

Hak5 Essentials Field Kit

CorkSec March 7th 2017

Dylan Smyth

Nimbus Centre, Cork Institute of Technology

Hak5 Essentials Field Kit



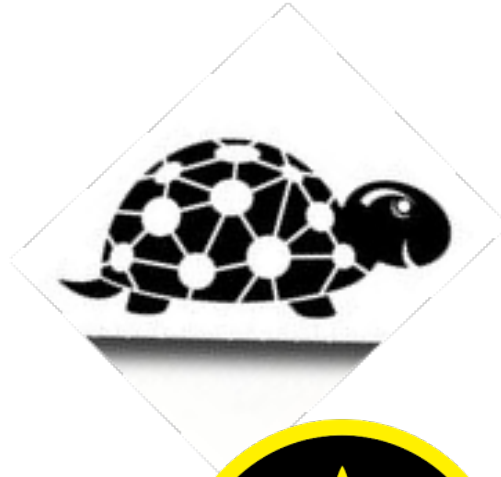
Hak5 Essentials Field Kit



<https://www.hak5.org>

Hak5 Essentials Field Kit

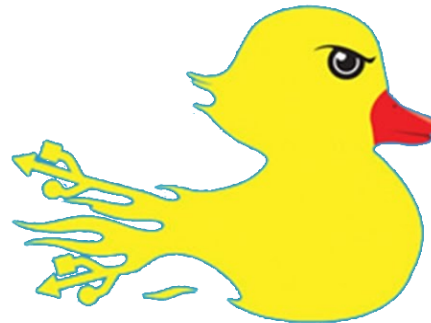
- LAN Turtle



- Wifi Pineapple



- USB Rubber Ducky



Hak5 Essentials Field Kit

LAN Turtle



Hak5 Essentials Field Kit

LAN Turtle - Description

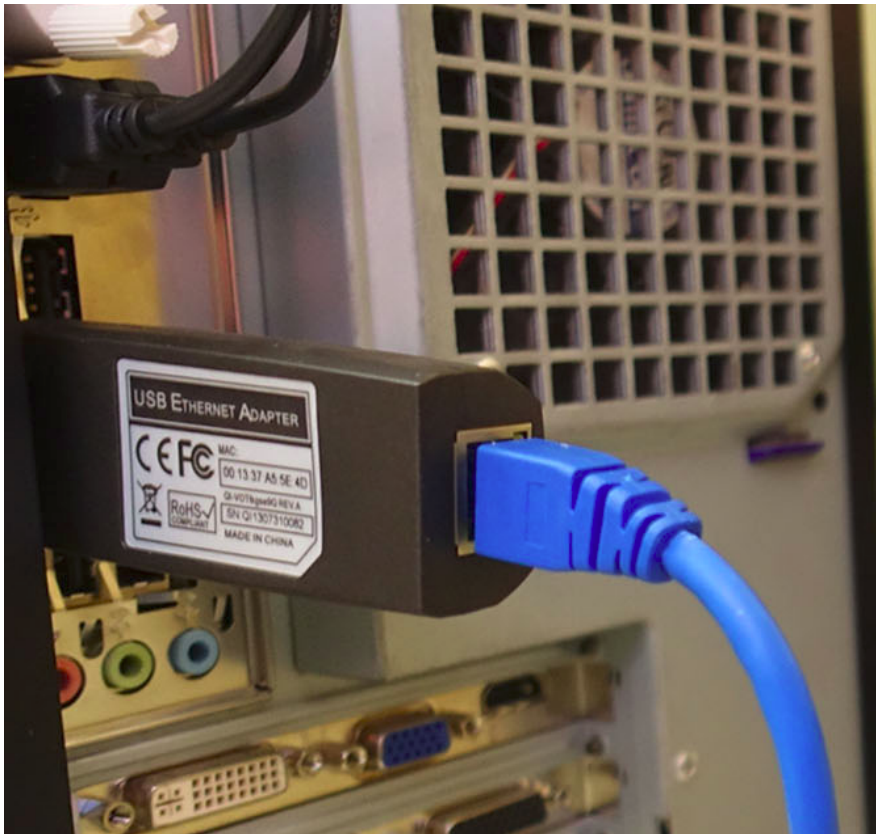
- Embedded computer with Linux based OS
- Housed in a generic USB-to-Ethernet



Hak5 Essentials Field Kit

LAN Turtle - Deployment

- Just needs power and a network connection



Hak5 Essentials Field Kit

LAN Turtle - Deployment

- Connect via SSH or have it connect back to you

DROP A LAN TURTLE. GET A SHELL.



Hak5 Essentials Field Kit

LAN Turtle - Deployment

- Run attacks against host or network

Modules

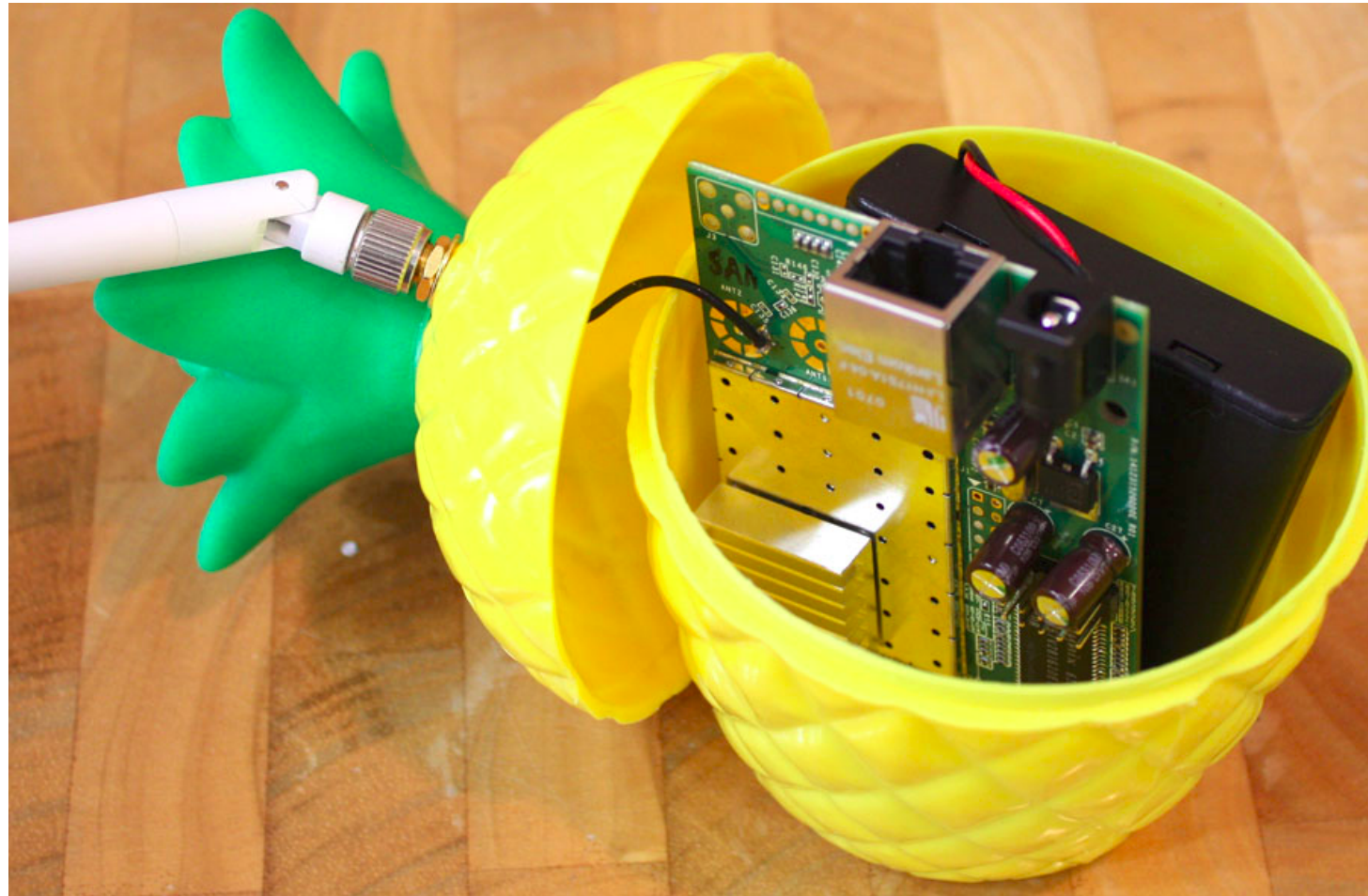
```
[ ] autossh      AutoSSH maintains persistent secure shells
[ ] cron         Schedule Tasks
[ ] dns-spoof    dnsspoof forges replies to arbitrary DNS addr
[X] dnsmasq-spoof DNSSpoof using DNSMasq instead of Dsniff tool
[ ] follow-file  Follow log printing data as file grows
[ ] keymanager   SSH Key Manager
[ ] meterpreter  Metasploit payload to maintain shells
[ ] netcat-revshell NetCat Reverse Shell
[ ] nmap-scan    Network Mapper discovers hosts and services o
[ ] openvpn      Openvpn client
[ ] ptunnel      Proxies TCP over Ping (ICMP) traffic
[ ] script2email Email script output via SMTP
v(+)                                                    75%
```

< SELECT >

< BACK >

Hak5 Essentials Field Kit

Wifi Pineapple



Hak5 Essentials Field Kit

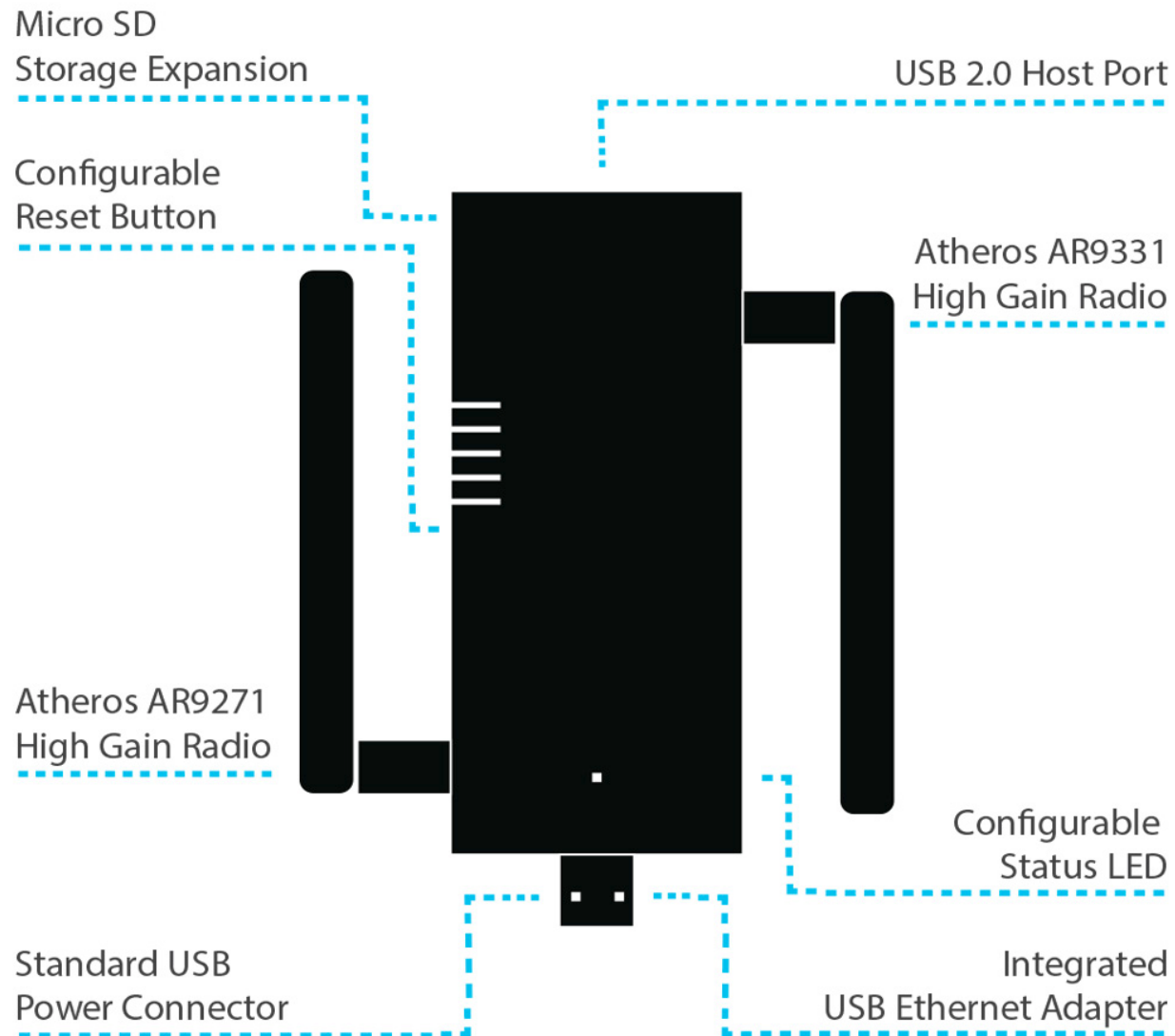
Wifi Pineapple - Description

- Wifi security auditing platform
- Kit contains the Wifi Pineapple Nano



Hak5 Essentials Field Kit

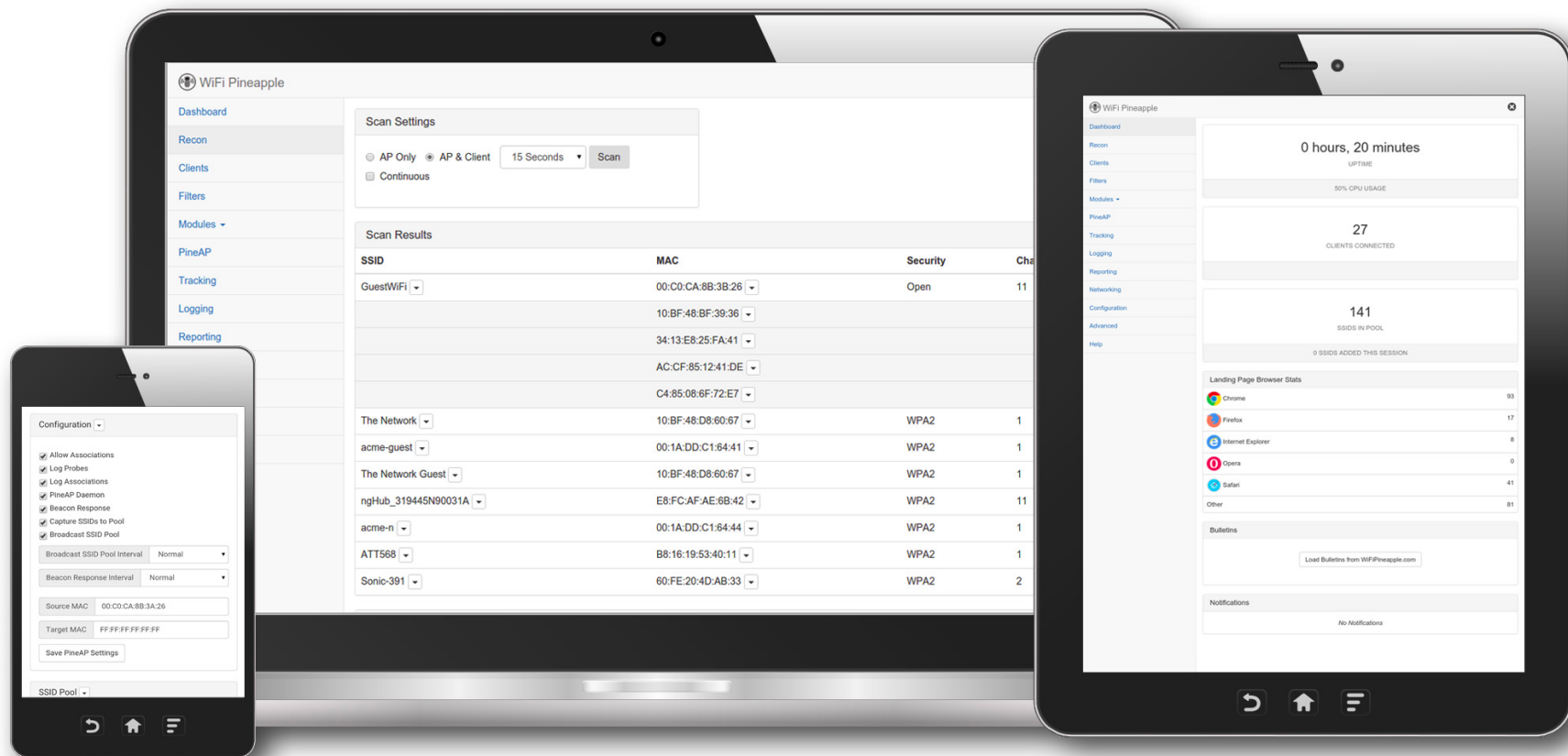
Wifi Pineapple - Description



Hak5 Essentials Field Kit

Wifi Pineapple - Deployment

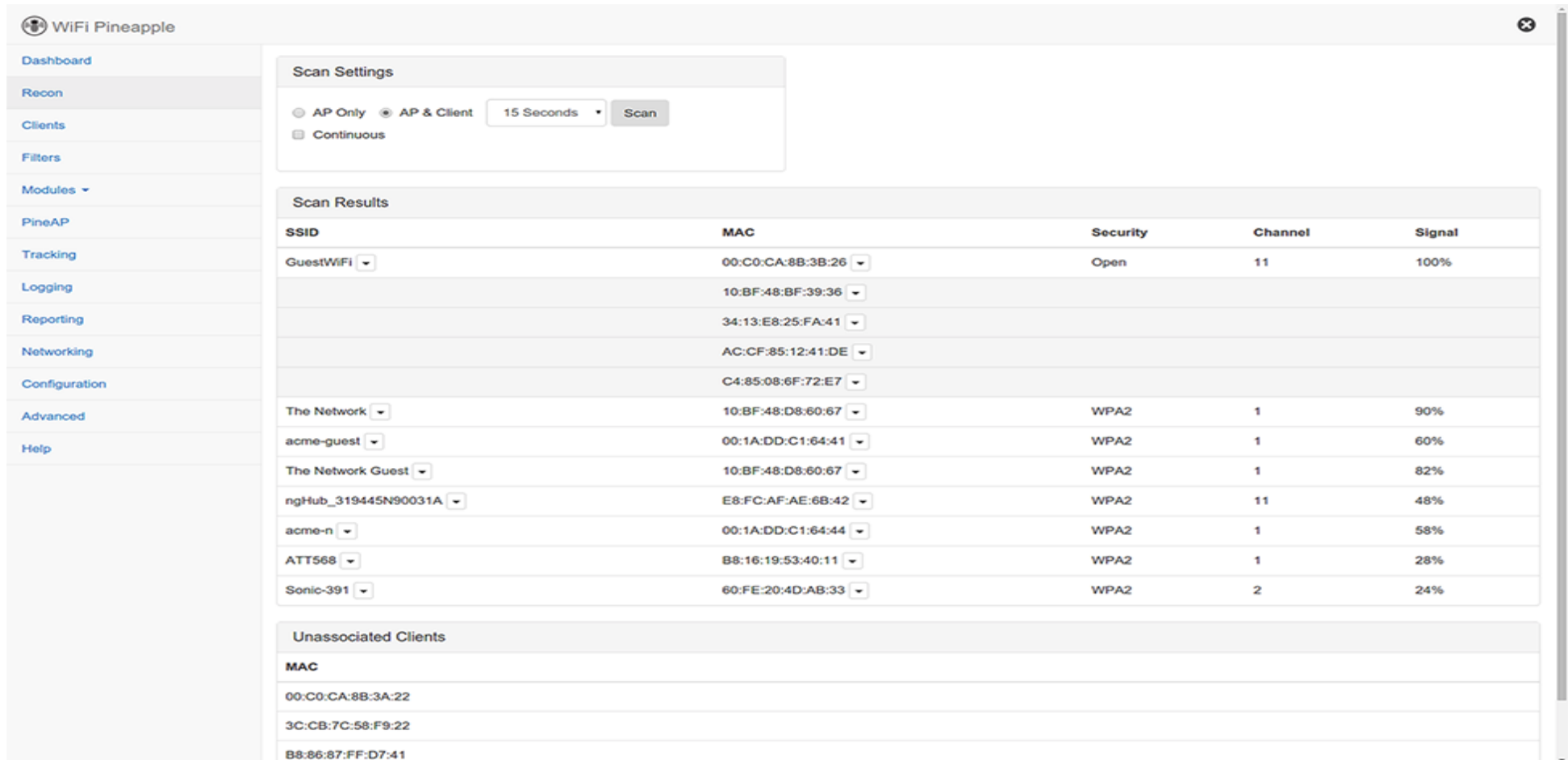
- Can be used over SSH or via a web interface



Hak5 Essentials Field Kit

Wifi Pineapple - Deployment

- Scans and attacks can be run from the GUI



The screenshot displays the WiFi Pineapple web interface. On the left is a navigation sidebar with menu items: Dashboard, Recon, Clients, Filters, Modules, PineAP, Tracking, Logging, Reporting, Networking, Configuration, Advanced, and Help. The main content area is divided into three sections:

- Scan Settings:** Includes radio buttons for 'AP Only' and 'AP & Client' (selected), a '15 Seconds' dropdown menu, and a 'Scan' button. There is also a checkbox for 'Continuous'.
- Scan Results:** A table with columns for SSID, MAC, Security, Channel, and Signal. It lists various detected networks and their associated MAC addresses and security protocols.
- Unassociated Clients:** A list of MAC addresses for clients that are not currently associated with any network.

SSID	MAC	Security	Channel	Signal
GuestWiFi	00:C0:CA:8B:3B:26	Open	11	100%
	10:BF:48:BF:39:36			
	34:13:E8:25:FA:41			
	AC:CF:85:12:41:DE			
	C4:85:08:6F:72:E7			
The Network	10:BF:48:D8:60:67	WPA2	1	90%
acme-guest	00:1A:DD:C1:64:41	WPA2	1	60%
The Network Guest	10:BF:48:D8:60:67	WPA2	1	82%
ngHub_319445N90031A	E8:FC:AF:AE:6B:42	WPA2	11	48%
acme-n	00:1A:DD:C1:64:44	WPA2	1	58%
ATT568	B8:16:19:53:40:11	WPA2	1	28%
Sonic-391	60:FE:20:4D:AB:33	WPA2	2	24%

MAC
00:C0:CA:8B:3A:22
3C:CB:7C:58:F9:22
B8:86:87:FF:D7:41

Hak5 Essentials Field Kit

Wifi Pineapple - Deployment

- Filters can be set up

The screenshot displays the configuration interface for a Wifi Pineapple device. At the top, a MAC address `9C:D9:17:6A:E0:CA` is shown. Below this, there are three main sections for configuring filters:

- PineAP Filter:** Includes buttons for "Add MAC" and "Remove MAC".
- PineAP Tracking:** Includes buttons for "Add MAC" and "Remove MAC".
- Deauth Client:** Features a "Deauth Multiplier" dropdown menu set to "1" and a "Deauth" button.

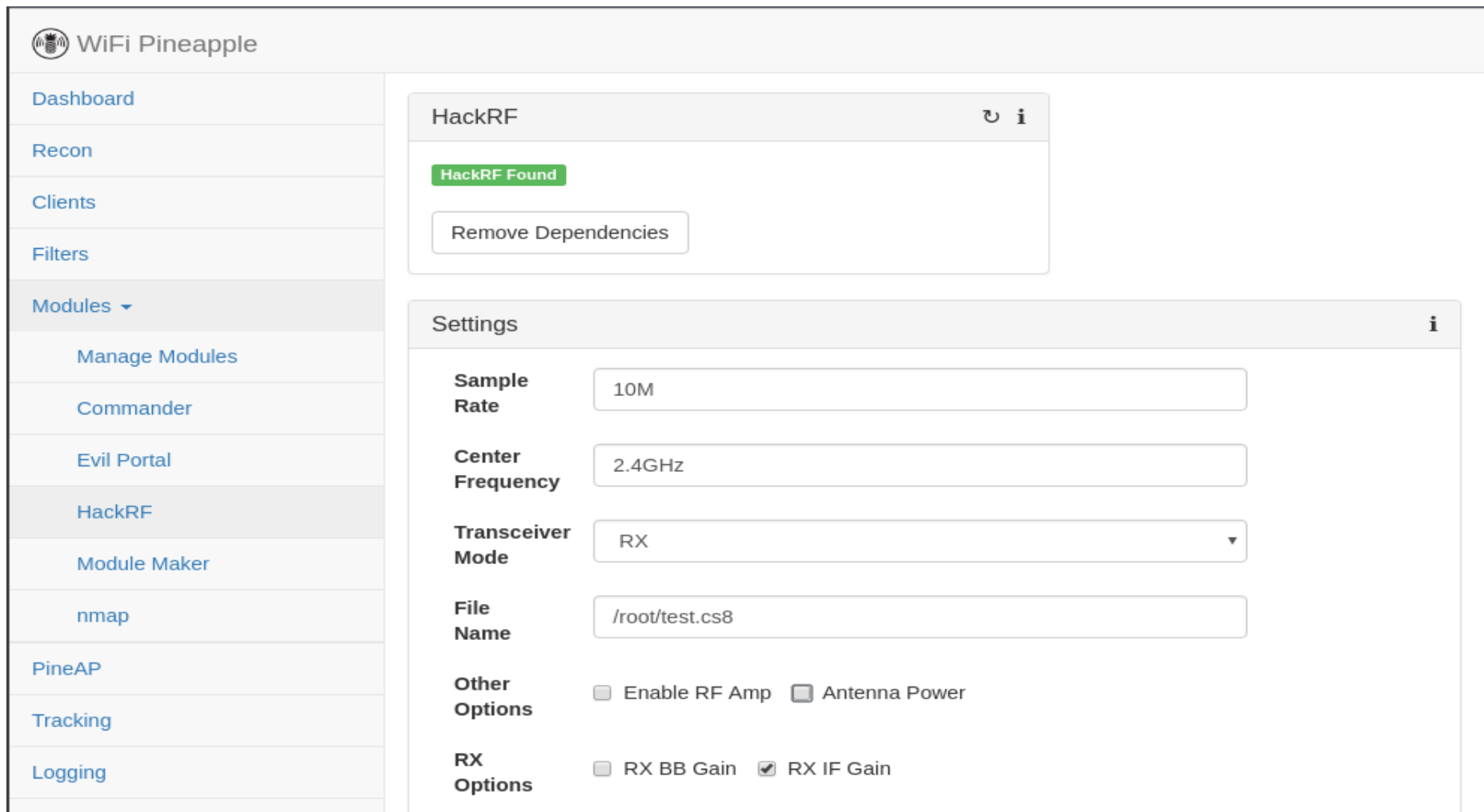
On the right side, there are two panels for advanced filtering:

- Client Filtering:** Has a "Deny Mode" switch and a list of MAC addresses: `9C:D9:17:6A:E0:CA`, `A4:34:D9:3F:5C:7D`, `AC:D1:B8:EE:77:8D`, `B4:52:7E:62:6C:4D`, `B4:52:7E:62:6C:4D`, and `EC:1F:72:83:12:88`. It includes "Add" and "Remove" buttons at the bottom.
- SSID Filtering:** Has a "Deny Mode" switch and an empty list area. It includes "Add" and "Remove" buttons at the bottom.

Hak5 Essentials Field Kit

Wifi Pineapple - Deployment

- Tools are installed as modules



The screenshot displays the WiFi Pineapple web interface. On the left is a navigation sidebar with the following menu items: Dashboard, Recon, Clients, Filters, Modules (with a dropdown arrow), Manage Modules, Commander, Evil Portal, HackRF (highlighted), Module Maker, nmap, PineAP, Tracking, and Logging. The main content area is divided into two panels. The top panel, titled 'HackRF', shows a green status message 'HackRF Found' and a 'Remove Dependencies' button. The bottom panel, titled 'Settings', contains the following configuration options: 'Sample Rate' set to '10M', 'Center Frequency' set to '2.4GHz', 'Transceiver Mode' set to 'RX' (with a dropdown arrow), 'File Name' set to '/root/test.cs8', 'Other Options' with 'Enable RF Amp' and 'Antenna Power' both unchecked, and 'RX Options' with 'RX BB Gain' unchecked and 'RX IF Gain' checked.

Hak5 Essentials Field Kit

Wifi Pineapple - PineAP

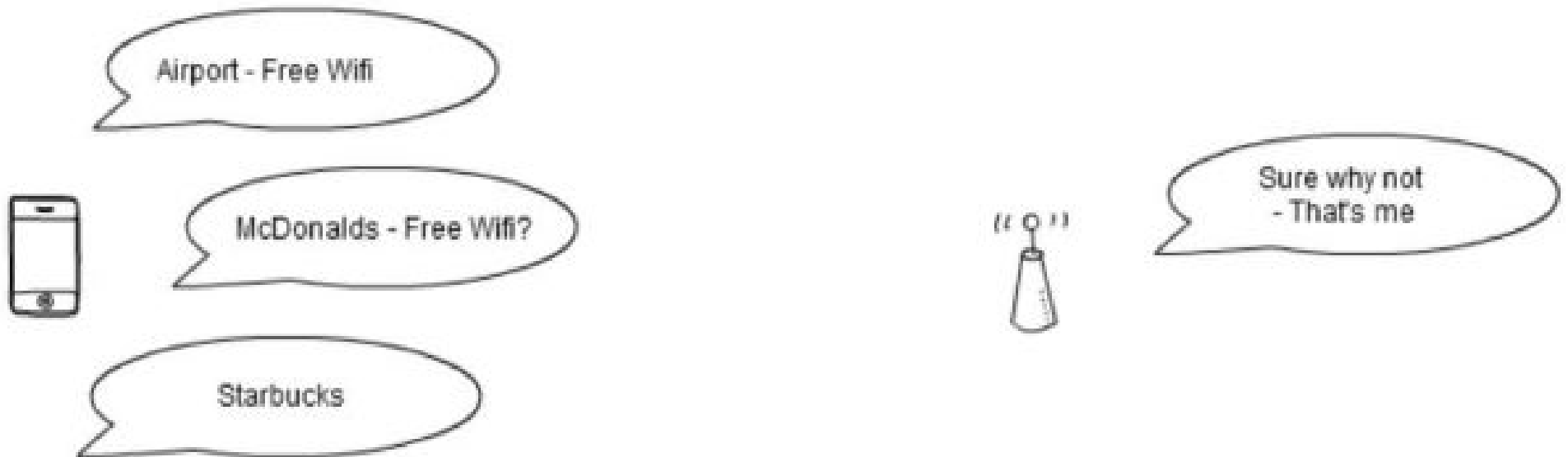
- Tool for deploying rogue access points

The screenshot displays the WiFi Pineapple web interface. On the left is a navigation sidebar with the following menu items: Dashboard, Recon, Clients, Filters, Modules (with a dropdown arrow), PineAP (highlighted), Tracking, Logging, Reporting, Networking, Configuration, Advanced, and Help. The main content area is divided into two panels. The left panel, titled 'Configuration', contains several settings: three checked checkboxes for 'Allow Associations', 'Log Probes', and 'Log Associations'; a 'PineAP Daemon: Enabled' status with a 'Switch' button; three checked checkboxes for 'Capture SSIDs to Pool', 'Beacon Response', and 'Broadcast SSID Pool'; a 'Beacon Response Interval' dropdown set to 'Normal'; a 'Broadcast SSID Pool Interval' dropdown set to 'Normal'; a 'Source MAC' field with the value '00:C0:CA:8B:3A:XX'; and a 'Target MAC' field with the value 'FF:FF:FF:FF:FF:FF'. A 'Save PineAP Settings' button is located at the bottom of this panel. The right panel, titled 'SSID Pool', features a 'Refresh' button and a scrollable list of SSIDs: GuestWiFi, The Network, acme-guest, Concourse-B, Free WiFi, University Open, acme-floor3, Tenant 201, default, FreeWifi, mobileAP, wireless, cablewifi, Home, and no_ssid. Below the list are 'Add' and 'Remove' buttons.

Hak5 Essentials Field Kit

Wifi Pineapple - PineAP

- Listens for and responds to beacon requests



Hak5 Essentials Field Kit

Wifi Pineapple - PineAP

- Observed SSIDs get added to a broadcast pool

The screenshot displays the WiFi Pineapple web interface. On the left is a navigation sidebar with the following menu items: Dashboard, Recon, Clients, Filters, Modules (expanded), PineAP (selected), Tracking, Logging, Reporting, Networking, Configuration, Advanced, and Help. The main content area is divided into two panels. The left panel, titled 'Configuration', contains several settings: 'Allow Associations', 'Log Probes', and 'Log Associations' are all checked. The 'PineAP Daemon' is set to 'Enabled' with a 'Switch' button. Below these are three checked options: 'Capture SSIDs to Pool', 'Beacon Response', and 'Broadcast SSID Pool'. The 'Beacon Response Interval' is set to 'Normal', and the 'Broadcast SSID Pool Interval' is also set to 'Normal'. At the bottom of this panel are two input fields: 'Source MAC' with the value '00:C0:CA:8B:3A:XX' and 'Target MAC' with the value 'FF:FF:FF:FF:FF:FF'. A 'Save PineAP Settings' button is located at the bottom left of the configuration panel. The right panel, titled 'SSID Pool', features a 'Refresh' button in the top right corner. It contains a scrollable list of SSIDs: GuestWiFi, The Network, acme-guest, Concourse-B, Free WiFi, University Open, acme-floor3, Tenant 201, default, FreeWifi, mobileAP, wireless, cablewifi, Home, and no_ssid. At the bottom of this panel, there is an input field labeled 'SSID' and two buttons, 'Add' and 'Remove'.

Hak5 Essentials Field Kit

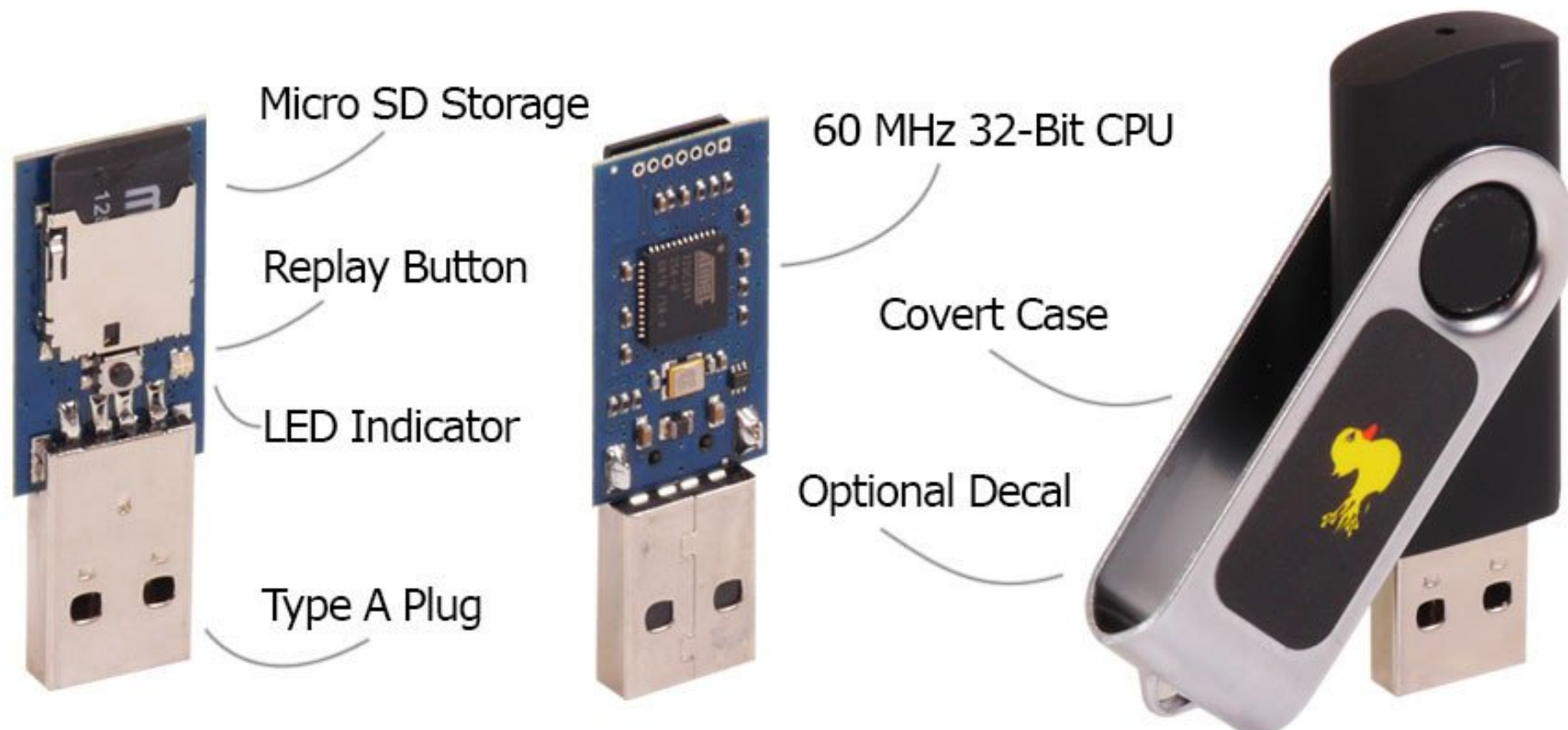
USB Rubber Ducky



Hak5 Essentials Field Kit

USB Rubber Ducky - Description

- Keystroke injection tool
- Housed in a generic USB drive case



Hak5 Essentials Field Kit

USB Rubber Ducky - Deployment

Step 1) Insert into device (PC, Phone, etc.)

Step 2) Ducky types very very fast (>1000 w/m)

Step 3) Profit!



Hak5 Essentials Field Kit

USB Rubber Ducky - Firmware

- Firmware options available:
 - Duck firmware
 - “Twin Duck”: allows storage on SD card
 - “FAT Duck”: No keystroke injection, just storage

Hak5 Essentials Field Kit

USB Rubber Ducky - Payloads

- Payloads are placed on the SD card
- “Ducky Script” is used to write the payloads

Command	Use	Command	Use
REM	Comment	ALT key	Type alt + key
DEFAULT_DELAY x or DEFAULTDELAY x	Set default delay to x	CONTROL key or CTRL key	Type control + key
DELAY x	Wait x milliseconds	REPLAY x	Replay last command n times
STRING abc	Type keys “a”, “b”, and “c”	F1, F2, F3, DELETE, CAPSLOCKS, etc.	
GUI or WINDOWS	Type windows key		
SHIFT key	Type shift + key		

Hak5 Essentials Field Kit

USB Rubber Ducky - Payloads

- Open Notepad and type “Hello World”

```
DELAY 3000
```

```
GUI r
```

```
DELAY 50
```

```
STRING notepad.exe
```

```
ENTER
```

```
DELAY 100
```

```
STRING Hello World
```

Hak5 Essentials Field Kit

USB Rubber Ducky – Use Cases

- Download and execute malware
- Open reverse shell
- Pull windows creds from memory (mimikatz)
- Bruteforce
 - Logins with a finite wordlist
 - Android screen lock pin!
- Automate non-malicious activity
- ...?

Hak5 Essentials Field Kit

USB Rubber Ducky – Caveats

- Need information on target device before creating payload
- Required physical access
- Not intelligent (no conditional statements, etc.)

Hak5 Essentials Field Kit

USB Rubber Ducky – Demo!

- “15 second Mr. Robot hack”
- Extract windows credentials with Mimikatz and send to a web server.



Hak5 Essentials Field Kit

Questions?