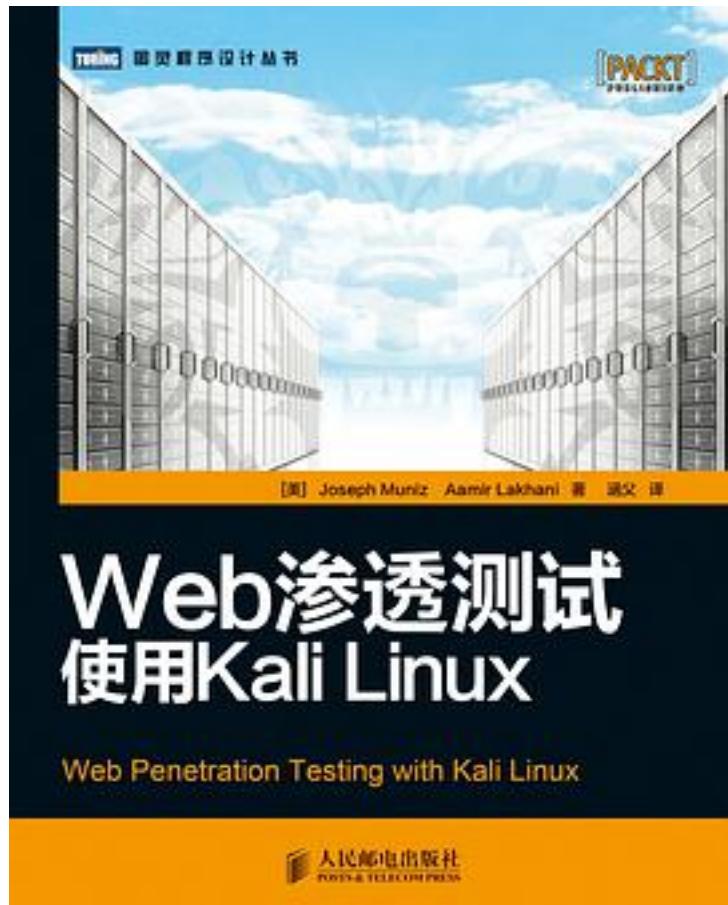


# Web渗透测试



[Web渗透测试 下载链接1](#)

著者:[美] Joseph Muniz

出版者:人民邮电出版社

出版时间:2014-8

装帧:平装

isbn:9787115363152

Kali

Linux是专业的渗透测试和安全审计工具，是世界上最流行的开源渗透工具包BackTrack的继任者。本书将教会读者怎样像真实的攻击者一样思考，以及理解他们如何利用系统和发现漏洞。

现实当中，就算你在极为安全的环境中开发Web应用，而且也有入侵检测系统和防火墙的保护，但要上线总得有一个对外开放的端口吧。这些端口在潜在攻击者眼里，就如同敞开的大门。因此，Web应用测试中绝不能缺少渗透测试这一环。本书是市面上第一本全面深入讲解Kali Linux工具包的专著，它注重实战、通俗易懂，强调换位思考，主张积极防御，是学习Kali Linux与渗透测试的必读之作。

本书作者均为国际知名的安全专家，其中Aamir Lakhani曾被《福布斯》杂志直言不讳地称为“间谍、超级英雄”，也是他们推荐的最值得关注的“46位美国联邦技术专家”之一。Joseph Muniz同样长期从事安全工作，现任思科公司系统安全工程师，并经常为《渗透测试》杂志撰稿。

本书适合所有渗透测试及对Web应用安全感兴趣的读者，特别是想学习使用Kali Linux的人阅读参考。有BackTrack经验的读者也可以通过本书了解这两代工具包的差异，学习下一代渗透测试工具和技术。

## 本书内容

进行安全漏洞侦察，收集目标信息

发现服务器安全漏洞，利用其获得高级访问权限

使用Web应用协议利用基于客户端的系统

使用SQL和跨站脚本（XSS）攻击

通过会话劫持技术窃取身份认证

加强系统防护，阻止其他攻击者利用系统

生成渗透测试报告

学习专业渗透测试人员的技巧，了解行业内幕

## 作者介绍：

Joseph Muniz

思科公司系统安全工程师、顾问，《渗透测试》杂志（PenTest Magazine）撰稿人，曾在多家安全公司任技术解决方案架构师一职。Muniz专攻网络安全管理，不仅拥有30多项网络安全技术认证，而且具有丰富的财富500强及政府网络大型项目经验。另外，他还是各安全会议活跃的演讲人，维护着优秀安全与产品实现网站TheSecurityBlogger.com。

Aamir Lakhani

国际知名网络安全专家，被《福布斯》杂志直言不讳地称为“间谍、超级英雄”及最值得关注的“46位美国联邦技术专家”。他不仅为美国国防和情报机构设计进攻性防御机制，还帮助其他组织机构防御地下网络组织的渗透攻击，是网络防御、移动应用风险、恶意软件、高级持续性威胁（APT）研究以及暗安全方面项目以及详细结构设计的业内领导者。另外，他以笔名Dr.

Chaos维护着网络反间谍与网络安全技术博客DrChaos.com，还作为网络安全专家接受

了美国全国公共广播电台的采访。

目录: 第1章 渗透测试概要及环境配置 1

1.1 Web应用渗透测试基础 2

1.2 渗透测试方法 3

1.3 Kali渗透测试基础 8

1.3.1 第一步: 侦察 8

1.3.2 第二步: 目标测试 9

1.3.3 第三步: 漏洞利用 9

1.3.4 第四步: 提升权限 10

1.3.5 第五步: 保持访问 10

1.4 Kali Linux简介 11

1.5 Kali系统环境配置 11

1.5.1 从外部存储媒体上运行Kali Linux 12

1.5.2 安装Kali Linux 12

1.5.3 首次运行Kali Linux和VM映像文件 18

1.6 Kali工具集概述 18

1.7 小结 20

第2章 侦察 21

2.1 侦察的对象 21

2.2 初期研究 22

2.2.1 公司网站 22

2.2.2 Web历史归档网站 23

2.2.3 区域互联网注册管理机构 25

2.2.4 电子化数据收集、分析及检索 (EDGAR) 26

2.2.5 社交媒体资源 27

2.2.6 信任关系 27

2.2.7 招聘广告 27

2.2.8 位置 27

2.2.9 Shodan搜索引擎 28

2.2.10 Google Hacking 29

2.2.11 Google Hacking数据库 30

2.2.12 研究网络 33

2.2.13 Nmap 42

2.3 小结 53

第3章 服务器端攻击 54

3.1 漏洞评估 54

3.1.1 Webshag 55

3.1.2 Skipfish 58

3.1.3 ProxyStrike 60

3.1.4 Vega 63

3.1.5 Owasp-Zap 67

3.1.6 Websploit 73

3.2 漏洞利用 73

3.2.1 Metasploit 74

3.2.2 w3af 79

3.3 利用电子邮件系统的漏洞 82

3.4 暴力破解攻击 83

3.4.1 Hydra 84

3.4.2 DirBuster 86

3.4.3 WebSlayer 89

3.5 破解密码 95

3.6 中间人攻击 97

3.7 小结 101  
第4章 客户端攻击 102  
4.1 社会工程 102  
4.2 社会工程工具集 (SET) 103  
4.3 MITM代理服务器 115  
4.4 主机扫描 116  
4.5 获取和破解用户密码 122  
4.6 Kali中的密码破解工具 125  
4.6.1 Johnny 126  
4.6.2 hashcat和oclHashcat 129  
4.6.3 samdump2 130  
4.6.4 chntpw 131  
4.6.5 Ophcrack 133  
4.6.6 Crunch 136  
4.7 Kali中的其他可用工具 138  
4.7.1 Hash-identifier 138  
4.7.2 dictstat 138  
4.7.3 RainbowCrack (rcracki\_mt) 139  
4.7.4 findmyhash 140  
4.7.5 phrasendrescher 140  
4.7.6 CmosPwd 140  
4.7.7 creddump 140  
4.8 小结 141

第5章 身份认证攻击 142  
5.1 攻击会话管理 143  
5.2 劫持Web会话的cookie 145  
5.3 Web会话工具 146  
5.3.1 Firefox插件 146  
5.3.2 Firesheep (Firefox插件) 146  
5.3.3 Web Developer (Firefox插件) 146  
5.3.4 GreaseMonkey (Firefox插件) 147  
5.3.5 Cookie Injector (Firefox插件) 148  
5.3.6 Cookies Manager+ (Firefox插件) 149  
5.3.7 Cookie Cadger 150  
5.3.8 Wireshark 153  
5.3.9 Hamster和Ferret 156  
5.3.10 中间人攻击 (MITM) 158  
5.3.11 dsniff和arpspoof 158  
5.3.12 Ettercap 161  
5.3.13 Driftnet 163  
5.4 SQL注入 164  
5.5 跨站脚本 (XSS) 168  
5.6 测试跨站脚本 169  
5.7 XSS cookie盗取/身份认证劫持 170  
5.8 其他工具 171  
5.8.1 urlsnarf 171  
5.8.2 acccheck 173  
5.8.3 hexinject 173  
5.8.4 Patator 173  
5.8.5 DBPwAudit 173  
5.9 小结 173  
第6章 Web攻击 174  
6.1 浏览器漏洞利用框架 (BeEF) 174  
6.2 FoxyProxy (Firefox插件) 178

6.3 BURP代理	179
6.4 OWASP (ZAP)	186
6.5 SET密码收集	190
6.6 Fimap	194
6.7 拒绝服务攻击 (DoS)	195
6.7.1 THC-SSL-DOS	197
6.7.2 Scapy	198
6.7.3 Slowloris	200
6.8 低轨道离子加农炮 (LOIC)	202
6.9 其他工具	205
6.9.1 DNSChef	205
6.9.2 SniffJoke	205
6.9.3 Siege	206
6.9.4 Inundator	207
6.9.5 TCPReplay	207
6.10 小结	208
第7章 防御对策	209
7.1 测试你的防御系统	210
7.1.1 安全基线	210
7.1.2 STIG	211
7.1.3 补丁管理	211
7.1.4 密码策略	212
7.2 构建测试镜像环境	213
7.2.1 HTTrack	214
7.2.2 其他克隆工具	215
7.3 防御中间人攻击	215
7.4 防御拒绝服务攻击	218
7.5 防御针对Cookie的攻击	219
7.6 防御点击劫持	219
7.7 数字取证	220
7.7.1 Kali取证启动模式	221
7.7.2 dc3dd	223
7.7.3 Kali中的其他取证工具	225
7.8 小结	229
第8章 渗透测试执行报告	230
8.1 遵从规范	231
8.2 行业标准	232
8.3 专业服务	232
8.4 文档	233
8.5 报告格式	234
8.5.1 封面页	234
8.5.2 保密声明	234
8.5.3 文档控制	235
8.5.4 时间表	235
8.5.5 执行总结	236
8.5.6 方法论	237
8.5.7 详细测试流程	238
8.5.8 调查结果总结	239
8.5.9 漏洞	240
8.5.10 网络考虑的因素及建议	242
8.5.11 附录	243
8.5.12 术语表	244
8.6 工作说明书	244
8.6.1 外部渗透测试	245

- 8.6.2 工作说明书附加材料 246
- 8.7 Kali报表工具 247
- 8.7.1 Dradis 248
- 8.7.2 KeepNote 248
- 8.7.3 Maltego CaseFile 248
- 8.7.4 MagicTree 249
- 8.7.5 CutyCapt 249
- 8.7.6 报告样例 249
- 8.8 小结 257
- 索引 259
- • • • • (收起)

[Web渗透测试](#) [下载链接1](#)

## 标签

Web安全

安全

网络安全

渗透测试

信息安全

技术

工具书

计算机科学

## 评论

这本书的kali版本还是1.0，在信息安全领域，工具、方法、漏洞利用的信息写成书已经有些落伍，如果是翻译成中文，这个周期更长，也可以对比一下kali2.0，了解一下工具

的变迁。

---

思路很清晰，讲的也很好，看得出作者是个很厉害的安全行业从业人员。虽然说很多内容只是面上带过，但是也是诚意满满了。版本会过时，但思路永远是有启发的，相比一些以“干货和诚意”做卖点的国内相关书籍，我觉得这本做的更好。另外，为啥我觉得讲的不仅仅是Web方面的内容呢。

---

大多数IT人都应该看看的一本书。

---

书中讲了很多工具，可以当作参考书来看

---

[Web渗透测试 下载链接1](#)

## 书评

---

[Web渗透测试 下载链接1](#)