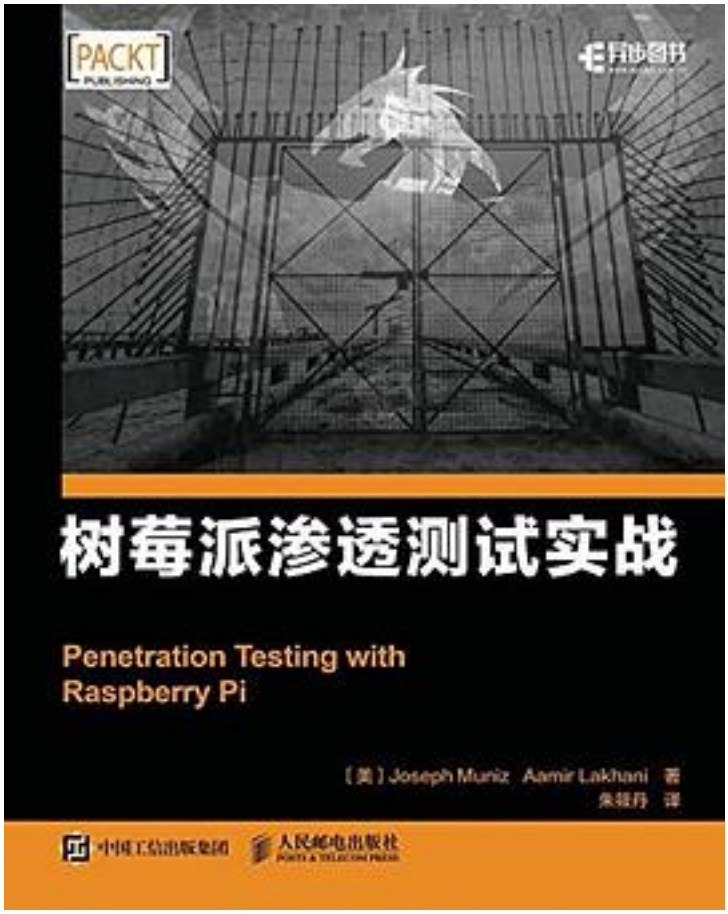
树莓派渗透测试实战



树莓派渗透测试实战_下载链接1_

著者:[美]约瑟夫·穆尼斯、阿米尔·拉克哈尼

出版者:人民邮电出版社

出版时间:2017-3-1

装帧:平装

isbn:9787115449078

《树莓派渗透测试实战》讲解了使用便携廉价的树莓派搭配Kali Linux进行渗透测试的方法。

《树莓派渗透测试实战》分为6章，介绍了树莓派和Kali

Linux的基础知识、适用于树莓派的Kali Linux
ARM版本的基本知识和环境优化、渗透测试相关的知识、树莓派的各种攻击手段、渗透测试后的工作，以及与树莓派相关的其他项目。

《树莓派渗透测试实战》内容组织有序，通过步骤式讲解来凸显实用性和实操性，适合信息安全从业人员阅读

作者介绍:

Aamir
Lakhani是一位知名的网络安全架构师、高级策略师兼研究员，负责为重要的商业和联邦企业部门提供IT安全解决方案。Lakhani曾经作为项目负责人，先后为世界500强公司、政府部门、重要的医疗服务提供商、教育机构、金融和媒体公司实施了安全策略。Lakhani曾经设计过以进攻为主的防御措施，并协助多家公司防御由地下安全组织发起的主动攻击。Lakhani被认为是行业领导者，他在网络防御、移动应用威胁、恶意软件、高级持续性威胁（APT）研究、暗安全（Dark
Security）等主题领域提供了详细的架构约定（architectural
engagements）和项目。Kakhani还是多本图书的作者和特约作者，其中包括Web
Penetration Testing with Kali Linux和XenMobile MDM（两者均为Packt
Publishing出版）。他还曾作为网络安全专家在美国国家公共广播电台上露面。

Lakhani运营着DrChaos.com博客，该站点被FedTech
Magazine评为网络安全技术的一个重要参考来源。他被评为社交媒体上知名的人物之一，在他的技术领域享有盛名。他将继续致力于网络安全、研究和教育领域。

Joseph
Muniz是思科公司的一名顾问，同时还是一位安全研究员。他的职业生涯始于软件开发，然后以外包技术人员的身份从事网络管理。Joseph后来进入咨询行业，而且在与许多不同的客户进行会谈时，发现自己对安全行业产生了激情。他曾经设计和实施过许多项目，其客户既有世界500强公司，也有大型的联邦网络。Joseph是多本图书的作者和特约作者，还是许多主流安全会议的发言人。通过访问他的博客www.thesecurityblogger.com可以看到全新的安全事件、研究和技术。

目录: 第1章 树莓派和Kali Linux基础知识 1
1．1 购买树莓派 2
1．2 组装树莓派 5
1．3 准备microSD卡 5
1．4 安装Kali Linux 8
1．5 把Kali和树莓派结合起来 13
1．6 树莓派的优点和缺点 15
1．7 树莓派渗透测试场景 16
1．8 克隆树莓派SD卡 18
1．9 避免常见问题 19
总结 22
第2章 树莓派预备步骤 23
2．1 树莓派的使用场景 24
2．2 C&C服务器 25
2．3 渗透测试需要做的准备 26
2．4 超频 27
2．5 设置无线网卡 30
2．6 设置Kali Linux使用的3G USB上网卡 32
2．7 设置SSH服务 33

2．8 SSH默认私钥和管理 34
2．9 通过SSH做反向Shell 35
2．10 Stunnel加密通道 39
2．11 安装Stunnel客户端 41
2．12 用例子总结以上步骤 43
总结 43
第3章 渗透测试 45
3．1 网络扫描 46
3．1．1 Nmap 47
3．1．2 无线安全 49
3．2 破解WPA/WPA2 50
3．3 捕获网络上的流量 56
3．4 中间人攻击（Man-in-the-middle） 58
3．4．1 从树莓派获得数据 58
3．4．2 ARP欺骗 61
3．4．3 Ettercap 63
3．4．4 Ettercap命令行 68
3．5 Driftnet 69
3．6 优化网络捕获 70
3．7 编写tcpdump文件上传脚本 72
3．8 Wireshark 74
3．8．1 捕获WordPress密码案例 76
3．8．2 tshark 79
3．9 用SSLStrip破解HTTPS 80
总结 84
第4章 树莓派攻击 85
4．1 攻击目标系统 86
4．2 Metasploit 86
4．2．1 用Metasploit创建自己的载荷 91
4．2．2 包装攻击载荷 94
4．3 社会工程 95
4．4 用BeEF钓鱼 100
4．5 恶意接入蜜罐 106
总结 112
第5章 结束渗透测试的工作 113
5．1 掩盖痕迹 114
5．2 清除日志 115
5．3 掩盖网络痕迹 119
5．3．1 代理链Proxychains 120
5．3．2 把树莓派重置成出厂设置 121
5．3．3 远程破坏Kali Linux 121
5．4 编写渗透测试报告 122
5．4．1 获得截图 123
5．4．2 压缩文件 125
总结 128
第6章 其他树莓派项目 129
6．1 PwnPi 130
6．2 Raspberry Pwn 133
6．3 PwnBerry Pi 135
6．4 网络防护 138
6．4．1 入侵检测和防护 138
6．4．2 内容过滤器 143
6．4．3 用OpenVPN做远程访问 150
6．4．4 Tor中继和路由routers 158

6．5 在PC上用QEMU模拟器运行树莓派 169
6．6 其他树莓派应用 172
6．6．1 用PiAware做飞行跟踪 172
6．6．2 PiPlay 174
6．6．3 PrivateEyePi 177
6．7 更多用途 178
总结 179
・・・・・・(收起)

树莓派渗透测试实战_下载链接1_

标签

黑客

渗透

测试

树莓派

安全

Linux

Kali

评论

翻译的第二本书，虽然比较薄比较入门，但适合开拓思路

下手，是因为本书是丹姐译的，所以翻译质量不用多说。但是...感觉作者写这本书完全不用心啊，行文啰嗦，各种语言逻辑错误，章节排版错误，很多贴图居然都贴错了...总的来说，干货比较少，书中很多工具都严重过时，而且树莓派用的居然是1代（现在3代

都成主流了好伐）。

技术很老，排版很差，内容很少。

树莓派渗透测试实战_下载链接1_

书评

树莓派渗透测试实战_下载链接1_