**Computer Security HW0**

R08946007 資科所 蔡昀達

Nickname : r08946007

1. Shellc0de

使用pwntools 的 shellcraft 模組產生shellcode，使用pwntools 的 encoders 將產生shellcode 替換 syscall的字元。

1. Open my backdoor

使用hackerbar的chrome 插件來建立get, post request。在url中利用\_GET[87]和\_POST[%23] 傳遞參數來控制php中執行的涵式和參數。在php中執行exec涵式並且執行一段php的reverse tcp shell就可以拿到flag。

1. M4chine

將pyc檔案反編譯之後可以得到source code，之後可以發現程式碼類似模擬一段組合語言的執行過程，一條一條反推之後可以得到flag。

1. Encrypt

由(E \*\* ( I \* pi ) + len(key) == 0) 可以知道key長度只有1，因此可以得知是由8種stage0和stage1的任一組合，將encrypt反過來之後 (主要為permutation的部分) ，就可以找到flag。

1. Winmagic

使用x86dgb工具開起exe檔，找到Give me maigc的字串之後，將斷點設在判斷password跟magic上面，在執行時將判斷值修改就可以執行到印出flag的分支。