Homework 0x01 Hint

ddaa

1-1 Tormity

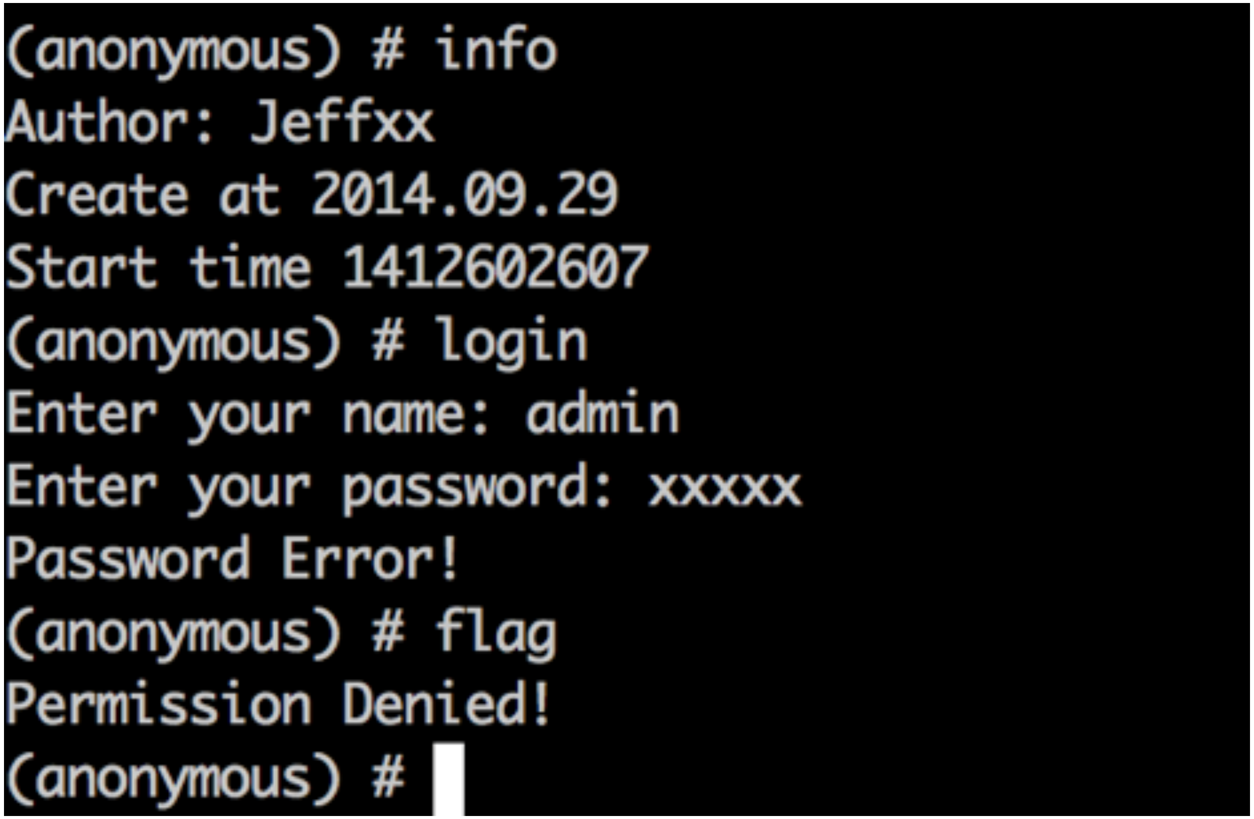
- This is bonus…
- All hints are on the website. :p

1-2 simpleshell

- Are you familiar with static analysis?
- nc secprog.cs.nctu.edu.tw 10001

- Using disassemblers, like ida pro, may help you a lot.

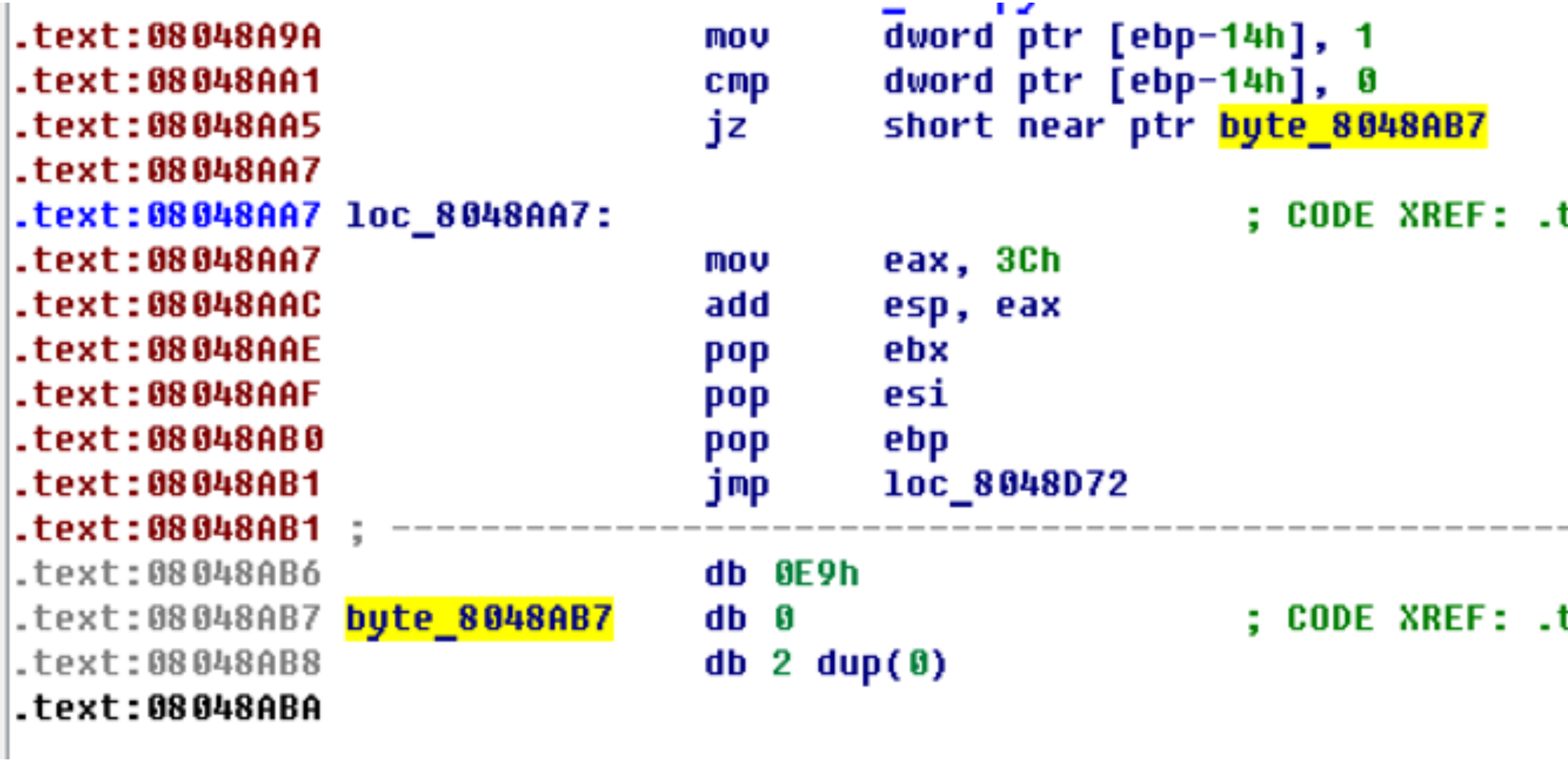
- All you need is
  - info
  - login
  - key



```
(anonymous) # info
Author: Jeffxx
Create at 2014.09.29
Start time 1412602607
(anonymous) # login
Enter your name: admin
Enter your password: xxxxx
Password Error!
(anonymous) # flag
Permission Denied!
(anonymous) #
```

Reverse Encryption Algorithm 1

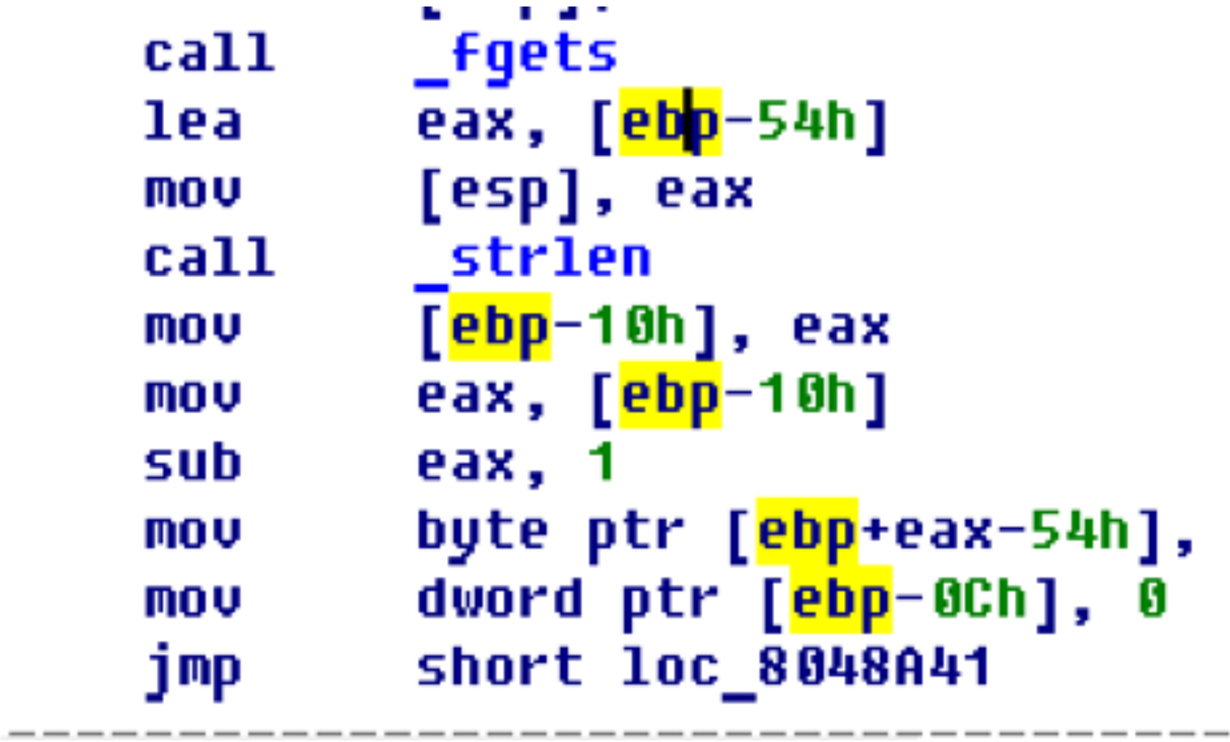
- Patch strange jump



```
.text:08048A9A                       mov     dword ptr [ebp-14h], 1
.text:08048AA1                       cmp     dword ptr [ebp-14h], 0
.text:08048AA5                       jz      short near ptr byte_8048AB7
.text:08048AA7
.text:08048AA7 loc_8048AA7:                                         ; CODE XREF: .t
.text:08048AA7                       mov     eax, 3Ch
.text:08048AAC                       add     esp, eax
.text:08048AAE                       pop     ebx
.text:08048AAF                       pop     esi
.text:08048AB0                       pop     ebp
.text:08048AB1                       jmp     loc_8048D72
.text:08048AB1 ; ---------------------------------------------------------------
.text:08048AB6                       db  0E9h
.text:08048AB7 byte_8048AB7          db  0                          ; CODE XREF: .t
.text:08048AB8                       db 2 dup(0)
.text:08048ABA
```

Reverse Encryption Algorithm 2

- Manually decode it! (from 080489C5)
  - – Ebp-54 = buf
  - – Ebp-10 = len
  - – ….
  - – ….
  - – …



```
call    _fgets
lea     eax, [ebp-54h]
mov     [esp], eax
call    _strlen
mov     [ebp-10h], eax
mov     eax, [ebp-10h]
sub     eax, 1
mov     byte ptr [ebp+eax-54h],
mov     dword ptr [ebp-0Ch], 0
jmp     short loc_8048A41
```

Decryption

- Get seed from “info” command
- A ^ B = C => A = C ^ B
- Bypass authentication

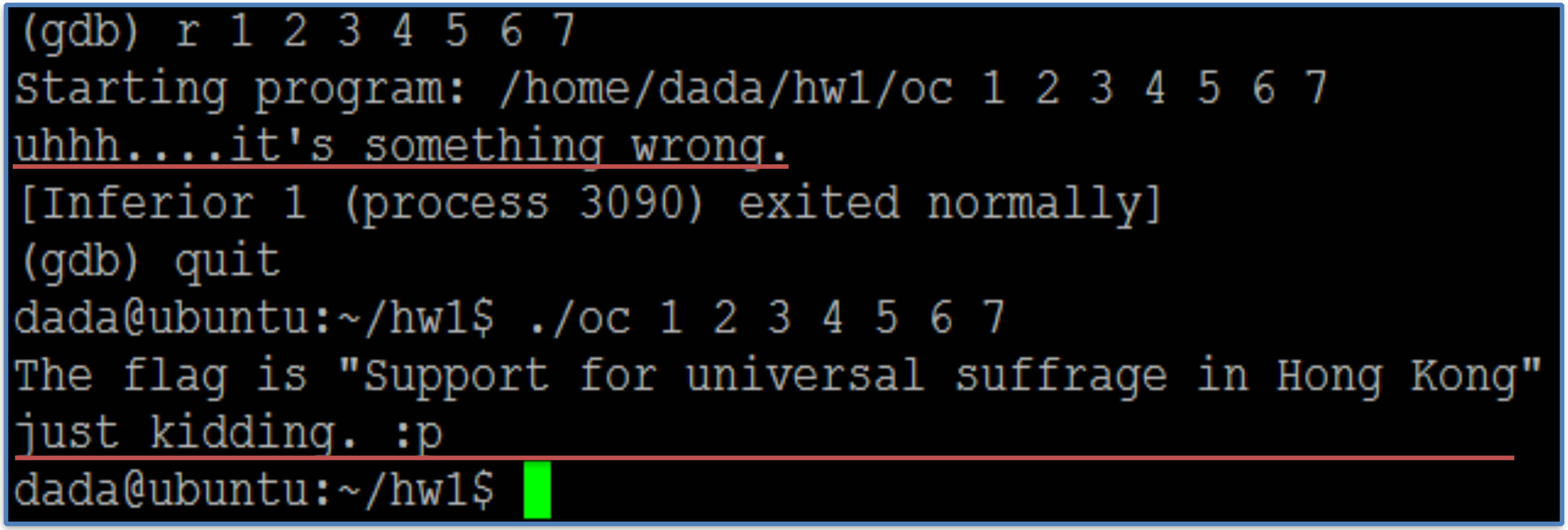
1-3 oc

- Something is happening in Hong Kong....
- nc 140.113.208.235 10002

- btw, oc = Occupy Central

!?

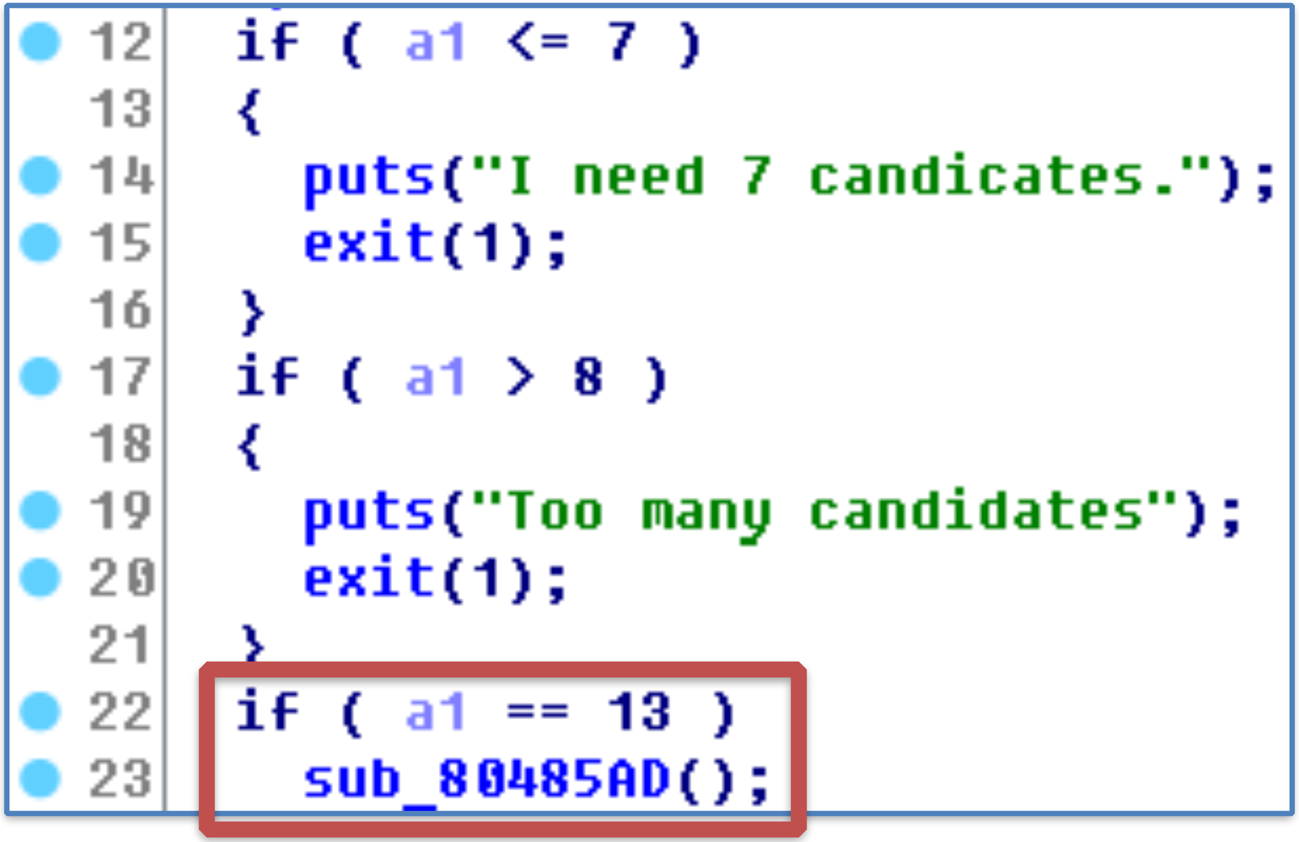
- http://repo.hackerzvoice.net/depot_ouah/linux-anti-debugging.txt



```
(gdb) r 1 2 3 4 5 6 7
Starting program: /home/dada/hw1/oc 1 2 3 4 5 6 7
uhhh....it's something wrong.
[Inferior 1 (process 3090) exited normally]
(gdb) quit
dada@ubuntu:~/hw1$ ./oc 1 2 3 4 5 6 7
The flag is "Support for universal suffrage in Hong Kong"
just kidding. :p
dada@ubuntu:~/hw1$
```

Mission Impossible?

- Using dynamic analysis to find how the program execute.



```
  if ( a1 <= 7 )
  {
    puts("I need 7 candicates.");
    exit(1);
  }
  if ( a1 > 8 )
  {
    puts("Too many candidates");
    exit(1);
  }
  if ( a1 == 13 )
    sub_80485AD();
```

Then…magic~~~~~

Write-up

- Subject: “0056059 Secprog HW1 Writeup”
- Attachment: “0056059_hw1.zip”
  - “0056059_hw1_1.pdf”
  - “0056059_hw1_2.pdf”
  - “0056059_hw1_3.pdf”
- Deadline: before 10/14 23:59