Bomb简要指导

From TA:杨瑞国
祝大家拆弹愉快 以下内容如有错误导致BOOM本人概不负责(

0.关于lab machine

账号、端口号见result.csv

初始密码为学号

登录方式：打开终端，输入ssh ${username}@162.105.31.232 -p ${port}

eg. 我的账号是i1700010000，端口号是2020，那我输入为：

linux> ssh i1700010000@162.105.31.232 -p 2020

登录后要求输入密码，注意密码没有回显，输入完回车就好

（当然也或许是要改密码？）

1.下载bomb

在autolab上面Download handout或Download your bomb均可（效果一样）

注意：如果下载了多个bomb，把其余的删掉只留一个做即可

2.解压bomb

可以直接linux中右键解压，也可以按照wp所写的方式

3.上传bomb

bomb只有在lab machine中才能运行，因此我们需要将bomb上传到服务器

用的是scp命令，可以百度或者通过--help等查看用法

我们这里只要在bombk文件夹中打开终端，输入scp -P ${port} bomb ${username}@162.105.31.232:~即可

同上eg.

linux> scp -P 2020 bomb i1700010000@162.105.31.232:~

输入密码即可将bomb上传到服务器

4. 反汇编

我们使用objdump命令来反汇编，可以参考wp或者--help

在这里我们一般可以用如下命令：

linux> objdump -d bomb > bomb.txt

将反汇编结果输出到bomb.txt中，之后就可以开始愉快读代码拆弹啦~

5.运行bomb

登录到服务器后，**千万不要直接./bomb运行！**

gdb是我们的调试神器，善用gdb可以帮你避免explode扣分！

gdb bomb即可开始调试

不管干啥首先一定要在explode函数那里下断点

b explode_bomb

之后再run

同时continue(c)也一定要看清楚停在了哪里再使用！如果在explode_bomb断点处继续按c就直接炸了... 具体调试方法可参考wp里面的链接~

6.其他

每次破解出一个phase的答案可以记下来到一个solution.txt里面，省的每次手打 只要在gdb中run的时候改成 run < solution.txt 即可

defuse或者explode都不会立刻显示在autolab的scoreboard上，一分钟以后再看。不要没看到成绩就不停地运行提交...