Cobalt Strike 后渗透工具

介绍

Cobalt Strike 一款以Metasploit为基础的GUI框架式渗透测试工具，集成了端口转发、服务扫描，自动化溢出，多模式端口监听，exe、powershell木马生成等。

钓鱼攻击包括：站点克隆，目标信息获取，java执行，浏览器自动攻击等。

Cobalt Strike 主要用于团队作战，可谓是团队渗透神器，能让多个攻击者同时连接到团体服务器上，共享攻击资源与目标信息和sessions。

基本功能

安装运行

Cobalt Strike 分为客户端和服务端，可分布式操作、协同作战。服务器端只能运行在Linux系统中，可搭建在VPS上。

服务端

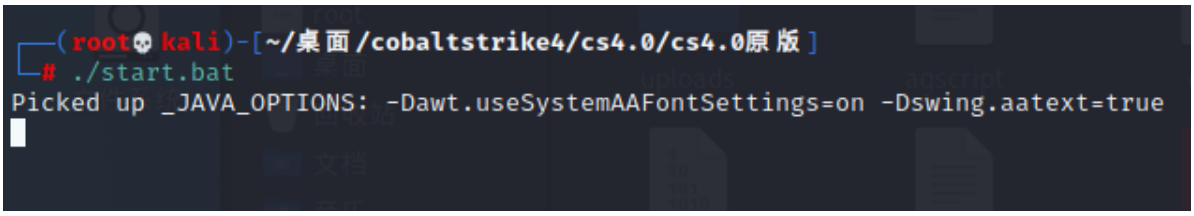
服务端关键的文件是teamserver以及cobaltstrike.jar，将这两个文件放到服务器上同一个目录，然后运行：

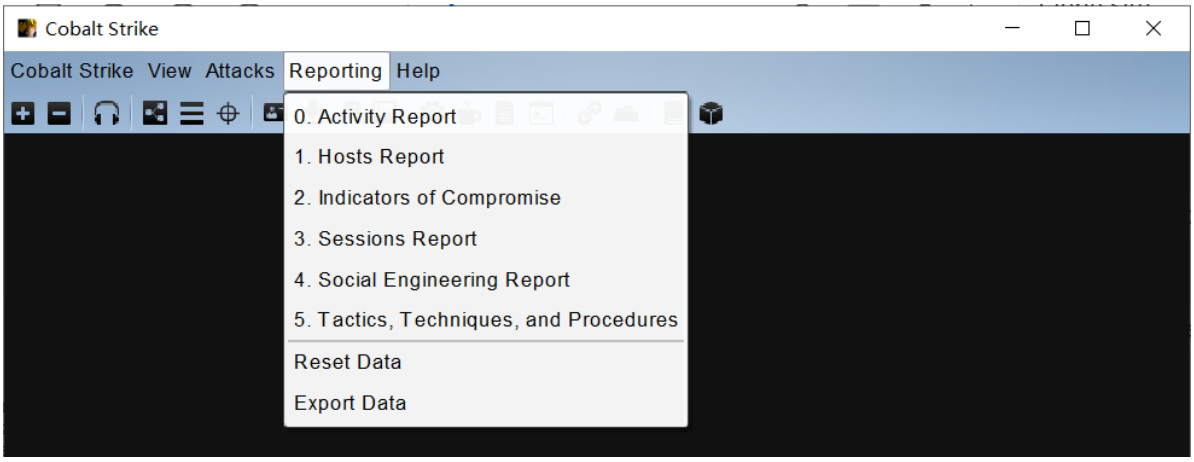
```
chmod +x teamserver
#赋予执行权限
./teamserver 192.168.2.112 123456
#服务器真实IP（不能使用0.0.0.0或127.0.0.1）和连接密码
```

客户端

客户端在Windows、Linux、Mac下都可以运行 (需要配置好Java环境)。启动Cobalt Strike客户端，输入服务端的IP以及端口、连接密码，用户名可以任意设置。

```
./start.bat
#启动cs
```

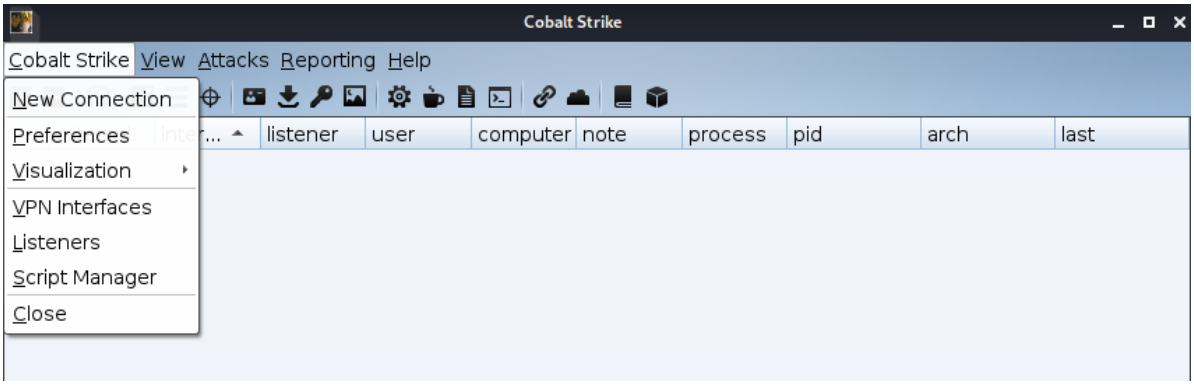




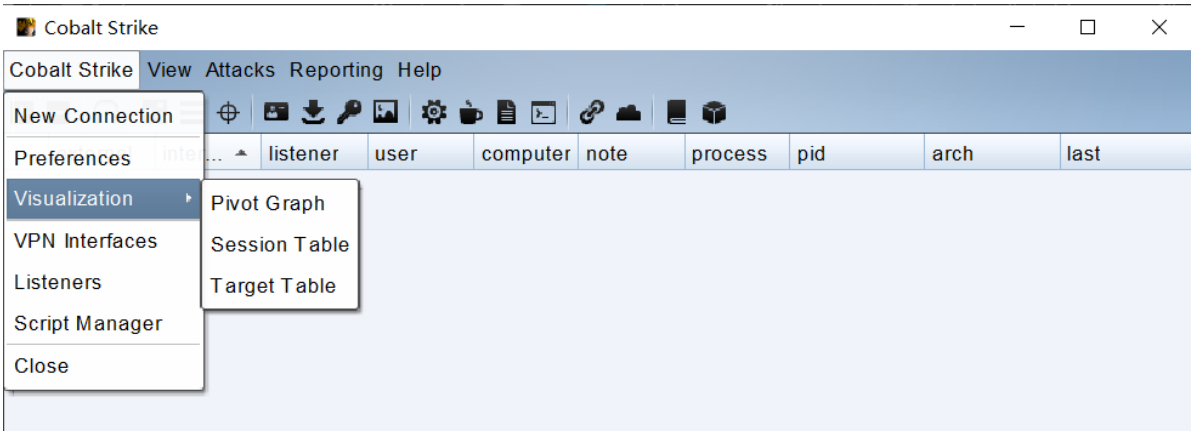
在控制台所有操作指令都会被记录保留在Cobalt Strike目录logs下。

参数介绍

Cobalt Strike

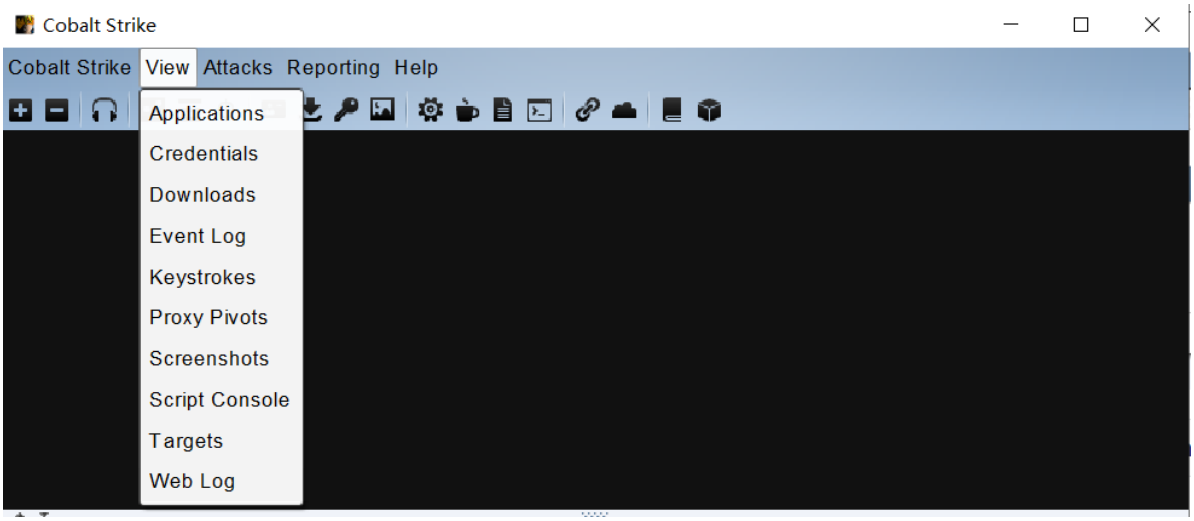


Cobalt Strike	
New Connection	#新的连接(支持连接多个服务器端)
Preferences	#偏好设置(设置Cobal Strike界面、控制台、以及输出报告样式、TeamServer连接记录等)
Visualization	#窗口视图模式(展示输出结果的形式)
VPN Interfaces	#VPN接入
Listenrs	#监听器(创建Listener)
Script Manager	#脚本管理
Close	#关闭



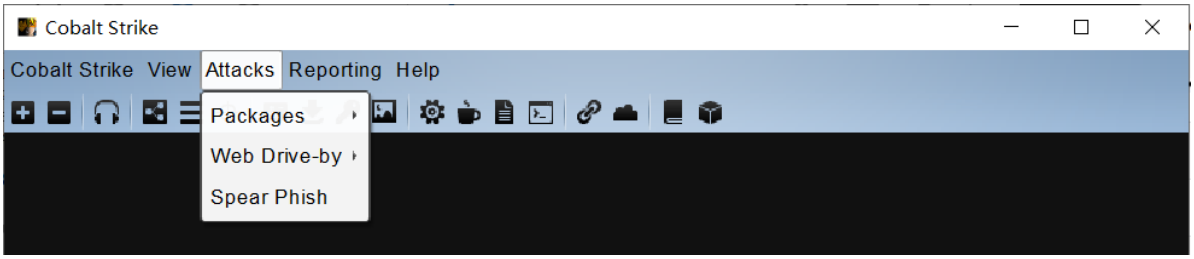
Visualization	
Privot Graph	#枢纽视图（可以显示各个目标的关系）
Session Table	#会话列表
Target Table	#目标列表

View

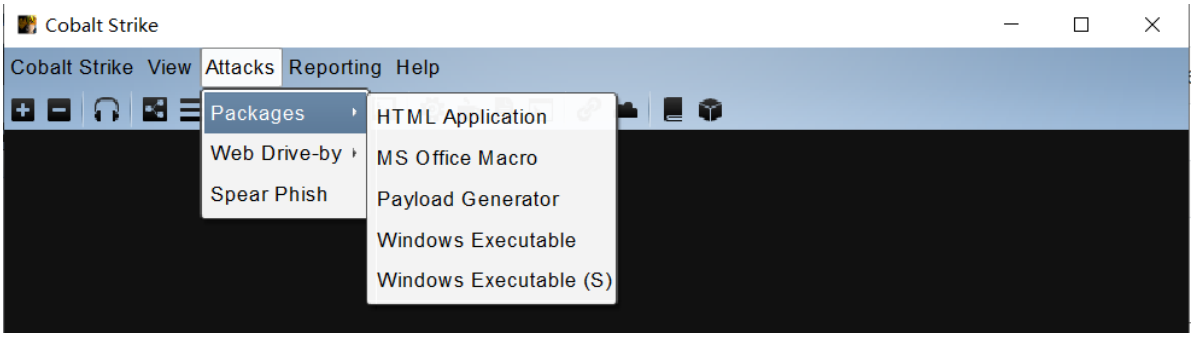


View	视图
Applications	#应用信息(显示受害者机器的应用信息)
Credentials	#凭证信息(通过hashdump或Mimikatz抓取过的密码都会储存在这里)
Downloads	#下载文件
Event Log	#事件日志(主机上线记录以及团队协作聊天记录)
Keystrokes	#键盘记录
Proxy Pivots	#代理模块
Screenshots	#截图
Script Console	#脚本控制台(可以加载各种脚本，增强功能)
Targets	#显示目标主机
Web Log	#Web日志

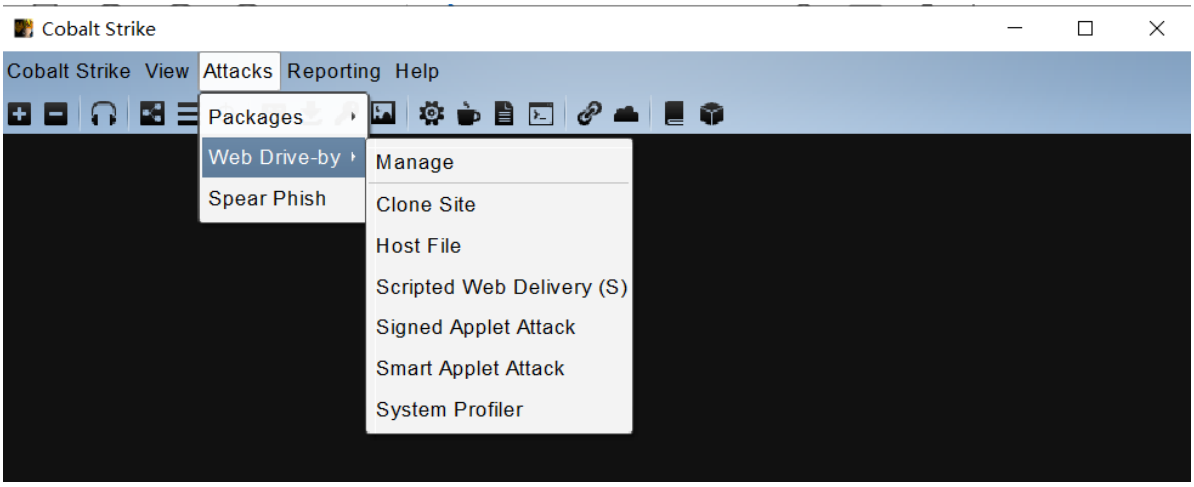
Attacks



Attacks	攻击
Packages	#生成后门
Web Drive-by	#钓鱼攻击
Spear Phish	#邮件攻击

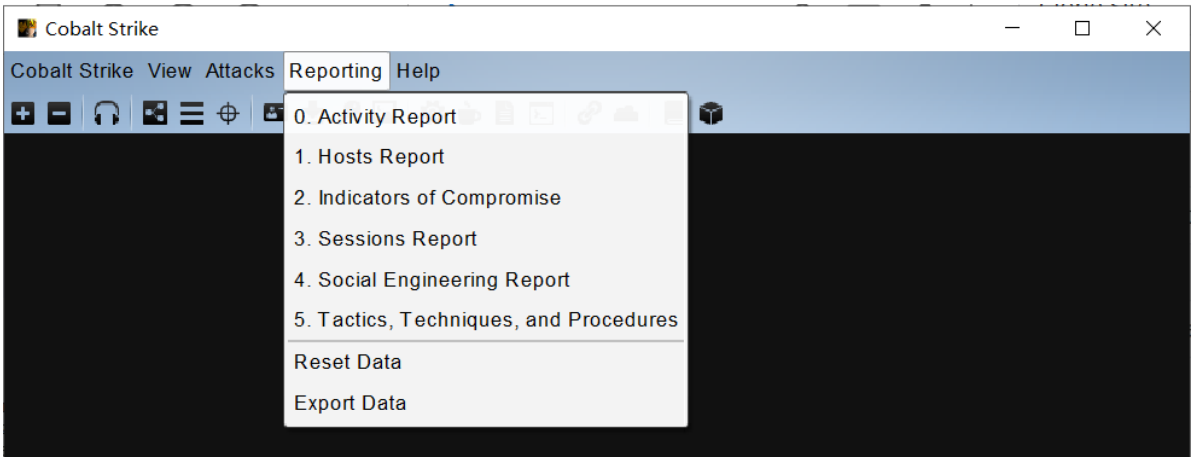


Packages	生成后门
HTML Application	#生成恶意的HTA木马文件
MS Office Macro	#生成office宏病毒文件
Payload Generator	#生成各种语言版本的payload
Windows Executable	#生成可执行Payload
Windows Executable(S)	#把包含payload,Stageless生成可执行文件(包含多数功能)



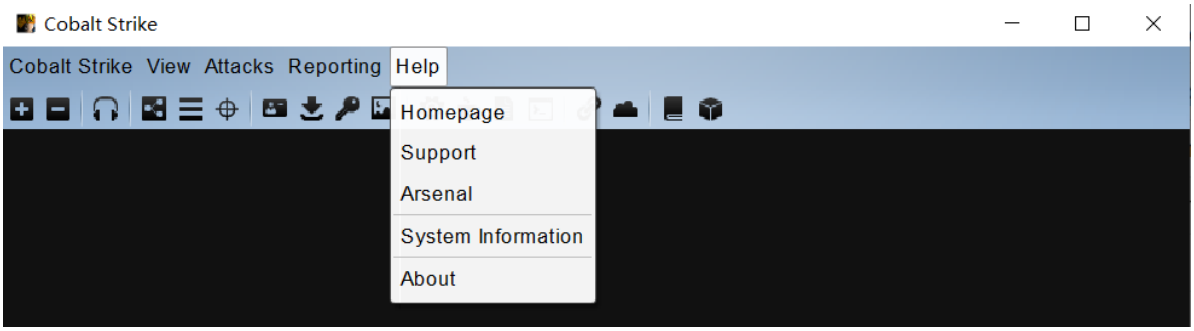
Web Drive-by	钓鱼攻击
Manage	#对开启的web服务进行管理
Clone Site	#克隆网站(可记录受害者提交的数据)
Host File	#提供Web以供下载某文件
Scripted Web Delivery（S）	#提供Web服务，便于下载和执行PowerShell Payload，类似于Metasploit的web_delive
Signed Applet Attack	#启动一个Web服务以提供自签名Java Applet的运行环境
Smart Applet Attack	#自动检测Java版本并利用已知的exploits绕过security
System Profiler	#用来获取一些系统信息，比如系统版本，Flash版本，浏览器版本等

Reporting



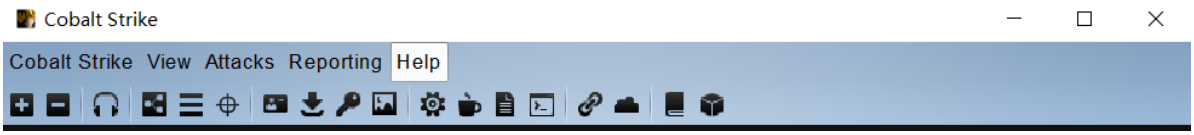
Reporting	**报告**
0. Activity report	#活动报告
1. Hosts report	#主机报告
2. Indicators of Compromise	#威胁报告
3. Sessions report	#会话报告
4. Social engineering report	#社会工程学报告
5. Tactics, Techniques, and Procedures	#策略、技巧和程序
Reset Data	#重置数据
Export Data	#导出数据

Help



Help	**帮助**
Homepage	#官方主页
Support	#技术支持
Arsenal	#开发者
System information	#版本信息
About	#关于

菜单栏视图



1.新建连接
2.断开当前连接
3.监听器
4.改变视图为Pivot Graph(可以显示各个目标的关系)
5.改变视图为Session Table(会话列表)
6.改变视图为Target Table(目标列表)
7.查看凭据信息a8.查看文件下载
9.查看键盘记录
10.查看屏幕截图
11.生成无状态Beacon后门
12.java自签名程序攻击
13.生成office宏后门
14.生成脚本通过web传递(利用powershell，bitsadmin，regsvr32生成会话)
15.在Cobalt Strike的web服务上托管一个文件(提供一个文件下载)
16.管理Cobalt Strike上运行的web服务
17.帮助
18.关于