# Breaking In

An Introduction to Device Security Testing

Start Presentation

# ABOUT THE SPEAKER

Currently in charge of Product Security Incident Response and the Security Operations Centre for Panasonic North America

- WRCCDC Red Team Member (for over a decade)
- DEFCON Goon
- BugCrowd / Synack / H1 Alum
- Leads up Product Security Incident Response for Panasonic North America
- Twitter: @g33kspeed

## RULES OF THE ROAD

Before we ju,mp in to the fun stuff, lets go over some basic ground rules

## WHAT YOU ARE GOING TO NEED

Building out your toolbox

## GETTING STARTED

How do we select our first target, what do we look for

## WHERE TO GO NEXT

# RULES OF THE ROAD

### BE SAFE

As with all things electronic the risk of fire or electrocution is always there. Be safe.

### BUY ANOTHER ONE

There is a greater than 0 chance you will destroy the target you are working on. If it means something to you, has sentimental or monetary value, or belongs to someone else – buy another one

### BE RESPONSIBLE

With testing and disclosure it always pays to not only be prudent, honest but also responsible

# BUILDING YOUR TOOLBOX


## YOU ARE GOING TO NEED A FEW THINGS

Fortunately, we have Amazon…

# WHAT YOU SHOULD HAVE IN YOUR TOOLBOX

## BASICS

- Soldering station
- BusPirate
- Serial Cables
- Screwdrivers
- Multimeter
- Screwdrivers
- Rubbing Alcohol
- Drinking Alcohol
- Screwdrivers
- Dry Chemical Fire Suppressant

## A BIT BEYOND BASICS

- Bench Power supply
- Jumper wire
- Snips
- De-Capping station
- Reflow Station

## ON THE FRINGE

- Toaster Oven
- FLIR Camera
- X-Ray machine
- A Good Lawyer

# GETTING STARTED

## TARGET SELECTION

Start small. Low voltage relatively simple devices

## RESEARCH

The FCC is your best friend. Lots of devices have to register with the FCC before they can go to market. It is all searchable, with pictures

## FIRMWARE IS YOUR FRIEND

Don’t have a device? Cant afford it? Analyze the firmware

# TARGET SELECTION


## TOYS!

Pretty cheap. Usually of “safe” build quality (won’t catch fire) and generally don’t have too much in the way of anti-tamper


## PERSONAL DEVICES

Cheap audio devices, iot ‘things’, stay away from battery packs and similar devices as they can be a bit more complicated

## LOW VOLTAGE

Stick to low voltage or battery powered.

# RESEARCH


## FCC

https://fccid.io/


## ODM/OEM WEBSITES

From the FCC website or any other intel – work your way to the Original Equipment Manufacturer (OEM) or Original Device Manufactueer

## DATASHEETS

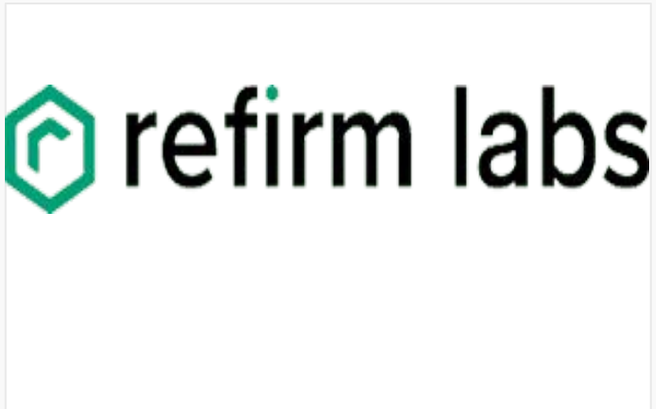
Once you have identified the components, start reading through the data sheets. Start drawing up a plan of attack

# SOFTWARE

Most embedded systems are going to run a flavor of Linux or some other RTOS (VxWorks etc)

Brush up on your knowledge. If the device can be controlled via an App - download the app and start researching that as well.

# FIRMWARE




## BINWALK

https://binwalkpro.refirmlabs.com/


## COMPANY WEBSITE

Google or Search the company website looking for firmware updates. Get used to figuring out how to unpack and reconstruct


## VMS

Depending on the device you may be able to mock up a “virtual machine” and not even need the hardware

# QUICK HIT LIST

### CPU/ARCH

ARM / MIPS? How much RAM? What kind of storage? NAND/FLASH?

### COMMS

Is there a JTAG port? Wireless? BLE? SPI?

### BOOTUP

Can we see it boot? Does it use secure boot? What kind of bootloader? Where is it getting its initial boot code?

### SOFTWARE

What is driving it? What was it written in? C? Python? Php?

### ACCOUNTS

Did they leave a backdoor in? Ssh keys? Is telnetd running as root?

### MORE INFO

https://adam-toscher.medium.com/a-red-team-guide-for-a-hardware-penetration-test-part-1-2d14692da9a1

# WHERE TO GO FROM HERE

## KEEP ON MOVING UP

Don’t be scared, and don’t get discouraged. As your skills progress and get better start moving up to more complex devices

## BUG BOUNTIES

There is a shortage of people with experience working on devices and a plethora of IoT devices hitting the market. Get in the game and start making some money

## IT REALLY CAN BE A JOB

Whether it is in Product Security Engineering or PSIRT there are real job opportunities for people who understand hardware, how to break it, and how to secure it

# QUESTIONS, COMMENTS, ETC?