

<<Metasploit渗透测试魔鬼训练营>>

图书基本信息

书名：<<Metasploit渗透测试魔鬼训练营>>

13位ISBN编号：9787111434993

10位ISBN编号：7111434994

出版时间：2013-9-20

出版时间：机械工业出版社

作者：诸葛建伟,陈力波,田繁

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：<http://www.tushu007.com>

<<Metasploit渗透测试魔鬼训练营>>

内容概要

首本中文原创Metasploit渗透测试著作，国内信息安全领域布道者和资深Metasploit渗透测试专家领衔撰写，极具权威性。

以实践为导向，既详细讲解了Metasploit渗透测试的技术、流程、方法和技巧，又深刻阐释了渗透测试平台背后蕴含的思想。

本书是Metasploit渗透测试领域难得的经典佳作，由国内信息安全领域的资深Metasploit渗透测试专家领衔撰写。

内容系统、广泛、有深度，不仅详细讲解了Metasploit渗透测试的技术、流程、方法和技巧，而且深刻揭示了渗透测试平台背后蕴含的思想。

书中虚拟了两家安全公司，所有内容都围绕这两家安全公司在多个角度的多次“对战”展开，颇具趣味性和可读性。

很多知识点都配有案例解析，更重要的是每章还有精心设计的“魔鬼训练营实践作业”，充分体现了“实践，实践，再实践”的宗旨。

本书采用了第二人称的独特视角，让读者跟随“你”一起参加魔鬼训练营，并经历一次极具挑战性的渗透测试任务考验。

你的渗透测试之旅包括10段精彩的旅程。

全书共10章。

第1章对渗透测试和Metasploit进行了系统介绍，首先介绍了渗透测试的分类、方法、流程、过程环节等，然后介绍了Metasploit的功能、结构和基本的使用方法。

第2章详细演示了渗透测试实验环境的搭建。

第3章讲解了情报收集技术。

第4章讲解了Web应用渗透技术。

第5章讲解了网络服务的渗透攻击技术。

第6章讲解了客户端的渗透攻击技术。

第7章讲解了社会工程学的技术框架和若干个社会工程学攻击案例。

第8章讲解了针对笔记本电脑、智能手机等各种类型移动设备的渗透测试技术。

第9章讲解了Metasploit中功能最为强大的攻击载荷模块Meterpreter的原理与应用。

第10章，魔鬼训练营活动大结局，本章发起了一个“黑客夺旗竞赛”实战项目，目的是进一步提高读者的实战能力。

<<Metasploit渗透测试魔鬼训练营>>

作者简介

诸葛建伟，国内信息安全领域的布道者，资深渗透测试技术专家，Metasploit领域的顶级专家之一，实战经验非常丰富。

在网络攻防、入侵检测、蜜罐、恶意代码分析、互联网安全威胁监测、智能终端恶意代码等领域都有深入的研究。

国际信息安全开源组织The HoneyNet Project团队正式成员，中国分支团队负责人；清华大学网络与信息安全实验室副研究员，狩猎女神科研团队技术负责人；蓝莲花（Blue-Lotus）CTF战队的合伙创始人与组织者，2013年带领战队在DEFCON CTF资格赛取得了全球第四、亚洲第一的中国历史最好战绩，首次闯入总决赛；活跃于新浪微博和看雪论坛等社区，出版了《网络攻防技术与实践》、《Metasploit渗透测试技术指南》、《数据包分析技术实战（第2版）》等多本信息安全相关的经典著作。

<<Metasploit渗透测试魔鬼训练营>>

书籍目录

前言

致谢

第1章 魔鬼训练营——初识Metasploit1

1.1 什么是渗透测试1

1.1.1 渗透测试的起源与定义1

1.1.2 渗透测试的分类2

1.1.3 渗透测试方法与流程4

1.1.4 渗透测试过程环节5

1.2 漏洞分析与利用6

1.2.1 安全漏洞生命周期7

1.2.2 安全漏洞披露方式8

1.2.3 安全漏洞公共资源库9

1.3 渗透测试神器Metasploit11

1.3.1 诞生与发展11

1.3.2 渗透测试框架软件16

1.3.3 漏洞研究与渗透代码开发平台18

1.3.4 安全技术集成开发与应用环境19

1.4 Metasploit结构剖析20

1.4.1 Metasploit体系框架21

1.4.2 辅助模块23

1.4.3 渗透攻击模块23

1.4.4 攻击载荷模块25

1.4.5 空指令模块26

1.4.6 编码器模块26

1.4.7 后渗透攻击模块27

1.5 安装Metasploit软件28

1.5.1 在Back Track上使用和更新Metasploit29

1.5.2 在Windows操作系统上安装Metasploit29

1.5.3 在Linux操作系统上安装Metasploit30

1.6 了解Metasploit的使用接口31

1.6.1 msfgui图形化界面工具32

1.6.2 msfconsole控制台终端34

1.6.3 msfcli命令行程序36

1.7 小结38

1.8 魔鬼训练营实践作业39

第2章 赛宁VS.定V——渗透测试实验环境40

2.1 定V公司的网络环境拓扑41

2.1.1 渗透测试实验环境拓扑结构42

2.1.2 攻击机环境44

2.1.3 靶机环境45

2.1.4 分析环境50

2.2 渗透测试实验环境的搭建55

2.2.1 虚拟环境部署56

2.2.2 网络环境配置56

2.2.3 虚拟机镜像配置57

<<Metasploit渗透测试魔鬼训练营>>

- 2.3 小结63
- 2.4 魔鬼训练营实践作业64
- 第3章 揭开“战争迷雾”——情报搜集技术65
 - 3.1 外围信息搜集65
 - 3.1.1 通过DNS和IP地址挖掘目标网络信息66
 - 3.1.2 通过搜索引擎进行信息搜集72
 - 3.1.3 对定V公司网络进行外围信息搜集79
 - 3.2 主机探测与端口扫描80
 - 3.2.1 活跃主机扫描80
 - 3.2.2 操作系统辨识85
 - 3.2.3 端口扫描与服务类型探测86
 - 3.2.4 Back Track 5的Autoscan功能90
 - 3.2.5 探测扫描结果分析91
 - 3.3 服务扫描与查点92
 - 3.3.1 常见的网络服务扫描93
 - 3.3.2 口令猜测与嗅探96
 - 3.4 网络漏洞扫描98
 - 3.4.1 漏洞扫描原理与漏洞扫描器98
 - 3.4.2 OpenVAS漏洞扫描器99
 - 3.4.3 查找特定服务漏洞108
 - 3.4.4 漏洞扫描结果分析109
 - 3.5 渗透测试信息数据库与共享110
 - 3.5.1 使用渗透测试信息数据库的优势111
 - 3.5.2 Metasploit的数据库支持111
 - 3.5.3 在Metasploit中使用PostgreSQL111
 - 3.5.4 Nmap与渗透测试数据库113
 - 3.5.5 OpenVAS与渗透测试数据库113
 - 3.5.6 共享你的渗透测试信息数据库114
 - 3.6 小结117
 - 3.7 魔鬼训练营实践作业118
- 第4章 突破定V门户——Web应用渗透技术119
 - 4.1 Web应用渗透技术基础知识119
 - 4.1.1 为什么进行Web应用渗透攻击120
 - 4.1.2 Web应用攻击的发展趋势121
 - 4.1.3 OWASP Web漏洞TOP 10122
 - 4.1.4 近期Web应用攻击典型案例126
 - 4.1.5 基于Metasploit框架的Web应用渗透技术128
 - 4.2 Web应用漏洞扫描探测130
 - 4.2.1 开源Web应用漏洞扫描工具131
 - 4.2.2 扫描神器W3AF133
 - 4.2.3 SQL注入漏洞探测135
 - 4.2.4 XSS漏洞探测144
 - 4.2.5 Web应用程序漏洞探测145
 - 4.3 Web应用程序渗透测试147
 - 4.3.1 SQL注入实例分析147
 - 4.3.2 跨站攻击实例分析158
 - 4.3.3 命令注入实例分析166

<<Metasploit渗透测试魔鬼训练营>>

- 4.3.4 文件包含和文件上传漏洞174
- 4.4 小结180
- 4.5 魔鬼训练营实践作业180
- 第5章 定V门大敞，哥要进内网——网络服务渗透攻击182
 - 5.1 内存攻防技术182
 - 5.1.1 缓冲区溢出漏洞机理183
 - 5.1.2 栈溢出利用原理184
 - 5.1.3 堆溢出利用原理186
 - 5.1.4 缓冲区溢出利用的限制条件188
 - 5.1.5 攻防两端的对抗博弈188
 - 5.2 网络服务渗透攻击面190
 - 5.2.1 针对Windows系统自带的网络服务渗透攻击191
 - 5.2.2 针对Windows操作系统上微软网络服务的渗透攻击193
 - 5.2.3 针对Windows操作系统上第三方网络服务的渗透攻击194
 - 5.2.4 针对工业控制系统服务软件的渗透攻击194
 - 5.3 Windows服务渗透攻击实战案例——MS08-067安全漏洞196
 - 5.3.1 威名远扬的超级大漏洞MS08-067196
 - 5.3.2 MS08-067漏洞渗透攻击原理及过程197
 - 5.3.3 MS08-067漏洞渗透攻击模块源代码解析200
 - 5.3.4 MS08-067安全漏洞机理分析205
 - 5.4 第三方网络服务渗透攻击实战案例——Oracle数据库211
 - 5.4.1 Oracle数据库的“蚁穴”212
 - 5.4.2 Oracle渗透利用模块源代码解析212
 - 5.4.3 Oracle漏洞渗透攻击过程214
 - 5.4.4 Oracle安全漏洞利用机理220
 - 5.5 工业控制系统服务渗透攻击实战案例——亚控科技KingView222
 - 5.5.1 中国厂商SCADA软件遭国外黑客盯梢222
 - 5.5.2 KingView 6.53 HistorySvr渗透攻击代码解析224
 - 5.5.3 KingView 6.53漏洞渗透攻击测试过程225
 - 5.5.4 KingView堆溢出安全漏洞原理分析228
 - 5.6 Linux系统服务渗透攻击实战案例——Samba安全漏洞232
 - 5.6.1 Linux与Windows之间的差异232
 - 5.6.2 Linux系统服务渗透攻击原理233
 - 5.6.3 Samba安全漏洞描述与攻击模块解析234
 - 5.6.4 Samba渗透攻击过程235
 - 5.6.5 Samba安全漏洞原理分析241
 - 5.7 小结244
 - 5.8 魔鬼训练营实践作业244
- 第6章 定V网络主宰者——客户端渗透攻击246
 - 6.1 客户端渗透攻击基础知识246
 - 6.1.1 客户端渗透攻击的特点247
 - 6.1.2 客户端渗透攻击的发展和趋势247
 - 6.1.3 安全防护机制248
 - 6.2 针对浏览器的渗透攻击249
 - 6.2.1 浏览器渗透攻击面250
 - 6.2.2 堆喷射利用方式250
 - 6.2.3 MSF中自动化浏览器攻击251

<<Metasploit渗透测试魔鬼训练营>>

- 6.3 浏览器渗透攻击实例——MS11-050安全漏洞254
 - 6.3.1 MS11-050漏洞渗透攻击过程254
 - 6.3.2 MS11-050漏洞渗透攻击源码解析与机理分析256
- 6.4 第三方插件渗透攻击实战案例——再探亚控科技KingView261
 - 6.4.1 移植KingView渗透攻击代码261
 - 6.4.2 KingView渗透攻击过程264
 - 6.4.3 KingView安全漏洞机理分析265
- 6.5 针对应用程序的渗透攻击269
 - 6.5.1 应用程序渗透攻击机理269
 - 6.5.2 内存攻击技术ROP的实现270
 - 6.5.3 MSF中的自动化fileformat攻击276
- 6.6 针对Office软件的渗透攻击实例——MS10-087安全漏洞276
 - 6.6.1 MS10-087渗透测试过程277
 - 6.6.2 MS10-087漏洞渗透攻击模块源代码解析278
 - 6.6.3 MS10-087漏洞原理分析279
 - 6.6.4 MS10-087漏洞利用原理282
 - 6.6.5 文件格式分析284
- 6.7 Adobe阅读器渗透攻击实战案例——加急的项目进展报告286
 - 6.7.1 Adobe渗透测试过程287
 - 6.7.2 Adobe渗透攻击模块解析与机理分析289
 - 6.7.3 Adobe漏洞利用原理293
- 6.8 小结298
- 6.9 魔鬼训练营实践作业299
- 第7章 甜言蜜语背后的危险——社会工程学300
 - 7.1 社会工程学的前世今生300
 - 7.1.1 什么是社会工程学攻击301
 - 7.1.2 社会工程学攻击的基本形式301
 - 7.1.3 社交网站社会工程学攻击案例302
 - 7.2 社会工程学技术框架303
 - 7.2.1 信息搜集303
 - 7.2.2 诱导306
 - 7.2.3 托辞308
 - 7.2.4 心理影响309
 - 7.3 社会工程学攻击案例——伪装木马311
 - 7.3.1 伪装木马的主要方法与传播途径312
 - 7.3.2 伪装木马社会工程学攻击策划313
 - 7.3.3 木马程序的制作314
 - 7.3.4 伪装木马的“免杀”处理319
 - 7.3.5 伪装木马社会工程学的实施过程323
 - 7.3.6 伪装木马社会工程学攻击案例总结325
 - 7.4 针对性社会工程学攻击案例——网站钓鱼325
 - 7.4.1 社会工程学攻击工具包SET325
 - 7.4.2 网站钓鱼社会工程学攻击策划325
 - 7.4.3 钓鱼网站的制作326
 - 7.4.4 网站钓鱼社会工程学的实施过程330
 - 7.4.5 网站钓鱼社会工程学攻击案例总结331
 - 7.5 针对性社会工程学攻击案例——邮件钓鱼331

<<Metasploit渗透测试魔鬼训练营>>

- 7.5.1 邮件钓鱼社会工程学攻击策划331
- 7.5.2 使用SET工具集完成邮件钓鱼332
- 7.5.3 针对性邮件钓鱼社会工程学攻击案例总结338
- 7.6 U盘社会工程学攻击案例——Hacksaw攻击338
 - 7.6.1 U盘社会工程学攻击策划339
 - 7.6.2 U盘攻击原理340
 - 7.6.3 制作Hacksaw U盘341
 - 7.6.4 U盘社会工程学攻击的实施过程345
 - 7.6.5 U盘攻击社会工程学攻击案例总结345
- 7.7 小结346
- 7.8 魔鬼训练营实践作业346
- 第8章 刀无形、剑无影——移动环境渗透测试348
 - 8.1 移动的Metasploit渗透测试平台348
 - 8.1.1 什么是BYOD348
 - 8.1.2 下载安装Metasploit349
 - 8.1.3 在iPad上手动安装Metasploit350
 - 8.2 无线网络渗透测试技巧351
 - 8.2.1 无线网络口令破解351
 - 8.2.2 破解无线AP的管理密码355
 - 8.2.3 无线AP漏洞利用渗透攻击360
 - 8.3 无线网络客户端攻击案例——上网笔记本电脑364
 - 8.3.1 配置假冒AP364
 - 8.3.2 加载karma.rc资源文件367
 - 8.3.3 移动上网笔记本渗透攻击实施过程369
 - 8.3.4 移动上网笔记本渗透攻击案例总结371
 - 8.4 移动环境渗透攻击案例——智能手机371
 - 8.4.1 BYOD设备的特点372
 - 8.4.2 苹果iOS设备渗透攻击372
 - 8.4.3 Android智能手机的渗透攻击377
 - 8.4.4 Android平台Metasploit渗透攻击模块的移植385
 - 8.5 小结391
 - 8.6 魔鬼训练营实践作业391
- 第9章 俘获定V之心——强大的Meterpreter393
 - 9.1 再探Metasploit攻击载荷模块393
 - 9.1.1 典型的攻击载荷模块394
 - 9.1.2 如何使用攻击载荷模块395
 - 9.1.3 meterpreter的技术优势398
 - 9.2 Meterpreter命令详解400
 - 9.2.1 基本命令401
 - 9.2.2 文件系统命令402
 - 9.2.3 网络命令404
 - 9.2.4 系统命令406
 - 9.3 后渗透攻击模块408
 - 9.3.1 为什么引入后渗透攻击模块408
 - 9.3.2 各操作系统平台分布情况409
 - 9.3.3 后渗透攻击模块的使用方法409
 - 9.4 Meterpreter在定V渗透测试中的应用411

<<Metasploit渗透测试魔鬼训练营>>

- 9.4.1 植入后门实施远程控制411
- 9.4.2 权限提升414
- 9.4.3 信息窃取417
- 9.4.4 口令攫取和利用419
- 9.4.5 内网拓展424
- 9.4.6 掩踪灭迹430
- 9.5 小结431
- 9.6 魔鬼训练营实践作业432
- 第10章 群狼出山——黑客夺旗竞赛实战433
- 10.1 黑客夺旗竞赛的由来434
- 10.2 让我们来玩玩“地下产业链”436
 - 10.2.1 “洗钱”的竞赛场景分析437
 - 10.2.2 “洗钱”规则438
 - 10.2.3 竞赛准备与任务分工439
- 10.3 CTF竞赛现场441
 - 10.3.1 解题“打黑钱”441
 - 10.3.2 GameBox扫描与漏洞分析443
 - 10.3.3 渗透Web应用服务448
 - 10.3.4 渗透二进制服务程序451
 - 10.3.5 疯狂“洗钱”459
 - 10.3.6 力不从心的防御459
- 10.4 CTF竞赛结果460
- 10.5 魔鬼训练营大结局461
- 10.6 魔鬼训练营实践作业461
- 附录A 如何撰写渗透测试报告462
- 附录B 参考与进一步阅读468

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:<http://www.tushu007.com>