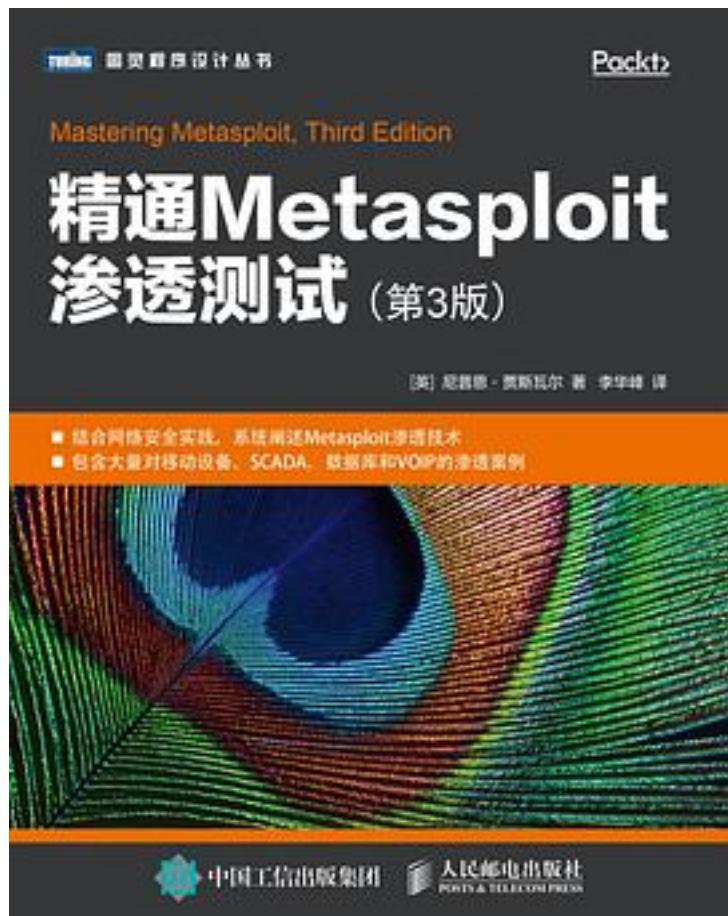


# 精通Metasploit渗透测试（第3版）



[精通Metasploit渗透测试（第3版）](#) [下载链接1](#)

著者:[英] 尼普恩·贾斯瓦尔

出版者:人民邮电出版社

出版时间:2019-6

装帧:平装

isbn:9787115511904

本书是Metasploit 渗透测试的权威指南，涵盖了使用Metasploit 实现渗透测试的诸多方面，主要包括：渗透测试的基础知识，编写自定义渗透测试框架，开发渗透模块，移植渗透模块，测试服务，虚拟化测试，客户端渗透，Metasploit 中的扩展功能、规避技术和“特工”技术，Metasploit

的可视化管理，以及加速渗透测试和高效使用Metasploit的各种技巧。

作者介绍：

尼普恩·贾斯瓦尔 (Nipun Jaswal)

信息安全专家、IT安全研究人员，在渗透测试、漏洞研究、监控解决方案等网络安全方面拥有10年专业经验。目前在Lucideus公司负责红队和漏洞研究服务以及其他企业客户服务。曾在Eforensics、Hakin9和Security Kaizen等著名安全杂志上发表过大量关于IT安全的文章，曾为Apple、Microsoft、AT&T等公司进行漏洞发掘。

目录: 第1章 走近Metasploit渗透测试框架 1

1.1 组织一次渗透测试 3

1.1.1 前期交互阶段 3

1.1.2 信息收集/侦查阶段 4

1.1.3 威胁建模阶段 6

1.1.4 漏洞分析阶段 7

1.1.5 渗透攻击阶段和后渗透攻击阶段 7

1.1.6 报告阶段 7

1.2 工作环境的准备 7

1.3 Metasploit基础 11

1.4 使用Metasploit进行渗透测试 12

1.5 使用Metasploit进行渗透测试的优势 14

1.5.1 源代码的开放性 14

1.5.2 对大型网络测试的支持以及便利的命名规则 14

1.5.3 灵活的攻击载荷模块生成和切换机制 15

1.5.4 干净的通道建立方式 15

1.5.5 图形化管理界面 15

1.6 案例研究：渗透进入一个未知网络 15

1.6.1 信息收集 16

1.6.2 威胁建模 21

1.6.3 漏洞分析——任意文件上传（未验证） 22

1.6.4 渗透与控制 23

1.6.5 使用Metasploit保持控制权限 30

1.6.6 后渗透测试模块与跳板功能 32

1.6.7 漏洞分析——基于SEH的缓冲区溢出 37

1.6.8 利用人为疏忽来获得密码 38

1.7 案例研究回顾 41

1.8 小结与练习 43

第2章 打造定制化的Metasploit渗透测试框架 45

2.1 Ruby——Metasploit的核心 46

2.1.1 创建你的第一个Ruby程序 46

2.1.2 Ruby中的变量和数据类型 47

2.1.3 Ruby中的方法 51

2.1.4 决策运算符 51

2.1.5 Ruby中的循环 52

2.1.6 正则表达式 53

2.1.7 Ruby基础知识小结 54

2.2 开发自定义模块 54

2.2.1 模块编写的概要 54

2.2.2 了解现有模块 58

2.2.3 分解已有的HTTP服务器扫描模块	59
2.2.4 编写一个自定义FTP扫描程序模块	63
2.2.5 编写一个自定义的SSH认证暴力破解器	67
2.2.6 编写一个让硬盘失效的后渗透模块	70
2.2.7 编写一个收集登录凭证的后渗透模块	75
2.3 突破Meterpreter脚本	80
2.3.1 Meterpreter脚本的要点	80
2.3.2 设置永久访问权限	80
2.3.3 API调用和 mixin类	81
2.3.4 制作自定义Meterpreter脚本	81
2.4 与RailGun协同工作	84
2.4.1 交互式Ruby命令行基础	84
2.4.2 了解RailGun及其脚本编写	84
2.4.3 控制Windows中的API调用	86
2.4.4 构建复杂的RailGun脚本	86
2.5 小结与练习	89
第3章 渗透模块的开发过程	90
3.1 渗透的最基础部分	90
3.1.1 基础部分	90
3.1.2 计算机架构	91
3.1.3 寄存器	92
3.2 使用Metasploit实现对栈的缓冲区溢出	93
3.2.1 使一个有漏洞的程序崩溃	93
3.2.2 构建渗透模块的基础	95
3.2.3 计算偏移量	96
3.2.4 查找JMP ESP地址	97
3.2.5 填充空间	99
3.2.6 确定坏字符	100
3.2.7 确定空间限制	101
3.2.8 编写Metasploit的渗透模块	101
3.3 使用Metasploit实现基于SEH的缓冲区溢出	104
3.3.1 构建渗透模块的基础	107
3.3.2 计算偏移量	107
3.3.3 查找POP/POP/RET地址	108
3.3.4 编写Metasploit的SEH渗透模块	110
3.4 在Metasploit模块中绕过DEP	113
3.4.1 使用msfrop查找ROP指令片段	115
3.4.2 使用Mona创建ROP链	116
3.4.3 编写绕过DEP的Metasploit渗透模块	117
3.5 其他保护机制	120
3.6 小结与练习	120
第4章 渗透模块的移植	121
4.1 导入一个基于栈的缓冲区溢出渗透模块	121
4.1.1 收集关键信息	123
4.1.2 构建Metasploit模块	124
4.1.3 使用Metasploit完成对目标应用程序的渗透	126
4.1.4 在Metasploit的渗透模块中实现一个检查方法	126
4.2 将基于Web的RCE导入Metasploit	127
4.2.1 收集关键信息	128
4.2.2 掌握重要的Web函数	128
4.2.3 GET/POST方法的使用要点	130
4.2.4 将HTTP渗透模块导入到Metasploit中	130
4.3 将TCP服务端/基于浏览器的渗透模块导入Metasploit	133
4.3.1 收集关键信息	134

4.3.2 创建Metasploit模块 135

4.4 小结与练习 137

第5章 使用Metasploit对服务进行测试 138

5.1 SCADA系统测试的基本原理 138

5.1.1 ICS的基本原理以及组成部分 138

5.1.2 ICS-SCADA安全的重要性 139

5.1.3 对SCADA系统的HMI进行渗透 139

5.1.4 攻击Modbus协议 142

5.1.5 使SCADA变得更加安全 146

5.2 数据库渗透 146

5.2.1 SQL Server 147

5.2.2 使用Metasploit的模块进行扫描 147

5.2.3 暴力破解密码 147

5.2.4 查找/捕获服务器的密码 149

5.2.5 浏览SQL Server 149

5.2.6 后渗透/执行系统命令 151

5.3 VOIP渗透测试 153

5.3.1 VOIP的基本原理 153

5.3.2 对VOIP服务踩点 155

5.3.3 扫描VOIP服务 156

5.3.4 欺骗性的VOIP电话 157

5.3.5 对VOIP进行渗透 158

5.4 小结与练习 160

第6章 虚拟化测试的原因及阶段 161

6.1 使用Metasploit集成的服务完成一次渗透测试 161

6.1.1 与员工和最终用户进行交流 162

6.1.2 收集信息 163

6.1.3 使用Metasploit中的OpenVAS插件进行漏洞扫描 164

6.1.4 对威胁区域进行建模 168

6.1.5 获取目标的控制权限 169

6.1.6 使用Metasploit完成对Active Directory的渗透 170

6.1.7 获取Active Directory的持久访问权限 181

6.2 手动创建报告 182

6.2.1 报告的格式 182

6.2.2 执行摘要 183

6.2.3 管理员级别的报告 184

6.2.4 附加部分 184

6.3 小结 184

第7章 客户端渗透 185

7.1 有趣又有料的浏览器渗透攻击 185

7.1.1 browser autopwn攻击 186

7.1.2 对网站的客户进行渗透 188

7.1.3 与DNS欺骗和MITM结合的browser autopwn攻击 191

7.2 Metasploit和Arduino——“致命”搭档 199

7.3 基于各种文件格式的渗透攻击 204

7.3.1 基于PDF文件格式的渗透攻击 204

7.3.2 基于Word文件格式的渗透攻击 205

7.4 使用Metasploit攻击Android系统 208

7.5 小结与练习 212

第8章 Metasploit的扩展功能 213

8.1 Metasploit后渗透模块的基础知识 213

8.2 基本后渗透命令 213

8.2.1 帮助菜单 213

8.2.2 后台命令 214

8.2.3 通信信道的操作	215
8.2.4 文件操作命令	215
8.2.5 桌面命令	216
8.2.6 截图和摄像头列举	217
8.3 使用Metasploit中的高级后渗透模块	220
8.3.1 获取系统级管理权限	220
8.3.2 使用timestamp修改文件的访问时间、修改时间和创建时间	220
8.4 其他后渗透模块	221
8.4.1 使用Metasploit收集无线SSID信息	221
8.4.2 使用Metasploit收集Wi-Fi密码	221
8.4.3 获取应用程序列表	222
8.4.4 获取Skype密码	223
8.4.5 获取USB使用历史信息	223
8.4.6 使用Metasploit查找文件	223
8.4.7 使用clearev命令清除目标系统上的日志	224
8.5 Metasploit中的高级扩展功能	224
8.5.1 pushm和popm命令的使用方法	225
8.5.2 使用reload、edit和reload_all命令加快开发过程	226
8.5.3 资源脚本的使用方法	226
8.5.4 在Metasploit中使用AutoRunScript	227
8.5.5 使用AutoRunScript选项中的multiscript模块	229
8.5.6 用Metasploit提升权限	231
8.5.7 使用mimikatz查找明文密码	233
8.5.8 使用Metasploit进行流量嗅探	233
8.5.9 使用Metasploit对host文件进行注入	234
8.5.10 登录密码的钓鱼窗口	235
8.6 小结与练习	236
第9章 Metasploit中的规避技术	237
9.1 使用C wrapper和自定义编码器来规避Meterpreter	237
9.2 使用Metasploit规避入侵检测系统	246
9.2.1 通过一个随机案例边玩边学	247
9.2.2 利用伪造的目录关系来欺骗IDS	248
9.3 规避Windows防火墙的端口阻塞机制	249
9.4 小结	253
第10章 Metasploit中的“特工”技术	254
10.1 在Meterpreter会话中保持匿名	254
10.2 使用通用软件中的漏洞维持访问权限	256
10.2.1 DLL加载顺序劫持	256
10.2.2 利用代码打洞技术来隐藏后门程序	260
10.3 从目标系统获取文件	262
10.4 使用venom实现代码混淆	262
10.5 使用反取证模块来消除入侵痕迹	265
10.6 小结	268
第11章 利用Armitage实现Metasploit的可视化管理	270
11.1 Armitage的基本原理	270
11.1.1 入门知识	270
11.1.2 用户界面一览	272
11.1.3 工作区的管理	273
11.2 网络扫描以及主机管理	274
11.2.1 漏洞的建模	275
11.2.2 查找匹配模块	275
11.3 使用Armitage进行渗透	276
11.4 使用Armitage进行后渗透攻击	277
11.5 使用团队服务器实现红队协同工作	278

11.6 Armitage脚本编写 282  
11.6.1 Cortana基础知识 282  
11.6.2 控制Metasploit 285  
11.6.3 使用Cortana实现后渗透攻击 286  
11.6.4 使用Cortana创建自定义菜单 287  
11.6.5 界面的使用 289  
11.7 小结 290  
第12章 技巧与窍门 291  
12.1 使用Minion脚本实现自动化 291  
12.2 用connect代替Netcat 293  
12.3 shell升级与后台切换 294  
12.4 命名约定 294  
12.5 在Metasploit中保存配置 295  
12.6 使用内联handler以及重命名任务 296  
12.7 在多个Meterpreter上运行命令 297  
12.8 社会工程学工具包的自动化 297  
12.9 Metasploit和渗透测试速查手册 299  
12.10 延伸阅读 300  
• • • • • (收起)

[精通Metasploit渗透测试（第3版）](#) [下载链接1](#)

## 标签

渗透测试

## 评论

行业必读书，读完之后受益匪浅，还有再读两遍的冲动

[精通Metasploit渗透测试（第3版）](#) [下载链接1](#)

## 书评

[精通Metasploit渗透测试（第3版）](#) [下载链接1](#)