**逆向研究工具清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工具类别** | **工具名称** | **功能简介** |
| 1 | 反编译器 | apktool | 是GOOGLE提供的APK编译工具，能够反编译及回编译apk |
| 2 | 反编译器 | XJAD | Jar文件反编译成class文件 |
| 3 | 反编译器 | dex2jar | 反编译安卓classes.dex和.class文件。把apk文件改名为.zip，然后解压缩找到其中的class.dex文件，用dex2jar工具来逆方向导出jar文件，然后使用XJAD工具生成java源文件.class |
| 4 | 反编译器 | dare | 功能要强大于apktool，主要用来重定向 dex 、apk、或者是class文件，它会输出class文件，但是是不经过优化的，反编译出的文件很难做追踪。这个时候你可以使用 soot文件来做优化 |
| 5 | 反编译器 | dex-decomplier | Dex文件反编译器 |
| 6 | 反编译器 | APK\_OneClick | Apk反编译工具 |
| 7 | 反编译器 | APK IDE | APK改之理（Apk IDE）是一款APK反编译可视化工具 全自动的反编译、编译、签名Apk |
| 8 | 反编译器 | ApkToolkit | 是一款可视化的用于修改安卓Apk程序文件的工具，多种功能集于一体 反编译.apk ，重建.apk，签名.apk，优化.apk，.apk转.jar，反编译.dex，重建.dex，.dex转.jar |
| 9 | 反汇编器 | smali-cfgs | 图形界面显示，函数调用关系图 |
| 10 | 反汇编器 | IDA PRO 6.1 | 是一个世界顶级的交互式反汇编工具 |
| 11 | 汇编器 | Smali  Baksmali | 是一种dex格式文件的汇编器  是一种dex格式文件的反汇编器 |
| 12 | 优化器 | Soot | Java优化框架 |
| 13 | 分析工具 | androguard | 用于生成字节码，根据字节码的特征分析得到函数调用图 |
| 14 | 行为分析 | AndBug | 是一款动态逆向分析apk工具，目前只实现了相对简单的功能，对apk运行时的行为进行动态监控 |
| 15 | 行为分析 | apkinspector | 可以帮助分析人员手动分析Android恶意软件样本 |
| 16 | 行为分析 | STOWAWAY | 通过静态路径和功能模块分析提取出程序所需的权限集合与预定义的权限策略进行对比 |
| 17 | 行为分析 | COMDROID | apk文件静态分析，ComDroid用于发现APP漏洞，主要是根据Intent进行分析 |
| 18 | 行为分析 | amatutor | 安卓代码恶意分析 |
| 19 | 行为分析 | apkstatics | APK静态安全检查工具 |
| 20 | 行为分析 | 金山火眼 | 在线APK文件扫描及行为分析  fireeye.ijinshan.com  ID:[firestar2008@163.com](mailto:firestar2008@163.com) pwd:jinshanhuoyan@163.com |
| 21 | 行为分析 | Android安全监测网 | 在线监测Android病毒检测  http://www.apk32.com/ |
| 22 | 行为分析 | Virustotal | 是一个提供免费的可疑文件分析服务的网站  https://www.virustotal.com/ |
| 23 | 行为分析 | AndroTotal | 安卓 apk 文件在线病毒扫描  http://andrototal.org/ |
| 24 | 签名工具 | APK上上签 | 一款独立签名的工具 |
| 25 | 模拟环境 | droidbox | 基于TanitDroid系统构建的沙盒 |
| 26 | 模拟环境 | TaintDroid | APK模拟运行环境 |
| 27 | 模拟环境 | SandDroid | APK模拟运行环境 |
| 28 | 开发调试 | Class-dump | 是一个用于导出frameWork文件中私有头文件的工具  可以从编译后的Objective-C的二进制文件中提取对应的数据结构及函数等声明 |
| 29 | 开发调试 | Theos | 越狱开发工具包 |
| 30 | 开发调试 | Reveal | APP 的UI布局查看 |
| 31 | 开发调试 | MesaSQLite | SQLite数据库查看工具 |
| 32 | 开发调试 | GDB | Unix/Windows动态调试工具(the GNU project debugger) |
| 33 | 脚本语言 | Cycript | App开发语言 |
| 34 | 开发调试 | BigBoss | IOS越狱主要工具之一 |
| 35 | 破壳工具 | Appcrackr | App破解去壳工具 |
| 36 | 文件管理 | Ifile | IOS设备上一款非常强大的文件管理软件 |
| 37 | 模拟环境 | Mobile Terminal | 开源版的IOS终端 |
| 38 | 汇编器 | gikdbg | 32位汇编级调试器，集openssh，putty，otool，class-dump，ida，gdb于一体。 |