Cobalt Strike | 从入门到入狱

Sec盾 6天前

编者荐语：

朋友文章~~~值得一看

以下文章来源于物联网IOT安全 ，作者lmnmn

物联网IOT安全

我们是一个专注于物联网IOT安全 固件逆向 近源攻击 硬件破解的公众号，与我们一起学习...

Hello大家好哇，我是你们的lmn小姐姐，从今天开始，我们要**发N期Cobalt Strike的教程**，主要是介绍**从入门到入狱**的过程，欢迎师傅们转发留言走起。

今天我们仅介绍一下Cobalt Strike的由来以及一些基本的操作，也希望通过这篇文章让大家**更快速的了解**Cobalt Strike。

0x00 什么是Cobalt Strike

Cobalt Strike是一款用于**模拟红队攻击**的软件，其目标是致力于「**缩小渗透测试工具和高级威胁恶意软件之间的差距**」。Cobalt Strike(CS)的创始人是Raphael Mudge，他之

前在2010年的时候就发布了一款MSF图形化工具Armitage。直到**2012年**，Raphael推出了Armitage的增强版**Cobalt Strike**。

“Raphael是我最最最崇拜的大黑阔之一”

0x01 环境准备

1. Cobalt Strike 开心版**（公众号后台回复CS获取）**
2. Vmware
3. Kali OR Parrot
4. Win7 OR Win10

0x02 前置定义

0. **C2**：C2 就是 Command & Control Server 的简称，也就是命令与控制服务器。

1. **Listener**：攻击者在C2上运行的服务，可以监听Beacon的请求(check in)。

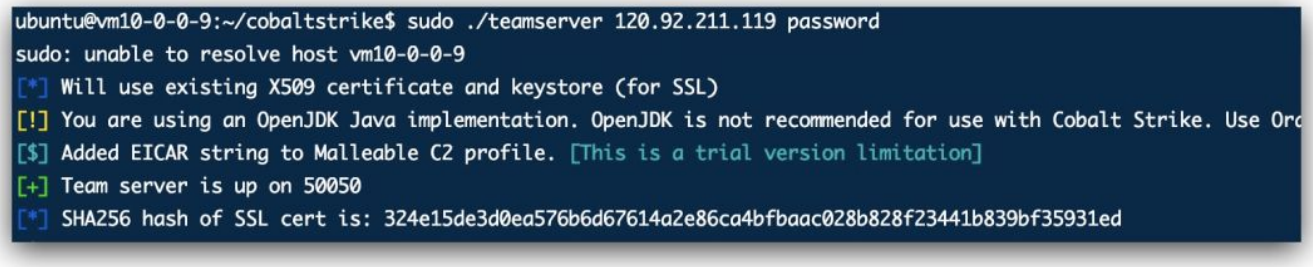
2. **Beacon**：植入到受感染系统中的恶意程序，可以请求C2服务器并在受感染系统中执行命令。

3. Team Server：Cobalt Strike的服务器组件。Team Server(TS)是配置和启动Listener的地方。

0x03 Getting Started

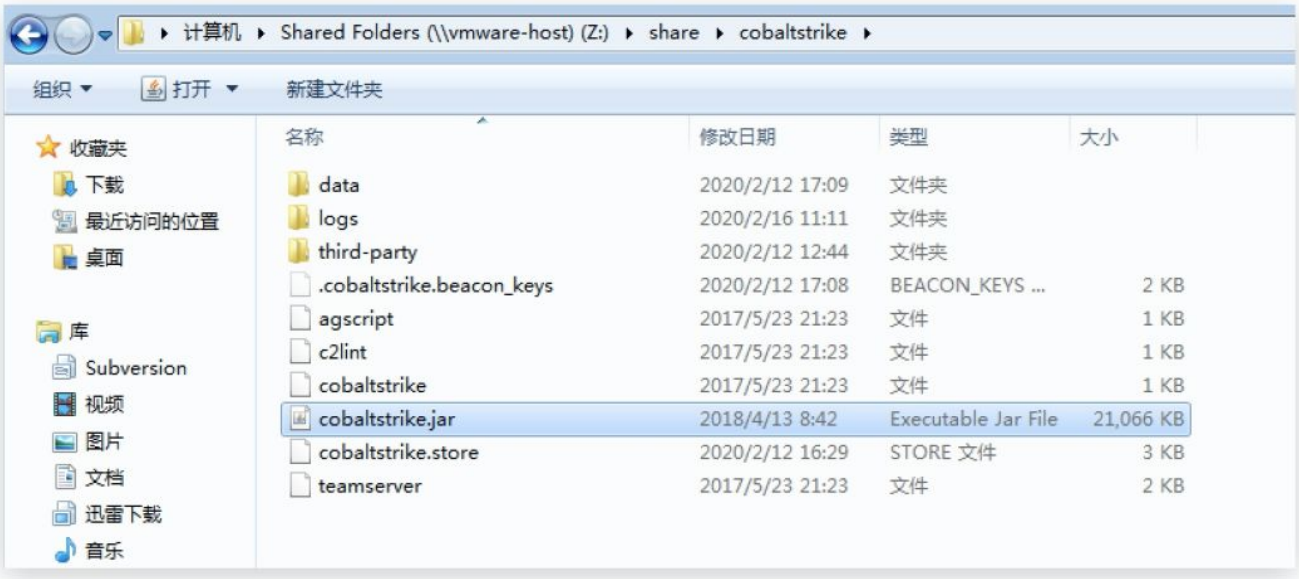
Team Server 启动

```
attacker@ubuntu
#启动方法：./teamserver <serverIP> <password> <~killdate> <~profile>
#~为可选参数
ubuntu@vm10-0-0-9:~/cobaltstrike$ sudo ./teamserver 120.92.211.119
```



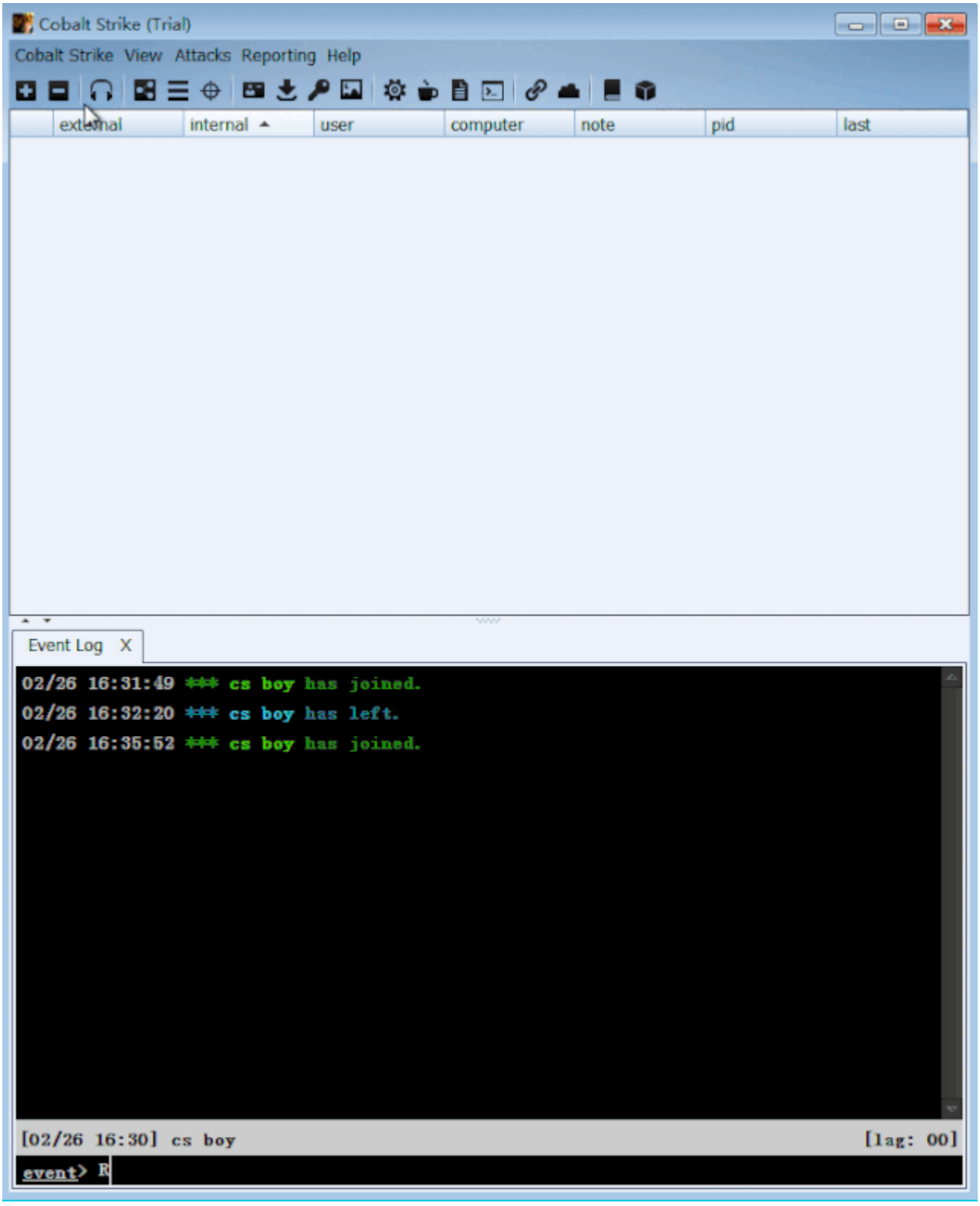
> 在实际红队行动中，我们一般会将真实C2服务器放置在转发服务器之后，后续文章将会详细阐述redirectors服务器。

客户端启动



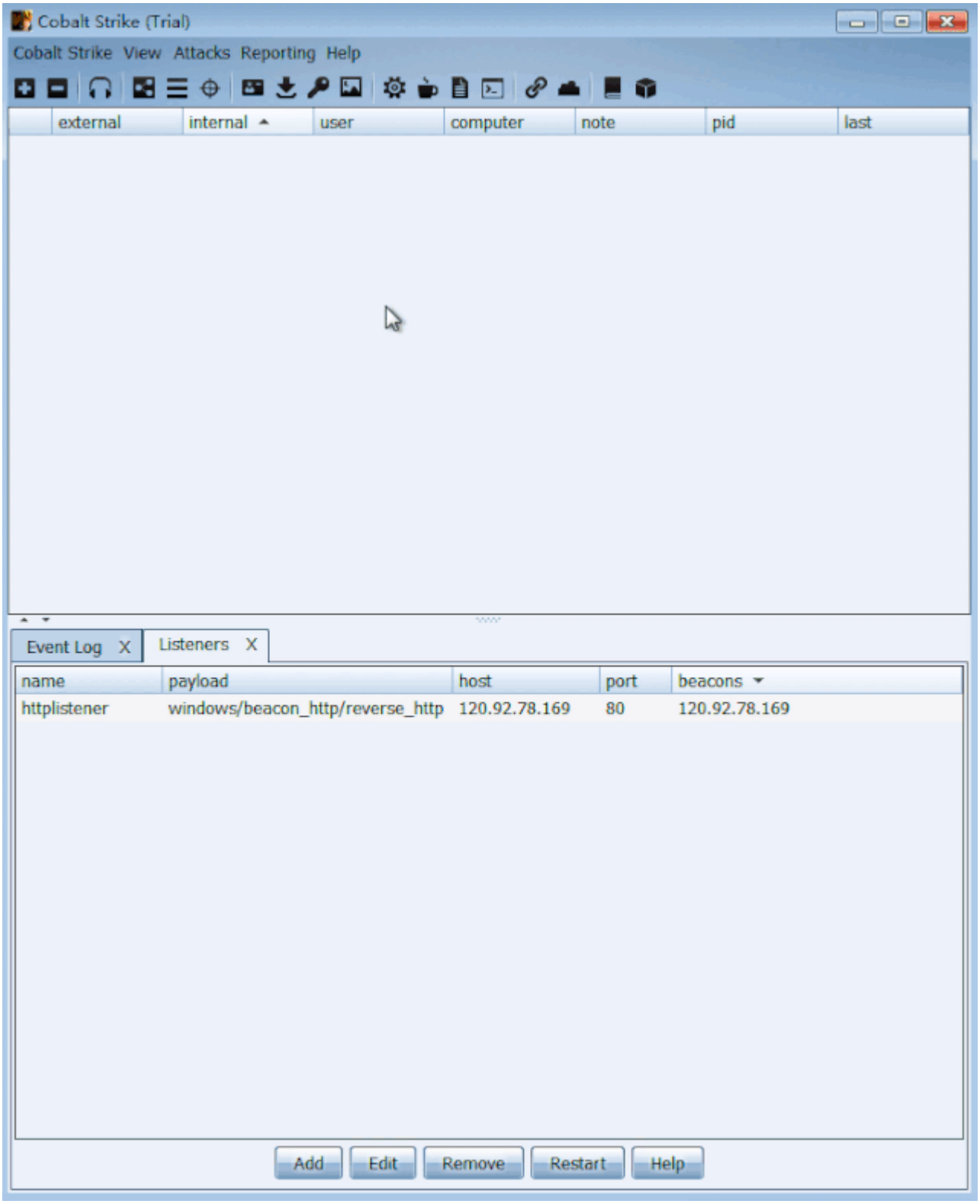
设置Listener

修改Listener**名称**以及在Team Server中**绑定并监听**的**端口**:



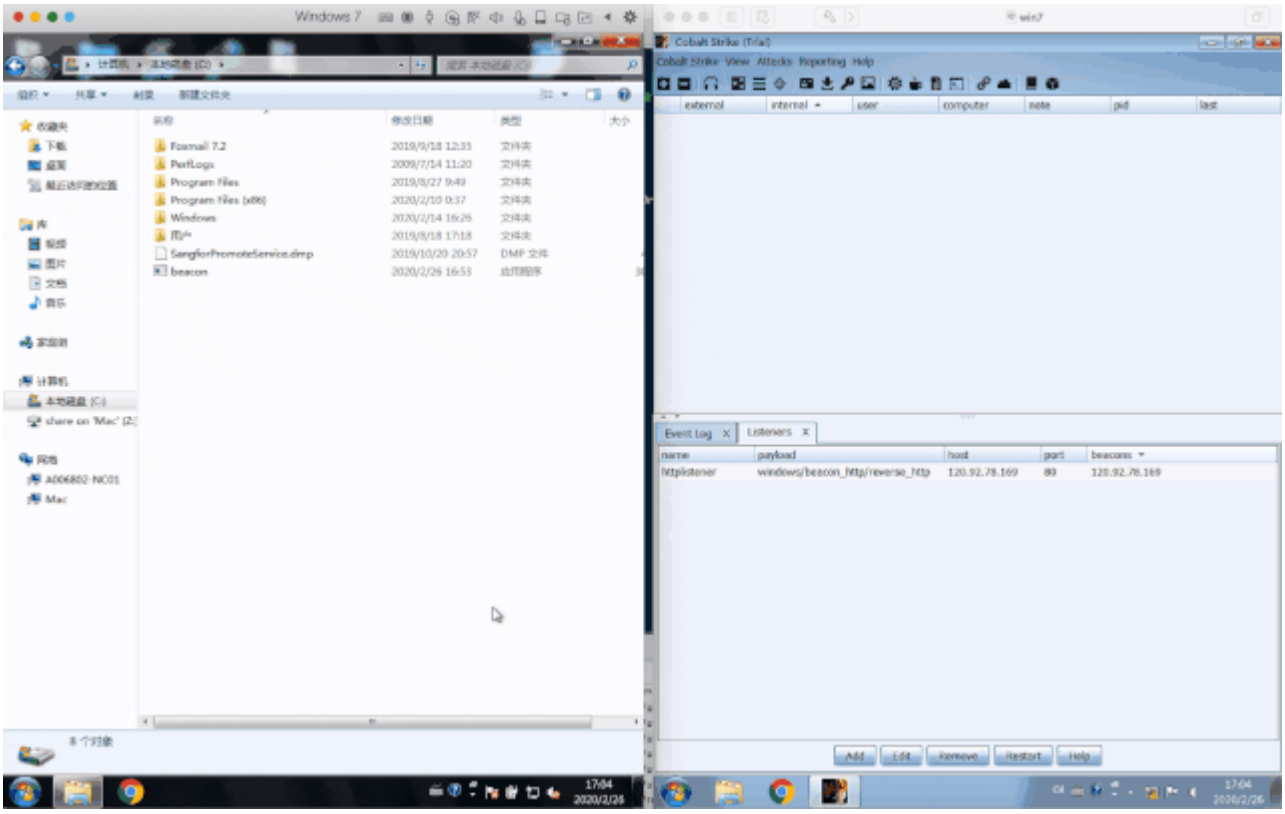
生成Stageless Payload

关于payload的类型我们下期会讲，大家现在只要先生成一个payload即可



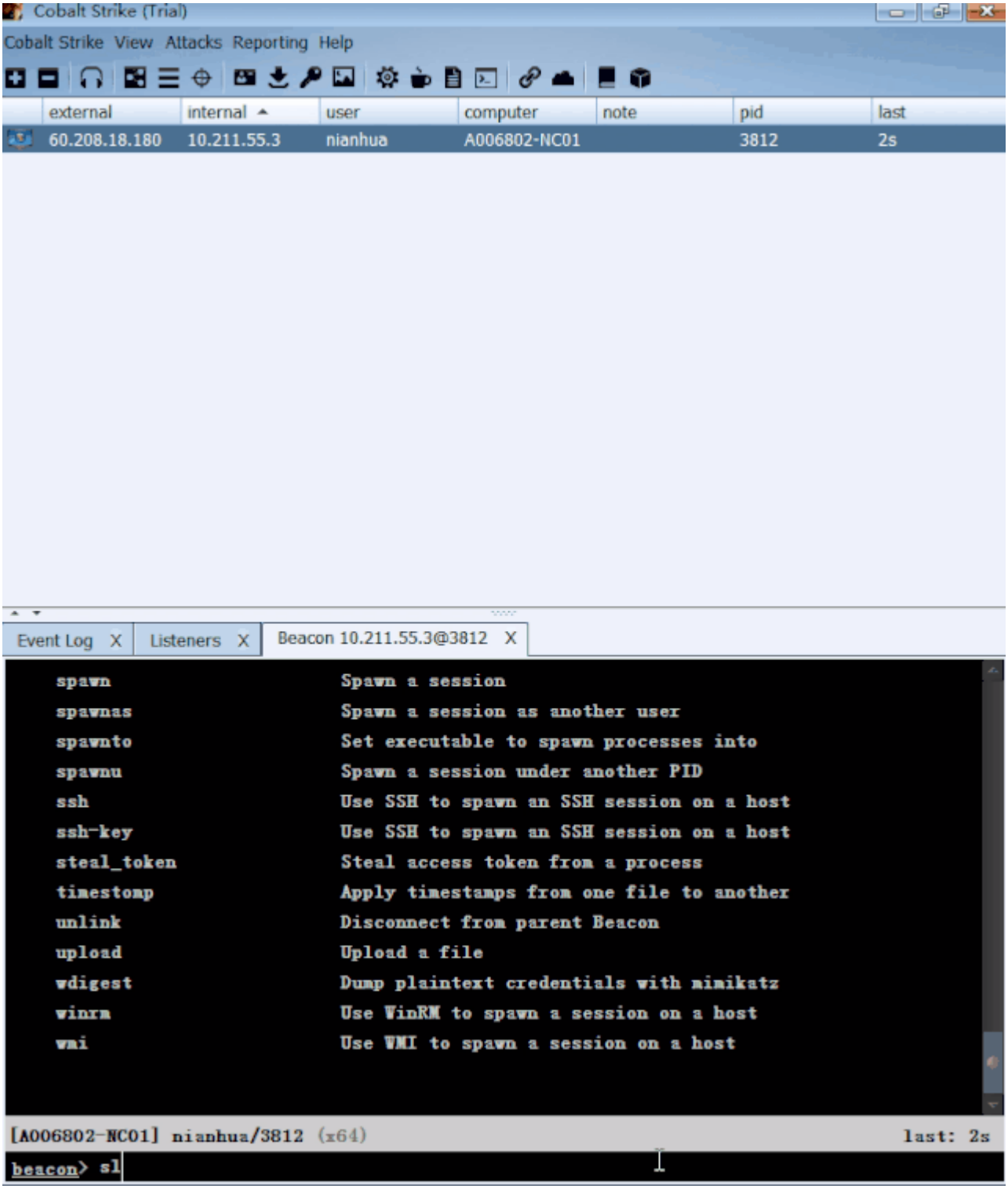
肉鸡上线

一直在想怎么描述Beacon Check in的过程，其实这个跟**肉鸡上线还是稍有区别的**，Beacon有一个睡眠的过程，它只会**每隔一段时间**来请求一次TeamServer



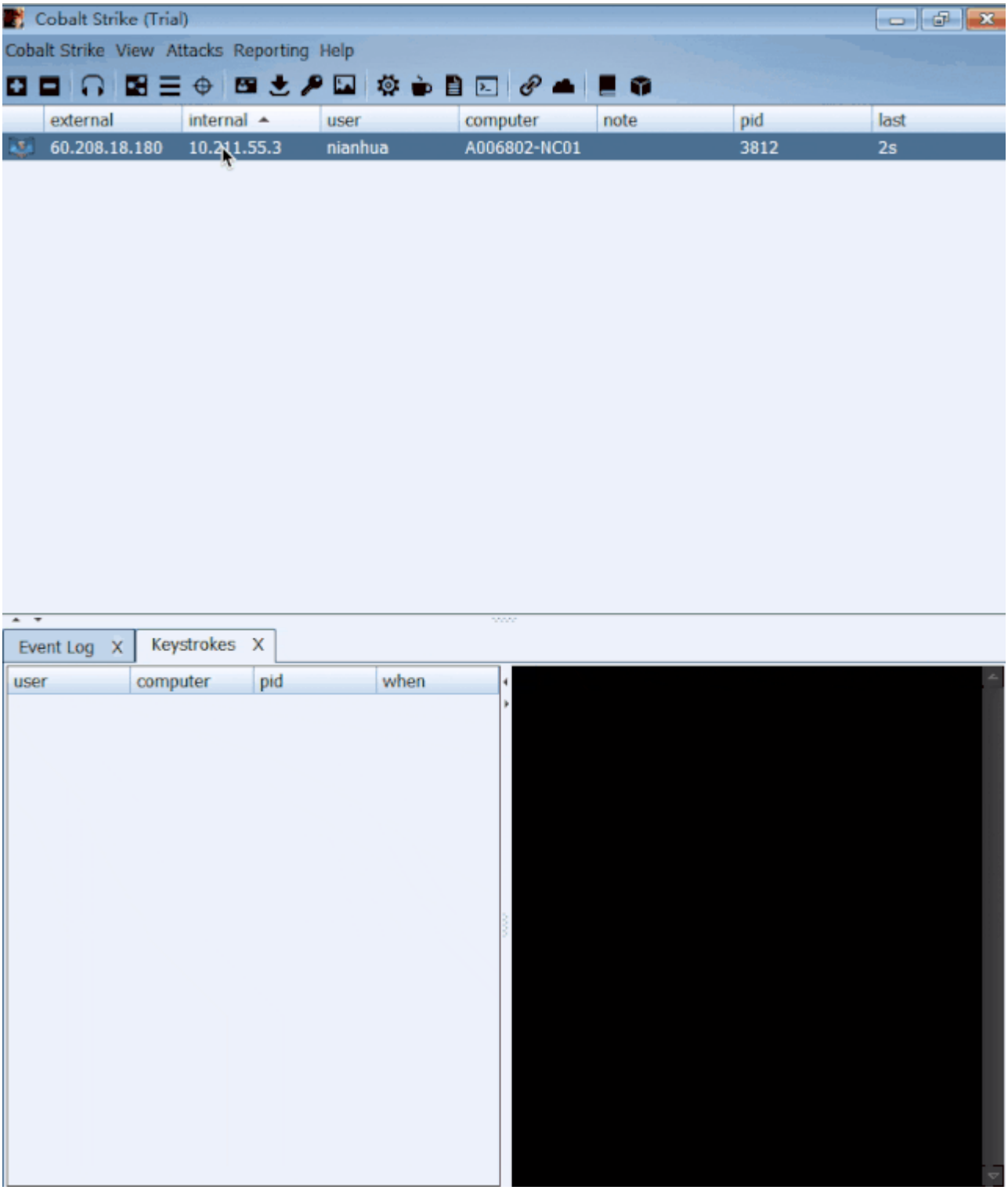
修改Beacon睡眠时间

我们可以通过sleep命令来**修改Beacon睡眠时间**



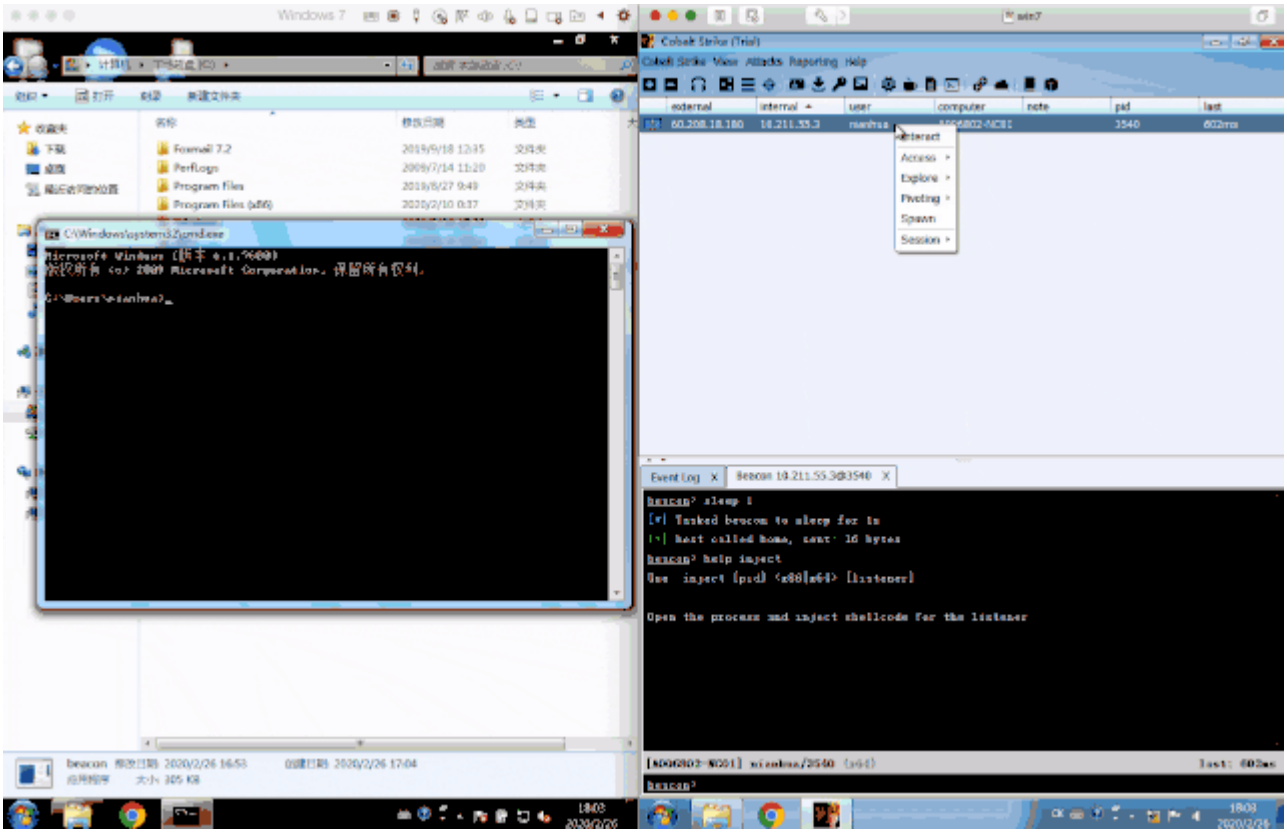
UAC提权

如果你在目标系统中的权限为普通用户，那我们可以使用这种方法将自己的权限**提升为管理员**



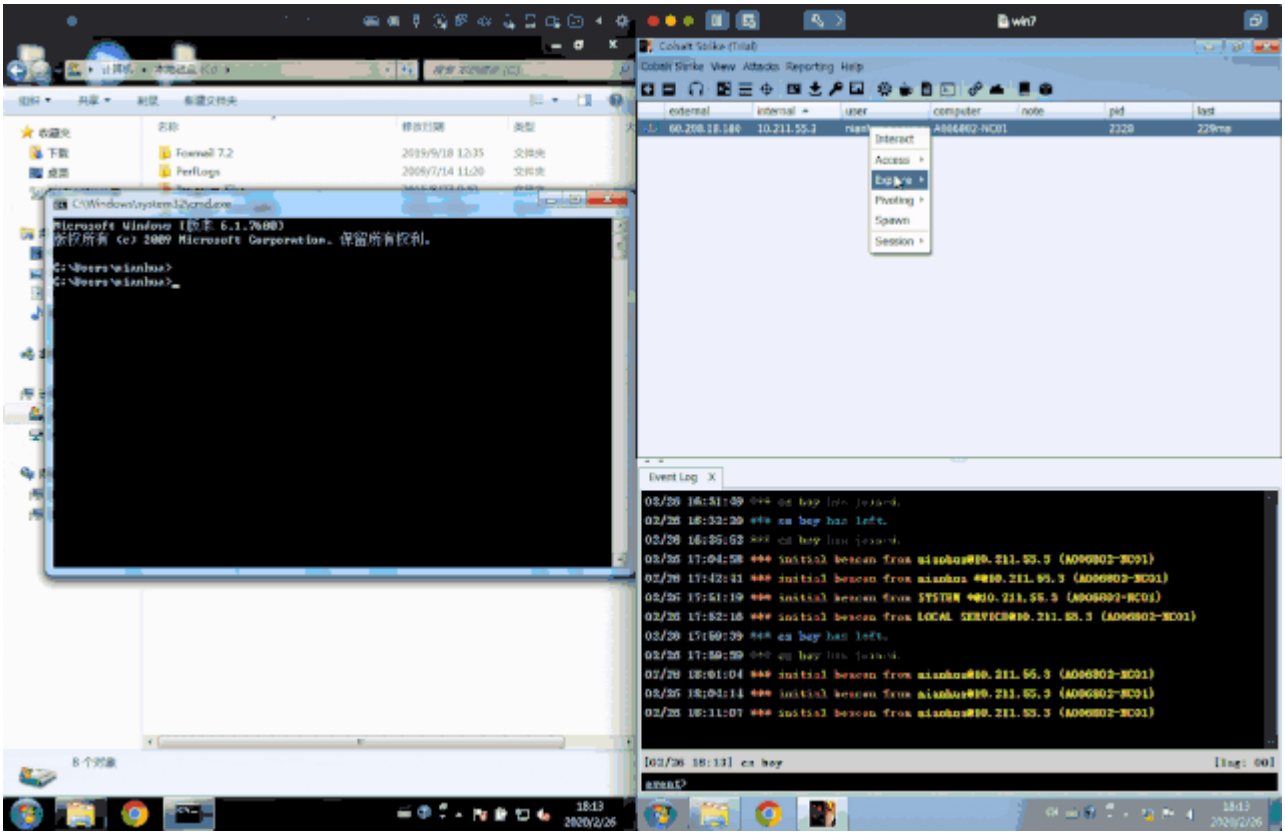
进程注入

我们可以将beacon**会话注入到另一个进程**之中，注入后，即使原来的后门进程被关闭，我们依然可以拥有目标主机的权限



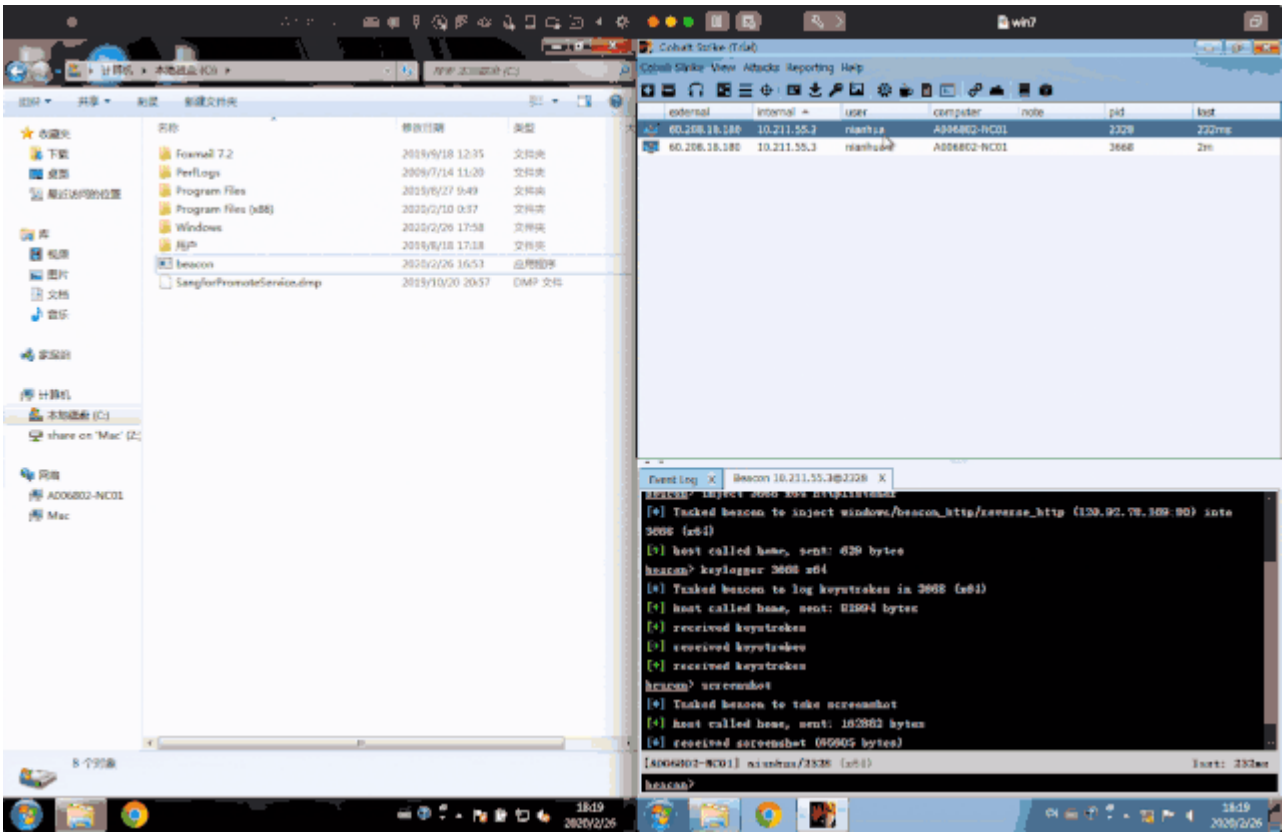
键盘窃听

这个键盘窃听和年华的键盘窃听不是一回事....



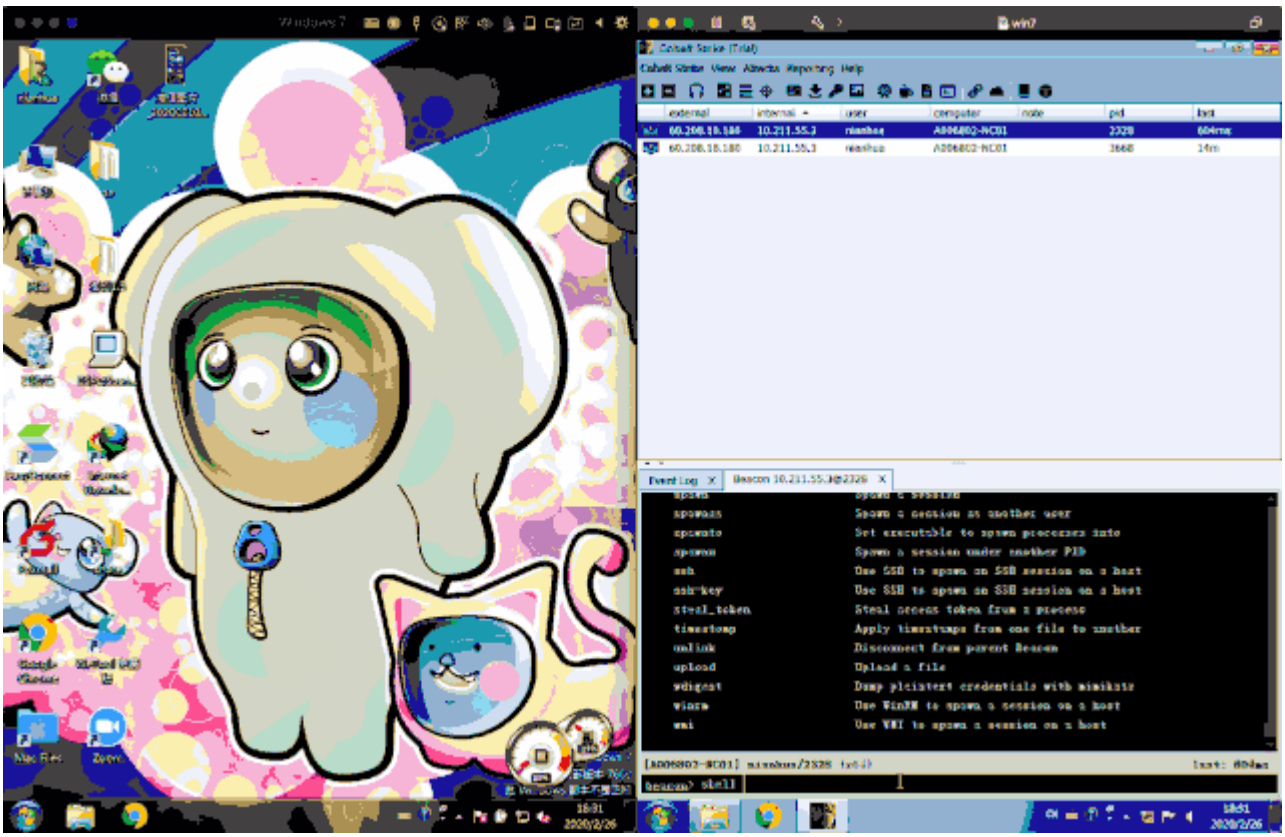
屏幕截图

Cobalt Strike 还支持屏幕截图功能，具体操作见下图



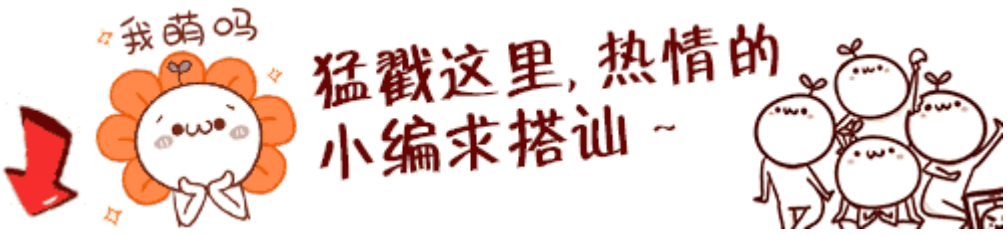
命令执行

在Cobalt Strike中我们可以使用shell + 命令的方式在目标主机上执行命令，十分方便



参考文章：

```
https://blog.csdn.net/qq_26091745/article/details/98994400
http://blog.leanote.com/post/snowming/62ec1132a2c9
```



喜欢的表哥点个

关注+再看