Format Strings Lab

Modern Binary Exploitation
CSCI 4968 - Spring 2015

Lab 4

- SSH: warzone.rpis.ec 22
- Username: lab4C
- Password: lab4start
- DUE: TUESDAY 1:59pm March 10th
  - Final exploit and descriptions sent to mbespring2015+lab4@gmail.com

```
push    edi
call    sub_314623
test    eax, eax
jz      short loc_31306D
cmp     [ebp+arg_0], ebx
jnz     short loc_313066
mov     eax, [ebp+var_70]
cmp     eax, [ebp+var_84]
jb      short loc_313066
sub     eax, [ebp+var_84]
push    esi
push    esi
push    eax
push    edi
mov     [ebp+arg_0], eax
call    sub_31486A
test    eax, eax
jz      short loc_31306D
push    esi
lea     eax, [ebp+arg_0]
push    eax
mov     esi, 1D0h
push    esi
push    [ebp+arg_4]
push    edi
call    sub_314623
test    eax, eax
jz      short loc_31306D
mov     [ebp+arg_0], esi
short loc_31308F
```

```
loc_313066:                              ; CODE XREF: sub_312FD8
                                         ; sub_312FD8+59
push    0Dh
call    sub_31411B
```

```
loc_31306D:                              ; CODE XREF: sub_312FD8
                                         ; sub_312FD8+49
call    sub_3140F3
test    eax, eax
jg      short loc_31307D
call    sub_3140F3
jmp     short loc_31308C
;----------------------------------------
```

```
loc_31307D:                              ; CODE XREF: sub_312FD8
call    sub_3140F3
and     eax, 0FFFFh
or      eax, 80070000h
```

```
loc_31308C:                              ; CODE XREF: sub_312FD8
mov     [ebp+var_4], eax
```

Lab 4C Hints

- %x.%x.%x.%x.%x…..
- Be mindful of endianness!
- password is 29 chars
- We don't expect you to use memory corruption or GOT/PLT Overwrites for 4C

```
            push    edi
            call    sub_314623
            test    eax, eax
            jz      short loc_31306D
            cmp     [ebp+arg_0], ebx
            jnz     short loc_313066
            mov     eax, [ebp+var_70]
            cmp     eax, [ebp+var_84]
            jb      short loc_313066
            sub     eax, [ebp+var_84]
            push    esi
            push    esi
            push    eax
            push    edi
            mov     [ebp+arg_0], eax
            call    sub_31486A
            test    eax, eax
            jz      short loc_31306D
            push    esi
            lea     eax, [ebp+arg_0]
            push    eax
            mov     esi, 1D0h
            push    esi
            push    [ebp+arg_4]
            push    edi
            call    sub_314623
            test    eax, eax
            jz      short loc_31306D

loc_313066:                              ; CODE XREF: sub_312FD8
                                         ; sub_312FD8+59
            push    0Dh
            call    sub_31411B

loc_31306D:                              ; CODE XREF: sub_312FD8
                                         ; sub_312FD8+49
            call    sub_3140F3
            test    eax, eax
            jg      short loc_31307D
            call    sub_3140F3
            jmp     short loc_31308C

loc_31307D:                              ; CODE XREF: sub_312FD8
            call    sub_3140F3
            and     eax, 0FFFFh
            or      eax, 80070000h

loc_31308C:                              ; CODE XREF: sub_312FD8
            mov     [ebp+var_4], eax
```