Syllabus: Hardware Hacking Expert - Level 1

About TrainSec Academy

TrainSec is an online learning hub for current and aspiring cybersecurity pros who understand the need for excellence. Level up or change career using skill-expanding modular learning way. We turn beginners into experts and experts into masters. TrainSec is designed for those who are serious about being at the vanguard of the latest knowledge, skills and trends. We're already working with the best.

Course Overview

The Hardware Hacking Expert course provides the essential knowledge, skills, and tools to become a proficient hardware hacker. Through a combination of theoretical concepts and hands-on exercises, participants will learn how to identify, analyze, and exploit vulnerabilities in embedded systems. The course offers a step-by-step guide from the basics of hardware components to advanced communication protocols and wireless hacking techniques.

Course Objectives

By completing this course, you will be able to:

- Fundamental Understanding: Gain a comprehensive understanding of embedded systems, their components, and high-level attack surfaces.
- Analytical Skills: Develop the ability to disassemble devices, identify key components, and log findings systematically.
- Datasheet Proficiency: Learn to locate, read, and interpret datasheets to understand embedded system components deeply.
- Tool Mastery: Become proficient with essential hardware hacking tools, including voltmeters, oscilloscopes, protocol analyzers, and RF sniffers.
- Communication Protocols: Acquire in-depth knowledge of various wired and wireless communication protocols, their uses, and how to exploit their vulnerabilities.
- Practical Application: Through demonstrations and hands-on exercises, apply theoretical knowledge to set up and analyze communication links.
- Advanced Techniques: Master advanced protocols like JTAG, SPI, I2C, USB, and CAN Bus, and understand their role in embedded systems.
- Security Insights: Learn to identify and exploit security flaws in RFID, NFC, Bluetooth, and BLE systems.

- Real-World Readiness: Successfully completes a comprehensive final challenge, demonstrating the ability to handle real-world hardware hacking scenarios and complex vulnerabilities.

By the end of this course, students will possess the knowledge, skills, and practical experience needed to excel in the field of hardware hacking, ready to tackle advanced challenges and contribute to cybersecurity efforts in embedded systems.

Course Format

- **URL:** https://trainsec.net/hardware-hacking-expert-level-1-2
- **Scope and Mode:** 16 classes, 48 learning materials, spanning over 36 hours of online videos and presentations.
- **Format:** Pre-recorded videos, presentations, interactive labs, discussion groups, and personal trainer support.
- **Pace:** Self-paced.
- **Platform**: TrainSec.net Learning Platform, Discord server.

Course Content

Embedded Systems introduction – Part 1&2

03:43 hours of video

This class provides a comprehensive overview of embedded systems, starting with what they are and why they are important. It introduces high-level components and defines potential attack surfaces. Key topics include processors, power supplies, timers, memory, input/output circuitry, communication ports, system-specific circuitry, secret ports, and attack vectors. Real-life examples and further reading resources are included to reinforce learning.

Student Achievements: By the end of this class, students will understand the fundamental concepts of embedded systems, recognize the main building blocks and their functions, and identify high-level attack surfaces. They will be equipped with the knowledge to start analyzing and hacking embedded systems.

The HWH Methodology

00:58 hours of video

This class explores different kinds of hacking scenarios, detailing the strategies and methodologies specific to hardware hacking. Students will learn the systematic approach to identify vulnerabilities and exploit embedded systems effectively.

Student Achievements: Students will understand various hacking scenarios, grasp the strategic approaches in hardware hacking, and learn the methodologies to systematically analyze and exploit embedded system vulnerabilities.

Embedded system: Components Identification – Part 1

01:16 hours of video

This class teaches students how to identify and define various components of embedded systems. Topics include safely disassembling devices, understanding PCBs, identifying entities of interest, and recognizing smart chips, communication methods, storage, and user interfaces.

Student Achievements: Students will develop the skills to methodically disassemble and analyze embedded systems, identify critical components, and document their findings for further analysis.

Embedded system: Datasheet Hunting – Part 1

01:17 hours of video

Focused on the importance of datasheets, this class covers how to find and read them, and how to identify and record points of interest. It emphasizes the role of datasheets in understanding and hacking hardware.

Student Achievements: By the end of this class, students will be proficient in locating and interpreting datasheets, which are crucial for understanding and manipulating embedded system componentsc

Embedded system: tools for analysis

01:34 hours of video

This class introduces the essential tools for hardware analysis, including power supplies, voltmeters, oscilloscopes, protocol analyzers, and RF sniffers. It also covers basic soldering techniques and provides further reading for in-depth understanding.

Student Achievements: Students will become familiar with various analytical tools, learn basic soldering skills, and understand how to apply these tools in hardware hacking projects

Introduction to Wired Communication Protocols

01:54 hours of video

Students will learn about the significance of communication in embedded systems, types of wired communication (serial and parallel), common protocols (UART, I2C, SPI, JTAG, RS232, CAN bus, USB, Ethernet), and their topologies.

Student Achievements: By the end of this class, students will understand the basics of wired communication protocols and their applications in embedded systems, preparing them for more detailed protocol analysis.

Communication Protocols: UART

02:00 hours of video

This class covers UART communication protocols, including physical attributes, signal identification, framing, flow control, and recommended tools. Demonstrations will show how to set up a UART link and sniffer.

Protocol Use: UART (Universal Asynchronous Receiver/Transmitter) is used for serial communication between microcontrollers and other hardware peripherals.

Student Achievements: Students will gain practical knowledge of UART protocols, enabling them to set up and analyze UART communication links effectively.

Communication Protocols: UART driven protocols

01:00 hours of video

Students will learn about UART-driven protocols such as RS232, RS422, and RS485, understanding why they exist, their importance, and hacking tips.

Protocols Use:

- RS232: Commonly used for serial communication between computers and peripherals.
- RS422: Utilized for long-distance communication with multiple receivers.
- RS485: Ideal for industrial control systems due to its robustness in noisy environments.

Student Achievements: By the end of this class, students will be able to work with various UART-driven protocols, recognizing their uses and potential vulnerabilities.

Communication protocols deep dive: SPI

02:00 hours of video

This class offers an in-depth look at SPI protocols, including definitions, physical attributes, signal identification, and advanced modes. Students will learn recommended tools and set up an SPI sniffer.

Protocol Use: SPI (Serial Peripheral Interface) is used for high-speed communication between microcontrollers and peripheral devices such as firmware storage devices, memory, sensors and SD cards.

Student Achievements: Students will master the SPI protocol, from basic concepts to advanced applications, enhancing their ability to hack and analyze SPI communication.

Communication protocols deep dive: I2C

02:15 hours of video

Focusing on I2C protocols, this class covers definitions, physical attributes, session signal definitions, master-slave sequences, and interesting aspects of I2C. Students will set up an I2C sniffer.

Protocol Use: I2C (Inter-Integrated Circuit) is used for communication between multiple integrated circuits using a simple two-wire interface.

Student Achievements: By the end of this class, students will have a thorough understanding of I2C protocols and be capable of setting up and analyzing I2C communication links.

Communication protocols deep dive: JTAG

01:30 hours of video

This class explores JTAG protocols, covering definitions, physical attributes, operational mechanics, uses, recommended tools, and practical demonstrations for firmware extraction and boundary scanning.

Protocol Use: JTAG (Joint Test Action Group) is primarily used for debugging and testing embedded systems, allowing direct access to the hardware.

Student Achievements: Students will gain expertise in JTAG protocols, enabling them to perform advanced hardware hacking tasks such as firmware extraction and debugging.

Communication protocols deep dive: USB

03:00 hours of video

Students will learn about USB protocols, including definitions, topologies, physical attributes, protocol basics, device structures, classes, enumeration, and live demonstrations of USB sniffing and analysis.

Protocol Use: USB (Universal Serial Bus) is used for connecting computers to peripheral devices like keyboards, mice, and storage devices, providing standardized communication and power supply.

Student Achievements: By the end of this class, students will be proficient in understanding and analyzing USB protocols, preparing them for practical USB hacking projects

Communication protocols deep dive: CAN BUS

01:49 hours of video

This class covers CAN Bus protocols, including definitions, physical attributes, signal identification, packet formats, network arbitration, recommended tools, and attack vectors such as sniffing, DoS, and MITM.

Protocol Use: CAN Bus (Controller Area Network) is used in automotive and industrial applications for robust communication between microcontrollers without a host computer.

Student Achievements: Students will master CAN Bus protocols and learn how to identify and exploit vulnerabilities in CAN Bus networks.

Introduction to Wireless Communication Protocols

02:45 hours of video

An overview of wireless communication types, topologies, digital wireless basics, radio concepts, and common protocols (RFID, NFC, Bluetooth, Wi-Fi). Students will learn about the conversion of RF signals to digital data.

Student Achievements: By the end of this class, students will understand the fundamentals of wireless communication and be familiar with key wireless protocols used in embedded systems.

Wireless networks: RFID & NFC

03:23 hours of video

This class focuses on RFID and NFC technologies, covering definitions, physical attributes, vulnerabilities, common protocols, and attack vectors. Students will learn about tools and techniques for hacking RFID and NFC systems.

Protocol Use:

- RFID (Radio Frequency Identification) is used for tracking and identifying objects using radio waves.

- NFC (Near Field Communication) is a subset of RFID used for short-range communication, often in contactless payment systems.

Student Achievements: Students will gain practical knowledge of RFID and NFC technologies, enabling them to identify vulnerabilities and perform attacks on these systems.

Wireless networks & protocols: Bluetooth & BLE

05:42 hours of video

Students will explore Bluetooth and BLE technologies, including their architecture, protocols, pairing processes, security measures, and tools for analysis. The class includes a live demo of BLE sniffing with Wireshark.

Protocol Use:

- Bluetooth is used for short-range wireless communication between devices, like headphones and smartphones.
- BLE (Bluetooth Low Energy) is optimized for lower power consumption, often used in fitness trackers and other IoT devices.

Student Achievements: By the end of this class, students will be proficient in Bluetooth and BLE protocols, capable of performing security assessments and analyzing wireless communication.

Required Materials

- **Prerequisites**: Basic knowledge of electronics, familiarity with operating systems, and a hacker state of mind.
- **Tools**: Multimeter, oscilloscope, protocol analyzer, soldering kit.
- **Additional Resources**: https://discord.com/invite/qugcNyWdaU

Instructor Information

- **Name**: Amichai Yifrach
- **Title**: Hardware Hacking Master
- **Bio**: Inventor and systems engineer for 30 years with expertise in electronics, coding, cybersecurity, R&D, and hardware hacking.
- **Social Handle**: @The_H1tchH1ker

Contact & Support

For any course-related or billing-related inquiries, please contact info@trainsec.net