



Joe Grand's Hardware Hacking Basics Training Course Agenda (NFI)

Last updated: February 4, 2026

This two-day comprehensive course teaches fundamental hardware hacking concepts and techniques used to reverse engineer and defeat the security of electronic systems. Combining lecture and hands-on exercises, it provides students with the skills, resources, and confidence to explore, manipulate, and exploit hardware devices once they leave the classroom. No prior hardware experience is required.

Additional information: [Grand Idea Studio Training](#)

A. Hardware Hacking Overview

1. Objectives and motivations
2. Common attack vectors
3. Methodology and process

B. Information Gathering

1. Open-source intelligence resources
2. Patents and certifications

C. Product Teardown

1. Opening housings
 - 1.1. Product assembly/disassembly methods
 - 1.2. Anti-tamper mechanisms
 - 1.3. Hands-on exercise: Defeat epoxy encapsulation
2. Component identification
 - 2.1. Discrete components
 - 2.2. Integrated circuits
 - 2.3. Obtaining and reading data sheets
 - 2.4. Hands-on exercise: Identify target components

D. Schematics and PCBs (Printed Circuit Boards)

1. Reading and creating schematics
2. PCB construction/fabrication methods
3. Hands-on exercise: Modify target PCB

E. Soldering and Desoldering

1. Tools and techniques
2. Hands-on exercise: Soldering
3. Hands-on exercise: Desoldering

F. Buses and Interfaces

1. Identifying interfaces
2. Determining pin function
 - 2.1. Hands-on exercise: Measurements w/ multimeter
 - 2.2. Hands-on exercise: Create block diagram/schematic
3. Signal monitoring and analysis
 - 3.1. Tools and techniques
 - 3.2. Serial communications interfaces (UART, I2C, SPI)
 - 3.3. Hands-on exercise: Signal monitoring w/ logic analyzer
 - 3.4. Hands-on exercise: Digital decoding w/ logic analyzer
 - 3.5. Hands-on exercise: Interactive console via UART

G. Signal/Data Manipulation

1. Tools and techniques
2. Debug interfaces (vendor-specific, JTAG, SWD)
3. Fault injection/glitching overview

H. Memory and Firmware

1. Memory types
2. Hands-on exercise: Extract/modify data from EEPROM
3. Firmware analysis tools and techniques

I. Hardware Hacking Challenge

Apply the knowledge and skills learned in the course to defeat the security mechanism of a custom electronic device.