

《Android恶意代码分析与渗透测试》

图书基本信息

书名：《Android恶意代码分析与渗透测试》

13位ISBN编号：9787115395934

出版时间：2015-7

作者：[韩] 赵涎元 等

页数：367

译者：金圣武

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《Android恶意代码分析与渗透测试》

内容概要

本书由“恶意代码分析”和“移动服务诊断”两大主题组成。各章节包含了分析步骤，作者们还亲自编写了黑客大赛应用程序试题，读者可以借此复习学过的内容。

Android应用程序分析环境构建

Android应用程序结构分析与各区域不同要素威胁

恶意代码分析工具讲解与具体示例

Android服务诊断方法与过程

Android黑客大赛试题详解与深入练习

《Android恶意代码分析与渗透测试》

作者简介

作者简介：

赵挺元 (chogar@naver.com)

目前在KB投资证券公司负责安全工作，管理安全防范项目 (<http://www.boanproject.com>)。在A3 Security公司做过5年渗透测试咨询顾问，在渗透测试项目管理、网络应用开发、源代码诊断等多种领域执行过漏洞诊断。之后在KTH安全团队负责移动服务和云服务安全、应对侵权事故等业务。著有《什么是渗透测试？》，与人合著《Kali Linux & BackTrack渗透测试实战》《Nmap NSE安全漏洞诊断实战》《数字取证的世界》《逮捕骇客的名侦探黑客》等。现为研究员、技术作家，与安全防范项目组成员们一起活跃在各个领域。

朴炳旭 (darkangelo@naver.com)

现任职于DO-IT公司安全小组，目前在LG电子负责个人信息安全保护工作。曾在韩国国会图书馆进行3年6个月的安全系统运营管理，分析各种日志、预先拦截内外部非法入侵及误用/滥用、应对入侵事故等。与人合著《Kali Linux & BackTrack渗透测试实战》《Nmap NSE安全漏洞诊断实战》。在安全防范项目组主要负责分析BackTrack/Kali Linux工具、Nmap NSE源代码及原理、Android恶意代码等，并与安全防范项目组成员们一起活跃在各个领域。

南大铉 (nam_daehyeon@naver.com)

目前负责智能TV安全漏洞诊断，在安全防范项目组担任移动PM。曾负责国企、银行、证券公司、信用卡公司等部门的渗透测试业务，还曾在S电子无线事业部执行移动漏洞诊断。一直关注移动安全、源代码审计、嵌入式、物联网 (IoT) 安全。

金衡范 (edwin_khb@naver.com)

在 (株) SSR管理咨询团队负责ISMS认证、ISO27001认证、PIMS认证、个人信息保护咨询等业务，在安全防范项目组负责组织并开展逆向工程相关技术线下活动。

译者简介：

金圣武

现居吉林，具有十多年网络安全领域工作经验，并翻译过大量安全主题相关文章。

电子邮件：xopensoft@163.com

个人主页：<http://tiefan.net>

OWASP子明

OWASP中国负责人，51CTO信息安全专家，微软信息安全白皮书译者。现为知道创宇信息技术有限公司技术总监。

书籍目录

第1章 Android的基本概念	1
1.1 Android的架构	1
1.1.1 Linux内核	2
1.1.2 库	2
1.1.3 Android运行时	2
1.1.4 应用程序与框架	4
1.1.5 设备文件目录结构	5
1.2 Android 重要组件	10
1.2.1 Activity	10
1.2.2 Service	11
1.2.3 Content Provider	11
1.3 Android应用程序的基本结构	11
1.4 小结	18
第2章 Android应用程序诊断环境	19
2.1 构建Android环境	19
2.1.1 安装Android SDK	19
2.1.2 安装ADK	23
2.1.3 测试Android开发环境	34
2.1.4 Linux 系统Android开发环境构建	38
2.2 构建数据包分析及检测环境	40
2.2.1 使用无线路由器收集信息	40
2.2.2 利用支持USB类型的AP（支持网关）收集信息	46
2.2.3 设置点对点网络以收集信息	48
2.2.4 使用tcpdump二进制文件收集信息	52
2.3 切换设备平台	55
2.3.1 通过攻击代码了解Rooting	55
2.3.2 使用Tegrak内核	66
2.3.3 使用CF-Auto-Root	69
2.4 Android诊断工具介绍	73
2.4.1 ADB基本命令	73
2.4.2 导出/导入设备中的apk文件	78
2.4.3 使用LogCat进行分析	80
2.4.4 使用pm命令获取设备信息	86
2.4.5 使用Busybox扩展Android系统命令	89
2.5 使用编辑器分析文件格式	91
2.6 小结	101
第3章 Android App分析方法	102
3.1 通过反编译进行静态分析	102
3.2 通过动态调试进行分析	107
3.3 通过代码修补绕过apk文件	115
3.4 使用AndroGuard进行分析	117
3.4.1 使用Androapkinfo查看信息	119
3.4.2 使用Androxml查看二进制XML 文件	120
3.4.3 使用Androlyze进行分析	121
3.4.4 使用Androdd查看apk文件结构	130
3.4.5 使用Androdiff和Androsim比较文件	133
3.5 使用DroidBox进行自动分析	135

3.5.1 path中添加adb命令	135
3.5.2 使用Android SDK Manager升级Packages	135
3.6 使用Sublime插件进行分析	144
3.7 使用APKInspector进行分析	147
3.8 使用dexplorer和dexdump进行分析	151
3.9 使用Santoku分析移动App	152
3.9.1 诊断工具Santoku	152
3.9.2 Santoku 安装与运行方法	153
3.9.3 使用Santoku对移动App进行逆向分析	158
3.10 小结	159
第4章 恶意代码分析	160
4.1 使用在线分析服务	160
4.1.1 使用Anubis分析恶意App	161
4.1.2 使用VirusTotal分析恶意App	162
4.1.3 使用VirusTotal App进行诊断	174
4.1.4 使用andrototal诊断	176
4.1.5 使用apkscan App进行诊断	179
4.1.6 使用Dexter进行诊断	184
4.1.7 使用APK Analyzer进行诊断	186
4.2 手动分析恶意代码App	187
4.2.1 分析smartbiling.apk恶意代码（获取设备信息）	188
4.2.2 分析alyac.apk恶意代码（伪造杀毒App）	199
4.2.3 分析miracle.apk恶意代码（发送设备信息）	219
4.2.4 分析phone.apk恶意代码（修改金融App）	224
4.2.5 apk-locker使用案例	231
4.3 用户应对恶意代码威胁的方法	235
4.3.1 禁止点击和下载可疑URL	236
4.3.2 安装手机杀毒软件并定期更新	238
4.3.3 关闭不使用的无线接口	239
4.3.4 禁止随意修改平台结构	240
4.3.5 使用三星KNOX（基于SEAndroid）保障安全	241
4.4 小结	242
第5章 Android 移动服务诊断	243
5.1 构建虚拟漏洞诊断测试环境	243
5.2 OWASP TOP 10移动安全威胁	248
5.3 保存不安全的数据	250
5.3.1 虚拟程序实操	252
5.3.2 查看/data/data/目录	253
5.3.3 应对方案	254
5.4 易受攻击的服务器端控制	255
5.5 使用易受攻击的密码	263
5.6 传输层保护不足（非加密通信）	264
5.7 源代码信息泄漏	270
5.8 泄漏重要信息	272
5.8.1 泄漏内存中的重要信息	273
5.8.2 虚拟程序实操	276
5.9 泄漏日志信息	280
5.10 Web服务漏洞项目诊断	281
5.11 App应对方案：加密源代码	283

5.11.1 ProGuard	283
5.11.2 用ProGaurd生成密钥	284
5.11.3 设置ProGuard	286
5.11.4 ProGuard生成文件简介	289
5.11.5 ProGuard的结果文件	291
5.12 小结	293
第6章 使用Android诊断工具	294
6.1 PacketShark：网络数据包截获工具	294
6.2 Drozer：移动诊断框架	298
6.3 ASEF：移动设备漏洞工具	307
6.3.1 通过安装apk文件进行检测	308
6.3.2 检测设备apk文件	312
6.4 DroidSheep：Web会话截取工具	319
6.5 dSploit：网络诊断工具	325
6.5.1 端口扫描	328
6.5.2 获取信息	329
6.5.3 破解账号	329
6.5.4 中间人攻击	330
6.6 AFLogical：移动设备取证工具	332
6.7 小结	333
第7章 Android黑客大赛App试题	334
7.1 Android App试题1	334
7.1.1 试题描述与出题目的	334
7.1.2 解题	334
7.2 Android App试题2	341
7.2.1 试题描述与出题目的	341
7.2.2 解题	341
7.3 Android App试题3	344
7.3.1 试题描述与出题目的	344
7.3.2 解题	345
7.4 Android App试题4	352
7.5 小结	361
参考网站	362
后记	363

《Android恶意代码分析与渗透测试》

精彩短评

- 1、一般吧，知道了一点新工具。恶意代码分析和最后四道题的思路还是值得看一下。
- 2、一般般，了解新工具可以。都是应用层的审计。

《Android恶意代码分析与渗透测试》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com