

《Metasploit渗透测试指南》

图书基本信息

书名：《Metasploit渗透测试指南》

出版时间：2012-1

作者：(美)David Kennedy Jim O'Gorman Devon Kearns Mati Aharoni

页数：312

译者：诸葛建伟,王珩,孙松柏

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

《Metasploit渗透测试指南》

内容概要

《metasploit渗透测试指南》介绍metasploit——近年来最强大、最流行和最有发展前途的开源渗透测试平台软件，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。

《metasploit渗透测试指南》共有17章，覆盖了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，本书一步一个台阶地帮助初学者从零开始建立起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用书。本书获得了metasploit开发团队的一致好评，metasploit项目创始人hd moore评价本书为：“现今最好的metasploit框架软件参考指南”。

《metasploit渗透测试指南》适合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阅读。

书籍目录

《metasploit渗透测试指南》	
第1章 渗透测试技术基础	1
1.1 ptes标准中的渗透测试阶段	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	2
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
1.3 漏洞扫描器	5
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	11
2.3 metasploit功能程序	12
2.3.1 msf攻击载荷生成器	12
2.3.2 msf编码器	13
2.3.3 nasm shell	13
2.4 metasploit express和metasploit pro	14
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
3.2 主动信息搜集	18
3.2.1 使用nmap进行端口扫描	18
3.2.2 在metasploit中使用数据库	20
3.2.3 使用metasploit进行端口扫描	25
3.3 针对性扫描	26
3.3.1 服务器消息块协议扫描	26
3.3.2 搜寻配置不当的microsoft sql server	27
3.3.3 ssh服务器扫描	28
3.3.4 ftp扫描	29
3.3.5 简单网管协议扫描	30

- 3.4 编写自己的扫描器 31
- 3.5 小结 33
- 第4章 漏洞扫描 35
 - 4.1 基本的漏洞扫描 36
 - 4.2 使用nexpose进行扫描 37
 - 4.2.1 配置 37
 - 4.2.2 将扫描报告导入到metasploit中 42
 - 4.2.3 在msf控制台中运行nexpose 43
 - 4.3 使用nessus进行扫描 44
 - 4.3.1 配置nessus 44
 - 4.3.2 创建nessus扫描策略 45
 - 4.3.3 执行nessus扫描 47
 - 4.3.4 nessus报告 47
 - 4.3.5 将扫描结果导入metasploit框架中 48
 - 4.3.6 在metasploit内部使用nessus进行扫描 49
 - 4.4 专用漏洞扫描器 51
 - 4.4.1 验证smb登录 51
 - 4.4.2 扫描开放的vnc空口令 52
 - 4.4.3 扫描开放的x11服务器 54
 - 4.5 利用扫描结果进行自动化攻击 56
- 第5章 渗透攻击之旅 57
 - 5.1 渗透攻击基础 58
 - 5.1.1 msf] show exploits 58
 - 5.1.2 msf] show auxiliary 58
 - 5.1.3 msf] show options 58
 - 5.1.4 msf] show payloads 60
 - 5.1.5 msf] show targets 62
 - 5.1.6 info 63
 - 5.1.7 set和unset 63
 - 5.1.8 setg和unsetg 64
 - 5.1.9 save 64
 - 5.2 你的第一次渗透攻击 64
 - 5.3 攻击一台ubuntu主机 68
 - 5.4 全端口攻击载荷：暴力猜解目标开放的端口 71
 - 5.5 资源文件 72
 - 5.6 小结 73
- 第6章 meterpreter 75
 - 6.1 攻陷windows xp 虚拟机 76
 - 6.1.1 使用nmap扫描端口 76
 - 6.1.2 攻击ms sql 76
 - 6.1.3 暴力破解ms sql服务器 78
 - 6.1.4 xp_cmdshell 79
 - 6.1.5 meterpreter基本命令 80
 - 6.1.6 获取键盘记录 81
 - 6.2 挖掘用户名和密码 82
 - 6.2.1 提取密码哈希值 82
 - 6.2.2 使用meterpreter命令获取密码哈希值 83
 - 6.3 传递哈希值 84
 - 6.4 权限提升 85

- 6.5 令牌假冒 87
- 6.6 使用ps 87
- 6.7 通过跳板攻击其他机器 89
- 6.8 使用meterpreter脚本 92
 - 6.8.1 迁移进程 92
 - 6.8.2 关闭杀毒软件 93
 - 6.8.3 获取系统密码哈希值 93
 - 6.8.4 查看目标机上的所有流量 93
 - 6.8.5 攫取系统信息 93
 - 6.8.6 控制持久化 94
- 6.9 向后渗透攻击模块转变 95
- 6.10 将命令行shell升级为meterpreter 95
- 6.11 通过附加的railgun组件操作windows api 97
- 6.12 小结 97
- 第7章 免杀技术 99
 - 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 100
 - 7.2 躲避杀毒软件的检测 101
 - 7.2.1 使用msf编码器 102
 - 7.2.2 多重编码 103
 - 7.3 自定义可执行文件模板 105
 - 7.4 隐秘地启动一个攻击载荷 106
 - 7.5 加壳软件 107
 - 7.6 小结：关于免杀处理的最后忠告 108
- 第8章 客户端渗透攻击 109
 - 8.1 基于浏览器的渗透攻击 110
 - 8.1.1 基于浏览器的渗透攻击原理 111
 - 8.1.2 空指令 112
 - 8.2 使用immunity调试器来揭秘空指令机器码 112
 - 8.3 对ie浏览器的极光漏洞进行渗透利用 116
 - 8.4 文件格式漏洞渗透攻击 119
 - 8.5 发送攻击负载 120
 - 8.6 小结 121
- 第9章 metasploit辅助模块 123
 - 9.1 使用辅助模块 126
 - 9.2 辅助模块剖析 128
 - 9.3 小结 133
- 第10章 社会工程学工具包 135
 - 10.1 配置set工具包 136
 - 10.2 针对性钓鱼攻击向量 137
 - 10.3 web攻击向量 142
 - 10.3.1 java applet 142
 - 10.3.2 客户端web攻击 146
 - 10.3.3 用户名和密码获取 148
 - 10.3.4 标签页劫持攻击 150
 - 10.3.5 中间人攻击 150
 - 10.3.6 网页劫持 151
 - 10.3.7 综合多重攻击方法 153
 - 10.4 传染性媒体生成器 157
 - 10.5 teensy usb hid攻击向量 157

- 10.6 set的其他特性 160
- 10.7 小结 161
- 第11章 fast-track 163
 - 11.1 microsoft sql注入 164
 - 11.1.1 sql注入——查询语句攻击 165
 - 11.1.2 sql注入——post参数攻击 166
 - 11.1.3 手工注入 167
 - 11.1.4 ms sql破解 168
 - 11.1.5 通过sql自动获得控制 (sqlpwnage) 172
 - 11.2 二进制到十六进制转换器 174
 - 11.3 大规模客户端攻击 175
 - 11.4 小结：对自动化渗透的一点看法 176
- 第12章 karmetasploit无线攻击套件 177
 - 12.1 配置 178
 - 12.2 开始攻击 179
 - 12.3 获取凭证 181
 - 12.4 得到shell 182
 - 12.5 小结 184
- 第13章 编写你自己的模块 185
 - 13.1 在ms sql上进行命令执行 186
 - 13.2 探索一个已存在的metasploit模块 187
 - 13.3 编写一个新的模块 189
 - 13.3.1 powershell 189
 - 13.3.2 运行shell渗透攻击 190
 - 13.3.3 编写powershell_upload_exec函数 192
 - 13.3.4 从十六进制转换回二进制程序 192
 - 13.3.5 计数器 194
 - 13.3.6 运行渗透攻击模块 195
 - 13.4 小结：代码重用的能量 196
- 第14章 创建你自己的渗透攻击模块 197
 - 14.1 fuzz测试的艺术 198
 - 14.2 控制结构化异常处理链 201
 - 14.3 绕过seh限制 204
 - 14.4 获取返回地址 206
 - 14.5 坏字符和远程代码执行 210
 - 14.6 小结 213
- 第15章 将渗透代码移植到metasploit框架 215
 - 15.1 汇编语言基础 216
 - 15.1.1 eip和esp寄存器 216
 - 15.1.2 jmp指令集 216
 - 15.1.3 空指令和空指令滑行区 216
 - 15.2 移植一个缓冲区溢出攻击代码 216
 - 15.2.1 裁剪一个已有的渗透攻击代码 218
 - 15.2.2 构造渗透攻击过程 219
 - 15.2.3 测试我们的基础渗透代码 220
 - 15.2.4 实现框架中的特性 221
 - 15.2.5 增加随机化 222
 - 15.2.6 消除空指令滑行区 223
 - 15.2.7 去除伪造的shellcode 223

- 15.2.8 我们完整的模块代码 224
- 15.3 seh覆盖渗透代码 226
- 15.4 小结 233
- 第16章 meterpreter脚本编程 235
 - 16.1 meterpreter脚本编程基础 235
 - 16.2 meterpreter api 241
 - 16.2.1 打印输出 241
 - 16.2.2 基本api调用 242
 - 16.2.3 meterpreter mixins 242
 - 16.3 编写meterpreter脚本的规则 244
 - 16.4 创建自己的meterpreter脚本 244
 - 16.5 小结 250
- 第17章 一次模拟的渗透测试过程 251
 - 17.1 前期交互 252
 - 17.2 情报搜集 252
 - 17.3 威胁建模 253
 - 17.4 渗透攻击 255
 - 17.5 msf终端中的渗透攻击过程 255
 - 17.6 后渗透攻击 257
 - 17.6.1 扫描metasploitable靶机 258
 - 17.6.2 识别存有漏洞的服务 259
 - 17.7 攻击apache tomcat 260
 - 17.8 攻击一个偏门的服务 262
 - 17.9 隐藏你的踪迹 264
 - 17.10 小结 266
- 附录a 配置目标机器 267
- 附录b 命令参考列表 275

精彩短评

- 1、开阔眼界，技术书
- 2、书有损毁！！！！！！
- 3、可以对metasploit有一个较全面的了解，对攻击技术有个概略的了解，不过关于技术方面不够深入。
- 4、上手应该有点问题，买了还没细读，还没时间折腾MS平台
- 5、比起手册那本要老，但竟然容易理解一点。
- 6、英文原版译过来的原书就很好 翻译的一般
书中不光讲metasploit还有些漏洞检测工具
- 7、内容很丰富，不仅仅是metasploit的使用，还包括所有可以与它搭配的软件，很实用。
- 8、目前市面上专门讲metasploit的唯一一本中文书籍，不过内容还不错，个人觉得翻译的一般，有些地方比较书面性，对照英文版比较容易理解。对插件的开发介绍的不够多，如果能够介绍一下metasploit的程序框架细节就好了。2.x版本是用perl编写的，3.x以后用ruby重构了。
- 9、这本书也仅仅只是告诉渗透者如何利用metasploit这个工具只是很大概的介绍下这个工具，细致的还是要自己去摸索
- 10、很不错，以前只是用Metasploit，也知道Metasploit可以进一步，但是一直没有办法入门，现在这本书可以看看，正在学习，希望有长进。
但书的质量一般，纸张比较粗和脆。
- 11、写的不错，理解起来比较流畅，适合网络安全入门者快速上手
- 12、Metasploit 还是很博大精深的，不过payload主要偏操作系统和应用程序的多些，Web渗透的话，一般还是用BurpSuite或者Zap Proxy为主吧，不过渗透分析的思路是相同的，前面三章还是很精彩的，有必要看下。
- 13、是msf方面介绍的最全面最权威的书籍，渗透测试必备
- 14、非常好的一本入门操作指南
- 15、Metasploit作为安全人员及黑客的必备工具,在安全社区内具有非同一般的地位.本书深入浅出地介绍了Metasploit的方方面面.对于新手,是一本必读书籍,对于老手及安全专业人员,更是一本案头必备书籍.,甚至应该人手一本.感谢H.D MOORE开发了Metasploit,感谢图书作者写了如此之棒的一本图书.
- 16、本书详细介绍了渗透测试工具Metasploit的使用方法，对新手和老手都有参考价值
- 17、讲的很细 很容易读
- 18、Very good
- 19、书很好，但是找配套免费软件很难了
- 20、很基础的，翻译也渣渣，而且不建议买，里面的东西都过时了。做真正入侵和渗透还很远，无聊看看还可以，想折腾的话，还是将计算机网络等基础摸熟吧。
- 21、看看之后 有点写的还是不够详尽
- 22、MSF
- 23、大开眼界
- 24、前几天91ri上看一篇黑Metasploit黑的飞起的文章，其实那作者根本就没系统的研究过，msf不是单一安全工具，他是在做一个渗透平台，从导入攻击脚本到hashdump、令牌盗用到内网跳板等等，这也绝不是工具集能完成的，这是一套完整的渗透流程实现。书不错，值得多读几遍。
- 25、没什么可以说的，一本直截了当介绍软件使用的书籍。
- 26、大概翻了一下比想象中的要好一些 . . .
- 27、说实话，这书我看完了，我自己都觉得不可思议
很久没认真看书了，今晚翻着翻着，突然发现，这书翻完了，已经完全不接触安全领域了，为什么有种淡淡的忧伤？
- 28、计算机的东西都是师傅领进门修行在个人。一本好“师傅”，目前还在读，还是比较浅显易懂的。内容安排从：1、前期知识准备、名词解释。2、开始的漏洞扫描与信息搜集。3、中段的渗透。4、后段的shellcode上传免杀。5、最后的高手进阶。挺全面的，由浅入深。
- 29、完美指南
- 30、讲metasploit 不错的书

《Metasploit渗透测试指南》

- 31、据说新版快出来了！！
 - 32、个人感觉价格挺便宜的，送货只用神速形容，昨晚10点下的单，今天中午就到，刚好有点事，没准时收取，让快递员等了很久，书的内容挺不错的，外国翻译过来的，水平不错，挺适合初学者看，理论分析很到位，非常推荐，不过，书的纸质希望可以稍加改进下。
 - 33、Metasploit是渗透利器
 - 34、对于Metasploit还不是很了解，大体浏览了这本书，很全面很细致
 - 35、纸张质量不错。要有些基础才看的懂，建议先学会用LINUX。
 - 36、这本书不错，基于msf讲解pentest的方法论。
 - 37、帮同事下单，同事说很好。
 - 38、非常喜欢，好书，值得一看
 - 39、正在看，准备安装工具，边看边做，是很好的工具书
 - 40、有个流程大致了解，思路清晰，但是有点脱节
 - 41、适合渗透测试用。可以说是metasploit实例教程
 - 42、是本不错的渗透测试的书。
 - 43、Metasploit渗透测试内容写的较全面
 - 44、书很好，写的也很详细，非常有用处
 - 45、metasploit是漏洞扫描一款很强大的工具，集成了各种漏洞扫描工具，本书的讲解也很详细，demo很多。
 - 46、不错。不错。这个书我很喜欢的。
 - 47、感觉写的还是挺有味道的，很适合入门
 - 48、只要多加练习，很快就能上手
 - 49、学习网络安全必看书之一
 - 50、非常不错，内容循序渐进，翻译的质量也非常赞，读起来很顺。
 - 51、没用过的话可以算一本很好的说明书
 - 52、本书详细介绍了渗透测试工具Metasploit的使用方法，对新手和老手都有参考价值。值得购买。
 - 53、挺详细的，msf入门必备
 - 54、冲着作者去买的，质量很放心。
 - 55、爱好信息安全或者搞测试的话值得一看
 - 56、非常值得读的一本书，写得比较详细，可以照着书籍做相应的试验，此书绝对超值，阅读后回味无穷！
 - 57、感觉还不错
 - 58、一般而已
 - 59、依据PTES标准的7个阶段：前期交互、情报收集、威胁建模、漏洞分析、渗透攻击、后渗透攻击、报告阶段，详细讲解的Metasploit的渗透攻击方法。
- tips: 书中实例可安装metasploit-latest-windows-installer.exe 64bit的进行学习；完整版最好使用linux虚拟机镜像。
- 60、是本好教程。
 - 61、一直等中文版，终于有了
 - 62、偷闲读的，当教材还行
 - 63、对metasploit讲解的很不错，
 - 64、理论不错~不知道是否有较强实践性~
 - 65、帮朋友买的，据说书还不错。
- 反正送到我这里是很快，内容我看不到。
- 66、朋友点名要我送他的~~~唉。。。自己都舍不得买本
 - 67、本来就比较感兴趣，能翻译成中文，作为入门真是非常不错。
 - 68、可操作性强，步骤非常详细！
 - 69、折腾kali linux时候读的。
 - 70、感觉整本书的架构上有点不够清晰，但是总体来说还是一本好书

《Metasploit渗透测试指南》

- 71、书很新，不过还没时间看，感觉当当网配货很快很好，感谢当当网
- 72、书的内容来看，不管是作者还是译者都花了很大心血，讲解由浅及深，不管是初学者还是已经具备一定经验的技术人员都会有收获，而且它不单单局限于对工具的介绍，更重要的是以测试者的角度出发，讲解了很多漏洞挖掘和利用的方法。
- 印刷不行，送货很慢。
- 73、图书馆借的，粗略看了一遍，觉得不如诸葛建伟博士的那本msf渗透测试集中营，工具和平台还是次要的。
- 74、精品必读
- 75、入门的经典，好东西啊
- 76、入门+基本操作覆盖很全
- 77、到货了，看上去不错的样子，现在开始看。
- 78、介绍metasploit的中文书籍，非常不错
- 79、主要讲msf怎么用，里面有很多模块，直接调就完了。对于应用运维的安全，没啥收获。而且翻译的一般。后面三分之一翻翻就过了。
- 80、简单的翻阅了一下，没有想象的那么好，但是还可以把
- 81、很给力！！不错！！还是中文版！！
- 82、内容还行，实践性比较强，但是环境搭建太麻烦。
- 83、刚看，还需要看一段时间才行
- 84、Metasploit渗透测试内容写的较全面。
- 85、只能说一句话：好书
- 86、这绝对是将渗透方面的好书，Metasploit是老外的东西，中文资料不多，这本译本不错
- 87、粗浅的看过，不搞这一行，也就只能走马观花地看看了。不过感觉没什么特别的营养。。
- 88、是跟着《网络安全评估（第二版）》一起买的，看了那本我我对这本更有体会了
- 89、渗透，是我刚接触的一门课程，这本书讲的比较详细
- 90、书很好，可惜不是软件不是新版本，期待下一版！
- 91、本书全面介绍了metasploit这个神器，内容没得挑剔，渗透专员都应该读一读，本书翻译的质量也很好
- 92、不实用，现在没打补丁的机器碰到简直交狗屎运，对渗透帮助不大，毕竟是高手用的，高手得会自己搞漏洞，才用这方便。玩玩可以，商业版本上百万，高手帮你写漏洞
- 93、经典数目、值得一看。。
- 94、读读读读读读读读读读ing
- 95、还算有诚意
- 96、精神,好书一本,很适合新手
- 97、因为同学参与了翻译，所以买来看看，版本太老，跟不上软件更新的速度
- 98、买了两本，这本还没看，看完后再来评价。
- 99、：
TP393.08/2272
- 100、好的框架可以大大提高工作的效率
- 101、就是拿过来看一下，学习一下。

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