Hak5 WiFi Pineapple Mark VII: A Comprehensive Toolset for Wireless Network Security Testing and Penetration Testing (Part 1)

Part 1: Introduction to WiFi Pineapple and Feature Overview

Jason Yee Follow 7 min read · Jul 26, 2023

12

What are Wireless Network Security Testing and Penetration Testing?

Wireless Network Security and Penetration Testing are critical methods of evaluating the security of a wireless network. Wireless network security testing involves assessing the security of a wireless network by identifying vulnerabilities and weaknesses that could be exploited by attackers. This testing may include using specialized tools to scan for open ports, weak passwords, or other security issues that could be targeted by attackers. The goal of wireless network security testing is to identify potential security risks and take measures to address them to improve the security of the network. Penetration testing, on the other hand, involves actively attempting to exploit vulnerabilities in a wireless network to gain unauthorized access. The results of these tests can be used to identify weaknesses and improve the overall security of the network. Both wireless network security testing and penetration testing are critical components of a comprehensive security strategy for wireless networks.

What is the Hak5 WiFi Pineapple Mark VII?

Image of WiFi Pineapple.

The **Hak5 WiFi Pineapple Mark VII** is a powerful wireless network auditing router and tool that provides a comprehensive suite of tools and modules for wireless security testing and penetration testing. It is designed to help security professionals identify, monitor, and manipulate Wi-Fi networks, and perform various security assessments and testing tasks. With its easy-to-use web-based interface, the WiFi Pineapple allows users to perform tasks such as packet capture, network reconnaissance, and client tracking, making it an essential tool for anyone involved in wireless network security testing. It also includes modules for creating rogue access points, performing MITM attacks, and analyzing wireless traffic, providing users with capabilities for identifying vulnerabilities in wireless networks.

In this article, we will explore the features and capabilities of the Hak5 WiFi Pineapple, and how it can be used for wireless network security testing and penetration testing. We will also discuss real-world scenarios where the WiFi Pineapple can be useful and provide tips and best practices for using it effectively. Whether you are a security professional, network administrator, or curious enthusiast, this article will provide valuable insights into the world of wireless network security testing with the Hak5 WiFi Pineapple.

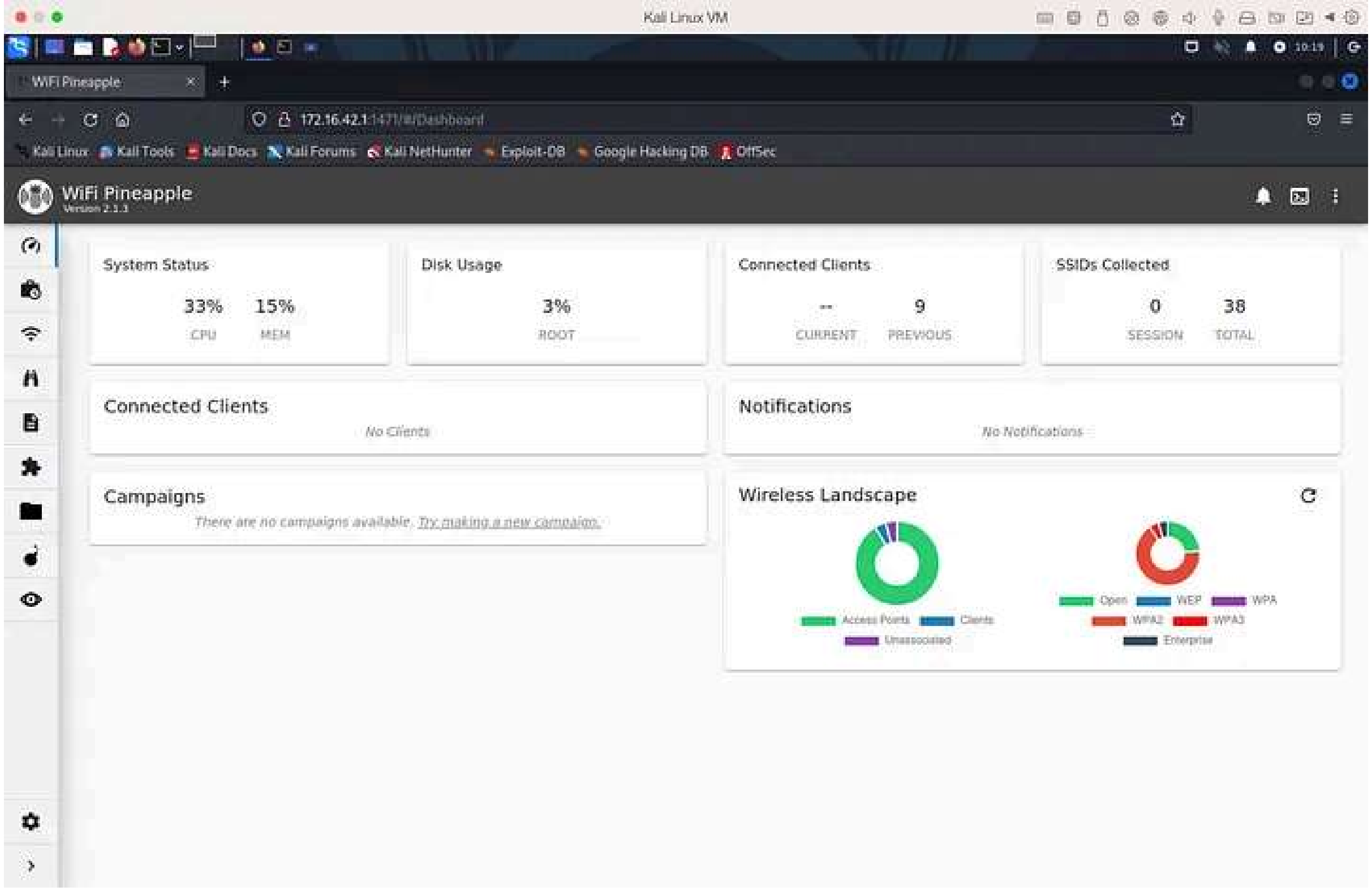
Official Hak5 Documentation: https://docs.hak5.org/wifi-pineapple/

WiFi Pineapple Features — General Overview

Note: The WiFi Pineapple Firmware on which this article is written is version 2.1.3, which may not be updated for later network tests.

Dashboard

The Dashboard module in Hak5 Pineapple WiFi is a web-based interface that provides an overview of the device's status, configuration, and activity logs. It allows users to monitor and manage their WiFi network using a visual interface. The Dashboard displays real-time information on connected clients, their MAC addresses, IP addresses, and the websites they are accessing. It also provides information on Pineapple's firmware version, available storage, and CPU usage.



System Status

33% CPU

15% MEM

Disk Usage

3% ROOT

Connected Clients

-- CURRENT

9 PREVIOUS

SSIDs Collected

0 SESSION

38 TOTAL

Connected Clients

No Clients

Notifications

No Notifications

Campaigns

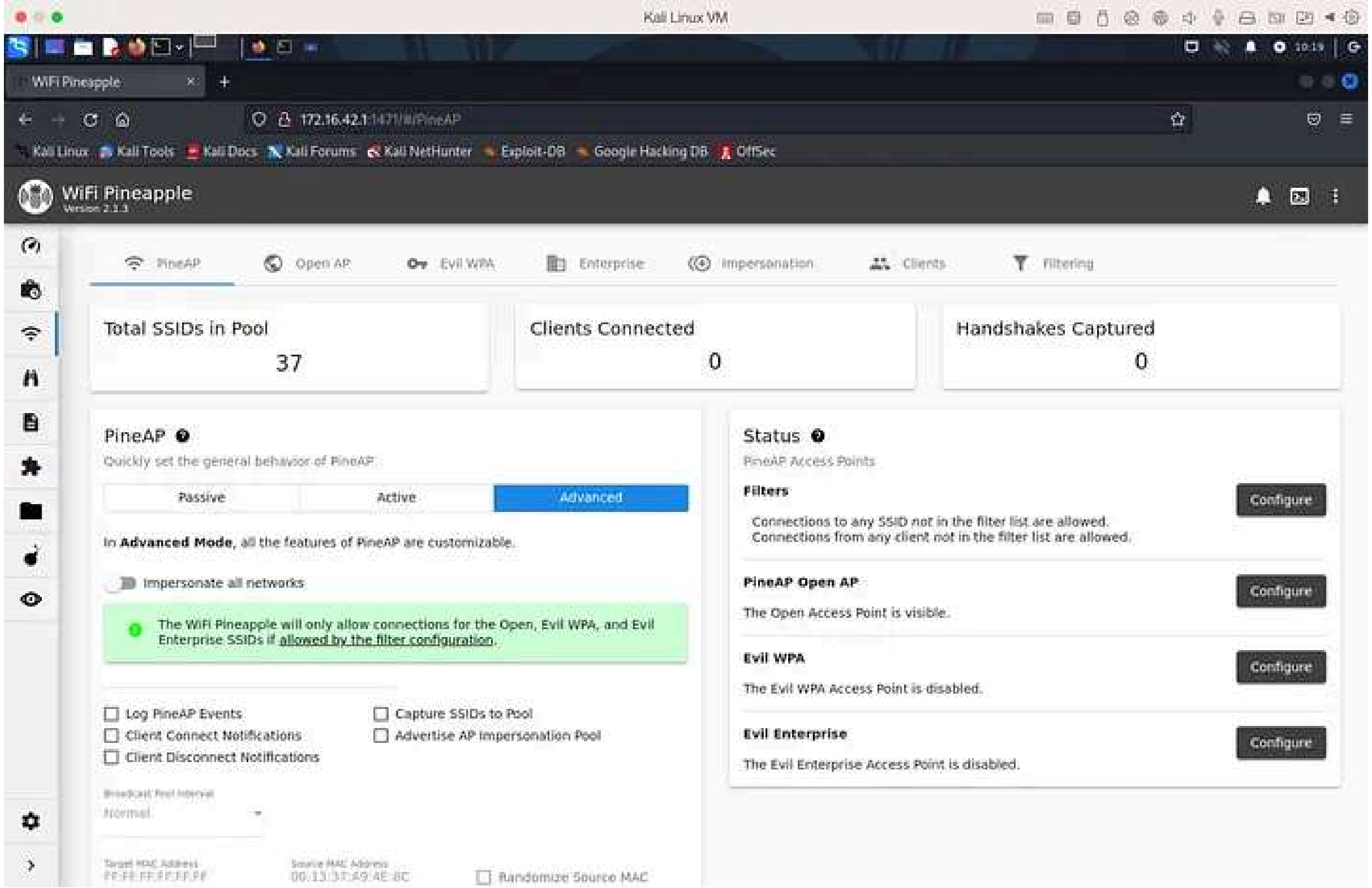
There are no campaigns available. Try making a new campaign.

Wireless Landscape

Screenshot of Hak5 WiFi Pineapple Dashboard Module.

PineAP Suite

The PineAP (Pineapple Access Point) Suite is a set of tools and modules available in the Hak5 Pineapple WiFi device that enables users to perform advanced WiFi network penetration testing and security assessments. The PineAP Suite includes modules for **capturing and analyzing wireless traffic, creating rogue access points, performing man-in-the-middle attacks, and conducting network reconnaissance**. The PineAP module can be used to create a fake access point to lure devices to connect to it, allowing attackers to intercept sensitive information such as login credentials and other data.



Total SSIDs in Pool
37

Clients Connected
0

Handshakes Captured
0

PineAP

Quickly set the general behavior of PineAP

Passive | Active | **Advanced**

In **Advanced Mode**, all the features of PineAP are customizable.

Impersonate all networks

The WiFi Pineapple will only allow connections for the Open, Evil WPA, and Evil Enterprise SSIDs if allowed by the filter configuration.

- □ Log PineAP Events
- □ Client Connect Notifications
- □ Client Disconnect Notifications
- □ Capture SSIDs to Pool
- □ Advertise AP Impersonation Pool

Broadcast Pool Interval
Normal

Target MAC Address
FF:FF:FF:FF:FF:FF

Source MAC Address
00:13:37:A9:4E:8C

□ Randomize Source MAC

Status

PineAP Access Points

Filters

Connections to any SSID not in the filter list are allowed.
Connections from any client not in the filter list are allowed.

PineAP Open AP

The Open Access Point is visible.

Evil WPA

The Evil WPA Access Point is disabled.

Evil Enterprise

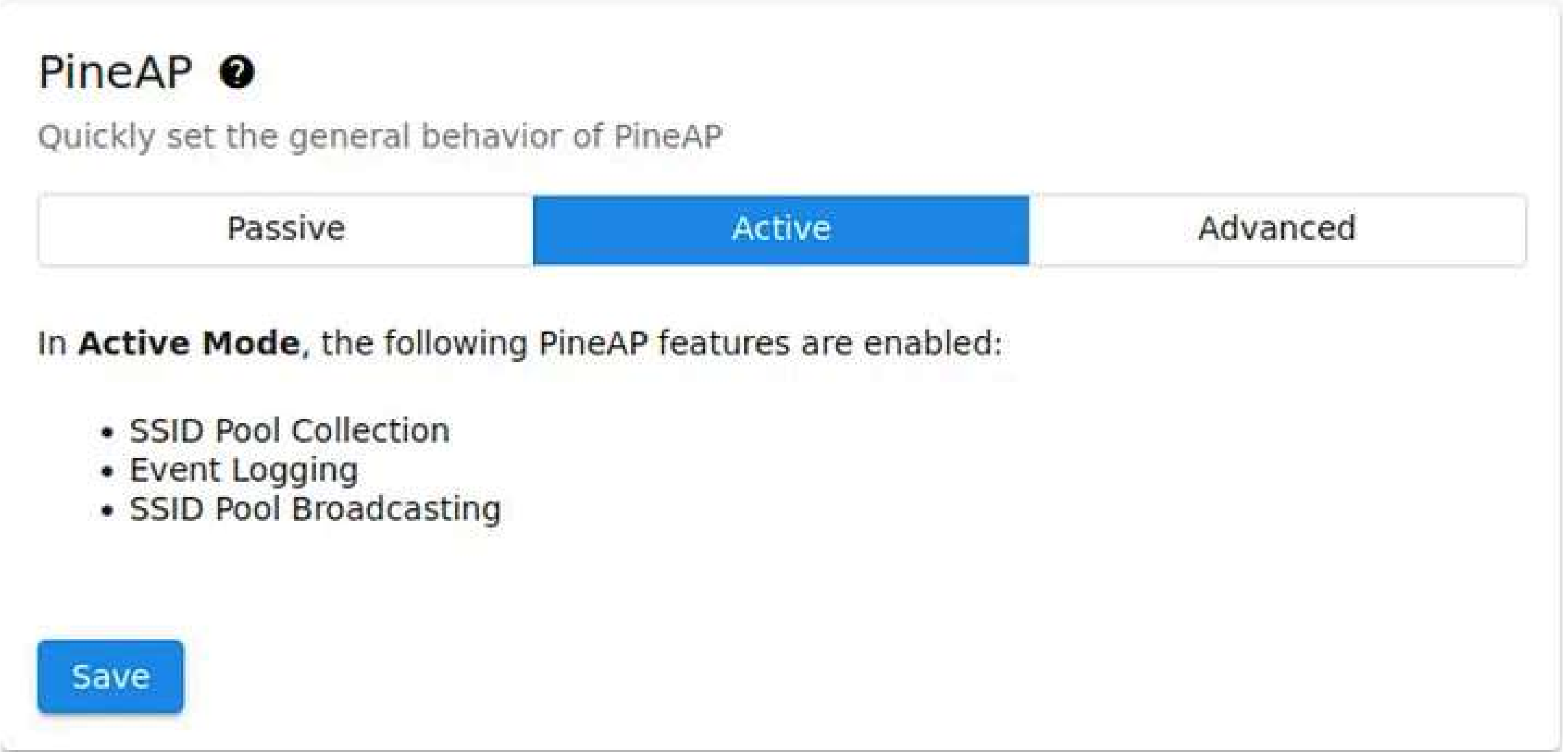
The Evil Enterprise Access Point is disabled.

Screenshot of Hak5 WiFi Pineapple PineAP Suite Module.

KARMA Attacks

A KARMA attack is a type of wireless network attack that exploits a feature in many Wi-Fi devices called “probe requests.” When a Wi-Fi device is not connected to a network, it periodically sends out probe requests to discover available Wi-Fi networks. These probe requests contain the device's MAC address and other information that can be used to identify the device.

A KARMA attack takes advantage of this behavior by impersonating a legitimate Wi-Fi network and responding to these probe requests with a fake access point that has the same name (SSID) as a known Wi-Fi network that the device has previously connected to. When the device tries to connect to the fake access point, the attacker can intercept and monitor the device's network traffic, steal sensitive information, or launch other attacks.

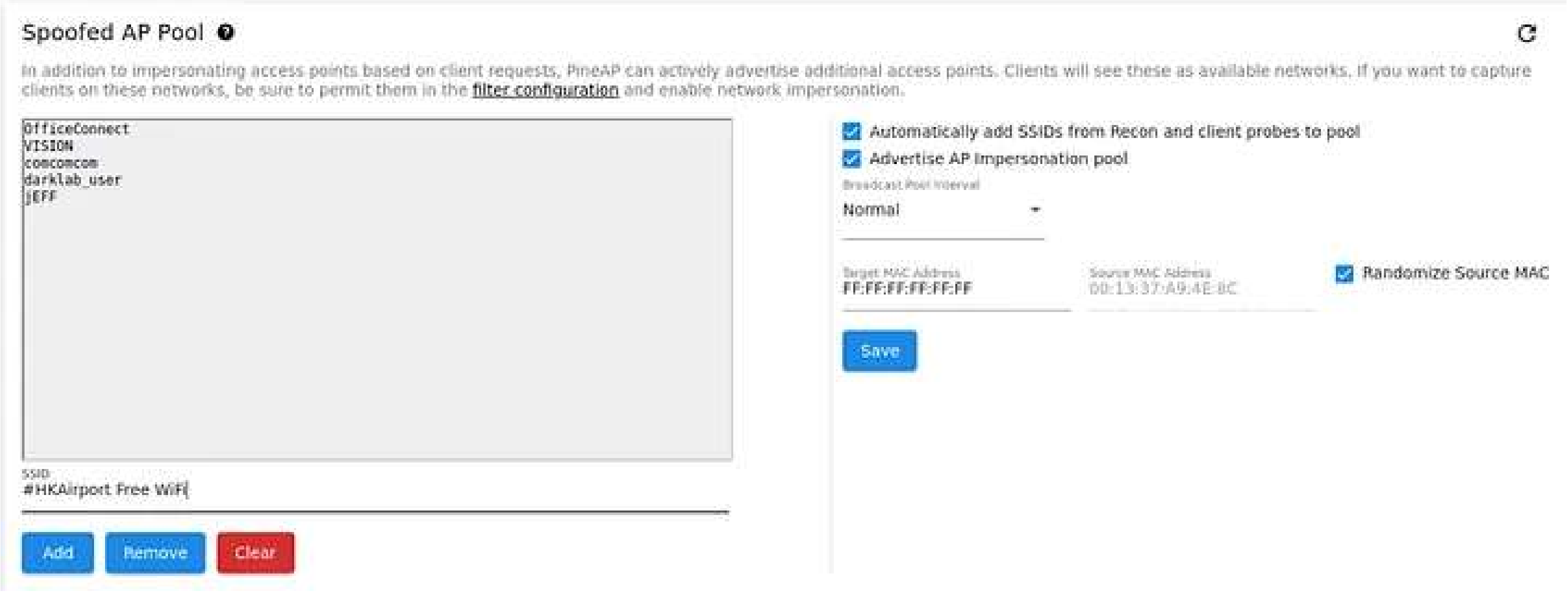


Quickly set the general behavior of PineAP

In **Active Mode**, the following PineAP features are enabled:

- SSID Pool Collection
- Event Logging
- SSID Pool Broadcasting

Set your PineAP to **Active Mode.** This will enable your Wifi Pineapple to begin scanning for probe requests, collecting SSIDs, and broadcasting access points impersonations, which will seem familiar to clients who try to connect to the internet.



Spoofed AP Pool

In addition to impersonating access points based on client requests, PineAP can actively advertise additional access points. Clients will see these as available networks. If you want to capture clients on these networks, be sure to permit them in the filter configuration and enable network impersonation.

```
OfficeConnect
VISION
comcomcom
darklab_user
jEFF
```

SSID: #HKAirport Free WiFi

☑ Automatically add SSIDs from Recon and client probes to pool

☑ Advertise AP Impersonation pool

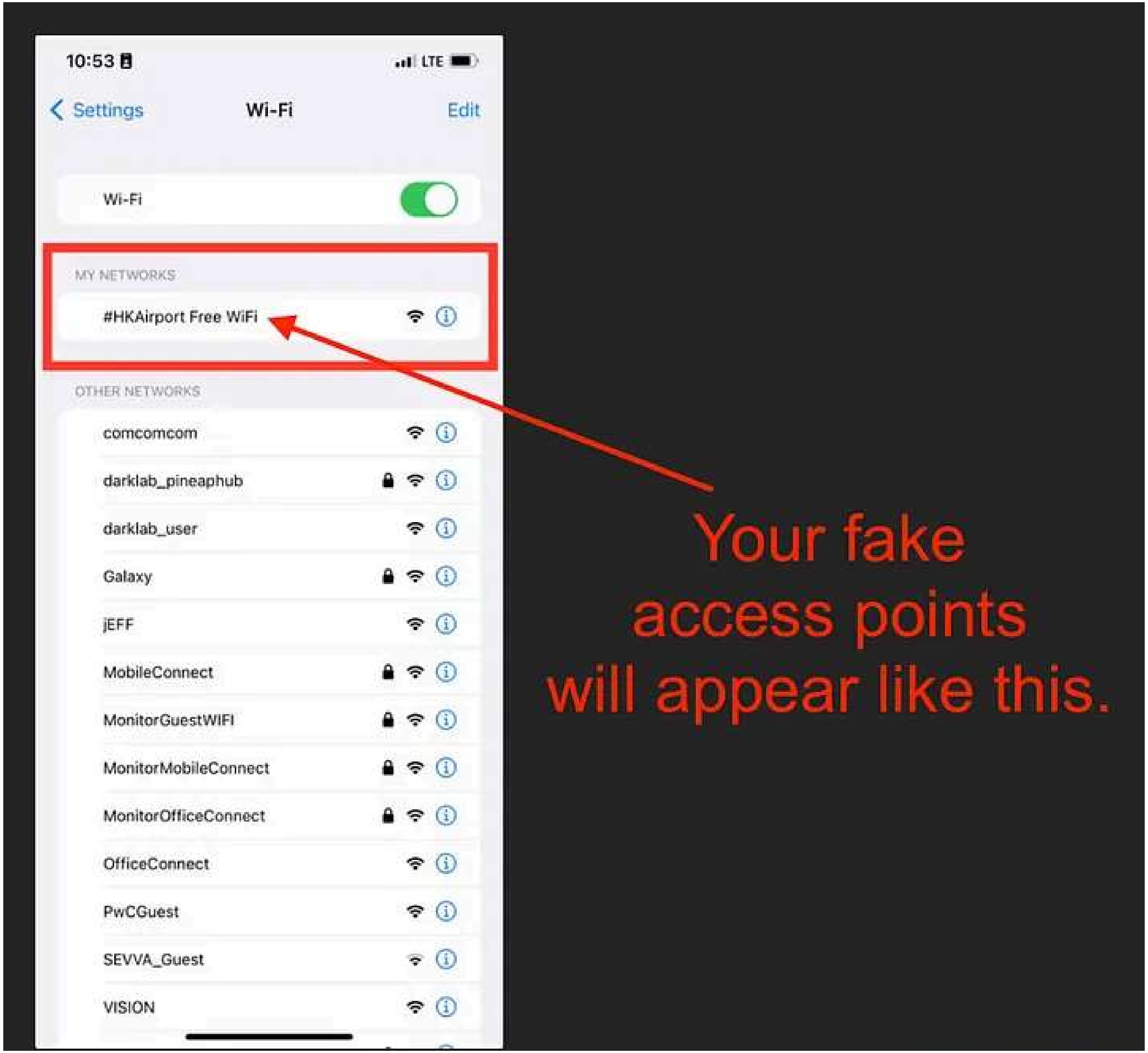
Broadcast Pool Interval: Normal

Target MAC Address: FF:FF:FF:FF:FF:FF

Source MAC Address: 00:13:37:A9:4E:8C

☑ Randomize Source MAC

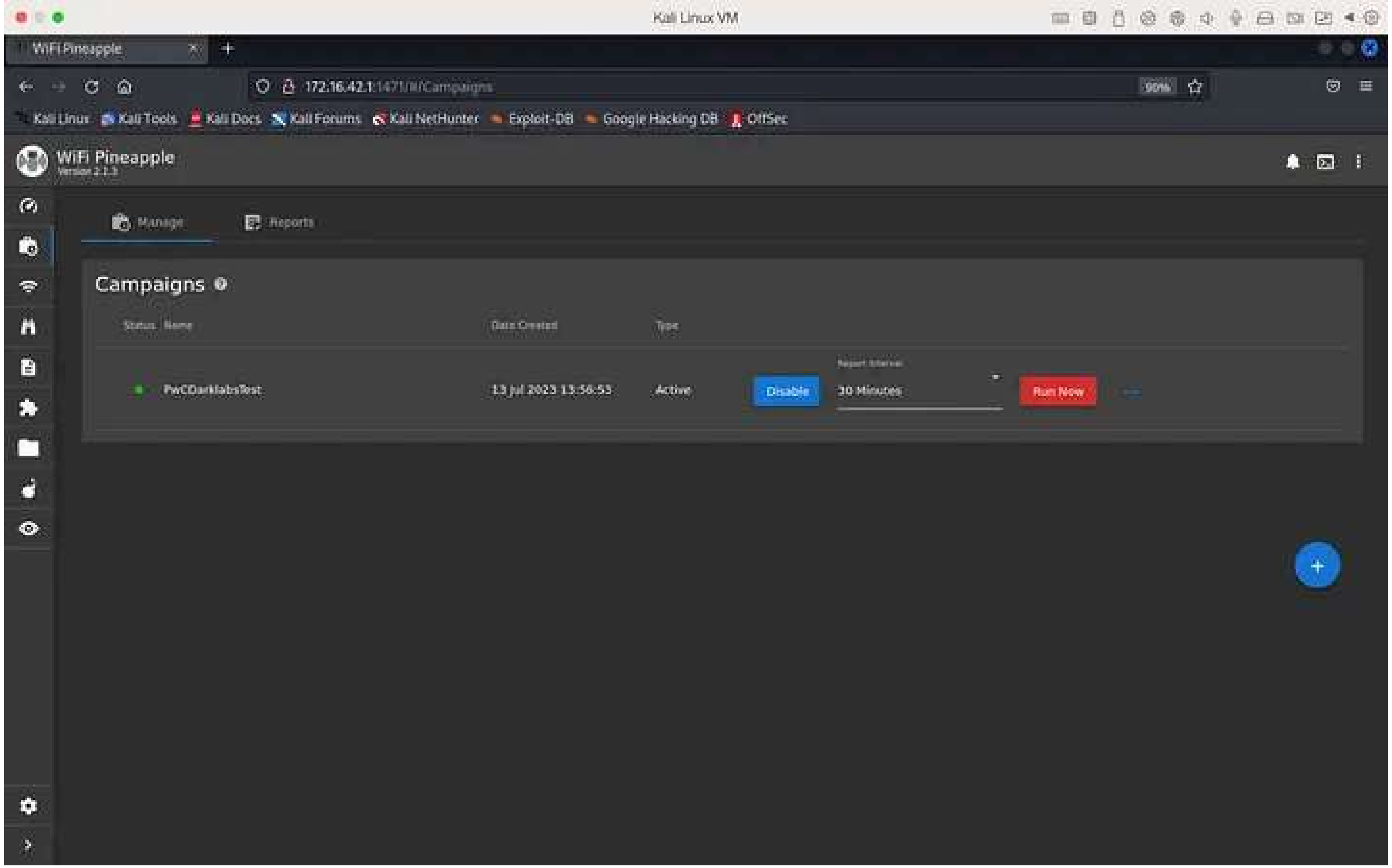
Collected SSIDs will appear in the Spoofed AP Pool, where you can configure AP pool settings, as well as add custom SSIDs (**Example SSID Broadcast Shown Below**). AP pool settings can also be edited through “Advanced” settings in the Dashboard.


10:53
LTE
Settings
Wi-Fi
Edit
Wi-Fi
MY NETWORKS
#HKAirport Free WiFi
OTHER NETWORKS
comcomcom
darklab_pineaphub
darklab_user
Galaxy
jEFF
MobileConnect
MonitorGuestWIFI
MonitorMobileConnect
MonitorOfficeConnect
OfficeConnect
PwCGuest
SEVVA_Guest
VISION
Your fake access points will appear like this.

To prevent KARMA attacks, it is important to configure Wi-Fi devices to only connect to trusted networks and to disable automatic Wi-Fi network connection features. Additionally, using secure Wi-Fi protocols such as WPA2 with strong passwords can help protect against KARMA attacks.

Campaigns

Campaigns in the WiFi Pineapple module are automated configurations to network engagement and report generation.



Campaigns

Status	Name	Date Created	Type		Report Interval	
●	PwCDarklabsTest	13 Jul 2023 13:56:53	Active	Disable	30 Minutes	Run Now

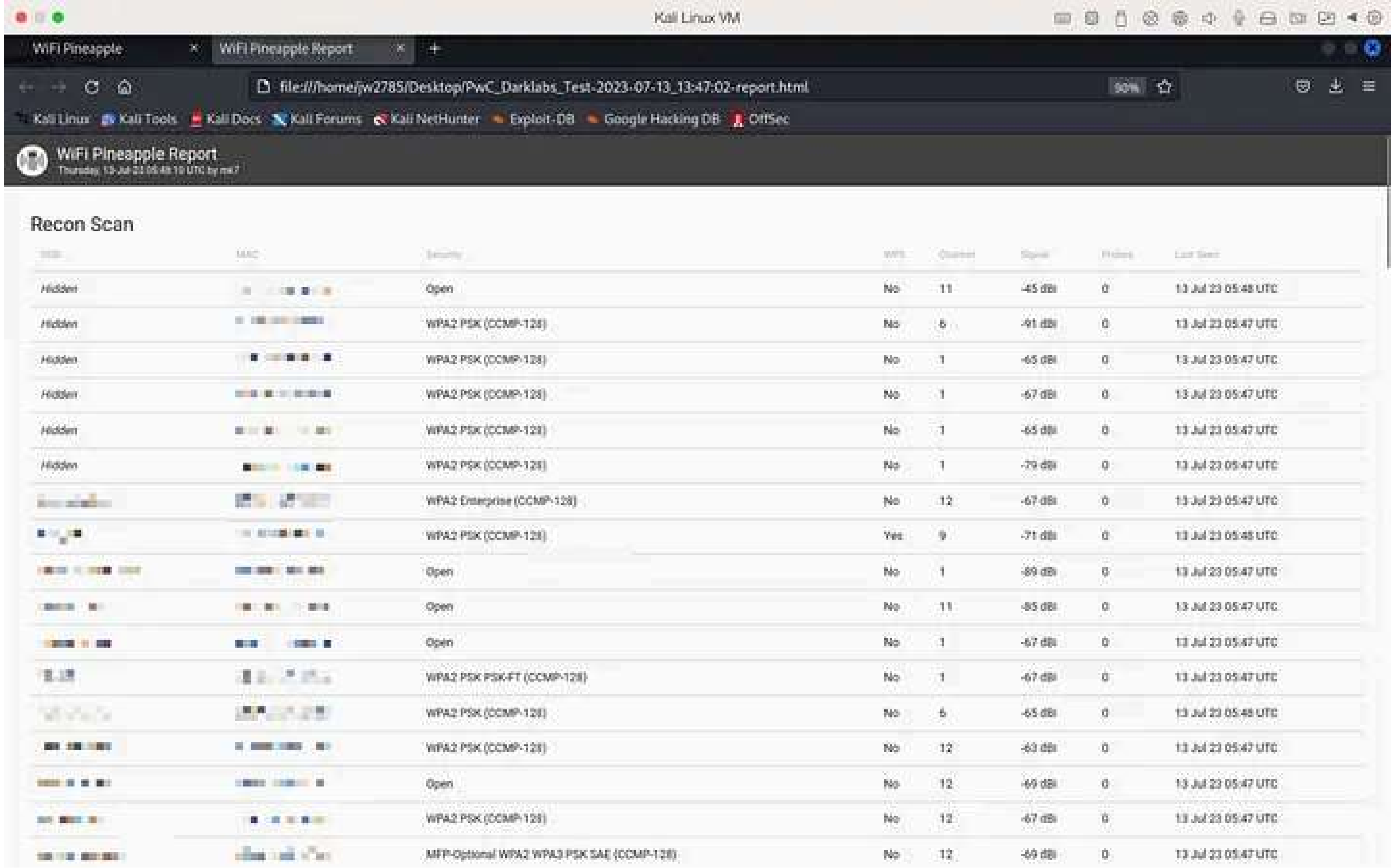
Screenshot of Hak5 WiFi Pineapple Campaigns Module.

There are 3 modes for campaigns in total.

1. **Reconnaisance — Monitor Only:** Reconnaisance mode observes the activity of client devices and access points within a specified area of the WiFi environment in a non-intrusive manner.

2. **Client Device Assessments — Passive:** This mode detects client devices vulnerable to simple rogue access points or evil twin attacks. This is achieved by utilizing a passive PineAP mode that imitates access points only when specifically requested. Depending on the filter settings, client devices may be permitted to connect with the WiFi Pineapple.

3. **Client Device Assessment — Active:** Through passive PineAP mode, this mode identifies client devices susceptible to basic rogue access points or evil twin attacks. The PineAP mode is activated only upon direct request and the filter configuration determines whether client devices are allowed to connect with the WiFi Pineapple.



WiFi Pineapple Report

Thursday, 13-Jul-23 05:48:10 UTC by mk7

Recon Scan

SSID	MAC	Security	WPS	Channel	Signal	Probes	Last Seen
Hidden	[redacted]	Open	No	11	-45 dBi	0	13 Jul 23 05:48 UTC
Hidden	[redacted]	WPA2 PSK (CCMP-128)	No	6	-91 dBi	0	13 Jul 23 05:47 UTC
Hidden	[redacted]	WPA2 PSK (CCMP-128)	No	1	-65 dBi	0	13 Jul 23 05:47 UTC
Hidden	[redacted]	WPA2 PSK (CCMP-128)	No	1	-67 dBi	0	13 Jul 23 05:47 UTC
Hidden	[redacted]	WPA2 PSK (CCMP-128)	No	1	-65 dBi	0	13 Jul 23 05:47 UTC
Hidden	[redacted]	WPA2 PSK (CCMP-128)	No	1	-79 dBi	0	13 Jul 23 05:47 UTC
[redacted]	[redacted]	WPA2 Enterprise (CCMP-128)	No	12	-67 dBi	0	13 Jul 23 05:47 UTC
[redacted]	[redacted]	WPA2 PSK (CCMP-128)	Yes	9	-71 dBi	0	13 Jul 23 05:48 UTC
[redacted]	[redacted]	Open	No	1	-89 dBi	0	13 Jul 23 05:47 UTC
[redacted]	[redacted]	Open	No	11	-85 dBi	0	13 Jul 23 05:47 UTC
[redacted]	[redacted]	Open	No	1	-67 dBi	0	13 Jul 23 05:47 UTC
[redacted]	[redacted]	WPA2 PSK PSK-FT (CCMP-128)	No	1	-67 dBi	0	13 Jul 23 05:47 UTC
[redacted]	[redacted]	WPA2 PSK (CCMP-128)	No	6	-65 dBi	0	13 Jul 23 05:48 UTC
[redacted]	[redacted]	WPA2 PSK (CCMP-128)	No	12	-63 dBi	0	13 Jul 23 05:47 UTC
[redacted]	[redacted]	Open	No	12	-69 dBi	0	13 Jul 23 05:47 UTC
[redacted]	[redacted]	WPA2 PSK (CCMP-128)	No	12	-67 dBi	0	13 Jul 23 05:47 UTC
[redacted]	[redacted]	MFP-Optional WPA2 WPA3 PSK SAE (CCMP-128)	No	12	-69 dBi	0	13 Jul 23 05:47 UTC

Screenshot of Hak5 WiFi Pineapple Campaign Generated Report.

An example of these modes, **Client Device Assessments (Active)**, works by sending de-authentication packets to client devices, forcing them to disconnect from the network and then reconnect. During this process, the

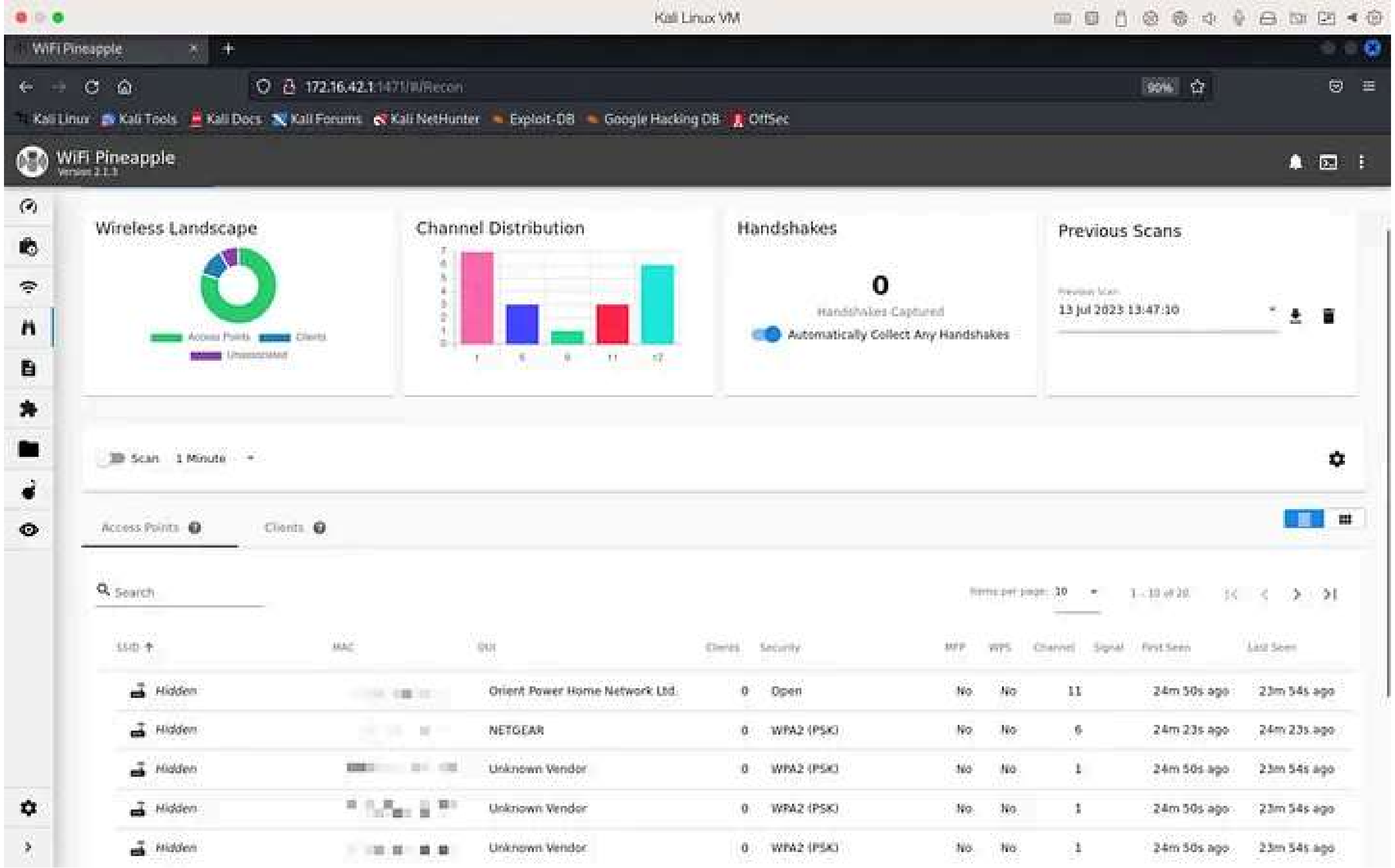
WiFi Pineapple automatically conducts reconnaissance scans and associated disconnections, capturing the client device's wireless credentials, such as the SSID, MAC address, and encryption type.

Once the credentials are captured, the WiFi Pineapple can analyze them to identify potential security weaknesses in the client device’s wireless configuration. For example, it may identify weak encryption settings or default passwords that could be exploited by attackers.

Client Device Assessments (Active) is a powerful tool to help identify potential security risks in wireless networks. However, it should be used responsibly and only with the permission of the network owner or administrator. Unauthorized use of this feature can lead to legal consequences.

Recon

The **Recon** (Reconnaissance) module is a feature of the WiFi Pineapple firmware that allows users to perform active and passive reconnaissance of wireless networks. It provides a comprehensive set of tools for scanning the surrounding WiFi environment and gathering information such as the names (SSIDs) of nearby access points, their channels, encryption types, and signal strengths. The Recon module can also detect connected client devices, their vendor information, and probe requests, and can also perform de-authentication attacks to disconnect client devices from their access points.



Automatically Collect Any Handshakes

13 Jul 2023 13:47:10

Scan 1 Minute

Access Points | Clients

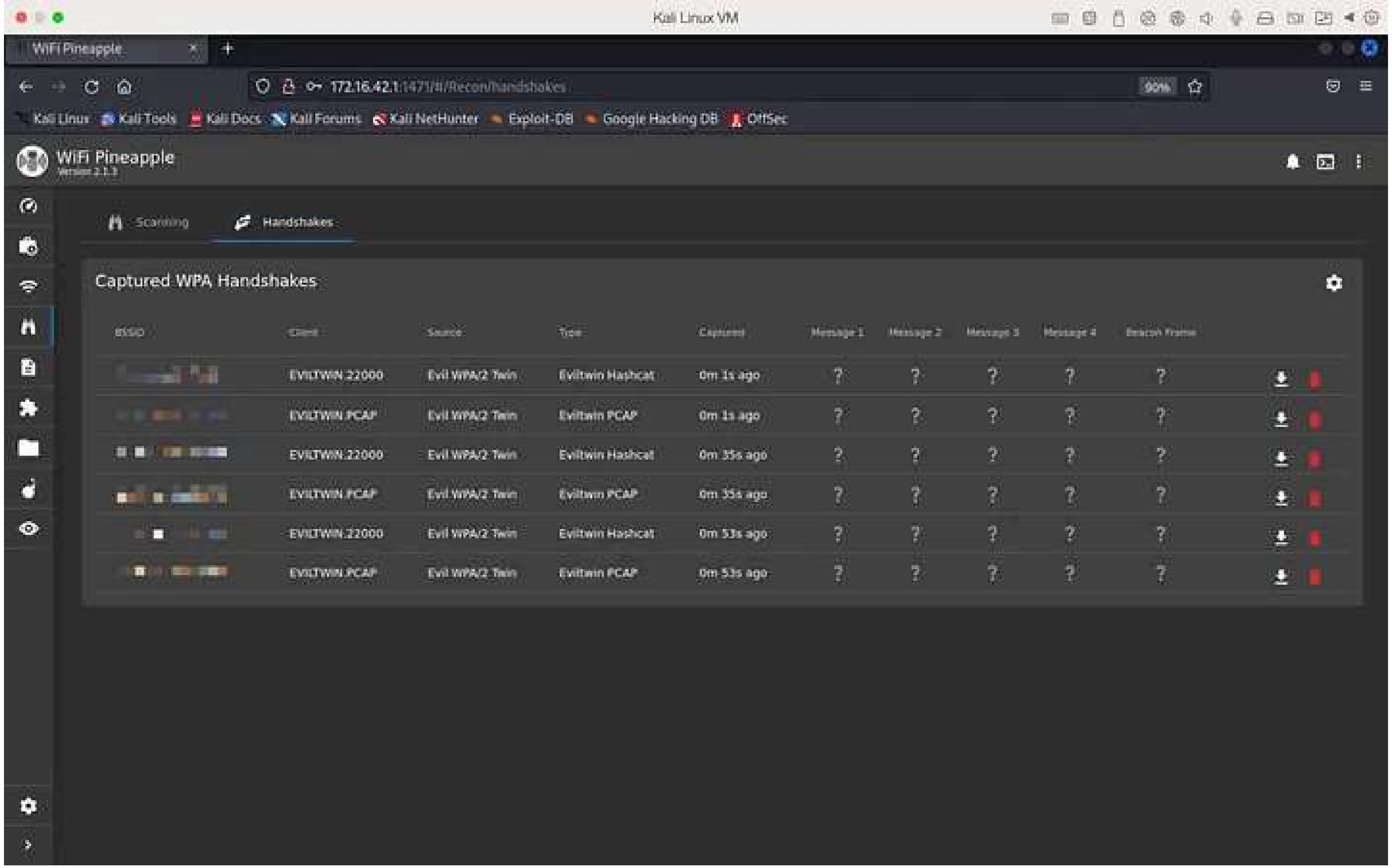
Search

Items per page: 10 | 1 – 10 of 20

SSID	MAC	OUI	Clients	Security	MFP	WPS	Channel	Signal	First Seen	Last Seen
Hidden	[redacted]	Orient Power Home Network Ltd.	0	Open	No	No	11		24m 50s ago	23m 54s ago
Hidden	[redacted]	NETGEAR	0	WPA2 (PSK)	No	No	6		24m 23s ago	24m 23s ago
Hidden	[redacted]	Unknown Vendor	0	WPA2 (PSK)	No	No	1		24m 50s ago	23m 54s ago
Hidden	[redacted]	Unknown Vendor	0	WPA2 (PSK)	No	No	1		24m 50s ago	23m 54s ago
Hidden	[redacted]	Unknown Vendor	0	WPA2 (PSK)	No	No	1		24m 50s ago	23m 54s ago

Screenshot of Hak5 WiFi Pineapple Recon Module.

Additionally, the module also displays captured WPA Handshakes if any of them are collected by the Evil WPA included in the WiFi Pineapple.



Captured WPA Handshakes

BSSID	Client	Source	Type	Captured	Message 1	Message 2	Message 3	Message 4	Beacon Frame
[redacted]	EVILTWIN.22000	Evil WPA/2 Twin	Eviltwin Hashcat	0m 1s ago	?	?	?	?	?
[redacted]	EVILTWIN.PCAP	Evil WPA/2 Twin	Eviltwin PCAP	0m 1s ago	?	?	?	?	?
[redacted]	EVILTWIN.22000	Evil WPA/2 Twin	Eviltwin Hashcat	0m 35s ago	?	?	?	?	?
[redacted]	EVILTWIN.PCAP	Evil WPA/2 Twin	Eviltwin PCAP	0m 35s ago	?	?	?	?	?
[redacted]	EVILTWIN.22000	Evil WPA/2 Twin	Eviltwin Hashcat	0m 53s ago	?	?	?	?	?
[redacted]	EVILTWIN.PCAP	Evil WPA/2 Twin	Eviltwin PCAP	0m 53s ago	?	?	?	?	?

Screenshot of Hak5 WiFi Pineapple Recon WPA Handshake Module.

Read Part 2 Here: https://medium.com/@jasony58/hak5-wifi-pineapple-mark-vii-a-comprehensive-toolset-for-wireless-network-security-testing-and-c9b8c80c661e

Cybersecurity Network Security Ethical Hacking Penetration Testing

Wifi Pineapple

Published in InfoSec Write-ups

Follow

70K followers · Last published 1 day ago

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: https://weekly.infosecwriteups.com/

Written by Jason Yee

Follow

44 followers · 42 following

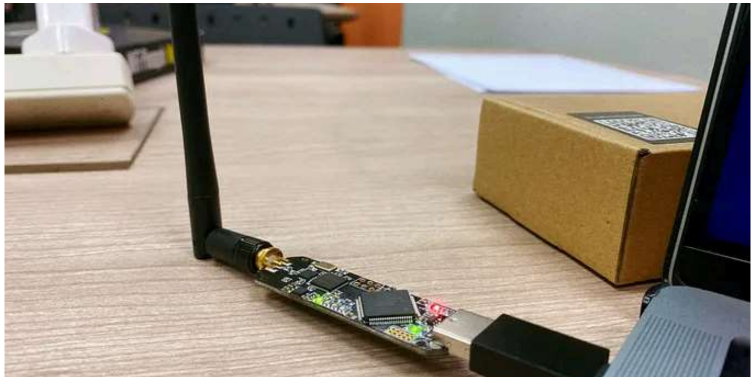
👋 IBDP Student, Front-End & AI Development. Cybersecurity Research tech.withjasony.com

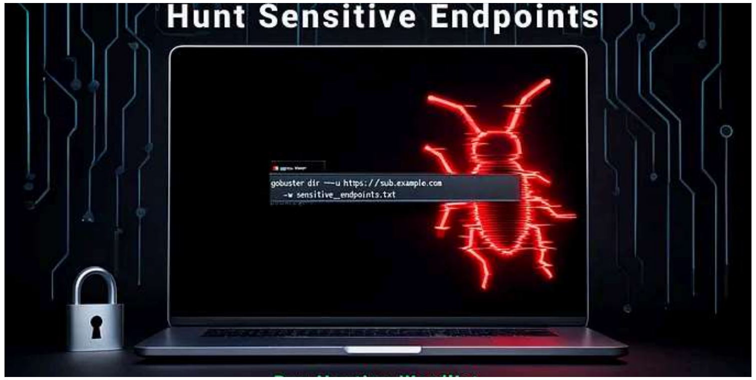
No responses yet

Write a response

What are your thoughts?

More from Jason Yee and InfoSec Write-ups





```
gobuster dir —-u https://sub.example.com
   -w sensitive_endpoints.txt
```

In InfoSec Write-ups by Jason Yee

Exploring the Capabilities of Flipper Zero and Ubertooth One:...

Part 2: Ubertooth One Features and Concluding Notes

Jul 24, 2023 45

In InfoSec Write-ups by Monika sharma

Sensitive Endpoint Wordlist for Bug Hunting

Uncover Hidden Flaws: A Powerful Wordlist for Bug Bounty Success

Sep 1 167 2

In InfoSec Write-ups by coffinxp

Mastering WordPress Bug Hunting: A Complete Guide for Security…

Learn step-by-step techniques, tools and strategies to uncover high-impact…

✦ Aug 22 456 8

In InfoSec Write-ups by Jason Yee

Exploring the Capabilities of Flipper Zero and Ubertooth One:…

Part 1: Introduction to Wireless Security Testing, Flipper Zero Features, and…

Jul 24, 2023 60

See all from Jason Yee

See all from InfoSec Write-ups

Recommended from Medium

Precious Uche Eze

TryHackMe Kenobi CTF Walkthrough

Task 1—Deploy the vulnerable machine Task 2

May 3 4 1

In System Weakness by Qasim Mahmood Khalid

🎯 Secret ChatGPT Prompts That 10x My Bug Bounty Success Rate...

Picture this: You're staring at a massive scope list with 50+ domains, knowing you need to...

✦ 5d ago 23

Kartik

Automating Subdomain Enumeration with Bash — My…

Subdomain enumeration is one of the most crucial steps in bug bounty hunting and…

Aug 26

In OSINT Team by Aj

How Pen Testers Really Break In: The Methodology Behind the…

It’s not just fancy tools — it’s patience, psychology, and a well-played game of digit…

5d ago 57

In Cyber Security Write-ups by Vipul Sonule

Bypassing WAFs Like a Hacker 🧙‍♂️: Tricks Hackers Use

✦ 5d ago 👏 171 💬 2

In InfoSec Write-ups by Aman Sharma

"Day 8: Mobile Hacking—How I Cracked a Banking App's PIN in 1…

Two weeks ago, I reverse-engineered a "secure" banking app that claimed to use…

✦ Aug 11 👏 310 💬 4

See more recommendations

Help Status About Careers Press Blog Privacy Rules Terms Text to speech