TURING 图灵程序设计丛书

[PACKT] PUBLISHING

【英】Nipun Jaswal 著 李华峰 译

精通Metasploit渗透测试

Mastering Metasploit

结合网络安全实践，系统阐述Metasploit渗透技术
对当前流行的VOIP、SCADA技术以及移动平台等热点提供精彩讲解
黑客进阶必读

中国工信出版集团 人民邮电出版社 POSTS & TELECOM PRESS

TURING 图灵程序设计丛书

【英】Nipun Jaswal 著 李华峰 译

精通Metasploit渗透测试

Mastering Metasploit

人民邮电出版社
北 京

图书在版编目（CIP）数据

精通Metasploit渗透测试 / （英）贾斯瓦尔（Jaswal,N.）著 ; 李华峰译. -- 北京 : 人民邮电出版社, 2016.6
（图灵程序设计丛书）
ISBN 978-7-115-42352-8

Ⅰ. ①精… Ⅱ. ①贾… ②李… Ⅲ. ①计算机网络－安全技术－应用软件 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2016)第095334号

内 容 提 要

本书是 Metasploit 渗透测试的权威指南，涵盖了使用 Metasploit 实现渗透测试的诸多方面，主要包括：渗透攻击，编写自定义渗透攻击模块，移植渗透攻击模块，测试服务，以及进行复杂的客户端测试。此外，作者还介绍了 Assembly、Ruby 及 Cortana 等语言知识，Metasploit 框架组件与模块，以及使用 SET 和 Fast Track 等工具。

本书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参考。

◆ 著 [英] Nipun Jaswal
译 李华峰
责任编辑 朱 巍
执行编辑 贺子娟
责任印制 彭志环

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京中新伟业印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：18.25
字数：437千字 2016年6月第1版
印数：1－3 000册 2016年6月北京第1次印刷
著作权合同登记号 图字：01-2016-2265号

定价：59.00元

读者服务热线：(010)51095186转600 印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广字第 8052 号

译 者 序

网络渗透攻击是一门新兴的热门技术。对很多人来说，在网络上神出鬼没的黑客如同武侠小说中的侠客一样神秘。那么如何才能成为一名黑客呢？这个问题的答案其实很简单。我个人觉得只需要具备两点：一是丰富的专业知识，二是灵活的思路。但是要做到这两点谈何容易。

我从2004年开始进入计算机教育行业，2009年正式涉足网络渗透领域。在这几年的工作中，我深深地感受到，要成为一名合格的网络渗透人员很难，要培养出一批合格的网络渗透人员则更难。可以说，现在缺乏一种有效的方式来培养网络渗透方面的人才。

目前全国的很多高校都开设了网络攻防或者网络安全方面的课程，但是大多数课程都只限于一个学期，而且很多学校采用的教学内容基本上与十年前没有太大差别。课程短、教学内容陈旧，这在很大程度上导致学生在学校学习的内容与社会的实际情况严重脱节。

这些年我一直在网络攻防的教学上苦苦挣扎，因为缺乏与时俱进的教材，缺乏与时俱进的工具，始终无法建立起一个全面而又实用的教学体系。

直到五年前，我一接触到Metasploit这款工具，就被它强大且全面的能力吸引了。有了Metasploit，只需要输入几条命令，就可以像电影中的黑客那样进行渗透。但是关于这款工具的资料始终很少，因此我一直希望有机会写一本书来系统地阐述Metasploit渗透测试技术。然而由于时间和能力方面的限制，这个愿意始终未能实现。不过幸运的是，前段时间我在图灵社区上发现了由Nipun Jaswal编写的这本*Mastering Metasploit*。这本书详细阐述了Metasploit的实用技术，更为可贵的是，书中的很多示例都结合了作者的亲身实践。另外，本书最让人眼前一亮的是对当前流行的VOIP、SCADA技术以及移动平台等热点技术的精彩讲解。作者以一个渗透者的身份将Metasploit的实用技术娓娓道来，条理清楚，化繁为简，向读者展示了一个神奇的黑客世界。

我一边从事本书的翻译工作，一边在学校里授课，有时难免把一些新的知识搬到课堂上，而最为无辜的大概要数我的这些可爱的学生了，他们总是为无法在教材上找到我讲解的内容而苦恼。在此，我首先要感谢这些孩子。另外，感谢图灵的朱巍编辑等人，在翻译本书的过程中，他们给了我极大的帮助和鼓励，并付出了辛勤的劳动。感谢家人对我的关心、支持和宽容。

最后，欢迎各位有志于从事网络渗透的爱好者和学生与我交流。我的电子邮箱为lihuafeng1999@163.com。

李华峰

2016年3月于唐山

献　词

献给我生命中最重要的两位女士：我的母亲Sushma Jaswal以及我的外祖母Malkiet Parmar。感谢她们对我的爱和支持。

前　言

如今，渗透测试已经成为每一个现代企业都必须掌握的一项关键技术。随着近年来网络和计算机犯罪的逐年递增，渗透测试已经成为网络安全研究的核心问题之一。应用渗透测试技术可以有效地避免来自企业内部和外部的威胁。而企业应用渗透测试的必要性就在于它可以发现网络、系统或者应用程序的漏洞。此外，由于渗透测试是从攻击者的角度出发，因而可以更好地发现企业的弱点和威胁。在发现系统中的各种潜在缺陷以后，渗透测试还要利用这些漏洞来评估系统存在的风险因素以及漏洞可能产生的影响。

不过，渗透测试能否成功很大程度上取决于渗透测试工程师对目标信息的掌握情况。因此渗透测试工程师通常会采用黑盒测试和白盒测试两种截然不同的方法进行工作。黑盒测试指的是渗透测试工程师在事先并没有目标内部信息的情况下开展的测试。因此渗透测试的第一步通常是系统地收集目标的信息。而在进行白盒渗透测试时，渗透测试工程师事先掌握了足够的目标环境的内部信息，可以直接验证目标系统可能存在的安全漏洞。

通常一次完整的渗透测试包含下面七个阶段。

(1) 前期交互阶段

在前期交互阶段，渗透测试工程师要确定渗透测试预期达到的目标，并确定测试的范围。渗透测试工程师将在这个阶段与客户展开讨论，确定本次渗透测试的所有业务与细节。

(2) 信息收集阶段

在信息收集阶段，渗透测试工程师在确定了目标和范围以后，就要采用主动和被动两种方法收集目标信息。其中被动信息收集可以在完全不接触目标的情况下进行。

(3) 威胁建模阶段

在威胁建模阶段，渗透测试工程师要根据之前获得的信息，找出对目标系统威胁最大的弱点，从而确定最为高效的渗透攻击方式。

(4) 漏洞分析阶段

在漏洞分析阶段，渗透测试工程师要找到并确认目标系统上存在的已知的和未知的漏洞，然

后在实验环境中进行验证。

(5) 渗透攻击阶段

在渗透攻击阶段，渗透测试工程师要利用之前得到的成果来入侵目标系统的漏洞。这意味着在这个阶段渗透测试工程师会尝试去获得目标系统的控制权。

(6) 后渗透攻击阶段

在后渗透攻击阶段，渗透测试工程师要开展一些实际的入侵行为。例如，盗取目标计算机的某个机密文件，直接关闭目标系统，或者在目标系统上创建一个新的远程管理账户，等等。一般来说，在这个阶段渗透测试工程师应该完成渗透攻击后的所有工作。

(7) 报告阶段

在报告阶段，渗透测试工程师需要将所有渗透测试过程中的工作进行汇总，并以书面报告的形式提交给客户。报告中还应该包括漏洞修补和安全升级的解决方案。

当渗透测试的目标仅仅是一台计算机时，完成以上七个阶段的难度似乎不大。可是当渗透测试工程师要面对的目标环境包含数以百计的计算机时，一切就不那么容易了。因此在对大型网络进行渗透测试的时候，往往需要使用自动化渗透测试框架来代替手工测试。可以设想这样一个场景，渗透的目标刚好包含了一百台运行着同样操作系统以及提供相同系统服务的计算机。如果渗透测试工程师手动对每一台计算机进行测试，那么将会耗费掉大量的时间和精力。这种复杂情况正是渗透测试框架可以应对的，通过使用渗透测试框架不仅会为渗透测试工程师节省大量时间，同时也可以提供更多和更加灵活的渗透测试方法。渗透测试框架可以帮助你自动实现大部分工作，例如对攻击向量、扫描过程、漏洞识别以及最重要的漏洞渗透攻击的处理，从而节省时间并控制节奏。

本书的目标就是为读者介绍世界上最为流行的渗透测试框架Metasploit。本书着重介绍在以下几个方面掌握Metasploit：渗透攻击、编写自定义渗透攻击模块、移植渗透攻击模块、测试服务以及进行复杂的客户端测试。本书还会指导读者将用指定的Ruby、汇编或者脚本语言（如Cortana）编写的外部渗透测试模块转换成Metasploit中的模块。阅读本书还将有助于提高读者的编程能力。

本书内容

第1章　走近Metasploit渗透测试框架。这一章将带领读者完成一次基础的渗透测试过程。这将有助于读者初步认识Metasploit，同时学会搭建测试环境。此外，还将带领读者系统地认识渗透测试的各个环节。最后介绍了与传统测试和人工测试相比，采用Metasploit渗透测试框架进

行渗透测试的优势。

第2章　打造定制化的Metasploit渗透测试框架。这一章中涵盖了编写Metasploit模块所必需的Ruby编程语言的基础知识，还介绍了如何掌握Metasploit的现有模块以及编写自己的模块，例如扫描模块、后渗透攻击模块、meterpreter模块。最后介绍了如何使用RailGun开发自定义模块。

第3章　渗透攻击模块的开发过程。这一章阐述了如何完成一个渗透攻击模块的开发过程，同时涵盖了必需的汇编语言基础知识。之后谈及了fuzz测试和调试器，着重讨论了如何通过分析调试器下应用程序的行为来收集必需的开发信息。最后展示了依靠收集来的信息在Metasploit模块下开发一个渗透攻击模块的过程。

第4章　渗透攻击模块的移植。这一章将帮助我们将那些已经公开的可用渗透工具移植到Metasploit框架中。这一章重点描述了如何找出那些使用Perl、Python以及PHP语言编写的模块的核心功能，并通过Metasploit库将这些功能转化为与Metasploit框架兼容的模块。

第5章　服务测试技术的幕后揭秘。这一章阐述了如何对各种服务进行渗透测试。首先介绍了一些重要的专门用来渗透SCADA（信息采集与监控）服务的Metasploit模块。之后讨论了针对数据库的测试，以及在其上运行的特权命令。接下来揭示了如何对VOIP进行欺骗性攻击。最后介绍了苹果设备上的后渗透攻击模块。

第6章　虚拟化测试的原因及阶段。这一章对如何开展白盒测试和黑盒测试进行了简要的论述。首先着重介绍了其他可以与Metasploit结合使用共同完成渗透测试任务的工具。之后展示了当前流行的漏洞扫描工具，例如Nmap、Nessus和OpenVAS，讲述了如何将这些软件的扫描报告导入到Metasploit中，并在Metasploit中运行这些工具。最后介绍了如何手动和自动生成渗透报告。

第7章　复杂的客户端攻击。这一章将学习重点转移到了客户端渗透攻击，重点讨论了如何从传统的客户端渗透攻击转变为更为复杂精准的方式。首先介绍了一个基于浏览器的渗透攻击和一个基于文件格式的渗透攻击模块。之后阐述了对被渗透的Web服务器和网站用户的影响。接下来演示了如何绕过目标的反病毒和安全保护机制。最后展示了如何通过Metasploit中的DNS欺骗模块，将浏览器的渗透攻击模块变成一个致命的武器。

第8章　社会工程工具包。这一章介绍了将Metasploit作为后台工具与社会工程工具包结合使用来发起自动化客户端攻击。这一章展示了各种网络页面攻击向量以及高级的网络钓鱼攻击手段。重点介绍了攻击向量，例如最新的浏览器标签劫持、Java applet伪装等。还讲解了目前最为优秀的社会工程工具包内的模块功能。最后讲解了如何使用社会工程工具包的图形用户界面，以及如何实现各种攻击的自动化。

第9章　提高渗透测试的速度。这一章主要介绍如何加快渗透测试的进程。首先介绍了Fast Track工具，并演示了使用Fast Track渗透攻击数据库的过程。之后讨论了一些在当前版本中已经去除了的Metasploit的经典功能，以及如何能够再次使用这些功能。最后，展示了另一个强大的

工具WebSploit，并利用它实现了一次巧妙的客户端渗透攻击。

第10章 利用Armitage实现Metasploit的可视化管理。Armitage是目前最流行的专门为Metasploit设计的图形用户界面。这一章首先使用Armitage进行目标扫描和目标渗透。然后讨论了Cortana，它可以用来开发在Armitage下的自动化攻击脚本以及开发虚拟机器人来辅助渗透攻击。最后讨论了如何在Armitage中添加自定义功能以及构建自定义界面和菜单。

本书要求

如果读者想完成本书中的示例，将需要两到三台计算机，其中一台作为渗透测试机，另外两台可以作为渗透测试的靶机。如果读者的硬件资源十分有限，也可以在同一台计算机上运行多个虚拟机来搭建渗透测试实验环境。

除此以外，读者还需要最新的Kali Linux安装镜像文件，Kali作为Metasploit的运行平台，同时集成了本书提到的其他渗透测试工具。

另外读者还需要Ubuntu、Windows XP、Windows Server 2003、Windows 7和Windows Server 2008这几个系统作为渗透测试的靶机。值得注意的是，本书会介绍所有其他工具及其具体版本。

读者对象

本书的读者群主要是从事专业渗透的测试者，安全领域的工程师，对Metasploit有简单了解并想要精通的分析师，希望提升渗透攻击模块编写能力的人，以及希望掌握各种服务的渗透测试技能的读者。此外，本书也可以帮助那些想将自己的模块添加到Metasploit渗透测试框架中的研究人员。通过阅读本书，读者将平稳地完成从一个初中级使用者到专家的转变。本书会涉及Ruby编程、汇编语言以及使用Cortana编写攻击脚本等内容，因此阅读本书需要具有一定的编程基础。

排版约定

本书采用了不同的文本格式，以区分不同类型的信息，以下是这些格式的解释。

正文中的代码、用户输入会以等宽字体进行表示，如：“这可以用`db_export`方法来实现。”

代码块的表示如下所示：

```
require 'msf/core'
require 'rex'
require 'msf/core/post/windows/registry'
class Metasploit3 < Msf::Post
```

```
include Msf::Post::Windows::Registry
def initialize
  super(
      'Name'          => 'Drive Disabler Module',
      'Description'   => 'C Drive Disabler Module',
      'License'       => MSF_LICENSE,
      'Author'        => 'Nipun Jaswal'
    )
  End
```

命令行输入和输出如下所示：

```
#services postgresql start
#services metasploit start
```

新术语或者关键词会使用楷体表示。

这个图标表示警告或需要特别注意的内容。

这个图标表示提示或者技巧。

读者反馈

我们欢迎读者的反馈意见。如果对本书有任何的想法，喜欢或者不喜欢哪些内容，都可以告诉我们。这些反馈意见对于帮助我们创作出对大家真正有所帮助的作品至关重要。

你可以将一般的反馈以电子邮件的形式发送到feedback@packtpub.com，并在邮件主题中包含本书书名。

如果你在某一方面很有造诣，并且愿意著书或参与合著，可以参考我们的作者指南http://www.packtpub.com/authors。

客户支持

现在你已经是我们Packt图书的尊贵读者了，我们会尽力帮助你充分利用手中的书籍。

勘误

虽然我们已尽力确保本书内容正确，但出错仍旧在所难免。如果读者在书中发现任何文字或者代码错误，欢迎将这些错误提交给我们，以便帮助我们改进本书的后续版本，从而避免其他读者产生不必要的误解。如果读者发现了错误，请访问网页http://www.packtpub.com/submit-errata，选择相应图书，单击errata submission form链接，然后填写具体的错误信息即可。勘误一经核实，读者的提交将被接受，此勘误将被上传到本公司网站或添加到现有勘误表。读者可以通过在网页http://www.packtpub.com/support上选择书名来查看该书的勘误表。

侵权声明

版权问题是每一个媒体都要面对的问题。Packt非常重视版权的保护。如果读者发现我们的作品在互联网上以任何形式被非法复制，请立即告知我们相关网址或网站名称，以便我们采取措施。

请将可疑盗版材料的链接发到copyright@packtpub.com。

非常感谢读者帮助我们保护作者的权益。

问题

如果对本书有任何方面的疑问，都可以通过questions@packpub.com与我们联系，我们将尽最大的努力解决。

致　谢

感谢母亲在人生的每一个关键阶段对我的帮助。感谢Youssef Rebahi-Gilbert先生提供的所有帮助以及创造性想法。感谢Joel Langill先生、Maninder Singh博士、Sagar A. Rahalkar先生、Krishan P. Singh先生和Kubilay Onur Gungor先生百忙之中抽出时间来审阅本书，以及在每一个阶段对我的帮助。感谢印度拉夫里科技大学的Gurpreet Singh先生和其他专家的不断支持。感谢Packt出版公司的Swati Kumari女士、James Jones先生、Akshay Nair先生和Kapil Hemnani先生，他们是一个优秀的团队，帮助我完成了本书写作的每一个阶段。感谢Packt出版公司的整个团队，他们给了我写作并出版本书的机会。最后，感谢全能的上帝给予我巨大的力量，让我得以完成这个项目。

目　录

第1章 走近Metasploit渗透测试框架

渗透测试是一种有目的性的、针对目标机构计算机系统安全的检测评估方法。渗透测试可以发现系统的漏洞和安全机制方面的隐患，并以此进行渗透攻击来取得目标计算机的控制权。通过渗透测试可以知道目标机构的计算机系统是否易于受到攻击，现有的安全部署是否能完善地抵御攻击，以及哪部分安全机制可能被绕过，等等。渗透测试的主要目的是改善目标机构的安全性。

正所谓“工欲善其事，必先利其器”，渗透测试能否成功很大程度上取决于测试时是否使用了正确的工具和技术。渗透测试工程师必须选择正确的渗透测试工具和技术，才能保证任务的完成。当提到最优秀的渗透测试工具时，安全业界的绝大多数人士都会首先想到Metasploit渗透框架。现在，Metasploit被公认是进行渗透测试最有效的安全审计工具，它提供了最全面的漏洞渗透模块库，集成了优秀的模块开发环境，具有强大的信息收集和Web测试能力及其他许多功能。

本书不仅介绍了Metasploit渗透框架的功能与用法，同时也重点讲解了如何开发Metasploit模块和扩展Metasploit框架。本书假定读者已经掌握了Metasploit渗透框架的基础知识。在本书的部分章节中，我们也将带读者回顾一些Metasploit渗透框架的基础性操作。

根据本书涵盖的所有知识，我们将按照下图所示的流程进行讲述。