Bit

Reversing - 100 points

# Soal

|  |
| --- |
| Service: 128.199.232.109  Port: 17846  \*Test Koneksi: #nc 128.199.232.109 17846  [bit](https://ctf.idsecconf.org/download?file_key=b78b8f66c9f00dd1bace2c159f65d3cc571a4a24666088a0a83fe5ac82d3c628&team_key=2a3d00950bcec988c6f9a00242687028ade2e180c4a337d64a8761b253b2df59) - a92562f03e45993bc45412a2f73a4dfa |

# Solusi

Diberikan file ELF 64-bit, stripped, jika di-decompile dengan IDA didapatkan source berikut (nama fungsi dan variabel lokal sudah saya rename sendiri secara manual):

|  |
| --- |
| int **\_\_cdecl** main(int argc, **const** char \*\*argv, **const** char \*\*envp) {  unsigned int t; *// eax@1*  signed **\_\_int64** r; *// rbx@1*  int result; *// eax@5*  signed int saldo; *// [sp+14h] [bp-2Ch]@7*  **\_\_int64** tebakanku; *// [sp+18h] [bp-28h]@3*  **\_\_int64** taruhanku; *// [sp+20h] [bp-20h]@3*  **\_\_int64** jawaban; *// [sp+28h] [bp-18h]@1*   t = time(0LL);  srand(t);  r = (signed **\_\_int64**)rand() << 32;  jawaban = r | rand();  **if** ( jawaban > 13 )  jawaban += 14LL;  puts("++++ BITCOIN KASINO ++++!");  fflush(0LL);  sleep(3u);  puts("Eddy Tongsis Masuk Dengan BTC90000...**\n**Gayus Timbunan Masuk Dengan BTC100000...**\n**Dan Kamu Dengan Saldo 100BTC.");  fflush(0LL);  sleep(3u);  puts("Tebak Angka Yang Akan Naik - (Diatas 13)");  fflush(0LL);  sleep(3u);  printf("Masukkan Angka Keberuntunganmu: ", argv);  fflush(0LL);  \_\_isoc99\_scanf(0x400D59LL, &tebakanku);  printf("Nilai Taruhanmu (BTC): ", &tebakanku);  fflush(0LL);  \_\_isoc99\_scanf(0x400D76LL, &taruhanku);  **if** ( (signed int)taruhanku <= 100 && taruhanku >= 0 )  {  progress(8);  puts("Hasilnya adalah...");  fflush(0LL);  sleep(3u);  **if** ( tebakanku == jawaban )  {  puts("Ajaib! Selamat Atas Tebakannya.");  saldo = taruhanku + 100;  }  **else**  {  saldo = 100 - taruhanku;  printf("Bukan %lld. Yang Benar Adalah %lld.**\n**", tebakanku, jawaban);  }  fflush(0LL);  sleep(3u);  **if** ( saldo > 100000 )  {  progress(5);  printf("Anda Memenangkan %dBTC**\n**Selain Itu Akan Kami Berikan Bonus Berupa**\n**", (unsigned int)saldo);  sleep(5u);  giveflag();  }  **else**  {  printf("Kamu Kalah! (%dBTC) **\n**", (unsigned int)saldo);  }  result = 0;  }  **else**  {  puts("Taruhan ditolak, saldo kamu hanya 100BTC");  result = 0;  }  **return** result; } |

Jadi intinya kita disuruh menebak suatu angka random, dan juga memberikan nilai taruhan. Jika tebakan kita benar, uang kita akan ditambah dengan taruhan, dan jika salah, akan dikurangi sebesar taruhan. Jika di akhir uang kita melebihi 100000, kita menang dan dapat flag.

Sekilas tidak mungkin, karena taruhan kita dibatasi dari 0 sampai 100. Kalaupun tebakan benar, uang kita hanya bertambah 100 menjadi 200, dan program juga tidak looping sehingga tidak mungkin mencapai nilai 100000.

Mungkin kita bisa mencurangi dengan memasukkan taruhan bernilai minus, dan memasukkan angka asal saja, sehingga kode ini:

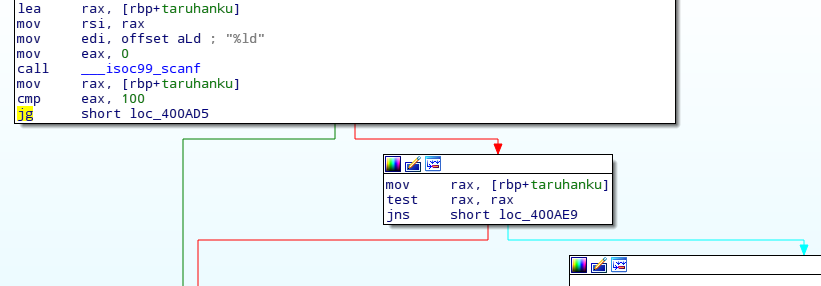
|  |
| --- |
| saldo = 100 - taruhanku;  printf("Bukan %lld. Yang Benar Adalah %lld.**\n**", tebakanku, jawaban); |

Akan membuat saldo kita menjadi jauh lebih besar (100 dikurangi -100000 akan menjadi 100100 misalnya).

Tapi sayangnya ada pengecekan berikut:

|  |
| --- |
| **if** ( (signed int)taruhanku <= 100 && taruhanku >= 0 ) |

Yang kalau di assembly adalah pengecekan dengan JG (cek <= 100) dan JNS (cek >= 0)



Salah satu yang terpikirkan adalah menggunakan nilai maksimum integer 32-bit, yaitu 4294967295, atau (11111111111111111111111111111111) dalam biner.

Pengecekan pertama, karena menggunakan “cmp eax, 100” dan test yang signed (JG), maka nilai pada register EAX (11111111111111111111111111111111) ini akan dianggap -1, sehingga lolos pengecekan <= 100.

Pengecekan kedua, adalah dengan “test rax, rax” dan JNS. Nilai taruhan kita tadi kalau disimpan di register RAX akan bernilai dalam biner:

(0000000000000000000000000000000011111111111111111111111111111111)

Jika dilakukan “test rax, rax”, bilangan tersebut dianggap bilangan positif 64-bit (karena bit depannya 0), sehingga akan lolos dari JNS dan cek >= 0.

Jika dimasukkan angka tersebut ke program (dengan angka tebakan asal saja supaya salah):

|  |
| --- |
| $ ./bit  ++++ BITCOIN KASINO ++++!  Eddy Tongsis Masuk Dengan BTC90000...  Gayus Timbunan Masuk Dengan BTC100000...  Dan Kamu Dengan Saldo 100BTC.  Tebak Angka Yang Akan Naik - (Diatas 13)  Masukkan Angka Keberuntunganmu: **0**  Nilai Taruhanmu (BTC): **4294967295**  ========= Hasilnya adalah...  Bukan 0. Yang Benar Adalah 5381429336863665181.  Kamu Kalah! (**101**BTC) |

Lihat bahwa kita kalah tapi saldo malah bertambah, artinya kita berhasil memasukkan angka -1. Dari sini sudah jelas, kita akan memasukkan angka (4294967295 - 100000 = 4294867295) supaya saldo bertambah 100001 meski kita kalah.

Langsung saja coba ke remote server soal:

|  |
| --- |
| $ nc 128.199.232.109 17846  ++++ BITCOIN KASINO ++++!  Eddy Tongsis Masuk Dengan BTC90000...  Gayus Timbunan Masuk Dengan BTC100000...  Dan Kamu Dengan Saldo 100BTC.  Tebak Angka Yang Akan Naik - (Diatas 13)  Masukkan Angka Keberuntunganmu: **0**  Nilai Taruhanmu (BTC): **4294867295**  ========= Hasilnya adalah...  Bukan 0. Yang Benar Adalah 1420821384614299086.  ====== Anda Memenangkan **100101**BTC  Selain Itu Akan Kami Berikan Bonus Berupa  flag{Integer\_H4ri\_Ini} |

Didapatkan flag:

**flag{Integer\_H4ri\_Ini}**