信息安全
技术大讲堂

从实践中学习 Metasploit 5 渗透测试

大学霸IT达人◎编著

从理论、应用和实践三个维度讲解新版Metasploit 5渗透测试的相关知识
通过153个操作实例手把手带领读者从实践中学习Metasploit 5渗透测试技术
涵盖环境搭建、漏洞信息获取、项目准备、实施攻击、漏洞利用等内容

机械工业出版社
China Machine Press

信息安全
技术大讲堂

从实践中学习 Metasploit 5 渗透测试

大学霸IT达人◎编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

从实践中学习Metasploit 5渗透测试 / 大学霸IT达人编著. —北京：机械工业出版社，2019.7

（信息安全技术大讲堂）

ISBN 978-7-111-63085-2

Ⅰ. 从… Ⅱ. 大… Ⅲ. 计算机网络－安全技术－应用软件 Ⅳ. TP393.08

中国版本图书馆CIP数据核字（2019）第129765号

从实践中学习 Metasploit 5 渗透测试

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）

责任编辑：欧振旭 李华君　　责任校对：姚志娟

印　　刷：中国电影出版社印刷厂　　版　　次：2019 年 7 月第 1 版第 1 次印刷

开　　本：186mm × 240mm 1/16　　印　　张：20.75

书　　号：ISBN 978-7-111-63085-2　　定　　价：89.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88379426 88361066　　投稿热线：（010）88379604

购书热线：（010）68326294　　读者信箱：hzit@hzbook.com

前言

Metasploit 是一款开源的安全漏洞利用工具。利用该工具，安全人员可以很容易地获取和利用计算机软件的漏洞，从而验证漏洞的危害性。该工具附带数百个已知软件漏洞的专业级攻击工具。借助该工具，安全人员可以将攻击载荷、编码器、生成器和漏洞捆绑起来直接使用，从而简化了漏洞利用的各种繁杂操作。

本书基于 Metasploit 5，详细讲解了 Metasploit 实施渗透攻击的方法。全书按照 Metasploit 的基本功能依次进行讲解，首先讲解了 Metasploit 的安装，然后介绍了它的接口及自带模块的使用，最后以实例形式介绍了使用 Metasploit 实施渗透攻击的具体方法。

本书有何特色

1. 使用最新的Metasploit 5版进行讲解

为了适应不断发展的技术环境，Metasploit 软件一直在不断更新。在 Metasploit 4 发布后，它已经经历了 17 次大的迭代和很多次小的迭代。Metasploit 5 版集合了每次更新所引入的新特性和新功能，更适合当前的渗透需求。

2. 着重介绍了Metasploit的专业化操作

Metasploit 作为一款专业渗透工具，提供了完备的功能。充分利用这些功能，可以大幅度提高相关技术人员的工作效率。本书从专业的角度，详细讲解了这些功能的使用方法。例如，通过 Metasploit 所提供的工作区功能，技术人员可以同时进行多个渗透测试任务，而互不干扰，而且渗透测试的各种数据都可以自动保存。

3. 充分讲解了漏洞利用的相关流程

随着人们对安全越来越重视，安全防范措施也越来越严密。在实际应用中，Metasploit 必须和上下游的各种工具配合使用，才能充分发挥其自身作用。本书详细讲解了 Metasploit 和知名安全软件的协调使用方法，如 Nessus、OpenVAS 和 SQLmap。

4. 由浅入深，容易上手

本书充分考虑了初学者的学习曲线，内容安排由易到难，讲解由浅入深，这使得读者比较容易上手。例如，本书讲解了 Metasploit 的各种基础知识，如获取合适的软件包、安装和配置 PostgreSQL 数据库、创建靶机、设置虚拟网络等，这些都是初学者必须要掌握的内容。

5. 环环相扣，逐步讲解

漏洞利用实施步骤较多，过程相对复杂。本书按照实施流程一步步展开，详细讲解了各流程的操作步骤和实施要点。同时，为了让读者更好地掌握相关知识点，书中的重点内容都配有实例、输出结果和对应的示例效果图。

6. 提供完善的技术支持和售后服务

本书提供了专门的 QQ 交流群（343867787），以方便大家交流和讨论学习中遇到的各种问题。另外，本书提供了专门的售后服务邮箱 hzbook2017@163.com。读者在阅读本书的过程中若有疑问，也可以通过该邮箱获得帮助。

本书内容

第 1 章环境配置，主要介绍了 Metasploit 的系统要求，以及在 Windows、Linux 和 Mac 系统中如何安装它；另外还介绍了 PostgreSQL 数据库服务配置、用户接口和靶机配置等内容。

第 2 章获取漏洞信息，主要介绍了如何使用 Nessus 和 OpenVAS 获取目标漏洞信息，以及如何在 Metasploit 中远程实施漏洞扫描。

第 3 章准备渗透项目，主要介绍了如何使用工作区管理渗透项目，如准备工作区、确定目标主机、管理渗透信息和信息维护等。另外，本章还介绍了 Metasploit 的模块体系，以及如何添加模块。

第 4 章实施攻击，主要介绍了如何使用 Metasploit 利用漏洞的流程，包括选择模块、设置模块、选择目标类型、选择攻击载荷、执行攻击和任务管理等。

第 5 章扩展功能，主要介绍了 Metasploit 提供的 3 个重要功能模块，分别为 Meterpreter 模块、攻击载荷生成器 Msfvenom 和免杀的 4 种方式。通过这 3 个模块，可以有效地提高渗透测试效率。

第 6 章漏洞利用，以实例方式介绍了在 Windows、Linux 和 Android 系统中如何利用 Metasploit 自带的模块实施攻击。

第 7 章辅助功能，主要介绍了 Metasploit 为渗透测试提供的多个辅助功能，如远程主机连接、批处理、会话管理和使用路由等。

附录 A 给出了 Metasploit 的常用命令。

附录 B 介绍了 Nessus 插件的使用方法。

附录 C 介绍了 openVAS 插件的使用方法。

本书配套资源获取方式

本书涉及的相关工具需要读者自行下载。下载途径如下：

- 根据书中对应章节给出的网址自行下载；
- 加入技术讨论 QQ 群（343867787）获取；
- 在华章公司网站 www.hzbook.com 上搜索到本书，然后单击“资料下载”按钮，在本书页面上找到“配书资源”下载链接即可下载。

本书内容更新文档获取方式

为了让本书内容紧跟技术的发展和软件更新步伐，我们会对书中的相关内容进行不定期更新，并发布对应的电子文档。需要的读者可以加入 QQ 交流群（343867787）获取，也可以通过华章公司网站上的本书配套资源链接下载。

本书读者对象

- 渗透测试技术人员；
- 网络安全和维护人员；
- 信息安全技术爱好者；
- 计算机安全技术自学者；
- 高校相关专业的学生；
- 专业培训机构的学员。

本书阅读建议

- Kali Linux 内置了 Metasploit，使用该系统的读者可以跳过 1.3～1.4 节。
- 学习阶段建议使用虚拟机靶机，避免因错误操作而造成目标主机无法正常工作的情况。
- Metasploit 工具经常会对工具模块进行增补，并修复原有的 Bug，读者学习的时候建议定期更新工具，以获取更稳定和更强大的环境。

本书作者

本书由大学霸 IT 达人技术团队编写。感谢在本书编写和出版过程中给予笔者大量帮助的各位编辑！

由于作者水平所限，加之写作时间较为仓促，书中可能还存在一些疏漏和不足之处，敬请各位读者批评指正。

编著者

目录

第1章 环境配置

如果要使用 Metasploit 实施渗透攻击，需要在系统中安装该工具，并且配置对应的攻击靶机。在 Kali Linux 中，默认已经安装了 Metasploit。但是在其他操作系统中，都没有安装该工具。所以，为了方便用户后面的操作，本章将介绍 Metasploit 工具的环境配置方法。

1.1 Metasploit 概述

Metasploit 是一个免费的、可下载的框架，通过它可以很容易地获取、开发并对计算机软件漏洞实施攻击。它本身附带数百个已知软件漏洞的专业级漏洞攻击工具。而且它还提供了许多个接口，其最受欢迎的是由 Rapid 7 和 Strategic Cyber LLC 公司维护的。由 Rapid 7 和 Strategic Cyber LLC 公司维护的接口包括 Metasploit Framework Edition、Metasploit Community Edition、Metasploit Express、Metasploit Pro、Armitage 和 Cobalt strike。其中，Metasploit Framework（命令行接口）和 Armitage（图形界面接口）是较常用的两种，并且是免费的。本书将选择使用 Metasploit Framework（命令行接口，即 MSFCONSOLE）接口来实施渗透攻击。

1.2 安装要求

为了能够顺利地安装 Metasploit 工具，需要先了解该工具对系统硬件、架构等的需求。由于 Metasploit 是一款漏洞扫描并实施攻击的工具，所以可能会被系统的杀毒软件或防火墙等拦截。本节将介绍 Metasploit 工具的安装要求。

1. 系统需求

- 2GHz 及以上的处理器；
- 4GB 可用内存（建议 8GB）；
- 1GB 以上的可用磁盘空间（建议 50GB）。

2. 支持的平台（64位架构）

- Red Hat Enterprise Linux Server 5.10 及以上；

- Red Hat Enterprise Linux Server 6.5 及以上；
- Red Hat Enterprise Linux Server 7.1 及以上；
- Ubuntu Linux 10.04 LTS；
- Ubuntu Linux 12.04 LTS；
- Ubuntu Linux 14.04 LTS（建议）；
- Ubuntu Linux 16.04 LTS；
- Kali Linux；
- Windows Server 2008 R2；
- Windows Server 2012 R2；
- Windows 7 SP1+；
- Windows 8.1；
- Windows 10。

3. 禁用杀毒软件

当系统中运行有杀毒软件时，将会检测到 Metasploit Framework 为恶意软件，并且可能导致它的安装和运行出现问题。Metasploit Framework 利用了与杀毒软件检测到的相同漏洞，因此，当安装 Metasploit Framework 时，杀毒软件将会阻止安装，并且提醒用户可能存在影响系统的安全风险。

如果想要安装 Metasploit Framework，在安装之前禁用所有杀毒软件。如果不能禁用杀毒软件的话，则需要设置杀毒软件不对 Metasploit 进行扫描。

4. 禁用防火墙

本地防火墙（包括 Windows 防火墙）会干扰渗透攻击和攻击载荷的操作。如果安装 Metasploit Framework 时开启防火墙的话，防火墙将探测到 Metasploit Framework 为恶意软件，中断其下载。

因此，在安装和运行 Metasploit Framework 之前，需要禁用本地防火墙。如果必须在安装有防火墙的计算机上操作，那么应该从外部网络下载 Metasploit Framework。

5. 获取管理员权限

为了能够成功地在系统上安装 Metasploit Framework，必须有该系统的管理员权限。

1.3 安装 Metasploit Framework

在用户准备好 Metasploit 的安装需求后，就可以开始安装 Metasploit Framework 了。该工具可以安装在 Windows、Linux 及 Mac OS X 系统中。本节将介绍在各种操作系统下安装 Metasploit Framework 的步骤。

1.3.1　获取安装包

Metasploit Framework 的下载地址为 https://www.rapid7.com/products/metasploit/download/editions/。在浏览器中输入该地址后，将显示如图 1.1 所示的页面。

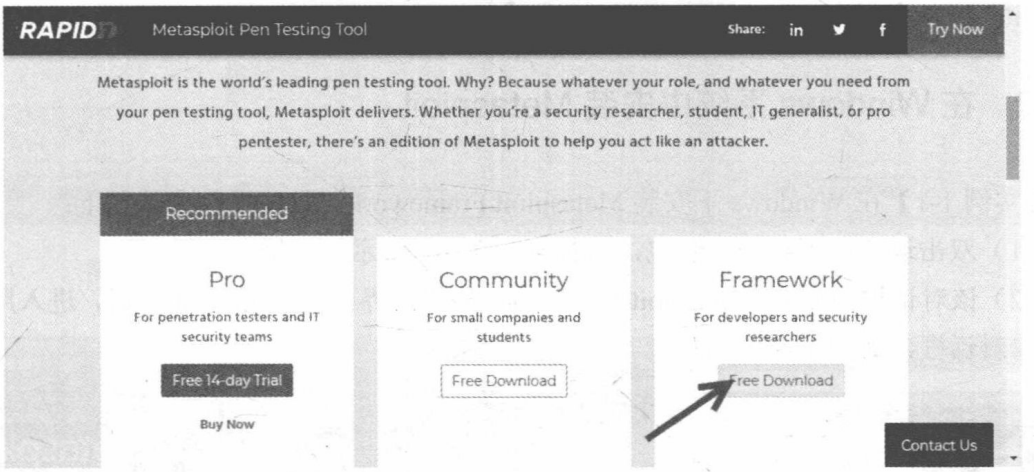

图 1.1　Metasploit Framework 下载页面

可以看到，该页面中提供了 3 个版本，分别是专业版（Pro，免费试用 14 天）、社区版（Community）和 Framework。本例中将选择下载 Framework。在该页面单击 Framework 下面的 Free Download 按钮，将跳转到 GitHub 网站，这里提供了各种操作系统平台的安装和下载方法，如图 1.2 所示。

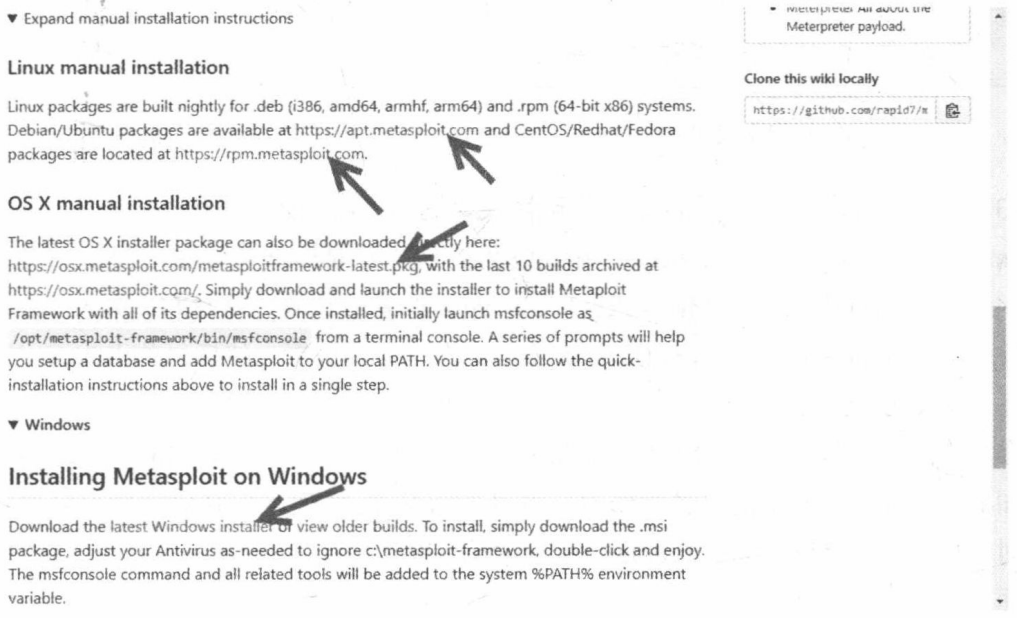

图 1.2　下载 Metasploit Framework 安装包

提示： 当打开 Metasploit Framework 包下载页面时，下载地址及安装包是折叠的，需要展开才可以看到其链接。

从图 1.2 中可以看到页面中分别提供了 Linux、Mac OS X 和 Windows 安装包。而且，所提供的 Linux 安装包包括.deb 和.rpm 格式。其中，.deb 包提供了 i386、amd64、armhf 和 arm64 这 4 个版本；.rpm 包只提供了 64-bit x86。

1.3.2 在 Windows 系统中安装 Metasploit

【实例 1-1】在 Windows 下安装 Metasploit Framework。具体操作步骤如下：

（1）双击运行已下载的安装包，将打开如图 1.3 所示对话框。

（2）该对话框为安装 Metasploit-framework 的欢迎界面，单击 Next 按钮，进入用户许可协议对话框，如图 1.4 所示。

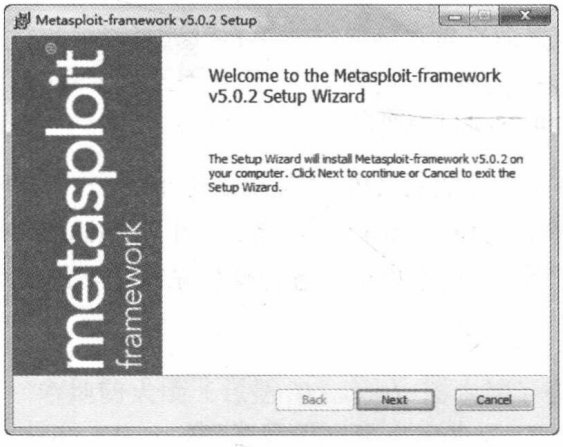

图 1.3 欢迎安装向导

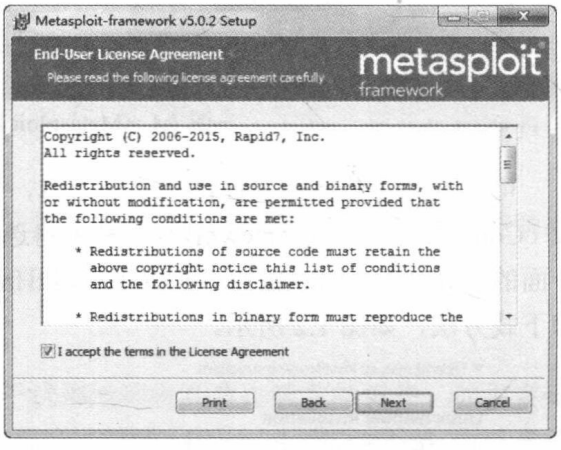

图 1.4 许可协议

（3）该对话框提示用户是否接受许可协议。这里勾选 I accept the terms in the License Agreement 复选框，然后单击 Next 按钮，进入安装位置对话框，如图 1.5 所示。

（4）该对话框用来设置 Metasploit Framework 的安装位置，默认将安装在 C 盘。如果希望安装到其他位置，可以单击 Browse 按钮，修改安装位置。然后，单击 Next 按钮，进入准备安装对话框，如图 1.6 所示。

（5）该对话框提示将开始安装，如果确定之前的配置无误，单击 Install 按钮将开始安装，如图 1.7 所示。如果需要进行修改，可以单击 Back 按钮。安装完成后，显示如图 1.8 所示对话框。表示 Metasploit Framework 已经安装成功了。单击 Finish 按钮，退出安装向导界面。

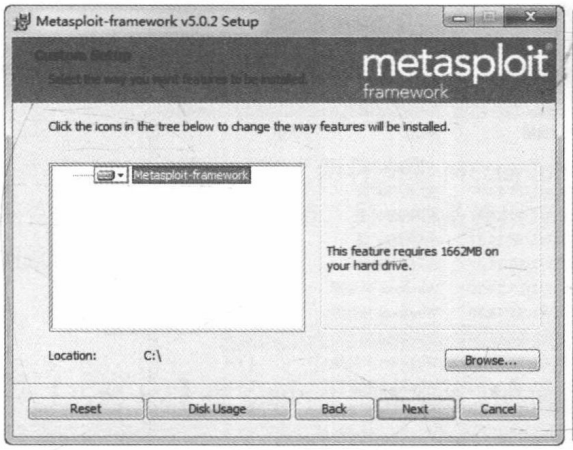

图 1.5　选择安装位置

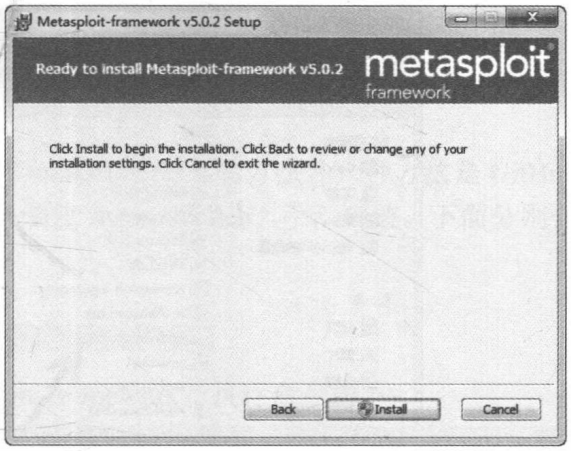

图 1.6　准备安装

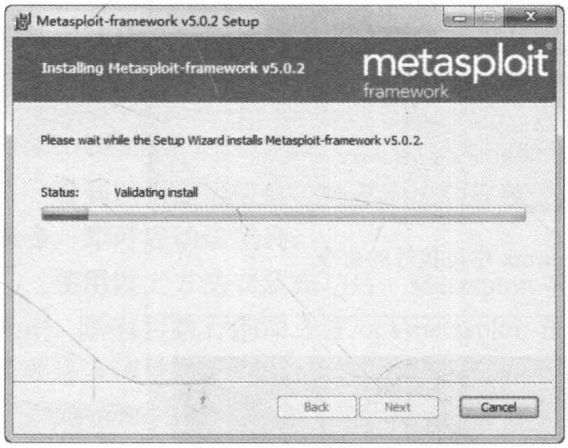

图 1.7　正在安装

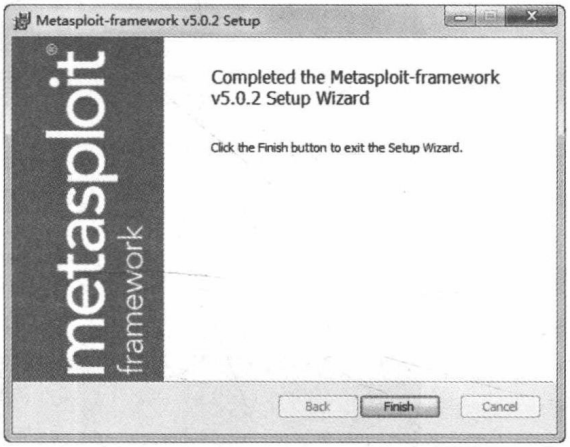

图 1.8　安装完成

现在，就可以启动 Metasploit Framework 了。启动方法如下：

（1）进入 Metasploit Framework 安装位置。本例中的安装位置是 C 盘，此时在 C 盘下面可以看到一个名为 metasploit-framework 的文件夹。

（2）依次打开 metasploit-framework|bin 目录，如图 1.9 所示。

（3）双击 msfconsole.bat 可执行文件，即可启动 Metasploit Framework。成功启动后，如图 1.10 所示。

（4）看到窗口中显示的 msf5 >提示符，则表示已成功启动了 Metasploit。接下来就可以使用该框架提供的模块及攻击载荷实施渗透了。

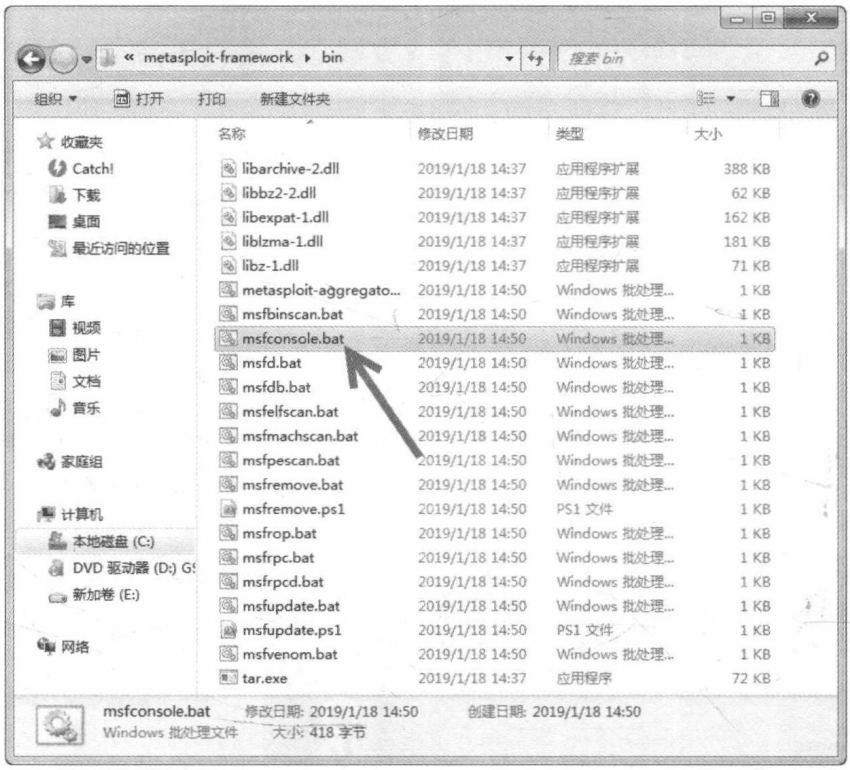

图 1.9　Metasploit Framework 中可执行的命令

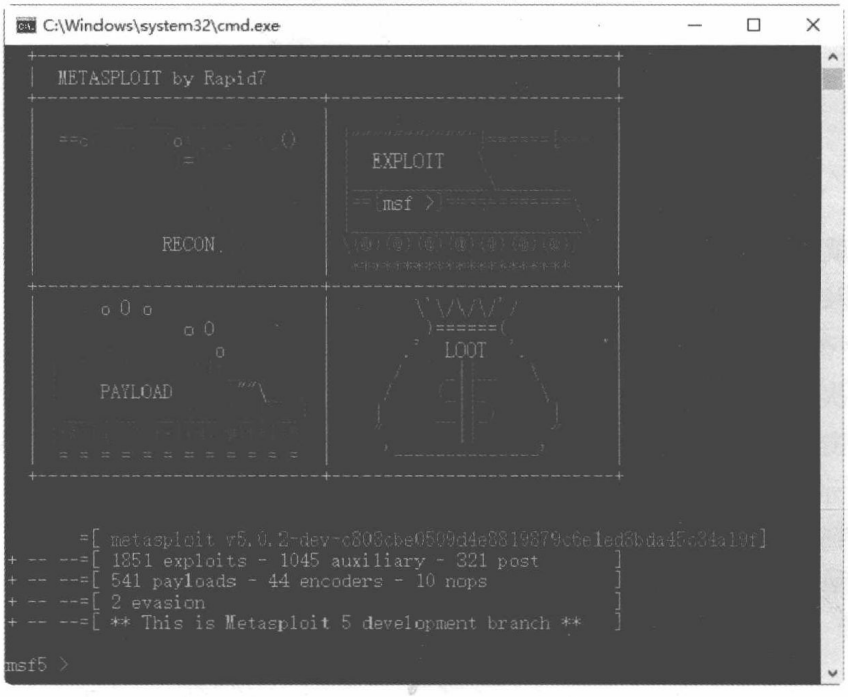

图 1.10　成功启动 Metasploit