Problem 1:

1. 操作步骤：
   1. 首先输入’p’使用公有权限登录
   2. 输入’rxxxxxxxxxxxxxxxs’，使得当前用户权限变为s，并且读入secret文件内容。
2. 原理：command数组和dataset数组的堆栈空间是连续的，而gets函数是不会检查输入字符串的长度的，所以输入一个超过command数组长度的字符串可以利用堆栈溢出漏洞覆盖掉dataset数组的内容。
3. 解决方法：将29行替换为fgets(str,字符串大小,stdin);

Problem 2:

1. 操作步骤：
   1. 输入’257’，使得uint8\_t类型溢出，即可读入secret文件内容。
2. 原理：因为uint8\_t类型最大值为2^8-1=255，将256赋值给一个uint8\_t类型的变量时，变量的实际值为0。将257赋值给一个uint8\_t类型的变量时，变量的实际值为1.
3. Change line 47 to: else if (command < 256)

processCommand(command);

Problem 3:

1. 操作步骤：

a) 输入 %d %d%d%d%d%d%d%s, 得到secret内容为 Oh,What a hack…what a lovely hack.

2.原理：因为printf没有格式化字符，那么input可以由用户控制，就会导致字符串漏洞的发生,输入多个 %d,printf便打出heap中的相应的地址，在通过%s输出字符串

3.解决方法：Change line 24 to printf(“%s”, input);

Problem 4:

1. 操作步骤：
   1. Mv修改public.txt为public.txt.bat,
   2. 输入命令 ln -s /home/netsec/secret4.txt
   3. 运行程序，得到secret的内容：The answer is 42.
2. 原理：linux映射到文件，在程序有权限的情况下，可获得内容
3. 解决方法：使用 stat结构体判断文件是否为链接型文件。 S\_ISLNK(m.st\_model)

Problem 5:

1. 操作步骤：
   1. 连续输入多个 %d 得知 minimum\_level 的位置
   2. 连续输入 十五个 %16x 获取宽字符，填充数据 然后使用 %n 对值赋值 成功绕过
   3. 获得secret的内容 whew, you are finally done with the homework
2. 原理： linux 字符串格式化漏洞，通过％ｄ　可以做到read anywhere 。通过查找到指针的偏移 在通过 %n 对指针赋值，从而修改权限码
3. 解决方法：change line 28 to printf(“%s”,user-username);