【Android 安全学习资料全集】android-security-awesome

https://github.com/ashishb/android-security-awesome

android-security-awesome backers 0 sponsors 0

A collection of android security related resources.

1. TOOLS
2. ACADEMIC / RESEARCH / PUBLICATIONS / BOOKS
3. EXPLOITS / VULNERABILITIES / BUGS

TOOLS

Online Analyzers

1. AndroTotal
2. Tracedroid
3. Visual Threat
4. Mobile Malware Sandbox
5. Appknox - not free
6. IBM Security AppScan Mobile Analyzer - not free
7. NVISO ApkScan
   10.AVC UnDroid
   12.habo 10/day
   13.Virustotal-max 128MB
   14.Fraunhofer App-ray - not free
   15.AppCritique - Upload your Android APKs and receive comprehensive free security assessments.
   16.NowSecure Lab Automated - Enterprise tool for mobile app security testing both Android and iOS mobile apps. Lab Automated features dynamic and static analysis on real devices in the cloud to return results in minutes. Not free
8. ~~CopperDroid~~
9. ~~SandDroid~~
10. ~~Stowaway~~
11. ~~Anubis~~
12. ~~Mobile app insight~~
13. ~~Mobile-Sandbox~~
14. ~~Ijiami~~
15. ~~Comdroid~~
16. ~~Android Sandbox~~
17. ~~Foresafe~~

18. ~~Dexter~~
19. ~~MobiSec Eacus~~
20. ~~Fireeye- max 60MB 15/day~~

Static Analysis Tools

1. Androwarn - detect and warn the user about potential malicious behaviours developped by an Android application.
2. ApkAnalyser
3. APKInspector
4. Droid Intent Data Flow Analysis for Information Leakage
5. DroidLegacy
6. Several tools from PSU
7. Smali CFG generator
8. FlowDroid
9. Android Decompiler – not free
10. PSCout - A tool that extracts the permission specification from the Android OS source code using static analysis
11. Amandroid
12. SmaliSCA - Smali Static Code Analysis
13. CFGScanDroid - Scans and compares CFG against CFG of malicious applications
14. Madrolyzer - extracts actionable data like C&C, phone number etc.
15. SPARTA - verifies (proves) that an app satisfies an information-flow security policy; built on the Checker Framework
16. ConDroid - Performs a combination of symoblic + concrete execution of the app
17. DroidRA
18. RiskInDroid - A tool for calculating the risk of Android apps based on their permissions, with online demo available.
19. SUPER - Secure, Unified, Powerful and Extensible Rust Android Analyzer
20. ClassyShark - Standalone binary inspection tool which can browse any Android executable and show important infos.
21. StaCoAn - Crossplatform tool which aids developers, bugbounty hunters and ethical hackers performing static code analysis on mobile applications. This tool was created with a big focus on usability and graphical guidance in the user interface.

App Vulnerability Scanners

1. QARK - QARK by LinkedIn is for app developers to scan app for security issues
2. AndroBugs
3. Nogotofail
4. Devknox - Autocorrect security issues as if it was spell check from your IDE
5. JAADAS - Joint intraprocedure and interprocedure program analysis tool to find vulnerabilities in Android apps, built on Soot and Scala

Dynamic Analysis Tools

1. Android DBI frameowork
2. Androl4b- A Virtual Machine For Assessing Android applications, Reverse Engineering and Malware Analysis
3. Android Malware Analysis Toolkit - (linux distro) Earlier it use to be an online analyzer

4. Mobile-Security-Framework MobSF - Mobile Security Framework is an intelligent, all-in-one open source mobile application (Android/iOS) automated pen-testing framework capable of performing static, dynamic analysis and web API testing.
5. AppUse – custom build for pentesting
6. Cobradroid – custom image for malware analysis
7. ~~ViaLab Community Edition~~
8. Droidbox
9. ~~Mercury~~
10. Drozer
11. Xposed - equivalent of doing Stub based code injection but without any modifications to the binary
12. Inspeckage - Android Package Inspector - dynamic analysis with api hooks, start unexported activities and more. (Xposed Module)
13. Android Hooker - Dynamic Java code instrumentation (requires the Substrate Framework)
14. ProbeDroid - Dynamic Java code instrumentation
15. Android Tamer - Virtual / Live Platform for Android Security Professionals
16. DECAF - Dynamic Executable Code Analysis Framework based on QEMU (DroidScope is now an extension to DECAF)
17. CuckooDroid - Android extension for Cuckoo sandbox
18. Mem - Memory analysis of Android (root required)
19. Crowdroid – unable to find the actual tool
20. AuditdAndroid – android port of auditd, not under active development anymore
21. Android Security Evaluation Framework - not under active development anymore
22. Android Reverse Engineering – ARE (android reverse engineering) not under active development anymore
23. Aurasium – Practical security policy enforcement for Android apps via bytecode rewriting and in-place reference monitor.
24. Android Linux Kernel modules
25. Appie - Appie is a software package that has been pre-configured to function as an Android Pentesting Environment.It is completely portable and can be carried on USB stick or smartphone.This is a one stop answer for all the tools needed in Android Application Security Assessment and an awesome alternative to existing virtual machines.
26. StaDynA - a system supporting security app analysis in the presence of dynamic code update features (dynamic class loading and reflection). This tool combines static and dynamic analysis of Android applications in order to reveal the hidden/updated behavior and extend static analysis results with this information.
27. DroidAnalytics - incomplete
28. Vezir Project - Virtual Machine for Mobile Application Pentesting and Mobile Malware Analysis
29. MARA - Mobile Application Reverse engineering and Analysis Framework
30. Taintdroid - requires AOSP compilation

Reverse Engineering

1. Smali/Baksmali – apk decompilation
2. emacs syntax coloring for smali files
3. vim syntax coloring for smali files
4. AndBug
5. Androguard – powerful, integrates well with other tools
6. Apktool – really useful for compilation/decompilation (uses smali)
7. Android Framework for Exploitation
8. Bypass signature and permission checks for IPCs

9. Android OpenDebug – make any application on device debuggable (using cydia substrate).
10. Dare – .dex to .class converter
11. Dex2Jar - dex to jar converter
12. Enjarify - dex to jar converter from Google
13. Dedexer
14. Fino
15. Frida - inject javascript to explore applications and a GUI tool for it
16. Indroid – thread injection kit
17. IntentSniffer
18. Introspy
19. Jad - Java decompiler
20. JD-GUI - Java decompiler
21. CFR - Java decompiler
22. Krakatau - Java decompiler
23. Procyon - Java decompiler
24. FernFlower - Java decompiler
25. Redexer – apk manipulation
26. Smali viewer
27. ~~ZjDroid~~, ~~fork/mirror~~
28. Simplify Android deobfuscator
29. Bytecode viewer
30. Radare2

Fuzz Testing

1. IntentFuzzer
2. Radamsa Fuzzer
3. Honggfuzz
4. An Android port of the melkor ELF fuzzer ELF 文件格式 fuzz
5. Media Fuzzing Framework for Android
6. AndroFuzz PDF fuzz

App Repackaging Detectors

1. FSquaDRA - a tool for detection of repackaged Android applications based on app resources hash comparison.

Market Crawlers

1. Google play crawler (Java)
2. Google play crawler (Python)
3. Google play crawler (Node) - get app details and download apps from official Google Play Store.
4. Aptoide downloader (Node) - download apps from Aptoide third-party Android market
5. Appland downloader (Node) - download apps from Appland third-party Android market

Misc Tools

1. smalihook
2. APK-Downloader
3. AXMLPrinter2 - to convert binary XML files to human-readable XML files

4. adb autocomplete
5. Dalvik opcodes
6. Opcodes table for quick reference
7. ExploitMe Android Labs - for practice
8. GoatDroid - for practice
9. mitmproxy
10. dockerfile/androguard
11. Android Vulnerability Test Suite - android-vts scans a device for set of vulnerabilities
12. AppMon- AppMon is an automated framework for monitoring and tampering system API calls of native macOS, iOS and android apps. It is based on Frida.

ACADEMIC / RESEARCH / PUBLICATIONS / BOOKS

Research Papers

1. Exploit Database
2. Android security related presentations
3. A good collection of static analysis papers

Books

1. SEI CERT Android Secure Coding Standard

Others

1. OWASP Mobile Security Testing Guide Manual
2. Android Reverse Engineering 101 by Daniele Altomare
3. doridori/Android-Security-Reference
4. android app security checklist
5. Mobile App Pentest Cheat Sheet
6. Mobile Security Reading Room - A reading room which contains well categorised technical reading material about mobile penetration testing, mobile malware, mobile forensics and all kind of mobile security related topics

EXPLOITS / VULNERABILITIES / BUGS

List

1. Android Security Bulletins
2. Android's reported security vulnerabilities
3. Android Devices Security Patch Status
4. AOSP - Issue tracker
5. OWASP Mobile Top 10 2016
6. Exploit Database - click search
7. Vulnerability Google Doc
8. Google Android Security Team’s Classifications for Potentially Harmful Applications (Malware)

Malware

1. androguard - Database Android Malwares wiki
2. Android Malware Github repo
3. Android Malware Genome Project - contains 1260 malware samples categorized into 49 different malware families, free for research purpose.
4. Contagio Mobile Malware Mini Dump
5. VirusTotal Malware Intelligence Service - powered by VirusTotal, not free
6. Admire
7. Drebin

Bounty Programs

1. Android Security Reward Program

How to report

1. Android - reporting security issues
2. Android Reports and Resources - List of Android Hackerone disclosed reports and other resources

---

Other Awesome Lists

Other amazingly awesome lists can be found in the awesome-awesomeness list.