Wifi Grenade

A PORTABLE RASPBERRY PI 2
MASS DEAUTH DEVICE

Tom Webster

“SAMURAILINK3”

SAMURAILINK3.COM

SAMURAILINK3@GMAIL.COM

PLUS.GOOGLE.COM/+TOMWEBSTER

@SAMURAILINK3

Disclaimer

1. I'M STANDING ON THE SHOULDERS OF GIANTS: THE HARD WORK HERE HAS BEEN DONE BY OTHER PEOPLE.

2. ONLY USE THIS ON A NETWORK YOU ARE LEGALLY ALLOWED TO ATTACK. THIS SHOULDN'T CAUSE PERMANENT DAMAGE, BUT I'M NOT BAILING YOU OUT IF YOU GET BUSTED.

3. THIS ISN'T TECHNICAL, IT'S NOT IMPRESSIVE, AT BEST IT'S A WAY TO SEE WHAT DEAUTH PACKETS DO, AT WORST THIS IS JUVENILE STUPIDITY. EITHER WAY, DON'T TAKE IT TOO SERIOUSLY AND HAVE SOME FUN.

Components

GET YOUR SHOPPING LIST TOGETHER

Hardware

- [$30] RASPBERRY PI 2
- [$6] 4GB MICRO SD CARD
- [$40] ALFA WIRELESS CARD (G/N 2W)
- [$40] ANKER 15000MAH BATTERY

Software

- ARCH LINUX ARM
- PYTHON 2
- DAN MCINERNEY'S WIFIJAMMER.PY
- SOME LIBRARIES AND TOOLS:
  - SCAPY
  - IW
  - WIRELESS_TOOLS
  - GIT

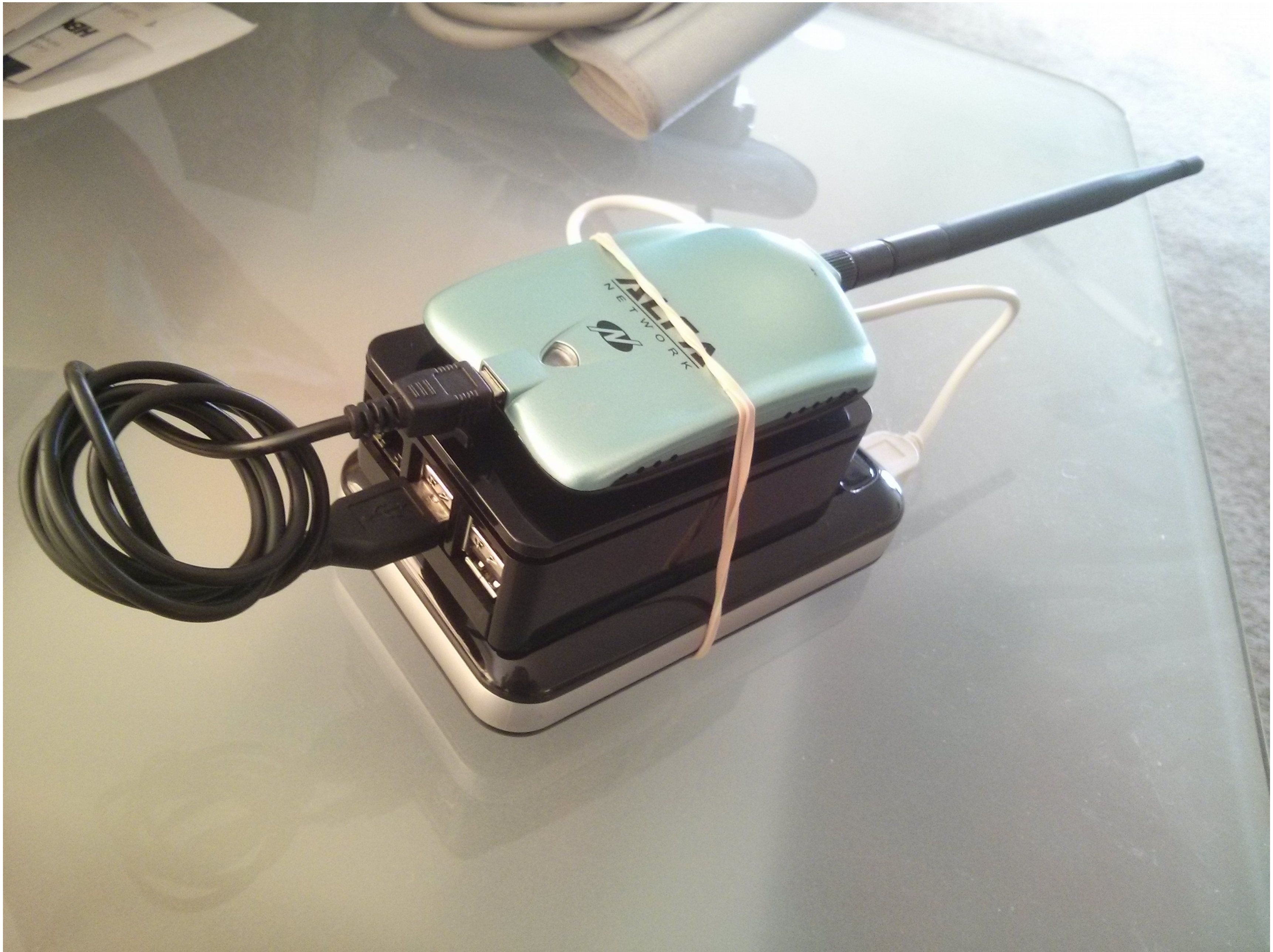
Quick How-To

- INSTALL ARCH LINUX ARM ON SD CARD
- INSTALL REQUIRED LIBRARIES AND TOOLS (SCAPY, IW, WIRELESS_TOOLS, GIT)
- CHECKOUT DAN MCINERNEY'S CODE FROM HTTPS://GITHUB.COM/DANMCINERNEY/WIFIJAMMER
- SET AUTOLOGIN
- CREATE A .BASHRC (OR .ZSHRC) WITH THE WIFIJAMMER COMMAND IN IT.
- ON BOOT, THE SYSTEM WILL LOG IN AND START THE JAMMER, NO USER INPUT REQUIRED.

- I'LL HAVE THE FULL INSTRUCTIONS AND TECHNICAL DETAILS POSTED ON MY SITE: SAMURAILINK3.COM

The Device Itself

IT'S STILL PRETTY BULKY, NEEDS SOME TRIMMING



What it does

LOTS OF DEAUTH PACKETS

- THE PI BOOTS
- THE ROOT USER IS AUTOMATICALLY LOGGED IN
- .BASHRC OR .ZSHRC WILL AUTOMATICALLY START WIFIJAMMER.PY
- THE SCRIPT FINDS THE MOST POWERFUL INTERFACE AVAILABLE AND TURNS ON MONITOR MODE
- MAKES A LIST OF ALL ACCESS POINTS IT CAN FIND
- SENDS DEAUTH PACKETS TO EVERYTHING IT CAN FIND
- ONE CAVEAT: THE SCRIPT DOESN'T WORK ON 5GHZ NETWORKS AT THE MOMENT, THE PROJECT IS STILL ACTIVE AND IF YOU'D LIKE TO FIX IT, GET TO GITHUB

THE BEST, MOST TECHNICAL EXPLANATION CAN BE FOUND HERE: HOW TO KICK EVERYONE AROUND YOU OFF WIFI WITH PYTHON

Why does this work?

AND HOW CAN WE STOP IT?

Why It Works

- WIFI MANAGEMENT FRAMES ARE NOT ENCRYPTED, MANY OF THEM CAN'T BE (WITHOUT SIGNIFICANTLY CHANGING HOW WIFI WORKS)
- "DEAUTHENTICATION IS NOT A REQUEST; IT IS A NOTIFICATION. DEAUTHENTICATION SHALL NOT BE REFUSED BY EITHER PARTY." - DEVIN AKIN
- WIRELESS SPOOFING IS EASY AND FUN!

To Stop It:

- 802.11W – PROTECTED MANAGEMENT FRAMES
  - NOT ALL MANAGEMENT FRAMES ARE PROTECTED, ONLY SOME (DEAUTH IS PROTECTED)
- SOME CUSTOM DRIVERS WILL IGNORE DEAUTH PACKETS (AND BREAK 802.11 STANDARDS), THIS ISN'T A GREAT SOLUTION (THINGS BREAK)
- ENCASE YOUR HOUSE/OFFICE IN A FARADAY CAGE

Interesting Finding

ANDROID RANDOMIZES THE MAC ADDRESS OF THE SOFT AP (WIFI TETHERING).
CHECK IT OUT: HTTPS://ANDROID.GOOGLESOURCE.COM/KERNEL/MSM/+/ANDROID-5.1.0_R0.7/DRIVERS/NET/WIRELESS/BCMDHD/DHD_LINUX.C#5353

```
#ifdef SET_RANDOM_MAC_SOFTAP
         SRANDOM32((uint)jiffies);
         rand_mac = RANDOM32();
         iovbuf[0] = (unsigned char)(vendor_oui >> 16) | 0x02;   /* locally administered bit
*/
         iovbuf[1] = (unsigned char)(vendor_oui >> 8);
         iovbuf[2] = (unsigned char)vendor_oui;
         iovbuf[3] = (unsigned char)(rand_mac & 0x0F) | 0xF0;
         iovbuf[4] = (unsigned char)(rand_mac >> 8);
         iovbuf[5] = (unsigned char)(rand_mac >> 16);
         bcm_mkiovar("cur_etheraddr", (void *)iovbuf, ETHER_ADDR_LEN, buf, sizeof(buf));
         ret = dhd_wl_ioctl_cmd(dhd, WLC_SET_VAR, buf, sizeof(buf), TRUE, 0);
         if (ret < 0) {
              DHD_ERROR(("%s: can't set MAC address , error=%d\n", __FUNCTION__, ret));
         } else
              memcpy(dhd->mac.octet, iovbuf, ETHER_ADDR_LEN);
#endif /* SET_RANDOM_MAC_SOFTAP */
```

THIS HAS BEEN MISTAKEN AS A BUG SEVERAL TIMES BY END USERS

Credit

WHERE IT'S DUE

DAN MCINERNEY DID THE HARD WORK OF MAKING THE WIFIJAMMER SCRIPT. HE DOES SOME PRETTY FANTASTIC WORK, GO CHECK OUT HIS STUFF.

ALFA NETWORKS FOR AN AWESOME WIRELESS CARD. EVEN WITHOUT THE INFOSEC TESTING BENEFITS, THEY MAKE A GREAT GENERAL USE CASE WIFI CARD.

ANKER FOR A NICELY BUILT PHONE CHARGER. I USE THIS THING TO DEATH.

THE RASPBERRY PI FOUNDATION FOR MAKING THE PI 2. THIS IS A HUGE IMPROVEMENT OVER THE ORIGINAL, AND AT THE SAME PRICE AS THE ORIGINAL.

Thanks!