

# 《Kali Linux高级渗透测试》

## 图书基本信息

书名：《Kali Linux高级渗透测试》

13位ISBN编号：9787111536398

出版时间：2016-5

作者：（加）罗伯特W. 贝格斯（Robert W. Beggs）

页数：223

译者：蒋溢 马祥均 陈京浩 罗文俊 祝清意

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](http://www.tushu000.com)

# 《Kali Linux高级渗透测试》

## 内容概要

Kali Linux向专业的渗透测试和安全审计，集成了大量精心挑选的安全检测工具。

本书在Kali Linux平台上从攻击者的角度来审视网络框架，详细介绍攻击者“杀链”采取的具体步骤。本书旨在帮助你开发自己的方法和方式来进行有效渗透测试，深入理解黑客怎样攻击数据系统，进而了解怎样在漏洞被利用之前弥补漏洞。如果你是一名专业的安全工程师、渗透测试员，或者是对复杂的数据环境的安全感兴趣的人，那么这本书是为你准备的。

通过阅读本书，你将学到：

采用真正黑客所有效使用的方法来确保最有效的网络渗透测试

Kali Linux渗透测试的最优配置

使用隐形技术来逃避被测试网络的检测

识别网络中的隐形攻击

使用有线和无线网络以及Web服务来利用网络和数据系统

从目标系统识别和下载有价值的数据

保持访问被入侵系统

利用社会工程学入侵网络的最弱部分——终端用户

# 《Kali Linux高级渗透测试》

## 作者简介

罗伯特W.贝格斯 ( Robert W. Beggs ) 是Digital Defence公司的创始人和首席执行官，该公司专门从事信息安全事件的预防和处理。他拥有超过15年的安全业务技术管理经验，涉及有线和无线网络的渗透测试、事件响应、数据取证等内容。

罗伯特是一个资深的信息安全传播者，并且是多伦多地区安全大会 ( Toronto Area Security Klatch , TASK ) 的联合创始人之一，在北美多伦多地区安全大会是众所周知的、最大的独立 – 供应商安全用户群。他是部门安全会议 ( SecTor Security Conference ) 咨询委员会的成员，以及其他几个安全学术委员会的成员。他是一个热心的安全培训教师，他在加拿大几所大学教授研究生、本科生和继续教育学生的信息安全课程。

罗伯特拥有女王大学的计算机科学与技术MBA学位，同时是一个认证信息系统安全专家。

## 书籍目录

推荐序

作者简介

审校者简介

前言

第一部分 攻击者杀链

第1章 走进Kali Linux 2

1.1 Kali Linux 2

1.2 配置网络服务和安全通信 4

1.2.1 调整网络代理设置 5

1.2.2 使用安全Shell保护通信安全 6

1.3 更新Kali Linux 7

1.4 配置和自定义Kali Linux 9

1.4.1 重置超级用户密码 9

1.4.2 添加普通用户 10

1.4.3 加速Kali运行 10

1.4.4 与Microsoft Windows共享文件夹 11

1.4.5 用TrueCrypt创建加密文件夹 13

1.5 第三方应用程序的管理 17

1.5.1 安装第三方应用程序 17

1.5.2 作为普通用户运行第三方应用程序 18

1.6 渗透测试的有效管理 19

1.7 总结 21

第2章 确定目标——被动侦察 22

2.1 侦察的基本原则 22

2.2 开源情报 23

2.3 DNS侦察和路由映射 25

2.3.1 WHOIS 25

2.3.2 DNS侦察 26

2.3.3 映射路由到目标 29

2.4 获得用户信息 31

2.4.1 收集姓名和电子邮件地址 31

2.4.2 收集文件元数据 32

2.5 分析用户密码列表 34

2.6 小结 35

第3章 主动侦察和漏洞扫描 36

3.1 隐形扫描策略 37

3.1.1 调整源IP栈和工具识别设置 37

3.1.2 修改数据包参数 38

3.1.3 使用匿名网络代理（Tor和Privoxy） 39

3.2 识别网络基础设施 42

3.3 枚举主机 43

3.4 端口、操作系统和发现服务 44

3.4.1 端口扫描 44

3.4.2 指纹识别操作系统 45

3.4.3 确定主动服务 46

3.5 采用综合侦察应用 47

3.5.1 nmap 47

- 3.5.2 recon-ng框架 49
- 3.5.3 Maltego 51
- 3.6 漏洞扫描 52
- 3.7 小结 53
- 第4章 漏洞利用 54
  - 4.1 威胁建模 55
  - 4.2 使用在线和本地漏洞资源 56
    - 4.2.1 Metasploit框架 59
    - 4.2.2 利用易受攻击的应用程序 63
  - 4.3 使用Armitage的多目标渗透 64
    - 4.3.1 Armitage 测试团队 66
    - 4.3.2 Armitage攻击脚本 66
  - 4.4 绕过IDS与反病毒侦测 67
  - 4.5 小结 73
- 第5章 后期利用——行动的目的 74
  - 5.1 绕过Windows用户账户控制 75
  - 5.2 对已入侵的系统进行快速侦察 77
  - 5.3 找到并提取敏感数据——掠夺目标 80
  - 5.4 创建附加账户 83
  - 5.5 使用Metasploit工具进行后期渗透活动 84
  - 5.6 在已入侵主机上提升用户权限 87
  - 5.7 使用incognito重放身份验证令牌 88
    - 5.7.1 使用Windows凭据编辑器操作访问凭据 89
    - 5.7.2 从管理员升级到系统管理员 90
  - 5.8 访问新账户实现横向升级 90
  - 5.9 消除痕迹 91
  - 5.10 小结 93
- 第6章 后期利用——持久性 94
  - 6.1 破解现有的系统和应用程序文件进行远程访问 95
    - 6.1.1 启用远程服务 95
    - 6.1.2 启用远程Windows终端服务 96
    - 6.1.3 启用远程虚拟网络计算 97
  - 6.2 使用持久代理 98
  - 6.3 使用Metasploit框架保持持久性 101
    - 6.3.1 使用metsvc脚本 101
    - 6.3.2 使用persistence脚本 103
  - 6.4 使用Metasploit框架创建一个独立持久代理 104
  - 6.5 重定向端口来绕过网络控制 106
    - 6.5.1 示例1——简单端口重定向 106
    - 6.5.2 示例2——双向端口重定向 107
  - 6.6 小结 107
- 第二部分 交付阶段
- 第7章 物理攻击与社会工程学 110
  - 7.1 社会工程工具包 111
    - 7.1.1 网络钓鱼攻击曝光 113
    - 7.1.2 使用网站攻击向量——Java小程序攻击方法 118
    - 7.1.3 使用网站攻击向量——凭据收割攻击方法 121
    - 7.1.4 使用网站攻击向量——标签钓鱼攻击方法 123
    - 7.1.5 使用网站攻击向量——综合攻击网页方法 124

7.2 使用PowerShell字母数字的shellcode注入攻击曝光 125

7.3 隐藏可执行文件与伪装攻击者的URL 126

7.4 使用DNS重定向攻击的升级攻击 127

7.5 物理访问与敌对设备 130

7.6 小结 133

第8章 利用无线通信 134

8.1 配置Kali实现无线攻击曝光 134

8.2 无线侦察 135

8.3 绕过一个隐藏的服务集标识符 138

8.4 绕过MAC地址验证 140

8.5 破解WEP加密 142

8.6 攻击WPA和WPA2 146

8.6.1 暴力攻击曝光 146

8.6.2 使用Reaver攻击无线路由器曝光 149

8.7 克隆接入点 149

8.8 拒绝服务攻击曝光 150

8.9 小结 151

第9章 基于Web应用的侦察与利用 153

9.1 对网站进行侦察 154

9.2 漏洞扫描器 158

9.2.1 扩展传统漏洞扫描器功能 158

9.2.2 扩展Web浏览器功能 159

9.2.3 具体网络服务的漏洞扫描器 160

9.3 使用客户端代理测试安全性 163

9.4 服务器漏洞 167

9.5 针对特定应用的攻击 168

9.5.1 暴力破解访问证书 169

9.5.2 数据库注入攻击曝光 169

9.6 使用网站后门维持访问 171

9.7 小结 172

第10章 利用远程访问通信 174

10.1 利用操作系统通信协议 175

10.1.1 破解远程桌面协议 175

10.1.2 破解安全外壳 177

10.2 利用第三方远程访问应用程序 179

10.3 攻击安全套接字层 180

10.3.1 为SSLv2扫描配置Kali 181

10.3.2 SSL连接的侦察 182

10.3.3 使用sslstrip进行中间人攻击曝光 186

10.3.4 针对SSL的拒绝服务攻击曝光 188

10.4 攻击IPSec虚拟专用网络 188

10.4.1 扫描VPN网关 189

10.4.2 指纹识别VPN网关 190

10.4.3 截获预共享密钥 191

10.4.4 执行离线PSK破解 191

10.4.5 确定默认用户账户 192

10.5 小结 192

第11章 客户端攻击技术详解 193

11.1 使用恶意脚本攻击系统曝光 193

- 11.1.1 使用VBScript进行攻击曝光 194
- 11.1.2 使用Windows PowerShell攻击系统曝光 196
- 11.2 跨站点脚本框架 198
- 11.3 浏览器开发框架——BeEF 204
- 11.4 BeEF浏览器的演练 206
  - 11.4.1 整合BeEF和Metasploit攻击 210
  - 11.4.2 用BeEF作为隧道代理 211
- 11.5 小结 213
- 附录 安装Kali Linux 214

# 《Kali Linux高级渗透测试》

## 精彩短评

- 1、内容不错，提纲挈领，系统性地讲述部分工具的应用。书总共两百来页，定价有点虚高了。
- 2、客观的说~作者还真是低估黑客了呢~



# 《Kali Linux高级渗透测试》

## 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](http://www.tushu000.com)