Mastering Metasploit
Second Edition

精通Metasploit渗透测试（第2版）

[英] Nipun Jaswal 著 李华峰 译

- 结合网络安全实践，系统阐述Metasploit渗透技术
- 包含大量对移动设备、SCADA、数据库、物联网设备的渗透案例

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

Mastering Metasploit
Second Edition

精通Metasploit渗透测试
(第2版)

[英] Nipun Jaswal 著 李华峰 译

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 : 第2版 / (英) 尼理·贾斯瓦尔 (Nipun Jaswal) 著 ; 李华峰译. -- 2版. -- 北京 : 人民邮电出版社, 2017.10
(图灵程序设计丛书)
ISBN 978-7-115-46940-3

Ⅰ. ①精… Ⅱ. ①尼… 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(2017)第235909号

内 容 提 要

本书介绍了时下流行的渗透测试框架——Metasploit。书中从其基本功能和传统使用方式开始，讲解编写 Metasploit 模块的基础知识，学习渗透模块的执行、构建与移植，详细解读客户端攻击、Metasploit 框架中的各种内置脚本。

与第 1 版相比，第 2 版增添了大量对移动设备、SCADA、数据库、物联网设备的渗透案例，并讲解了如何将全新的渗透模块导入到 Metasploit。此外，还囊括了大量出色的专业工具使用教程，采用了新版的社会工程学工具包，增加了大量经典详实的渗透模块编写实例。

本书适合网络与系统安全领域的技术爱好者和学生，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　夏静文
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
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：18
字数：443千字　2017年 10 月第 2 版
印数：3 001－6 000册　2017年 10 月北京第 1 次印刷
著作权合同登记号　图字：01-2017-4858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：京东工商广登字 20170147 号

站在巨人的肩上

Standing on Shoulders of Giants

iTuring.cn

版权声明

纪念所有为国捐躯的英勇战士。

译 者 序

如果要选出2017年最热门的词汇，一定非“网络安全”莫属。从年初勒索者病毒大爆发，到年中《中华人民共和国网络安全法》的施行，这一切都表明网络安全已经成为了国家发展的一个重要问题。可是如何才能有效保证网络安全呢？

著名电影《金蝉脱壳》中曾经提到了一种特殊的职业——监狱安管专家。史泰龙饰演的雷·布雷斯林是最强的越狱高手，曾在8年内成功逃出14座安全防卫工程最严密的重刑监狱。而他的真正身份是美国国家安全局的监狱安管专家，每一次成功越狱，就代表他能找出该监狱的安管漏洞，进而强化改善。现在和上面例子中提到的监狱安管测试相类似的网络安全渗透测试也应运而生。

目前，我国的网络安全渗透测试行业还存在着巨大的缺口。随着互联网的高速发展，对渗透测试的需求将会越来越大。国内的网络安全渗透测试正处于起步阶段，从业人员大都是编程和网络经验都极为丰富的计算机从业人员。不过，随着Metasploit的问世，渗透测试技术将不再专属于那些高高在上的计算机天才。Metasploit作为一款开源的渗透测试工具，能够帮助你像电影中的专业人士一样，仅凭轻轻敲打几下键盘就完成整个渗透测试。而你所需要掌握的，只是敲击几个简单的命令。

但是和所有的开源软件一样，强大的Metasploit也一直都没有一本全面而又详细的使用教程。这种情形就如同把M16突击步枪摆在古代人面前一样——缺乏系统的指导和训练，任何利器都无法发挥作用。缺少一本详实深入的教材，也正是像我这样的教师最为苦恼的。

幸运的是在2015年的时候，我在图灵社区发现了Nipun Jaswal编写的《精通Metasploit渗透测试（第1版）》，而且还有幸承担了这本书的翻译工作。作者以丰富的行业背景、幽默的语言风格使这本书异常的精彩。可以说，这本书对Metasploit的讲解在国内甚至国际范围内都是极出色的。作为一名经验丰富的渗透测试专家，Nipun Jaswal将自己的经验与Metasploit的实际应用相结合，介绍了大量罕见且使用价值极高的技术。在《精通Metasploit渗透测试（第1版）》面世之后，我收到了来自读者的大量电子邮件，这些读者包括高校网络安全方面的教师、专业从事网络渗透测试的工程师、有志于此的大学生和爱好者，甚至还有从事网络安全管理的警察。从各行各业读者的反馈来看，这本书是相当成功的。

Nipun Jaswal在一年之后，将原先的版本重新整理，又加入了大量与时俱进的内容，出版了

《精通Metasploit渗透测试（第2版）》。相对其他图书，这个更新速度可能显得有些快了，但是对于一本网络安全的图书来说，这个速度却是极为合适的。回头看看这一年，微软的操作系统推出了多少补丁，浏览器的版本又升级了多少次，你就会明白网络安全技术进步得有多快了。

我一直觉得翻译这个职业和演员很像。演员为了演好一个角色就要将自己想象成角色，而翻译的时候，译者也要将自己代入到作者这个角色中，按照作者的思路去考虑问题，甚至模仿作者的语言习惯。一本书翻译完，我发现自己的写作习惯居然也和Nipun Jaswal有几分相像了。也正如人无完人，在这本书的翻译过程中，我发现了其中的一些疏漏和错误，也都在译文中做出了修正或者标注。

本书的翻译工作完结之时，也正是我所在学校又一届毕业生离校的时候。今年的几个毕业班是我从事教学工作以来相处时间最长的班级。在学校的这些年来，他们总得忍受我那些突发奇想的教学方式。也正是这几个班级的同学陪我走过人生最为低落的时候，在此感谢他们对我的善意和包容，我会永远想念他们！

感谢图灵的朱巍和夏静文编辑，在二位的鼓励和帮助引导下，我才能顺利地翻译完全部书稿。

感谢我的母亲，是她将我养育成人，并在人生的每一个关键阶段给予我帮助。感谢我深爱的妻子和可爱的儿子，感谢他们在我翻译此书时，给我无条件的理解和支持。

欢迎有志于从事网络安全渗透的诸位与我交流，我的Email地址为lihuafeng1999@163.com。

李华峰

2017年6月于唐山

序　言

随着科技的发展，IT安全已经不只是一项需求，还是每个组织都必须遵循的一项实践。渗透测试是一种保证企业和组织免受来自外部和内部威胁（信息泄露，对各种资源、关键业务数据等的非法访问）的方法。

专业机构提供的渗透测试和漏洞评估等服务可以理解为雇用一群专家入侵组织的网络，从而避免日后其他人的入侵。不过，世界各地的执法机构对渗透测试这一概念有着完全不同的理解。

渗透测试包括很多阶段，通常从收集目标信息开始，继而扫描各种开放的入口（也就是端口扫描），利用漏洞进入系统，保持对目标的访问控制，最后清除所有痕迹。

最近，0day漏洞和高级持久性威胁导致大大小小的企业泄露了关键数据，占领了全世界的网络安全舞台。因此，渗透测试工程师的职业生涯目前充满了挑战，他们必须不断学习并掌握最新的渗透工具和技术。

这本书用一种非常实用的方法介绍了渗透测试。作者是一位著名的安全专家，上至企业安全架构，下至漏洞模块的编写，他都有十分丰富的经验。

现在市面上有很多关于渗透测试的图书，也有很多图书介绍了渗透测试领域的专用安全工具。本书完美地结合了这两者，同时详细介绍了当前使用最为广泛的渗透测试框架Metasploit的使用方法。

Metasploit作为使用最广泛的渗透测试框架之一，从各类企业到执法机构都能看到它的身影。Metasploit包含了1500多个模块，所涉及的功能涵盖了渗透测试的各个阶段，渗透测试工程师利用这些模块可以轻松完成渗透测试工作。Metasploit不仅提供了全面、有效的渗透测试方法，同时还是一个开源框架，提供了广泛的功能，例如新漏洞的开发与各种任务的自动化，从而减少了大量的人工工作，也节省了大量的时间。

在大型社区的支持下，Metasploit的技术和工具也不断更新。这个更新过程十分频繁，有的技术可能一夜之间就更新了，因此本书的编写过程也变得十分艰难。我相信你会体会到本书所涉及技术的价值，它们对你的未来职业生涯也会有很大的帮助。

J.P. Singh少将，Shaurya Chakra奖章获得者（已退役）
理学硕士、工商管理硕士、管理科学硕士、哲学硕士
印度亚米提大学主任

前　言

如今，在商业领域到处都需要渗透测试。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开展工作。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7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，渗透测试工程师应该在这个阶段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7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。这正是Metasploit的作用所在。

Metasploit是目前最优秀，同时也是使用最广泛的渗透测试框架之一。在IT安全社区推广者的支持下，Metasploit不仅满足了一款大型渗透测试工具的需求，也提供了创新性功能，为渗透测试工程师带来了极大的便利。

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。本书着重从以下几个方面掌握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。本章将带领我们使用Metasploit进行一次基础的渗透测试，从而帮助我们学习渗透测试方法和建立渗透测试环境；此外，还将系统讲解渗透测试的各个阶段。

第2章，打造定制化的Metasploit渗透测试框架。本章将系统讲解用来构建Metasploit模块所需的Ruby编程要点，并对现有Metasploit模块的结构进行说明。此外，还将详细介绍如何完成扫描器、认证测试工具、后渗透模块以及登录凭证采集模块的编写。

第3章，渗透模块的开发过程。本章将系统演示渗透模块的开发过程，并研究其中的开发要点；此外，将讲解如何使用程序测试和调试器，以及如何通过在调试器下观察应用程序的行为来收集开发所需要的重要信息；最后，还将演示如何利用这些收集到的重要信息编写一个Metasploit模块，并讨论绕过SEH和DEP这类系统保护机制的方法。

第4章，渗透模块的移植。本章将讲解如何将那些已经公开的可用渗透工具移植到Metasploit框架中，重点描述如何找出那些使用Perl、Python以及PHP语言编写的模块的核心功能，并通过Metasploit库将这些模块转化为成Metasploit框架的一部分。

第5章，使用Metasploit对服务进行测试。本章将带领我们对各种常见服务进行渗透测试，其中还包含了Metasploit中的一些重要模块，这些模块可以用来对SCADA、数据库和VOIP服务进行测试。

第6章，虚拟化测试的原因和阶段。本章将简要介绍使用Metasploit进行渗透测试的过程，并重点介绍那些可以协同Metasploit完成渗透测试任务的工具（例如Nmap、Nessus和OpenVAS）以及它们在Metasploit中的使用方法。最后，将讲解如何手动和自动地生成报表。

第7章，客户端渗透。本章将学习重点转移到了客户端渗透攻击，重点讨论如何将传统的客户端渗透攻击转变得更加复杂、精准。首先，将介绍一个基于浏览器的渗透模块和一个基于文件格式的渗透模块，并讲解这些模块对被渗透的Web服务器和网站用户的影响；然后，将展示如何通过Metasploit中的DNS欺骗模块将浏览器的渗透模块变成一个致命的武器；最后，将讲解如何使用Metasploit来完成对Android和Linux系统的渗透。

第8章，Metasploit的扩展功能。本章将首先研究Meterpreter中提供的基本后渗透功能和高级后渗透功能，并在此基础上进行更深入的研究；同时，还将讨论一些更高级的和基于硬件的后渗透模块。

第9章，提高渗透测试的速度。本章的重点是那些能加快渗透测试速度的策略和脚本，其中不仅会讲解如何加快渗透测试，还会介绍如何在编写渗透模块时利用Metasploit中的辅助功能来节省大量时间；最后，还将讨论如何自动地完成后渗透测试。

第10章，利用Armitage实现Metasploit的可视化管理。本章将会讲解当前Metasploit最为流行的图形用户界面——Armitage，并使用Armitage对目标进行扫描和渗透。此外，还将详细讲解Cortana，并利用它来编写自动化渗透攻击的脚本。最后，将讨论如何在Armitage中添加自定义的功能和创建自定义的界面菜单。

本书要求

如果读者想完成本书中的示例，将需要6到7台计算机，其中一台作为渗透测试机，另外几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。

读者还需要将Ubuntu、Windows XP、Windows 7、Windows Server 2008、Windows Server 2012、Metasploitable 2 和 Windows 10这些系统安装到虚拟机中，或者直接安装到计算机上，因为这些操作系统将成为Metasploit渗透测试的靶机。

此外，本书的每一章都提供了示例中使用的其他工具和存在漏洞的软件的下载链接。

读者对象

本书是Metasploit使用者的渗透测试指南，包含了完整的Metasploit渗透模块开发过程。在这个过程中，你将会见识到大量的技术和方法。通过学习这些技术和方法，你将掌握如何运用Metasploit框架，并且了解如何在高度安全的环境中进行高级渗透测试。

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：

```
def exploit
    connect
    weapon = "HEAD "
    weapon << make_nops(target['Offset'])
    weapon << generate_seh_record(target.ret)
    weapon << make_nops(19)
    weapon << payload.encoded
    weapon << " HTTP/1.0\r\n\r\n"
    sock.put(weapon)
    handler
    disconnect
  end
end
```

当需要特别注意代码块的某一部分时，将会加粗显示。

```
weapon << make_nops(target['Offset'])
weapon << generate_seh_record(target.ret)
weapon << make_nops(19)
weapon << payload.encoded
```

命令行输入和输出如下所示：

```
irb(main):003:1> res = a ^ b
irb(main):004:1> return res
```

新术语或者关键词会使用**黑体**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，并在邮件主题中注明书名。

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。

有关中文版的勘误内容请提交至图灵社区，地址是www.ituring.com.cn/book/2048。

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。

电子书

扫描如下二维码，即可购买本书的电子版。

致　谢

首先，我要感谢本书第1版的每一位读者，是你们造就了本书的成功；感谢我的母亲Sushma Jaswal和祖母Malkiet Parmar，感谢她们在我生命中的每个阶段对我的帮助；感谢Mini Malhotra在本书写作过程中给予我的大力支持；感谢Adrian Pruteanu审阅本书初稿并提出修改建议；感谢Packt这支优秀团队中的每一位成员，包括Prachi Bisht和Trusha Shriyan，感谢他们给我机会从事这个非常精彩的项目；最后，我还要感谢上帝，感谢他赐予我巨大的力量来完成这个项目。