Week2

ROP Primary

首先打开checksec，发现没有PIE，然后打开IDA。

要算a * b,bss段里abc三个变量，abc前八位存了行和列，后八位是地址，输出了ab，要算c，而且a的列数和b的行数相等，大致知道是矩阵乘法，学了下python循环给了答案。

然后到了vuln，很明显的栈溢出，然后rop。但是需要地址，然后有puts，然后写了leak用dyn，over，得到system的地址。接下来构造ROP链，选择_libc_csu_init()函数里的gadget()，然后是跳到6个pop，写入寄存器，然后返回跳到前面的mov，传递参数，然后调用read，之后继续执行了6个pop，传递了system的参数，然后一样的方法调用system。这些在一条语句里完成，但是调用system失败，尝试栈对齐，加一个ret，没有用。

之后在学长的帮助下，想到也许是dyn的问题，因为有动态加载，所以system的地址不能常用，但是可以知道他和别的函数的偏移，再开了一次，输出了system和puts的偏移，然后重写一个exploit，利用puts泄露puts的真实地址，然后的到system的地址，然后ROP，OVER！！