Hacking WiFi with the Pineapple Tetra

Agenda

- Benefits
- Methodology
- Resources

Benefits (1 of 3)

- GUI or Terminal Driven
- Dedicated Hardware (No need to fight with Kali / Airmon-ng etc.)
- Can be Battery Powered (hide it and walk away)

Benefits (2 of 3)

- Maintain Remote Access
- Operate With a Mobile Device
- Targeted Access Points or Targeted Clients (easily stay in scope)

Benefits (3 of 3)

- Connection Sharing over Ethernet
- Community Developed Modules
- MAC Address spoofing (Persists through Pineapple Reboots)

Methodology (1 of 4)

- Discovery / Scanning
  - WPS
  - WEP
  - WPA/WPA2
  - WPA3
  - WPA-Enterprise

Methodology (2 of 4)

- Capture Handshakes
  - WPA
  - EAP (Enterprise)
- Trying to capture the 4 way handshake
  - 1) SNonce
  - 2) ANonce
  - 3) AP MAC
  - 4) Client MAC
    - Either all 4 packets, OR packet 1 and 2, OR packet 2 and 3

Methodology (3 of 4)

- Attacking Access Points

Methodology (4 of 4)

- Attacking Clients

Resources 1 of 2

Purchase Page - $100 for Nano or $200 for Tetra (Device We Demoed)

Support Page

Tetra Setup Basics

WiFi Pineapple Tetra - Linux Setup

WiFi Pineapple Wiki

Hacking Exposed Wireless 3rd Edition

Lynda.com - Ethical Hacking: Wireless Networks local library card for free access

Resources 2 of 2

Key Reinstallation Attacks - KRACK

DragonBlood White Paper

DragonBlood HomePage