# 如何快进到炸弹爆炸

**1.** 从 autolab 网站上下载 writeup 和 bombxxx.tar 到虚拟机。

**2.** 用 ssh 命令连接到服务器并修改初始密码。

大家好，目前小班的服务器已经搭好。后续部分 lab 有在服务器运行的要求。

lab machine 说明如下：

1、登录 IP 地址：162.105.31.232

2、登录账号：i+学号

3、端口号：查询 result.csv，第二列为端口号

4、登录协议：ssh

5、初始密码：学号

ssh 命令的基本格式是 ssh [-p port] user@host

port 是从 result.csv 中查询到的端口号，user 是用户名，即 i+学号，host 是服务器 ip 地址。

例如，查询到端口号是 22100，则连接命令即为

ssh -p 22100 i19000xxxxx@162.105.31.232

之后按照提示修改初始密码，并重新连接即可。

若 ssh 服务未安装，可以尝试命令

sudo apt-get install openssh-server

sudo apt-get install openssh-client

进行安装。

**3.** 用 scp 命令将 bombxxx.tar 文件传到服务器上指定路径。

这个命令需要在本地操作，可以用 exit 命令断开与服务器的连接。

scp 命令的基本格式是：scp [-P port] path1 user@host:path2

其中 port 是端口号，user 是用户名,host 是服务器 ip 地址，path1 是本地待传文件的相对路径，path2 是传递到服务器上的路径。

假设已经 cd 进入本地 bombxxx.tar 所在的目录，且在服务器上用 touch workspace 命令在根目录上新建了 workspace 文件夹。端口号为 22100，则传送文件命令即为

scp -P 22100 bombxxx.tar i19000xxxxx@162.105.31.232:/home/i19000xxxxx/workspace

注意这里 P 是大写的，并且/home/i19000xxxxx 才是我们在服务器上所看到的根目录文件夹。

**4.** 按照 writeup 的提示，将 bombxxx.tar 的文件夹解压，然后就可以开始尝试~~让炸弹爆炸~~拆炸弹了。

一些可能用不上的提示：

1.可以用 objdump -t bomb>bomb.txt 将 bomb 整个反汇编到 bomb.txt 文本文件中，这样就可以用文本工具快速查找特定的汇编代码了。

2.服务器上没有安装文本处理工具，可以用命令

sudo apt-get install vim

进行安装。如果安装失败，可以尝试运行命令

apt-get update

后再进行安装。

3.可以通过在炸弹爆炸的地方添加断点的方式来防止炸弹爆炸。

4.灵活运用调试工具，很多时候可以不必和汇编代码死磕。