格式: msfconsole [参数]

常用选项

-E, --environment 环境 The Rails environment. Will use RAIL\_ENV environment variable if that is set. Defaults to production if neither option not RAILS\_ENV environment variable is set.

数据库选项

-M, --migration-path DIRECTORY 指定一个包含额外数据库迁移的目录

-n, --no-database 禁用数据库支持

-y, --yaml PATH 指定一个包含数据库设置YAML文件

框架选项

-c FILE 加载指定的配置文件

-v, --version 显示当前版本

模块选项

--defer-module-loads Defer module loading unless explicitly asked.

-m, --module-path DIRECTORY 一个额外的模块路径

控制台选项:

-a, --ask Ask before exiting Metasploit or accept 'exit -y'

-L, --real-readline 系统是用的 Readline 库而不是 RbReadline

-o, --output FILE 输出到指定的文件

-p, --plugin PLUGIN 在启动时加载一个插件

-q, --quiet Do not print the banner on startup

-r, --resource FILE 执行指定的资源文件（为stdin）

-x, --execute-command COMMAND 执行指定的字符串作为控制台命令 (use ; for multiples)

-h, --help 显示帮助文件

核心命令

=============

命令 描述

------- -----------

? 帮助菜单

advanced 显示一个或多个模块的高级选项

back 从当前当前模块返回

banner 显示一个msfconsole LOGO

cd 更改当前工作目录

color 切换颜色

connect 与一个主机通信

edit 编辑当前模块和显示输出

exit 退出控制台

get 获取上个模块的特定变量的值

getg 获取全局变量的值

grep 在另一个命令的输出

help 帮助菜单

info 显示关于一个或多个模块的信息

irb 加载一个IRB脚本模式

jobs Displays and manages jobs

kill 杀死一个进程

load 加载一个框架插件

loadpath 从路径搜索或者加载模块

makerc 从开始到文件时保存输入的命令（保存所有输入的命令）

options 显示全局选项或为一个或多个模块显示

popm 从堆栈中弹出最新的模块，并使其活动

previous 将先前加载的模块设置为当前模块

pushm 将模块的活动或列表推到模块堆栈上

quit 退出控制台

reload\_all 重新加载所有模块的所有模块定义的路径

rename\_job 重命名工作

resource 运行存储在文件中的命令

route 查看会话的路由流量

save 保存活动数据存储

search 搜索模块的名称和描述

sess 与一个给定的会话交互

sessions 转储会话列表和显示会话的信息

set 将特定上下文变量设置为值

setg 将一个全局变量设置为一个值

show 显示一个给定类型的模块或所有模块

sleep Do nothing for the specified number of seconds

spool 将控制台输出写入到一个文件中，以及屏幕

threads 查看和处理后台线程

unload 卸载一个框架插件

unset 设定一个或多个上下文特定的变量

unsetg 设定一个或多个全局变量

use 按名称选择模块

version 显示框架和控制台库版本号

后台数据库命令

=========================

命令 释义

------- -----------

creds 列出数据库中的所有凭据

db\_connect 连接到现有的数据库

db\_disconnect 从当前数据库实例断开连接

db\_export 导出包含数据库内容的文件

db\_import 进口扫描结果文件（文件类型将被自动检测到）

db\_nmap 执行nmap和记录的自动输出

db\_rebuild\_cache 重建数据库存储模块的缓存

db\_status 显示当前数据库状态

hosts 列出数据库中的所有主机

loot 列出数据库中的所有战利品

notes 列出数据库中的所有注释

services 列出数据库中的所有服务

vulns 列出数据库中的所有漏洞

workspace 数据库的工作区之间切换