【译】Metasploit：Wiki 主页 & 目录

- 原文：https://github.com/rapid7/metasploit-framework/wiki
- 译者: 王一航 & Google 2018-05-14
- 校对: 王一航 2018-05-14
- 说明：
  - 本篇文章为目录，文章中链接在未翻译状态时会指向原始链接，文章在翻译完成之后则会在文章标题前添加【已翻译】字样，并且文章指向的链接会修改为简书的链接
  - 不保证按照顺序进行翻译。

你是否渴望得到配置你的 Metasploit 开发环境，开始发起 GitHub Pull Request 并且提供精彩的漏洞利用代码？如果是这样，那么你来对地方了！

你是一个 Metasploit 的使用者吗？并且想像电影中演绎的破解东西 (首先保证你经过授权) 吗？
最快开始的方法是下载 Metasploit 二进制安装包。这将会给你访问所有 Metasploit 版本的权限：

- 自由，开放源代码的 Metasploit Framewrok 免费社区版本
- Metasploit Pro 的试用版本。

如果你正在使用 Kali Linux，那么 Metasploit 已经在你的系统中预先安装，请查看 Kali 文档 来获取如何在 Kali Linux 中使用 Metasploit 的详情信息。

如果你是一个 Exploit 开发者，你或许想要查看我们的 可接受模块以及增强指南（译者注：Guidelines for Accepting Modules and Enhancements），在这个文档中你会找到：当我们看到关于新的 Metasploit 模块的 Pull Request 的时候所有我们期望看到的东西。(译者注：Pull Request的规格和标准，融入一个社区当然要遵守社区既定的规则)
如果你对于你想要做什么没有什么想法的话，你也可以参考这个指南：为 Metasploit 做出贡献，然后就可以着手 配置 Metasploit 开发环境

开始

- Setting Up a Metasploit Development Environment
- Using Metasploit
- 【已翻译】使用 Git
- Reporting a Bug

贡献代码

- Contributing to Metasploit
- Creating Metasploit Framework LoginScanners
- Guidelines for Accepting Modules and Enhancements
- Common Metasploit Module Coding Mistakes
- 【已翻译】代码风格小建议
- Committer Rights
- Landing Pull Requests

Metasploit 开发

- 【已翻译】为什么选择 Ruby ？
- 【已翻译】代码风格小建议
- How to get started with writing an exploit
- How to get started with writing an auxiliary module
- How to get started with writing a post module
- How to get started with writing a Meterpreter script
- Loading External Modules
- 【已翻译】漏洞利用程序评级
- Metasploit module reference identifiers
- How to check Microsoft patch levels for your exploit
- How to clean up files using FileDropper
- How to deprecate a Metasploit module
- How to do reporting or store data in module development
- How to log in Metasploit

- [How to obfuscate JavaScript in Metasploit](#)
- [How to parse an HTTP response](#)
- [How to Send an HTTP Request Using HTTPClient](#)
- [How to send an HTTP request using Rex::Proto::Http::Client](#)
- [How to use command stagers](#)
- [How to use datastore options](#)
- [How to use Msf::Auxiliary::AuthBrute to write a bruteforcer](#)
- [How to use PhpEXE to exploit an arbitrary file upload bug](#)
- [How to use Powershell in an exploit](#)
- [How to use Railgun for Windows post exploitation](#)
- [How to Use the FILEFORMAT mixin to create a file format exploit](#)
- [How to use the Msf::Exploit::Remote::Tcp mixin](#)
- [How to use the Seh mixin to exploit an exception handler](#)
- [How to use WbemExec for a write privilege attack on Windows](#)
- [How to write a browser exploit using BrowserExploitServer](#)
- [How to write a browser exploit using HttpServer](#)
- [How to write a check() method](#)
- [How to write a HTTP LoginScanner Module](#)
- [How to write a module using HttpServer and HttpClient](#)
- [How to zip files with Rex::Zip::Archive](#)
- [Oracle Usage](#)
- [Rex Layout](#)

Metasploit Payloads（译者注：有时候被翻译为"攻击载荷"）

- [【已翻译】How Payloads Work](#)
- [Merging Metasploit Payload Gem Updates](#)
- [Meterpreter Configuration](#)
- [Meterpreter HTTP Communication](#)
- [Meterpreter Paranoid Mode](#)
- [Meterpreter Reliable Network Communication](#)
- [Meterpreter Sleep Control](#)
- [Meterpreter Stageless Mode](#)
- [Meterpreter Timeout Control](#)
- [Meterpreter Transport Control](#)
- [Meterpreter Unicode Support](#)
- [Payload UUID](#)
- [Python Extension](#)
- [The ins and outs of HTTP and HTTPS communications in Meterpreter and Metasploit Stagers](#)

其他 Metasploit 相关的资源

- [Downloads by Version](#)
- [Evading Anti Virus](#)
- [【已翻译】Metasploit module 的正确打开方式](#)
- [【已翻译】如何在 Metasploit 中使用反弹 Shell](#)
- [Information About Unmet Browser Exploit Requirements](#)
- [【已翻译】如何使用 msfvenom](#)
- [How to use exim_gethostbyname_bof.rb (Exim GHOST Buffer Overflow)](#)
- [What does my Rex::Proto::SMB Error mean?](#)

GitHub 相关的资源

- [Git Cheatsheet](#)
- [Git Gotchas](#)
- [Git Reference Sites](#)
- [Remote Branch Pruning](#)

点击收藏 | 0 关注 | 1

1. 3 条回复

papas****@aliyun 2018-09-17 14:39:43

沙发

0 回复Ta

左右 2019-03-25 12:24:43

谢谢师傅的分享

0 回复Ta

[左右](#) 2019-03-25 12:30:34

#https://xzfile.aliyuncs.com/media/upload/picture/20190325122948-a010ca12-4eb6-1.jpg)

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)