# Adventures in IoT Hacking

# Software Notes

1. Download the log file “USB\_TTL\_Boot\_JEN.log” to your linux machine
   1. Capture the admin hash in “hashfile.txt” and the dropbear hash in “dropbearhash.txt”
   2. We can run hashcat to crack the hashes in the file
   3. hashcat -m 5000 hashfile.txt /usr/share/wordlists/rockyou.txt
   4. hashcat -m 0 dropbearhash.txt /usr/share/wordlists/rockyou.txt
2. Download the firmware binary from class github to your Linux machine

<https://github.com/shaq-qa/Iot-adventure>

it is called “TL-WR841N(US)\_V14\_231119.zip

unzip it. There should be 2 pdf’s and one binary

unzip TL-WR841N(US)\_V14\_231119.zip

1. We will be using:
   1. binwalk
   2. sasquatch
   3. dd
   4. ghidra

If you do not have these, they can be installed on Kali with

sudo apt install <name>

Except for sasquatch! When you run binwalk, sasquatch errors will appear. To fix these, see below

**Directions for sasquatch installation**

sudo apt-get install zlib1g-dev liblzma-dev liblzo2-dev

cd /opt

sudo git clone <https://github.com/devttys0/sasquatch>

cd /opt/sasquatch

sudo ./build.sh (this will fail)

cd patches

wget <https://github.com/devttys0/sasquatch/files/7776843/M1-Kali.patch.txt>

sudo patch patch0.txt M1-Kali.patch.txt

cd ..

./build.sh

Now binwalk will work without sasquatch errors.