+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 24/01/2024

Sign up

Pentest Mobile training

5 days (35 hours)

Presentation

Mobile security has come a long way in recent years. It has gone from "should it be done?" to "must it be done!" Alongside the growing number of devices and applications, there's also an increasing volume of personally identifiable information (PII), financial data and much more. This data needs to be secured.

That's why Pentesting is so important for modern application developers. You need to know how to identify weaknesses in a mobile application, and how to fix them in an optimal way to ensure the security of user data.

This cybersecurity training course gives you the skills you need to test your mobile apps as a beginner, developer or security professional. You'll start by discovering the internal components of an Android and iOS application.

Moving forward, you'll understand the inter-process operation of these applications. Then, you'll set up a test environment for this application, using various tools to identify flaws and vulnerabilities in the application structure. In particular, participants will have the opportunity to run a series of exercises covering the major areas of mobile security, namely :

- Static analysis
- Security of data storage mechanisms
- Dynamic analysis
- Transport layer security

All the exercises are inspired by exploitation scenarios and vulnerabilities already found in real applications. Once we've gathered all the information on these security vulnerabilities, we'll start securing our applications against the various threats we've identified.

Objectives

- Knowledge of Android and iOS system architecture
- Setting up a test environment
- Replay and simulate attacks on Android and iOS applications
- Understand and implement measures for developing natively secure mobile applications

Target audience

- Developers
- Project managers
- SSI technicians
- Auditors
- Sliders
- CISO

Prerequisites

- Knowledge of Linux
- Good knowledge of networks, systems and security is a plus

Technical requirements

- Having a bare Ubuntu Linux 22.04 machine

Mobile Pentesting training program

General information on mobile application security

- Smartphone market share
- Different types of mobile applications (Native, Mobile web, Hybrid)
- Public vulnerabilities in Android and iOS
- The main security challenges facing mobile applications
- Mobile application penetration testing methodology (Discovery, Analysis/evaluation, Exploitation, Reporting)
- The OWASP mobile security project (MSTG and MASVS)

Digging into architecture

- The importance of architecture
- Android architecture
- iOS architecture

Preparation of test environment and tools

- Mobexler: the virtual machine for pentesting mobile applications
- Android Studio and SDK: setting up an emulator or connecting to a real device
- Apktool: utility for modifying installation programs
- JADX: application decompilation utility
- Ghidra: advanced reverse application tool
- Frida: dynamic analysis tool
- Objection: additional dynamic analysis tool
- Configuring iOS platform-specific tools

Modeling threats to an application

- Assets
- Threats
- Vulnerabilities
- Risk
- Threat model approach
- Threat modeling for a mobile application

Attacks on Android applications

- Getting to grips with the environment and running basic tests
- Modifying and patching binaries
- Analysis and operation of local data storage mechanisms
- Identifying insecure encryption mechanisms
- Analysis of Android components (activities, receivers, etc.)
- Interception and analysis of network traffic
- Assessment of anti-reverse defense mechanisms
- Bypassing detection mechanisms in a rooted environment
- Analysis and exploitation of backup mechanisms
- Analysis and evaluation of build parameters
- Analysis and operation of inter-process communication mechanisms (IPC)
- Static analysis of source code

Attacks on iOS applications

- Getting to grips with the environment and performing basic tests
- Modifying and patching binaries
- Static analysis of source code
- Analysis and operation of local data storage mechanisms
- Identifying insecure encryption mechanisms
- Using Frida
- Interception and analysis of network traffic
- Assessment of anti-reverse defense mechanisms
- Bypassing jailbreak detection mechanisms
- Analysis and exploitation of backup mechanisms
- Analysis and evaluation of build parameters
- Analysis and operation of inter-process communication mechanisms (IPC)

Securing your Android and iOs applications

- Design natively secure mobile applications
- Security mind map for developers (iOS and Android) on the Top 10 risks for mobile applications
- OWASP checklist of best practices for secure mobile development
- Automating safety recipes in a CI/CD chain
- Anti-reverse mechanisms to protect binaries

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.