TURING 图灵程序设计丛书

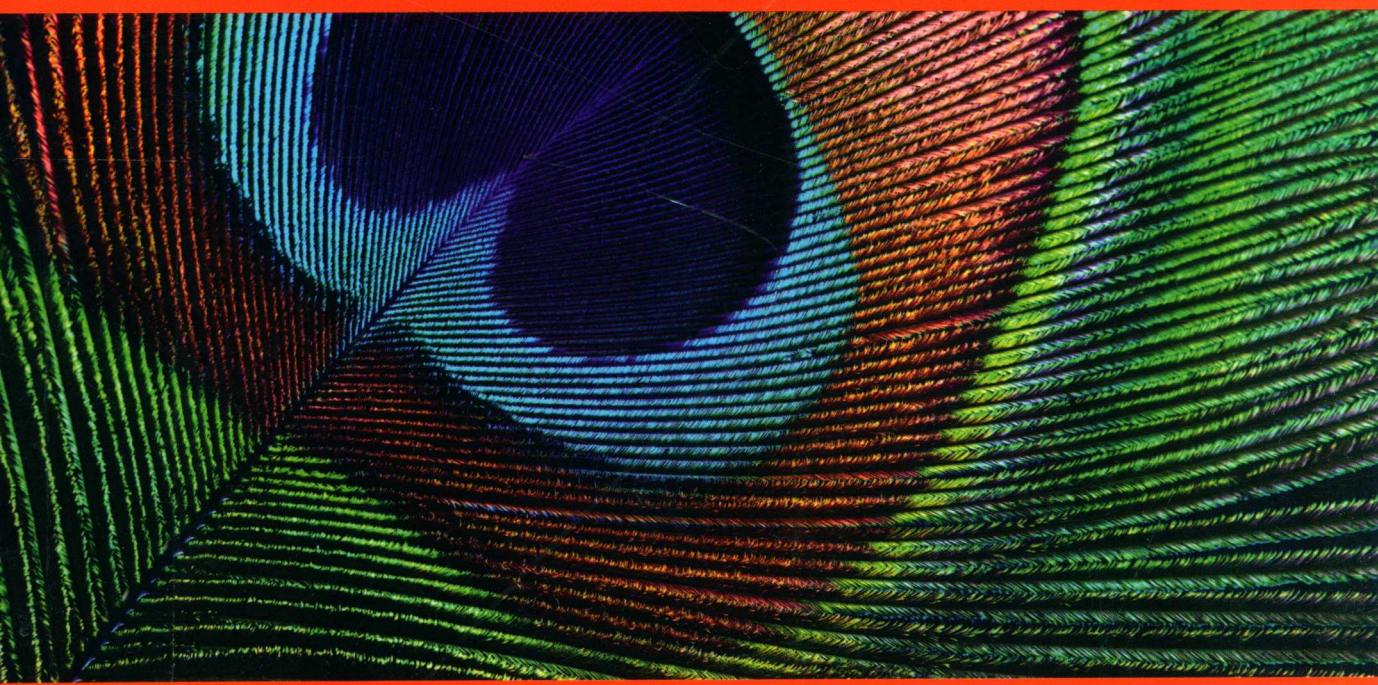
Packt>

Mastering Metasploit, Third Edition

精通Metasploit渗透测试（第3版）

[英] 尼普恩·贾斯瓦尔 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、数据库和VOIP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, Third Edition

精通Metasploit渗透测试

（第3版）

[英] 尼普恩·贾斯瓦尔 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 / （英）尼普恩·贾斯瓦尔（Nipun Jaswal）著 ; 李华峰译. -- 3版. -- 北京 : 人民邮电出版社, 2019.6
（图灵程序设计丛书）
ISBN 978-7-115-51190-4

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(2019)第082350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：渗透测试的基础知识，编写自定义渗透测试框架，开发渗透模块，移植渗透模块，测试服务，虚拟化测试，客户端渗透，Metasploit 中的扩展功能、规避技术和“特工”技术，Metasploit 的可视化管理，以及加速渗透测试和高效使用 Metasploit 的各种技巧。

本书适合渗透测试工程师、信息安全工程师、执法机构分析人员，以及网络与系统安全领域的技术爱好者和学生阅读。

◆ 著　[英] 尼普恩·贾斯瓦尔
译　李华峰
责任编辑　岳新欣
责任印制　周昇亮

◆ 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
三河市祥达印刷包装有限公司印刷

◆ 开本：800×1000　1/16
印张：19.75
字数：467千字　2019年6月第3版
印数：6 001－8 500册　2019年6月河北第1次印刷
著作权合同登记号　图字：01-2019-0843号

定价：79.00元

读者服务热线：(010)51095183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。——尼普恩·贾斯瓦尔

前　言

如今，在商业领域到处都需要渗透测试。近年来，随着网络和计算机犯罪现象的逐年递增，渗透测试已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。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信息的情况下开展的测试。因此渗透测试的第一步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如下 7 个阶段。

- **前期交互阶段**：渗透测试工程师要确定渗透测试的目标和测试范围。他们要和客户讨论渗透测试的所有关键细节。
- **信息收集阶段**：渗透测试工程师采用主动和被动两种方法来收集目标信息，其中被动信息收集可以在完全不接触目标的情况下进行。
- **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。
- **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。
- **渗透攻击阶段**：渗透测试工程师要利用在上一阶段发现的漏洞来入侵目标系统。这通常意味着渗透测试工程师会尝试获得目标系统的控制权。
- **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。总之，渗透测试工程师应该完成渗透攻击后的所有工作。
- **报告阶段**：渗透测试工程师需要将渗透测试的结果汇总为一个文件，并提供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。设想这样一个场景：渗透的目标刚好是 100 台计算机，它们运行着同样的操作系统和服务。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。使用渗透测试框架不仅可以节省大量的时间，同时也可以提供更大的灵活性，从而灵活地改变攻击向量，覆盖更多的目标系统。渗透测试框架还可以将大部分攻击向量、扫描过程、漏洞识别以及（最重要的）漏洞渗透攻击自动化，从而节省时间并控制测试节奏。这就是 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。Metasploit 在 IT 安全社区享有盛名，不仅是一种优秀的渗透测试框架，还有很多创新特性，能让渗透测试更加轻松。

本书的目标就是为你介绍这个传奇性的渗透测试框架。本书着重介绍 Metasploit 渗透测试框架的开发、渗透模块的编写、其他平台成熟渗透模块的移植、系统服务的测试以及复杂的客户端测试。此外，本书还会指导你将用 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。阅读本书不仅能丰富你的渗透测试知识，还能提高你的编程能力。

读者对象

本书的目标读者是专业的渗透测试工程师、信息安全工程师和执法机构分析人员，这些人已经具备了 Metasploit 的基础知识，希望掌握 Metasploit 框架的使用技巧，同时增强渗透模块开发技能。本书还适合想要向 Metasploit 中添加自定义功能的研究人员阅读。本书可帮助初级和中级 Metasploit 框架使用者顺利成长为专家级使用者。此外，本书还讨论了 Ruby 编程和用 Cortana 编写攻击模块脚本，所以读者应该对这些编程语言有所了解。

本书内容

第 1 章“走近 Metasploit 渗透测试框架”，将介绍 Metasploit 渗透测试的基础知识。我们将学习渗透测试的方法论以及如何建立一个渗透测试的模拟环境。此外还将系统地介绍渗透测试的各个阶段，并讨论使用 Metasploit 相较于采用传统手工测试的优势。

第 2 章“打造定制化的 Metasploit 渗透测试框架”，将介绍为构建 Metasploit 渗透模块所需具备的 Ruby 编程基础，分析现有 Metasploit 模块的结构，还将详细介绍如何编写自定义扫描器、认证测试工具、后渗透模块和登录凭证采集模块。最后阐明如何使用 RailGun 开发自定义模块。

第 3 章“渗透模块的开发过程”，将系统演示如何编写渗透模块，并研究其中的开发要点。之后将讲解如何进行 fuzz 测试，以及如何利用调试器观察应用程序的行为，进而收集开发模块所需的重要信息。最后演示如何利用收集到的信息编写一个 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”，将讲解如何将公开可用的渗透工具移植到 Metasploit 框架中，重点描

述如何找出那些使用 Perl、Python 和 PHP 语言编写的模块的核心功能，并通过 Metasploit 库和函数将它们转化成与 Metasploit 兼容的渗透模块。

第 5 章“使用 Metasploit 对服务进行测试”，将讨论如何对各种常见服务进行渗透测试，并介绍 Metasploit 中的一些重要模块，这些模块可用来对 SCADA、数据库和 VOIP 服务进行测试。

第 6 章“虚拟化测试的原因及阶段”，将简要介绍使用 Metasploit 进行渗透测试的整个过程，并重点介绍可与 Metasploit 协同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。最后讲解如何手动和自动生成报表。

第 7 章“客户端渗透”，重点讨论如何将传统的客户端渗透攻击变得更加复杂、精准。首先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“致命武器”。最后讲解如何使用 Kali NetHunter 渗透 Android 系统。

第 8 章“Metasploit 的扩展功能”，将研究 Metasploit 的基本后渗透功能和高级后渗透功能。首先讨论 Meterpreter 提供的基本后渗透功能，然后讨论高级的后渗透模块。这一章不仅有助于你快速了解如何加快渗透测试过程，同时还会介绍 Metasploit 中的许多功能，它们可以在你编写漏洞脚本时帮你节省大量时间。这一章最后将探讨如何实现后渗透过程的自动化。

第 9 章“Metasploit 中的规避技术”，将研究如何使用 Metasploit 的功能来实现攻击载荷对各种高级防御机制（例如杀毒软件）的规避，还会概述如何绕过各种 IDPS 工具（例如 Snort）的签名过滤功能，以及如何绕过 Windows 防火墙的端口阻塞机制。

第 10 章“Metasploit 中的‘特工’技术”，讨论执法机构如何使用 Metasploit。这一章的内容包括：会话代理，使用 APT 技术实现控制持久化，从目标系统中清除文件，利用代码打洞技术隐藏后门程序，使用 Venom 框架生成无法检测的攻击载荷，以及使用反取证模块避免在目标系统上留下痕迹。

第 11 章“利用 Armitage 实现 Metasploit 的可视化管理”，将讲解当前 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。之后介绍在渗透测试中红队如何使用 Armitage。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。最后讨论如何在 Armitage 中添加自定义功能，以及如何创建自定义界面和菜单。

第 12 章“技巧与窍门”，会讲解加速渗透测试和高效使用 Metasploit 的各种技巧。

本书要求

如果你想完成本书中的示例，将需要六七台计算机（也可以是虚拟机），其中一台作为渗透测试机，其他几台则作为渗透测试的靶机。

除此以外，你还需要 Kali Linux 的最新 VMware 映像文件，它在默认情况下已经包含了 Metasploit，并且包含创建本书示例所需的所有其他工具。不过，在某些情况下，你可以使用安装了 Metasploit 的

最新版 Ubuntu 桌面操作系统。

你还需要将 Ubuntu、Windows 7、Windows 10、Windows Server 2008、Windows Server 2012 和 Metasploitable 2 安装到虚拟机中，或者直接安装到计算机上，这些操作系统将作为 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。

下载示例代码文件

你可以使用自己的账户从 www.packtpub.com 下载本书的代码示例文件。如果你是通过其他途径购买的本书，那么可以访问 www.packtpub.com/support 进行注册，这些文件将会通过电子邮件发送给你。

你可以通过以下步骤来下载这些代码文件。

(1) 在 www.packtpub.com 进行登录或者注册。
(2) 选择“SUPPORT”标签。
(3) 点击“Code Downloads & Errata”。
(4) 在搜索框中输入书名，并遵循提示指令。

下载之后，请确保使用如下软件的最新版本来解压该文件：

- WinRAR / 7-Zip（Windows）
- Zipeg / iZip / UnRarX（Mac）
- 7-Zip / PeaZip（Linux)

也可以在 GitHub 上获取本书的代码文件：https://github.com/PacktPublishing/Mastering-Metasploit-Third-Edition。如果代码有所更新，我们将会在 GitHub 中更新。

https://github.com/PacktPublishing/上还有很多其他 Packt 图书的代码和视频。欢迎查看！

下载彩色图片

本书提供了一个 PDF 文件，其中包含了书中出现的屏幕截图和图表的彩色版本，下载链接是：https://www.packtpub.com/sites/default/files/downloads/MasteringMetasploitThirdEdition_ColorImages.pdf。

排版约定

本书采用以下排版约定。

正文中的代码、数据库表名和用户输入用等宽字体表示。例如：“可以看到，我们在会话 1 里面使用了 `post/windows/manage/inject_host` 模块。”

代码段的格式如下：

```
irb(main):001:0> 2
=> 2
```

命令行输入或者输出写成如下形式：

```
msf > openvas_config_list
[+] OpenVAS list of configs
```

新术语和重点强调的内容以黑体字显示。

此图标表示警告或重要说明。

此图标表示提示和技巧。

联系我们

欢迎你与我们取得联系。

一般反馈：请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。如果你对本书有任何疑问，可以将问题发送至 questions@packtpub.com。

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。如果你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。如果你发现了错误，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。[①]

反盗版：如果你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送到 copyright@packtpub.com。

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

评论

我们欢迎读者的反馈意见。如果你阅读并使用了本书，为什么不在购书网站上发表一条评论呢？如果你发表了评论，那么潜在的读者就可以看到并根据你公正的意见来做出购买决定，Packt 也可以了解你对我们产品的看法，作者也可以看到你对他们的书的反馈。谢谢！

有关 Packt 的更多信息，请访问 packtpub.com。

① 本书中文版勘误请到 http://www.ituring.com.cn/book/2657 查看和提交。——编者注

免责声明

本书内容仅限于以合乎道德的方式使用。如果你没有得到目标系统所有者的书面许可，请勿使用本书中的任何内容发起渗透攻击。如果你采取非法行动，很可能会被逮捕并起诉。如果你滥用本书中的任何信息，Packt 出版社将不承担任何责任。本书内容只能在测试环境时使用，并且须得到目标系统负责人的书面授权。

电子书

扫描如下二维码，即可购买本书的电子版。

致　谢

首先，我要感谢阅读过本书前两版的每一位读者，是你们造就了本书的成功。感谢我的母亲 Sushma Jaswal 和外婆 Malkiet Parmar，她们在我人生的每个阶段都曾给予我帮助。感谢审阅本书并提出修改建议的 Sagar Rahalkar。感谢上帝赐予我写作本书的无穷力量。

目　录