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。

2. 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。

3. 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。

4. 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。

5. 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。