Offensive IoT Exploitation

Trainer: Aditya Gupta (Attify)

Overview

Offensive Internet of Things Exploitation is a 3-day hands-on class focusing on finding vulnerabilities and exploiting IoT devices. The training has been developed after number of years of research and experience performing pentesting of IoT devices, which is what this training aims to teach the attendees, in action packed 3 days.

“Offensive IoT Exploitation” is a class offering attendees the ability to assess and exploit the security of these smart devices - by looking at the devices from an attacker’s approach, diving deep into Embedded security issues, reverse engineering firmware, analyzing radio communications and more. The training takes advantage of both custom made vulnerable setup as well as real-world devices to ensure that the attendees get maximum exposure and get to apply the skill sets they have learnt in the class.

After the 3-days class, the attendees will be able to:

- Extract, dump and analyze device firmwares
- Analyzing ARM and MIPS binaries and find vulnerabilities
- Understanding various hardware communication protocols and interfaces
- Gain access to device and sensitive information using UART, SPI and JTAG
- Conventional attack vectors applied to the IoT world
- Understanding, Sniffing and Reversing radio signals
- Interacting, Sniffing and exploiting BLE and ZigBee based devices
- Performing an effective pentest of an IoT device - tips and techniques

Offensive IoT Exploitation is the course for you if you want to try exploitation on new hardwares and find security vulnerabilities and 0-days in IoT devices.

Agenda:

Day 1:

- IoT Security internals
- Firmware analysis and reversing
- Emulating firmware binaries and full firmware emulation
- Real-time debugging emulated binaries
- ARM and MIPS architecture and exploitation
- Advanced binary exploitation
- MQTT, CoAP and communication exploitation
- Conventional exploitation techniques

Day 2:

- Introduction to Embedded device hacking
- Electronics internals for IoT pentesting
- Hardware recon
- Serial communication to IoT devices
- Gaining unauthenticated root shells
- Memory internals in Hardware devices
- Reading, Writing and Manipulating memory
- JTAG debugging and exploitation

Day 3:

- Software Defined Radio for pentesters
- Capturing and assessing radio signals
- Radio reversing
- Sniffing, Replaying and Modifying ZigBee packets
- Exploiting BLE based devices
- Group discussion and QnA

What will you get

- IoT devices to use and exploit during the class
- 600+ pages slides
- Lab materials, reference docs and cheatsheets
- IoT pentesting VM
- IoT Hackers Handbook - Author signed copy
- Access to private Slack group to have future discussions with the trainer

Expectation from the students:

- Basic linux experience
- Python script knowledge is a plus
- Must have the hardware and software prerequisites

Pre-requisites:

- Minimum 25 GB hard disk space
- 4 GB RAM
- Administrative access on the system
- USB access
- Virtualization software