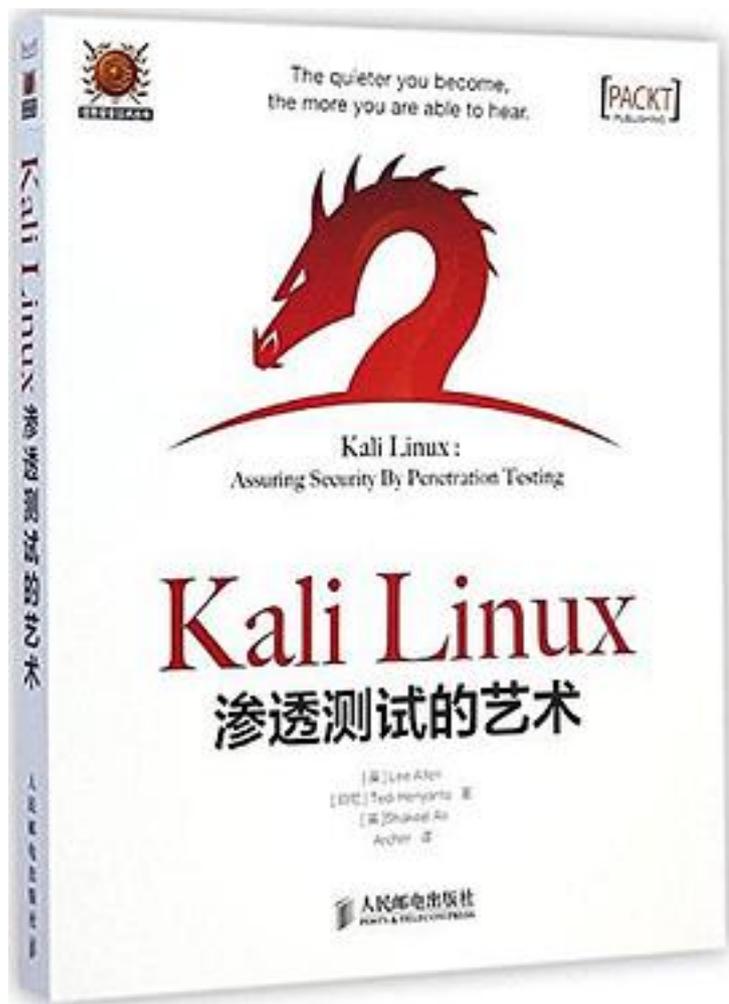


Kali Linux渗透测试的艺术



[Kali Linux渗透测试的艺术_下载链接1](#)

著者:Lee Allen

出版者:人民邮电出版社

出版时间:2015-2

装帧:平装

isbn:9787115378446

Kali

Linux是一个渗透测试兼安全审计平台，集成了多款漏洞检测、目标识别和漏洞利用工具，在信息安全业界有着广泛的用途。

本书从业务角度出发，通过真实攻击案例并辅之以各种实用的黑客工具，探讨了进行渗透测试所需的各种准备工序和操作流程。本书共分为12章，其内容涵盖了Kali Linux的使用、渗透测试方法论、收集评估项目需求的标准流程、信息收集阶段的工作流程、在目标环境中探测终端设备的方法、服务枚举及用途、漏洞映射、社会工程学、漏洞利用、提升权限、操作系统后门和Web后门的相关技术、渗透测试文档报告的撰写等。

本书适合讲解步骤清晰易懂、示例丰富，无论是经验丰富的渗透测试老手，还是刚入门的新手，都会在本书中找到需要的知识。

作者介绍:

Lee Allen是在顶尖大学里任职的安全架构师。多年以来，他持续关注信息安全行业和安全界内的新近发展。他有15年以上的IT行业经验，并且持有OSWP等多项业内的资格认证。Lee Allen还是Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide（由Packt Publishing出版，人民邮电出版社出版了其中文版）一书的作者。

Tedi Heriyanto是印尼一家信息安全公司的首席顾问。他一直在与（印尼）国内外的多家知名机构进行信息安全渗透测试方面的合作。他擅长设计安全网络架构、部署与管理企业级的信息安全系统、规范信息安全制度和流程、执行信息安全审计和评估，以及提供信息安全意识培训。在闲暇之余，他在印尼安全界的各种活动中不停地研究和学习。他还通过写作各种安全图书与大家分享界内知识。有兴趣的读者可以访问他的博客<http://theriyanto.wordpress.com>。

Shakeel Ali在世界500强公司里担任安全和风险管理顾问。在此之前，他是英国Cipher Storm Ltd.的核心创始人。他从事过安全评估、系统审计、合规部门顾问、IT管理和法证调查工作，积累了信息安全领域的各种知识。他还是CSS Providers SAL的首席安全员。他以废寝忘食的工作态度，为全球各类商业公司、教育机构和政府部门提供了不间断的安全支持服务。作为一名活跃的业内独立研究人员，他发表了大量的文章和白皮书。有兴趣的读者可以访问他的个人博客Ethical-Hacker.net。此外，他还长期参与墨西哥举办的BugCon Security Conferences活动，定期报告最前沿的网络安全威胁，并分享相应的应对方案。

目录: 目录

第1部分 系统的搭建与测试	
第1章 Kali Linux入门	3
1.1 Kali的发展简史	3
1.2 Kali Linux工具包	4
1.3 下载Kali Linux	5
1.4 使用Kali Linux	7
1.4.1 Live DVD方式	7
1.4.2 硬盘安装	7
1.4.3 安装在USB闪存上	16
1.5 配置虚拟机	18
1.5.1 安装客户端功能增强包	18

1.5.2	网络设置	20
1.5.3	文件夹共享	23
1.5.4	快照备份	25
1.5.5	导出虚拟机	25
1.6	系统更新	26
1.7	Kali Linux的网络服务	27
1.7.1	HTTP	28
1.7.2	MySQL	29
1.7.3	SSH	31
1.8	安装脆弱系统	32
1.9	安装额外工具包	34
1.9.1	安装Nessus漏洞扫描程序	36
1.9.2	安装Cisco密码破解工具	37
1.10	本章总结	38
第2章	渗透测试方法论	41
2.1	渗透测试的种类	41
2.1.1	黑盒测试	42
2.1.2	白盒测试	42
2.2	脆弱性评估与渗透测试	42
2.3	安全测试方法论	43
2.3.1	开源安全测试方法论 (OSSTMM)	44
2.3.2	信息系统安全评估框架	46
2.3.3	开放式Web应用程序安全项目	48
2.3.4	Web应用安全联合威胁分类	49
2.4	渗透测试执行标准	51
2.5	通用渗透测试框架	52
2.5.1	范围界定	52
2.5.2	信息收集	53
2.5.3	目标识别	54
2.5.4	服务枚举	54
2.5.5	漏洞映射	54
2.5.6	社会工程学	54
2.5.7	漏洞利用	55
2.5.8	提升权限	55
2.5.9	访问维护	55
2.5.10	文档报告	56
2.6	道德准则	56
2.7	本章总结	57
第2部分	渗透测试人员的军械库	
第3章	范围界定	61
3.1	收集需求	62
3.1.1	需求调查问卷	62
3.1.2	可交付成果的需求调查表	63
3.2	筹划工作	64
3.3	测试边界分析	66
3.4	定义业务指标	67
3.5	项目管理和统筹调度	68
3.6	本章总结	69
第4章	信息收集	71
4.1	公开网站	72
4.2	域名的注册信息	73
4.3	DNS记录分析	75
4.3.1	host	75
4.3.2	dig	77

- 4.3.3 dnsenum 79
- 4.3.4 dnsdict6 82
- 4.3.5 fierce 84
- 4.3.6 DMitry 85
- 4.3.7 Maltego 88
- 4.4 路由信息 95
 - 4.4.1 tcptraceroute 95
 - 4.4.2 tctrace 97
- 4.5 搜索引擎 98
 - 4.5.1 theharvester 98
 - 4.5.2 Metagoofil 100
- 4.6 本章总结 103
- 第5章 目标识别 105
 - 5.1 简介 105
 - 5.2 识别目标主机 106
 - 5.2.1 ping 106
 - 5.2.2 arping 108
 - 5.2.3 fping 110
 - 5.2.4 hping3 112
 - 5.2.5 nping 115
 - 5.2.6 alive6 117
 - 5.2.7 detect-new-ip6 118
 - 5.2.8 passive_discovery6 119
 - 5.2.9 nbtscan 119
 - 5.3 识别操作系统 121
 - 5.3.1 p0f 121
 - 5.3.2 Nmap 125
 - 5.4 本章总结 125
- 第6章 服务枚举 127
 - 6.1 端口扫描 127
 - 6.1.1 TCP/IP协议 128
 - 6.1.2 TCP和UDP的数据格式 129
 - 6.2 网络扫描程序 133
 - 6.2.1 Nmap 133
 - 6.2.2 Unicornscan 155
 - 6.2.3 Zenmap 157
 - 6.2.4 Amap 160
 - 6.3 SMB枚举 162
 - 6.4 SNMP枚举 163
 - 6.4.1 onesixtyone 163
 - 6.4.2 snmpcheck 165
 - 6.5 VPN枚举 166
 - 6.6 本章总结 170
- 第7章 漏洞映射 171
 - 7.1 漏洞的类型 171
 - 7.1.1 本地漏洞 172
 - 7.1.2 远程漏洞 172
 - 7.2 漏洞的分类 173
 - 7.3 OpenVAS 174
 - 7.4 Cisco分析工具 178
 - 7.4.1 Cisco Auditing Tool 178
 - 7.4.2 Cisco Global Exploiter 180
 - 7.5 Fuzz (模糊) 分析工具 181
 - 7.5.1 BED 181

- 7.5.2 JBroFuzz 183
- 7.6 SMB分析工具 185
- 7.7 SNMP分析工具 187
- 7.8 Web程序分析工具 190
 - 7.8.1 数据库评估工具 190
 - 7.8.2 Web应用程序评估工具 199
- 7.9 本章总结 209
- 第8章 社会工程学攻击 211
 - 8.1 人类心理学建模 211
 - 8.2 攻击过程 212
 - 8.3 攻击方法 213
 - 8.3.1 冒名顶替 213
 - 8.3.2 投桃报李 213
 - 8.3.3 狐假虎威 214
 - 8.4 啖以重利 214
 - 8.5 社会关系 214
 - 8.6 Social Engineering Toolkit (SET) 215
 - 定向钓鱼攻击 216
 - 8.7 本章总结 220
- 第9章 漏洞利用 221
 - 9.1 漏洞检测 221
 - 9.2 漏洞和exploit资料库 223
 - 9.3 漏洞利用程序工具集 224
 - 9.3.1 MSFConsole 225
 - 9.3.2 MSFCLI 227
 - 9.3.3 忍者操练101 228
 - 9.3.4 编写漏洞利用模板 249
 - 9.4 本章总结 255
- 第10章 提升权限 257
 - 10.1 利用本地漏洞 258
 - 10.2 密码攻击 261
 - 10.2.1 离线攻击工具 262
 - 10.2.2 在线破解工具 280
 - 10.3 网络欺骗工具 285
 - 10.3.1 DNSChef 286
 - 10.3.2 arpspoof 288
 - 10.3.3 Ettercap 290
 - 10.4 网络嗅探器 294
 - 10.4.1 Dsniff 294
 - 10.4.2 tcpdump 295
 - 10.4.3 Wireshark 296
 - 10.5 本章总结 299
- 第11章 访问维护 301
 - 11.1 操作系统后门 301
 - 11.1.1 Cymothoa 301
 - 11.1.2 Intersect 304
 - 11.1.3 Meterpreter后门 307
 - 11.2 隧道工具 310
 - 11.2.1 dns2tcp 310
 - 11.2.2 iodine 312
 - 11.2.3 ncat 314
 - 11.2.4 proxychains 316
 - 11.2.5 ptunnel 317
 - 11.2.6 socat 318

- 11.2.7 sslh 321
- 11.2.8 stunnel4 323
- 11.3 创建Web后门 327
 - 11.3.1 WeBaCoo 327
 - 11.3.2 weevely 330
 - 11.3.3 PHP Meterpreter 332
- 11.4 本章总结 335
- 第12章 文档报告 337
 - 12.1 文档记录与结果验证 338
 - 12.2 报告的种类 339
 - 12.2.1 行政报告 339
 - 12.2.2 管理报告 340
 - 12.2.3 技术报告 340
 - 12.3 渗透测试报告（样文） 341
 - 12.4 准备演示的资料 342
 - 12.5 测试的后期流程 343
 - 12.6 本章总结 344
- 第3部分 额外资源
- 附录A 辅助工具 347
- 附录B 关键资源 369
- • • • • [\(收起\)](#)

[Kali Linux渗透测试的艺术_下载链接1](#)

标签

渗透测试

kali

计算机

安全

linux

计算机安全

网络安全

计算机科学与技术

评论

作为一本渗透测试基础教程，还可以。各种工具的介绍，比自己搜索省点时间。

其实是3-3.5分。很多内容已经更新了。涉及工具比较多，每个都来不及细讲，但是可以有一个基本的理解，拿来打基础还可以。

速读而过，章节组织有序条理清晰，比较系统地介绍了渗透测试的几个步骤，比较规范化。每章节开头和总结基本上看看就好，所以说总结的很好，读者不用很花费时间就能get到了。最后的输出报告可以参考。当然如果想深入学习的话可以详细看看书中提到的各类渗透工具。

不知道这书到底要怎么定位 就是一本kali内置工具的简易说明书嘛

除了第二章，剩下的就是把文档放在书里

渗透入门，了解了解

工具不全

这种书随便翻翻就是，别认真

感觉还行吧，比较适合小白入门的那种，如果是想深入的话还是得自己找资料呐。

[Kali Linux渗透测试的艺术_下载链接1](#)

书评

[Kali Linux渗透测试的艺术_下载链接1](#)