01-开班第一课

目录

**[一、](#_Toc138683320)****[作业内容](#_Toc138683320)** [3](#_Toc138683320)

[1. xxxx 3](#_Toc138683321)

[2. xxxxx 3](#_Toc138683322)

[3. …… 3](#_Toc138683323)

**[二、](#_Toc138683324)****[操作步骤](#_Toc138683324)** [4](#_Toc138683324)

[1. xxxxx 4](#_Toc138683325)

[2. xxxxx 4](#_Toc138683326)

[3. …… 4](#_Toc138683327)

**[三、](#_Toc138683328)****[作业总结](#_Toc138683328)** [5](#_Toc138683328)

[1. xxxxx 5](#_Toc138683329)

[2. xxxxx 5](#_Toc138683330)

[3. …… 5](#_Toc138683331)

1. **作业内容**

完成cs搭建上线windows主机

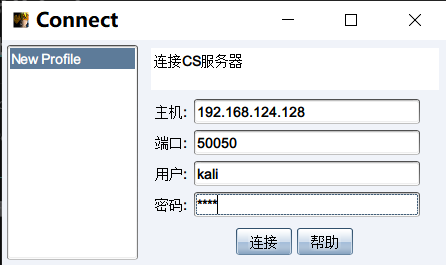
完成步骤截图放进word中

1. **操作步骤**

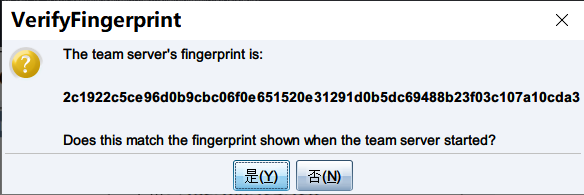
Kali虚拟机上安装Cobalt Strike



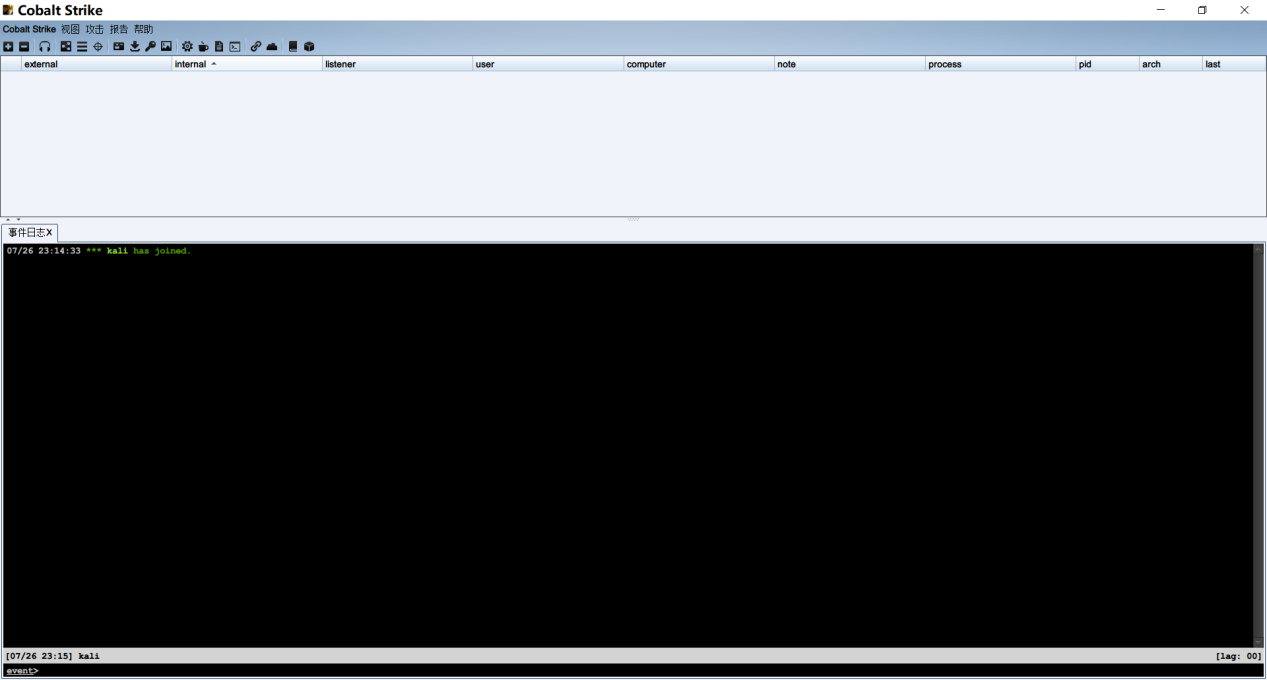
在Windows客户端上连接cs服务器



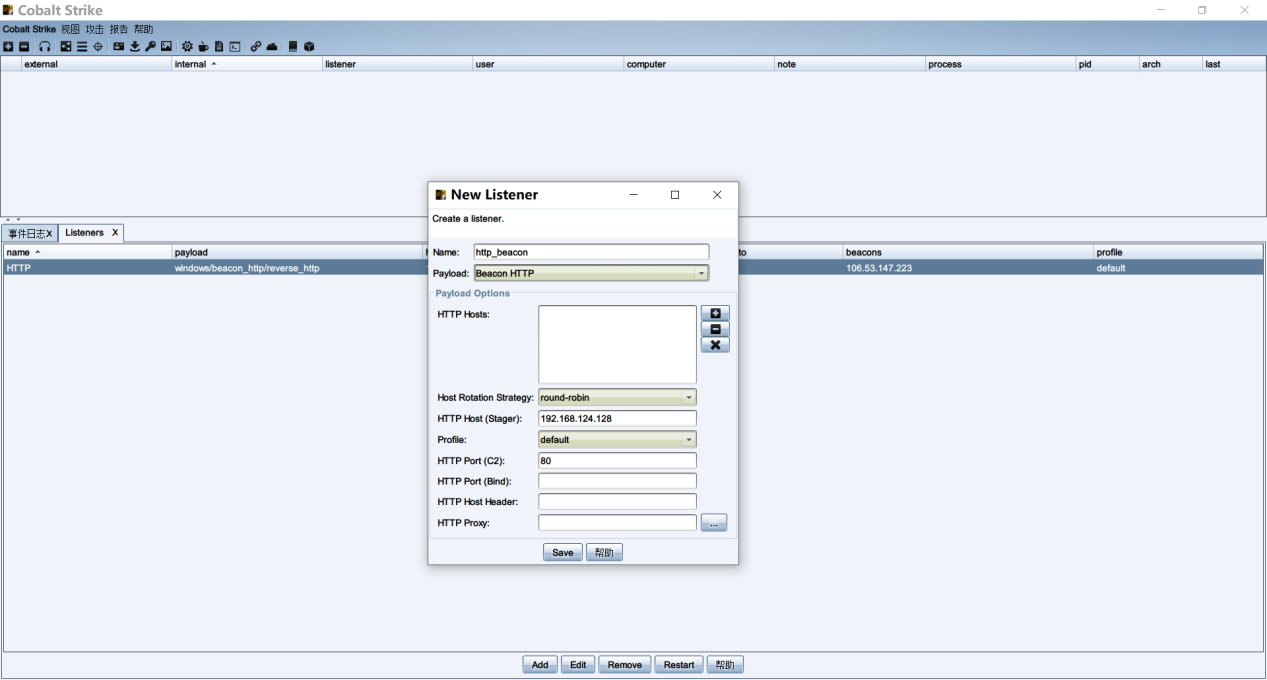
点击是



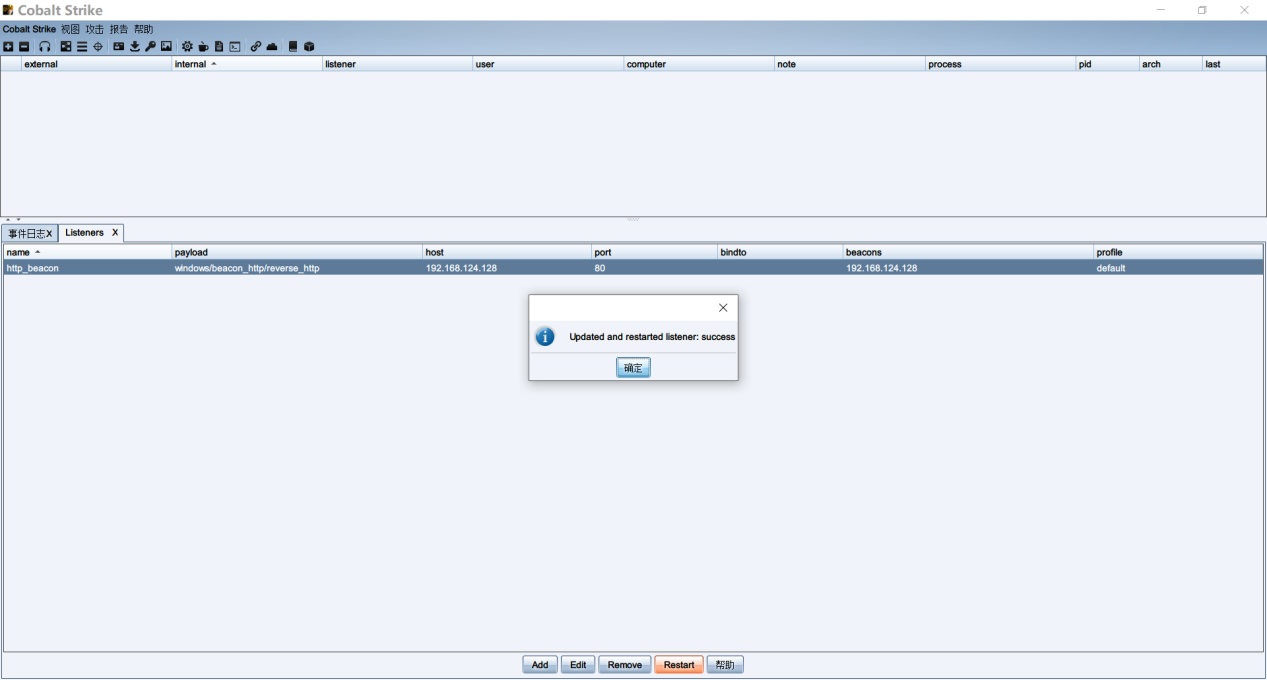
进入主界面



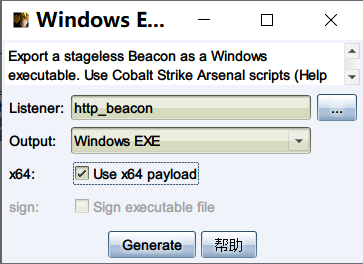
创建新监听器



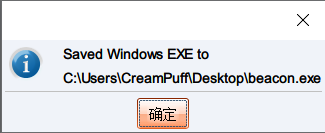
添加成功



新建Windows 无阶段木马



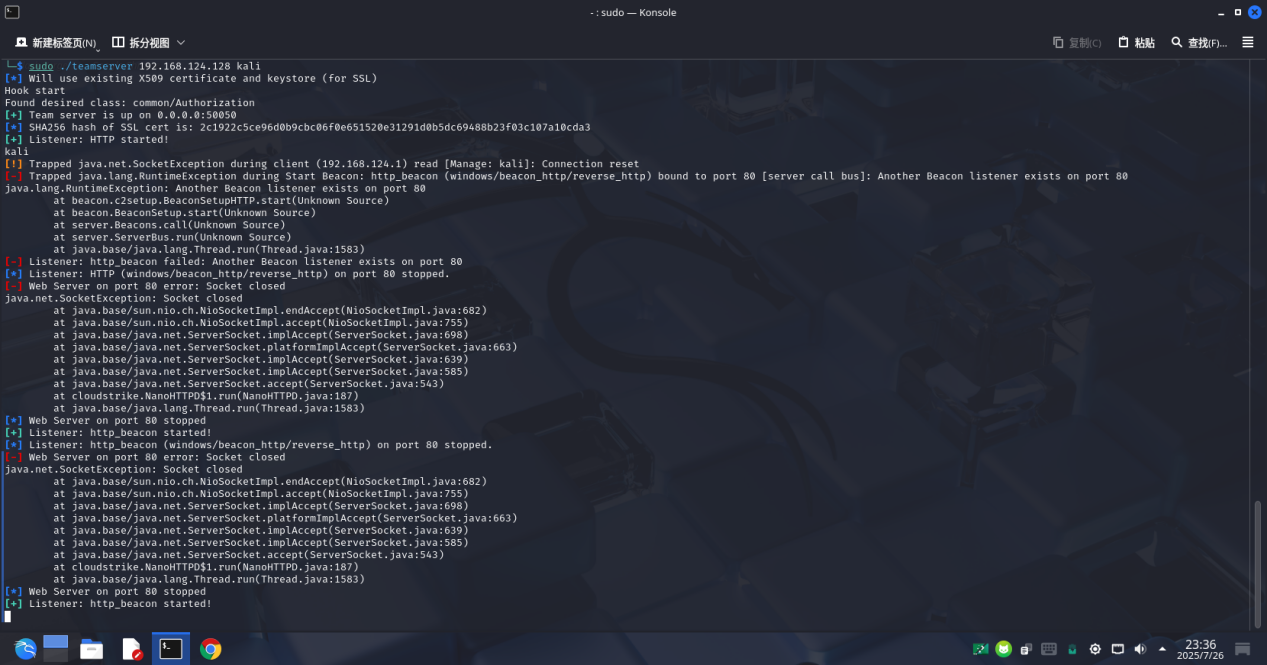
保存到桌面方便寻找



添加成功



返回kali发现连接成功



1. **作业总结**

1.掌握了C2框架基本架构：

本次作业让我对Cobalt Strike这一经典的C2（命令与控制）框架有了直观的认识。我理解了其“客户端/服务器”（Client/Server）的工作模式：需要在攻击机（Kali）上运行Team Server作为服务端，然后在另一台机器上运行客户端进行连接和管理。同时，我也明白了监听器（Listener）是接收“回连”信号的桥梁，而Payload（攻击载荷）是在目标机上执行的“后门”程序，整个流程清晰地展示了远程控制的基本原理。

2.体会到环境配置与细节的重要性：

在操作过程中，我深刻体会到环境配置的严谨性。首先，正确的Java环境是CS运行的基础，由于Kali软件源的更新，老版本的JDK无法直接安装，需要灵活更换为当前可用的兼容版本。其次，网络配置至关重要，必须确保攻击机和目标机处于可互相通信的网络（如桥接模式）。此外，Linux命令行的细节，如使用sudo提权运行服务、用引号处理带空格的文件路径等，都是确保每一步成功的关键，任何一个细节疏忽都可能导致操作失败。

3.学会了基础的故障排查与解决：

本次作业最有价值的部分是解决了一系列实际问题。从最初的openjdk-8-jdk软件包无法定位，到后来通过find命令才找到teamserver的正确位置，再到因权限不足需要加上sudo才能成功启动服务。这些问题让我明白，完全按照教程操作也可能因环境不同而遇到障碍。通过主动搜索和排查，我不仅完成了搭建任务，更学会了如何定位和解决问题的基本方法，这比单纯地完成操作更有收获。