# Android App Dynamic Runtime Analysis

Ruby & Jade

# Whoami

Role: Security Analyst

Interests: Mobile Security and Network Security Monitoring

Twitter: @r_doobie_

Shehacks KE

# Whoami

Role: Senior Security Engineer

Speciality: I do dope things

Projects: github.com/0x7678

Blog: 0x7678.com

Twitter:  0x7678

# Why are we here???

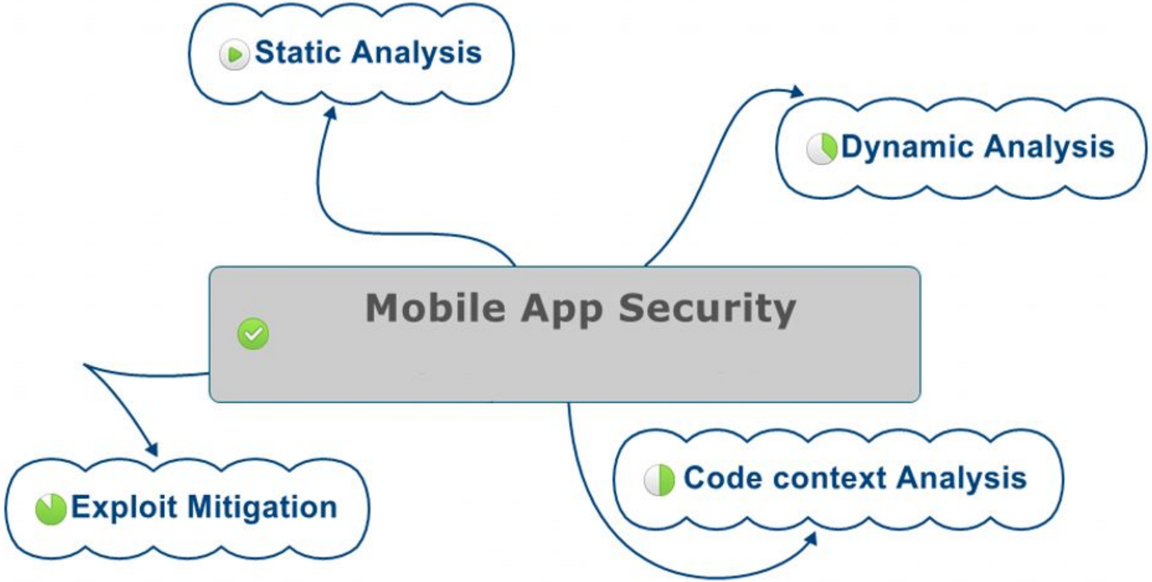
- Dynamically analyze android apps

# Key Takeaways!

- Learn something new!!
- Gain some PRACTICAL skills and TECHNICAL knowledge
  - How to break android apps
  - How to identify potential vulnerabilities

# ANDROID APP DYNAMIC RUNTIME ANALYSIS

# Mobile app security



# Types of Analysis

- Dynamic Analysis
  - Hook processes
  - Inject code to app or processes
  - Fuzz data input
  - Decompile binaries and libraries – low level

- Static Analysis
  - Disassemble the application
  - Read some low level bytecode
  - Explore binaries – high level

HACK
ALL
THE
THINGS

# Dynamic Analysis

Dynamic analysis entails executing the application, typically in an instrumented or monitored manner, to garner more concrete information on its behavior.

This often entails tasks like ascertaining artifacts the application leaves on the file system, observing network traffic, monitoring process behavior…basically all things that occur during execution.

# Why Perform Dynamic Runtime Analysis?

- Monitor process activity
- Observing file access
- Monitoring network activity
- Analyzing logs using logcat
- Memory dumps and analysis

# Xposed Framework

# Xposed Framework

Xposed is a framework for modules that enable you to modify the system or applications aspect and behavior at runtime, without modifying any Android application package (APK) or re-flashing.

# Xposed Modules

- RootCloak - this allows you to run apps that detect root without disabling root. It will completely hide root from the app of your choice. This includes hiding the su binary, superuser/supersu apks, processes run by root and more.

- SSLUnpinning - This is used to bypass certificate validation (Certificate Pinning).

# Xposed Modules

- Inspeckage - Android Package Inspector. It has more than 30 features. Inspeckage is a all-in-one tool developed to offer dynamic analysis of Android applications. Create hooks at runtime, enable predefined hooks and more. This tool helps you understand what an Android application is doing at runtime.

# DEMO

# FRIDA

# FRIDA

Frida is a Dynamic instrumentation toolkit. Frida is used for reverse engineering in general. This entails Dynamic binary instrumentation and debugging.

“Dynamic Binary Instrumentation (DBI) is the behavior of a binary application at runtime through the injection of instrumentation code. This makes it possible to gain insight into the behavior and state of an application at various points in execution.”

# FRIDA

Frida is multi-platform toolkit and multi-arch. It can be used on Windows/Mac/Linux/Android/iOS - i386/AMD64/ARM/ARM64

# DEMO