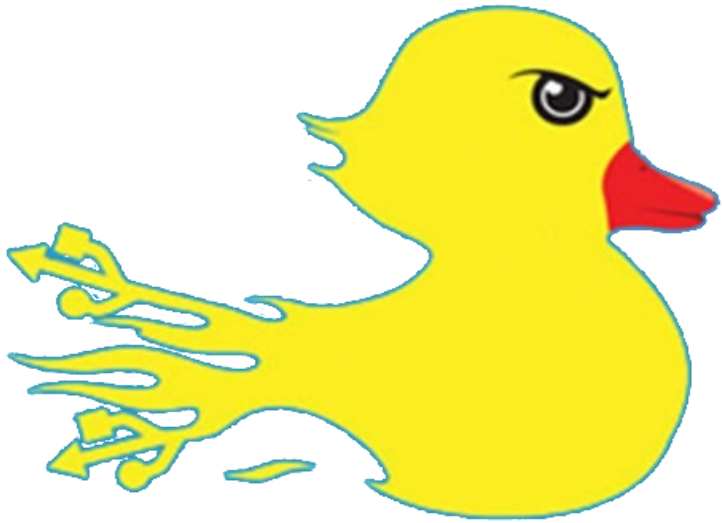


Hak5 Essentials Field Kit

CorkSec March 7th 2017

Dylan Smyth

Nimbus Centre, Cork Institute of Technology

Hak5 Essentials Field Kit

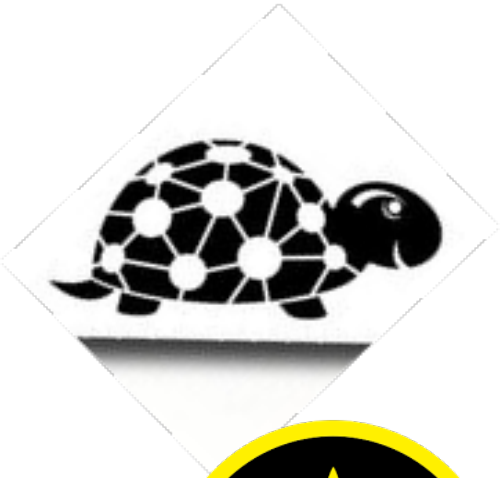
Hak5 Essentials Field Kit

TRUST YOUR TECHNOLUST

https://www.hak5.org

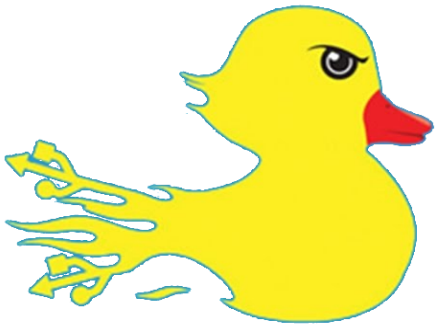
Hak5 Essentials Field Kit

- LAN Turtle



- Wifi Pineapple

- USB Rubber Ducky



Hak5 Essentials Field Kit

LAN Turtle

Hak5 Essentials Field Kit

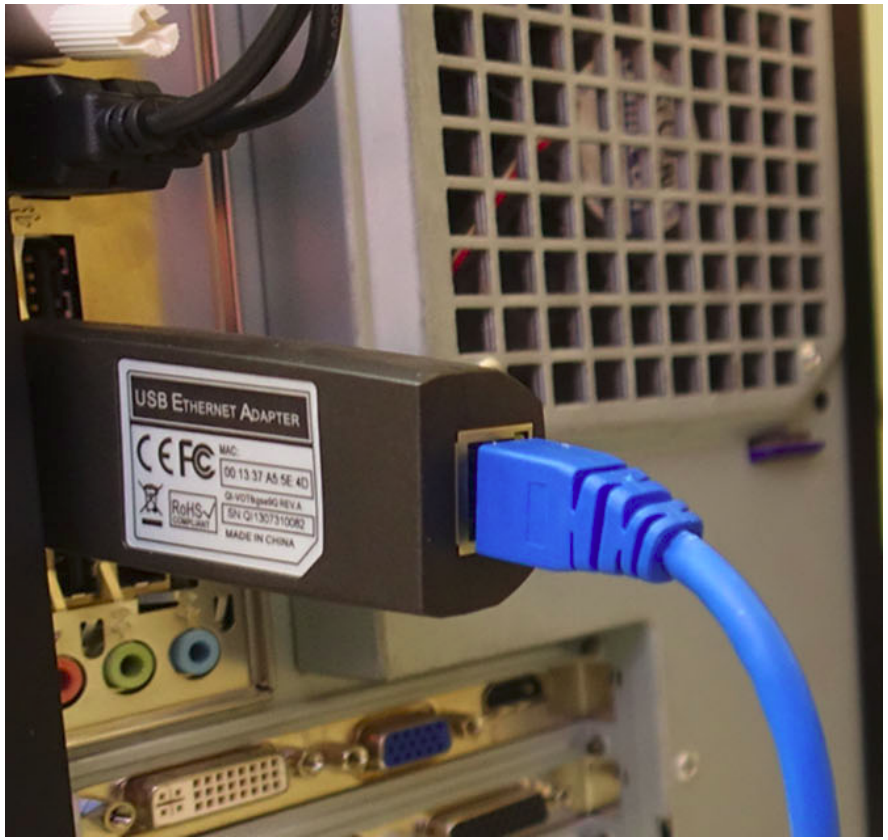
LAN Turtle - Description

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

Hak5 Essentials Field Kit

LAN Turtle - Deployment

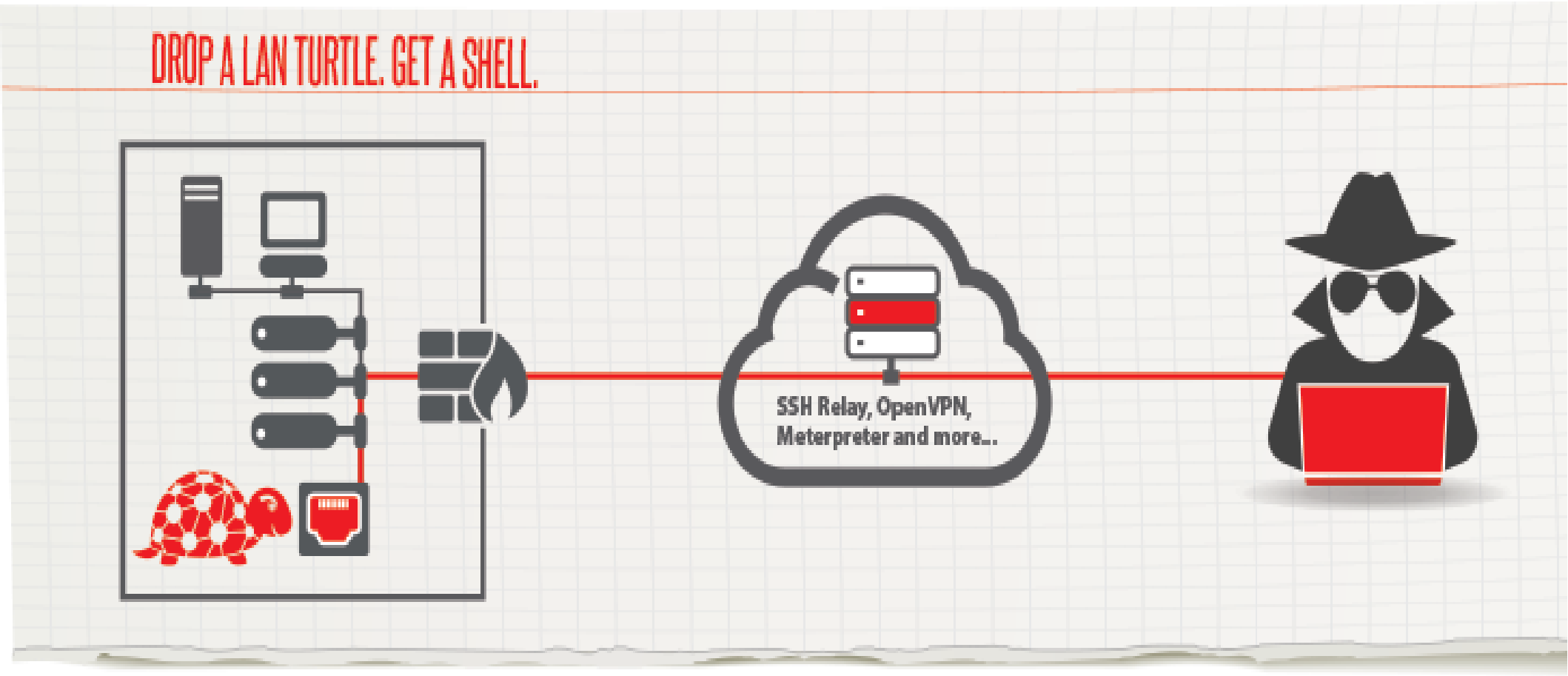
- Just needs power and a network connection



Hak5 Essentials Field Kit

LAN Turtle - Deployment

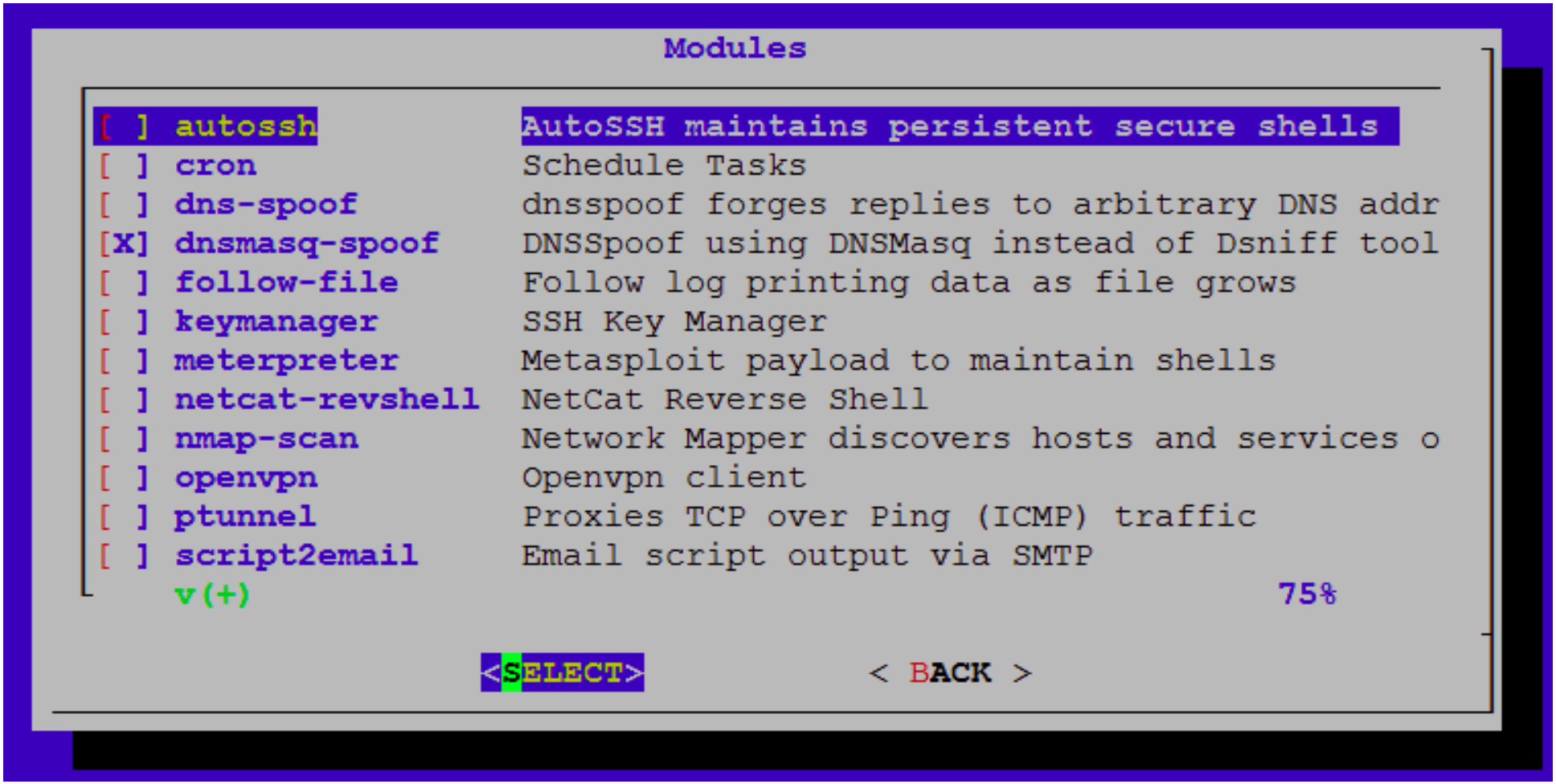
- Connect via SSH or have it connect back to you



Hak5 Essentials Field Kit

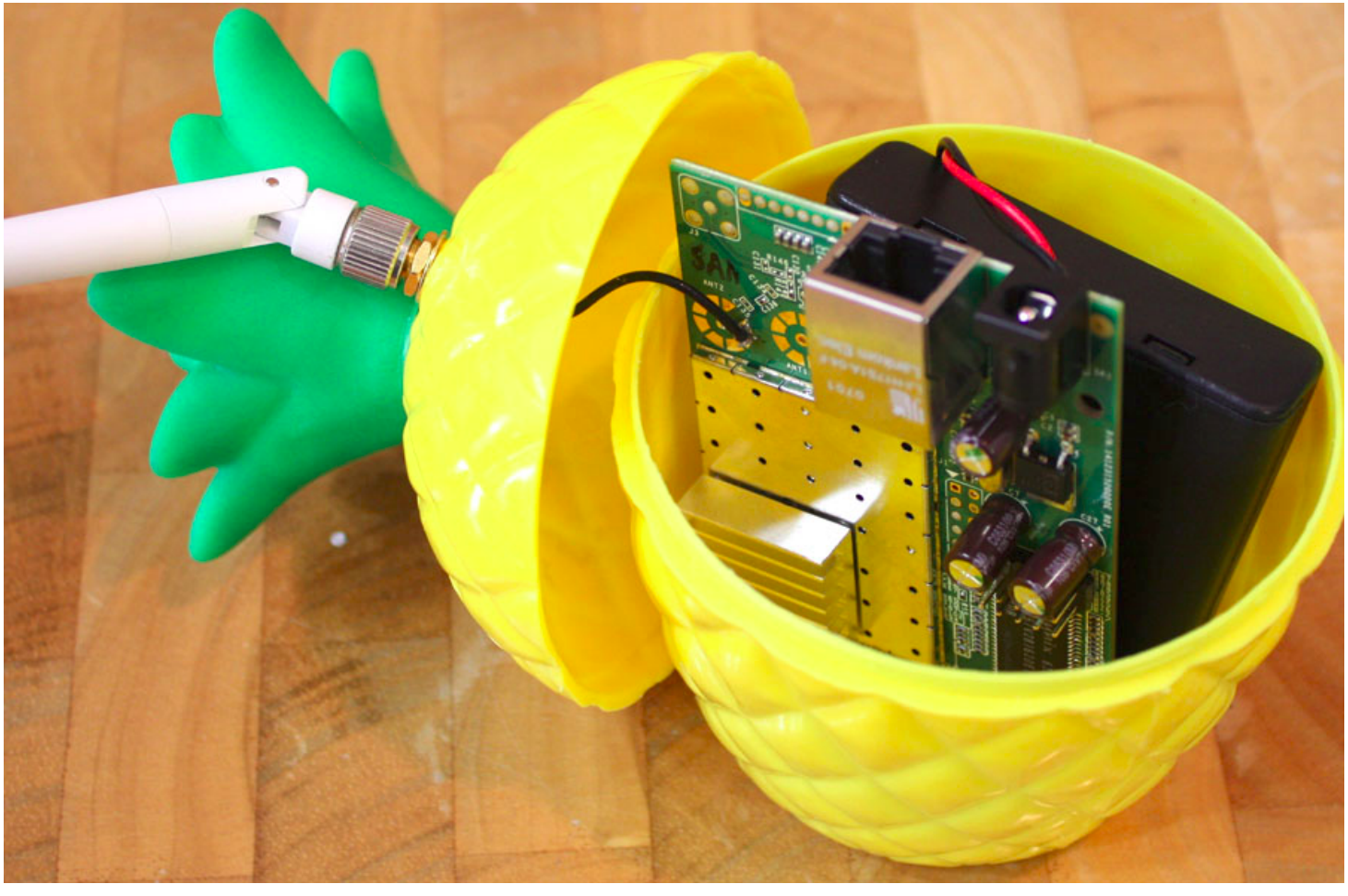
LAN Turtle - Deployment

- Run attacks against host or network



Hak5 Essentials Field Kit

Wifi Pineapple



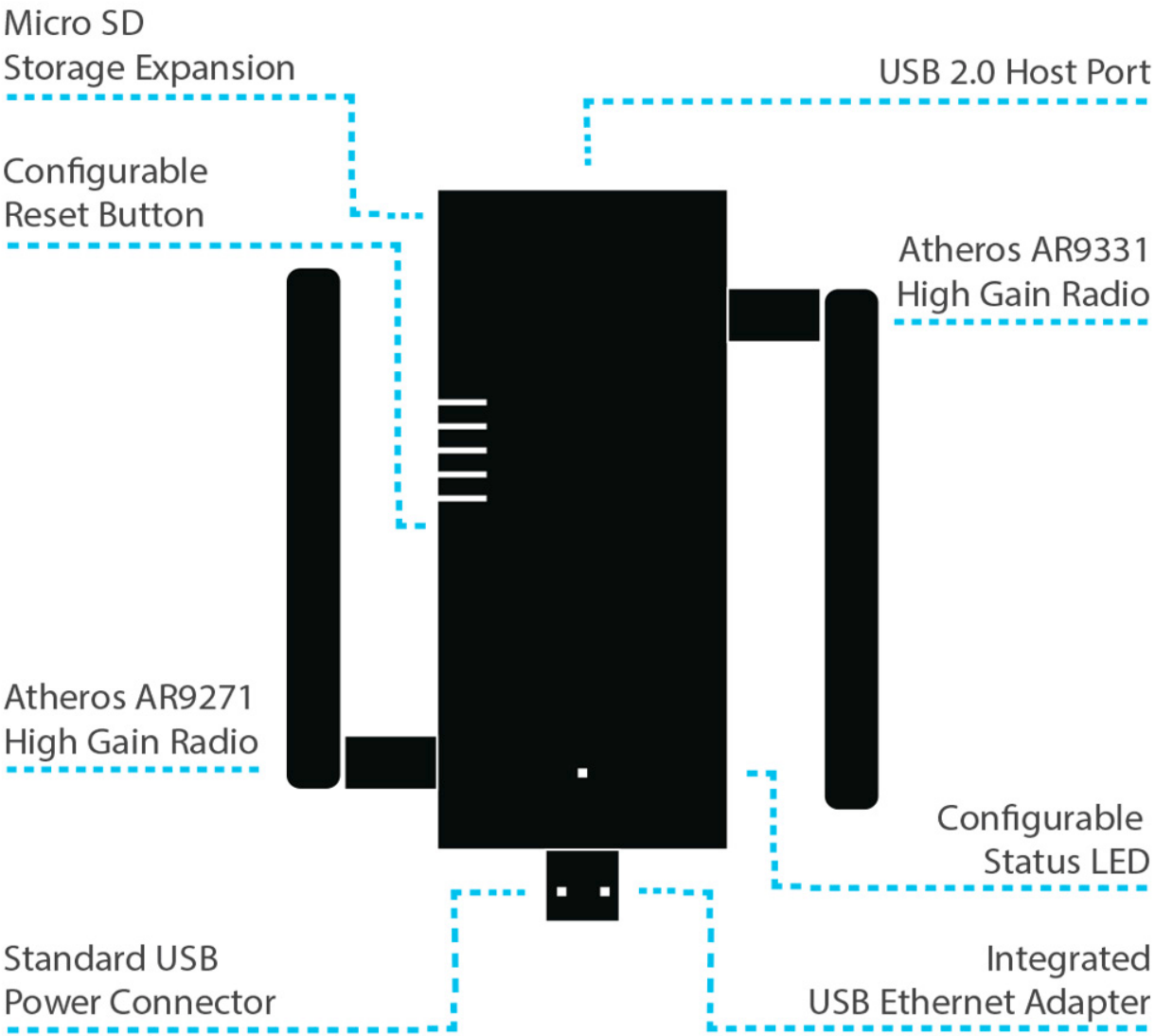
Hak5 Essentials Field Kit

Wifi Pineapple - Description

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

Hak5 Essentials Field Kit

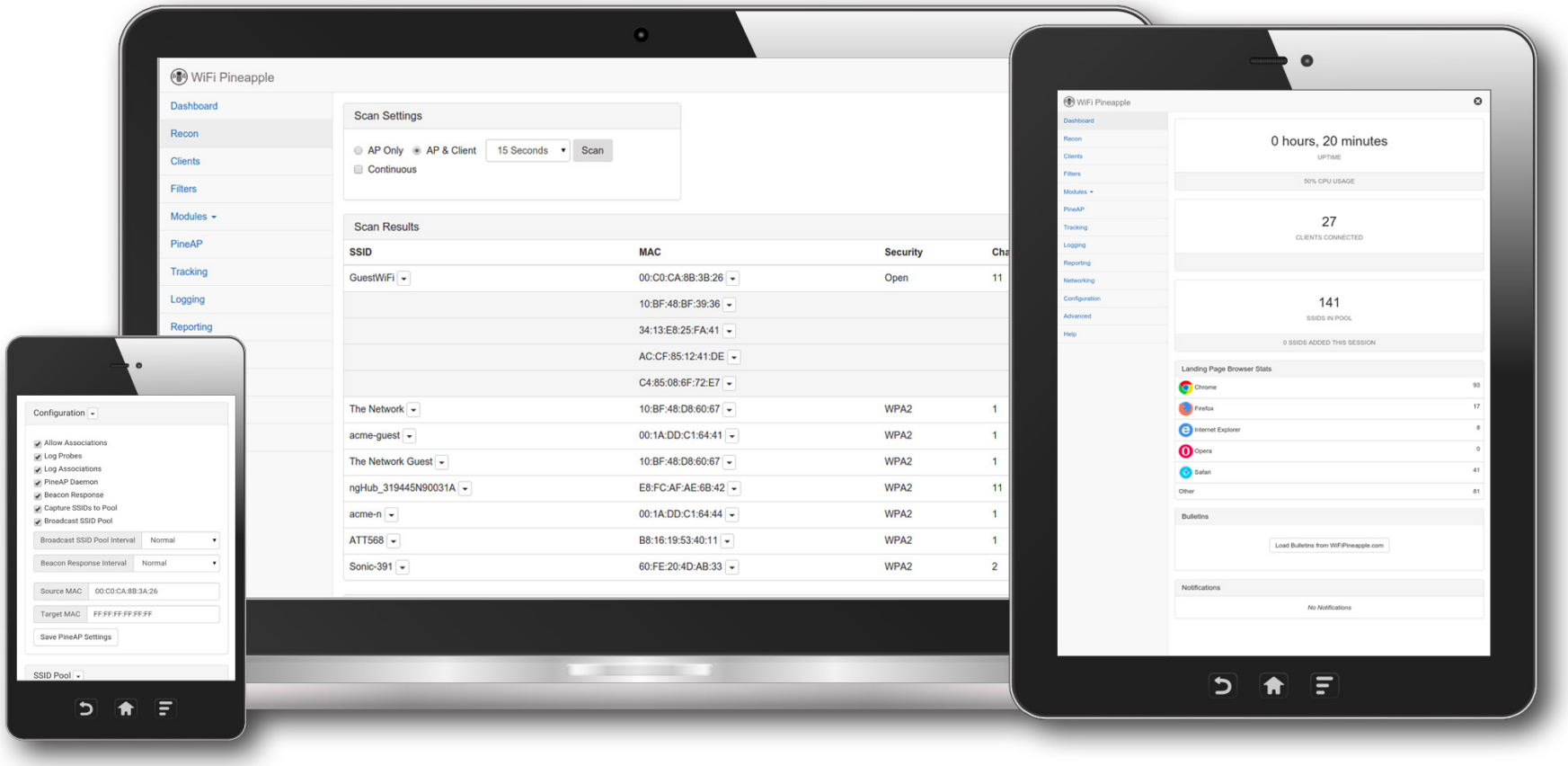
Wifi Pineapple - Description



Hak5 Essentials Field Kit

Wifi Pineapple - Deployment

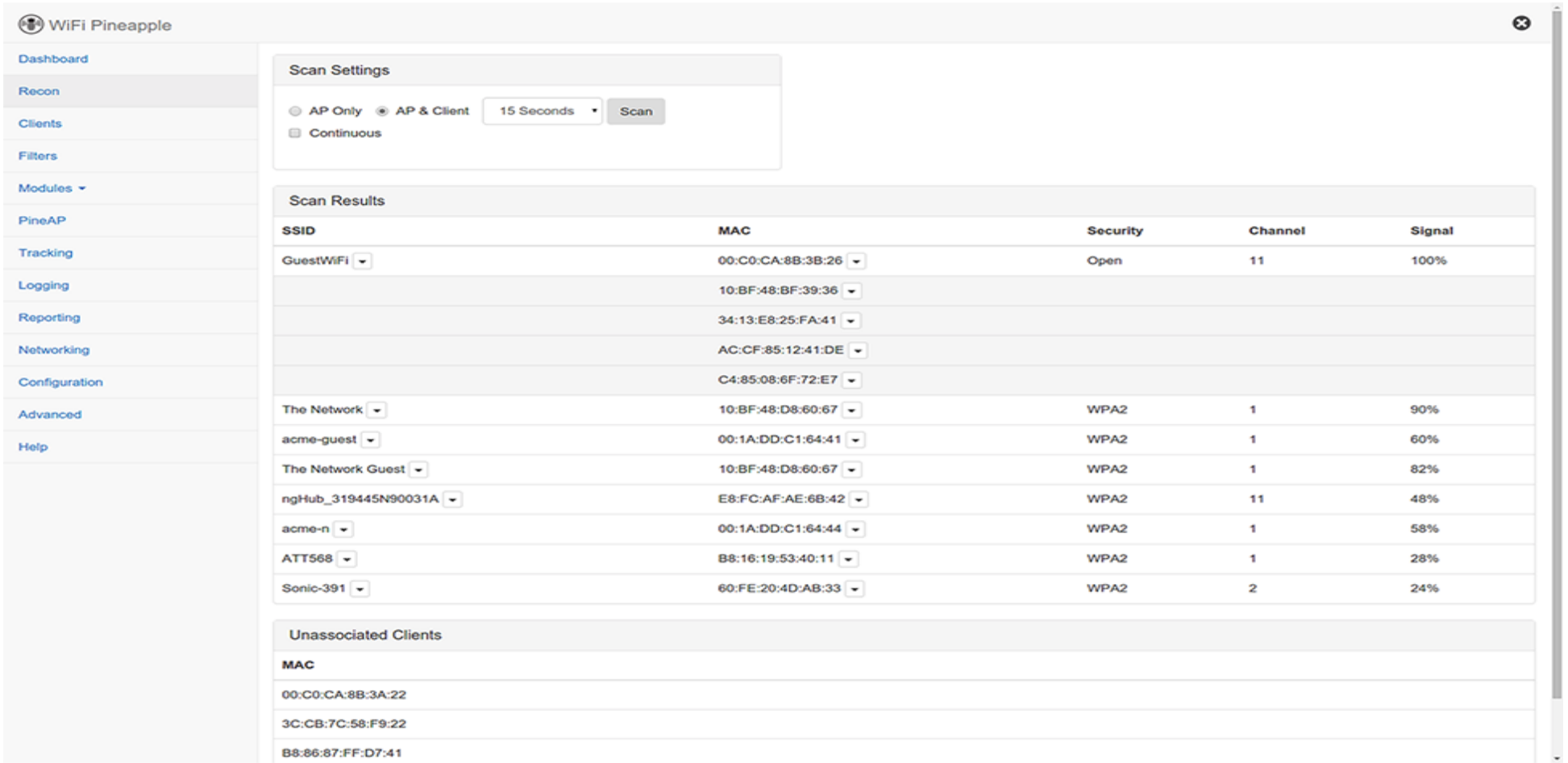
- Can be used over SSH or via a web interface



Hak5 Essentials Field Kit

Wifi Pineapple - Deployment

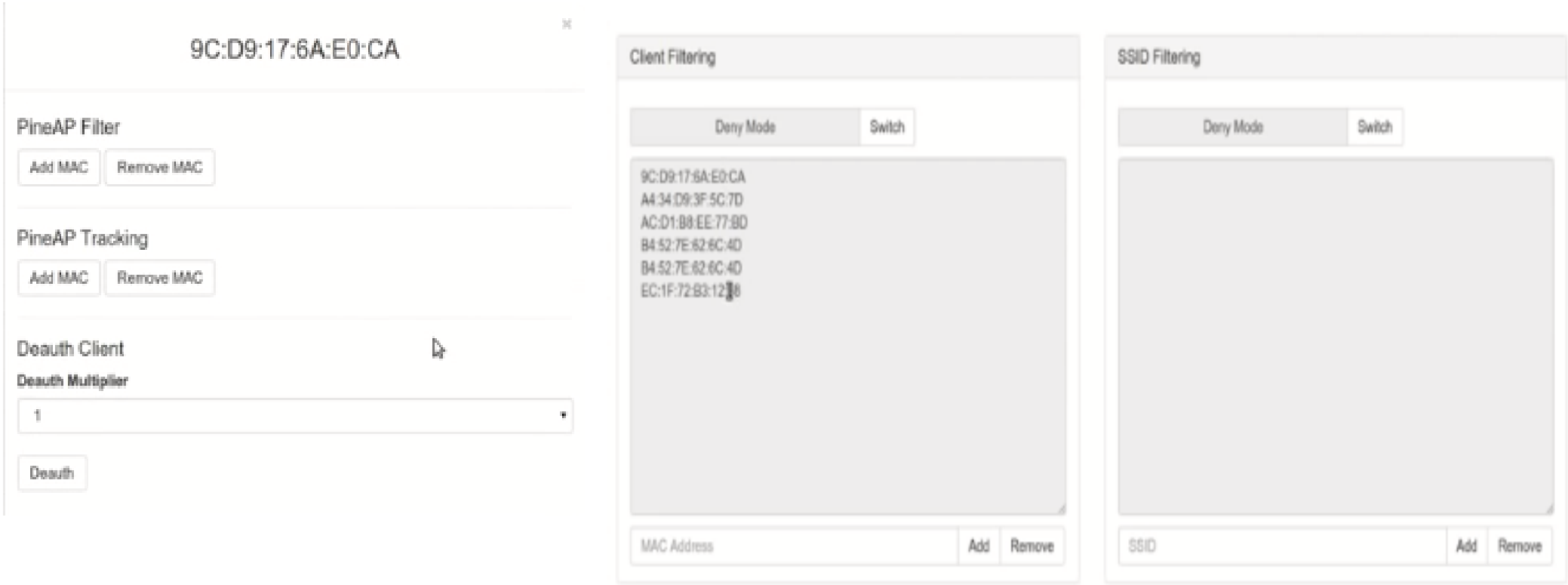
- Scans and attacks can be run from the GUI



Hak5 Essentials Field Kit

Wifi Pineapple - Deployment

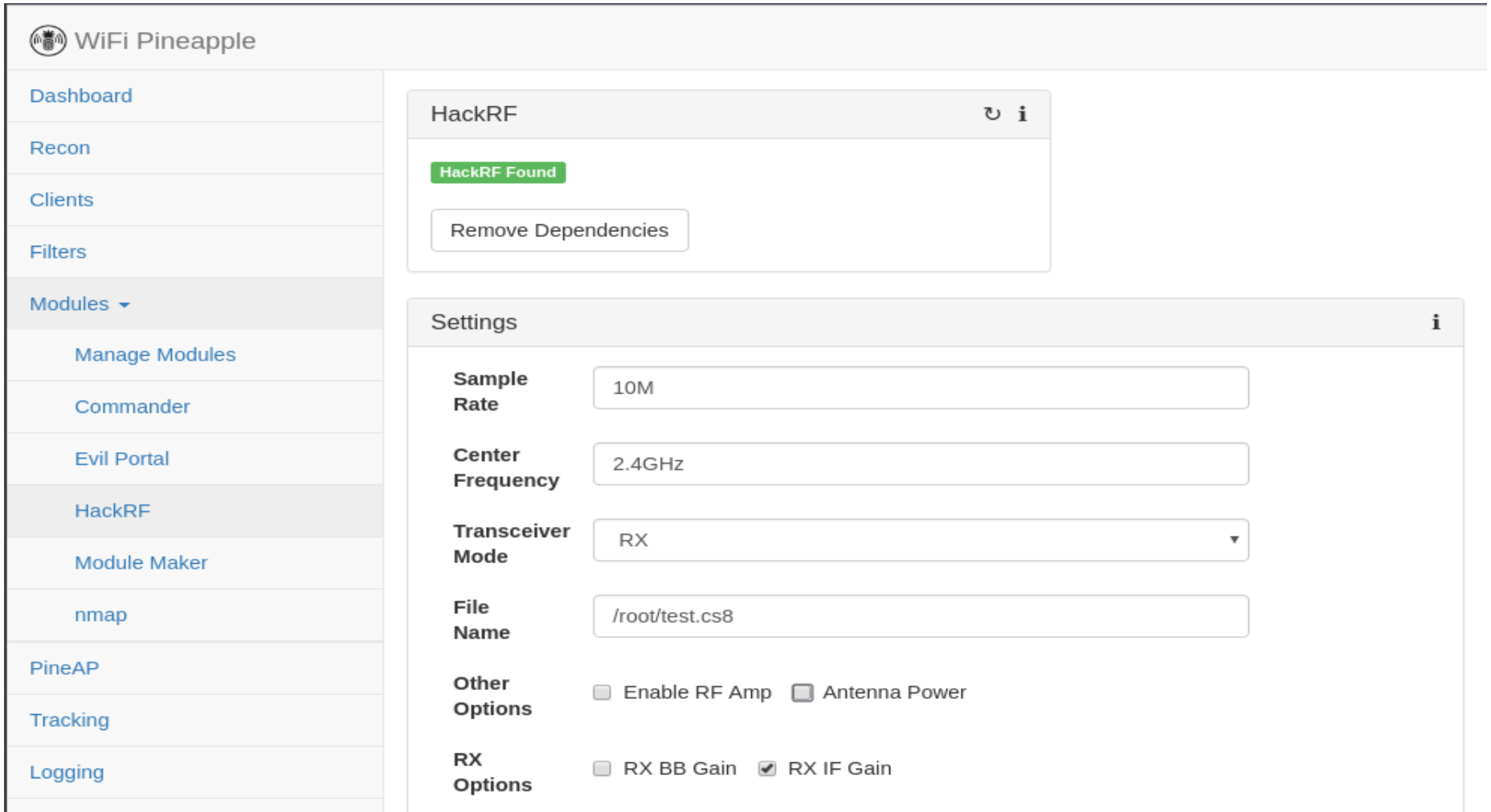
- Filters can be set up



Hak5 Essentials Field Kit

Wifi Pineapple - Deployment

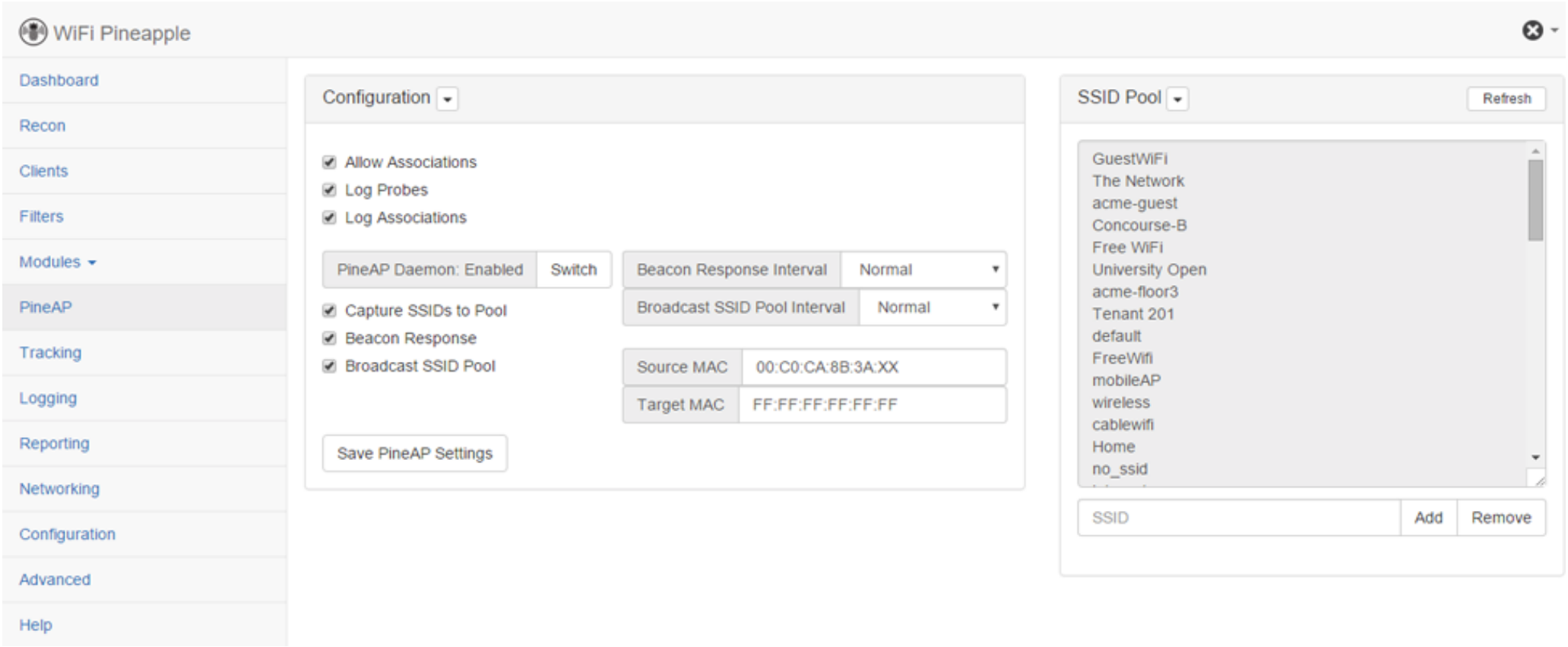
- Tools are installed as modules



Hak5 Essentials Field Kit

Wifi Pineapple - PineAP

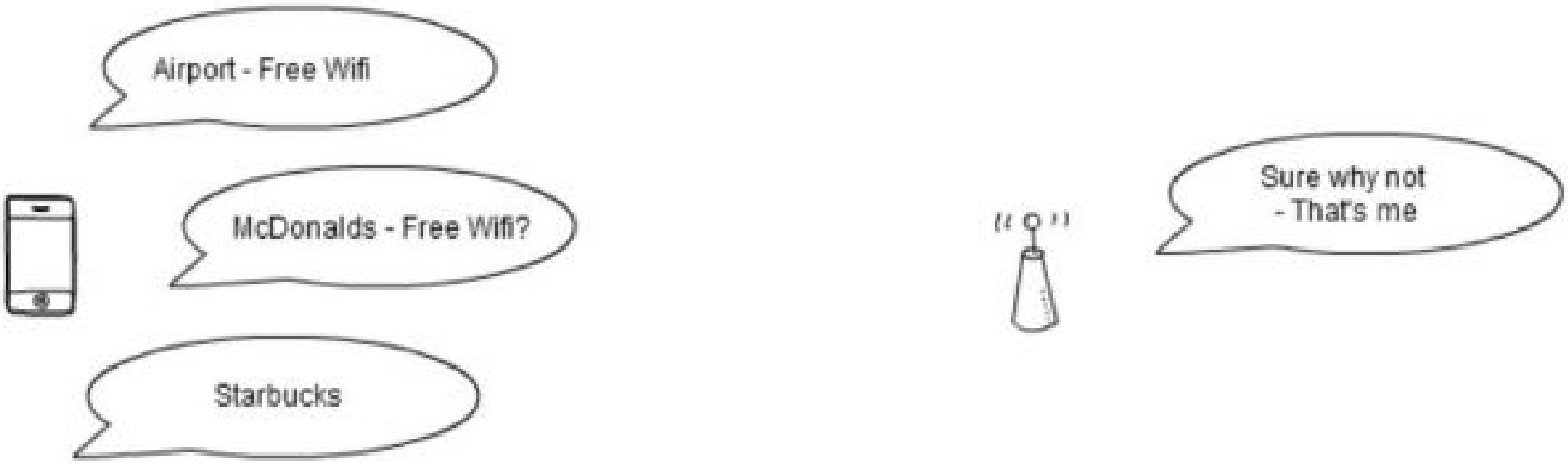
- Tool for deploying rogue access points



Hak5 Essentials Field Kit

Wifi Pineapple - PineAP

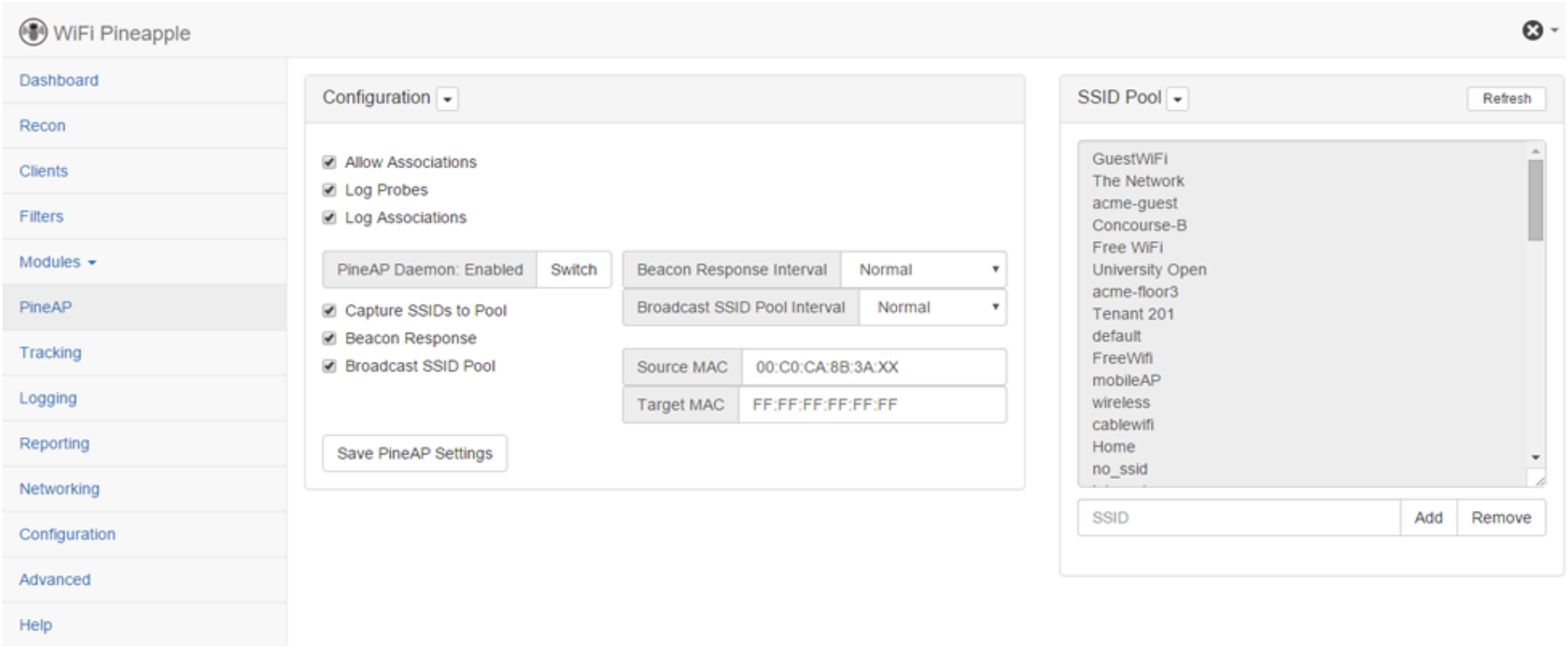
- Listens for and responds to beacon requests



Hak5 Essentials Field Kit

Wifi Pineapple - PineAP

- Observed SSIDs get added to a broadcast pool



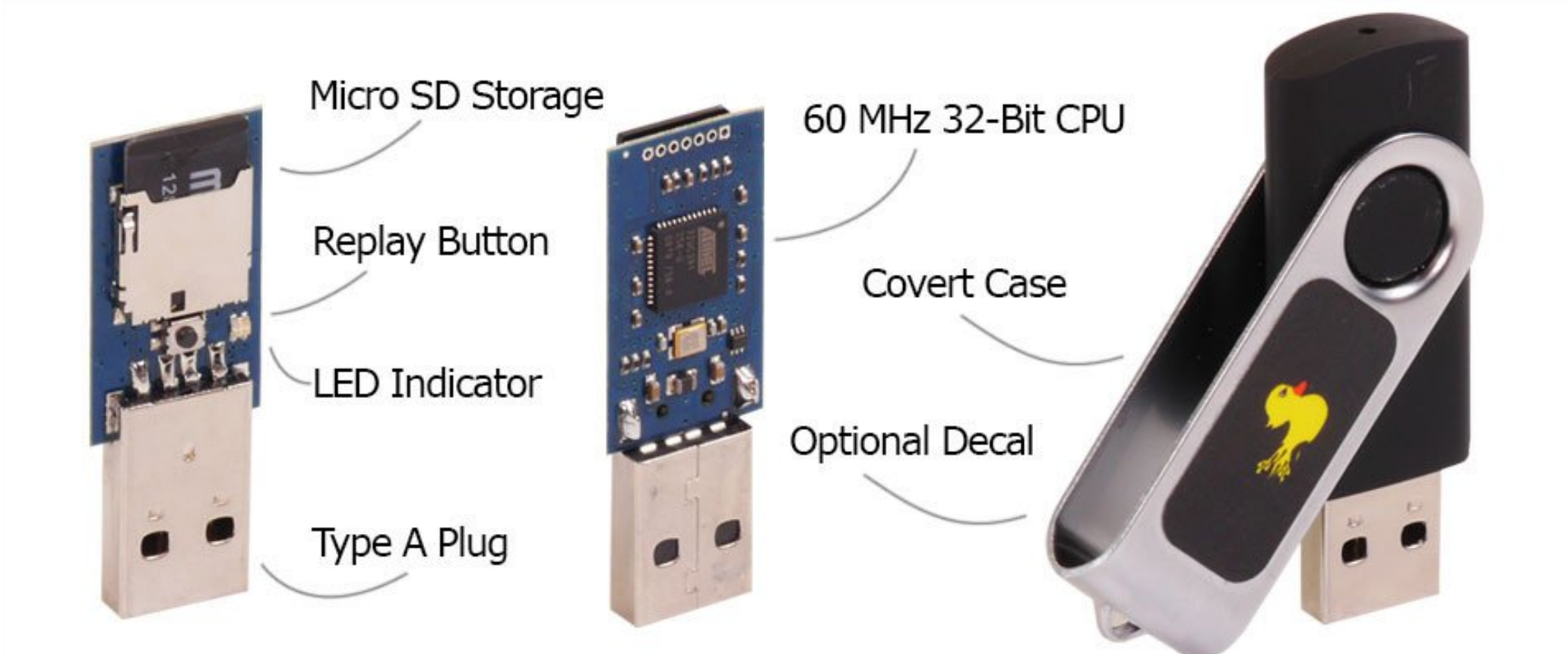
Hak5 Essentials Field Kit

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?