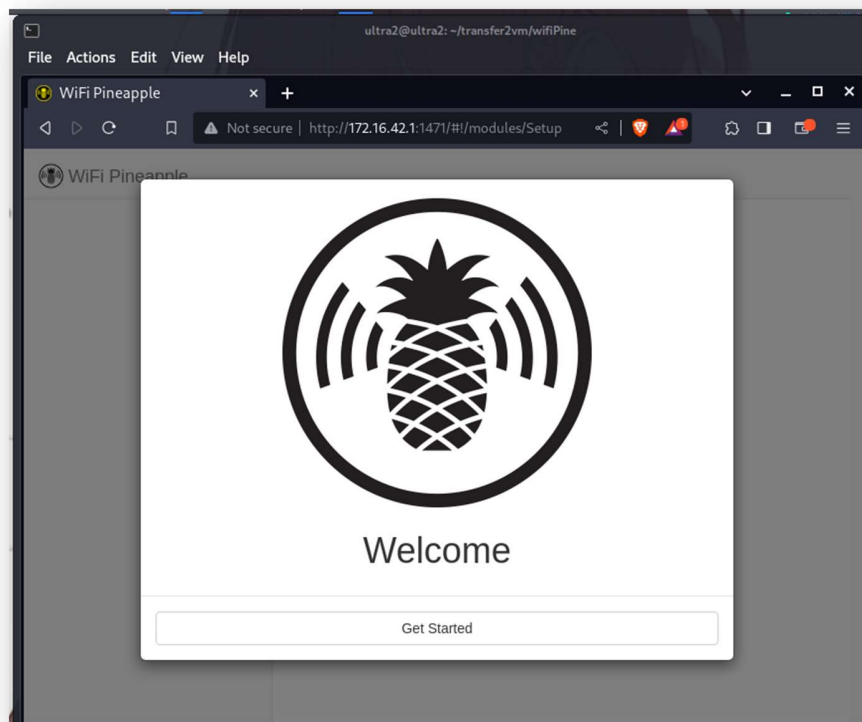
You will lose access to the internet.



Now use your browser inside Kali to navigate to the default IP address if the Wi-Fi pineapple

172.16.42.1:1471

And if everything goes well, you should see the Wi-Fi pineapple **web interface**



Settings

Enter your password for root web interface and SSH access etc.

The screenshot shows the WiFi Pineapple web interface in a browser. The address bar displays the URL `172.16.42.1:1471/#/modules/Setup`. The left sidebar contains a navigation menu with items: Dashboard, Recon, Clients, Tracking, Modules (expanded), Manage Modules, Commander, DNSMasq Spoof, DNSspoof, DWall, MAC info, OccupyPineapple, Papers, RandomRoll, SSLsplit, and Status. The main content area is titled "Device Configuration" and includes three sections: "Set Root Password" (with fields for Password and Confirm Password), "Set Time Zone" (with a dropdown menu showing "(UTC) Western Europe Time, London, Lisbon, Ca"), and "Radio Configuration" (with a "Management AP Setup" section containing fields for Management SSID, WPA2 Password, and Confirm Password).

This screenshot shows the lower portion of the WiFi Pineapple setup interface. The "SSID Filters Setting" section explains that SSID filters specify network names for association and offers two modes: "Allow Mode" (selected) and "Deny Mode". The "Firewall Settings" section states that these rules configure access to SSH and Web via the WAN Ethernet port, with checkboxes for "Allow SSH Access via WAN" and "Allow Web Access via WAN", both of which are checked. Below this is the "License & EULA" section, which includes a "Legal" subsection with checkboxes for "I accept the EULA" and "I accept the Software Licence", both checked. A "Complete Setup" button is located at the bottom of this section.

And here is the important part
Allow **SSH and Web access**.

Client filters(I have both **deny**
mode) and click complete
setup

Portability

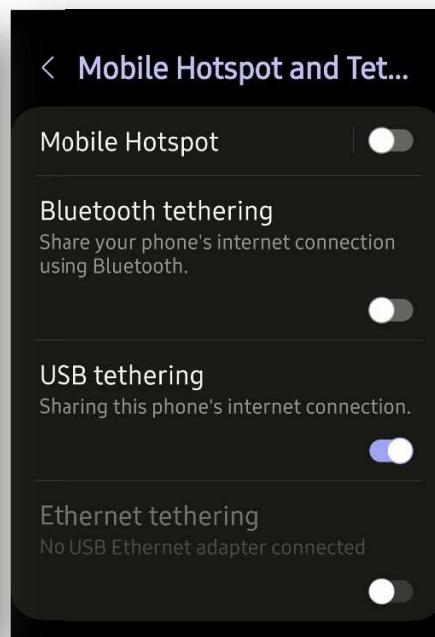
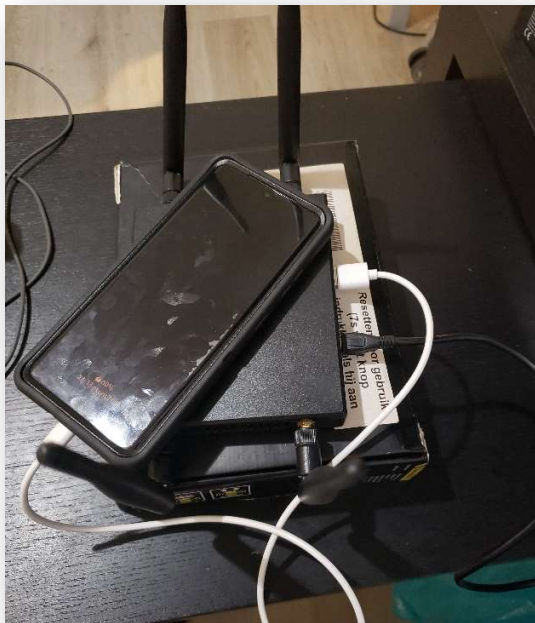
How can the Wi-Fi pineapple be used with a android device?

We only need **3 things** to make this possible:

- Android phone (with mobile data & USB tethering)
- A Power bank for power supply.
- A standard USB C cable.



STEP 1 Now plug in your phone with the pineapple and enable USB tethering(can be found in settings).



STEP 2 Navigate back to the web interface, go to the networking tab and you will see that the routing table has been updated automatically.

Do NOT click update route (it will remove the default gateway and you will have to do additional trouble shooting)

Gateway of android device's mobile data.

usb0 is the new interface added to the table.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	192.168.200.252	0.0.0.0	UG	0	0	0	usb0
172.16.42.0	*	255.255.255.0	U	0	0	0	br-lan
192.168.200.0	*	255.255.255.0	U	0	0	0	usb0

Default Route: 172.16.42.42 Interface: br-lan Update Route

STEP 3 is to verify that we have an internet connection via the bulletin section in the dashboard tab. If it loads, we're set!

Bulletins

Load Bulletins from Hak5

Bulletins

Firmware 1.1.0 - Buffalo Bulldozer 2016-08-23

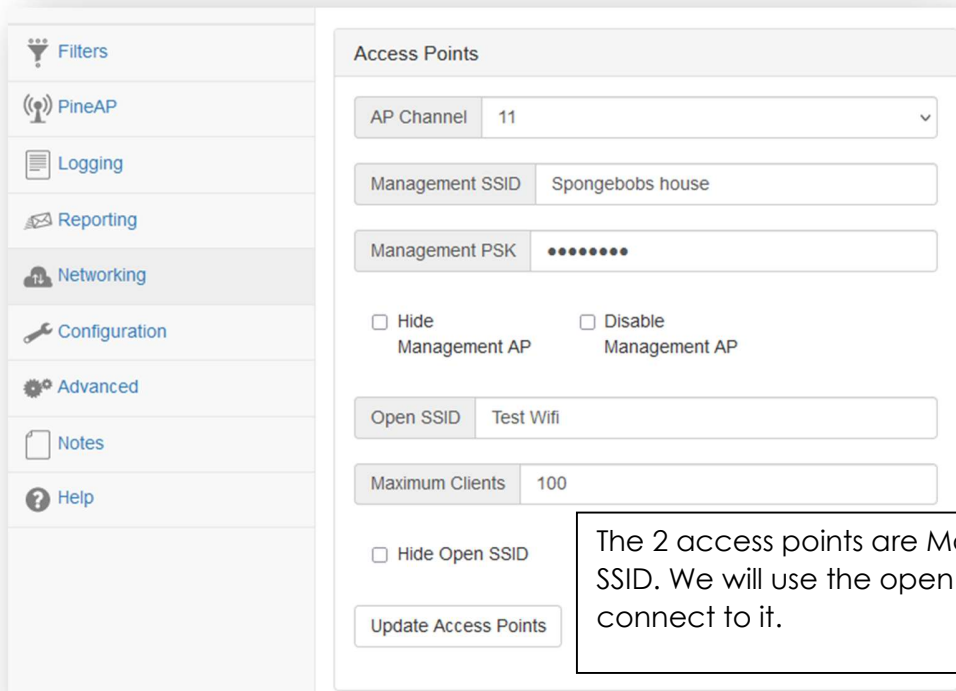
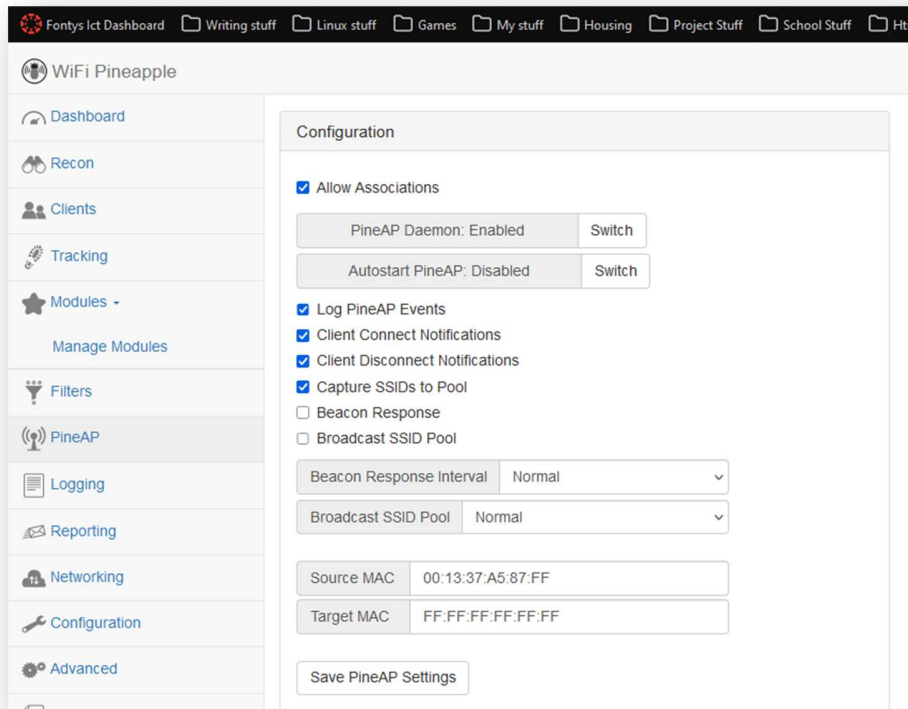
This week sees a major milestone for the project with the release of Buffalo Bulldozer - a rock solid firmware serving to synchronizing a stable base for both the NANO and TETRA. Update today and enjoy the latest enhancements to the PineAP engine, improved performance and new features in Recon mode and updates to the base. Learn more from the full [release notes on the forums](#) and [update over-the-air from the advanced page](#).

Project Update 2016-03-02

The 6th Generation WiFi Pineapple platform and ecosystem are developing nicely. Here are some quick insights:

New first-party module: DWall. Based on feedback from Renderman, DWall has been developed to display real-time HTTP URLs, Cookies, POST DATA, and images from

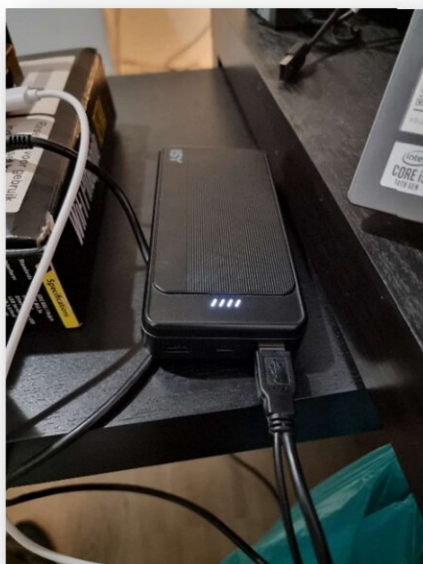
STEP 4 Enable the PineAP daemon and allow association. Then go to the networking tab to see the name of 2 access.



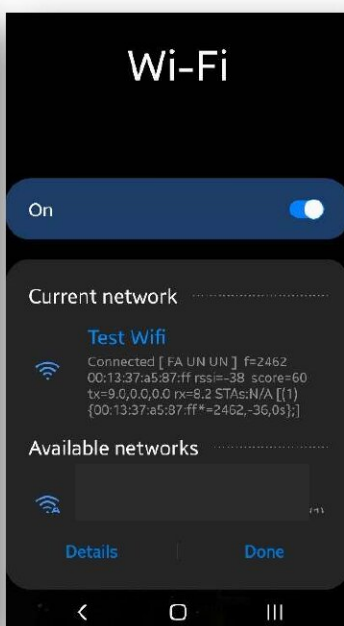
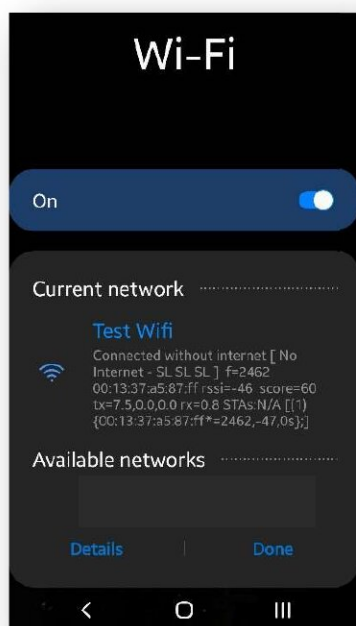
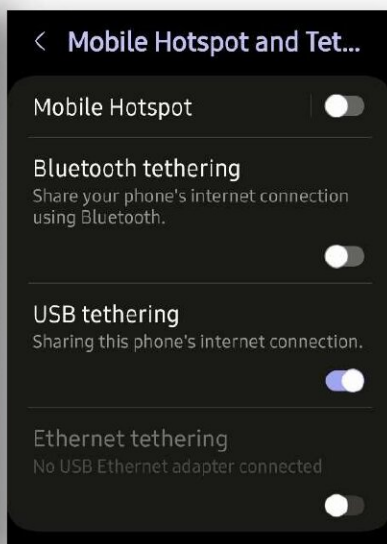
The 2 access points are Management & Open SSID. We will use the open SSID **“Test Wifi”** to connect to it.

STEP 5 Now we can unplug the Wi-Fi pineapple Tetra from our laptop!

This is where the power bank comes into play.



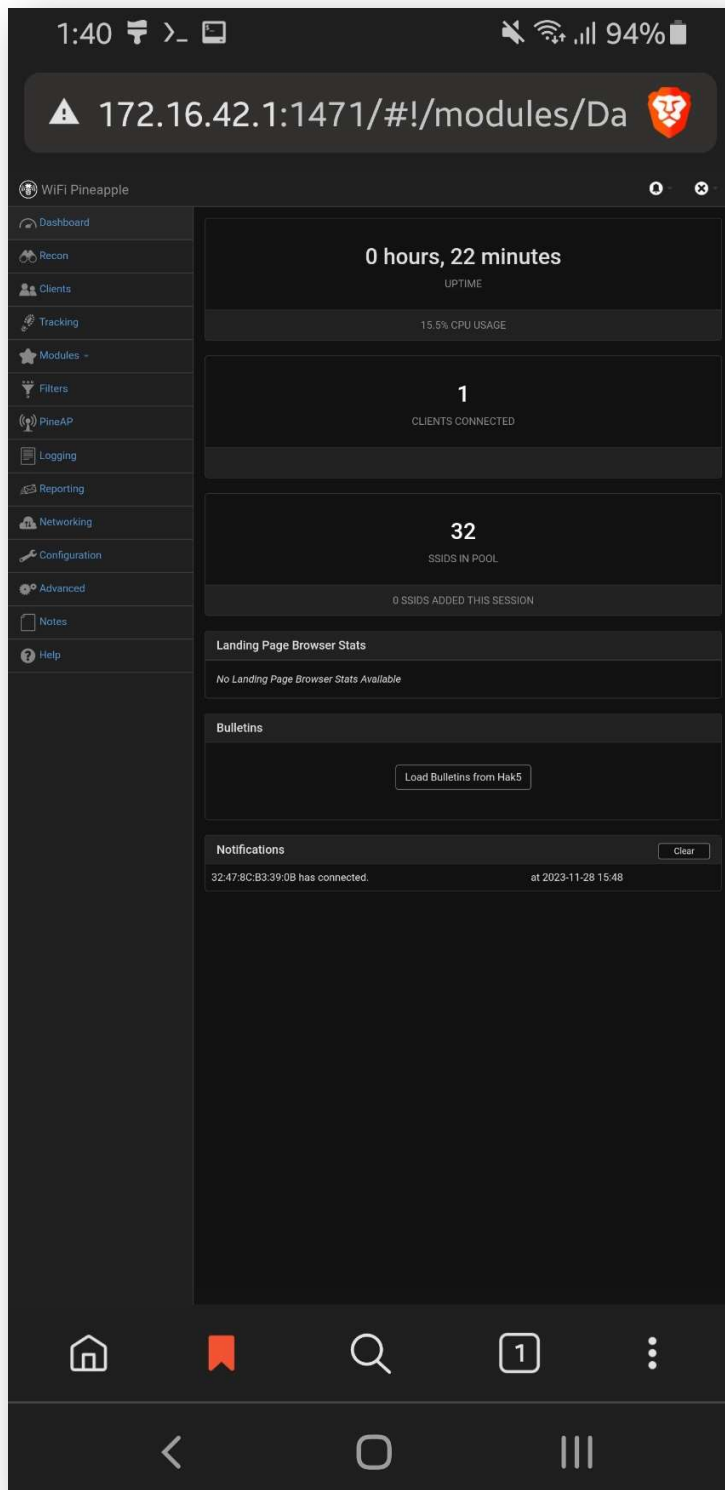
STEP 6 Now go to your android device and activate USB tethering again.



STEP 7 go to your Wi-Fi settings and connect to the open Wi-Fi SSID, in my case it's "**Test Wifi**"

As you can see, at first we won't have internet access,

but once we enable USB tethering, We will have internet access for our clients to browse.



STEP 8 go to your browser to the Wi-Fi pineapple web interface (**172.16.42.1:1471**)

Now a **recap** of what we have done:

We have configured the pineapple to have internet access with **USB tethering** and to be able to use the device **anywhere at anytime**. Why?

Because when you connect the Wi-Fi Pineapple Tetra to the internet via Wi-Fi, it restricts the use of **PineAP** features due to potential conflicts.

PineAP is a feature on the Wi-Fi Pineapple Tetra that enables various advanced Wi-Fi attack and reconnaissance functionalities. It allows the device to perform tasks such as beaconing, capturing and analyzing Wi-Fi data, conducting man-in-the-middle attacks, and creating rogue access points.

So, to use the Pineapple's full capabilities and be portable, we needed an alternate way of connecting to the internet. That's why we decided to go with **USB tethering**.

Effectiveness in Hacking

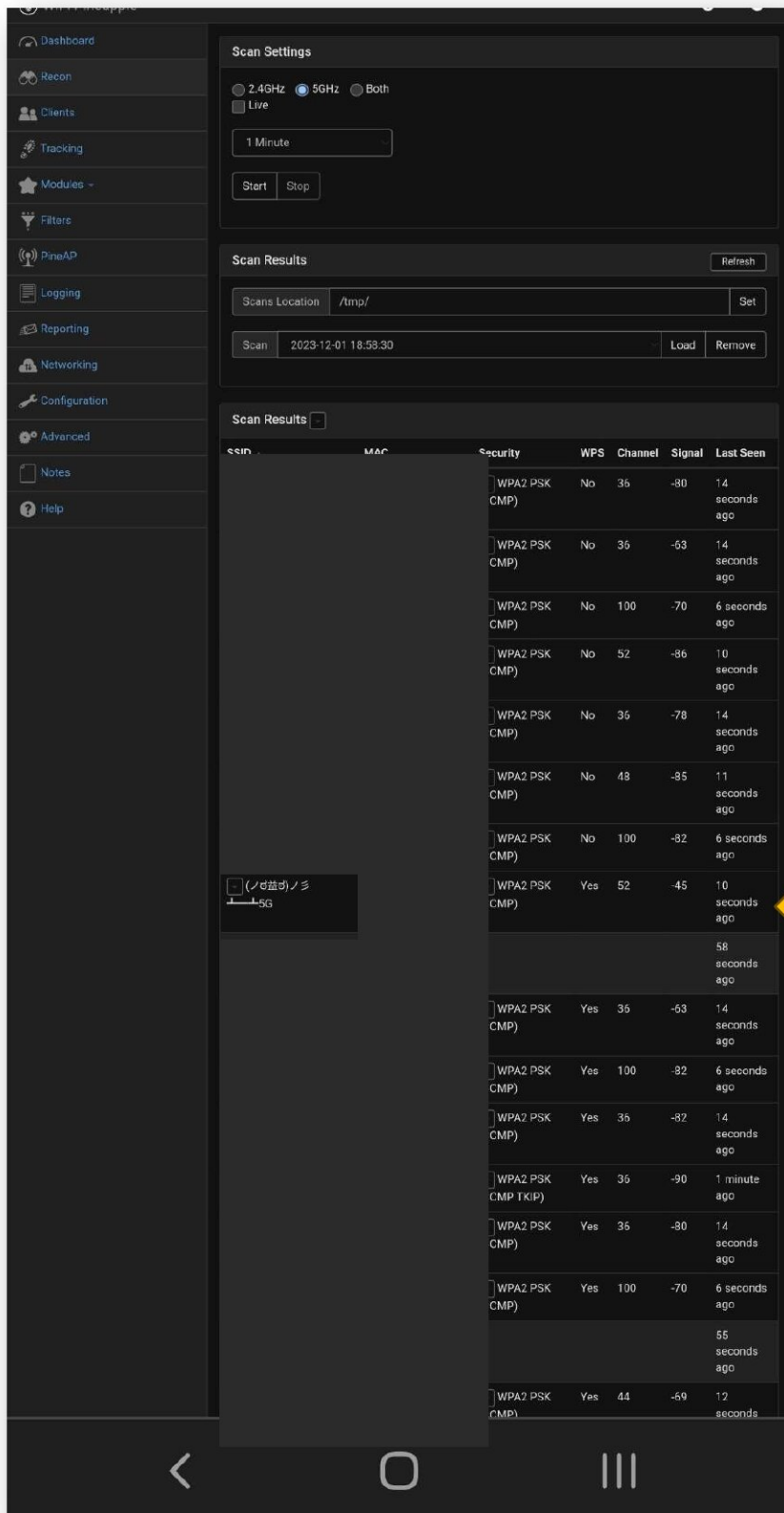
In what ways does the Wi-Fi Pineapple Tetra effectively create real-world security threats?

There are several sophisticated **attack techniques** the Wi-Fi Pineapple Tetra can do:

1. **Rogue Access Points (APs):** It can create rogue APs that mimic legitimate networks, tricking devices into connecting. This enables eavesdropping, man-in-the-middle attacks, and the interception of sensitive information.
2. **Man-in-the-Middle (MITM) Attacks:** The Pineapple Tetra can intercept and modify traffic between devices, allowing attackers to monitor, alter, or steal data passing through the network. This is especially potent when combined with its ability to create rogue APs.
3. **PineAP Reconnaissance:** It actively gathers information about nearby Wi-Fi networks, devices, and clients. This information can be exploited to tailor attacks, profile users, or identify vulnerable devices.
4. **Wi-Fi DE-authentication and Jamming:** The device can send DE-authentication frames, disrupting connections between devices and legitimate networks. It can also perform Wi-Fi jamming, denying service to users in the vicinity.
5. **Capturing Sensitive Data:** Through the capture and analysis of Wi-Fi traffic, the Pineapple Tetra can extract sensitive data like login credentials, personal information, or unencrypted communications.
6. **Credential Harvesting:** It can perform captive portal attacks, tricking users into entering login credentials or personal details on fake login pages.
7. **Evading Security Measures:** By exploiting vulnerabilities and weaknesses in various Wi-Fi protocols and devices, the Pineapple Tetra can bypass security measures implemented by networks and devices.

For our research purposes,
we will take a look at **1** and **3**.

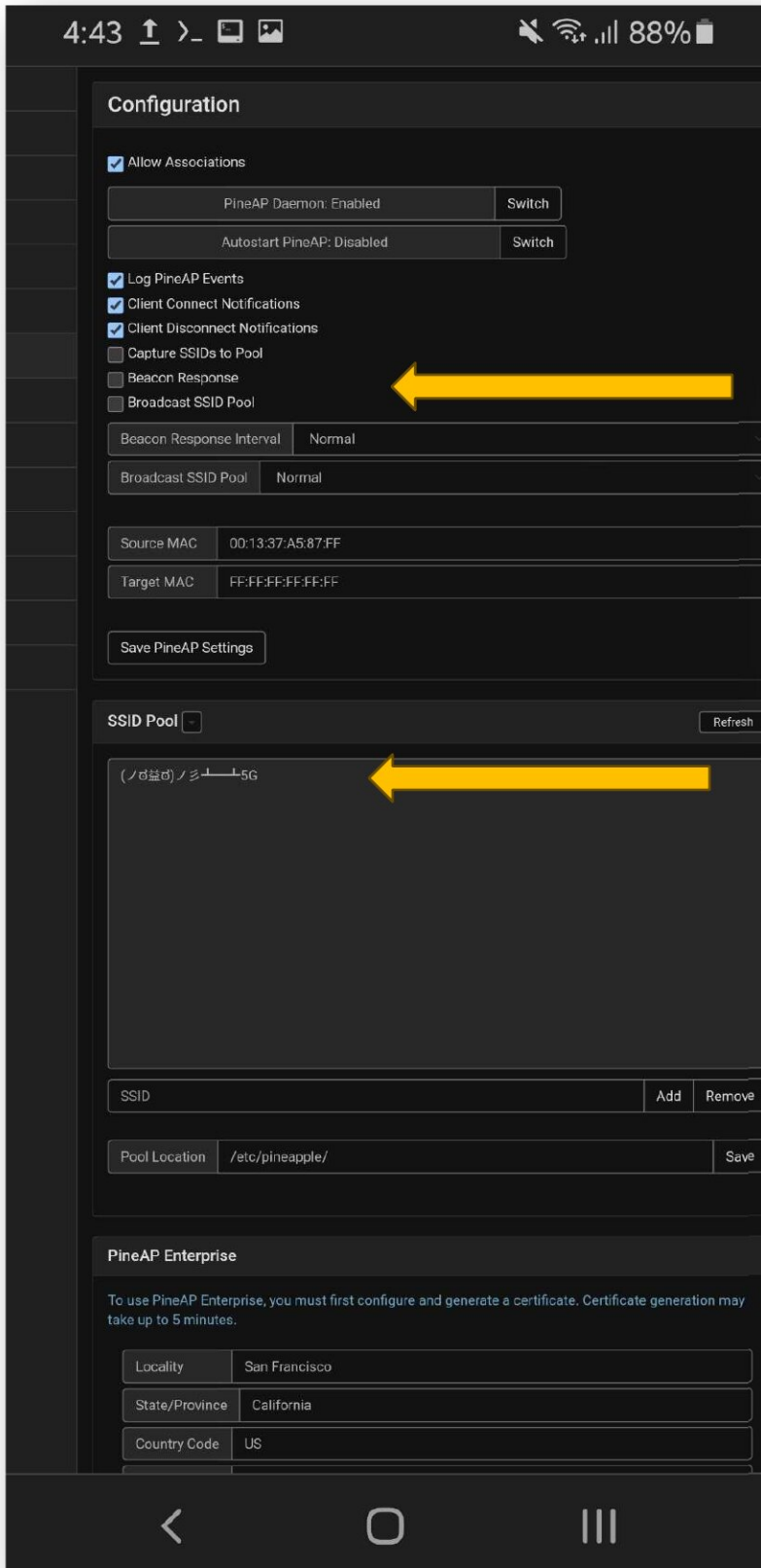
For the **Rogue Access Points**, I will mimic my own home network.



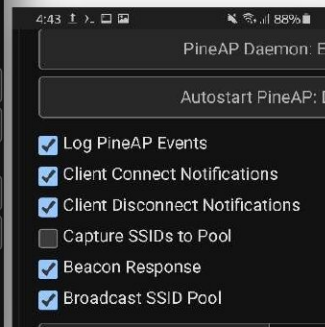
To create a fake access point you can either type the Wi-Fi name manually in the SSID pool, or you can do a reconnaissance to find the Wi-Fi network name and add it to the pool automatically.

The device's scanning range is very wide, it scanned almost my whole neighborhood.

That arrow is pointing at my Wi-Fi SSID. I will add it to the pool.



Make sure to tick beacon response & Broadcast SSID pool to create the Rogue Access Point.



Once added to the pool. It will create a fake access point with that name.



What are the Risks if people unknowingly connect to the Rogue AP?

Rogue APs enable attackers to capture and analyze sensitive data transmitted over the network, compromising user privacy and potentially exposing confidential information by positioning itself between the victim's device and the internet.

In some cases, rogue APs may disrupt the normal operation of legitimate networks, causing interference or denial of service to users attempting to connect to authorized networks.

So how can you defend against it?

The ideal option for home access points would be to enable WPA2-PSK authentication and then only establish a connection to secure networks. **Open networks**, such as the Wi-Fi at coffee shops, are the main target of attacks like Rogue Aps, therefore if you use an open network, make sure you are using a VPN!

What modules are used for the most common hacks?

As of **November 2023** there are **54 modules** to choose from in the Wi-Fi pineapples modules section. And some of them don't even work properly anymore, due to the lack of maintenance and/or counter measures are in place. For example, we cannot use **SSLstrip** module anymore on modern browsers because companies are working with the developers of these browsers to implement counter measures.

The image shows two side-by-side screenshots of the Wi-Fi Pineapple Module Manager interface. The left screenshot shows the 'Available Modules' list, and the right screenshot shows the 'Installed Modules' list. A yellow arrow points from the 'Installed Modules' list to a text box.

Available Modules

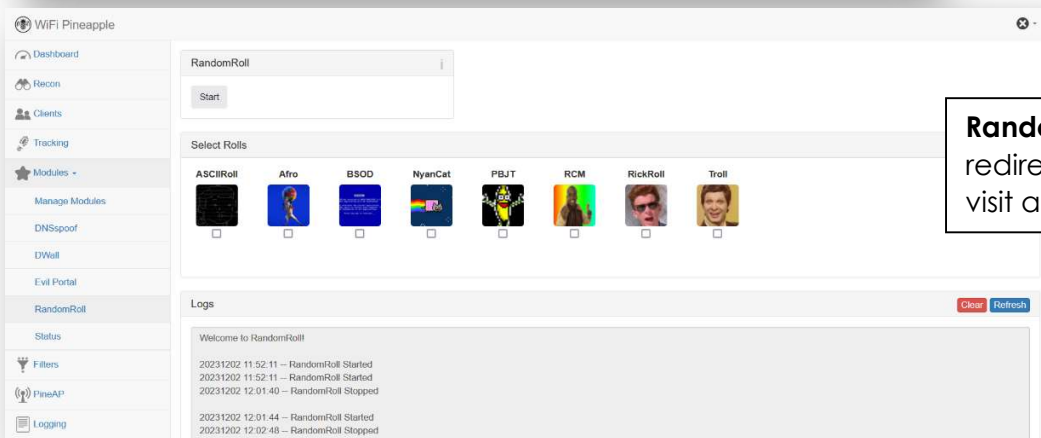
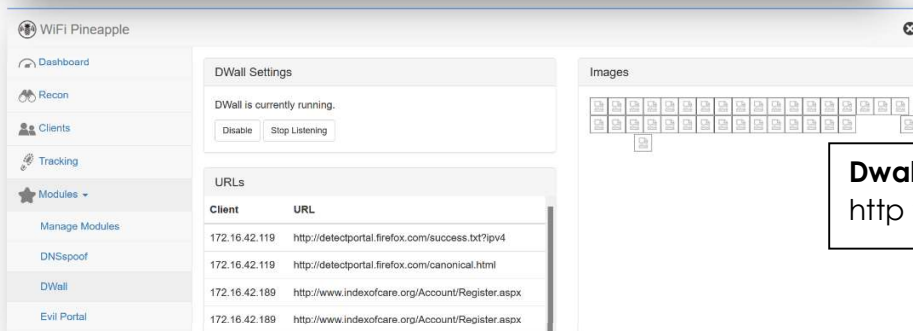
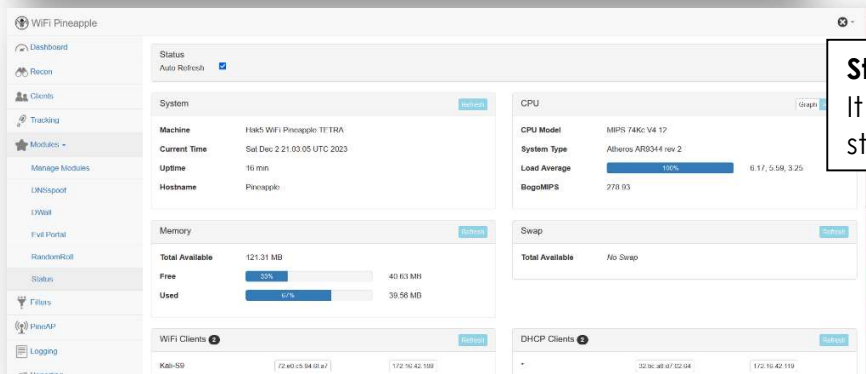
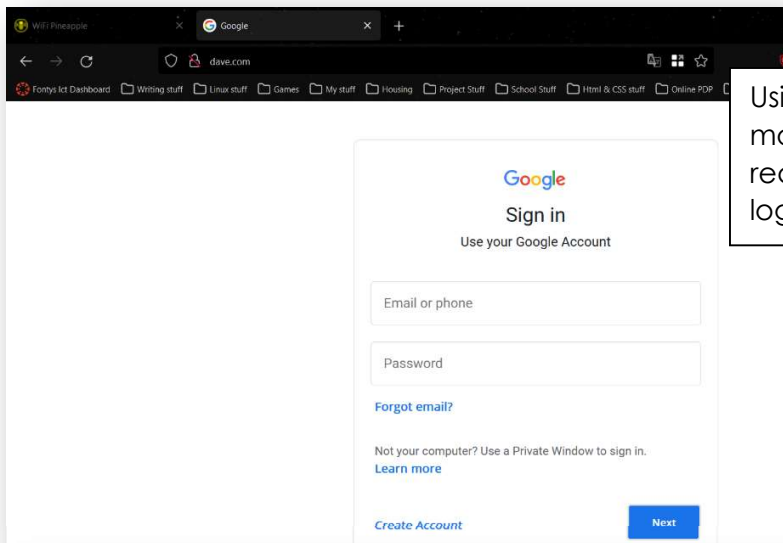
Module	Version	Description	Author	Size
Site Survey	1.6	WiFi site survey	whistlemaster	105K
Meterpreter	1.1	meterpreter configuration utility	audibleblink	7.4K
get	1.2	Profile clients through the browser plugins supported by their browser	dustbyter	1.1K
nmap	1.9	GUI for security scanner	whistlemaster	8.1K
wps	1.7	WPS brute force attack using Reaver, Bully and Pixiewps	whistlemaster	122K
Occupineapple	1.7	Broadcast spoofed WiFi SSIDs	whistlemaster	1134K
Status	1.5	Display status information of the device	whistlemaster	43.7K
Portal Auth	2.0	Captive portal cloner and payload distributor	sudnick	39.23K
SignalStrength	1.0	Displays signal strength for wireless cells that are within range. Can be used to physically locate cells.	r3d4sh	164K
topdump	1.8	Dump traffic on network using tcpdump	whistlemaster	4.3K
urlsnarf	1.9	Output all requested URLs sniffed from http traffic using urlsnarf	whistlemaster	8.0K
DNSspooof	1.7	Forge replies to arbitrary DNS queries using DNSspooof	whistlemaster	9.7K
ConnectedClients	1.4	Shows currently connected clients, DHCP leases and blacklist management.	r3d4sh	2.14K
RandomRoll	1.2	This module allows you to troll unsuspecting clients connected to your WiFi Pineapple.	foxtrot	20403.19K
Online Hash Crack	1.5	Submit Hash and WPA Handshake to www.onlinehashcrack.com web service	whistlemaster	4.57K
Responder	1.2	LLMNR, NBT-NS and MDNS poisoner with built in HTTP, SMB, MSSQL, FTP and LDAP rogue authentication server using Responder	whistlemaster	139.09K
Cabinet	1.1	A file manager for the Web Interface	newbi3	4.91K
HackRF	1.4	HackRF on the WiFi Pineapple	foxtrot	4.64K

Installed Modules

Module	Version	Description	Size	Author	Type	Action
DNSspooof	1.7	Forge replies to arbitrary DNS queries using DNSspooof	112.0K	Whistle Master	GUI	Remove
DWall	1.4	Display's Plaintext HTTP URLs, Cookies, POST DATA, and images from browsing clients.	44.0K	Sebkinne	GUI	Remove
Evil Portal	3.2	An Evil Captive Portal.	180.0K	newbi3	GUI	Remove
RandomRoll	1.2	This module allows you to troll unsuspecting clients connected to your WiFi Pineapple.	20.2M	Foxtrot	GUI	Remove
Status	1.5	Display status information of the device	192.0K	Whistle Master	GUI	Remove

But there are still some useful modules we can use.

Here are 5 modules that are functional.



Social Engineering with NFC tags

Possibilities of the Tetra in conjunction with NFC tags

There are many possibilities for the Wi-Fi pineapple tetra now that we are aware of its capabilities. The way this can be utilized in conjunction with NFC tags is one of the applications that isn't often discussed. The primary focus of the vulnerability investigation is this.

Now what are NFC tags?

Near-field communication technology allows two devices to communicate wirelessly. To enable data transfer between nearby mobile phones, computers, tablets, and other electronics, the technology can be integrated into a tiny tag.



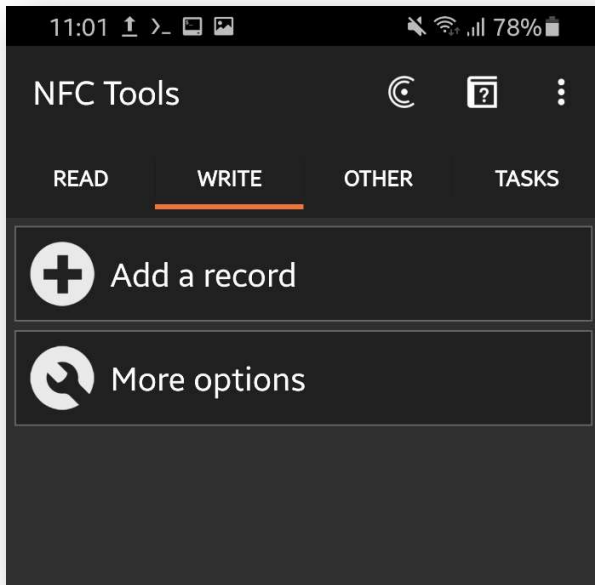
You can write about 888 bytes of data with this NFC tag. That data can be anything! Text records, Custom URL's, email records, phone numbers, SMS, Custom location, Bitcoin address, and many more!

And so, that is where I came up with the Idea, **what if I can add Wi-Fi data to it and connect unsuspecting users to the pineapple device?**

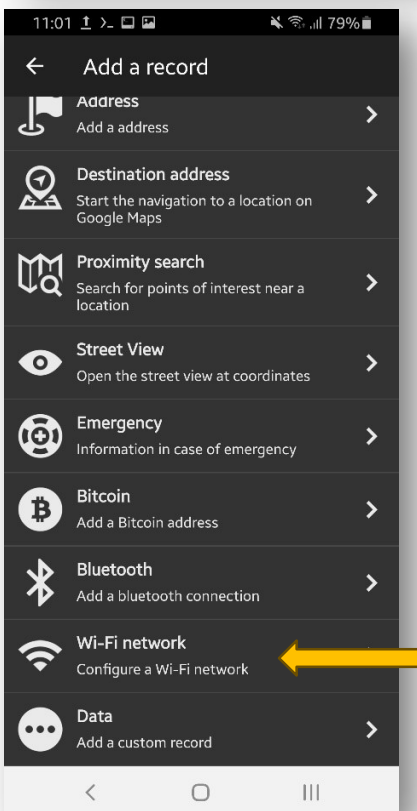


I found this app in the google play store called NFC tools.

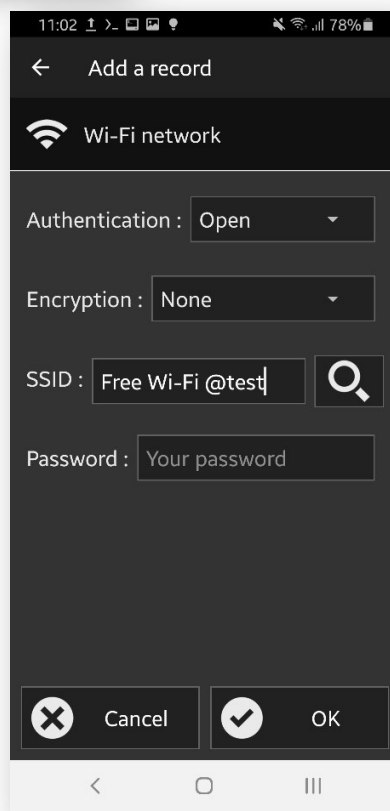
It allows you to read and write NFC tags.



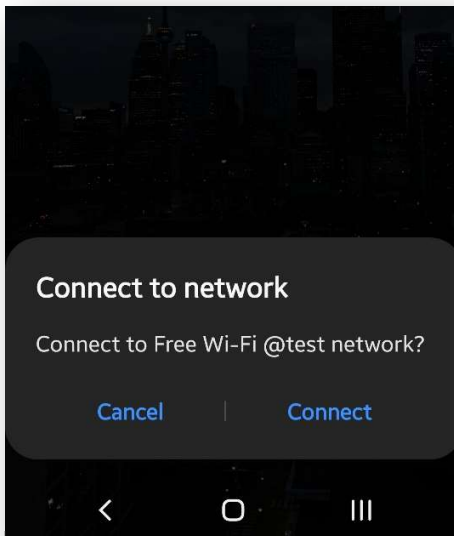
This is how it looks like when you open the app. I will now go and add a record to my NFC tag.



Here you can see that there is Wi-Fi network option.



I just need to add the Pine apple Rogue Access point and done! My tag is ready to go.



When I held my other phone close to the NFC tag, this was the prompt. I clicked connect and it connected to the Wi-Fi network with no issues.



If you are connecting for the **first time**, it will display this security alert. The attacker can just click add to exception and the victim would be clueless.

In conclusion, I cant believe how **easy** it is to connect to Wi-Fi networks via **NFC**. I was expecting at least a **password prompt** to connect to the network with this method, but nope that's not the case.

In my opinion, this is a **vulnerability** that the Developers didn't intend to have with the **Android Software** and its **NFC functionality**. A password prompt would be a great layer of security when connecting to Wi-Fi networks via NFC tags. I believe it is also the same on the IOS software as well. **Update: it doesn't work with iPhone.**

References

<https://docs.hak5.org/wifi-pineapple-6th-gen-nano-tetra/setup/wifi-pineapple-nano-windows-setup>

<https://docs.hak5.org/wifi-pineapple-6th-gen-nano-tetra/internet-connectivity/internet-connectivity-basics>

https://archive.org/details/JackkTutorials_Me/20161206-How+to+setup+Wifi+Pineapple+Tetra+and+Basic+Attack.mp4#

<https://docs.hak5.org/wifi-pineapple-6th-gen-nano-tetra/getting-started/about-the-wifi-pineapple-nano-tetra>

<https://www.nomtek.com/blog/what-are-nfc-tags#:~:text=NFC%20%E2%80%94%20FAQs-What%20Are%20NFC%20Tags%3F,but%20the%20two%20are%20different.>