My Hacking Roadmap

**What I’ve learned and why I think it’s important**

I began looking into reverse engineering and hacking in March ’24. I wanted to work on practical engineering problems as college work largely felt futile and impractical. I wanted to bridge my knowledge of software and hardware and though Arduino has always been useful in this regard, I was more interested in higher level systems.

**Radio:**

I began looking into radio hacking, buying a Flipper Zero (Pen testing gadget), to explore various radio protocols and their security measures. Shortly after I bought an SDR & antenna. I did some basic radio hobbyist stuff, listening to various frequencies and playing around with GQRX.

**Wi-Fi:**

I purchased an ESP-32 for the Flipper Zero, allowing me to perform Wi-Fi attacks on my home network. Mostly script kiddie stuff, getting myself familiar with common payloads and how they work.

I downloaded Wireshark, a free software that I used for packet sniffing. I need to go through this in more depth to understand the intercepted data better.

**Raspberry Pi:**

After purchasing a Raspberry Pi 5, I wanted to explore network hacking. I started by writing an ARM version of Kali to an SD card, set up SSH and accessed it remotely. Setting up my own network, setting up a cloud storage, penetration testing targeted at the pi; these are some ideas I have for this.

**Linux:**

Work in progress… I’m currently using OccupyTheWeb’s book “Linux Basics for Hackers”

I’m going to need to buy a dedicated laptop for this work. For now I’m using the Pi.

**Physical Entry:**

I became interested in physical pen testing after watching videos from a hacking expo. I hadn’t really considered lock picking as hacking previously. I found this very intriguing and bought a beginner lock pick set online.

With some time, the practice locks were easy. So far I’ve been able to pick Jamie’s back door, my front door, padlocks and others. This has become a side hobby.

**Projects**

**Project 1 -** **Linux Basics**. Exploring Linux using a Raspberry Pi 5 running a 64 bit img of Kali Linux. (ARM took a while to find on GItHub)

Spent time learning some basic commands, learning about Linux and other OS with ‘Linux Basics for Hackers’ by OTW

**Project 2 -** **Flipper Zero Firmware**. My next project, spanning over a long period involved testing different firmware options for the Flipper. I landed on Momentum, Unleashed and the original Flipper firmware. Between the three I find momentum to be the easiest to work with/ least prone to crashing. Next, I’m going to write some applications!

**Project 3 -** **Software Defined Radio.** The next piece of hardware I found to waste money on was an SDR. This allowed me to listen to a wide range of frequencies being transmitted from nearby. My antenna is not of good quality so I struggled to filter out noise on certain frequencies, (assumption being large distance between us or weak signal at output). I wanted to listen to police/airport frequencies but couldn’t and gave up pretty quickly.

**Project 4 - Packet Sniffing with WireShark.** Next I wanted to explore network protocols and how hackers intercept and interpret data. To do this I used WireShark.

**Project 5 - Using Nmap in Kali Linux.** For my first project using Kali Linux payloads, I wanted to explore Nmap. It’s known for it’s utility and being relatively beginner friendly. I was able to map my network and identify different devices based on port number, assigned IP addresses etc. More contained in the project brief.

**Project 6 - Controlling Pi with SSH.** Pretty self-explanatory, I wanted to get used to headless systems and controlling them from the command line. To do this I used some basic linux commands on the Pi to verify IP address, username and password. After I had gained access I was able to create, delete and write to files for testing. Next will be setting up a NAS using SSH.

**Project 7 - Soldering an LED display.**  I wanted to build on my lacklustre soldering skills by doing a project. I landed on soldering LEDs in parallel in the shape of a heart. This went well and I learned some important lessons about soldering. You need flux. Despite this, the heart has held up and 6 months later it shines brightly.

**Project 8 - Building a Raspberry Pi NAS.** This project is ongoing. I wanted to create a headless system that plugs directly into my router via ethernet and can be used for remote storage by my devices. Currently, the raspberry pi and SSH are functioning but when installing NAS software remotely the connection timed out. This is likely a Wi-Fi issue on the Razz Pi side, will test using a physical connection next.