



GenCyber

NSA GenCyber WiFi Pineapple Demo!

Debasis Bhattacharya
UH Maui College
debasisb@hawaii.edu



A large, stylized blue brushstroke graphic that sweeps across the left side of the slide, partially overlapping a white-bordered box.

Agenda

- What is the WiFi Pineapple?
- Case Study -
 - GenCyber 2022 Teacher Camp
 - Pre-Camp - Setup
 - Sample Module - Evil Portal
- Lessons learned from 2022 Camp



WiFi Pineapple from Hak5.org

\$120 WiFi Pentest tool.
Mark VII edition



FEATURES



Leading Rogue Access Point

Patented PineAP Suite thoroughly mimics preferred networks, enabling man-in-the-middle attacks



WPA and WPA Enterprise Attacks

Capture WPA handshakes and imitate enterprise access points, capturing enterprise credentials



Precision Targeting Filters

Stay within the scope of engagement and limit collateral damage with MAC and SSID filtering



Simple Web Interface

Fast and intuitive with an emphasis on workflow and actionable intelligence – just click to attack



Cross-Platform

No software to install. Works in any modern web browser on Windows, Mac, Linux, Android, iOS



Advanced Reconnaissance

Visualize the WiFi landscape and the relationships between access points and devices



Actionable Intelligence

Identify vulnerable devices, gather intelligence on the target and direct attacks



Passive Surveillance

Monitor and collect data from all devices in the vicinity. Save and recall reports at any time



Automated Campaigns

Guided campaign wizards deliver repeatable, actionable results with custom reports



Cloud C² Enabled

Deploy with confidence. Remotely command and control the airwaves with Hak5 [Cloud C²](#)



System Status

42.5% 11%
CPU MEM

Disk Usage

0%
ROOT

Connected Clients

2 5
CURRENT PREVIOUS

SSIDs Collected

0
SESSION TO

Connected Clients

MAC Address	IP Address	Connected Time	
30:52:CB:81:EA:D5	172.16.42.109	59m 32s	Kick
F0:C9:D1:E4:49:47		58m 45s	Kick



Notifications

● Started Campaign Site Survey
3 Aug 2020 15:36:17


Campaigns

Status	Name	Type	
●	Site Survey	Monitor	Enable
●	Vulnerable Client Assessment	Passive	Enable

Wireless Landscape



News and Updates



GenCyber 2022
Virtual Teacher Camp
Case Study

University of Hawaii Maui College



Create an Evil Portal!

Teach teachers about realistic looking “login”
pages that are fake!

Sign in to Free Wifi
connectivitycheck.gstatic.com



Log in to Twitter

Phone, email, or username

Password

Log in

[Forgot Password?](#) · [Sign up for Twitter](#)

Sign in to Free Wifi
connectivitycheck.gstatic.com



Sign in

using your Yahoo account

Username, email, or mobile

Password

Next

[Forgot username?](#)

[Create an account](#)

Or, continue with



Sign in to Free Wifi
connectivitycheck.gstatic.com



Sign in

Use your Google Account

Email or phone

Password

[Forgot email?](#)

Not your computer? Use a Private Window to sign in.

[Learn more](#)

[Create Account](#)

Next

Sign in to Free Wifi
connectivitycheck.gstatic.com



Free Wi-Fi

From our friends at Google

Accept & Connect

I agree to the [Terms of Service](#) and have reviewed the [Google Privacy Policy](#)

Need help? 855-446-2374

Sign in to Free Wifi
connectivitycheck.gstatic.com



Welcome @ McDonald's

love free wi-fi

I accept the terms of use

No account?
Click to create an account

To use free WiFi, accept the [terms and conditions](#).

Sign in to Free Wifi
connectivitycheck.gstatic.com



Firmware Upgrade

A new version of the firmware has been detected and awaiting installation. Please review our new terms and conditions and proceed.

Terms And Conditions:

GNU General Public License Notice

This product includes software code developed by third parties, including software code subject to the GNU General Public License

I Agree With Above Terms And Conditions

Enter your WiFi WPA2 Pre-Shared Password Key to continue:

Confirm your WiFi Password:

Start Upgrade



“

This is why you **NEVER**
connect to an
unsecured Wifi SSID in
public!

This is Phishing. Attackers would setup the Wifi Pineapple in a popular location hoping that someone is not paying attention, and connects to their device through an “evil portal”.

Some “free wifi” providers have you “sign-in” in order to access the internet. We will do the same, but we will collect the Username and Passwords.

Pre-Camp - Setup

Camp - Use Evil Portal

Pre-Camp

All teachers were sent one WiFi Pineapple via USPS. They were given setup instructions during the pre-camp 2. Time required - 1 hour to setup

Summer Virtual Camp - Day 3

Teachers were given a detailed module to create an Evil Portal, that was a fake login page. They used their phones to connect to this fake page on the WiFi Pineapple

Wifi Pineapple Evil Portal Setup

45 minutes

Before we begin with the Wifi Pineapple, download, then unzip the files in the "[evilportal-master-THIS ONE.zip](#)" from the Google Drive - Day 3. Link is [here](#)

Set up evil portal

Power on your wifi-Pineapple by plugging in the USB-C cable.

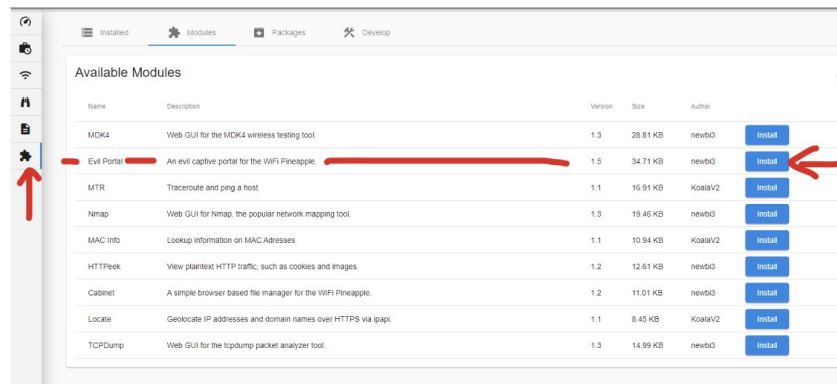
Wait for the blue light to stop blinking.

Your Windows wireless icon should change to



Go to <http://172.16.42.1:1471/> and log in to your Pineapple (**Remember your Username and Password... you will need that later**)

1. Go to Modules -> Available Modules and install the "Evil Portal"



The screenshot shows the Pineapple web interface with the 'Available Modules' page. The 'Evil Portal' module is highlighted with a red box and a red arrow pointing to its 'Install' button. The table below lists the available modules:

Name	Description	Version	Size	Author	Install
MDK4	Web GUI for the MDK4 wireless testing tool	1.3	28.61 KB	newb03	Install
Evil Portal	An evil captive portal for the WiFi Pineapple.	1.5	34.71 KB	newb03	Install
MTR	Traceroute and ping a host.	1.1	16.91 KB	KoalaV2	Install
Nmap	Web GUI for Nmap, the popular network mapping tool	1.3	19.46 KB	newb03	Install
MAC Info	Lookup information on MAC Addresses	1.1	10.94 KB	KoalaV2	Install
HTTPeek	View plaintext HTTP traffic, such as cookies and images.	1.2	12.61 KB	newb03	Install
Cabinet	A simple browser based file manager for the WiFi Pineapple.	1.2	11.01 KB	newb03	Install
Locate	Geoblocate IP addresses and domain names over HTTPS via ipapi.	1.1	8.45 KB	KoalaV2	Install
TCPDump	Web GUI for the tcpdump packet analyzer tool.	1.3	14.99 KB	newb03	Install

Lessons Learned - during 2022 camp with WiFi Pineapple

Setup Time

Given that the camp was online, it was critical to spend adequate time to prepare teachers to setup the WiFi pineapple. Some teachers needed additional help after the pre-camp

Camp Activity

Key was to give detailed step by step instructions in the module, with pictures and notes. Once the portal was working, explain how it can trick people to giving up passwords!

Caution!

The WiFi Pineapple is professional pen testing tool, that scans networks, creates fake portals and other network activities. It should be used in schools only with permission from admin/IT



Questions, Comments, Feedback?

Debasis Bhattacharya, JD, DBA

debasisb@hawaii.edu