|  |  |
| --- | --- |
| 命令 | 描述 |
| browserpivot | 设置浏览器的主会话 |
| bypassuac | 绕过目标验证，返回一个高权限账号 |
| cancel | 取消一个正在下载的任务 |
| cd | 切换目录 |
| checkin | 强制dns beacon连接，在登记期间，beacon会发布元数据和存储键盘记录。 |
| clear | 清除beacon序列 |
| covertvpn | 部署隐蔽的vpn客户端 |
| cp | 复制文件 |
| dcsync | 从dc中提取密码hash |
| desktop | 查看目标的桌面并与之交互 |
| dllinject | 注入反射的dll进程 |
| dllload | 使用loadlibrary将dll加载到进程中 |
| download | 下载文件 |
| downloads | 列出正在下载的文件 |
| drives | 列出目标驱动 |
| elevate | 尝试进行提权 |
| execute | 执行目标上的程序（没有输出） |
| execute-assembly | 在内存中执行一个本地的net程序 |
| exit | 终止beacon会话 |
| getprivs | 启用当前令牌的系统权限 |
| getsystem | 尝试获取system |
| getuid | 获取用户id |
| hashdump | 存储密码hash值 |
| help | 帮助菜单 |
| inject | 在指定的进程中派生出新的会话 |
| jobkill | 杀死长时间运行的后期开发任务 |
| jobs | 列出长期运行的后期开发任务 |
| kerberos\_ccache\_use | 将缓存中的kerberos票证应用于此会话 |
| kerberos\_ticket\_purge | 从本次会话中清除kerberos票据 |
| kerberos\_ticket\_use | 将kerberos票证应用于此会话 |
| keylogger | 将键盘记录器注入到进程中 |
| kill | 杀死一个进程 |
| link | 通过smb连接到beacon对等端 |
| logonpasswords | 使用mimikatz转储凭据和hash值 |
| ls | 列出文件 |
| make\_token | 创建一个令牌 |
| mimikatz | 运行mimikatz命令 |
| mkdir | 新建一个目录 |
| mode dns | 使用dns a作为数据通道（仅限dns beacon） |
| mode dns-txt | 使用dns txt作为数据通道（仅限dns beacon） |
| mode dns6 | 使用dns aaaa作为数据通道（仅限dns beacon） |
| mode http | 使用http作为数据通道 |
| mode smb | 使用smb进行通信 |
| mv | 移动文件 |
| net | 网络和主机枚举工具 |
| note | 为beacon分配注释 |
| portscan | 扫描网络获取开放的服务 |
| powerpick | 通过unmanaged powershell执行命令 |
| powershell | 通过powershell执行命令 |
| powershell-import | 导入powershell脚本 |
| ppid | 为生成的post-ex设置父pid |
| ps | 显示进程列表 |
| psexec | 使用服务在主机上生成会话 |
| psexec\_psh | 使用powershell在主机上生成会话 |
| psinject | 在特定的进程中执行powershell命令 |
| pth | 使用mimikatz传递hash |
| pwd | 打印当前的位置 |
| reg | 查询注册表 |
| rev2self | 恢复原始令牌 |
| rm | 删除文件或文件夹 |
| rportfwd | 设置一个方向转发端口 |
| run | 执行程序（返回输出） |
| runas | 以另一个用户身份执行程序 |
| runasadmin | 使用令牌复制方法绕过用户账户控制 |
| runu | 在另一个pid下执行程序 |
| screenshot | 截取屏幕 |
| setenv | 设置环境变量 |
| shell | 通过cmd来执行命令 |
| shinject | 将shellcode注入进程 |
| shspawn | 生成进程并将shellcode注入其中 |
| sleep | 设置beacon的休眠时长 |
| socks | 启动socks4a服务器以中继流量 |
| socks stop | 停止socks4a服务器 |
| spawn | 产生一个新的会话 |
| spawnto | 设置可执行文件以生成进程 |
| spawnu | 在另一个pid下产生一个会话 |
| ssh | 使用ssh在主机上生成ssh会话 |
| ssh-key | 使用ssh在主机上生成ssh会话 |
| steal\_token | 从进程中窃取访问令牌 |
| timestomp | 应用一个时间戳 |
| unlink | 断开与父beacon的连接 |
| upload | 上传文件 |
| wdigest | 使用mimikatz转储明文凭证 |
| winrm | 使用winrm在主机上生成会话 |
| wmi | 使用wmi在主机上生成会话q |