Beefest1 (penyisihan): Hexamethics

Deskripsi: Apakah anda suka menghitung? (Jawaban dalam hexadecimal)

Writeup:

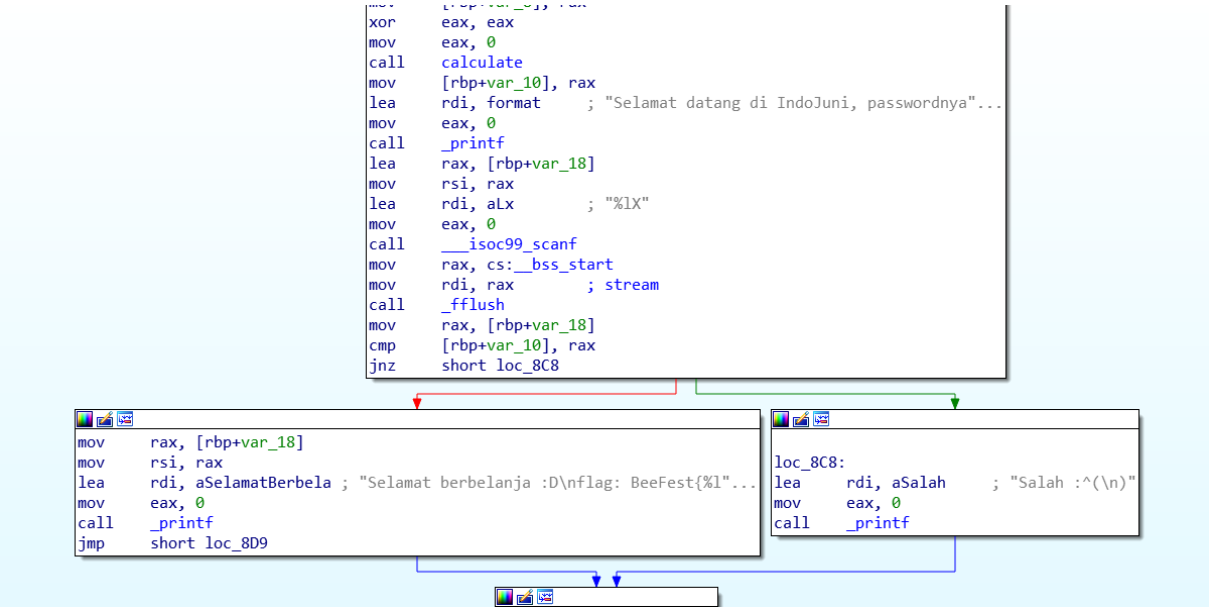
Pertama kita coba lihat dengan menggunakan *file*:

```
nacl@ubuntu:~$ file beefest1
beefest1: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-
x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=fb5244d59fd824ea438fc1eddf0e34de1897eb1d, not stripped
```

File merupakan ELF. Saat dijalankan ia meminta sebuah password:

```
nacl@ubuntu:~$ ./beefest1
Selamat datang di IndoJuni, passwordnya apa?:
```

Dengan menggunakan IDA, kita bisa melihat bahwa program melakukan function calculate, lalu membandingkan hasil dari function tersebut dan jika inputnya benar, maka flag kita merupakan password tersebut.



Selanjutnya kita melihat lebih dekat function calculate:

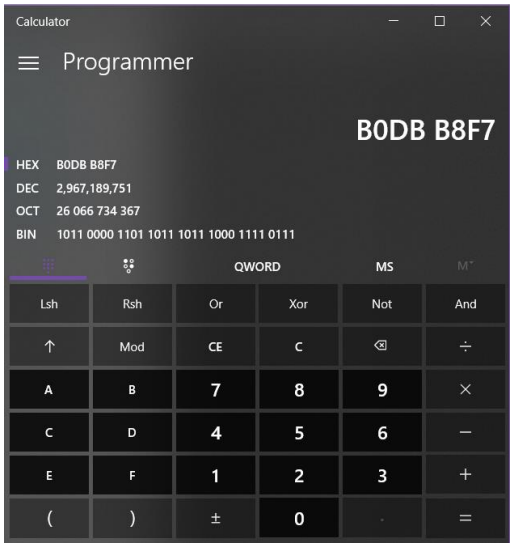
```
public calculate
calculate proc near

var_20= qword ptr -20h
var_18= qword ptr -18h
var_10= qword ptr -10h
var_8= qword ptr -8

; __unwind {
push    rbp
mov     rbp, rsp
mov     eax, 0BEEFE518h
mov     [rbp+var_20], rax
mov     eax, 0DEADF00Dh
mov     [rbp+var_18], rax
mov     [rbp+var_10], 10C4115Eh
mov     [rbp+var_8], 0FF1C1A1h
mov     rax, [rbp+var_20]
imul    rax, [rbp+var_8]
mov     [rbp+var_20], rax
mov     rax, [rbp+var_20]
cqo
idiv    [rbp+var_10]
mov     [rbp+var_20], rax
mov     rax, [rbp+var_18]
cqo
idiv    [rbp+var_10]
mov     [rbp+var_18], rdx
mov     rax, [rbp+var_18]
sub     [rbp+var_20], rax
mov     rax, [rbp+var_20]
pop     rbp
retn
; } // starts at 7EA
calculate endp
```

Terdapat 4 variabel yang berisi bilangan hexadecimal: 0xBEEFE518, 0xDEADF00D, 0x10C4115E, dan 0x0FF1C1A1. Pertama, program mengalikan 0xBEEFE518 dengan 0x0FF1C1A1 lalu melakukan pembagian antara hasilnya dengan 0x10C4115E. Selanjutnya 0xDEADF00D dimodulo dengan 0x10C4115E. Hasil dari pembagian lalu dikurangkan dengan hasil dari modulo.

Kita dapat melakukan langkah-langkah tersebut dengan menggunakan programmer calculator:



Lalu untuk mengecek jawabannya, kita memasukkan bilangan hexadecimal yang kita dapat dalam program:

```
nacl@ubuntu:~$ ./beefest1
Selamat datang di IndoJuni, passwordnya apa?: b0dbb8f7
Selamat berbelanja :D
flag: BeeFest{B0DBB8F7}
```

Flag: BeeFest{B0DBB8F7}