So Long, and Thanks for All the Fish

JUST SOME RANDOM THOUGHTS ABOUT THE MEANING OF LIFE, THE UNIVERSE, AND EVERYTHING

MENU

RECENT POSTS

Reverse engineering and penetration testing on Android apps: my own list of tools

July 18, 2019

Reverse engineering and penetration testing on Android apps: my own list of tools

Written by Andrea Fortuna • on July 18, 2019 • in Cybersecurity, Penetration Testing

This list of tools is really useful both in penetration testing on an Android application and in reverse engineering of a suspicious application.
All tools are OSS and freely available: *so, enjoy*!

Reverse Engineering

APKInspector

GUI tool for analysis of Android applications.
The goal of this project is to aide analysts and reverse engineers to visualize compiled Android packages and their corresponding DEX code.

APKTool

Elon Musk unveils Neuralink: tiny wires in the brain to read electrical pulses and let humans 'merge with computers'

July 17, 2019

Commando VM: a full Windows-based penetration testing virtual machine distribution

July 17, 2019

Zoom RCE vulnerability also affects RingCentral and Zhumu

July 16, 2019

CATEGORIES

Select Category

A tool for reverse engineering 3rd party, closed, binary Android apps.
It can decode resources to nearly original form and rebuild them after making some modifications.

objection

A runtime mobile exploration toolkit, powered by **Frida**.

> *It was built with the aim of helping assess mobile applications and their security posture without the need for a jailbroken or rooted mobile device.*

Sign.jar

Automatically signs an apk with the Android test certificate.

Bytecode Viewer

Bytecode Viewer is an Advanced Lightweight Java Bytecode Viewer, It's written completely in Java, and it's open sourced.

RECENT COMMENTS

wendolynn on Nope, 432 Hz is not the "frequency of universe"

DC-6 on Exploiting SUDO for Linux privilege escalation

www.it-swarm.net on How to check Cloudflare cache status programmatically

Ransomware analysis with Volatility on Volatility, my own cheatsheet (Part 2): Processes and DLLs

Andrea Fortuna on How to extract data and timeline from Master File Table on NTFS filesystem

Jadx

Dex to Java decompiler: Command line and GUI tools for produce Java source code from Android Dex and Apk files.

Oat2dex

A tool for converting .oat file to .dex files.

FindSecurityBugs

FindSecurityBugs is a extension for **FindBugs** which include security rules for Java applications.

Quick Android Review Kit (Qark)

A tool designed to look for several security related Android application vulnerabilities, either in source code or packaged APKs.

Secure, Unified, Powerful and Extensible Rust Android Analyzer

SUPER is a command-line application, developed in **Rust**, that can be used in Windows, MacOS X and Linux, that analyzes .apk files in search for vulnerabilities.

AndroBugs Framework

Android vulnerability scanner that helps pentesters to find potential security vulnerabilities in Android applications.

Simplify

Tool for de-obfuscating android package into Classes.dex which can be use Dex2jar and JD-GUI to extract contents of dex file.

ClassNameDeobfuscator

Python script to parse through the .smali files produced by **apktool** and extract the .source annotation lines.

Android backup extractor

Utility to extract and repack Android backups created with **adb backup** (ICS+). More info about adb backup **here**.

Dynamic Analysis

Cydia Substrate

Android version of well-known **iOS's Cydia Substrate**: it enables developers to make changes to existing software with extensions that are injected in to the target process's memory.

Xposed Framework

Xposed framework enables analysts to modify the system or application behaviour at runtime, without modifying any package or re-flashing.

---

logcat-color

A colorful and highly configurable alternative to the **adb logcat** command from the Android SDK.

Inspeckage

Tool developed for dynamic analysis of Android applications.
By applying hooks to functions of the Android API, **Inspeckage** will help analysts to track what an Android application is doing at runtime.

Frida

The toolkit works using a client-server model and lets you inject in to running processes not just on Android, but also on iOS, Windows and Mac.

Diff-GUI

A Web framework to start instrumenting with the available modules, hooking on native, inject JavaScript using Frida.

House

A runtime mobile application analysis toolkit with a Web GUI, powered by Frida, is designed for helping assess mobile applications by implementing dynamic function hooking and intercepting and intended to make Frida script writing as simple as possible.

AndBug

AndBug is a debugger targeting the Android platform's Dalvik virtual machine intended for reverse engineers and developers.

Introspy-Android

Blackbox tool to help understand what an Android application is doing at runtime and assist in the identification of potential security issues.

Drozer

Drozer allows you to search for security vulnerabilities in apps and devices by assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

Bypassing Root Detection and SSL Pinning

Xposed: Just Trust Me

Xposed Module to bypass SSL certificate pinning.

Xposed: SSLUnpinning

Android Xposed Module to bypass SSL certificate validation (Certificate Pinning).

Cydia Substrate: Android SSL Trust Killer

Blackbox tool to bypass SSL certificate pinning for most applications running on a device.

Cydia Substrate: RootCoak Plus

Patch root checking for commonly known indications of root.

Android Pinning

A standalone library project for certificate pinning on Android.

Android-ssl-bypass

Android debugging tool that can be used for bypassing SSL, even when certificate pinning is implemented, as well as other debugging tasks.

Related posts

Share this:

Like this:

Loading...

TAGS

ANDROID PENETRATION TESTING TOOLS

PRINT

Andrea Fortuna

Elon Musk unveils Neuralink: tiny wires in the brain to read electrical pulses and let humans 'merge with computers'

COMMENTS

Enter your comment here...

This site uses Akismet to reduce spam. Learn how your comment data is processed.