ADVANCED CYBER TRAINING PROGRAM

EMBEDDED CNO

5-Day course

COURSE DESCRIPTION

The **Embedded CNO** course introduces hardware hacking to students with prior software CNO knowledge. Learn to exploit both physical and emulated embedded systems. Using hands-on tools and techniques, students will work through each step of the hardware hacking process on four different platforms. Course explores how to communicate with devices using industry-standard serial and testing protocols, and learn to extract, reverse engineer, and modify firmware from several common platforms.

Developed by a team of computer engineers and embedded developers, the course uses QEMU to emulate devices for safe practice. Students will also gain a high-level understanding of physical exploitation techniques like fault injection and side channel attacks, and may even get to practice them in a lab environment.

Prerequisites: Strong programming skills in C and Python, be comfortable with reverse engineering software using Ghidra.

Relevant Today

Hands-on skills in hardware hacking and firmware analysis that are essential for today's cybersecurity landscape, especially with the growth of IoT and embedded devices.

Inclusive Approach

Designed for a software CNO background, includes a take-home physical toolkit and practical labs, making advanced hardware concepts accessible and easy to apply.

Topics Include:

Communication protocols (SPI, I2C, UART, JTAG), hardware emulation, and firmware analysis, as well as the use of industry-standard tools like logic analyzers and multimeters.

ACTP
ADVANCED CYBER TRAINING PROGRAM

EMBEDDED CNO

5-Day course

AGENDA COURSE CONTENT

DAY 1

- Definition of an embedded system
- Overview of course tools
- PCB analysis and target enumeration concepts
- Raspberry Pi Pico deep dive and labs
  SPI and I2C flash memory labs

DAY 2

- Bootloader overview
- File systems and flash memory dumps lecture and lab
- Travel router firmware VR/E (6 part lab)

DAY 3

- Dancing Cactus enumeration and PCB analysis
- QEMU intro and labs
- Intro to verilog and digital logic

DAY 4

- Intro to FPGA
- Designing an embedded system with peripherals
- FPGA based hardware acceleration

DAY 5

- Advanced topics in hardware hacking attack techniques
- Crypto wallet voltage fault injection lab
- JTAG and RTOS discussions
  FINAL EXAM

TARGETS

- Travel router
- Dancing Cactus
- Crypto Wallet

EQUIPMENT

- Raspberry Pi 5 8GB RAM, with 128GB SD card and chassis
- Raspberry Pi Pico2
- iCESugar-nano *(Mini FPGA)*
- Logic analyzer *(Sigrok, USB)*
- Pomona SOIC clip
- Multimeter
- FTDI serial adapter
- I2C &SPI Flash breakout boards
- Mini soldering project
- Prototyping materials *(breadboard, resistors, wires, etc)*
- Peripherals *(7 segment display, OLED screen)*

**The full course syllabus is available upon request*

actp.mantech.com

actp@mantech.com