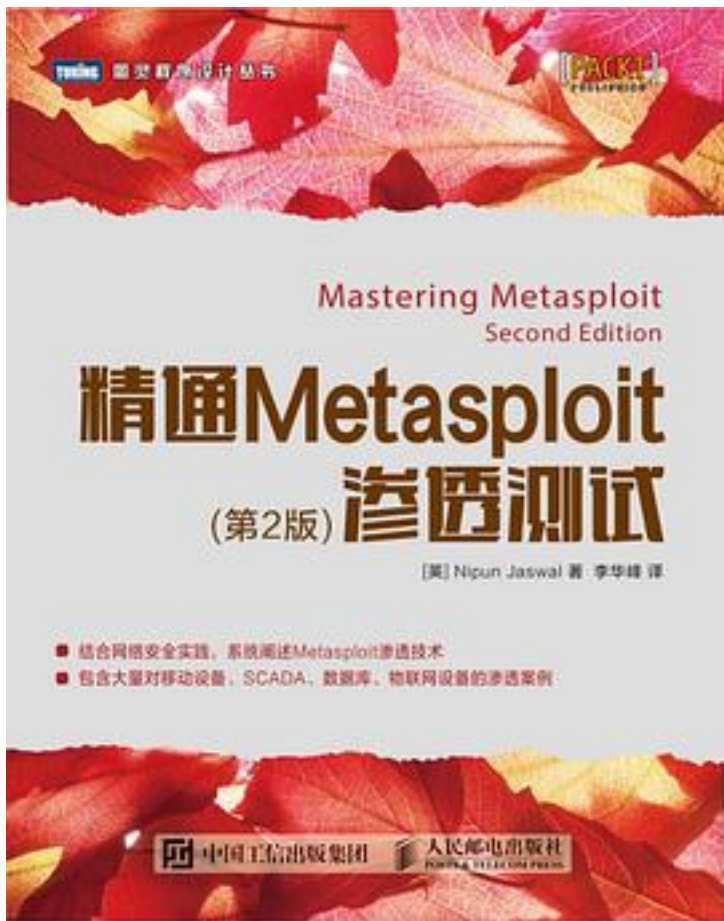


精通Metasploit渗透测试（第2版）



[精通Metasploit渗透测试（第2版）_下载链接1](#)

著者:[英] Nipun Jaswal

出版者:人民邮电出版社

出版时间:2017-10

装帧:平装

isbn:9787115469403

本书介绍了时下流行的渗透测试框架——Metasploit。书中从其基本功能和传统使用方式开始，讲解编写Metasploit模块的基础知识，学习渗透模块的执行、构建与移植，详细解读客户端攻击、Metasploit框架中的各种内置脚本。

与第1版相比，第2版增添了大量对移动设备、SCADA、数据库、物联网设备的渗透案例，并讲解了如何将全新的渗透模块导入到Metasploit。此外，还新增了大量优秀的出色工具的使用教程，采用了新版的社会工程学工具包，增加了大量经典详实的渗透模块编写实例。

作者介绍:

作者简介:

Nipun Jaswal

IT安全业务践行者，充满激情的IT安全研究人员。拥有7年专业经验，IT安全测试技能娴熟。曾在Eforensics、Hakin9和Security Kaizen等著名安全杂志上发表过大量关于IT安全文章，并因为Apple、Microsoft、AT&T、Offensive Security、Rapid7、Blackberry、Nokia、Zynga.com等知名公司进行漏洞发掘而为人熟知。邮箱地址：mail@nipunjaswal.info。

译者简介:

李华峰

信息安全顾问、自由撰稿人。从事网络安全研究与教学多年，在网络安全部署、网络渗透测试、社会工程学等方面有十分丰富的实践经验。目前已经出版《诸神之眼——Nmap网络安全审计技术揭秘》《机器人学经典教程》《精通Metasploit渗透测试（第1版）》等多本著作和译著。

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
- 1.2 前期交互阶段 3
- 1.3 信息收集/侦查阶段 5
- 1.4 了解测试环境 7
 - 1.4.1 威胁建模阶段 7
 - 1.4.2 漏洞分析阶段 8
 - 1.4.3 渗透阶段和后渗透阶段 8
 - 1.4.4 报告阶段 9
 - 1.4.5 工作环境的准备 9
- 1.5 在虚拟环境中安装Kali Linux 9
- 1.6 Metasploit基础 13
- 1.7 使用Metasploit进行渗透测试 14
- 1.8 使用Metasploit进行渗透测试的优势 15
 - 1.8.1 源代码的开放性 16
 - 1.8.2 对大型网络测试的支持以及便利的命名规则 16
 - 1.8.3 灵活的攻击载荷模块生成和切换机制 16
 - 1.8.4 干净的通道建立方式 16
 - 1.8.5 图形化管理界面 17
- 1.9 对未知网络的渗透测试 17
 - 1.9.1 假设 17
 - 1.9.2 信息收集 17
- 1.10 在Metasploit中使用数据库 18
- 1.11 威胁建模 20
- 1.12 VSFTPD 2.3.4后门的漏洞分析 21

1.12.1 攻击过程	22
1.12.2 漏洞渗透的过程	22
1.12.3 渗透模块和后渗透模块	23
1.13 PHP-CGI查询字符串参数漏洞的分析	29
1.14 HFS 2.3上的漏洞分析	34
1.15 渗透访问控制的持久化	37
1.16 清除渗透痕迹	38
1.17 回顾入侵过程	39
1.18 小结	41
第2章 打造定制化的Metasploit渗透测试框架	42
2.1 Ruby——Metasploit的核心	43
2.1.1 创建你的第一个Ruby程序	43
2.1.2 Ruby中的变量和数据类型	45
2.1.3 Ruby中的方法	48
2.1.4 决策运算符	49
2.1.5 Ruby中的循环	50
2.1.6 正则表达式	50
2.1.7 Ruby 基础知识小结	52
2.2 开发自定义模块	52
2.2.1 模块编写的概要	52
2.2.2 了解现有模块	57
2.2.3 分解已有的HTTP服务器扫描模块	58
2.2.4 编写一个自定义FTP扫描程序模块	62
2.2.5 编写一个自定义的SSH认证暴力破解器	65
2.2.6 编写一个让硬盘失效的后渗透模块	69
2.2.7 编写一个收集登录凭证的后渗透模块	73
2.3 突破Meterpreter脚本	77
2.3.1 Meterpreter脚本的要点	78
2.3.2 以被控制的计算机为跳板	78
2.3.3 设置永久访问权限	81
2.3.4 API 调用和mixins类	82
2.3.5 制作自定义Meterpreter脚本	83
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	85
2.4.3 控制Windows中的API调用	87
2.4.4 构建复杂的RailGun脚本	87
2.5 小结	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	94
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	98
3.2.5 填充空间	100
3.2.6 确定坏字符	102
3.2.7 确定空间限制	102
3.2.8 编写Metasploit的渗透模块	103
3.3 使用Metasploit实现基于SEH的缓冲区溢出	106
3.3.1 构建渗透模块的基础	108

- 3.3.2 计算偏移量 109
- 3.3.3 查找POP/POP/RET地址 110
- 3.3.4 编写Metasploit的SEH渗透模块 112
- 3.4 在Metasploit模块中绕过DEP 115
 - 3.4.1 使用msfrop查找ROP指令片段 117
 - 3.4.2 使用Mona 创建ROP链 118
 - 3.4.3 编写绕过DEP的Metasploit渗透模块 120
- 3.5 其他保护机制 122
- 3.6 小结 123
- 第4章 渗透模块的移植 124
 - 4.1 导入一个基于栈的缓冲区溢出渗透模块 124
 - 4.1.1 收集关键信息 127
 - 4.1.2 构建Metasploit模块 127
 - 4.1.3 使用Metasploit完成对目标应用程序的渗透 129
 - 4.1.4 在Metasploit的渗透模块中实现一个检查（check）方法 130
 - 4.2 将基于Web的RCE导入Metasploit 131
 - 4.2.1 收集关键信息 132
 - 4.2.2 掌握重要的Web函数 132
 - 4.2.3 GET/POST方法的使用要点 133
 - 4.2.4 将HTTP渗透模块导入到Metasploit中 134
 - 4.3 将TCP服务端/基于浏览器的渗透模块导入Metasploit 136
 - 4.3.1 收集关键信息 138
 - 4.3.2 创建Metasploit 模块 138
 - 4.4 小结 141
- 第5章 使用Metasploit对服务进行测试 142
 - 5.1 SCADA系统的基本原理 142
 - 5.1.1 ICS的基本原理以及组成部分 143
 - 5.1.2 ICS-SCADA安全的重要性 143
 - 5.1.3 SCADA系统的安全性分析 143
 - 5.1.4 使SCADA变得更加安全 147
 - 5.2 数据库渗透 148
 - 5.2.1 SQL Server 148
 - 5.2.2 使用Nmap对SQL Server进行踩点 149
 - 5.2.3 使用Metasploit的模块进行扫描 150
 - 5.2.4 暴力破解密码 151
 - 5.2.5 查找/捕获服务器的口令 152
 - 5.2.6 浏览SQL Server 153
 - 5.2.7 后渗透/执行系统命令 154
 - 5.3 VOIP渗透测试 156
 - 5.3.1 VOIP的基本原理 156
 - 5.3.2 对VOIP服务踩点 158
 - 5.3.3 扫描VOIP服务 159
 - 5.3.4 欺骗性的VOIP电话 160
 - 5.3.5 对VOIP进行渗透 162
 - 5.4 小结 163
- 第6章 虚拟化测试的原因及阶段 164
 - 6.1 使用Metasploit集成的服务完成一次渗透测试 164
 - 6.1.1 与员工和最终用户进行交流 165
 - 6.1.2 收集信息 166
 - 6.1.3 使用Metasploit中的OpenVAS插件进行漏洞扫描 167
 - 6.1.4 对威胁区域进行建模 171
 - 6.1.5 获取目标的控制权限 172
 - 6.1.6 保持控制权限和掩盖入侵痕迹 178
 - 6.1.7 使用Faraday管理渗透测试 178

- 6.1.8 手动创建报告 180
- 6.2 小结 183
- 第7章 客户端渗透 184
 - 7.1 有趣又有料的浏览器渗透攻击 184
 - 7.1.1 browser autopwn攻击 185
 - 7.1.2 对网站的客户进行渗透 188
 - 7.1.3 与DNS欺骗的结合使用 191
 - 7.2 Metasploit和Arduino——致命搭档 196
 - 7.3 基于各种文件格式的渗透攻击 201
 - 7.3.1 基于PDF文件格式的渗透攻击 201
 - 7.3.2 基于Word文件格式的渗透攻击 203
 - 7.4 使用Metasploit实现对Linux客户端的渗透 205
 - 7.5 使用Metasploit攻击Android系统 206
 - 7.6 小结 210
- 第8章 Metasploit的扩展功能 211
 - 8.1 Metasploit后渗透模块的基础知识 211
 - 8.2 基本后渗透命令 211
 - 8.2.1 帮助菜单 212
 - 8.2.2 后台命令 212
 - 8.2.3 机器ID和UUID命令 213
 - 8.2.4 通信信道的操作 213
 - 8.2.5 获取用户名和进程信息 213
 - 8.2.6 获取系统信息 214
 - 8.2.7 网络命令 214
 - 8.2.8 文件操作命令 215
 - 8.2.9 桌面命令 217
 - 8.2.10 截图和摄像头列举 218
 - 8.3 使用Metasploit中的高级后渗透模块 220
 - 8.3.1 迁移到更安全的进程上 220
 - 8.3.2 获取系统级管理权限 221
 - 8.3.3 使用hashdump获取密码的哈希值 221
 - 8.3.4 使用timestomp修改文件的访问时间、修改时间和创建时间 222
 - 8.4 其他后渗透模块 223
 - 8.4.1 使用Metasploit收集无线SSID信息 223
 - 8.4.2 使用Metasploit收集Wi-Fi密码 223
 - 8.4.3 获取应用程序列表 224
 - 8.4.4 获取Skype密码 225
 - 8.4.5 获取USB使用历史信息 225
 - 8.4.6 使用Metasploit查找文件 225
 - 8.4.7 使用clearev命令清除目标系统上的日志 226
 - 8.5 Metasploit中的高级扩展功能 227
 - 8.5.1 用Metasploit提升权限 227
 - 8.5.2 使用mimikatz查找明文密码 228
 - 8.5.3 使用Metasploit进行流量嗅探 229
 - 8.5.4 使用Metasploit对host文件进行注入 230
 - 8.5.5 登录密码的钓鱼窗口 231
 - 8.6 小结 232
- 第9章 提高渗透测试的速度 233
 - 9.1 pushm和popm命令的使用方法 233
 - 9.2 loadpath命令的使用 234
 - 9.3 使用reload、edit和reload_all命令加快开发过程 235
 - 9.4 资源脚本的使用方法 236
 - 9.5 在Metasploit中使用AutoRunScript 237
 - 9.6 Metasploit中的全局变量 240

9.7 自动化社会工程学工具包	241
9.8 小结	243
第10章 利用Armitage实现Metasploit的可视化管理	244
10.1 Armitage的基本原理	244
10.1.1 入门知识	245
10.1.2 用户界面一览	246
10.1.3 工作区的管理	247
10.2 网络扫描以及主机管理	248
10.2.1 漏洞的建模	250
10.2.2 查找匹配模块	250
10.3 使用Armitage进行渗透	251
10.4 使用Armitage进行后渗透攻击	252
10.5 使用Armitage进行客户端攻击	253
10.6 Armitage脚本编写	257
10.6.1 Cortana基础知识	258
10.6.2 控制Metasploit	260
10.6.3 使用Cortana实现后渗透攻击	261
10.6.4 使用Cortana创建自定义菜单	262
10.6.5 界面的使用	264
10.7 小结	266
10.8 延伸阅读	266
• • • • •	(收起)

[精通Metasploit渗透测试（第2版） 下载链接1](#)

标签

黑客

Metasploit

网络安全

渗透测试

计算机

Pen-Test

TP自动化技术、计算机技术

2018

评论

李总推荐的书就是碉，一口气看完心满意足，pentester必读

ituring购买。翻一翻的工具书。

本书的精华部分是脚本开发和漏洞发掘。

随便翻翻

挺好的，脚本是ruby的，比较想看python版的

[精通Metasploit渗透测试（第2版）_下载链接1](#)

书评

[精通Metasploit渗透测试（第2版）_下载链接1](#)