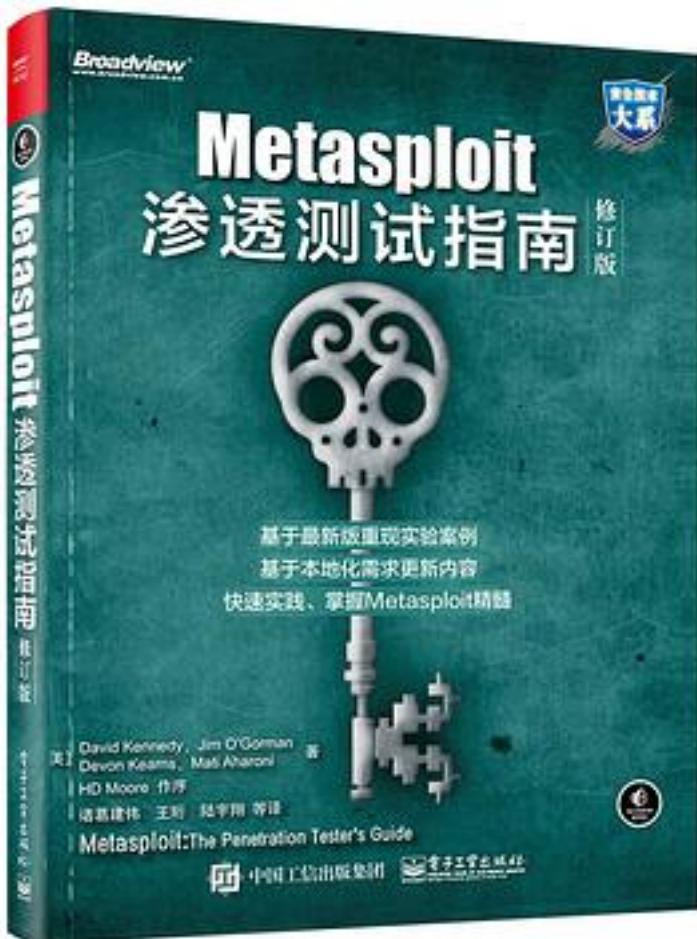


# Metasploit渗透测试指南（修订版）



[Metasploit渗透测试指南（修订版）\\_下载链接1](#)

著者:【美】 David Kennedy (戴维·肯尼) 等

出版者:电子工业出版社

出版时间:2017-7

装帧:平装

isbn:9787121318252

《Metasploit渗透测试指南（修订版）》介绍开源渗透测试框架平台软件Metasploit，以及基于Metasploit进行网络渗透测试与安全漏洞研究分析的技术、流程和方法，帮助初学者从零开始建立

作为渗透测试者的基本技能，也为职业的渗透测试工程师提供一本参考索引。

《Metasploit渗透测试指南（修订版）》分为17章，覆盖渗透测试的情报搜集、威胁建模、漏洞分析、渗透攻击和后渗透攻击各个环节，并包含了免杀技术、客户端渗透攻击、社会工程学、自动化渗透测试、无线网络攻击等高级技术专题，以及如何扩展Metasploit情报搜集、渗透攻击与后渗透攻击功能的实践方法。此修订版尽量保持原著的实验案例选择，仅根据Metasploit版本更新的实际情况来复现实验，同步更新操作流程的命令输入和输出结果。对于少量国内读者不便重现的实验案例，将实验对象、分析工具等替换为更容易接触和使用的替代品。

《Metasploit渗透测试指南（修订版）》的读者群主要是网络与系统安全领域的技术爱好者与学生，以及渗透测试与漏洞分析研究方面的安全从业人员。

作者介绍：

## 目录: 第1章 渗透测试技术基础 1

1.1 PTES 中的渗透测试阶段 2

1.1.1 前期交互阶段 2

1.1.2 情报搜集阶段 2

1.1.3 威胁建模阶段 3

1.1.4 漏洞分析阶段 3

1.1.5 渗透攻击阶段 3

1.1.6 后渗透攻击阶段 3

1.1.7 报告阶段 4

1.2 渗透测试类型 4

1.2.1 白盒测试 5

1.2.2 黑盒测试 5

1.2.3 灰盒测试 5

1.3 漏洞扫描器 6

1.4 小结 6

## 第2章 Metasploit 基础 7

2.1 专业术语 7

2.1.1 渗透攻击 (Exploit) 8

2.1.2 攻击载荷 (Payload) 8

2.1.3 Shellcode 8

2.1.4 模块 (Module) 8

2.1.5 监听器 (Listener) 8

2.2 Metasploit 用户接口 8

2.2.1 MSF 终端 9

2.2.2 MSF 命令行 9

2.2.3 Armitage 10

2.3 Metasploit 功能程序 11

2.3.1 MSF 攻击载荷生成器 11

2.3.2 MSF 编码器 12

2.3.3 Nasm Shell 13

2.4 Metasploit Express 和 Metasploit Pro 13

2.5 小结 14

## 第3章 情报搜集 15

3.1 被动信息搜集 16

3.1.1 Whois 查询 16

3.1.2 Netcraft	17
3.1.3 nslookup	18
3.1.4 Google Hacking	18
3.2 主动信息搜集	20
3.2.1 使用Nmap 进行端口扫描	20
3.2.2 在Metasploit 中使用数据库	22
3.2.3 使用Metasploit 进行端口扫描	27
3.3 针对性扫描	28
3.3.1 服务器消息块协议扫描	28
3.3.2 搜寻配置不当的Microsoft SQL Server	29
3.3.3 SSH 服务器扫描	30
3.3.4 FTP 扫描	30
3.3.5 简单网管协议扫描	31
3.4 编写自己的扫描器	33
3.5 展望	35
第4章 漏洞扫描	36
4.1 基本的漏洞扫描	37
4.2 使用Nexpose 进行扫描	38
4.2.1 配置	38
4.2.2 将扫描报告导入到Metasploit 中	44
4.2.3 在MSF 控制台中运行Nexpose	44
4.3 使用Nessus 进行扫描	46
4.3.1 配置Nessus	46
4.3.2 创建Nessus 扫描策略	47
4.3.3 执行Nessus 扫描	49
4.3.4 Nessus 报告	50
4.3.5 将扫描结果导入Metasploit 框架中	50
4.3.6 在Metasploit 内部使用Nessus 进行扫描	52
4.4 专用漏洞扫描器	54
4.4.1 验证SMB 登录	54
4.4.2 扫描开放的VNC 空口令	56
4.4.3 扫描开放的X11 服务器	58
4.5 利用扫描结果进行自动化攻击	59
第5章 渗透攻击之旅	65
5.1 渗透攻击基础	66
5.1.1 msf> show exploits	66
5.1.2 msf> show auxiliary	66
5.1.3 msf> show options	66
5.1.4 msf> show payloads	68
5.1.5 msf> show targets	70
5.1.6 info	71
5.1.7 set 和unset	71
5.1.8 setg 和unsetg	72
5.1.9 save	72
5.2 你的第一次渗透攻击	72
5.3 攻击Metasploitable 主机	76
5.4 全端口攻击载荷：暴力猜解目标开放的端口	79
5.5 资源文件	80
5.6 小结	82
第6章 Meterpreter	83
6.1 攻陷Windows XP 虚拟机	83
6.1.1 使用nmap 扫描端口	84
6.1.2 攻击MS SQL	84
6.1.3 暴力破解MS SQL 服务	86

6.1.4 xp_cmdshell	87
6.1.5 Meterpreter 基本命令	88
6.1.6 获取键盘记录	89
6.2 挖掘用户名和密码	90
6.2.1 提取密码哈希值	90
6.2.2 使用Meterpreter 命令获取密码哈希值	91
6.3 传递哈希值	92
6.4 权限提升	93
6.5 令牌假冒	95
6.6 使用PS	95
6.7 通过跳板攻击其他机器	97
6.7.1 使用Meterpreter 进行跳板攻击	97
6.7.2 使用Metasploit Pro 的VPN 跳板	100
6.8 使用Meterpreter 脚本	105
6.8.1 迁移进程	105
6.8.2 关闭杀毒软件	106
6.8.3 获取系统密码哈希值	106
6.8.4 查看目标机上的所有流量	106
6.8.5 攫取系统信息	107
6.8.6 控制持久化	107
6.9 向后渗透攻击模块转变	108
6.10 将命令行shell 升级为Meterpreter	109
6.11 通过附加的Railgun 组件操作Windows API	110
6.12 小结	110
第7章 免杀技术	112
7.1 使用MSF 攻击载荷生成器创建可独立运行的二进制文件	113
7.2 躲避杀毒软件的检测	114
7.2.1 使用MSF 编码器	114
7.2.2 多重编码	117
7.3 自定义可执行文件模板	118
7.4 隐秘地启动一个攻击载荷	120
7.5 加壳软件	122
7.6 使用Metasploit Pro 的动态载荷实现免杀	123
7.7 关于免杀处理的最后忠告	126
第8章 客户端渗透攻击	127
8.1 基于浏览器的渗透攻击	128
8.1.1 基于浏览器的渗透攻击原理	128
8.1.2 关于空指令	129
8.2 使用ollydbg 调试器揭秘空指令机器码	130
8.3 对IE 浏览器的极光漏洞进行渗透利用	134
8.4 文件格式漏洞渗透攻击	137
8.5 发送攻击负载	139
8.6 小结	140
第9章 Metasploit 辅助模块	141
9.1 使用辅助模块	144
9.2 辅助模块剖析	146
9.3 展望	152
第10章 社会工程学工具包	153
10.1 配置SET 工具包	154
10.2 针对性钓鱼攻击向量	155
10.3 Web 攻击向量	160
10.3.1 Java Applet	160
10.3.2 客户端Web 攻击	165
10.3.3 用户名和密码获取	167

10.3.4 标签页劫持攻击 (Tabnabbing)	169
10.3.5 中间人攻击	169
10.3.6 网页劫持	169
10.3.7 综合多重攻击方法	171
10.4 传染性媒体生成器	176
10.5 USB HID 攻击向量	177
10.6 SET 的其他特性	181
10.7 展望	181
第11章 Fast-Track	183
11.1 Microsoft SQL 注入	184
11.1.1 SQL 注入——查询语句攻击	185
11.1.2 SQL 注入——POST 参数攻击	186
11.1.3 手工注入	187
11.1.4 MS SQL 破解	188
11.1.5 通过SQL 自动获得控制 (SQL Pwnage)	192
11.2 二进制到十六进制转换器	194
11.3 大规模客户端攻击	195
11.4 对自动化渗透的一点看法	197
第12章 Karmetasploit 无线攻击套件	198
12.1 配置	199
12.2 开始攻击	200
12.3 获取凭证	203
12.4 得到Shell	203
12.5 小结	206
第13章 编写你自己的模块	207
13.1 在MS SQL 上进行命令执行	208
13.2 探索一个已存在的Metasploit 模块	209
13.3 编写一个新的模块	211
13.3.1 PowerShell	211
13.3.2 运行Shell 渗透攻击	213
13.3.3 编写Powershell_upload_exec 函数	215
13.3.4 从十六进制转换回二进制程序	215
13.3.5 计数器	217
13.3.6 运行渗透攻击模块	218
13.4 小结——代码重用的能量	219
第14章 创建你自己的渗透攻击模块	220
14.1 Fuzz 测试的艺术	221
14.2 控制结构化异常处理链	225
14.3 绕过SEH 限制	227
14.4 获取返回地址	230
14.5 壳字符和远程代码执行	235
14.6 小结	238
第15章 将渗透代码移植到Metasploit	239
15.1 汇编语言基础	240
15.1.1 EIP 和ESP 寄存器	240
15.1.2 JMP 指令集	240
15.1.3 空指令和空指令滑行区	240
15.2 移植一个缓冲区溢出攻击代码	240
15.2.1 裁剪一个已有的渗透攻击代码	242
15.2.2 构造渗透攻击过程	243
15.2.3 测试我们的基础渗透代码	244
15.2.4 实现框架中的特性	245
15.2.5 增加随机化	246
15.2.6 消除空指令滑行区	247

15.2.7 去除伪造的Shellcode	247
15.2.8 我们完整的模块代码	249
15.3 SEH 覆盖渗透代码	250
15.4 小结	257
第16章 Meterpreter 脚本编程	258
16.1 Meterpreter 脚本编程基础	258
16.2 Meterpreter API	265
16.2.1 打印输出	265
16.2.2 基本API 调用	266
16.2.3 Meterpreter Mixins	266
16.3 编写Meterpreter 脚本的规则	267
16.4 创建自己的Meterpreter 脚本	268
16.5 小结	275
第17章 一次模拟的渗透测试过程	276
17.1 前期交互	277
17.2 情报搜集	277
17.3 威胁建模	278
17.4 渗透攻击	280
17.5 MSF 终端中的渗透攻击过程	280
17.6 后渗透攻击	281
17.6.1 扫描Metasploitable 靶机	282
17.6.2 识别存有漏洞的服务	284
17.7 攻击Postgresql 数据库服务	286
17.8 攻击一个偏门的服务	288
17.9 隐藏你的踪迹	289
17.10 小结	291
附录A 配置目标机器	293
附录B 命令参考列表	301
· · · · · (收起)	

[Metasploit渗透测试指南（修订版）](#) [\[下载链接1\]](#)

## 标签

安全

黑客

信息安全

计算机

## 评论

怎么这本2017年出的书到现在一个短评也没有？总的来说很基础，但也涉及到不少高级的技巧比如调试，比如编写meterpreter脚本，比如创建自己的模块并移植到msf，这几章要求有ruby和汇编基础。好书就是这样的由浅入深。因为主要内容都是2011年的东西所以即便修订了一次，还是有不少内容还是过时了。这本书是由offsite security几位大神写的，也就是kali的核心团队。HD more (msf创始人) 作序，真是经典啊惭愧今天才拜读

---

[Metasploit渗透测试指南（修订版）](#) [下载链接1](#)

## 书评

以往对MSF的使用，全来自网上一篇一篇的教程或入侵实例，偶尔翻翻一个英文的pdf文档。从《程序员》杂志看到了这篇杂志的节选，从而认识了这本书。觉得优点在于1.中文。2.全面。3.详细———这是一本好的说明书和入门指南

---

大家好，我是这本书的主要翻译者之一。这本书对研究计算机和网络安全，进行渗透测试和风险评估是有很大帮助的，目前metasploit的更新的速度也是非常快的，如果大家有什么新的问题，欢迎提出来，我们会尽量解决。  
同时欢迎大家在阅读此书的同时，提出自己宝贵的建议和意见并反馈...

---

一直在读这本书，整体感觉很好，说不上来到底好在哪里，但是每次阅读总能发现点以往没注意到的东西，我对书的观念就是“一本好书它不在于价格的高低，不在于阅读人数的多少，而在于每次阅读时是否能带给你不一样的东西！”恰巧这本书做到了，所以我推荐大家一起来阅读以下吧。

---

[Metasploit渗透测试指南（修订版）](#) [下载链接1](#)