Offensive **Internet of Things** Exploitation

3 DAYS COURSE

BASIC to ADVANCED

A 3-day class exploring the Internet of Things (IoT) taking a practitioner's approach to identify security vulnerabilities in these smart devices.

Offensive IoT Exploitation offers pentesters and security researchers, the ability to assess and exploit the security of these smart devices.

The Offensive IoT Exploitation class is an ideal class for you if you want to pentest real-world devices and find vulnerabilities and 0-days.

After the completion of this course, you will have a real world skill set of pentesting, exploiting and security any real world IoT device.

Hands-on Labs

Cutting-edge tools and techniques to exploit IoT devices

Real world examples and lab exercises

Taken by 1000+ security professionals so far

SOLD OUT at BlackHat, OWASP AppSec, HackInParis and other popular security conferences

Conducted by Attify's in-house IOT Security experts

WHO SHOULD TAKE THIS COURSE

- IoT Security Enthusiasts
- Embedded device developers
- Anyone interested to start professional IoT pentesting

DELIVERABLES

- 600+ Slides
- Lab Manual and Reference materials
- IoT Pentesting VM
- Devices to use during the class
- Training and CTF completion certification

HARDWARE / SOFTWARE REQUIREMENTS

- Laptop with minimum 25 GB free space and 4 GB RAM
- 2 functional USB ports
- VirtualBox/VMWare
- Administrative access on the system

AFTER THE COURSE, YOU'LL BE ABLE TO

- Analyze any real-world IoT device and map the attack surface
- Identify hardware, software, firmware, radio vulnerabilities
- Use various software and hardware tools during penetration tests
- Gain an extremely in-depth picture of IoT security with practical and hands-on experience

ABOUT ATTIFY

Attify is a specialized IoT security firm helping organizations secure their IoT devices by offering pentesting ("Attacker Simulated Exploitation") and training services. The team has huge experience in penetration testing of connected devices and it's associated applications.

Attify's team has authored books such as "Learning Pentesting for Android Devices", "IoT Hackers Handbook", published research papers like "A Short Guide on ARM Exploitation", is a member of the "Securing smart cities" initiative and regularly contributes to the public domain knowledge via talks and new research.

Attify has delivered research talks and training at various international security conferences including BlackHat, Defcon, OWASP AppSec, Syscan, Toorcon, Nullcon, Clubhack, phdays, Brucon, HackInParis and many more.

For more information, please contact us at secure@attify.com .

COURSE OUTLINE

GETTING STARTED WITH IOT SECURITY

- Introduction to IoT Security Architecture
- Getting Familiar with IoT Security and Components
- IoT Device Attack Surface Mapping
- Case Studies of IoT Vulnerabilities
- Attack Vectors for Smart Devices

FIRMWARE ANALYSIS

- Firmware internals
- Boot loaders for pentesters
- Understanding Device File Systems
- Getting access to the firmware
- Firmware Extraction Techniques
- Extracting file systems from firmware
- Analyzing and Backdooring Firmware
- Getting Around with Encrypted Firmware
- Emulating Firmware and Binaries
- Remote Live Debugging Firmware Binaries
- Identifying Vulnerabilities in Firmware
- Exploiting vulnerabilities to gain remote control

CONVENTIONAL ATTACK TECHNIQUES

- Conventional Attack Techniques of exploiting IoT
- Information Gathering and Reconnaissance
- Mobile Based Exploitation
- Intercepting mobile to device network communication
- Exploiting mobile application for Smart Device takeover
- Web application vulnerabilities for IoT devices
- Network Services Exploitation
- Insecure Encryption Components in use
- Password Cracking and Additional Attack Techniques

HARDWARE EXPLOITATION TECHNIQUES

- Hardware Hacking 101
- Basic Electronic Components and Analysis
- Analyzing Boards and chipsets
- Identifying Serial Interfaces and Pinouts
- UART Introduction and Interaction
- Serial to Root
- Introduction to SPI Flash
- Dumping Firmware from a Real Device
- JTAG – Introduction and finding pinouts
- JTAG Enabling and Exploitation
- Bypassing authentication using JTAG debugging

- Firmware Dumping - via UART and JTAG Debug
- USB Based Attack Vectors
- Fuzzing IoT Devices
- Side Channel and Timing Based Attacks overview
- Industrial Grade IoT Ecosystem and Security Issues
- Hardware Protections

ARM AND MIPS EXPLOITATION

- ARM and MIPS Assembly Basics
- Architecture, Registers and Flags
- Disassembling and Debugging Binaries
- Analyzing native libraries
- Overflow based exploitation
- Command Injection vulnerabilities
- ROP based exploitation

RADIO HACKING

- Getting started with SDR
- Radio Interfaces and Architecture
- Commonly used IoT Communication Techniques
- Setting up a Radio Pentesting Lab
- GNURadio for pentesters
- Capturing and Streaming Radio signals
- Recording and Replaying Radio Traffic
- Reversing Radio Communication Protocols for an IoT Device
- BLE in IoT devices
- Sniffing BLE packets

- Modifying and sending own packets
- Taking over an IoT device using BLE
- ZigBee - Versions and Security Issues
- Zigbee packet sniffing
- Replaying Zigbee packets
- Additional exploitation possibilities in Radio

CONCLUSION

- Writing a pentesting report
- Group Discussion
- CTF (if time permits)
- QnA

For additional details, contact us at secure@attify.com .