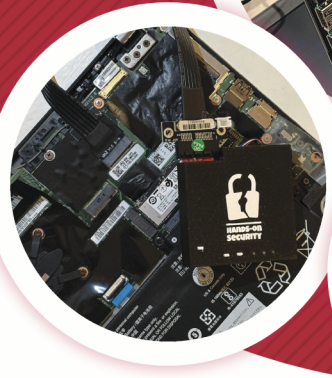
HANDS-ON SECURITY

BREAKING BITLOCKER

From zero to working BitLocker bypasses: Learn micro soldering, TPM sniffing, direct memory access (DMA) attacks, and bootloader patching. Walk out with working tools and the skills to attack BitLocker in real-world setups.



https://pcsfreebies.com/

CONTENT

In two days, we'll show you how to break into BitLocker protected systems using real hardware attacks. You'll start with micro soldering and logic sniffing on TPM buses - then move on to DMA attacks with PCILeech and exploiting an old Windows bootloader to extract BitLocker keys from RAM. No soldering experience needed. We'll cover everything hands-on - and you'll leave with a prepped test laptop, all attack gear, and working code.
Ideal for red teamers, forensic analysts, and anyone looking to challenge and harden BitLocker setups.

INCLUDING ALL HARDWARE

3499.–

CHF

SOLDERING

You will solder your own attack adapters. After in-depth theory and a warmup with the soldering iron you will learn how to micro solder on target devices.

LOGIC ANALYZER

Understand the capabilities and limitations of logic analyzers and undertake common bus sniffing attacks.

DMA & BOOTLOADER ATTACKS

Dump BitLocker keys from RAM using PCILeech or the BitPixie bootloader exploit.

HARDWARE KIT

- detailed slide set
- script to extract VMKs
- script to decrypt BitLocker recovery passwords working bitpixie exploit
- extensive hardware kit including:
  - Logic analyzer (U3Pro16)
  - Microsolder iron + tips
  - custom TPM attack adapter
  - target device with dTPM

UPCOMING TRAINING
29. – 30.01.2026

BBZ, Reishauerstrasse 2,
8090 Zürich, Switzerland

training@hands-on-security.com
www.hands-on-security.com