

# gc's reverse1

## no source provided

This binary was sent to me by a friend. He was also sent another person and the source is unknown. In this same folder you can download the binary.

**Date: 03/oct/2019**

To solve this crack I used my **Kali Linux VM** and the **edb debugger** that were more than enough to solve it.

- After locating the main function we can see where the text string is loaded that asks us to enter the text and two specific call calls, one that asks for the text string and another that checks the password we have entered.

```

000055a1:b68c8273  c3          ret
000055a1:b68c8274  55          push rbp
000055a1:b68c8275  48 89 e5    mov rbp, rsp
000055a1:b68c8278  48 83 ec 30 sub rsp, 0x30
000055a1:b68c827c  89 7d dc    mov [rbp-0x24], edi
000055a1:b68c827f  48 8d 05 b8 0d 00 00 lea rax, [rel 0x55a1b68c903e]
000055a1:b68c8286  48 89 45 f8 mov [rbp-8], rax
000055a1:b68c828a  48 8d 3d ba 0d 00 00 lea rdi, [rel 0x55a1b68c904b]
000055a1:b68c8291  b8 00 00 00 00 mov eax, 0
000055a1:b68c8296  e8 b5 fd ff ff call 0x55a1b68c8050
000055a1:b68c829b  48 8d 45 eb lea rax, [rbp-0x15]
000055a1:b68c829f  48 89 c6    mov rsi, rax
000055a1:b68c82a2  48 8d 3d bc 0d 00 00 lea rdi, [rel 0x55a1b68c9065]
000055a1:b68c82a9  b8 00 00 00 00 mov eax, 0
000055a1:b68c82ae  e8 cd fd ff ff call enter_password
000055a1:b68c82b3  48 8d 45 eb lea rax, [rbp-0x15]
000055a1:b68c82b7  48 89 c7    mov rdi, rax
000055a1:b68c82ba  e8 c6 fe ff ff call check_password
000055a1:b68c82bf  b8 00 00 00 00 mov eax, 0
000055a1:b68c82c4  c9          leave
000055a1:b68c82c5  c3          ret
000055a1:b68c82c6  66 2e 0f 1f 84 00 00 ... nop word cs:[rax+rax]
000055a1:b68c82d0  41 57      push r15
000055a1:b68c82d2  49 89 d7    mov r15, rdx

```

qword ptr [rip + 0xd8a] = [0x000055a1b68c904b] = 0x63617243205d2b5b  
rdi = 0x0000000000000001

- We are going to focus on the second call, because the others are not relevant.
- We enter a text that we can identify well and locate ourselves to know where it is stored in memory. This will help us later to see where the comparison is made (if necessary).

Data Dump

Address	Disassembly	Comment
0x000055a1b68c8000-0x000055a1b68c9000	0x00007ffde395a000-0x00007ffde397b000	[+] Crackea el programa: my_password

edb output

```

[+] Crackea el programa: my_password

```

- In the subroutine we have called "check\_password" we can see how at the beginning of this a movement of fixed values is made to memory positions. Later we can verify how these values correspond to the representation in ASCII of a hexadecimal string.

```

000055a1:b68c818d 48 89 7d a8      mov [rbp-0x58], rdi
000055a1:b68c8191 48 8d 05 6c 0e 00 00 lea rax, [rel 0x55a1b68c9004]
000055a1:b68c8198 48 89 45 f0      mov [rbp-0x10], rax
000055a1:b68c819c 48 b8 37 34 36 66 36 3... movabs rax, 0x6636343666363437
000055a1:b68c81a6 48 ba 35 66 36 65 36 6... movabs rdx, 0x3237663665366635
000055a1:b68c81b0 48 89 45 c0      mov [rbp-0x40], rax
000055a1:b68c81b4 48 89 55 c8      mov [rbp-0x38], rdx
000055a1:b68c81b8 c7 45 d0 36 64 36 31 mov dword [rbp-0x30], 0x31366436
000055a1:b68c81bf 66 c7 45 d4 36 63   mov word [rbp-0x2c], 0x6336
000055a1:b68c81c5 c6 45 d6 00        mov byte [rbp-0x2a], 0

```

word ptr [rbp - 0x30] = [0x00007ffde3978de0] = 0x00000000

Hex Dump

Address	Hex	ASCII
00000000	0x00007ffde395a000-0x00007ffde397b000	0x00007ffde395a000-0x00007ffde397b000
00000000	00 00 00 00 00 00 00 00	
00000001	00 00 00 00 00 00 00 00	
00000002	00 00 00 00 00 00 00 00	
00000003	00 00 00 00 00 00 00 00	
00000004	00 00 00 00 00 00 00 00	
00000005	00 00 00 00 00 00 00 00	
00000006	00 00 00 00 00 00 00 00	
00000007	00 00 00 00 00 00 00 00	
00000008	00 00 00 00 00 00 00 00	
00000009	00 00 00 00 00 00 00 00	
0000000a	00 00 00 00 00 00 00 00	
0000000b	00 00 00 00 00 00 00 00	
0000000c	00 00 00 00 00 00 00 00	
0000000d	00 00 00 00 00 00 00 00	
0000000e	00 00 00 00 00 00 00 00	
0000000f	00 00 00 00 00 00 00 00	
00000010	00 00 00 00 00 00 00 00	
00000011	00 00 00 00 00 00 00 00	
00000012	00 00 00 00 00 00 00 00	
00000013	00 00 00 00 00 00 00 00	
00000014	00 00 00 00 00 00 00 00	
00000015	00 00 00 00 00 00 00 00	
00000016	00 00 00 00 00 00 00 00	
00000017	00 00 00 00 00 00 00 00	
00000018	00 00 00 00 00 00 00 00	
00000019	00 00 00 00 00 00 00 00	
0000001a	00 00 00 00 00 00 00 00	
0000001b	00 00 00 00 00 00 00 00	
0000001c	00 00 00 00 00 00 00 00	
0000001d	00 00 00 00 00 00 00 00	
0000001e	00 00 00 00 00 00 00 00	
0000001f	00 00 00 00 00 00 00 00	
00000020	00 00 00 00 00 00 00 00	
00000021	00 00 00 00 00 00 00 00	
00000022	00 00 00 00 00 00 00 00	
00000023	00 00 00 00 00 00 00 00	
00000024	00 00 00 00 00 00 00 00	
00000025	00 00 00 00 00 00 00 00	
00000026	00 00 00 00 00 00 00 00	
00000027	00 00 00 00 00 00 00 00	
00000028	00 00 00 00 00 00 00 00	
00000029	00 00 00 00 00 00 00 00	
0000002a	00 00 00 00 00 00 00 00	
0000002b	00 00 00 00 00 00 00 00	
0000002c	00 00 00 00 00 00 00 00	
0000002d	00 00 00 00 00 00 00 00	
0000002e	00 00 00 00 00 00 00 00	
0000002f	00 00 00 00 00 00 00 00	
00000030	00 00 00 00 00 00 00 00	
00000031	00 00 00 00 00 00 00 00	
00000032	00 00 00 00 00 00 00 00	
00000033	00 00 00 00 00 00 00 00	
00000034	00 00 00 00 00 00 00 00	
00000035	00 00 00 00 00 00 00 00	
00000036	00 00 00 00 00 00 00 00	
00000037	00 00 00 00 00 00 00 00	
00000038	00 00 00 00 00 00 00 00	
00000039	00 00 00 00 00 00 00 00	
0000003a	00 00 00 00 00 00 00 00	
0000003b	00 00 00 00 00 00 00 00	
0000003c	00 00 00 00 00 00 00 00	
0000003d	00 00 00 00 00 00 00 00	
0000003e	00 00 00 00 00 00 00 00	
0000003f	00 00 00 00 00 00 00 00	
00000040	00 00 00 00 00 00 00 00	
00000041	00 00 00 00 00 00 00 00	
00000042	00 00 00 00 00 00 00 00	
00000043	00 00 00 00 00 00 00 00	
00000044	00 00 00 00 00 00 00 00	
00000045	00 00 00 00 00 00 00 00	
00000046	00 00 00 00 00 00 00 00	
00000047	00 00 00 00 00 00 00 00	
00000048	00 00 00 00 00 00 00 00	
00000049	00 00 00 00 00 00 00 00	
0000004a	00 00 00 00 00 00 00 00	
0000004b	00 00 00 00 00 00 00 00	
0000004c	00 00 00 00 00 00 00 00	
0000004d	00 00 00 00 00 00 00 00	
0000004e	00 00 00 00 00 00 00 00	
0000004f	00 00 00 00 00 00 00 00	
00000050	00 00 00 00 00 00 00 00	
00000051	00 00 00 00 00 00 00 00	
00000052	00 00 00 00 00 00 00 00	
00000053	00 00 00 00 00 00 00 00	
00000054	00 00 00 00 00 00 00 00	
00000055	00 00 00 00 00 00 00 00	
00000056	00 00 00 00 00 00 00 00	
00000057	00 00 00 00 00 00 00 00	
00000058	00 00 00 00 00 00 00 00	
00000059	00 00 00 00 00 00 00 00	
0000005a	00 00 00 00 00 00 00 00	
0000005b	00 00 00 00 00 00 00 00	
0000005c	00 00 00 00 00 00 00 00	
0000005d	00 00 00 00 00 00 00 00	
0000005e	00 00 00 00 00 00 00 00	
0000005f	00 00 00 00 00 00 00 00	
00000060	00 00 00 00 00 00 00 00	
00000061	00 00 00 00 00 00 00 00	
00000062	00 00 00 00 00 00 00 00	
00000063	00 00 00 00 00 00 00 00	
00000064	00 00 00 00 00 00 00 00	
00000065	00 00 00 00 00 00 00 00	
00000066	00 00 00 00 00 00 00 00	
00000067	00 00 00 00 00 00 00 00	
00000068	00 00 00 00 00 00 00 00	
00000069	00 00 00 00 00 00 00 00	
0000006a	00 00 00 00 00 00 00 00	
0000006b	00 00 00 00 00 00 00 00	
0000006c	00 00 00 00 00 00 00 00	
0000006d	00 00 00 00 00 00 00 00	
0000006e	00 00 00 00 00 00 00 00	
0000006f	00 00 00 00 00 00 00 00	
00000070	00 00 00 00 00 00 00 00	
00000071	00 00 00 00 00 00 00 00	
00000072	00 00 00 00 00 00 00 00	
00000073	00 00 00 00 00 00 00 00	
00000074	00 00 00 00 00 00 00 00	
00000075	00 00 00 00 00 00 00 00	
00000076	00 00 00 00 00 00 00 00	
00000077	00 00 00 00 00 00 00 00	
00000078	00 00 00 00 00 00 00 00	
00000079	00 00 00 00 00 00 00 00	
0000007a	00 00 00 00 00 00 00 00	
0000007b	00 00 00 00 00 00 00 00	
0000007c	00 00 00 00 00 00 00 00	
0000007d	00 00 00 00 00 00 00 00	
0000007e	00 00 00 00 00 00 00 00	
0000007f	00 00 00 00 00 00 00 00	
00000080	00 00 00 00 00 00 00 00	
00000081	00 00 00 00 00 00 00 00	
00000082	00 00 00 00 00 00 00 00	
00000083	00 00 00 00 00 00 00 00	
00000084	00 00 00 00 00 00 00 00	
00000085	00 00 00 00 00 00 00 00	
00000086	00 00 00 00 00 00 00 00	
00000087	00 00 00 00 00 00 00 00	
00000088	00 00 00 00 00 00 00 00	
00000089	00 00 00 00 00 00 00 00	
0000008a	00 00 00 00 00 00 00 00	
0000008b	00 00 00 00 00 00 00 00	
0000008c	00 00 00 00 00 00 00 00	
0000008d	00 00 00 00 00 00 00 00	
0000008e	00 00 00 00 00 00 00 00	
0000008f	00 00 00 00 00 00 00 00	
00000090	00 00 00 00 00 00 00 00	
00000091	00 00 00 00 00 00 00 00	
00000092	00 00 00 00 00 00 00 00	
00000093	00 00 00 00 00 00 00 00	
00000094	00 00 00 00 00 00 00 00	
00000095	00 00 00 00 00 00 00 00	
00000096	00 00 00 00 00 00 00 00	
00000097	00 00 00 00 00 00 00 00	
00000098	00 00 00 00 00 00 00 00	
00000099	00 00 00 00 00 00 00 00	
0000009a	00 00 00 00 00 00 00 00	
0000009b	00 00 00 00 00 00 00 00	
0000009c	00 00 00 00 00 00 00 00	
0000009d	00 00 00 00 00 00 00 00	
0000009e	00 00 00 00 00 00 00 00	
0000009f	00 00 00 00 00 00 00 00	
000000a0	00 00 00 00 00 00 00 00	
000000a1	00 00 00 00 00 00 00 00	
000000a2	00 00 00 00 00 00 00 00	
000000a3	00 00 00 00 00 00 00 00	
000000a4	00 00 00 00 00 00 00 00	
000000a5	00 00 00 00 00 00 00 00	
000000a6	00 00 00 00 00 00 00 00	
000000a7	00 00 00 00 00 00 00 00	
000000a8	00 00 00 00 00 00 00 00	
000000a9	00 00 00 00 00 00 00 00	
000000aa	00 00 00 00 00 00 00 00	
000000ab	00 00 00 00 00 00 00 00	
000000ac	00 00 00 00 00 00 00 00	
000000ad	00 00 00 00 00 00 00 00	
000000ae	00 00 00 00 00 00 00 00	
000000af	00 00 00 00 00 00 00 00	
000000b0	00 00 00 00 00 00 00 00	
000000b1	00 00 00 00 00 00 00 00	
000000b2	00 00 00 00 00 00 00 00	
000000b3	00 00 00 00 00 00 00 00	
000000b4	00 00 00 00 00 00 00 00	
000000b5	00 00 00 00 00 00 00 00	
000000b6	00 00 00 00 00 00 00 00	
000000b7	00 00 00 00 00 00 00 00	
000000b8	00 00 00 00 00 00 00 00	
000000b9	00 00 00 00 00 00 00 00	
000000ba	00 00 00 00 00 00 00 00	
000000bb	00 00 00 00 00 00 00 00	
000000bc	00 00 00 00 00 00 00 00	
000000bd	00 00 00 00 00 00 00 00	
000000be	00 00 00 00 00 00 00 00	
000000bf	00 00 00 00 00 00 00 00	
000000c0	00 00 00 00 00 00 00 00	
000000c1	00 00 00 00 00 00 00 00	
000000c2	00 00 00 00 00 00 00 00	
000000c3	00 00 00 00 00 00 00 00	
000000c4	00 00 00 00 00 00 00 00	
000000c5	00 00 00 00 00 00 00 00	
000000c6	00 00 00 00 00 00 00 00	
000000c7	00 00 00 00 00 00 00 00	
000000c8	00 00 00 00 00 00 00 00	
000000c9	00 00 00 00 00 00 00 00	
000000ca	00 00 00 00 00 00 00 00	
000000cb	00 00 00 00 00 00 00 00	
000000cc	00 00 00 00 00 00 00 00	
000000cd	00 00 00 00 00 00 00 00	
000000ce	00 00 00 00 00 00 00 00	
000000cf	00 00 00 00 00 00 00 00	
000000d0	00 00 00 00 00	

Data Dump										Stack									
00000000-0x00000000-0x00000000-0x00000000										00000000-0x00000000-0x00000000-0x00000000									
00007ffd:e3978dc0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00007ffd:e3978dd0	37	34	36	66	36	34	36	66	35	66	36	65	36	66	37	32	74	6f	64
00007ffd:e3978de0	36	64	36	31	36	63	00	00	00	00	00	00	00	00	74	6f	64	6d	61
00007ffd:e3978df0	6f	5f	6e	6f	72	6d	61	6c	00	00	00	00	00	00	16	00	00	00	00
00007ffd:e3978e00	04	90	8c	b6	a1	55	00	00	16	00	00	0b	00	00	00	00	00	00	00
00007ffd:e3978e10	50	8e	97	e3	fd	7f	00	00	bf	82	8c	b6	a1	55	00	00	00	00	00
00007ffd:e3978e20	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00	00	00	00
00007ffd:e3978e30	d0	82	8c	b6	a1	55	00	00	a0	80	8c	6d	79	5f	70	61	00	00	00

- Here we can see the code that loads the two text strings and calls the function that compares them and then checks the result to see if they are the same.

Registers <2>									
RAX 00007ffd:e3978ded ASCII "todo_normal"									
RCX 0000000000000000									
RDX 00007ffd:e3978e3b ASCII "my_password"									
RBP 00007ffd:e3978db0									
RSP 00007ffd:e3978db0									
RDI 00007ffd:e3978e3b ASCII "my_password"									
RDI 00007ffd:e3978ded ASCII "todo_normal"									
R0 0000000000000000									
R9 0000000000000000									
R10 0000000000000000									
R11 00007f3fa5ca63c0									
R12 000055a1b68c80a0									
R13 00007ffd:e3978f30									
R14 0000000000000000									

  

000055a1:b68c823f	48	8d	45	dd	lea rax, [rbp-0x23]	
000055a1:b68c8243	48	89	d6		mov rsi, rdx	
000055a1:b68c8246	48	89	c7		mov rdi, rax	
000055a1:b68c8249	e8	12	fe	ff	call compare_strings	Compare strings
000055a1:b68c8251	89	45	e8		mov [rbp-0x18], eax	<- Result compare
000055a1:b68c8255	75	0e			cmp dword [rbp-0x18], 0	
000055a1:b68c8257	48	8d	3d	bb	0d	00
000055a1:b68c825e	e8	cd	fd	ff	jne 0x55a1b68c8265	
000055a1:b68c8263	eb	0c			lea rdi, [rel 0x55a1b68c9019]	ASCII "Felicidades!!!"
000055a1:b68c8265	48	8d	3d	bc	0d	00
000055a1:b68c8266	e8	bf	fd	ff	call 0x55a1b68c8030	
000055a1:b68c8271	90				jmp 0x55a1b68c8271	
000055a1:b68c8272	c9				lea rdi, [rel 0x55a1b68c9028]	ASCII "Intentalo de nuevo!!!"
000055a1:b68c8273	c3				call 0x55a1b68c8030	
					nop	
					leave	
					ret	