eshard

Your trusted partner in embedded security

Learn techniques and tools for reverse engineering Android applications. Specific focus will be put on practical exercises.

Android Security - Level 2

Benefits of training with eshard

Expand your knowledge and learn from the experts. We share our expertise with you in a hands-on manner to provide a pro-active learning experience. During the training you will get examples of real-case weaknesses and understand how to attack these weaknesses. After the training, you will be able to apply this knowledge straight away to your daily work. We will show you what measures to put in place to break as well as patch these weakness, to avoid future attacks.

Android Security - Level 2

About the course

Take your knowledge of mobile application attack techniques to the next level. During this training, you will learn advanced techniques and reverse engineering frameworks that can be used by powerful attacker to target Android applications. This training is intended for seasoned reverse engineer that are familiar with IDA and binary reverse engineering. Focus will be split between theoretical and practical parts. This course is particularly dedicated to those willing to extend their skills for conducting in-depth analyses and for improving the security of their developments.

Duration

Three days.

Target audience

Security analysts and ethical hackers.

Attendees will receive

The attendees will be given the presentation slides and a software package.

Pre-requisites

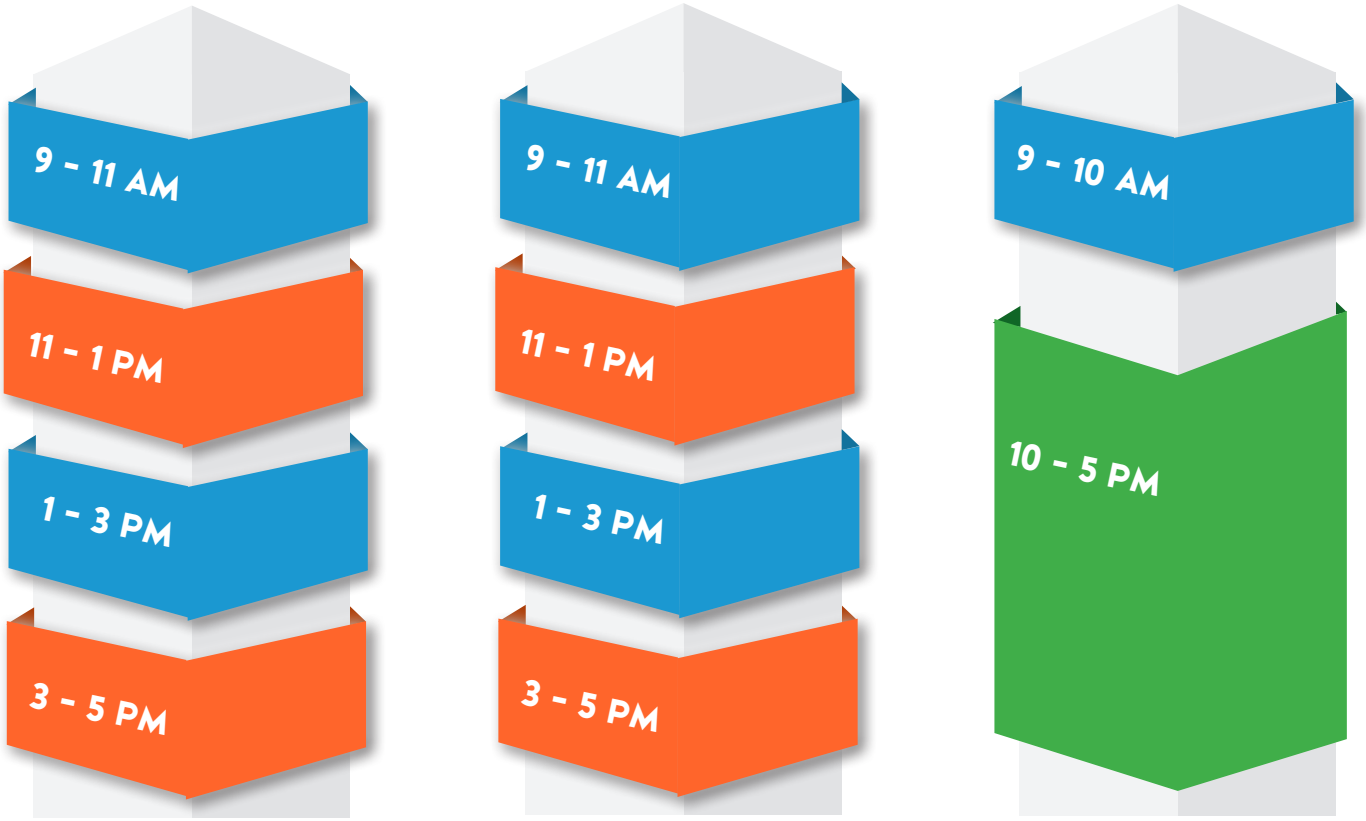
- Proficient in Reverse Engineering
- OS understanding
- Experience with C
- IDA experience
- Python experience

Why choose eshard as your trainer?

- Opportunity to work on real life cases.
- Access to years of hands-on knowledge. eshard's engineers have been working on several evaluation of SDKs and sensitive Android applications to measure their resilience against reverse engineering and tampering attacks.
- Having several engineers coming from the evaluation area provide a very good combination between evaluation methodology and reverse engineering expertise.
- We are flexibile regarding timing, customization and location. Training can be done onsite or hosted from two locations - Bordeaux and Marseille, in France. It's your call!

Course outline

Practical work Theoretical courses Challenge



Day 1

Day 1:

On the first day, we cover advanced SMALI

In this part the trainee will dig deeper into the smali instructions, tailor and run smali shellcodes, see how it can be useful for strings decryption or to make some quick checks before repackaging an application. We will apply theory into practical axercises throughout the day.

Day 2 AM:

In the morning, we cover IDA Advanced

In this part the trainee will play with IDA scripting modules, learn how to make plugins, automatically deobfuscate code with Python bindings, play with structure, enumerations and more.

Day 3 AM:

Before we dive into the pratical session, in the morning we give a good overview of symbolic execution, taint analysis, concolic testing will be reviewed and discussed to understand how, when and why it should be used.

Day 2

After, we cover Python Frameworks. An important part of reverse engineering is the capability of the attacker to adapt to a specific problem and to have the right tools to help him be performant. In this parts, we will review 3 importants frameworks that are a great assets to a reverse engineer to assemble, disassemble and execute code through python. In between these theoretical sessions, we have some time to cover practical exercises.

Day 2 PM:

In the afternoon, we will cover Advanced Hooking, where the trainee will learn differents ways to perform advanced hooking, see advanced used of Frida framework, play with customs memory allocators and others hooks and see advanced GDB usage.

Day 3 PM:

The last part of our training will be our 'crack me if you can' challenge representing a real case application that a participant will have to complete.

Day 3

Want to know more?

@eshardnews

companies/eshard

www.eshard.com
contact@eshard.com

ASIA

19 Keppel Road
#03-07 Jit Poh Building
Singapore 089058

EUROPE

1 Allée Jean Rostand Martillac
Bordeaux 33650 France

7 Rue Gaston de Flotte
Marseille 13012 France