

Training:

Hacking Mobile Apps

Date of the training: **March 16-17, 2020** in Heidelberg, Germany

Book now using the voucher code: **TR20_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

The Hacking Mobile Apps Workshop covers the ethical hacking methodology of mobile apps and applies them to the three most prevalent mobile app types: Android, iOS and hybrid Apps. It also introduces the security architecture of Android and iOS platforms, as well as common vulnerabilities with web applications. Demos and exercises are included to teach different approaches of penetration testing, such as static and dynamic analysis and instrumentation with Frida.

What you will learn

- Setting up a penetration testing environment
- Different types of mobile apps vulnerabilities
- Static and dynamic analysis of mobile apps using state of the art methods and tools
- Understanding the security architecture of Android and iOS, including concepts like sandboxes and permissions
- Exploiting common vulnerabilities in mobile applications
- Understanding how rooting and jailbreaking works and why it is necessary for mobile penetration testing
- Manipulating mobile apps using Frida

By the end of this workshop, attendees will be able to conduct a full penetration test of mobile applications. We start from the basics, so no experience in the mobile security field is required.

What you can expect

The workshop is given by professionals in mobile apps penetration testing. During the workshop, we will provide you with rooted and jailbroken devices to do the exercises. Additionally, you will receive a virtual machine image equipped with tools and materials, so that you can use it to perform penetration tests.

Moreover, there will be optional exercises and support after the course, which will guide you along the journey of learning mobile application penetration testing.

Agenda

1. Introduction
2. Methodology and common Vulnerabilities
3. Android Platform
4. Pentesting of Android Apps
5. iOS Platform
6. Pentesting of iOS Apps
7. Hybrid Apps

Who should attend this training?

Due to the workshop starting at a basic level, it fits for everyone interested in the topic of mobile application security, including but not limited to:

- Mobile application developers who want to understand how to secure their Apps;
- Penetration testers and security analysts starting to look at mobile applications;
- IT-Professionals transitioning to security;
- Everyone interested in mobile security.

Prerequisites

Very basic scripting/programming experience, you should be able to understand simple code.

Requirements

- Laptop with VirtualBox and at least 40GB of disk space, 6GB of RAM and an UNLOCKED USB port
- Willingness to learn

About the Trainers:

Tobias Kopf is a Pentester and Security Researcher at ERNW focusing on mobile and embedded security. His fields of interest include iOS security, binary exploitation and fuzzing. He is a speaker at conferences, gives a lecture at DHBW Mosbach and various trainings about IT security. He also audits and advises big and very big companies in the area of IT security.

Ahmad Abolhadid is a security Analyst at ERNW GmbH. His expertise in the security field include Web and Mobile Apps, Telecommunications and infrastructure. He has developed mobile pentesting tools and gives workshops about security and pentesting.

Booking

Recommended online booking of trainings through:

<https://troopers.de/tickets/>

Voucher code: TR20_HMTS

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German.

+49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com