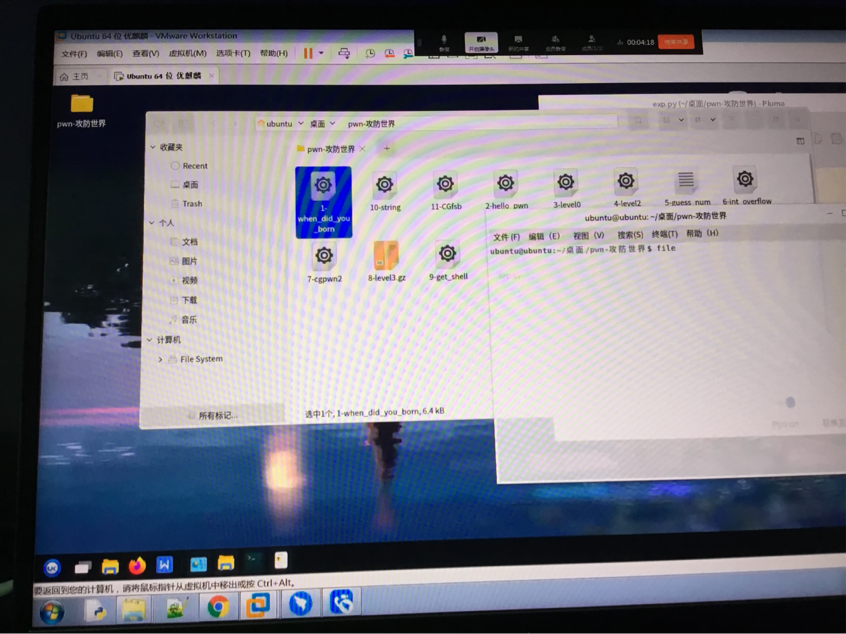
ctf wiki

做pwn题，lf文件用Linux首先看多少位，命令：file + 文件名

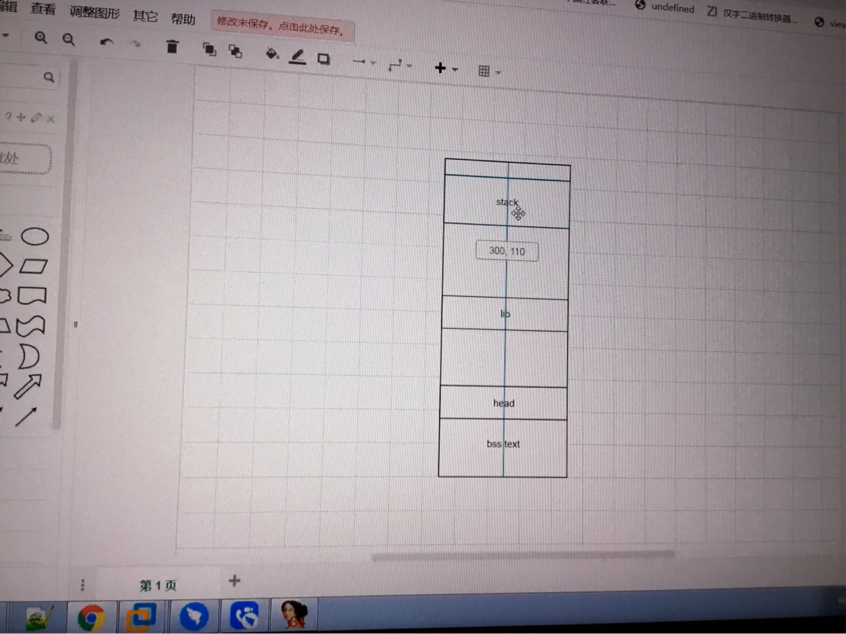
看文件保护，命令：checksec —file=文件名

canary 金丝雀保护 NX堆保护

多使用字符可导致溢出

gdb 调试函数

断电 b + 函数名

lf文件结构 

Stack 栈 heap 堆

清晰结构以后，编写一个exp脚本（在Linux内部）

1、导入一个函数库，用pwn的工具

2、脚本方便调试

3、content = 1；连接

4、创建主函数main

5、返回其数据。近端采用process，远端采用remote（地址要用双引号，端口不用

6、使用payload来发送数据（类似于输入）

7、使用ida来计算数据的长度，用垃圾数据来覆盖

（b‘a'指的是a字符，p64（1926）指的是将1926以64位打包发送）

8、recvuntil指什么时候接收到哪句话 sendlineafter：遇到哪一条语句会发送哪一句话

（进入pwn，运行 ./1可以运行程序

9、sendline指发送数据给对象

10、最后再接收一下数据

11、写main，运行一下程序python3 exp\py

没有找到目录，意味着已经打通，然后将content = 0；去打远端（攻防世界的靶机

