《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

《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。

《Metasploit渗透测试指南》

书籍目录

《Metasploit渗透测试指南》

精彩短评

1、开阔眼界，技术书
2、书有损毁！！！！！！！
3、可以对metapoilt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、Metaspolit 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

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、非常不错的书，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

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。

《Metasploit渗透测试指南》

版权说明