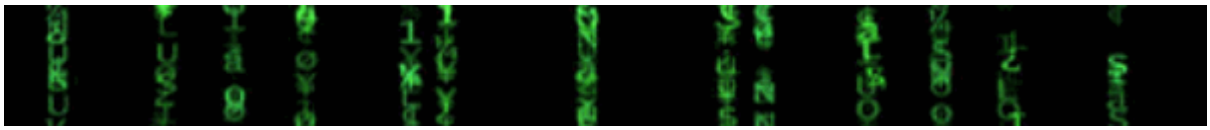
HW：Cobalt Strike 应该这样学

黑白之道 1周前

以下文章来源于七夜安全博客 ，作者七夜安全

七夜安全博客

本公众号分享的内容不仅仅是python开发，还有更多的安全内容。 主要内容： python 爬虫； pyt...



> **文章来源：七夜安全博客**

前言

> 良好的习惯是人生产生复利的有力助手

上一篇文章中讲解了elf loader的实现，接下来会有文章继续拓展这个内容：打造无execve的shellcode版bash，未来的linux渗透大杀器。

今天不分享这个，之前分享HW资料的时候，有朋友后台给我留言让我分享一下HW中的攻击，有点超出我的能力边界了。

但是想想 HW中使用 Cobalt-Strike 还是挺多的，于是就分享一下Cobalt-Strike的学习吧，花了一周的时间看了官方手册，以及网上公开的资料，对Cobalt-Strike有了整体认识。

这次的分享比较宏观，希望能对大家Cobalt-Strike的学习有一定的启发作用吧。

一.高质量的输入

> 输入

Cobalt Strike 4.0 手册：

关注公众号，回复 【13】返回下载链接。

Cobalt Strike | Beacon原理浅析:

https://www.secpulse.com/archives/124454.html

启明星辰ADLab：渗透利器Cobalt Strike在野利用情况专题分析:

https://nosec.org/home/detail/4449.html

Cobalt-Strike 系列:

http://blog.leanote.com/cate/snowming/Cobalt-Strike

Cross C2:

https://github.com/gloxec/CrossC2/blob/master/README_zh.md

基于DNS、HTTP和HTTPS隧道协议的木马流量分析:

http://www.lucien116.com/archives/261

渗透测试神器Cobalt Strike使用教程:

https://www.freebuf.com/company-information/167460.html

渗透利器Cobalt Strike - 第2篇 APT级的全面免杀与企业纵深防御体系的对抗:

https://xz.aliyun.com/t/4191

Cobalt-Strike-Aggressor-Scripts:

https://github.com/qiyeboy/Cobalt-Strike-Aggressor-Scripts

Cobalt Strike手册-环境搭建与基本功能:

https://cloud.tencent.com/developer/article/1512022

70.远控免杀专题(70)-终结篇:

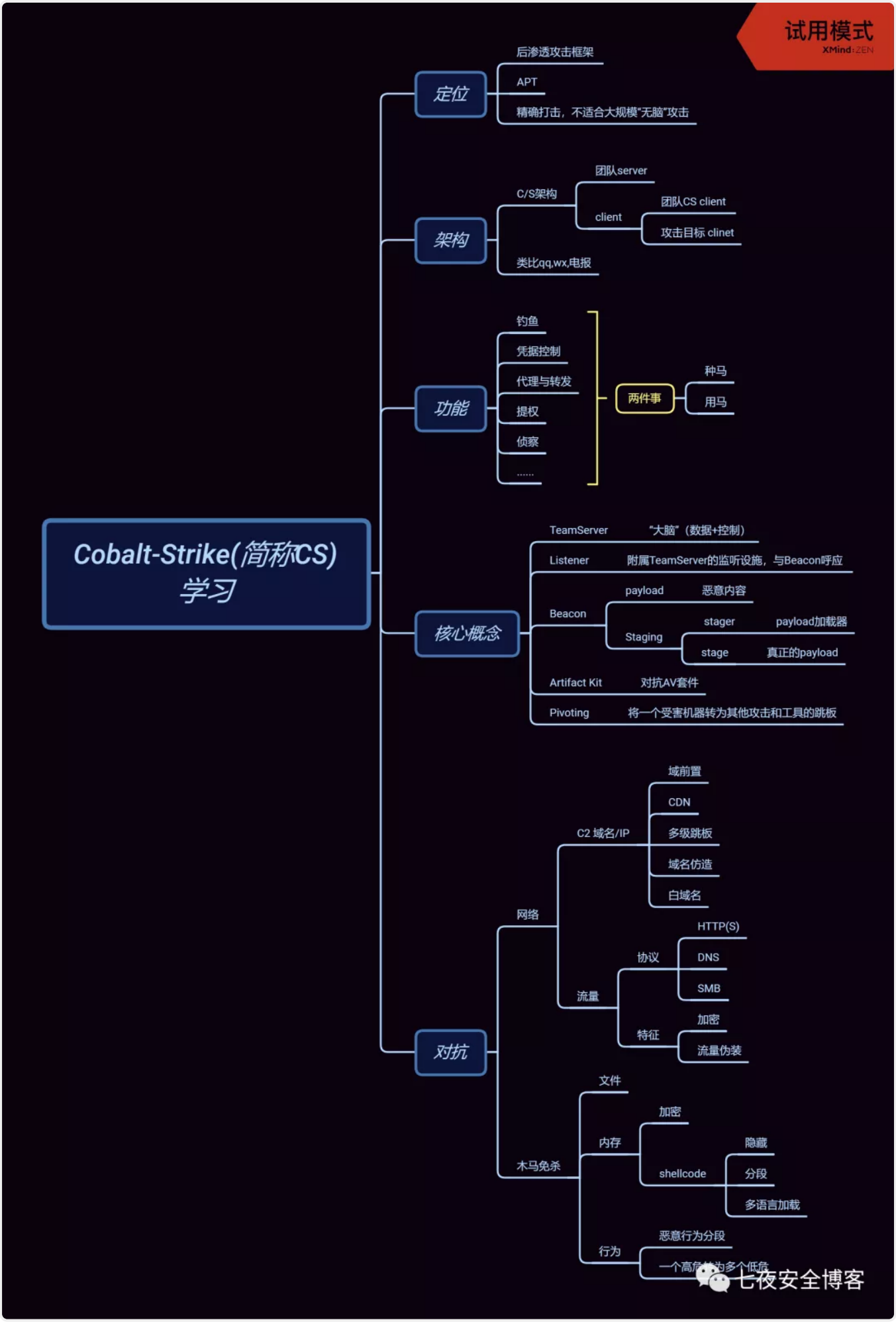
https://mp.weixin.qq.com/s/4shT8tP-Gu3XX7fnWKQHAA

二.思考整理输出

> 思考整理输出

找到比较合适资料后，不要匆忙地去学习细节，容易陷入里面，无法产生对Cobalt-Strike的整体认知，无法实现对知识的降维打击。

在学习Cobalt-Strike的过程中 ，先从定位，架构，功能，核心概念四个方面入手，至于对抗就属于比较细节的内容了，大家实践就可以了。整体思路如下图所示。


试用模式
XMind:ZEN
Cobalt-Strike(简称CS)学习
定位
后渗透攻击框架
APT
精确打击，不适合大规模"无脑"攻击
架构
C/S架构
团队server
client
团队CS client
攻击目标 clinet
类比qq,wx,电报
功能
钓鱼
凭据控制
代理与转发
提权
侦察
.....
两件事
种马
用马
核心概念
TeamServer
"大脑"（数据+控制）
Listener
附属TeamServer的监听设施，与Beacon呼应
Beacon
payload
恶意内容
Staging
stager
payload加载器
stage
真正的payload
Artifact Kit
对抗AV套件
Pivoting
将一个受害机器转为其他攻击和工具的跳板
对抗
网络
C2 域名/IP
域前置
CDN
多级跳板
域名仿造
白域名
流量
协议
HTTP(S)
DNS
SMB
特征
加密
流量伪装
木马免杀
文件
内存
加密
shellcode
隐藏
分段
多语言加载
行为
恶意行为分段
一个高危行为多个低危
七夜安全博客

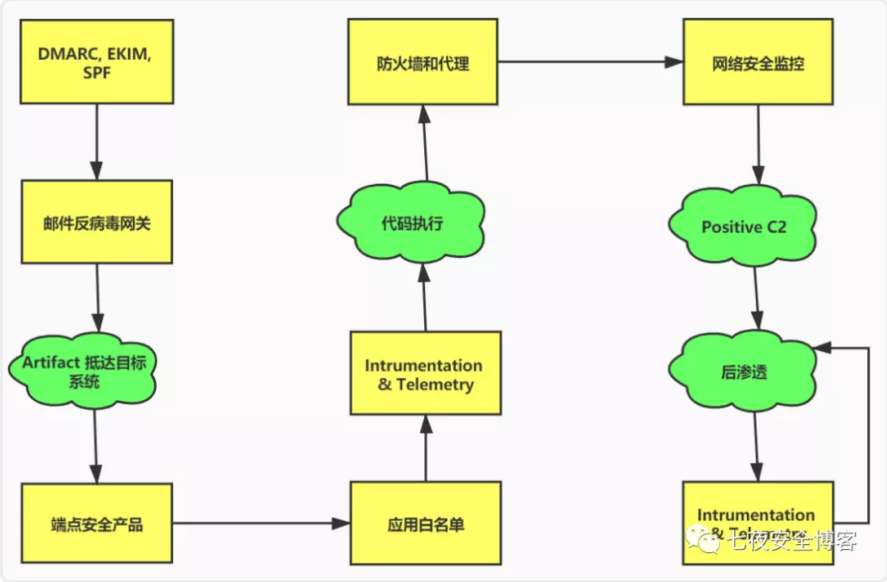
定位

首先需要了解一下Cobalt-Strike 的定位，没有什么解决方案是万能的，了解它的定位才能知道它的适用边界。在官方手册中有说明：

> Cobalt Strike 是一个为对手模拟和红队行动而设计的平台，主要用于执行有目标的攻击和模拟高级威胁者的后渗透行动

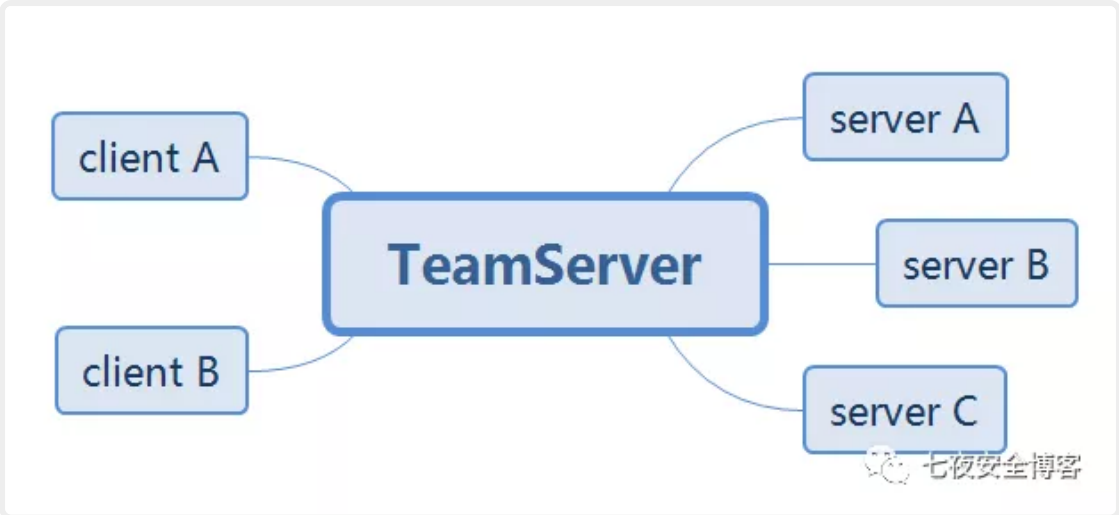
简单说就是适合有确定目标的apt攻击，对那种大范围的“无脑”攻击，例如ddos,僵尸网络，是不适用的。

下图是官方手册中描述Cobalt-Strike的一个攻防过程，有各种安全防御工具，也有攻击突破。

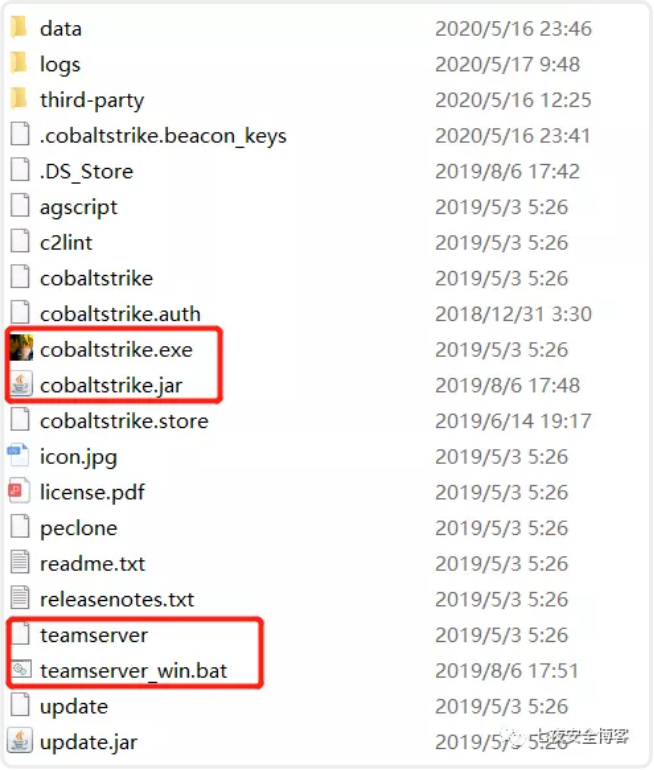


架构

Cobalt-Strike 是一个C/S结构，比较特殊的是属于多对多的关系，如下图所示：



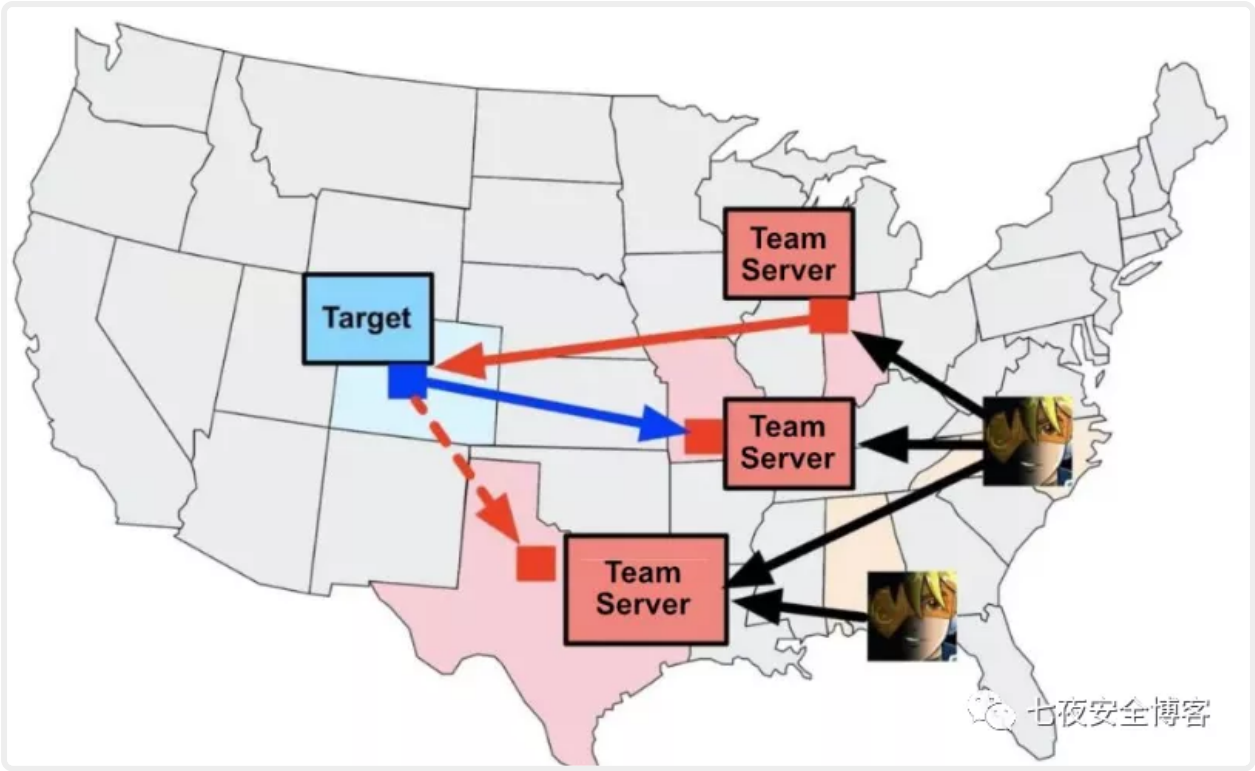
一个client可以连接多个server, 一个server可以被 多个client连接，在下图中 cobaltstrike.exe对应的是client，teamserver 对应的是 server。



虽然很多文章也是如上文描述Cobalt-Strike的架构，但是我个人认为**被攻击机器上的木马也应该属于client端**，只是功能和角色不一样罢了。

类比一下，比如我们使用的QQ和微信，腾讯的服务器属于server端，里面维持着所有client的通信和数据存储，每个人的QQ APP 属于client，而QQ项目组员工的运维平台也应该属于client。

下图描述了Cobalt-Strike在攻击过程中的架构关系：



功能

总结起来，Cobalt-Strike 就干了两件事 ： 种马 和 用马。在本机，简单使用Cobalt-Strike 演示一下种马和用马。

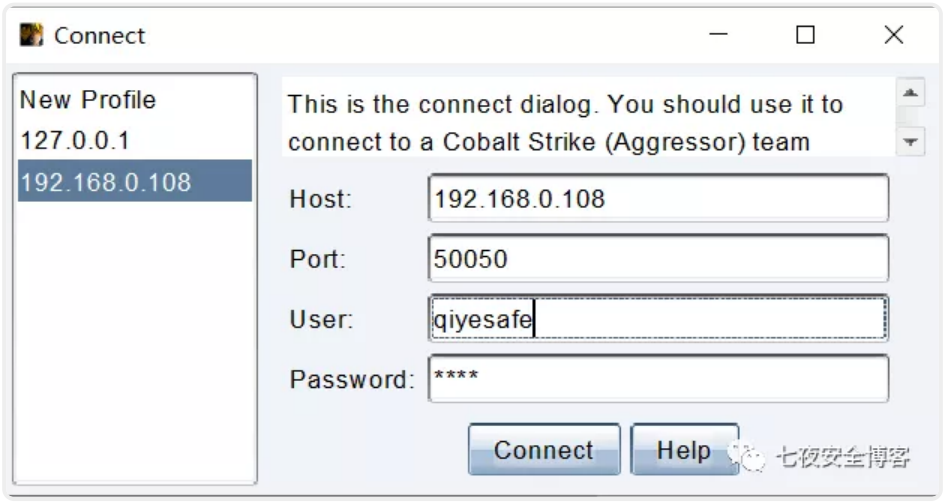
1. 启动TeamServer

192.168.0.108：这是主机ip

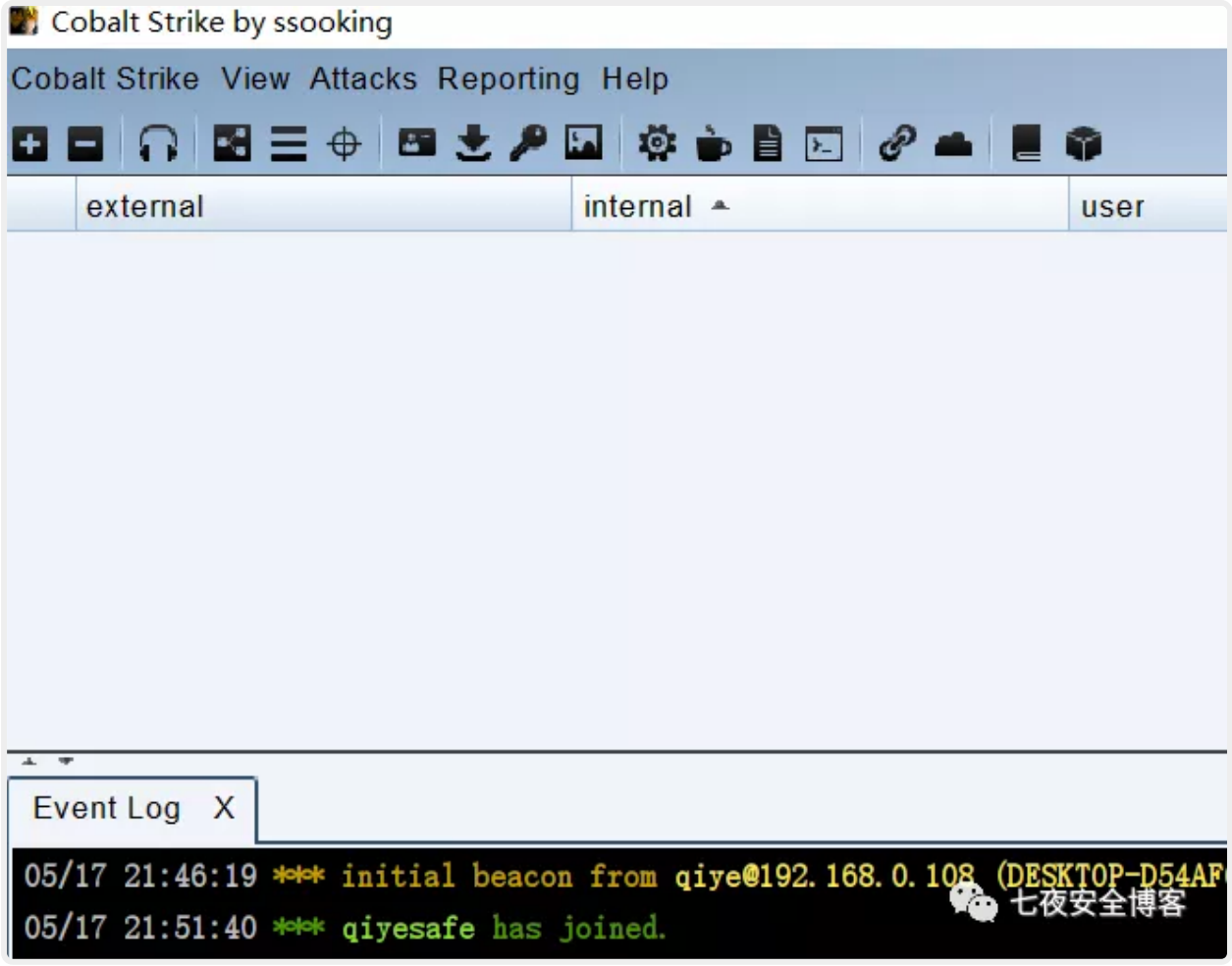
qiye：这是client 与teamserver 连接使用的口令

2. 启动Cobalt-Strike 连接teamserver

双击 cobaltstrike.exe，teamserver默认端口 为50050，输入User（随意只是个标识），输入password（见上文） 。

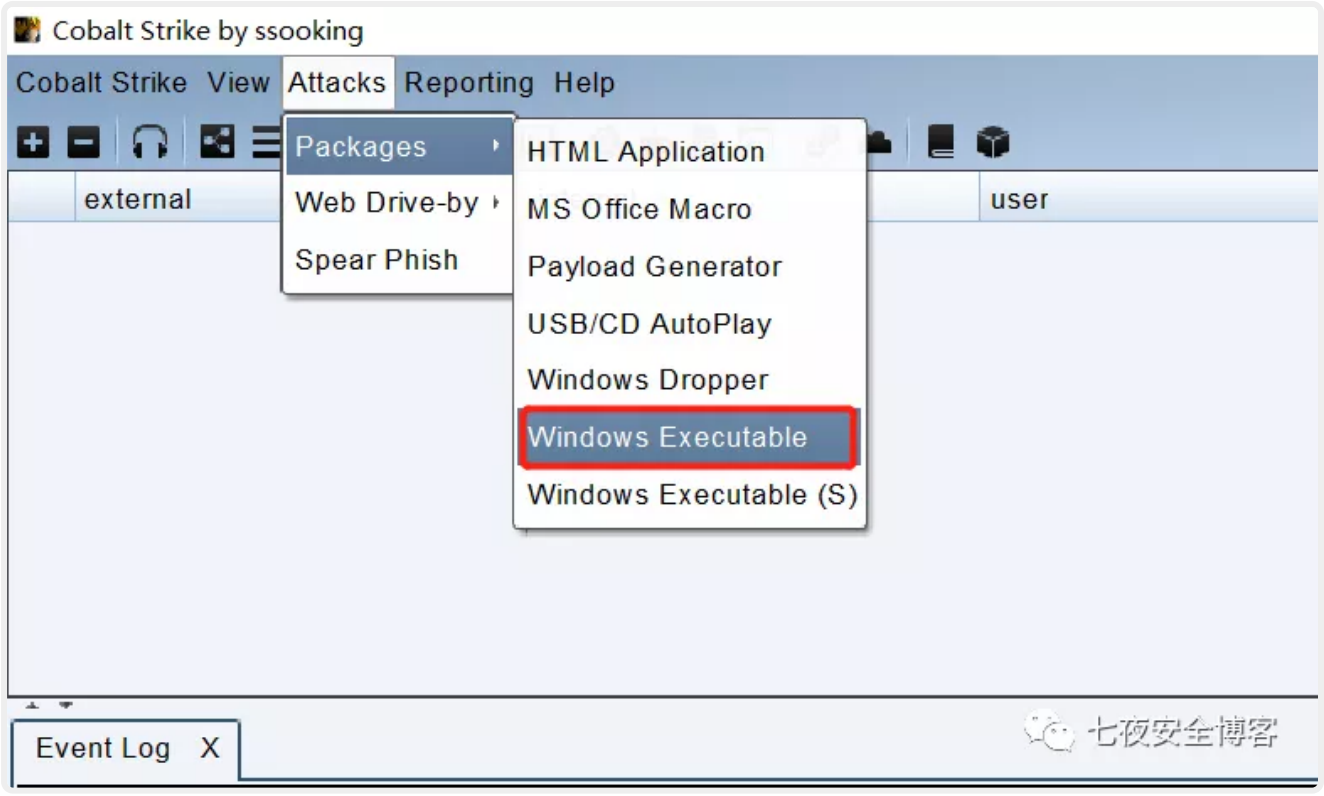


最后connect 连接上线：

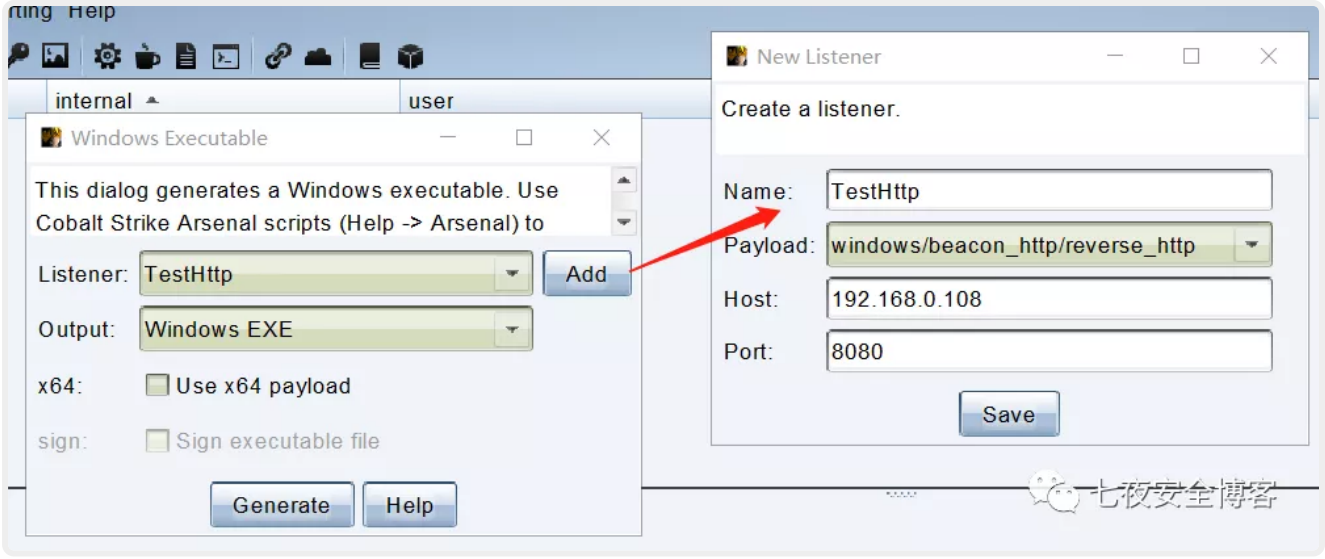


3. 创建Listener和beacon

在Attacks中选择 PE的攻击方案生成 exe,你也可以选择其他的payload，比如生成 宏和html 应用。

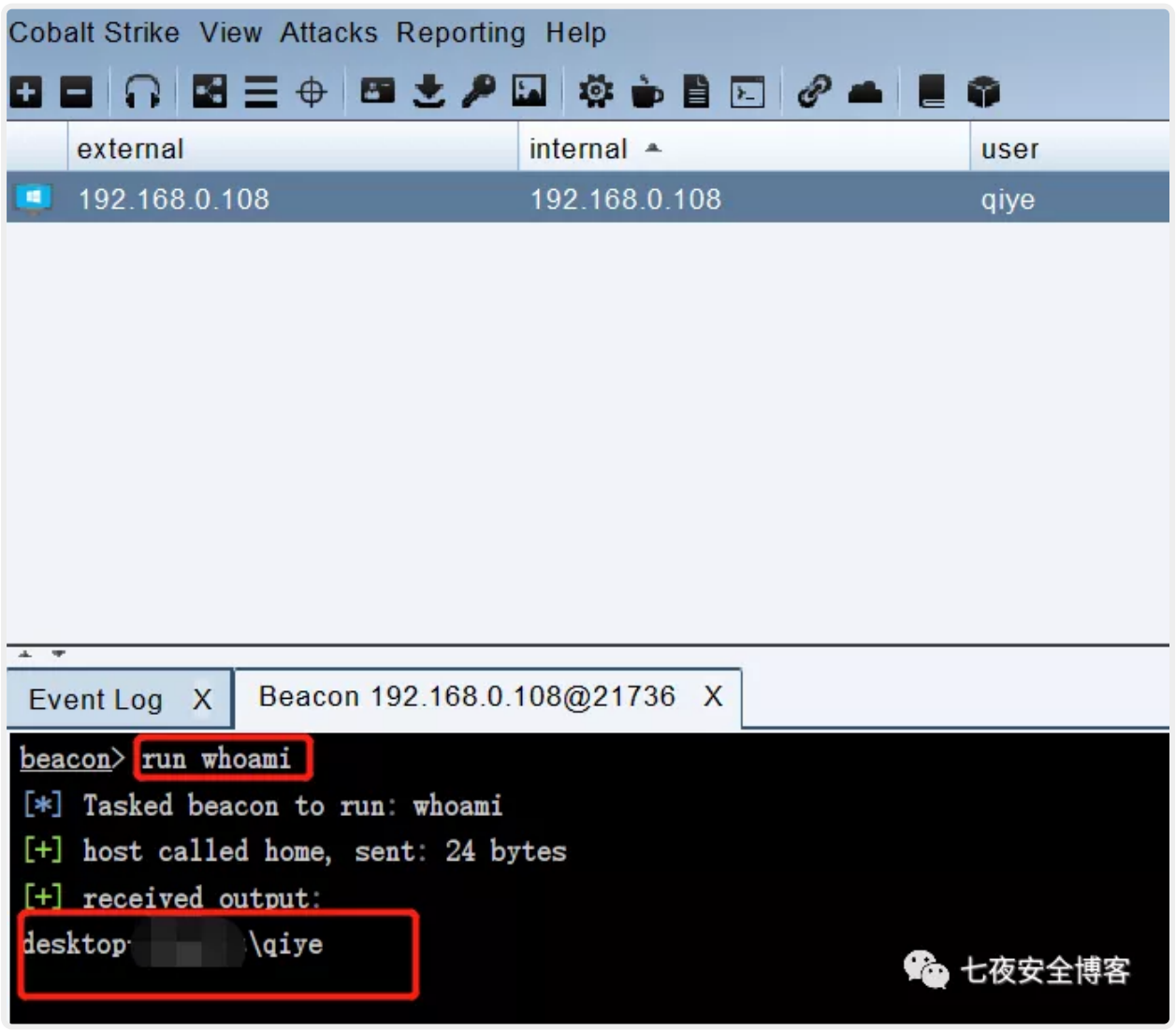


接着选择反连http的payload，选择listener中监听的ip和端口，listener是和teamserver是一侧的，生成的木马文件则是位于被攻击主机，木马保存为artifact.exe。



4．木马上线

双击artifact.exe，木马上线，在被攻陷主机上执行个whoami。



核心概念

看你对一个事物是否清楚，主要是能明白其中的核心概念。

TeamServer

TeamServer是整个系统中的“大脑”，包括数据的存储和共享，并维持着client的连接和流量中转

Listener

附属TeamServer的监听设施，与Beacon呼应 ，生成一个Beacon 对应一个Listener与之连接。

Beacon

Beacon 在Cobalt-Strike 中是很常见的概念,它是Cobalt Strike运行在目标主机上的payload，Beacon在隐蔽信道上为我们提供服务，用于长期控制受感染主机，简单理解的话就是一个木马。Beacon payload 有两种传输方式，第一种，像我上文使用的那样，是生成一个完整功能的payload。第二种是分段传输payload，属于 Staging模式，主要分为两个部分：

1. stager ： payload加载器，很精简的汇编指令
2. stage：真正的payload

这种模式适用于漏洞场景。假如windows有一个远程代码漏洞，exp 需要使用较短的shellcode，有长度限制，这很常见，不然无法触发，如果Cobalt-Strike 直接生成一个完整木马，是无法使用的，那可以先生一个精简的payload加载器，里面的功能只有下载和执行，完整的payload在下载的内容中。

对抗

Cobalt-Strike 在渗透测试过程中，主要对抗以下安全防御产品：

1. 防火墙
2. 杀软
3. EDR
4. IDS

检测手段无外乎，针对**文件，流量和行为，具体在思维导图中**，大家可以看一下 高质量的输入 章节中的对抗方式，不再赘述。

最后

Cobalt-Strike 进行对抗很灵活，大家按照官方手册好好练习，提供一份 破解版 cobaltstrike3.14 ，大家在公众号 回复【3.14】即可。

END