Buy tickets: https://romhack.io/buy-tickets/

ROMHACK TRAINING

HUNTING ZERO-DAYS IN EMBEDDED DEVICES

by Pedro Ribeiro & Radek Domanski


TRAINING DESCRIPTION

Hunting Zero-Days in Embedded Devices is a unique, hands-on training course that teaches students how to find and exploit vulnerabilities in embedded devices such as routers, cameras, industrial devices, televisions, microcontrollers, automotive, etc. As a student, you will be taught the essential tips and tricks on how to debug an embedded device and extract firmware, and you will also be taught some exploitation techniques for ARM and MIPS. But the main aim of this course is to provide students with the necessary knowledge to find a zero day vulnerability in a device and exploit it. The course will go in depth into several classes of vulnerabilities, with practical exercises on real and emulated devices of different CPU architectures. Each vulnerability class will be described, studied and then exploited in a variety of different ways. Students will be given unique and publicly unknown tips from the trainers, which have a proven and public track record of finding and exploiting hundreds of zero days in embedded devices and other commercial products, as well as winning several prizes in Pwn2Own competitions. Have you ever wondered how real hackers are finding and exploiting vulnerabilities in embedded devices? Would you like to include those methodologies into your own product security testing? Are you an enthusiast that loves taking things apart, understanding and breaking them? Or are you a security specialist in another area that wants to dip your toes into embedded device hacking? If you answered yes to any of the above, this is the right course for you. There are many hardware hacking and exploit development courses in the market. But none of them provide a full top down view of how to find, understand and exploit vulnerabilities in embedded devices. This course aims to bridge the gap between hardware hacking and exploitation, giving students the necessary knowledge they need to become product security experts, embedded device reverse engineers and / or vulnerability researchers.

TRAINING TOPICS

Training page: https://romhack.io/hunting-zero-days-in-embedded-devices/
RomHack Training 2024: https://romhack.io/training/

- > Introduction to embedded devices
- > How to open, access and understand the hardware
- > Experiment with different techniques for hardware analysis, firmware extraction and control.
- > How embedded devices work with regards to their firmware
- > Common and advanced techniques for analyzing firmware
- > Vulnerability discovery and exploitation
- > How to find and exploit the most common vulnerability classes

TRAINING OUTCOMES

- > Evaluate and understand IoT device security, both hardware and software
- > Learn "old-school" techniques to facilitate security research on IoT devices
- > Break into devices using hardware and software tricks learned from years of hacking experience
- > Find and exploit vulnerabilities in IoT devices!

ABOUT THE TRAINER

Pedro Ribeiro is a vulnerability researcher and reverse engineer with over 10 years of commercial experience. Pedro has found and exploited hundreds of vulnerabilities in software and hardware products. He has over 150 CVE ID's attributed to his name (most of which related to remote code execution vulnerabilities) and has authored over 60 Metasploit modules that have been released publicly. Besides his vulnerability research activities, he is the founder and director of a penetration testing and reverse engineering consultancy based in London (Agile Information Security), with a variety of clients worldwide. More information about Pedro's publicly disclosed vulnerabilities can be found at https://github.com/pedrib/PoC

Radek Domanski started his professional career 12 years ago securing large networks and systems and transitioned afterwards into offensive security. He worked on high profile projects within the largest Internet Service Provider in Europe and in the research center of one of the world's largest telecommunications equipment companies. Radek found a number of critical vulnerabilities in real products and systems that are used by millions of users worldwide. Throughout the years of working on offensive product security Radek developed a unique methodology and honed his skills of vulnerability hunting. At the moment Radek is focusing on hardware, automotive hacking, exploitation and reverse engineering of embedded systems.

WHAT TO BRING

Please bring a laptop with a "bare metal" Linux install. We highly recommend Ubuntu 22.04+, Debian 11+ or the latest Kali Linux, unless you are very familiar with other distros and can fulfill the requirements below and fix problems yourself. Note that Linux really needs to be installed on the computer natively (either as the only operating system or as "dual boot"). This is a hard requirement, as the hardware tools we will be using do not work properly with Linux virtual machines. We will NOT BE ABLE TO HELP YOU if you encounter any problems and don't have a native Linux installation. You have been warned! Further requirements will be provided by email before the start of the course.

WHAT WILL BE PROVIDED

> Lab manual
> Access to cloud based exercises
> A selection of devices and tools to facilitate hardware hacking

PARTICIPANT SKILL SET

This is an Intermediate level course. You are not required to have experience in vulnerability discovery, exploitation or hardware hacking. However we recommend knowledge in the following topics:

> Linux command line
> Python and / or Ruby scripting
> Assembly language (x86 or any other architecture)
> Basic understanding of buffer overflows and other security vulnerability concepts
> Basic working proficiency with Ghidra (preferably) or IDA
> The course will be difficult at times, but the trainers will make sure no-one is left behind.

CLASS SYLLABUS

MODULE 1: Hardware Hacking and Firmware Extraction

> Course Introduction
> Embedded Device Landscape
> Intro to Hardware Hacking, Hardware / Software Tools and Storage Media
> Identifying and making use of debug interfaces (UART, JTAG, etc)
> Analyzing Analog and Digital Signals
> NOR Flash firmware extraction and handling
> NAND firmware extraction
> eMMC firmware extraction

MODULE 2: Firmware Analysis and Emulation;Intro to Vulnerabilities

> Introduction to MIPS
> RTOS: Loading and Analyzing
> Embedded devices file systems and formats
> Emulating and Debugging Firmware
> Knowing Your Target (Reconnaissance)
> Embedded Device Fuzzing
> Vulnerabilities Part 1: Information Leaks and Logic Flow Bypasses

MODULE 3: Finding and Exploiting Vulnerabilities

> Vulnerabilities Part 2: Buffer and Integer Over / Underflows
> Vulnerabilities Part 3: Owning Parsers
> Vulnerabilities Part 4: Command Injection
> Vulnerabilities Part 5: Directory Traversal
> Vulnerabilities Part 6: Insecure Configuration, Hardcoded Accounts and Backdoors

> Final lab: Capture-The-Flag competition on MIPS and/or ARM devices (time permitting!)