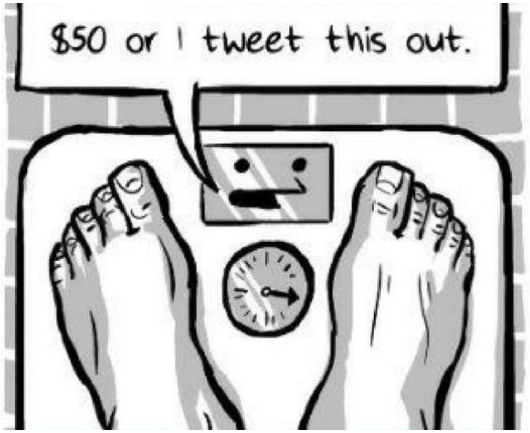
JSOF

Course Intro

Embedded Exploitation & vulnerability hunting



About Us

- JSOF is a Jerusalem-Based information security company
- We do consulting, training, and projects
- Focus is on **IoT**, **Embedded**, **Exploitation**, **Low-level**
- Course developed & taught in collaboration with Adir Nahum- Security Researcher & Engineer

About the course

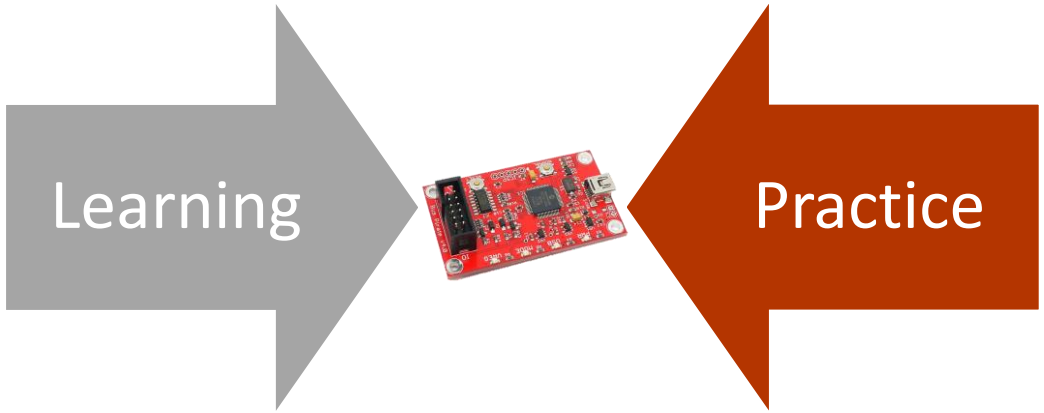
- Built specifically for [redacted]
- We will learn vulnerability hunting and exploitation
- Focus on embedded devices and ARM architecture
  - HW & SW!
- Will go from basic to very advanced
  - Advanced Focus on Exploit Productization

At the end of the course You will..

- Be able to find vulnerabilities in open and closed source
- Be able to go from device-in-a-box to Exploit on Embedded HW
- Be able to exploit vulnerabilities on ARM devices
- Know how a product-grade exploit-chain is built
- Know a little about reverse engineering hardware
- Know where to find more info

Course structure

- 10 days
- 1-day a week
- Lots of hands-on
  - Mornings are for learning
  - Afternoons for guided practice
- Semi self-paced

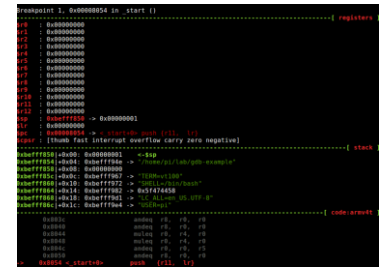


Course structure

- Every students will get a raspberry PI device

ARM

- HW exercises will be performed on routers
- Bug hunting exercises will be performed on laptop



- Exploitation exercises will be performed on the Raspberry
- At the end of the course you will take home the raspberry and all the exercises and material so that you can continue to practice

Course structure

- 5 chapters
  - Hardware hacking – 2 days (this starts today..)
  - Vulnerability basics – 1 day
  - Vulnerability hunting – 2 days
  - Basic exploitation – 2 days
  - Advanced exploitation – 3 days (hardcore..)
- Adapted to class


LET'S GO