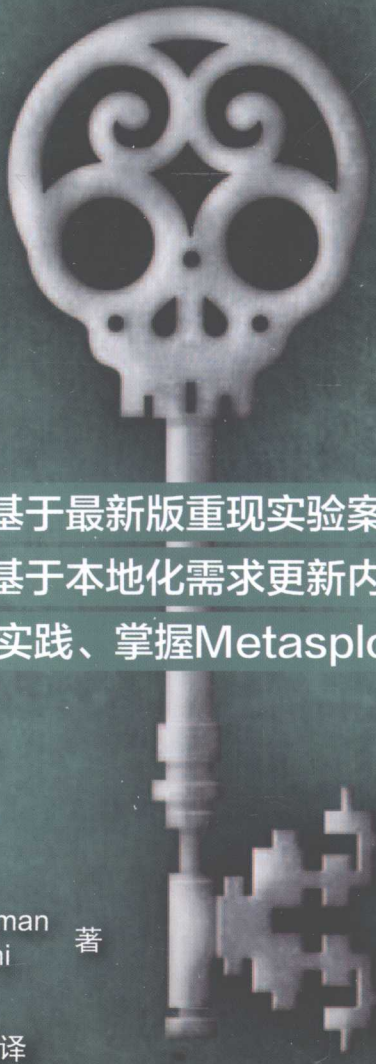
Broadview
www.broadview.com.cn

安全技术大系

Metasploit 渗透测试指南 修订版



基于最新版重现实验案例
基于本地化需求更新内容
快速实践、掌握Metasploit精髓

[美] David Kennedy，Jim O'Gorman
Devon Kearns，Mati Aharoni 著
HD Moore 作序
诸葛建伟 王珩 陆宇翔 等译

Metasploit: The Penetration Tester's Guide

no starch press

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Metasploit: The Penetration Tester's Guide

Metasploit 渗透测试指南

修订版

[美] David Kennedy，Jim O'Gorman
Devon Kearns，Mati Aharoni 著

HD Moore 作序

诸葛建伟 王珩 陆宇翔 孙松柏 译

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书介绍开源渗透测试框架平台软件 Metasploit，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，帮助初学者从零开始建立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索引。

本书分为 17 章，覆盖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。此修订版尽量保持原著的实验案例选择，仅根据 Metasploit 版本更新的实际情况来复现实验，同步更新操作流程的命令输入和输出结果。对于少量国内读者不便重现的实验案例，将实验对象、分析工具等替换为更容易接触和使用的替代品。

本书的读者群主要是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。

版权贸易合同登记号 图字：01-2011-7695

图书在版编目（CIP）数据

Metasploit 渗透测试指南 /（美）戴维·肯尼（David Kennedy）等著；诸葛建伟等译. —修订本.
北京：电子工业出版社，2017.7
书名原文：Metasploit: The Penetration Tester's Guide
ISBN 978-7-121-31825-2

Ⅰ. ①M… Ⅱ. ①戴… ②诸… Ⅲ. ①计算机网络－安全技术－应用软件－指南 Ⅳ. ①TP393.08-62

中国版本图书馆 CIP 数据核字(2017)第 129487 号

策划编辑：刘 皎
责任编辑：许 艳
印 刷：北京京科印刷有限公司
装 订：北京京科印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×980 1/16 印张：21 字数：450.5 千字
版 次：2012 年 1 月第 1 版
2017 年 7 月第 2 版
印 次：2017 年 7 月第 1 次印刷
定 价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：010-51260888-819，faq@phei.com.cn。

推荐序

IT 是一个非常复杂和混沌的领域，充斥着各种已经半死不活的过时技术和数量更多的新系统、新软件和新协议。保护现在的企业网络不能仅仅依靠补丁管理、防火墙和用户培训，而更需要周期性地对网络中的安全防御机制进行真实环境下的验证与评估，以确定哪些是有效的哪些是缺失的，而这就是渗透测试所要完成的目标。

渗透测试是一项非常具有挑战性的工作。你拿着客户付的钱，却像犯罪者那样去思考，使用你所掌握的各种“游击”战术，在一个高度复杂的防御网络中找出最为薄弱的环节，来实施致命一击。在渗透测试中，你能够发现的事情可能是既让你的雇主惊奇，又让他烦恼的：从他的服务器可以被攻陷并架设色情网站，到公司业务可以被实施大规模的欺诈与犯罪行为。

渗透测试过程需要绕过目标组织的安全防御阵线，探测出系统中存在的弱点。一次成功的渗透测试可能获取到一些敏感数据，而这通常是安全体系结构审查或漏洞评估所无法找出的，系统被发现的典型弱点包括共享口令、非法外联的网络，以及一些被发掘曝光的隐私信息。由马虎草率的系统管理员和匆匆赶工完成的系统部署会造成各种各样的安全问题，经常会对一个组织造成严重的安全威胁，然而对应的解决方案与计划措施可能还积压在系统管理员冗长的 TO-DO 列表中。渗透测试可以将这些被忽略的问题及时揭示出来，让目标组织更加清晰地了解到在防御一次真正的入侵时哪些问题更需要被立即解决。

渗透测试者会接触到一个公司中最敏感的资源，他们也会访问到公司中最关键的区域，而如果有人针对这些资源和区域实施一些邪恶的攻击行为，那将给这个公司带来极其严重的影响和后果。仅仅一个神秘出现的数据包就可能导致整个工厂停工，从而造成每小时数百万美元的损失；被当成攻击跳板时没有察觉并向有关部门进行通报，也可能导致最后遭遇到警方令人不自在且难堪的问询。医疗系统是一个甚至连非常有经验的渗透测试师都不太乐意进行测试的领域，没有人愿意承担这个领域一些系统故障的后果与责任：比如由于 OpenVMS 大型机系统故障导致将患者的血型搞混，或者由于运行 Windows XP 的一台 X 光机内存破坏对患者进行超辐

射量的扫描。最为关键的系统经常也是最为脆弱的，没有几个系统管理员愿意承担业务中断的风险关闭一台核心数据库服务器来安装安全补丁。

在利用潜在攻击路径和造成损害的风险中进行权衡是所有渗透测试师都必须掌握的技能，这个过程不仅仅依赖于对渗透工具和技术的了解，也取决于对目标组织业务流程的深入理解，以及对其中最脆弱环节的定位能力。

在本书中，你将透过四位安全专家的视角来认识渗透测试，而他们拥有不同的背景与技术专长，其中有在企业安全架构方面拥有丰富经验的安全专家，也有熟知安全漏洞挖掘和渗透代码开发地下经济链的资深黑客。在市面上已经有一些关于渗透测试与安全评估技术的书籍，也有一些完全聚焦于某种工具的实践参考书。而这本书尝试在这两者之间取得平衡，既覆盖了一些基础的工具和技术，同时又展示了如何实施一次渗透测试的方法与经验。有经验的渗透测试者也可以从基于最新渗透测试执行标准的方法学中得到一些启示，而新接触到渗透测试领域的新手们也将不仅仅能够看到关于如何入门的参考指南，也可以了解到哪些技术步骤是关键的、为什么关键，以及它们在整个渗透测试流程中的地位。

这本书是专注于 Metasploit 渗透测试框架软件的专题指南。Metasploit 开源平台提供了一个包含大量通用可靠并且经常更新的渗透攻击代码库，同时也为编写新的渗透工具及自动化渗透测试过程提供了一个完整的研究与开发环境。本书也介绍了 Metasploit Express 和 Metasploit Pro——Metasploit 框架中商业化的两个同胞姐妹，她们为如何进行一次自动化的大规模渗透测试提供了独树一帜的能力。

Metasploit 框架在代码的反复无常上是“声名狼藉”的，它的代码库每天被一个核心的开发团队和数百位来自社区的贡献者更新数十次。在我看来，为 Metasploit 写一本书根本就是一种自虐行为：完成的一章刚刚经过了试读，可能它里面的内容就已经过时了。然而，作者们接受了这项艰巨的任务，并成功地让这本书在到达读者手中时，内容还仍然是适用的。

Metasploit 开发团队也参与了这本书的评审，以确保对代码的最新修改能够精确地反映到书中，而最终的评审结果是：这本书对 Metasploit 框架软件的“0day”覆盖已经达到人力的极限。我们可以很负责任地说——这是现今已有最好的 Metasploit 框架软件参考指南。我们希望本书能够在你的工作中发挥价值，并且是指导你在渗透测试技术道路上不断探索前行的一本优秀参考指南。

HD Moore

Metasploit 项目创始人

修订版译者序

2017 年春节假期前，当博文视点编辑皎子老师在微信聊天中提及要重新出《Metasploit 渗透测试指南》这本书的时候，我的第一感受还是蛮激动的，以为 Offensive Security 的几位大神们终于想起对这本 Metasploit 入门宝典做更新了。因为这本书对于我而言还是蛮有感情的，她是我技术书籍翻译的处女作，自此书出版之后，我就像打开了在网络安全技术书籍出版领域的大门，在之后的三年里组织和参与翻译了五本网络安全知名巨著，包括畅销经典《线上幽灵：世界头号黑客米特尼克自传》、大部头的《恶意代码分析实战》、安卓安全重头书《Android 安全攻防权威指南》等，也和本书译者团队共同出版了一本原创书《Metasploit 渗透测试魔鬼训练营》，算是“集齐七龙珠”，可以“召唤神龙”了。然而等我平复心情去查了下原版的更新情况，却意识到可能有人在给我挖坑了。原书的作者大神们可能根本没有想起来要去更新这本经典书籍，而是在专注一本新书 *Kali Revealed* 的最后冲刺吧。

由于“欠债”太多的缘故，我无法拒绝皎子编辑的殷切期盼，答应她尽快利用春节假期的时间对这本 Metasploit 入门宝典进行修订，以适应读者需求并重新出版。为了能够让读者参考修订版来使用最新版本的 Metasploit 渗透测试框架软件，我重新召集了原来译者团队中的核心成员——王珩（好在他已经加入赛宁创业团队），并让赛宁网络安全工程师陆宇翔全职加入一起进行全书操作流程的复现和更新工作。此外，为了让读者们能更容易地进行修订版中的全部实验，除了同步更新附录 A 中的实验环境部署流程之外，我们还在赛宁运营的 XCTF-OJ 实训平台（http://oj.xctf.org.cn）中提供完整的实验环境，让读者无须自己配置环境即可在线快速进行全书大部分的实验操作。

在本书的修订过程中，我们采取的原则是尽量保持原书作者的实验案例选择，仅根据 Metasploit 版本更新的实际情况来复现实验，同步更新实验操作流程的命令输入和输出结果，这样让读者在阅读本书时能够实践和掌握 Metasploit 最新版本的使用方法和应用技巧。对于少量我们觉得国内读者不便重现的实验案例，我们将实验对象、分析工具等替换为国内读者更容易

接触和使用的替代品，在保持实验目的和功能展示效果不变的前提下，让大家更容易通过复现实验过程掌握相关渗透技巧。

基于以上修订原则，我们对原书进行的具体修订内容如下。

- 第 1 章“渗透测试技术基础”：1.2 节“渗透测试类型”中，在原书作者描述的黑盒测试和白盒测试之外，增加了对实际测试环境中更推荐的灰盒渗透方法进行了介绍。
- 第 2 章“Metasploit 基础”：2.2 节“Metasploit 用户接口”中，根据 Metasploit 2015 年 1 月版本之后的更新，移除了其不再支持的 msfcli 命令行工具的说明，并介绍了可替代命令行工具的 MSF 终端“-x”选项的用法。2.3 节“Metasploit 功能程序”中，说明了 MSF 攻击载荷生成器和编码器不再以单独的程序（分别为 msfpayload、msfencode）实现，而是将功能集成到 msfvenom 程序中。2.4 节“Metasploit Express 和 Metasploit Pro”中，增加了 Metasploit 商业版本和免费版本的功能差异。
- 第 3 章“情报搜集”：3.1 节“被动信息搜集”中，由于原书作者用于示例的 secmaniac.net 域名不再维护，我们将相关示例的域名更新为 testfire.net，增加了原书作者未覆盖到的 Google Hacking 基本技巧。
- 第 4 章“漏洞扫描”：4.2 节“使用 Nexpose 进行扫描”中，更新了用 Nexpose 免费社区版进行漏洞扫描过程的演示。4.3 节“使用 Nessus 进行扫描”中，更新了用免费家用版 Nessus 4.4.1 进行漏洞扫描的过程演示。4.5 节“利用扫描结果进行自动化攻击”中，由于 Metasploit 最新版本中已移除对 db_autopwn 功能的支持，更新使用了 Metasploit Pro 商业版本进行自动化攻击的演示。
- 第 5 章“渗透攻击之旅”：5.2 节“你的第一次渗透攻击”中，将攻击机从 Back Track 更新至目前流行的 Kali Linux，Windows 靶标从 Windows XP 英文版更新为国内读者更容易获取到的 Windows XP 中文版。5.3 节“攻击 Metasploitable 主机”中，将 Linux 靶标从 Metasploitable v1 更新至 Metasploitable v2，将攻击服务同步更新至 Metasploitable v2 环境中包含的 vsftpd 网络服务。
- 第 6 章“Meterpreter”：6.7 节“通过跳板攻击其他机器”中，增加了使用 Metasploit Pro 的 VPN 跳板的功能介绍和演示。
- 第 7 章“免杀技术”：7.1 节“使用 MSF 攻击载荷生成器创建可独立运行的二进制文件”中，Metasploit 新版本使用 msfvenom 集成原先的载荷生成器 msfpayload 和编码器 msfencode 的功能，更新了利用 msfvenom 进行攻击载荷生成的命令。7.2 节“躲避杀毒软件检测和后续”中，使用国内的杀毒软件代替原书中国外杀毒软件进行实验更新。我们增加了 7.6“使用 Metasploit Pro 的动态载荷实现免杀”，向读者们演示了 Metasploit Pro 商业版中特有的动态载荷生成功能。
- 第 8 章“客户端渗透攻击”：使用了国内读者更熟悉的 Ollydbg 代替原书的 Immunity Dbg

更新对浏览器漏洞分析的实验过程。

- 第 9 章“Metasploit 辅助模块”：9.2 节“辅助模块剖析”中，根据原书作者采用的 Foursquare 基于用户地理位置信息的手机服务网站案例的 API 更新，将自动签到的辅助模块代码进行了同步更新，并解释了为了适用 API 更新而做出的修改。
- 第 10 章“社会工程学工具包”：根据 Kali Linux 中社会工程学工具包 SET 的版本更新，对原书实验进行了完整重复并更新了过程中的输入命令和输出结果。10.5 节“USB HID 攻击向量”中，采用国内淘宝可采购到的 Teensy USB HIB 主板进行攻击过程重现，并提供了完整的代码，使得国内读者能够通过具体实验实际掌握此项渗透技术。
- 第 11 章“Fast-Track”：由于 Kali Linux 中将 Fast-Track 集成进 SET 且没有进行任何更新和维护，因此译者没有对本章进行任何修订。
- 第 12 章“Karmetasploit 无线攻击套件”：使用国内更流行的采用 Realtek RTL8188EUS 802.11n 芯片无线网卡进行了实验重现，并更新了实验过程的命令输入和结果输出。
- 第 13 章“编写你自己的模块”：重新部署了 Windows 7 靶标环境代替原书中使用的 Windows Server 2008 R2 重现实验，并更新了实验过程的命令输入和结果输出。
- 第 14 章“创建你自己的渗透攻击模块”：使用了国内读者更熟悉的 Ollydbg 代替原书使用的 Immunity Dbg 更新实验过程。
- 第 15 章“将渗透代码移植到 Metasploit”：没有对本章进行任何修订。
- 第 16 章“Meterpreter 脚本编程”：在更新后的 Kali Linux 操作机中对实验进行了完整复现，并更新了实验过程的命令输入和结果输出。
- 第 17 章“一次模拟的渗透测试过程”：采用更新后的 Metasploitable Linux v2.0 作为靶标环境，针对靶标环境中存在漏洞网络服务的变化，选择了攻击 PostgreSQL 数据库服务案例代替了 Metasploitable v1.0 中的 Apache Tomcat 网络服务案例，使用 unreal IRC 网络服务案例代替了 DistCC 网络服务案例。

深夜里打算就以上内容将修订版译者序收场之时，突然一眼瞄到了之前译者序中立下的 flag：“译者团队在充分吸收本书技术精华之后，也仍有计划推出基于最新发布的 Metasploit v4.0，分别面向渗透测试技术人员、漏洞研究与利用技术人员的 Metasploit 宝典姊妹篇”，瞬间心理防线崩塌“压力山大”了起来。将近六年之后，原先立的 flag 还只实现了一半（2014 年推出的那本面向渗透测试技术人员的《Metasploit 渗透测试魔鬼训练营》），flag 的另一半还尚无头绪，只能在这里征集合作者，咱们一起争取“八年抗战”把这立在心头的 flag 拔掉，也算是给一直支持我们的读者朋友还有给我“挖坑”的编辑一个交代。

诸葛建伟

2017 年 6 月 5 日深夜于北京西山

译者序

本书介绍 Metasploit——近年来非常流行和极有发展前途的开源渗透测试框架平台软件，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从2004年横空出世之后，立即引起了整个安全社区的高度关注，作为“黑马”很快就排进安全社区流行软件的五强之列。Metasploit不仅为渗透测试的初学者提供了一款简单易用、功能强大的软件，对于职业的渗透测试工程师而言更是在他们的“兵器库”中增加了一件神器，此外 Metasploit也已经成为安全社区进行软件安全漏洞分析研究与开发的一个通用平台。现在，安全社区中的漏洞利用程序往往以 Metasploit 模块方式进行发布，大量书籍（如著名的《黑客大曝光》系列，国内的《0day 安全：软件漏洞分析技术（第 2 版）》等）也都采用 Metasploit 作为案例讲解分析的基本工具。毋庸置疑，Metasploit 已经是安全社区一颗璀璨的“明星”，成为安全社区各个层次上的技术人员都爱不释手的一款软件。

本书虽不是第一本介绍 Metasploit 软件的书籍（第一本是由 Syngress 在 2007 年出版的 *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research*，但内容组织很差，大部分内容直接照搬一些公开的 Metasploit 文档，Amazon 上都是一星和二星的负面评价），却是第一本真正能够全面且深入地展示 Metasploit 在网络渗透测试和漏洞研究方面强大能力的指南书籍。一方面 Metasploit 在 2007 年之后的 v3.0 版中重新设计并以 Ruby 完全重写，进一步提升了它作为网络渗透测试和漏洞研究框架平台性软件的功能与号召力；另一方面，来自著名黑客团队 Offensive Security 的本书作者们拥有着丰富的网络渗透测试、安全漏洞研究与渗透软件开发的实践经验，他们对网络渗透攻击的基本理论、实施流程，以及 Metasploit 软件及相关工具的使用与开发都非常熟悉和了解。在这本书中，他们不仅对利用 Metasploit 来实施网络渗透测试的各个流程环节进行了细致流畅的描述和案例讲解，还结合他们的实际经验展示了如何在 Metasploit 平台基础上扩展开发模块，以解决一些实际情况中遇到的渗透测试需求。

因此，一方面，本书能够逐步引导网络渗透测试的入门读者了解 Metasploit 的基本框架，

并且结合 Metasploit 软件的功能进行案例讲解，从而使读者能够理解和掌握渗透攻击的基本原理、流程方法与实践技能；另一方面也能为一些较高水平的读者提供 Metasploit 功能的实际参考手册，及进一步扩展 Metasploit 完成实际需求的方法指引。正因为如此，本书也获得了 Metasploit 项目发起人、著名黑客 HD Moore 的好评，并专门为本书撰写了序言。

在本书正式出版之前，译者团队——清华大学信息与网络安全实验室狩猎女神科研小组就一直在渗透测试与漏洞分析技术的学习、探索和研究中使用 Metasploit 框架软件，也在今年 5 月开始规划一本向国内读者全面介绍 Metasploit 的原创书。然而到 6 月我们就关注到了 Offensive Security 黑客团队创作的 Metasploit 书籍马上要于 7 月出版，而且和我们之前所规划的原创书目标基本一致，同时我们对 Offensive Security 黑客团队之前维护的“Metasploit 揭秘”在线教程质量非常认可，因此对他们出版的 Metasploit 书籍的质量与市场销售前景也非常看好，所以选择将此书推荐给电子工业出版社进行引进翻译，电子工业出版社也很顺利地与外方出版社签订了版权引进协议。令我们意想不到的是本书在 Amazon 上的市场销售表现甚至超过了我们的预期，在 7 月本书出版后的相当长一段时间内，都占据了 Amazon“安全与加密”类技术书籍的销量冠军宝座，直到让位于 8 月出版的米特尼克自传。

HD Moore 在为本书撰写的序言中说：“为 Metasploit 写一本书根本就是一种自虐行为：完成的一章刚刚经过了试读，可能它里面的内容就已经过时了”。为了尽快让国内读者阅读到这本“新鲜出炉”极具影响力的 Metasploit 参考指南，译者团队在接受出版社的翻译任务之后，就“马不停蹄”地开始了翻译工作，由于我们对 Metasploit 都有较多的了解与实践经验，书籍专业内容方面并没有给我们带来太多障碍。正值学校暑假，因此译者团队也都投入了充分的时间来保障翻译质量，在书籍翻译所要达到的“信、达、雅”目标中，我们自信能够基本达到前两个目标。

对于“信”，我们在分配翻译任务时考虑了每位译者的技术优势和关注点，来保证对翻译内容的技术掌控，从而能够忠实地描述出原书作者期望传递给读者的技术知识。在翻译过程中，对于不太确认的一些疑问点，我们也祭出 Metasploit 软件进行实验验证，并将发现的几个原作者由于疏忽而引入的错误通过出版社提交给原作者进行勘误。对于“达”，我们在翻译之前对全书出现的技术词汇进行了整理与翻译对照，统一全书对关键技术词汇的翻译，并在初译结束之后，由诸葛建伟进行全书内容的语句修改、润色与审校。完成修改之后的初稿又由各自负责的译者进行试读、修改与格式调整，最后由诸葛建伟与责任编辑进行全书通读、审校与文字修改，通过认真负责的翻译与审校，应能保证最终译稿的达意。而对于翻译的最高境界“雅”，作为具有很强时效性需求的技术类书籍，译者团队在权衡之后，还是选择更加注重在确保前两者翻译质量目标的前提下尽快完成译稿，从而让本书更快与国内读者见面，因此在翻译的“雅”上会有所欠缺，也请读者们谅解。

本书的读者群主要是网络与系统安全领域的技术爱好者与学生，渗透测试与漏洞分析研究

方面的安全从业人员，由于 Metasploit 在国外安全社区中已经成为事实上的渗透测试与漏洞分析平台，相信国内也会有很多对此书感兴趣的读者。在本书翻译过程中，译者也发现国内安全社区对本书非常关注，并对中文版的尽早问世给予了很高的期望，也有两位热心人士计划自愿进行翻译，并分享给社区。然而由于本书是具有版权的发行作品，因此译者善意提醒了他们可能存在的侵权法律问题，也告知他们译者团队在当时已经完成了全部章节的初稿翻译并已进入到审校阶段，他们也非常配合地放弃了重复翻译的想法。而这次小风波也反映了国内安全社区对本书的期待，也促使译者团队尽快完成了书稿翻译与审校，为国内读者们献上一本具有良好翻译质量的 Metasploit 经典作品。

客观而言，本书也还存在着一些不足之处，比如没有包含目前非常热门的 Web 应用渗透攻击测试与漏洞分析内容，渗透技术方面没有紧跟发展潮流（如 VoIP、 SCADA、移动平台等热点攻击技术），没有引入真实的渗透测试案例以说明 Metasploit 在实际网络渗透测试中的实用性等等。当然，“瑕不掩瑜”，这并不妨碍本书能够成为一本优秀的网络渗透测试专业书籍。这也为我们进一步开发出更加全面深入的原创书提供了空间，而译者团队在充分吸收本书技术精华之后，也仍有计划推出基于最新发布的 Metasploit v4.0，分别面向渗透测试技术人员、漏洞研究与利用技术人员的 Metasploit 宝典姊妹篇，也请国内感兴趣的读者们给予关注。

本书翻译工作的具体分工是：诸葛建伟译序、前言和第 1、2、13、14、15、17 章，王珩译第 3、4、5、7、9 章，孙松柏译第 10、11、16 章和附录 B，李聪译第 6 章，陈力波译第 8 章，田繁译第 12 章与附录 A。全书内容由诸葛建伟进行全面、仔细的统稿与审校。

在本书的版权引进和翻译过程中，电子工业出版社的毕宁编辑给予了我们非常大的支持，顾慧芳编辑在审核、校对与排版等方面付出了辛勤的劳动。在此，一并表示深切的谢意。

诸葛建伟

2011 年 8 月于北京清华园

作者序

Metasploit 框架跻身信息安全职业者们最广泛使用的工具软件行列已经相当长时间了，但是除了源码本身和在博客上的一些评论之外，有价值的文档却一直非常少。这种状态在 Offensive Security 团队开发了“Metasploit 揭秘”在线教程之后得到了显著改观。在这部教程上线之后不久，No Starch 出版社就联系我们探讨扩展“Metasploit 揭秘”教程来编写一本参考书的可行性。

而这本书就是设计来让你了解 Metasploit 的输入输出，以及如何极致地发挥 Metasploit 框架能力的。而我们的章节内容覆盖也是经过深思熟虑和精心选择的——我们不会覆盖到每个参数或渗透攻击模块，但我们会让你了解必须掌握的基础技术，以及现在和将来如何使用 Metasploit 的方法。

开始写作本书时，我们得到 Metasploit 项目创始人 HD Moore 的一次善意提醒。在和 HD 的一次关于开发我们的“Metasploit 揭秘”在线教程的谈话中，我们中的一位成员对他说了一句：“我想教程质量会很好的”。对于这句漫不经心的自我评价，HD 仅仅回应了一句“那就确保好的质量吧”。这就是我们期望本书所达到的效果。

作为一个团队，我们都是富有经验的渗透测试师，每天都在使用 Metasploit 框架系统性地挫败安全控制措施、绕过防御机制，并攻击系统。我们写作此书的目的是帮助读者成为具备能力的渗透测试师。HD 对高质量的关注和追求也在 Metasploit 框架中得到了非常显著的体现，我们也期望本书能够达到与之相匹配的程度。而我们到底完成得如何，这将由你们来判断。

致 谢

我们要对许多人致以谢意，首先是那些辛勤工作并为社区提供了如此一款优秀软件的勇士们。特别的感谢致以 Metasploit 开发团队：HD Moore, James Lee, David D. Rude II, Tod Beardsley, Jonathan Cran, Stephen Fewer, Joshua Drake, Mario Ceballos, Ramon Valle, Patrick Webster, Efrain Torres, Alexandre Maloteaux, Wei Chen, Steve Tornio, Nathan Keltner, Chris Gates, Carlos Perez, Matt Weeks 和 Raphael Mudge。另外一个额外的感谢给 Carlos Perez，他帮助我们编写了 Meterpreter 脚本章节的部分内容。

非常感谢本书的技术评审 Scott White，感谢他令人敬畏的工作态度。谢谢 Offensive Security 团队将我们团结在一起，Offensive Security 团队的座右铭“Try Harder”经常激励和折磨我们的灵魂（包括邪恶的 ryujin）。

我们还有许多信息安全社区的同仁们要感谢，但要感谢的人实在太多了，难以在此一一列举，而且遗漏某人的几率很高。所以——我们对安全社区中的所有朋友们表示感谢，致以我们所有人最热烈的拥抱。一个非常特殊的致谢送给 No Starch 出版社全体同仁们，感谢他们为本书出版所做出的难以衡量的努力工作。Bill、Alison、Travis 和 Tyler，与你们和 No Starch 出版社幕后工作的所有人共同工作，我们非常高兴！

最后，非常非常感谢我们的家人，我们都已经结婚而且一半都已经有了孩子，我们花了太多的时间在键盘上，而没有足够的时间和他们在一起。对于我们的家人，谢谢你们的理解，我们将马上回报你们——等我们搞定下一行代码，或找出这个内存破坏的源头，或 svn 更新完代码，或把这个 Fuzz 测试跑起来，或……

个人特别致谢

Dave（Twitter: @dave_rel1k）：我将本书（我的那部分工作）献给我可爱的妻子 Erin，她忍

受了我在深夜中不断地敲击键盘。献给我的三个孩子，他们让我同时年轻和老成。献给我的父亲 Jim 和母亲 Janna，以及继母 Deb，谢谢他们和我在一起并培养我成才。感谢 Jim、Dookie 和 Muts 在本书中付出的辛勤工作，以及成为我的好朋友。感谢我在 Offensive Security 团队中的好友 Chris“Logan”Hadnagy、我的兄弟 Shawn Sullivan，以及我在 Diebold 公司的同事们。感谢我的好朋友 HD Moore，他对安全业界的专注和投入给我们很多启示。感谢在我生活中的所有朋友，谢谢 Scott Angelo 给我一个机会并信任我。最后，感谢上帝，没有他，这世上没有人能够存在。

Devon（@dookie2000ca）：感谢我美丽且包容的妻子。你不但支持还鼓励了我对技术的狂热，你不仅仅是我的灵感与动力的源泉，如果没有你在这些事务中为我考虑，我将永远不可能取得任何成绩。感谢我的合作者，谢谢你们信任我这个新人并接受我入伙。特别要感谢 Mati，不仅组建了这支欢乐的乐队，还给我也提供了机会。

Muts（@backtracklinux）：特别感谢本书的合作者，他们对本书投入的时间和热情真是令人鼓舞。我将 Jim、Devon 和 Dave 看作最好的朋友和在安全领域最好的伙伴。

Jim（@_Elwood_）：谢谢 Matteo、Chris “Logan”和所有 Offensive Security 团队的伙伴们。另外也很感谢 Robert、Matt、Chris 和我在 StrikeForce 的同事们。谢谢我的好妻子 Melissa：你手中拿着的这本书是证明我之前并非有意逃避家务劳动的证据。感谢 Jack 和 Joe，请不要在妈妈面前揭发我告诉她“我正在工作”的时候是在和你们一起玩游戏，你们三个人是我生命中最重要的人。最后感谢我的合作者 Mati、Devon 和 Dave：谢谢你们让我把名字署在书上——我真的是在逃避家务。

作译者介绍

作者简介

David Kennedy Diehold 公司首席信息安全官，社会工程学工具包（SET）、Fast-Track 和其他开源工具的作者，他同时也是 Back Track 和 Exploit Database 的开发团队成员，以及社会工程学博客网站的核心成员。Kennedy 曾在 Black Hat、Defcon、ShmooCon、Security B-Sides 等一些安全会议上发表过演讲。

Jim O'Gorman CSC 公司 StrickForce 团队的职业渗透测试工程师，Social-Engineer.org 网站的共同创办者，Offensive Security 团队的培训讲师。他经常进行数字取证分析调查和恶意代码分析，并协助在 Back Track 中集成取证分析工具。在业余时间里，他会帮助自己的孩子们大战僵尸。

Devon Kearns Offensive Security 团队的培训讲师，Back Track 的开发者，以及 Exploit Database 网站的管理员。他也为 Metasploit 贡献过一些渗透攻击模块，并且是《Metasploit 揭秘》教程 Wiki 的维护者。

Mati Aharoni Back Track 发行版的创建者，以及安全培训界领军团队 Offensive Security 的创始人。

译者简介

诸葛建伟 博士，清华大学网络空间安全研究室副研究员，狩猎女神科研团队负责人，蓝莲花战队联合创始人及领队，XCTF 联赛发起人及组委会副主任委员，信息安全领域培训讲师和自由撰稿人，撰写和翻译过多部教材和技术书籍。个人网站：netsec.ccert.edu.cn/zhugejw。

王珩 清华大学硕士毕业，蓝莲花创始团队队员，资深信息安全从业者，在 Web 应用程序安全、网络渗透测试等方面有丰富的实践经验，现任赛宁网安副总经理、产品总监。微博：@evan-css。

孙松柏 清华大学硕士毕业，从事网络安全相关工作十余年，在 Web 渗透测试等方面有丰富实践经验。

陆宇翔 北京邮电大学信息安全专业毕业，现就职于赛宁网安，参与网络安全实训产品的相关工作。

前 言

想像一下在不久的将来，一位攻击者决定要攻击一家跨国企业的数字资产，目标是从花费数百万美元构建的安全防御基础设施中挖掘出价值数亿的知识产权。攻击者很娴熟地祭出“神器”——最新版本 Metasploit，在攻破目标组织的网络边界防御之后，他找到了一个“软肋”，并有条不紊地实施一系列渗透攻击，但是直到他攻陷网络中每一个角落之后，好戏才刚刚上演。他在系统之间神出鬼没，寻找核心业务组件，而企业仍然在按部就班地运营，没人能够察觉到他的存在。弹指之间，他让数百万美元的安全防御设施灰飞烟灭，将公司最敏感的知识产权数据手到擒来。

恭喜你完成了一次漂亮的工作，你已经展示出真正的业务影响和后果，现在是写报告和收钱的时候了。令人称奇的是，现今的渗透测试者就已经处在上面场景所描述的假想攻击者角色，应那些需要高度安全等级的企业邀请，来实施合法的攻击。欢迎来到渗透测试的神奇世界。

为什么进行渗透测试？

企业在保护关键基础设施的安全计划中投入数百万美元，来找出防护盔甲的缝隙，防止敏感数据外泄。而渗透测试是能够识别出这些安全计划中的系统弱点与不足之处的一种最为有效的技术方式。通过尝试挫败安全控制措施并绕开防御机制，渗透测试师能够找出攻击者可能攻陷企业安全计划、并对企业带来严重破坏后果的方法。

当你在阅读本书时，请记住你并不是非要攻陷哪个或者哪些系统，你的目标是以一种安全和受控的方式，来展示攻击者可以如何对一个组织造成严重破坏，并影响它的业务盈利、维持声誉和保护客户的能力。

为什么是 Metasploit?

Metasploit 并不仅仅是一个工具软件，它是为自动化地实施经典的、常规的，或复杂新颖的攻击提供基础设施支持的一个完整框架平台。它使你可以将精力集中在渗透测试过程中那些独特的方面上，以及如何识别信息安全计划的弱点上。

当你通过逐章阅读本书并建立起一个完整全面的渗透测试方法体系的同时，你可以看到如何在你的渗透测试过程中以多种方式来使用 Metasploit 框架软件。Metasploit 能够让你通过选择它的渗透攻击模块、攻击载荷和编码器来轻易实施一次渗透攻击，也可以更进一步编写并执行更为复杂的攻击技术。在本书中，我们也会介绍几个基于 Metasploit 框架所构建的第三方工具——其中一些是由本书作者所编写的。我们的目标是让你充分认识 Metasploit 框架，为你展示一些高级的攻击技术，并确保你能够可靠地应用这些技术。我们希望你能够像我们编写过程中一样享受这本书。进入游戏，让我们开始玩吧！

Metasploit 发展简史

Metasploit 最初是由 HD Moore 所开发和孕育的，当时 HD 只是一个安全公司的雇员，当他意识到他的绝大多数时间是在用来验证和处理那些公开发布的渗透代码时，他便开始为编写和开发渗透代码构建一个灵活且可维护的框架平台。2003 年的 10 月 HD 发布了他的第一个基于 Perl 语言的 Metasploit 版本，当时一共集成了 11 个渗透攻击模块。

HD 于 2004 年 4 月发布了完全重写后的 Metasploit 2.0，这个版本包含了 19 个渗透攻击模块和超过 27 个攻击载荷。在这次发布之后不久，Matt Miller（Skape）加入了 Metasploit 开发团队，随着项目逐步获得关注，Metasploit 框架也获得了来自信息安全社区的大量代码贡献，并很快成为了一个渗透测试与攻击的必备工具。

在使用 Ruby 编程语言进行了一次完全重写之后，Metasploit 团队在 2007 年发布了 Metasploit 3.0。Metasploit 框架从 Perl 到 Ruby 的移植整整花了 18 个月，结果造就了超过 15 万行的新代码。随着 3.0 版本的发布，Metasploit 在安全社区获得了更加广泛的用户群，并在代码贡献方面也得到了快速的发展。

2009 年秋季，Metasploit 被漏洞扫描领域的一家领军企业 Rapid7 公司收购，Rapid7 公司允许 HD 来招募一支团队，专注于 Metasploit 框架的开发。自从被收购之后，Metasploit 上的代码更新比任何人所预期的都要快得多。Rapid7 公司在 Metasploit 框架的基础上也发布了两款商业版本：Metasploit Express 和 Metasploit Pro。Metasploit Express 是一个带有 GUI 界面的轻量级 Metasploit 框架软件，并增加了一些额外的功能，包括报告生成和其他一些很有用的特性。Metasploit Pro 则是 Metasploit Express 的扩展版本，能够支持以团队协作方式实施的渗透测试过程，并拥有如一键创建 VPN 通道等很多有用的特性。