# A Quick and Dirty into Features and Fun with the WiFi Pineapple Mark IV

By:
Acexor

# Introduction

- Ac3 x04:@acexor/ac3x04@gmail.com
- Security Enthusiast
- Linux Enthusiast
- Privacy Enthusiast
- Active Hack Miami Member
- CTFU team member

# Disclaimer

- Ac3_X0r does not condone or promote the use of this device for criminal activity. This presentation is for educational purposes only. I am not held criminally responsible or liable for your misconduct with this device. Use Lab Networks.

# Pineapple Mark IV Hardware

- Atheros AR9331 SoC at 400 MHz
- 802.11 b/g/n 150 Mbps wireless
- 2x Ethernet, one PoE (Power-Over-Ethernet) capable
- USB 2.0 for expanded storage, WiFi Interfaces and Mobile Broadband
- Fast Linux Kernel 3.2-based Jasager firmware (built on OpenWRT)

# Features at a glance

- Stealth Man-in-the-Middle Access Point
- Mobile Broadband Modems and Android Tethering
- Manage from afar with persistent SSH tunnels
- Relay or Deauth attack with auxiliary WiFi radio
- Web-based management simplifies MITM attacks
- Easily concealed and battery powered

# How does the Pineapple Mark IV work?

# At Its Core

- Most wireless devices such as laptops, smartphones, and tablets have network software installed that automatically connects you to the access points they remember.
- This convenient feature allows you to get online at home, at work, and various other places seamlessly and without any hassle.
- When your computer turns on, your wireless card sends out probe requests. These probe requests say “is such-and-such wireless

# What is KARMA?

# KARMA in a Nutshell

- KARMA is a set of tools for assessing the security of wireless clients at multiple layers.
- Wireless sniffing tools discover clients and their preferred/trusted networks by passively listening for 802.11 Probe Request frames.
- From there, individual clients can be targeted by creating a Rogue AP for one of their probed networks (which they may join automatically) or using a custom driver that responds to probes and association requests for any SSID.

# Pineapple Modules

# URL Snarf

- URL Snarf outputs all requested URLs sniffed from HTTP traffic in CLF (Common Log Format, used by almost all web servers), suitable for post-processing with your favorite web log analysis tool (analog, wwwstat, etc.).

# SSLStrip

- SSLStrip is an SSL (Secure Socket Layer) downgrade attack.
- It fools people into using insecure HTTP connections instead of HTTPS with SSL.
- SSLStrip prevents the client from seeing secure HTTPS links. It prevents the server from forcing a secure HTTPS connection.
- SSLStrip “strips out” HTTPS links from unencrypted web pages and replaces them with HTTP links.

# DNS Spoof

- DNS spoofing (or DNS cache poisoning) is an attack, whereby data is introduced into a Domain Name System (DNS) name server's cache database, causing the name server to return an incorrect IP address, diverting traffic to another computer (the attacker).

# WiFi Jammer

- Very Simple to Use
- Using deauth with aireplay
- Whitelist / Blacklist based on regexp
- Makes Evil Twin AP attacks even eaiser

# Visual Tour

- Easy to Manage Web Interface
- Auto-start modules
- Pineapple Bar(Community Modules)
- Scripting
- WPS Button Functionality
- Pairing the Pineapple with WiFi Dongle

# Questions?

# Sources

- http://mason.gmu.edu/~msherif/isa564/projects/ssls
- http://www.wirelessdefence.org/Contents/KARMAM
- cloud.wifipineapple.com
- http://en.wikipedia.org/wiki/DNS_spoofing
- http://forums.hak5.org/index.php?/forum/71-mark-iv