Postage example(Week 4)

We need to get the address in main memory pointing to the last of the rax values listed, namely 0xD000FACEEE. The highlighted portion in Figure 1 is explained as follows. Rdx is given the value pointed by rax in main memory. Rax is then given a hex value. This value is compared with rdx. Rdx and rax should now have the same values. i.e 0D000DFACEEE This means that initially [rax] was 0D000DFACEEE.

rax	User input
rdx	D000DFACEEE
rcx	

Main memory

Address	**value**
User input	0xD000DFACEEE

```
var_10= qword ptr -10h
var_8= qword ptr -8

push    rbp
mov     rbp, rsp
sub     rsp, 10h
mov     eax, 0
call    init
mov     edi, offset aCanYouTellMeWh ; "Can you tell me where to mail t
call    _puts
mov     eax, 0
call    get_number
mov     [rbp+var_10], rax
mov     rax, [rbp+var_10]
mov     [rbp+var_8], rax
mov     rax, [rbp+var_8]
mov     rdx, [rax]
mov     rax, 0D000DFACEEEh
cmp     rdx, rax
jnz     short loc_4008F8
```

Figure 1

In order to find the address, I ran the following commands in order. But first go the directory where the executable exists.

- Gdb ./postage
- Run
- Disas main (use this command to find the starting and ending address of your find command. The value that you want should be assigned somewhere in the middle).

```
Dump of assembler code for function main:
   0x0000000000400895 <+0>:     push   %rbp
   0x0000000000400896 <+1>:     mov    %rsp,%rbp
   0x0000000000400899 <+4>:     sub    $0x10,%rsp
   0x000000000040089d <+8>:     mov    $0x0,%eax
   0x00000000004008a2 <+13>:    callq  0x40080d <init>
   0x00000000004008a7 <+18>:    mov    $0x400aa8,%edi
   0x00000000004008ac <+23>:    callq  0x400600 <puts@plt>
   0x00000000004008b1 <+28>:    mov    $0x0,%eax
   0x00000000004008b6 <+33>:    callq  0x400831 <get_number>
   0x00000000004008bb <+38>:    mov    %rax,-0x10(%rbp)
   0x00000000004008bf <+42>:    mov    -0x10(%rbp),%rax
   0x00000000004008c3 <+46>:    mov    %rax,-0x8(%rbp)
   0x00000000004008c7 <+50>:    mov    -0x8(%rbp),%rax
=> 0x00000000004008cb <+54>:    mov    (%rax),%rdx
   0x00000000004008ce <+57>:    movabs $0xd000dfaceee,%rax
   0x00000000004008d8 <+67>:    cmp    %rax,%rdx
   0x00000000004008db <+70>:    jne    0x4008f8 <main+99>
   0x00000000004008dd <+72>:    mov    $0x400ad8,%edi
   0x00000000004008e2 <+77>:    callq  0x400600 <puts@plt>
   0x00000000004008e7 <+82>:    mov    $0x0,%eax
   0x00000000004008ec <+87>:    callq  0x40077d <print_flag>
   0x00000000004008f1 <+92>:    mov    $0x0,%eax
```

- Find 0x400895, 0x4008f1, 0xd000dfaceee
  (find start_addr, end_addr, value)

We get the following output. This is the address we are looking for.

```
---Type <return> to continue, or q <return> to quit---Quit
(gdb) find 0x0000000000400895, 0x00000000004008f1, 0xd000dfaceee
0x4008d0 <main+59>
1 pattern found.
```

Convert to decimal and get your flag.

```
adeenayub@ubuntu:~/Desktop$ nc offsec-chalbroker.osiris.cyber.nyu.edu 1247
Please input your NetID (something like abc123): aa6243
hello, aa6243. Please wait a moment...
Can you tell me where to mail this postage?
4196560
Got it! That's the right number!
Here's your flag, friend: flag{i_hope_ur_ready_4_some_pwning_in_a_few_weeks_5b22
a8af4524}
```

Thank Allah over and over again.