RANDORISEC

| Training: Mobile Hacking

Objective: Learn how to find security issues on Android and iOS apps
Level: beginner/intermediate
Duration: 3 days

1 500 € VAT excluded

Davy Douhine and Guillaume Lopes will deliver a 100% hands-on training to learn and understand the techniques, tips and tools used to perform vulnerability research on mobile applications. Goal is to introduce tools (such as adb, apktool, jadx, Frida, Objection and Hopper.) and techniques to work faster and in a more efficient way in the mobile (Android and iOS) ecosystem.

The following items will be provided to the attendees:

- **A VM with the pre-installed tools to cover most of the labs**
- **A Corellium access (iOS virtualization)**

Key Learning Objectives

- ✓ Introduce the OWASP MSTG and the MASVS
- ✓ Review Android and iOS security basics
- ✓ Build an Android and iOS pentest toolset
- ✓ Perform static analysis on the codebase of a mobile application
- ✓ Run the mobile application on a rooted device to check data security issues
- ✓ Hook the mobile application using Frida
- ✓ Analyze network communications with Burp and bypass Certificate Pinning

Who Should Attend?

- Prior knowledge on web security
- Intermediate to experienced administrators, developers, pentesters, bug hunters, security researchers and security experts

Prerequisite Knowledge

- Network and Linux knowledge

Agenda

Day 1

iOS

- iOS architecture and security features
- Introduction of OWASP MSTG and MASVS
- Set-up a testing environment
- Jailbreaks: History and types
- Corellium presentation
- Static analysis
- Metadata analysis
- Decryption of an iOS app
- iOS app decompilation with Hopper

Android

- Android architecture (components and sandbox)
- APK structure
- AndroidManifest presentation
- Set-up a testing environment
- Static analysis (jadx and apktool)
- Code Tampering (apktool)

Day 2

iOS

- Data analysis
  - iTunes backups
  - Data storage
  - Logs
- Dynamic analysis
  - Objective-C interfaces and implementations
  - Reverse-engineering with Frida
- Bypass security features
  - PIN/Login bypass
  - Jailbreak detection bypass

Android

- Data storage
  - SharedPrefs
  - Databases (SQLite)
  - Internal / External storage
- Dynamic analysis
  - Emulator vs Physical device
  - Root detection techniques
- Access control
  - Exported components
  - Content providers

Day 3

iOS

- Network security
  - Intercepting traffic with Burp
  - Certificate Pinning
- Analyze without a jailbroken device
  - Backup analysis
  - Network traffic
  - Side-loading Cycript/Frida/Objection

Android

- Network security
  - SSL/TLS common issues
  - Intercepting traffic with Burp
  - Certificate Pinning
- Frida Hooking
  - Frida scripts creation
  - Hooking native code