TOREON

PWN ANDROID APPS WITH YOUR CUSTOM BUILT TOOLBOX

Frustrated with the various tools and environments needed to perform mobile pentesting?
All available Android test distributions have drawbacks and missing and/or non-working tools etc. Learn how to create your own customized mobile pentesting toolbox with the tools you really want/need.

Not sure which steps to follow when performing a mobile application security assessment?
Our renowned trainer, Steven Wierckx, will show you which steps to follow and what issues to focus on.

Course Description

This course is based on real-life experience of consultants in the field and will help you with your professional challenges. During the 1-day course you will build a toolbox to test Android applications. This course is meant for technical testers that have some experience in performing penetration tests against mobile or web applications. The main focus of this course will be on selecting and installing tools. In addition, we will provide you with a plan of attack for testing Android applications. Finally, we will provide some real life examples.

We will start with an empty Kali distribution for building our customized toolbox. During the training you will build a toolbox that fits your testing style; no more switching between different distributions to use certain tools! We will introduce you to a process to keep your tools up to date. Together with you, we will build a robust and re-usable testing environment from scratch. Tailor made for you and meeting your specific needs.

A plan of action will be provided in order to complete a comprehensive mobile application test.
The course will focus on:

- intercepting and analyzing traffic, setting up man in the middle proxies;
- performing static and dynamic code analysis;
- taking a look at the OWASP top 10 server side vulnerabilities.

Toreon CVBA
Grotehondstraat 44 1/1, B-2018 Antwerpen, België | T +32 33 69 33 96
BTW BE0542.795.568 | info@toreon.com | www.toreon.com

TOREON

Course contents

- Introduction to the Kali minimal distribution:
    - installing Kali tools;
    - adding repositories;
    - setting up your test environment;
    - creating and managing Android Virtual Devices;
    - maintaining your distribution and tools;
    - ADB tips and tricks.

- Introduction to Android application security:
    - threat landscape;
    - introduction to action, intent, broadcast, service,...;
    - Android application test process;
    - books, references, OWASP Mobile top-10.

- Android application reverse engineering:
    - .apk file content;
    - file storage;
    - decoding;
    - inspecting Smali code;
    - decompiling;
    - inspecting JAVA code;
    - static code analysis.

- Traffic capture and analysis:
    - intercepting HTTP proxies;
    - other data traffic.

- Dynamic Android application testing:
    - processes and permissions;
    - memory dumping;
    - debugging.

- Binding things together:
    - real life examples;
    - where to go from here.

At the end of the course the students will be able to create, update and manage a robust test environment for Android testing. This toolbox can easily be expanded for other activities such as web application testing etc. The student will also have a good knowledge of the tools used and how they are used together, what to do if a certain tool does not work etc.

This course will touch upon, but not go into detail, topics such as applications attacking other applications, non-HTTP traffic, kernel security and back end systems. The course focuses on applications running on the device.

Target audience

Everyone with an inquisitive mind that wants to learn:

- how to build and maintain a toolbox that can be used in various different scenario's.
- how to test the security of an Android application.

Requirements

Students should:
- know the basics of navigating a Linux command line (experience with Kali is a plus but certainly not a requirement).
- be able to create a virtual machine.
- know the basics of JAVA (or any other similar programming language) to read code.
- know the basics of penetration testing.

Students are required to bring a laptop (no netbook) with VMware Workstation/VirtualBox and enough processing power and RAM (we recommend at least 4Gb of RAM for the virtual machine) to run 1 virtual machine.
Note: do not install a VM image – you will receive the exact installation instructions and all images needed during the training.

All required tools and applications will be provided during the training or will be downloaded from the internet during the training.

You must have full administrator access to all machines. You must be able to install and remove software; and you must be able to disable and/or remove firewall/antivirus/… when necessary.