IoC Analysis: CrackMe4

Información

Tipo:	ELF	**Firma:**	[]
Bits:	x32	**Arquitectura:**	X86
Endiness:	little	**Entry point:**	0x470
Image Address:	0		

Hashes

MD5	ae07ac4b058e4284594210a7f83c0b29
SHA1	bc71a737dd52dc7d73668aa89cc521a474dad03a
SHA256	a45063610ab24b3b3205848117adbf6164ab31d6000fecc889653c9d1c5d5807

Otros Hashes:

Imphash MD5	
SSDeep	96:bLPl6rB+BLjEXMwN0ECp9ijEf0cgnp1w7yZlBrGBe7V9Os90h0:ewZEXR0ECp9iIscgpOKUE7uE
TLSH	T162E1740AFBE1CE37D883073D405B475962B3DC559717E723620825562E33AF8AFA624A

Secciones/segmentos

Nombre	Dirección
	0x400000
.interp	0x400154
.note.ABI-tag	0x400168
.note.gnu.build-id	0x400188
.gnu.hash	0x4001ac
.dynsym	0x4001cc
.dynstr	0x40027c
.gnu.version	0x40032a
.gnu.version_r	0x400340
.rel.dyn	0x400370
.rel.plt	0x4003b0
.init	0x4003d8
.plt	0x400400
.plt.got	0x400460
.text	0x400470
.fini	0x4006b4
.rodata	0x4006c8
.eh_frame_hdr	0x4007c8
.eh_frame	0x4007fc
.init_array	0x401ef4
.fini_array	0x401ef8
.dynamic	0x401efc
.got	0x401fec
.got.plt	0x402000
.data	0x402020
.bss	0x402028
.comment	0x400000
.symtab	0x400000
.strtab	0x400000
.shstrtab	0x400000

Cadenas de interés

hDDPtd	GNU GNU	getsputs	printf
strcmp			
siSii	St	PPPQV	Reto superado, guarda la password para las respuestas
Pista en https://www.youtube.com/watch?v=HEXWRTEbj1I&list=RDjrGx_MAlP1Q&index=6			
FJtx?	DGuDux	GAAA	

Símbolos

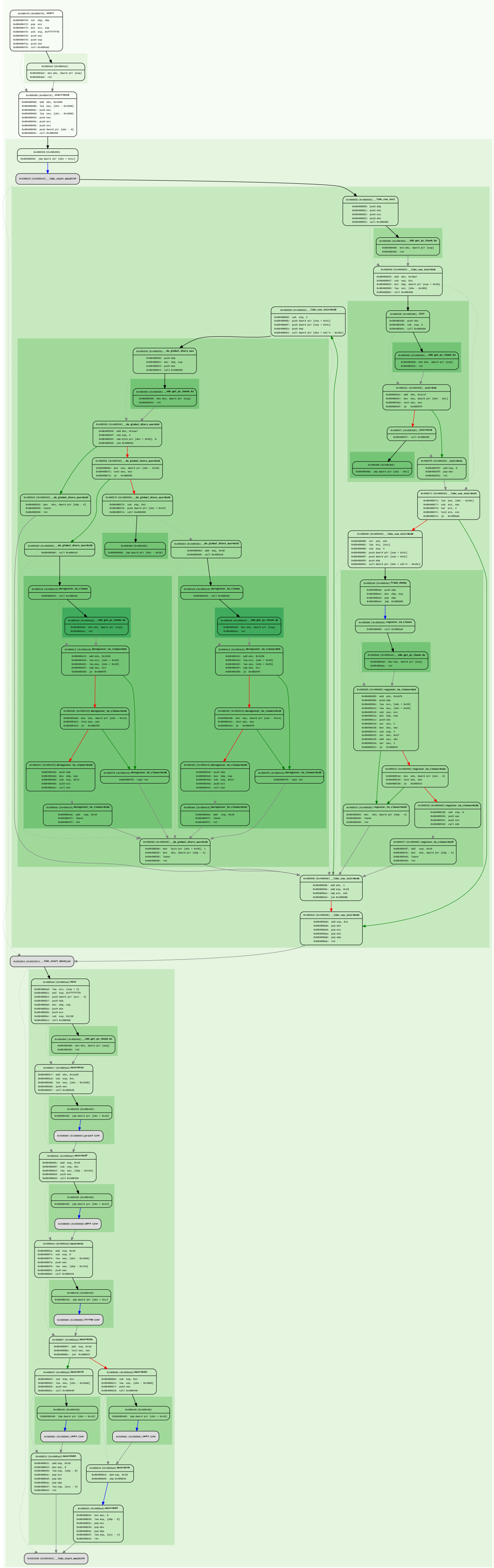
Nombre	Dirección	Tipo
	0x0	SymbolType.TYPE_NONE
strcmp	0x0	SymbolType.TYPE_FUNCTION
_ITM_deregisterTMCloneTable	0x0	SymbolType.TYPE_NONE
printf	0x0	SymbolType.TYPE_FUNCTION
gets	0x0	SymbolType.TYPE_FUNCTION
__cxa_finalize	0x0	SymbolType.TYPE_FUNCTION
puts	0x0	SymbolType.TYPE_FUNCTION
__gmon_start__	0x0	SymbolType.TYPE_NONE
__libc_start_main	0x0	SymbolType.TYPE_FUNCTION
_ITM_registerTMCloneTable	0x0	SymbolType.TYPE_NONE

	0x0	SymbolType.TYPE_NONE
strcmp	0x0	SymbolType.TYPE_FUNCTION
_ITM_deregisterTMCloneTable	0x0	SymbolType.TYPE_NONE
printf	0x0	SymbolType.TYPE_FUNCTION
gets	0x0	SymbolType.TYPE_FUNCTION
__cxa_finalize	0x0	SymbolType.TYPE_FUNCTION
puts	0x0	SymbolType.TYPE_FUNCTION
__gmon_start__	0x0	SymbolType.TYPE_NONE
__libc_start_main	0x0	SymbolType.TYPE_FUNCTION
_ITM_registerTMCloneTable	0x0	SymbolType.TYPE_NONE
	0x0	SymbolType.TYPE_NONE
	0x0	SymbolType.TYPE_SECTION
crtstuff.c	0x0	SymbolType.TYPE_OTHER
crackme.c	0x0	SymbolType.TYPE_OTHER
crtstuff.c	0x0	SymbolType.TYPE_OTHER
	0x0	SymbolType.TYPE_OTHER
strcmp@@GLIBC_2.0	0x0	SymbolType.TYPE_FUNCTION
_ITM_deregisterTMCloneTable	0x0	SymbolType.TYPE_NONE
printf@@GLIBC_2.0	0x0	SymbolType.TYPE_FUNCTION
gets@@GLIBC_2.0	0x0	SymbolType.TYPE_FUNCTION
__cxa_finalize@@GLIBC_2.1.3	0x0	SymbolType.TYPE_FUNCTION
puts@@GLIBC_2.0	0x0	SymbolType.TYPE_FUNCTION
__gmon_start__	0x0	SymbolType.TYPE_NONE
__libc_start_main@@GLIBC_2.0	0x0	SymbolType.TYPE_FUNCTION
_ITM_registerTMCloneTable	0x0	SymbolType.TYPE_NONE
	0x154	SymbolType.TYPE_SECTION
	0x168	SymbolType.TYPE_SECTION
	0x188	SymbolType.TYPE_SECTION
	0x1ac	SymbolType.TYPE_SECTION
	0x1cc	SymbolType.TYPE_SECTION
	0x27c	SymbolType.TYPE_SECTION
	0x32a	SymbolType.TYPE_SECTION
	0x340	SymbolType.TYPE_SECTION
	0x370	SymbolType.TYPE_SECTION
	0x3b0	SymbolType.TYPE_SECTION
	0x3d8	SymbolType.TYPE_SECTION
_init	0x3d8	SymbolType.TYPE_FUNCTION
	0x400	SymbolType.TYPE_SECTION
	0x460	SymbolType.TYPE_SECTION
	0x470	SymbolType.TYPE_SECTION
_start	0x470	SymbolType.TYPE_FUNCTION
__x86.get_pc_thunk.bx	0x4b0	SymbolType.TYPE_FUNCTION
deregister_tm_clones	0x4c0	SymbolType.TYPE_FUNCTION
register_tm_clones	0x500	SymbolType.TYPE_FUNCTION
__do_global_dtors_aux	0x550	SymbolType.TYPE_FUNCTION
frame_dummy	0x5a0	SymbolType.TYPE_FUNCTION
__x86.get_pc_thunk.dx	0x5a9	SymbolType.TYPE_FUNCTION
main	0x5ad	SymbolType.TYPE_FUNCTION
__libc_csu_init	0x650	SymbolType.TYPE_FUNCTION
__libc_csu_fini	0x6b0	SymbolType.TYPE_FUNCTION
	0x6b4	SymbolType.TYPE_SECTION
_fini	0x6b4	SymbolType.TYPE_FUNCTION
	0x6c8	SymbolType.TYPE_SECTION
_fp_hw	0x6c8	SymbolType.TYPE_OBJECT
_IO_stdin_used	0x6cc	SymbolType.TYPE_OBJECT
_IO_stdin_used	0x6cc	SymbolType.TYPE_OBJECT
_IO_stdin_used	0x6cc	SymbolType.TYPE_OBJECT
	0x7c8	SymbolType.TYPE_SECTION
__GNU_EH_FRAME_HDR	0x7c8	SymbolType.TYPE_NONE
	0x7fc	SymbolType.TYPE_SECTION
__FRAME_END__	0x8e0	SymbolType.TYPE_OBJECT
	0x1ef4	SymbolType.TYPE_SECTION
__frame_dummy_init_array_entry	0x1ef4	SymbolType.TYPE_OBJECT
__init_array_start	0x1ef4	SymbolType.TYPE_NONE
	0x1ef8	SymbolType.TYPE_SECTION
__do_global_dtors_aux_fini_array_entry	0x1ef8	SymbolType.TYPE_OBJECT
__init_array_end	0x1ef8	SymbolType.TYPE_NONE
	0x1efc	SymbolType.TYPE_SECTION
_DYNAMIC	0x1efc	SymbolType.TYPE_OBJECT
	0x1fec	SymbolType.TYPE_SECTION
	0x2000	SymbolType.TYPE_SECTION
_GLOBAL_OFFSET_TABLE_	0x2000	SymbolType.TYPE_OBJECT
	0x2020	SymbolType.TYPE_SECTION
data_start	0x2020	SymbolType.TYPE_NONE
__data_start	0x2020	SymbolType.TYPE_NONE
__dso_handle	0x2024	SymbolType.TYPE_OBJECT
	0x2028	SymbolType.TYPE_SECTION
completed.6586	0x2028	SymbolType.TYPE_OBJECT
_edata	0x2028	SymbolType.TYPE_NONE
__bss_start	0x2028	SymbolType.TYPE_NONE
__TMC_END__	0x2028	SymbolType.TYPE_OBJECT
_end	0x202c	SymbolType.TYPE_NONE
strcmp	0x0	SymbolType.TYPE_FUNCTION
printf	0x4	SymbolType.TYPE_FUNCTION
gets	0x8	SymbolType.TYPE_FUNCTION
puts	0xc	SymbolType.TYPE_FUNCTION
__libc_start_main	0x10	SymbolType.TYPE_FUNCTION
UnresolvableJumpTarget	0x104c	SymbolType.TYPE_FUNCTION
UnresolvableCallTarget	0x1050	SymbolType.TYPE_FUNCTION
__libc_start_main.after_init	0x1054	SymbolType.TYPE_OTHER
__libc_start_main.after_main	0x1058	SymbolType.TYPE_OTHER

Funciones

Nombre	Dirección	Hash SSDeep
_init	0x4003d8	3:vsAHd/MAWzz0d/FEBa+gXgAExkKX57ovRvmWhExbPA0ZVETvoKtaEOTJ2drd:vh5BWzzk2BxgXFEp570vBEJPbZVEjpa8
sub_400400	0x400400	3:vsB5Rv7usXHSQ7u4n:vg7DyQ7v
strcmp	0x400410	3:gXQ7uFv:gXQ7yv
printf	0x400420	3:gXQ7uFM4:gXQ7y5
gets	0x400430	3:gXQ7uFI4:gXQ7yF
puts	0x400440	3:gXQ7uFE4:gXQ7yR
__libc_start_main	0x400450	3:gXQ7uFf4:gXQ7yf4
sub_400460	0x400460	3:gXQ7ovLn:gXQ7En
sub_400466	0x400466	3:X:X
sub_400468	0x400468	3:gXQ7ovRn:gXQ70n
sub_40046e	0x40046e	3:X:X
_start	0x400470	6:QexdJp0KhEbWznk8X07ghYFwEtSk2bEbGt9/WR7GoVn:QebJp0Kh0Wzk57rFwcS30Gt9/WR7GIn
sub_4004a1	0x4004a1	3:1sn:mn
sub_4004a2	0x4004a2	3:3TRLFL5q3K:jNFL5IK
sub_4004a6	0x4004a6	3:WVO+VO+VO+Vs:WVDVDVDVs
__x86.get_pc_thunk.bx	0x4004b0	3:3TRLFL5q3K:jNFL5IK
sub_4004b4	0x4004b4	3:WVO+VO+VO+VO+Vs:WVDVDVDVDVs
deregister_tm_clones	0x4004c0	6:FJkxBiIVU4A0QUfViJDVYPF7shp594ZEJPbZVB5ThD4pW/GtTBD3cGhtd:oxtVUN0QU9it69GX2A75TmpW/GtThsG9
sub_4004f3	0x4004f3	3:V+g4:V+g4
sub_4004fa	0x4004fa	3:rEg4:wg4
register_tm_clones	0x400500	12:oxnb7UN0QU+t23W2GpJsg7t5y4hWTh0GtTRw7d:onnULUnmPJNlhWJtTRq
sub_400547	0x400547	3:3TAM0RJF4:jANRJC
__do_global_dtors_aux	0x400550	6:vh5ThDxdHk2BxggoX9FgJ+iy50T/F+p57EZEJPbZVgIIhrFL57nr6+VZWpz7yZzU:vh5TndEmxGtuNyKd+X7EAPQ7W+LWpz7J
sub_400597	0x400597	3:3TAM0RJF4:jANRJC
frame_dummy	0x4005a0	3:vsAHVfTsAHj6JPokR/wn:vh5ThDqPoYw
__x86.get_pc_thunk.dx	0x4005a9	3:3TXdJF5q3K:jbF5IK
main	0x4005ad	12:/p0Kgw5TnxhGtXBWpmmxupPAyE2ymWpPfyEu+ymWaxhcSfyE0LevUPCoWpPQyEtX:/p0KDTxQtwpTupv2hpyn+yhoqTevpoWG
sub_400643	0x400643	3:WVO+VO+VO+VO+VO+Vs:WVDVDVDVDVDVs
__libc_csu_init	0x400650	12:vhTmWsdEmxOp1Q8c6la4vwNt2WN1z/XunTNMZYNuNbDm7b4vILRRYcYNuNbDm7b4:5VEOp1BoNt2A17G4FlgLRR/Fln
sub_4006ad	0x4006ad	3:rEg4:wg4
__libc_csu_fini	0x4006b0	3:tKn:Qn
_fini	0x4006b4	3:vsAHd/MAWzz0d/FEBa+gT0UtaEs:vh5BWzzk2BxgtaEs
strcmp	0x500000	
printf	0x500004	
gets	0x500008	
puts	0x50000c	
__libc_start_main	0x500010	
UnresolvableJumpTarget	0x60104c	
UnresolvableCallTarget	0x601050	

Control-Flow graph


_start
_start+0x10
__libc_start_main@PLT
__libc_csu_init
__x86.get_pc_thunk.bx
__libc_csu_init+0x8
_init
_init+0x8
__libc_csu_init+0x21
__libc_csu_init+0x38
__do_global_dtors_aux
__do_global_dtors_aux+0x9
deregister_tm_clones
deregister_tm_clones+0x9
register_tm_clones
register_tm_clones+0x9
frame_dummy
__libc_csu_init+0x4b
__libc_csu_init+0x55
__libc_start_main@PLT
main
__x86.get_pc_thunk.ax
printf
puts
strcmp
__libc_start_main@PLT

Estado del proceso

EMU CFG: OK
Nodos CFG: 76

FAST CFG: OK
Vertices CFG: 107