HACKINGPOINT

IoT Hacking Bootcamp

1 day class

"The great power of Internet of Things comes with the great responsibility of security". Being the hottest technology, the developments and innovations are happening at a stellar speed, but the security of IoT is yet to catch up. Since the safety and security repercussions are serious and at times life threatening, there is no way you can afford to neglect the security of IoT products. "IoT Hacking" is a unique workshop which offers security professionals, an understanding of IoT Technology suite including, IoT protocols, firmware and their underlyingweaknesses. The hands-on labs enable attendees to identify vulnerabilities in IoT. The workshop focuses on the attack surface on current and evolving IoT technologies in various domains such as home, enterprise automation etc.

It covers specific attack scenarios and open source software tools one needs to have in theirIoT penetration testing arsenal. Throughout the course, We will use Exos VM and EXPLIoT – open source IoT security testing framework which was created by us specifically for IoT penetration testing. Training modules are backed with Hands-on so attendees get to perform action on topics that are taught. Most modules have hands-on labs after the theory is completed.

N.B : Each participant would be given practical lab files and Exos VM that they would have to install prior to the workshop start date.

WHO SHOULD TAKE THIS CLASS

- Penetration testers tasked with auditing IoT
- Bug hunters who want to find new bugs in IoT products
- Government officials from defensive or offensive units
- Red team members tasked with compromising the IoT infrastructure
- Security professionals who want to build IoT security skills
- Embedded security enthusiasts
- IoT Developers and testers
- Anyone interested in IoT security

COURSE OUTLINE

Introduction to IoT

- Introduction
- IoT Architecture
- Frameworks

IoT Security Testing

- IoT Attack surface
- IoT Security Testing Process

IoT Protocols

* MQTT
  - Introduction
  - Protocol Internals
  - Reconnaissance
  - Information leakage
  - DOS attackss
  - Hands-on with open source tools
* CoAP
  - Introduction
  - Protocol Internals
  - Reconnaissance
  - Security issues
  - Hands-on with open source tools

Firmware

- Types
- Firmware updates
- Firmware analysis and reversing
- Firmware modification
- Firmware encryption
- Identifying Instruction Sets
- Simulating device environments

PRE-REQUISITES

- Basic knowledge of web and mobile security
- Knowledge of Linux OS
- Basic knowledge of programming - python

WHAT ATTENDEES SHOULD BRING

- Laptop with:
  - At least 50 GB free space
  - 8+ GB minimum RAM (4+GB for the VM)
- Administrative privileges on the system
- VirtualBox software – Latest VirtualBox version (including Virtualbox extension pack for the same version)
- Linux host machines should have exfat-utils and exfat-fuse installed (ex: sudo apt-get install exfat-utils exfat-fuse).
- Virtualization (Vx-t) option enabled in the BIOS settings for virtualbox to work.

WHAT ATTENDEES WILL BE PROVIDED WITH

- Training Slides (PDF)
- Hands-on Lab files
- Hands-on Lab manual (PDF)
- Exos VM with most of the IoT pentesting tools pre-installed

WHAT TO EXPECT

- Hands-on Labs
- Reverse Engineering
- Getting familiar with the IoT security
- This course will give you a direction to start performing pentests on IoT

WHAT NOT TO EXPECT

- Becoming an IoT hacker overnight. Use the knowledge gained in the training to start pentesting IoT devices and sharpen your skills.

ABOUT TRAINERS

Payatu is a research powered cyber security services and training organization. We specialize in IoT, embedded, cloud, mobile and infrastructure security assessments. Payatu trainers are highly specialized security professionals in the respective field and deliver hi-tech trainings and workshops around the world for private customers as well as global cyber security conferences including Blackhat, Cansecwest, Defcon, Brucon, Hack in Paris, Zerocon to name a few.

Check Point SOFTWARE TECHNOLOGIES LTD.