Verkefni 1

sbb51@hi.is

October 2022

Phase 1

Bytjaði á að setja inn skipunina **disas phase_1** til að sjá assembly kóðann fyrir phase 1.
Sjáum að með skipuninni **sub $0x8,%rsp** erum við að taka frá pláss fyrir %rsp. Í næstu línu, **lea 0x1b3a(%rip),%rsi**, er verið að hliðra því sme er inní %rip um 0x1b3a og setja það í %rsi. Sjáum síðan að það er komment hjá þessarri línu. Nota skipunina **p (char*) 0x555555557150** til að sjá hvað er þar inní. Og fæ út strenginn "Do not mess with me, I am one crazy mofo.".

```
Dump of assembler code for function phase_1:
   0x0000555555555607 <+0>:     endbr64
   0x000055555555560b <+4>:     sub    $0x8,%rsp
   0x000055555555560f <+8>:     lea    0x1b3a(%rip),%rsi        # 0x555555557150
   0x0000555555555616 <+15>:    call   0x555555555b8f <strings_not_equal>
   0x000055555555561b <+20>:    test   %eax,%eax
   0x000055555555561d <+22>:    jne    0x555555555624 <phase_1+29>
   0x000055555555561f <+24>:    add    $0x8,%rsp
   0x0000555555555623 <+28>:    ret
   0x0000555555555624 <+29>:    call   0x555555555ca3 <explode_bomb>
   0x0000555555555629 <+34>:    jmp    0x55555555561f <phase_1+24>
End of assembler dump.
(gdb) p (char*) 0x555555557150
$27 = 0x555555557150 "Do not mess with me, I am one crazy mofo."
(gdb) r
```

Keyri forritið aftur og nota strenginn sem inntak og fæ **"Phase 1 defused. How about the next one?**

```
Starting program: /home/mint/Downloads/bombs/bomb159/bomb
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Do not mess with me, I am one crazy mofo.
Phase 1 defused. How about the next one?
```

Phase 2

Bytjaði á að setja inn skipunina **disas phase_2** til að sjá assembly kóðann fyrir phase 2.

Byrjum á að skoða línu +29. Kíkjum á hvað er inní þeirri línu og assembly kóða. Skoðum hvað er í kommentinu og fáum að lykilorðið okkar er á forminu **"%d %d %d %d %d %d"**.

Skoðum svo hvað er að gerast fyrir neðan línu +29.

```
+34   mov   $0x0,(%rsp)
+38   jne   $0x5555555565d <phase_2+50>
# Ef %rsp er ekki 0, þá hoppum við í línu 50 og springum.
+40   mov   %rsp,%rbp
# Færum %rsp í %rbp
+43   mov   $0x1,%ebx
# Frumstillit %ebx sem 1
+48   jmp   $0x55555555670 <phase_2+69>
+50   call  $0x55555555ca3 <explode_bomb>
+55   jmp   $0x55555555653 <phase_2+40>
+57   add   $0x1,%ebx
# Bætum einum við %ebx
+60   add   $0x4,%rbp
# Losum okkur við fyrsta gildi í %rbp og setjum annað gildið í %rbp sem fyrsta gildið.
+64   cmp   $0x6,%ebx
# Tékkum hvort %ebx sé orðið 6
+67   je    $0x55555555681 <phase_2+86>
+69   mov   %ebx,%eax
# Setjum %ebx í %eax
+71   add   0x0(%rbp),%eax
# Bætum fyrsta gildi %rbp við %eax
+74   cmp   %eax, 0x4(%rbp)
# Skoðum hvort annað gildið í %eax = %eax + %rbp[0] (fyrsta gildi %rbp)
+77   je    $0x55555555664 <phase_2+57>
+79   call  $0x55555555ca3 <explode_bomb>
+84   jmp   $0x55555555664 <phase_2+57>
+86   mov   0x18(%rsp),%rax
+91   sub   %fs:0x28,%rax
```

Setjum þessa útreikninga okkar upp í töflu.

%rbp[0]	%eax	%rbp[1]
0	1	0+1=1
1	2	1+2=3
3	3	3+3=6
6	4	6+4=10
10	5	10+5=15
15	6	15+6=21

Fáum þá út að lykilorðið okkar er **0 1 3 6 10 15 21**

```
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Do not mess with me, I am one crazy mofo.
Phase 1 defused. How about the next one?
0 1 3 6 10 15 21
That's number 2.  Keep going!
```