IoT Exploitation Training

Hands-On IoT Security Training

JSOF

Exploring the Depths of Security

IoT Exploitation Training - at a glance

Scope

- 8-10 days of training - study sessions and hands-on training
- Training focused on Hacking and Exploitation of vulnerabilities on Embedded platforms (IoT), as well as vulnerability hunting
- Training performed by experts in the field of exploitation
- Focus on the ARM architecture.
- Courses are offered in the form of open registration of, or as a private course for your company

Course Targets

After attending this course, you will be able to:

- Find vulnerabilities in closed and open source embedded software
- Use state-of-the-art tools and techniques for finding vulnerabilities
- Perform exploitation of vulnerabilities in order to achieve Remote Code Execution, Privilege Escalation and other goals
- Overcome exploit mitigations
- Understand how to approach an embedded device
- Assess the viability of exploitation for a given vulnerability
- Reverse engineer the Hardware of an embedded device (if opting for the HW reverse engineering module)

You will understand:

- Modern exploit mitigations
- The exploiter mindset
- Advanced methods of bug hunting
- How a product-grade exploit works

Course outline

- **Basics of Vulnerabilities – 1 day**
  - Types of vulnerabilities
  - Modern methods for finding vulnerabilities
  - Vulnerability case studies
  - Vulnerability landscape – who's who and where to learn
  - Basic Mitigations

- **Basic Exploitation – 2 days**
  - Different types of vulnerabilities and how to exploit them
  - Basic mitigation bypasses
  - Modern mitigations – CFI, SMAP, W^X, UAF protections, Sandboxing
  - Exploitation techniques

- **Vulnerability Hunting – 2 days**
  - Vulnerability Search techniques
  - How to approach a new system for vulnerability research
  - Advanced Fuzzing
  - Modern techniques – Feedback-based fuzzing, Symbolic Execution, Taint analysis
  - Understanding attack surface

- **Hardware reverse engineering (optional) – 2 days**
  - Hardware reversing
  - Debugging embedded devices
  - Gaining / sourcing Firmware
  - Detecting instruction set and peripheral HW
  - Exploring Firmware and using binwalk
  - Exploring Firmware Code

- **Advanced Exploitation on ARM – 3 days**
  - Advanced Exploit case study
  - Exploit productization
    - How to handle multiple product variants, real-world scenarios "in the wild"
  - Exploit chaining
  - Vulnerabilities from A-Z – the whole process from vulnerability hunting, triage, exploitation, mitigation bypass and productization
  - Final exercise

A more detailed Syllabus is available upon request.