Hanna Rakhsha h_r77
CS 4371 – Gu
Homework 3

1(a) This is a discretionary system. The creator is the user. The owner of the file (object) is the user. The system is Linux. The admin of the system is the root user of the system. The users and the root can decide permission.

(b) This is an originator system. The creator is the software's author. The owner of the software packages (object) is the author. The system is the software repository. The software author is the admin of the system and decides permissions.

(c) This is a mandatory system. The creator is the NSA. The owner of the database (object) is the NSA. The system is the database. The admin of the system is the NSA, who also decides permissions.

2(a) Paul cannot read or write the document. Paul can only read and write a document with (Top Secret{A, C}) classification.

(b) Anna cannot read or write the document. Anna can only read and write a document with (Confidential, {C}) classification.

(c) Jesse can only read the document. Jesse can write to a document with (Top Secret, {C})classification.

(d) Sammie can only read the document. Sammie can write (and read) a document with (Top Secret, {A, C}).

(e) Robin cannot read the document. Robin can read (and write) a document with (Unclassified, {B}) classification.

3.

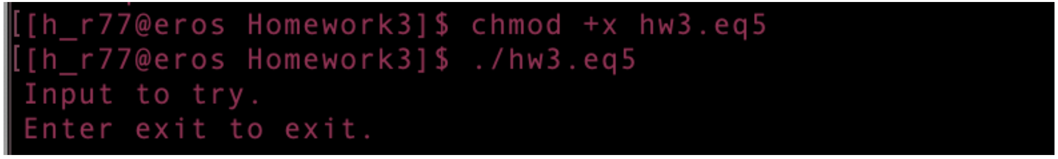
	TS	S	C	UC
TS	rw	--	--	--
S	--	rw	--	--
C	--	--	rw	--
UC	--	--	--	rw

4(a) 249346712

(b) 3989547392

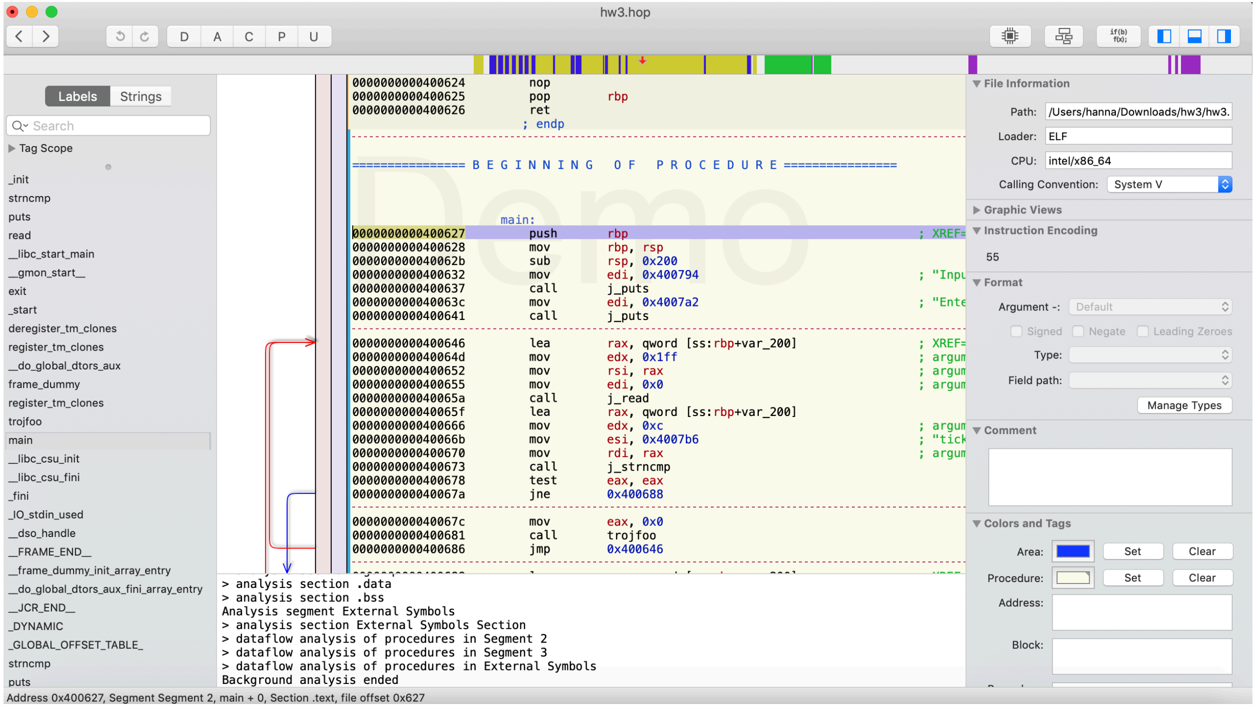
(c) X = 1333/7

5(a)



```
[[h_r77@eros Homework3]$ chmod +x hw3.eq5
[[h_r77@eros Homework3]$ ./hw3.eq5
 Input to try.
 Enter exit to exit.
```

(b)



```
0000000000400624         nop
0000000000400625         pop        rbp
0000000000400626         ret
                        ; endp

================ B E G I N N I N G   O F   P R O C E D U R E ================

                     main:
0000000000400627         push       rbp                                     ; XREF=
0000000000400628         mov        rbp, rsp
000000000040062b         sub        rsp, 0x200
0000000000400632         mov        edi, 0x400794                           ; "Inpu
0000000000400637         call       j_puts
000000000040063c         mov        edi, 0x4007a2                           ; "Ente
0000000000400641         call       j_puts

0000000000400646         lea        rax, qword [ss:rbp+var_200]             ; XREF=
000000000040064d         mov        edx, 0x1ff                              ; argum
0000000000400652         mov        rsi, rax                                ; argum
0000000000400655         mov        edi, 0x0                                ; argum
000000000040065a         call       j_read
000000000040065f         lea        rax, qword [ss:rbp+var_200]
0000000000400666         mov        edx, 0xc                                ; argum
000000000040066b         mov        esi, 0x4007b6                           ; "tick
0000000000400670         mov        rdi, rax                                ; argum
0000000000400673         call       j_strncmp
0000000000400678         test       eax, eax
000000000040067a         jne        0x400688

000000000040067c         mov        eax, 0x0
0000000000400681         call       trojfoo
0000000000400686         jmp        0x400646
```

```
> analysis section .data
> analysis section .bss
Analysis segment External Symbols
> analysis section External Symbols Section
> dataflow analysis of procedures in Segment 2
> dataflow analysis of procedures in Segment 3
> dataflow analysis of procedures in External Symbols
Background analysis ended
```

Path: /Users/hanna/Downloads/hw3/hw3.

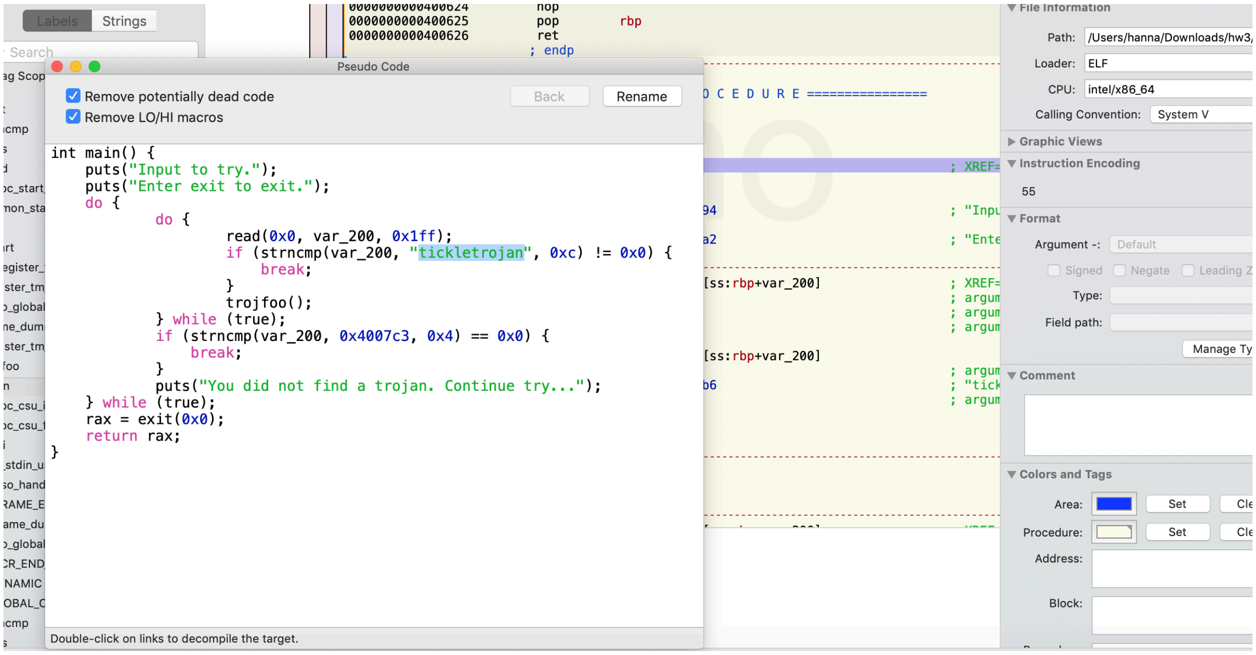
Loader: ELF

CPU: intel/x86_64

Calling Convention: System V

Instruction Encoding: 55

Address 0x400627, Segment Segment 2, main + 0, Section .text, file offset 0x627



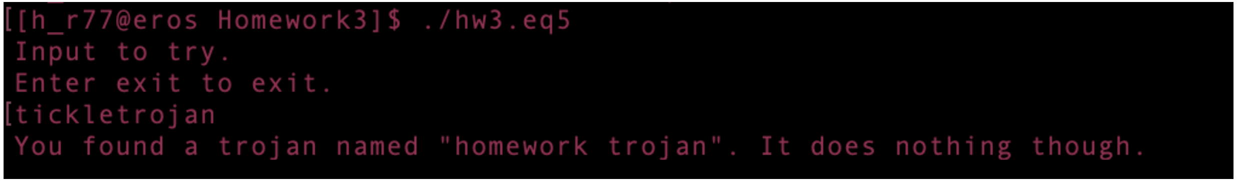
☑ Remove potentially dead code

☑ Remove LO/HI macros

```
int main() {
    puts("Input to try.");
    puts("Enter exit to exit.");
    do {
            do {
                    read(0x0, var_200, 0x1ff);
                    if (strncmp(var_200, "tickletrojan", 0xc) != 0x0) {
                        break;
                    }
                    trojfoo();
            } while (true);
            if (strncmp(var_200, 0x4007c3, 0x4) == 0x0) {
                break;
            }
            puts("You did not find a trojan. Continue try...");
    } while (true);
    rax = exit(0x0);
    return rax;
}
```

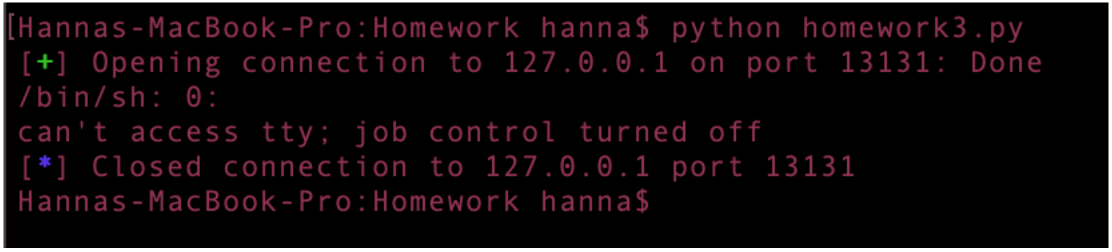
Double-click on links to decompile the target.

(c)



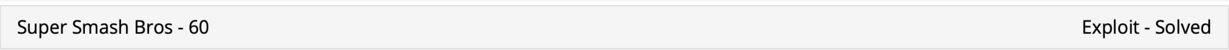
```
[[h_r77@eros Homework3]$ ./hw3.eq5
 Input to try.
 Enter exit to exit.
[tickletrojan
 You found a trojan named "homework trojan". It does nothing though.
```

6(a)

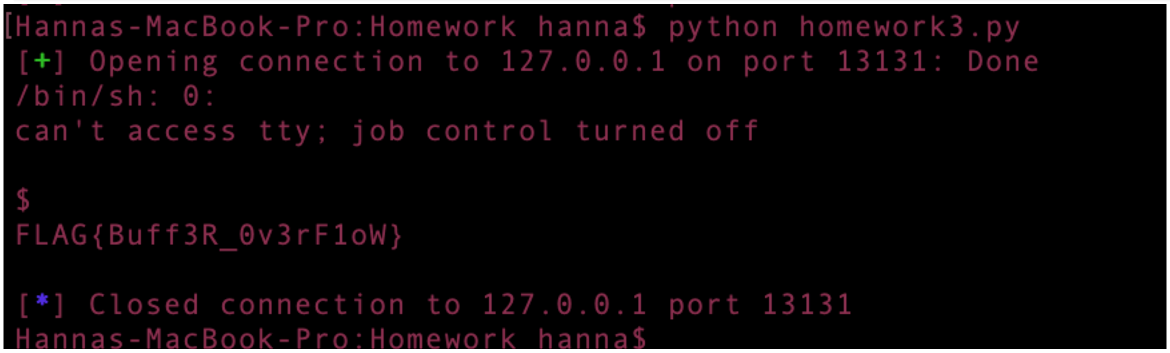


```
[Hannas-MacBook-Pro:Homework hanna$ python homework3.py
 [+] Opening connection to 127.0.0.1 on port 13131: Done
 /bin/sh: 0:
 can't access tty; job control turned off
 [*] Closed connection to 127.0.0.1 port 13131
 Hannas-MacBook-Pro:Homework hanna$
```

(b)

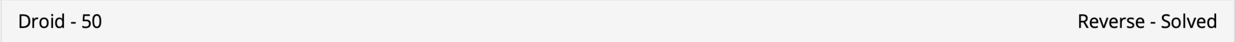


Super Smash Bros - 60 Exploit - Solved

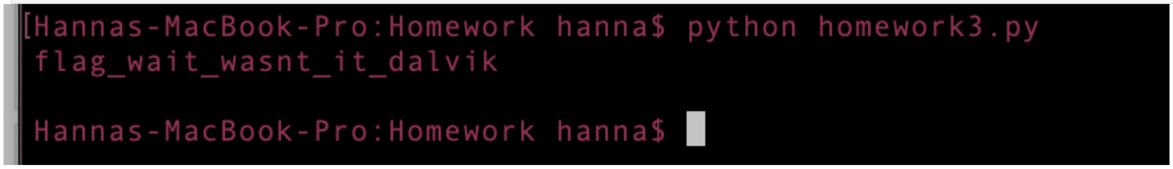


```
[Hannas-MacBook-Pro:Homework hanna$ python homework3.py
 [+] Opening connection to 127.0.0.1 on port 13131: Done
 /bin/sh: 0:
 can't access tty; job control turned off

 $
 FLAG{Buff3R_0v3rF1oW}

 [*] Closed connection to 127.0.0.1 port 13131
 Hannas-MacBook-Pro:Homework hanna$
```

7



Droid - 50 Reverse - Solved



```
[Hannas-MacBook-Pro:Homework hanna$ python homework3.py
 flag_wait_wasnt_it_dalvik

 Hannas-MacBook-Pro:Homework hanna$
```