The Mobile App Pentest cheat sheet was created to provide concise collection of high value information on specific mobile application penetration testing topics.

mobile-app pentesting android-application ios-app runtime-analysis network-analysis static-analysis reverse-engineers dynamic-analysis

MobileApp_Checklist_2017.xlsx	Updated Mobile application pentest checklist	7 months ago
README.md	Update README.md	12 days ago

README.md

Mobile Application Penetration Testing Cheat Sheet

The Mobile App Pentest cheat sheet was created to provide concise collection of high value information on specific mobile application penetration testing topics and checklist, which is mapped OWASP Mobile Risk Top 10 for conducting pentest.

Mobile Application Security Testing Distributions

- Appie - A portable software package for Android Pentesting and an awesome alternative to existing Virtual machines.
- Android Tamer - Android Tamer is a Virtual / Live Platform for Android Security professionals.
- AppUse - AppUse is a VM (Virtual Machine) developed by AppSec Labs.
- Androl4b - A Virtual Machine For Assessing Android applications, Reverse Engineering and Malware Analysis
- Mobisec - Mobile security testing live environment.
- Santoku - Santoku is an OS and can be run outside a VM as a standalone operating system.
- Vezir Project - Mobile Application Pentesting and Malware Analysis Environment.

All-in-One Mobile Security Frameworks

- 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 and dynamic analysis.
    - `python manage.py runserver 127.0.0.1:1337`
- Needle - Needle is an open source, modular framework to streamline the process of conducting security assessments of iOS apps including Binary Analysis, Static Code Analysis, Runtime Manipulation using Cycript and Frida hooking, and so on.
- Objection - Objection is 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.

Android Application Penetration Testing

Reverse Engineering and Static Analysis

- APKInspector - APKinspector is a powerful GUI tool for analysts to analyze the Android applications.
- APKTool - 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.
  - Disassembling Android apk file
    - `apktool d <apk file>`
  - Rebuilding decoded resources back to binary APK/JAR with certificate signing
    - `apktool b <modified folder>`
    - `keytool -genkey -v -keystore keys/test.keystore -alias Test -keyalg RSA -keysize 1024 -sigalg SHA1withRSA -validity 10000`
    - `jarsigner -keystore keys/test.keystore dist/test.apk -sigalg SHA1withRSA -digestalg SHA1 Test`
- Sign - Sign.jar automatically signs an apk with the Android test certificate.
- 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.
  - Deoptimize boot classes (The output will be in "odex" and "dex" folders)
    - `java -jar oat2dex.jar boot <boot.oat file>`
  - Deoptimize application
    - `java -jar oat2dex.jar <app.odex> <boot-class-folder output from above>`
  - Get odex from oat
    - `java -jar oat2dex.jar odex <oat file>`
  - Get odex smali (with optimized opcode) from oat/odex
    - `java -jar oat2dex.jar smali <oat/odex file>`
- FindBugs + FindSecurityBugs - FindSecurityBugs is a extension for FindBugs which include security rules for Java applications.

- Qark - This tool is designed to look for several security related Android application vulnerabilities, either in source code or packaged APKs.
- SUPER - SUPER is a command-line application that can be used in Windows, MacOS X and Linux, that analyzes .apk files in search for vulnerabilities. It does this by decompressing APKs and applying a series of rules to detect those vulnerabilities.
- AndroBugs - AndroBugs Framework is an efficient Android vulnerability scanner that helps developers or hackers find potential security vulnerabilities in Android applications. No need to install on Windows.
- Simplify - A tool for de-obfuscating android package into Classes.dex which can be use Dex2jar and JD-GUI to extract contents of dex file.
  - `simplify.jar -i "input smali files or folder" -o <output dex file>`
- ClassNameDeobfuscator - Simple 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+). Largely based on BackupManagerService.java from AOSP. Tip !! "adb backup" command can also be used for extracting application package with the following command:
  - `adb backup <package name>`
  - `dd if=backup.ab bs=1 skip=24 | python -c "import zlib,sys;sys.stdout.write(zlib.decompress(sys.stdin.read()))" > backup.tar`

Dynamic and Runtime Analysis

- Cydia Substrate - Cydia Substrate for Android enables developers to make changes to existing software with Substrate extensions that are injected in to the target process's memory.
- Xposed Framework - Xposed framework enables you to modify the system or application aspect and behaviour at runtime, without modifying any Android application package(APK) or re-flashing.
- logcat-color - A colorful and highly configurable alternative to the adb logcat command from the Android SDK.

- Inspeckage - Inspeckage is a tool developed to offer dynamic analysis of Android applications. By applying hooks to functions of the Android API, Inspeckage will help you understand 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 avaliable modules, hooking on native, inject JavaScript using Frida.
- AndBug - AndBug is a debugger targeting the Android platform's Dalvik virtual machine intended for reverse engineers and developers.
  - Identifying application process using adb shell
    - `adb shell ps | grep -i "App keyword"`
  - Accessing the application using AndBug in order to identify loaded classes
    - `andbug shell -p <process number>`
  - Tracing specific class
    - `ct <package name>`
  - Debugging with jdb
    - `adb forward tcp:<port> jdwp:<port>`
    - `jdb -attach localhost:<port>`
- Cydia Substrate: 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.
  - Starting a session
    - `adb forward tcp:31415 tcp:31415`
    - `drozer console connect`
  - Retrieving package information
    - `run app.package.list -f <app name>`

        - `run app.package.info -a <package name>`
    - Identifying the attack surface
        - `run app.package.attacksurface <package name>`
    - Exploiting Activities
        - `run app.activity.info -a <package name> -u`
        - `run app.activity.start --component <package name> <component name>`
    - Exploiting Content Provider
        - `run app.provider.info -a <package name>`
        - `run scanner.provider.finduris -a <package name>`
        - `run app.provider.query <uri>`
        - `run app.provider.update <uri> --selection <conditions> <selection arg> <column> <data>`
        - `run scanner.provider.sqltables -a <package name>`
        - `run scanner.provider.injection -a <package name>`
        - `run scanner.provider.traversal -a <package name>`
    - Exploiting Broadcast Receivers
        - `run app.broadcast.info -a <package name>`
        - `run app.broadcast.send --component <package name> <component name> --extra <type> <key> <value>`
        - `run app.broadcast.sniff --action <action>`
    - Exploiting Service
        - `run app.service.info -a <package name>`
        - `run app.service.start --action <action> --component <package name> <component name>`
        - `run app.service.send <package name> <component name> --msg <what> <arg1> <arg2> --extra <type> <key> <value> --bundle-as-obj`

Network Analysis and Server Side Testing

- Tcpdump - A command line packet capture utility.
- Wireshark - An open-source packet analyzer.
  - Live packet captures in real time
    - `adb shell "tcpdump -s 0 -w - | nc -l -p 4444"`
    - `adb forward tcp:4444 tcp:4444`
    - `nc localhost 4444 | sudo wireshark -k -S -i –`
- Canape - A network testing tool for arbitrary protocols.
- Mallory - A Man in The Middle Tool (MiTM) that use to monitor and manipulate traffic on mobile devices and applications.
- Burp Suite - Burp Suite is an integrated platform for performing security testing of applications.
- OWASP ZAP - OWASP Zed Attack Proxy Project is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.
- Proxydroid - Global Proxy App for Android System.

Bypassing Root Detection and SSL Pinning

- Xposed Module: Just Trust Me - Xposed Module to bypass SSL certificate pinning.
- Xposed Module: SSLUnpinning - Android Xposed Module to bypass SSL certificate validation (Certificate Pinning).
- Cydia Substrate Module: Android SSL Trust Killer - Blackbox tool to bypass SSL certificate pinning for most applications running on a device.
- Cydia Substrate Module: RootCoak Plus - Patch root checking for commonly known indications of root.
- Android-ssl-bypass - an Android debugging tool that can be used for bypassing SSL, even when certificate pinning is implemented, as well as other debugging tasks. The tool runs as an interactive console.
- Frida CodeShare - The Frida CodeShare project is comprised of developers from around the world working together with one goal - push Frida to its limits in new and innovative ways.
  - Bypassing Root Detection
    - `frida --codeshare dzonerzy/fridantiroot -f YOUR_BINARY`

    - Bypassing SSL Pinning
        - `frida --codeshare pcipolloni/universal-android-ssl-pinning-bypass-with-frida -f YOUR_BINARY`

Security Libraries

- PublicKey Pinning - Pinning in Android can be accomplished through a custom X509TrustManager. X509TrustManager should perform the customary X509 checks in addition to performing the pinning configuration.
- Android Pinning - A standalone library project for certificate pinning on Android.
- Java AES Crypto - A simple Android class for encrypting & decrypting strings, aiming to avoid the classic mistakes that most such classes suffer from.
- Proguard - ProGuard is a free Java class file shrinker, optimizer, obfuscator, and preverifier. It detects and removes unused classes, fields, methods, and attributes.
- SQL Cipher - SQLCipher is an open source extension to SQLite that provides transparent 256-bit AES encryption of database files.
- Secure Preferences - Android Shared preference wrapper than encrypts the keys and values of Shared Preferences.
- Trusted Intents - Library for flexible trusted interactions between Android apps.
- End-to-end encryption - Capillary is a library to simplify the sending of end-to-end encrypted push messages from Java-based application servers to Android clients.

iOS Application Penetration Testing

Access Filesystem on iDevice

- FileZilla - It supports FTP, SFTP, and FTPS (FTP over SSL/TLS).
- Cyberduck - Libre FTP, SFTP, WebDAV, S3, Azure & OpenStack Swift browser for Mac and Windows.
- itunnel - Use to forward SSH via USB.
- iProxy - Let's you connect your laptop to the iPhone to surf the web.

- iFunbox - The File and App Management Tool for iPhone, iPad & iPod Touch.

Reverse Engineering and Static Analysis

- otool - The otool command displays specified parts of object files or libraries.
- Clutch - Decrypted the application and dump specified bundleID into binary or .ipa file.
- Dumpdecrypted - Dumps decrypted mach-o files from encrypted iPhone applications from memory to disk. This tool is necessary for security researchers to be able to look under the hood of encryption.
  - `iPod:~ root# DYLD_INSERT_LIBRARIES=dumpdecrypted.dylib /var/mobile/Applications/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/Scan.app/Scan`
- class-dump - A command-line utility for examining the Objective-C runtime information stored in Mach-O files.
- Weak Classdump - A Cycript script that generates a header file for the class passed to the function. Most useful when you cannot classdump or dumpdecrypted , when binaries are encrypted etc.
  - `iPod:~ root# cycript -p Skype weak_classdump.cy; cycript -p Skype`
  - `#cy weak_classdump_bundle([NSBundle mainBundle],"/tmp/Skype")`
- IDA Pro - IDA is a Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger that offers so many features it is hard to describe them all.
- HopperApp - Hopper is a reverse engineering tool for OS X and Linux, that lets you disassemble, decompile and debug your 32/64bits Intel Mac, Linux, Windows and iOS executables.
- hopperscripts - Hopperscripts can be used to demangle the Swift function name in HopperApp.
- Radare2 - Radare2 is a unix-like reverse engineering framework and commandline tools.
- iRET - The iOS Reverse Engineering Toolkit is a toolkit designed to automate many of the common tasks associated with iOS penetration testing.

Dynamic and Runtime Analysis

- cycript - Cycript allows developers to explore and modify running applications on either iOS or Mac OS X using a hybrid of Objective-C++ and JavaScript syntax through an interactive console that features syntax highlighting and tab completion.
  - Show currently visible view controller
    - `cy# UIApp.keyWindow.rootViewController.visibleViewController`
  - Show view controller at the top of the navigation stack
    - `cy# UIApp.keyWindow.rootViewController.topViewController`
  - Get an array of existing objects of a certain class
    - `cy# choose(UIViewController)`
  - List method at runtime
    - `cy# classname.messages` or `cy# function printMethods(className, isa) { var count = new new Type("I"); var classObj = (isa != undefined) ? objc_getClass(className)->isa : objc_getClass(className); var methods = class_copyMethodList(classObj, count); var methodsArray = []; for(var i = 0; i < *count; i++) { var method = methods[i]; methodsArray.push({selector:method_getName(method), implementation:method_getImplementation(method)}); } free(methods); return methodsArray; }`
  -
    - `cy# printMethods("<classname>")`
  - Prints out all the instance variables
    - `cy# a=#0x15d0db80`
    - `cy# *a` or
    - `cy# function tryPrintIvars(a){ var x={}; for(i in *a){ try{ x[i] = (*a)[i]; } catch(e){} } return x; }`
    - `cy# a=#0x15d0db80`
    - `cy# tryPrintIvars(a)`
  - Manipulating through property
    - `cy# [a pinCode]`

        - `cy# [a setPinCode: @"1234"]` or `cy# a.setPinCode= @"1234"`
    - Method Swizzling
        - `cy# [a isValidPin]`
        - `cy# <classname>.prototype.isValidPin = function(){return 1;}`
- Frida-cycript - This is a fork of Cycript in which we replaced its runtime with a brand new runtime called Mjølner powered by Frida. This enables frida-cycript to run on all the platforms and architectures maintained by frida-core.
- Fridpa - An automated wrapper script for patching iOS applications (IPA files) and work on non-jailbroken device.
- bfinject - bfinject loads arbitrary dylibs into running App Store apps. It has built-in support for decrypting App Store apps, and comes bundled with iSpy and Cycript.
- iNalyzer - AppSec Labs iNalyzer is a framework for manipulating iOS applications, tampering with parameters and method.
- Passionfruit - Simple iOS app blackbox assessment tool with Fully web based GUI. Powered by frida.re and vuejs.
- idb - idb is a tool to simplify some common tasks for iOS pentesting and research.
- snoop-it - A tool to assist security assessments and dynamic analysis of iOS Apps.
- Introspy-iOS - Blackbox tool to help understand what an iOS application is doing at runtime and assist in the identification of potential security issues.
- gdb - A tool to perform runtime analysis of IOS applications.
- keychaindumper - A tool to check which keychain items are available to an attacker once an iOS device has been jailbroken.
- BinaryCookieReader - A tool to dump all the cookies from the binary Cookies.binarycookies file.

Network Analysis and Server Side Testing

- Canape - A network testing tool for arbitrary protocols.
- Mallory - A Man in The Middle Tool (MiTM) that use to monitor and manipulate traffic on mobile devices and applications.
- Burp Suite - Burp Suite is an integrated platform for performing security testing of applications.

- OWASP ZAP - OWASP Zed Attack Proxy Project is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.
- Charles Proxy - HTTP proxy / HTTP monitor / Reverse Proxy that enables a developer to view all of the HTTP and SSL / HTTPS traffic between their machine and the Internet.

Bypassing Root Detection and SSL Pinning

- SSL Kill Switch 2 - Blackbox tool to disable SSL certificate validation - including certificate pinning - within iOS and OS X Apps.
- iOS TrustMe - Disable certificate trust checks on iOS devices.
- Xcon - A tool for bypassing Jailbreak detection.
- tsProtector - Another tool for bypassing Jailbreak detection.
- Frida CodeShare - The Frida CodeShare project is comprised of developers from around the world working together with one goal - push Frida to its limits in new and innovative ways.
  - Bypassing SSL Pinning
    - `frida --codeshare lichao890427/ios-ssl-bypass -f YOUR_BINARY`
    - `frida --codeshare dki/ios10-ssl-bypass -f YOUR_BINARY`

Security Libraries

- PublicKey Pinning - iOS pinning is performed through a NSURLConnectionDelegate. The delegate must implement connection:canAuthenticateAgainstProtectionSpace: and connection:didReceiveAuthenticationChallenge:. Within connection:didReceiveAuthenticationChallenge:, the delegate must call SecTrustEvaluate to perform customary X509 checks.
- OWASP iMAS - iMAS is a collaborative research project from the MITRE Corporation focused on open source iOS security controls.

Contribution

Your contributions and suggestions are welcome.

License