```
Last login: Sun Jan 24 11:47:04 on ttys000
Dhrumils-Air:~ Dhrumil$ ssh Dpate85@23.99.192.124
Dpate85@23.99.192.124's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-43-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sun Jan 24 17:46:53 UTC 2016

  System load:  0.0               Processes:           116
  Usage of /:   5.8% of 28.80GB   Users logged in:     0
  Memory usage: 6%                IP address for eth0: 10.2.0.4
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

23 packages can be updated.
21 updates are security updates.


Last login: Sun Jan 24 17:46:54 2016 from 104-1-26-208.lightspeed.cicril.sbcgloba
l.net
Dpate85@Dhrumil:~$ cd dpate85
Dpate85@Dhrumil:~/dpate85$ ls
hw1  hw2  README.md
Dpate85@Dhrumil:~/dpate85$ cd hw2
Dpate85@Dhrumil:~/dpate85/hw2$ ls
puzzles
Dpate85@Dhrumil:~/dpate85/hw2$ cd pizzles
-bash: cd: pizzles: No such file or directory
Dpate85@Dhrumil:~/dpate85/hw2$ cd puzzles
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  lib361.so  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ rm lib361.so
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc 4 -shared -o lib361.so
/usr/bin/ld: warning: Cannot create .eh_frame_hdr section, --eh-frame-hdr ignored
.
/usr/bin/ld: error in 4(.eh_frame); no .eh_frame_hdr table will be created.
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -a 4
ELF Header:
  Magic:   7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF64
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
```

```
  Machine:                           Advanced Micro Devices X86-64
  Version:                           0x1
  Entry point address:               0x4007e0
  Start of program headers:          64 (bytes into file)
  Start of section headers:          8792 (bytes into file)
  Flags:                             0x0
  Size of this header:               64 (bytes)
  Size of program headers:           56 (bytes)
  Number of program headers:         9
  Size of section headers:           64 (bytes)
  Number of section headers:         28
  Section header string table index: 27

Section Headers:
  [Nr] Name              Type             Address           Offset
       Size              EntSize          Flags  Link  Info  Align
  [ 0]                   NULL             0000000000000000  00000000
       0000000000000000  0000000000000000           0     0     0
  [ 1] .interp           PROGBITS         0000000000400238  00000238
       000000000000001c  0000000000000000   A       0     0     1
  [ 2] .note.ABI-tag     NOTE             0000000000400254  00000254
       0000000000000020  0000000000000000   A       0     0     4
  [ 3] .note.gnu.build-i NOTE             0000000000400274  00000274
       0000000000000024  0000000000000000   A       0     0     4
  [ 4] .gnu.hash         GNU_HASH         0000000000400298  00000298
       0000000000000038  0000000000000000   A       5     0     8
  [ 5] .dynsym           DYNSYM           00000000004002d0  000002d0
       00000000000001c8  0000000000000018   A       6     1     8
  [ 6] .dynstr           STRTAB           0000000000400498  00000498
       000000000000010e  0000000000000000   A       0     0     1
  [ 7] .gnu.version      VERSYM           00000000004005a6  000005a6
       0000000000000026  0000000000000002   A       5     0     2
  [ 8] .gnu.version_r    VERNEED          00000000004005d0  000005d0
       0000000000000030  0000000000000000   A       6     1     8
  [ 9] .rela.dyn         RELA             0000000000400600  00000600
       0000000000000018  0000000000000018   A       5     0     8
  [10] .rela.plt         RELA             0000000000400618  00000618
       00000000000000f0  0000000000000018   A       5    12     8
  [11] .init             PROGBITS         0000000000400708  00000708
       000000000000001a  0000000000000000  AX       0     0     4
  [12] .plt              PROGBITS         0000000000400730  00000730
       00000000000000b0  0000000000000010  AX       0     0     16
  [13] .text             PROGBITS         00000000004007e0  000007e0
       0000000000000532  0000000000000000  AX       0     0     16
  [14] .fini             PROGBITS         0000000000400d14  00000d14
       0000000000000009  0000000000000000  AX       0     0     4
  [15] .rodata           PROGBITS         0000000000400d20  00000d20
       00000000000000bf  0000000000000000   A       0     0     8
  [16] .eh_frame_hdr     PROGBITS         0000000000400de0  00000de0
       0000000000000044  0000000000000000   A       0     0     4
  [17] .eh_frame         PROGBITS         0000000000400e28  00000e28
       000000000000013c  0000000000000000   A       0     0     8
  [18] .init_array       INIT_ARRAY       0000000000601e00  00001e00
```

```
       0000000000000008  0000000000000000  WA       0     0     8
  [19] .fini_array       FINI_ARRAY       0000000000601e08  00001e08
       0000000000000008  0000000000000000  WA       0     0     8
  [20] .jcr              PROGBITS         0000000000601e10  00001e10
       0000000000000008  0000000000000000  WA       0     0     8
  [21] .dynamic          DYNAMIC          0000000000601e18  00001e18
       00000000000001e0  0000000000000010  WA       6     0     8
  [22] .got              PROGBITS         0000000000601ff8  00001ff8
       0000000000000008  0000000000000008  WA       0     0     8
  [23] .got.plt          PROGBITS         0000000000602000  00002000
       0000000000000068  0000000000000008  WA       0     0     8
  [24] .data             PROGBITS         0000000000602080  00002080
       000000000000008c  0000000000000000  WA       0     0     32
  [25] .bss              NOBITS           000000000060210c  0000210c
       0000000000000004  0000000000000000  WA       0     0     1
  [26] .comment          PROGBITS         0000000000000000  0000210c
       000000000000004d  0000000000000001  MS       0     0     1
  [27] .shstrtab         STRTAB           0000000000000000  00002159
       00000000000000f8  0000000000000000           0     0     1
Key to Flags:
  W (write), A (alloc), X (execute), M (merge), S (strings), l (large)
  I (info), L (link order), G (group), T (TLS), E (exclude), x (unknown)
  O (extra OS processing required) o (OS specific), p (processor specific)

There are no section groups in this file.

Program Headers:
  Type           Offset             VirtAddr           PhysAddr
                 FileSiz            MemSiz              Flags  Align
  PHDR           0x0000000000000040 0x0000000000400040 0x0000000000400040
                 0x00000000000001f8 0x00000000000001f8  R E    8
  INTERP         0x0000000000000238 0x0000000000400238 0x0000000000400238
                 0x000000000000001c 0x000000000000001c  R      1
      [Requesting program interpreter: /lib64/ld-linux-x86-64.so.2]
  LOAD           0x0000000000000000 0x0000000000400000 0x0000000000400000
                 0x0000000000000f64 0x0000000000000f64  R E    200000
  LOAD           0x0000000000001e00 0x0000000000601e00 0x0000000000601e00
                 0x000000000000030c 0x0000000000000310  RW     200000
  DYNAMIC        0x0000000000001e18 0x0000000000601e18 0x0000000000601e18
                 0x00000000000001e0 0x00000000000001e0  RW     8
  NOTE           0x0000000000000254 0x0000000000400254 0x0000000000400254
                 0x0000000000000044 0x0000000000000044  R      4
  GNU_EH_FRAME   0x0000000000000de0 0x0000000000400de0 0x0000000000400de0
                 0x0000000000000044 0x0000000000000044  R      4
  GNU_STACK      0x0000000000000000 0x0000000000000000 0x0000000000000000
                 0x0000000000000000 0x0000000000000000  RW     10
  GNU_RELRO      0x0000000000001e00 0x0000000000601e00 0x0000000000601e00
                 0x0000000000000200 0x0000000000000200  R      1

 Section to Segment mapping:
  Segment Sections...
   00
   01     .interp
```

```
   02     .interp .note.ABI-tag .note.gnu.build-id .gnu.hash .dynsym .dynstr .gnu
.version .gnu.version_r .rela.dyn .rela.plt .init .plt .text .fini .rodata .eh_fr
ame_hdr .eh_frame
   03     .init_array .fini_array .jcr .dynamic .got .got.plt .data .bss
   04     .dynamic
   05     .note.ABI-tag .note.gnu.build-id
   06     .eh_frame_hdr
   07
   08     .init_array .fini_array .jcr .dynamic .got

Dynamic section at offset 0x1e18 contains 25 entries:
  Tag        Type                         Name/Value
 0x0000000000000001 (NEEDED)             Shared library: [lib361.so]
 0x0000000000000001 (NEEDED)             Shared library: [libc.so.6]
 0x000000000000000c (INIT)               0x400708
 0x000000000000000d (FINI)               0x400d14
 0x0000000000000019 (INIT_ARRAY)         0x601e00
 0x000000000000001b (INIT_ARRAYSZ)       8 (bytes)
 0x000000000000001a (FINI_ARRAY)         0x601e08
 0x000000000000001c (FINI_ARRAYSZ)       8 (bytes)
 0x000000006ffffef5 (GNU_HASH)           0x400298
 0x0000000000000005 (STRTAB)             0x400498
 0x0000000000000006 (SYMTAB)             0x4002d0
 0x000000000000000a (STRSZ)              270 (bytes)
 0x000000000000000b (SYMENT)             24 (bytes)
 0x0000000000000015 (DEBUG)              0x0
 0x0000000000000003 (PLTGOT)             0x602000
 0x0000000000000002 (PLTRELSZ)           240 (bytes)
 0x0000000000000014 (PLTREL)             RELA
 0x0000000000000017 (JMPREL)             0x400618
 0x0000000000000007 (RELA)               0x400600
 0x0000000000000008 (RELASZ)             24 (bytes)
 0x0000000000000009 (RELAENT)            24 (bytes)
 0x000000006ffffffe (VERNEED)            0x4005d0
 0x000000006fffffff (VERNEEDNUM)         1
 0x000000006ffffff0 (VERSYM)             0x4005a6
 0x0000000000000000 (NULL)               0x0

Relocation section '.rela.dyn' at offset 0x600 contains 1 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000601ff8  000a00000006 R_X86_64_GLOB_DAT 0000000000000000 __gmon_start__ + 0

Relocation section '.rela.plt' at offset 0x618 contains 10 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000602018  000200000007 R_X86_64_JUMP_SLO 0000000000000000 puts + 0
000000602020  000300000007 R_X86_64_JUMP_SLO 0000000000000000 secretoperation + 0
000000602028  000400000007 R_X86_64_JUMP_SLO 0000000000000000 strlen + 0
000000602030  000500000007 R_X86_64_JUMP_SLO 0000000000000000 __stack_chk_fail +
0
000000602038  000600000007 R_X86_64_JUMP_SLO 0000000000000000 printf + 0
000000602040  000700000007 R_X86_64_JUMP_SLO 0000000000000000 __assert_fail + 0
000000602048  000800000007 R_X86_64_JUMP_SLO 0000000000000000 __libc_start_main +
 0
```

```
000000602050  000900000007 R_X86_64_JUMP_SLO 0000000000000000 calloc + 0
000000602058  000a00000007 R_X86_64_JUMP_SLO 0000000000000000 __gmon_start__ + 0
000000602060  000b00000007 R_X86_64_JUMP_SLO 0000000000000000 getlogin_r + 0

The decoding of unwind sections for machine type Advanced Micro Devices X86-64 is
 not currently supported.

Symbol table '.dynsym' contains 19 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMClone
Tab
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND puts@GLIBC_2.2.5 (2)
     3: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND secretoperation
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strlen@GLIBC_2.2.5 (2)
     5: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __stack_chk_fail@GLIBC
_2.4 (3)
     6: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND printf@GLIBC_2.2.5 (2)
     7: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __assert_fail@GLIBC_2.
2.5 (2)
     8: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@GLIB
C_2.2.5 (2)
     9: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND calloc@GLIBC_2.2.5 (2)
    10: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
    11: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND getlogin_r@GLIBC_2.2.5
 (2)
    12: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
    13: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTa
ble
    14: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   24 _edata
    15: 0000000000602110     0 NOTYPE  GLOBAL DEFAULT   25 _end
    16: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   25 __bss_start
    17: 0000000000400708     0 FUNC    GLOBAL DEFAULT   11 _init
    18: 0000000000400d14     0 FUNC    GLOBAL DEFAULT   14 _fini

Histogram for `.gnu.hash' bucket list length (total of 3 buckets):
 Length  Number     % of total  Coverage
      0  0          (  0.0%)
      1  1          ( 33.3%)     20.0%
      2  2          ( 66.7%)    100.0%

Version symbols section '.gnu.version' contains 19 entries:
 Addr: 00000000004005a6  Offset: 0x0005a6  Link: 5 (.dynsym)
  000:   0 (*local*)       0 (*local*)       2 (GLIBC_2.2.5)   0 (*local*)
  004:   2 (GLIBC_2.2.5)   3 (GLIBC_2.4)     2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)
  008:   2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)   0 (*local*)       2 (GLIBC_2.2.5)
  00c:   0 (*local*)       0 (*local*)       1 (*global*)      1 (*global*)
  010:   1 (*global*)      1 (*global*)      1 (*global*)

Version needs section '.gnu.version_r' contains 1 entries:
 Addr: 0x00000000004005d0  Offset: 0x0005d0  Link: 6 (.dynstr)
  000000: Version: 1  File: libc.so.6  Cnt: 2
  0x0010:   Name: GLIBC_2.4  Flags: none  Version: 3
```

```
  0x0020:   Name: GLIBC_2.2.5  Flags: none  Version: 2

Displaying notes found at file offset 0x00000254 with length 0x00000020:
  Owner                 Data size       Description
  GNU                  0x00000010       NT_GNU_ABI_TAG (ABI version tag)
    OS: Linux, ABI: 2.6.24

Displaying notes found at file offset 0x00000274 with length 0x00000024:
  Owner                 Data size       Description
  GNU                  0x00000014       NT_GNU_BUILD_ID (unique build ID bitstrin
g)
    Build ID: 516c99c45c7b1cd513589f91ae029c0f1528d553
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s
readelf: Warning: Nothing to do.
Usage: readelf <option(s)> elf-file(s)
 Display information about the contents of ELF format files
 Options are:
  -a --all               Equivalent to: -h -l -S -s -r -d -V -A -I
  -h --file-header       Display the ELF file header
  -l --program-headers   Display the program headers
     --segments          An alias for --program-headers
  -S --section-headers   Display the sections' header
     --sections          An alias for --section-headers
  -g --section-groups    Display the section groups
  -t --section-details   Display the section details
  -e --headers           Equivalent to: -h -l -S
  -s --syms              Display the symbol table
     --symbols           An alias for --syms
  --dyn-syms             Display the dynamic symbol table
  -n --notes             Display the core notes (if present)
  -r --relocs            Display the relocations (if present)
  -u --unwind            Display the unwind info (if present)
  -d --dynamic           Display the dynamic section (if present)
  -V --version-info      Display the version sections (if present)
  -A --arch-specific     Display architecture specific information (if any)
  -c --archive-index     Display the symbol/file index in an archive
  -D --use-dynamic       Use the dynamic section info when displaying symbols
  -x --hex-dump=<number|name>
                         Dump the contents of section <number|name> as bytes
  -p --string-dump=<number|name>
                         Dump the contents of section <number|name> as strings
  -R --relocated-dump=<number|name>
                         Dump the contents of section <number|name> as relocated
bytes
  -w[lLiaprmfFsoRt] or
  --debug-dump[=rawline,=decodedline,=info,=abbrev,=pubnames,=aranges,=macro,=fra
mes,
               =frames-interp,=str,=loc,=Ranges,=pubtypes,
               =gdb_index,=trace_info,=trace_abbrev,=trace_aranges,
               =addr,=cu_index]
                         Display the contents of DWARF2 debug sections
  --dwarf-depth=N        Do not display DIEs at depth N or greater
  --dwarf-start=N        Display DIEs starting with N, at the same depth
```

```
                        or deeper
  -I --histogram         Display histogram of bucket list lengths
  -W --wide              Allow output width to exceed 80 characters
  @<file>                Read options from <file>
  -H --help              Display this information
  -v --version           Display the version number of readelf
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s 4

Symbol table '.dynsym' contains 19 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMClone
Tab
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND puts@GLIBC_2.2.5 (2)
     3: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND secretoperation
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strlen@GLIBC_2.2.5 (2)
     5: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __stack_chk_fail@GLIBC
_2.4 (3)
     6: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND printf@GLIBC_2.2.5 (2)
     7: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __assert_fail@GLIBC_2.
2.5 (2)
     8: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@GLIB
C_2.2.5 (2)
     9: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND calloc@GLIBC_2.2.5 (2)
    10: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
    11: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND getlogin_r@GLIBC_2.2.5
 (2)
    12: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
    13: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTa
ble
    14: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   24 _edata
    15: 0000000000602110     0 NOTYPE  GLOBAL DEFAULT   25 _end
    16: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   25 __bss_start
    17: 0000000000400708     0 FUNC    GLOBAL DEFAULT   11 _init
    18: 0000000000400d14     0 FUNC    GLOBAL DEFAULT   14 _fini
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump 4
Usage: objdump <option(s)> <file(s)>
 Display information from object <file(s)>.
 At least one of the following switches must be given:
  -a, --archive-headers    Display archive header information
  -f, --file-headers       Display the contents of the overall file header
  -p, --private-headers    Display object format specific file header contents
  -P, --private=OPT,OPT... Display object format specific contents
  -h, --[section-]headers  Display the contents of the section headers
  -x, --all-headers        Display the contents of all headers
  -d, --disassemble        Display assembler contents of executable sections
  -D, --disassemble-all    Display assembler contents of all sections
  -S, --source             Intermix source code with disassembly
  -s, --full-contents      Display the full contents of all sections requested
  -g, --debugging          Display debug information in object file
  -e, --debugging-tags     Display debug information using ctags style
  -G, --stabs              Display (in raw form) any STABS info in the file
  -W[lLiaprmfFsoRt] or
```

```
  --dwarf[=rawline,=decodedline,=info,=abbrev,=pubnames,=aranges,=macro,=frames,
         =frames-interp,=str,=loc,=Ranges,=pubtypes,
         =gdb_index,=trace_info,=trace_abbrev,=trace_aranges,
         =addr,=cu_index]
                         Display DWARF info in the file
  -t, --syms             Display the contents of the symbol table(s)
  -T, --dynamic-syms     Display the contents of the dynamic symbol table
  -r, --reloc            Display the relocation entries in the file
  -R, --dynamic-reloc    Display the dynamic relocation entries in the file
  @<file>                Read options from <file>
  -v, --version          Display this program's version number
  -i, --info             List object formats and architectures supported
  -H, --help             Display this information
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -S 4

4:     file format elf64-x86-64


Disassembly of section .init:

0000000000400708 <_init>:
  400708:       48 83 ec 08             sub    $0x8,%rsp
  40070c:       48 8b 05 e5 18 20 00    mov    0x2018e5(%rip),%rax        # 601ff
8 <_fini+0x2012e4>
  400713:       48 85 c0                test   %rax,%rax
  400716:       74 05                   je     40071d <_init+0x15>
  400718:       e8 a3 00 00 00          callq  4007c0 <__gmon_start__@plt>
  40071d:       48 83 c4 08             add    $0x8,%rsp
  400721:       c3                      retq

Disassembly of section .plt:

0000000000400730 <puts@plt-0x10>:
  400730:       ff 35 d2 18 20 00       pushq  0x2018d2(%rip)        # 602008 <_f
ini+0x2012f4>
  400736:       ff 25 d4 18 20 00       jmpq   *0x2018d4(%rip)        # 602010 <_
fini+0x2012fc>
  40073c:       0f 1f 40 00             nopl   0x0(%rax)

0000000000400740 <puts@plt>:
  400740:       ff 25 d2 18 20 00       jmpq   *0x2018d2(%rip)        # 602018 <_
fini+0x201304>
  400746:       68 00 00 00 00          pushq  $0x0
  40074b:       e9 e0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400750 <secretoperation@plt>:
  400750:       ff 25 ca 18 20 00       jmpq   *0x2018ca(%rip)        # 602020 <_
fini+0x20130c>
  400756:       68 01 00 00 00          pushq  $0x1
  40075b:       e9 d0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400760 <strlen@plt>:
  400760:       ff 25 c2 18 20 00       jmpq   *0x2018c2(%rip)        # 602028 <_
```

```
fini+0x201314>
  400766:       68 02 00 00 00          pushq  $0x2
  40076b:       e9 c0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400770 <__stack_chk_fail@plt>:
  400770:       ff 25 ba 18 20 00       jmpq   *0x2018ba(%rip)        # 602030 <_
fini+0x20131c>
  400776:       68 03 00 00 00          pushq  $0x3
  40077b:       e9 b0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400780 <printf@plt>:
  400780:       ff 25 b2 18 20 00       jmpq   *0x2018b2(%rip)        # 602038 <_
fini+0x201324>
  400786:       68 04 00 00 00          pushq  $0x4
  40078b:       e9 a0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400790 <__assert_fail@plt>:
  400790:       ff 25 aa 18 20 00       jmpq   *0x2018aa(%rip)        # 602040 <_
fini+0x20132c>
  400796:       68 05 00 00 00          pushq  $0x5
  40079b:       e9 90 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007a0 <__libc_start_main@plt>:
  4007a0:       ff 25 a2 18 20 00       jmpq   *0x2018a2(%rip)        # 602048 <_
fini+0x201334>
  4007a6:       68 06 00 00 00          pushq  $0x6
  4007ab:       e9 80 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007b0 <calloc@plt>:
  4007b0:       ff 25 9a 18 20 00       jmpq   *0x20189a(%rip)        # 602050 <_
fini+0x20133c>
  4007b6:       68 07 00 00 00          pushq  $0x7
  4007bb:       e9 70 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007c0 <__gmon_start__@plt>:
  4007c0:       ff 25 92 18 20 00       jmpq   *0x201892(%rip)        # 602058 <_
fini+0x201344>
  4007c6:       68 08 00 00 00          pushq  $0x8
  4007cb:       e9 60 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007d0 <getlogin_r@plt>:
  4007d0:       ff 25 8a 18 20 00       jmpq   *0x20188a(%rip)        # 602060 <_
fini+0x20134c>
  4007d6:       68 09 00 00 00          pushq  $0x9
  4007db:       e9 50 ff ff ff          jmpq   400730 <_init+0x28>

Disassembly of section .text:

00000000004007e0 <.text>:
  4007e0:       31 ed                   xor    %ebp,%ebp
  4007e2:       49 89 d1                mov    %rdx,%r9
  4007e5:       5e                      pop    %rsi
  4007e6:       48 89 e2                mov    %rsp,%rdx
```

```
  4007e9:       48 83 e4 f0             and    $0xfffffffffffffff0,%rsp
  4007ed:       50                      push   %rax
  4007ee:       54                      push   %rsp
  4007ef:       49 c7 c0 10 0d 40 00    mov    $0x400d10,%r8
  4007f6:       48 c7 c1 a0 0c 40 00    mov    $0x400ca0,%rcx
  4007fd:       48 c7 c7 cd 08 40 00    mov    $0x4008cd,%rdi
  400804:       e8 97 ff ff ff          callq  4007a0 <__libc_start_main@plt>
  400809:       f4                      hlt
  40080a:       66 0f 1f 44 00 00       nopw   0x0(%rax,%rax,1)
  400810:       b8 17 21 60 00          mov    $0x602117,%eax
  400815:       55                      push   %rbp
  400816:       48 2d 10 21 60 00       sub    $0x602110,%rax
  40081c:       48 83 f8 0e             cmp    $0xe,%rax
  400820:       48 89 e5                mov    %rsp,%rbp
  400823:       77 02                   ja     400827 <getlogin_r@plt+0x57>
  400825:       5d                      pop    %rbp
  400826:       c3                      retq
  400827:       b8 00 00 00 00          mov    $0x0,%eax
  40082c:       48 85 c0                test   %rax,%rax
  40082f:       74 f4                   je     400825 <getlogin_r@plt+0x55>
  400831:       5d                      pop    %rbp
  400832:       bf 10 21 60 00          mov    $0x602110,%edi
  400837:       ff e0                   jmpq   *%rax
  400839:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400840:       b8 10 21 60 00          mov    $0x602110,%eax
  400845:       55                      push   %rbp
  400846:       48 2d 10 21 60 00       sub    $0x602110,%rax
  40084c:       48 c1 f8 03             sar    $0x3,%rax
  400850:       48 89 e5                mov    %rsp,%rbp
  400853:       48 89 c2                mov    %rax,%rdx
  400856:       48 c1 ea 3f             shr    $0x3f,%rdx
  40085a:       48 01 d0                add    %rdx,%rax
  40085d:       48 d1 f8                sar    %rax
  400860:       75 02                   jne    400864 <getlogin_r@plt+0x94>
  400862:       5d                      pop    %rbp
  400863:       c3                      retq
  400864:       ba 00 00 00 00          mov    $0x0,%edx
  400869:       48 85 d2                test   %rdx,%rdx
  40086c:       74 f4                   je     400862 <getlogin_r@plt+0x92>
  40086e:       5d                      pop    %rbp
  40086f:       48 89 c6                mov    %rax,%rsi
  400872:       bf 10 21 60 00          mov    $0x602110,%edi
  400877:       ff e2                   jmpq   *%rdx
  400879:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400880:       80 3d 85 18 20 00 00    cmpb   $0x0,0x201885(%rip)        # 60210
c <_edata>
  400887:       75 11                   jne    40089a <getlogin_r@plt+0xca>
  400889:       55                      push   %rbp
  40088a:       48 89 e5                mov    %rsp,%rbp
  40088d:       e8 7e ff ff ff          callq  400810 <getlogin_r@plt+0x40>
  400892:       5d                      pop    %rbp
  400893:       c6 05 72 18 20 00 01    movb   $0x1,0x201872(%rip)        # 60210
c <_edata>
```

```
  40089a:       f3 c3                   repz retq
  40089c:       0f 1f 40 00             nopl   0x0(%rax)
  4008a0:       48 83 3d 68 15 20 00    cmpq   $0x0,0x201568(%rip)        # 601e1
0 <_fini+0x2010fc>
  4008a7:       00
  4008a8:       74 1e                   je     4008c8 <getlogin_r@plt+0xf8>
  4008aa:       b8 00 00 00 00          mov    $0x0,%eax
  4008af:       48 85 c0                test   %rax,%rax
  4008b2:       74 14                   je     4008c8 <getlogin_r@plt+0xf8>
  4008b4:       55                      push   %rbp
  4008b5:       bf 10 1e 60 00          mov    $0x601e10,%edi
  4008ba:       48 89 e5                mov    %rsp,%rbp
  4008bd:       ff d0                   callq  *%rax
  4008bf:       5d                      pop    %rbp
  4008c0:       e9 7b ff ff ff          jmpq   400840 <getlogin_r@plt+0x70>
  4008c5:       0f 1f 00                nopl   (%rax)
  4008c8:       e9 73 ff ff ff          jmpq   400840 <getlogin_r@plt+0x70>
  4008cd:       55                      push   %rbp
  4008ce:       48 89 e5                mov    %rsp,%rbp
  4008d1:       48 83 ec 10             sub    $0x10,%rsp
  4008d5:       c7 45 f4 01 00 00 00    movl   $0x1,-0xc(%rbp)
  4008dc:       c7 45 f8 02 00 00 00    movl   $0x2,-0x8(%rbp)
  4008e3:       c7 45 fc 00 00 00 00    movl   $0x0,-0x4(%rbp)
  4008ea:       bf 70 0d 40 00          mov    $0x400d70,%edi
  4008ef:       e8 4c fe ff ff          callq  400740 <puts@plt>
  4008f4:       be 06 00 00 00          mov    $0x6,%esi
  4008f9:       bf 03 00 00 00          mov    $0x3,%edi
  4008fe:       e8 4d fe ff ff          callq  400750 <secretoperation@plt>
  400903:       89 45 fc                mov    %eax,-0x4(%rbp)
  400906:       83 7d fc 0a             cmpl   $0xa,-0x4(%rbp)
  40090a:       74 19                   je     400925 <getlogin_r@plt+0x155>
  40090c:       b9 da 0d 40 00          mov    $0x400dda,%ecx
  400911:       ba 12 00 00 00          mov    $0x12,%edx
  400916:       be b7 0d 40 00          mov    $0x400db7,%esi
  40091b:       bf c1 0d 40 00          mov    $0x400dc1,%edi
  400920:       e8 6b fe ff ff          callq  400790 <__assert_fail@plt>
  400925:       8b 55 f8                mov    -0x8(%rbp),%edx
  400928:       8b 45 f4                mov    -0xc(%rbp),%eax
  40092b:       89 d6                   mov    %edx,%esi
  40092d:       89 c7                   mov    %eax,%edi
  40092f:       e8 1c fe ff ff          callq  400750 <secretoperation@plt>
  400934:       89 45 fc                mov    %eax,-0x4(%rbp)
  400937:       83 7d fc 04             cmpl   $0x4,-0x4(%rbp)
  40093b:       74 19                   je     400956 <getlogin_r@plt+0x186>
  40093d:       b9 da 0d 40 00          mov    $0x400dda,%ecx
  400942:       ba 14 00 00 00          mov    $0x14,%edx
  400947:       be b7 0d 40 00          mov    $0x400db7,%esi
  40094c:       bf ce 0d 40 00          mov    $0x400dce,%edi
  400951:       e8 3a fe ff ff          callq  400790 <__assert_fail@plt>
  400956:       48 8b 05 33 17 20 00    mov    0x201733(%rip),%rax        # 60209
0 <_fini+0x20137c>
  40095d:       48 89 c7                mov    %rax,%rdi
  400960:       e8 28 00 00 00          callq  40098d <getlogin_r@plt+0x1bd>
```

```
  400965:       48 89 c2                mov    %rax,%rdx
  400968:       48 8b 0d 31 17 20 00    mov    0x201731(%rip),%rcx        # 6020a
0 <_fini+0x20138c>
  40096f:       48 8b 05 22 17 20 00    mov    0x201722(%rip),%rax        # 60209
8 <_fini+0x201384>
  400976:       48 89 ce                mov    %rcx,%rsi
  400979:       48 89 c7                mov    %rax,%rdi
  40097c:       b8 00 00 00 00          mov    $0x0,%eax
  400981:       e8 fa fd ff ff          callq  400780 <printf@plt>
  400986:       b8 00 00 00 00          mov    $0x0,%eax
  40098b:       c9                      leaveq
  40098c:       c3                      retq
  40098d:       55                      push   %rbp
  40098e:       48 89 e5                mov    %rsp,%rbp
  400991:       53                      push   %rbx
  400992:       48 81 ec 38 04 00 00    sub    $0x438,%rsp
  400999:       48 89 bd c8 fb ff ff    mov    %rdi,-0x438(%rbp)
  4009a0:       64 48 8b 04 25 28 00    mov    %fs:0x28,%rax
  4009a7:       00 00
  4009a9:       48 89 45 e8             mov    %rax,-0x18(%rbp)
  4009ad:       31 c0                   xor    %eax,%eax
  4009af:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
  4009b6:       be 00 04 00 00          mov    $0x400,%esi
  4009bb:       48 89 c7                mov    %rax,%rdi
  4009be:       e8 0d fe ff ff          callq  4007d0 <getlogin_r@plt>
  4009c3:       c7 85 d4 fb ff ff 00    movl   $0x0,-0x42c(%rbp)
  4009ca:       00 00 00
  4009cd:       eb 3e                   jmp    400a0d <getlogin_r@plt+0x23d>
  4009cf:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  4009d5:       48 98                   cltq
  4009d7:       0f b6 94 05 e0 fb ff    movzbl -0x420(%rbp,%rax,1),%edx
  4009de:       ff
  4009df:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  4009e5:       48 63 c8                movslq %eax,%rcx
  4009e8:       48 8b 85 c8 fb ff ff    mov    -0x438(%rbp),%rax
  4009ef:       48 01 c8                add    %rcx,%rax
  4009f2:       0f b6 00                movzbl (%rax),%eax
  4009f5:       31 c2                   xor    %eax,%edx
  4009f7:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  4009fd:       48 98                   cltq
  4009ff:       88 94 05 e0 fb ff ff    mov    %dl,-0x420(%rbp,%rax,1)
  400a06:       83 85 d4 fb ff ff 01    addl   $0x1,-0x42c(%rbp)
  400a0d:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  400a13:       48 63 d8                movslq %eax,%rbx
  400a16:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
  400a1d:       48 89 c7                mov    %rax,%rdi
  400a20:       e8 3b fd ff ff          callq  400760 <strlen@plt>
  400a25:       48 39 c3                cmp    %rax,%rbx
  400a28:       72 a5                   jb     4009cf <getlogin_r@plt+0x1ff>
  400a2a:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  400a30:       48 63 c8                movslq %eax,%rcx
  400a33:       48 8d 95 d8 fb ff ff    lea    -0x428(%rbp),%rdx
  400a3a:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
```

```
400a41:       48 89 ce                mov    %rcx,%rsi
400a44:       48 89 c7                mov    %rax,%rdi
400a47:       e8 1e 00 00 00          callq  400a6a <getlogin_r@plt+0x29a>
400a4c:       48 8b 75 e8             mov    -0x18(%rbp),%rsi
400a50:       64 48 33 34 25 28 00    xor    %fs:0x28,%rsi
400a57:       00 00
400a59:       74 05                   je     400a60 <getlogin_r@plt+0x290>
400a5b:       e8 10 fd ff ff          callq  400770 <__stack_chk_fail@plt>
400a60:       48 81 c4 38 04 00 00    add    $0x438,%rsp
400a67:       5b                      pop    %rbx
400a68:       5d                      pop    %rbp
400a69:       c3                      retq
400a6a:       55                      push   %rbp
400a6b:       48 89 e5                mov    %rsp,%rbp
400a6e:       48 83 ec 40             sub    $0x40,%rsp
400a72:       48 89 7d d8             mov    %rdi,-0x28(%rbp)
400a76:       48 89 75 d0             mov    %rsi,-0x30(%rbp)
400a7a:       48 89 55 c8             mov    %rdx,-0x38(%rbp)
400a7e:       48 8b 45 d0             mov    -0x30(%rbp),%rax
400a82:       48 83 c0 02             add    $0x2,%rax
400a86:       48 ba ab aa aa aa aa    movabs $0xaaaaaaaaaaaaaaab,%rdx
400a8d:       aa aa aa
400a90:       48 f7 e2                mul    %rdx
400a93:       48 89 d0                mov    %rdx,%rax
400a96:       48 d1 e8                shr    %rax
400a99:       48 8d 14 85 00 00 00    lea    0x0(,%rax,4),%rdx
400aa0:       00
400aa1:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400aa5:       48 89 10                mov    %rdx,(%rax)
400aa8:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400aac:       48 8b 00                mov    (%rax),%rax
400aaf:       be 01 00 00 00          mov    $0x1,%esi
400ab4:       48 89 c7                mov    %rax,%rdi
400ab7:       e8 f4 fc ff ff          callq  4007b0 <calloc@plt>
400abc:       48 89 45 f8             mov    %rax,-0x8(%rbp)
400ac0:       48 83 7d f8 00          cmpq   $0x0,-0x8(%rbp)
400ac5:       75 0a                   jne    400ad1 <getlogin_r@plt+0x301>
400ac7:       b8 00 00 00 00          mov    $0x0,%eax
400acc:       e9 c0 01 00 00          jmpq   400c91 <getlogin_r@plt+0x4c1>
400ad1:       c7 45 e0 00 00 00 00    movl   $0x0,-0x20(%rbp)
400ad8:       c7 45 e4 00 00 00 00    movl   $0x0,-0x1c(%rbp)
400adf:       e9 3b 01 00 00          jmpq   400c1f <getlogin_r@plt+0x44f>
400ae4:       8b 45 e0                mov    -0x20(%rbp),%eax
400ae7:       48 98                   cltq
400ae9:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400aed:       73 1b                   jae    400b0a <getlogin_r@plt+0x33a>
400aef:       8b 45 e0                mov    -0x20(%rbp),%eax
400af2:       8d 50 01                lea    0x1(%rax),%edx
400af5:       89 55 e0                mov    %edx,-0x20(%rbp)
400af8:       48 63 d0                movslq %eax,%rdx
400afb:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400aff:       48 01 d0                add    %rdx,%rax
400b02:       0f b6 00                movzbl (%rax),%eax
```

```
400b05:       0f b6 c0                movzbl %al,%eax
400b08:       eb 05                   jmp    400b0f <getlogin_r@plt+0x33f>
400b0a:       b8 00 00 00 00          mov    $0x0,%eax
400b0f:       89 45 e8                mov    %eax,-0x18(%rbp)
400b12:       8b 45 e0                mov    -0x20(%rbp),%eax
400b15:       48 98                   cltq
400b17:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400b1b:       73 1b                   jae    400b38 <getlogin_r@plt+0x368>
400b1d:       8b 45 e0                mov    -0x20(%rbp),%eax
400b20:       8d 50 01                lea    0x1(%rax),%edx
400b23:       89 55 e0                mov    %edx,-0x20(%rbp)
400b26:       48 63 d0                movslq %eax,%rdx
400b29:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400b2d:       48 01 d0                add    %rdx,%rax
400b30:       0f b6 00                movzbl (%rax),%eax
400b33:       0f b6 c0                movzbl %al,%eax
400b36:       eb 05                   jmp    400b3d <getlogin_r@plt+0x36d>
400b38:       b8 00 00 00 00          mov    $0x0,%eax
400b3d:       89 45 ec                mov    %eax,-0x14(%rbp)
400b40:       8b 45 e0                mov    -0x20(%rbp),%eax
400b43:       48 98                   cltq
400b45:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400b49:       73 1b                   jae    400b66 <getlogin_r@plt+0x396>
400b4b:       8b 45 e0                mov    -0x20(%rbp),%eax
400b4e:       8d 50 01                lea    0x1(%rax),%edx
400b51:       89 55 e0                mov    %edx,-0x20(%rbp)
400b54:       48 63 d0                movslq %eax,%rdx
400b57:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400b5b:       48 01 d0                add    %rdx,%rax
400b5e:       0f b6 00                movzbl (%rax),%eax
400b61:       0f b6 c0                movzbl %al,%eax
400b64:       eb 05                   jmp    400b6b <getlogin_r@plt+0x39b>
400b66:       b8 00 00 00 00          mov    $0x0,%eax
400b6b:       89 45 f0                mov    %eax,-0x10(%rbp)
400b6e:       8b 45 e8                mov    -0x18(%rbp),%eax
400b71:       c1 e0 10                shl    $0x10,%eax
400b74:       89 c2                   mov    %eax,%edx
400b76:       8b 45 ec                mov    -0x14(%rbp),%eax
400b79:       c1 e0 08                shl    $0x8,%eax
400b7c:       01 c2                   add    %eax,%edx
400b7e:       8b 45 f0                mov    -0x10(%rbp),%eax
400b81:       01 d0                   add    %edx,%eax
400b83:       89 45 f4                mov    %eax,-0xc(%rbp)
400b86:       8b 45 e4                mov    -0x1c(%rbp),%eax
400b89:       8d 50 01                lea    0x1(%rax),%edx
400b8c:       89 55 e4                mov    %edx,-0x1c(%rbp)
400b8f:       48 63 d0                movslq %eax,%rdx
400b92:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400b96:       48 01 c2                add    %rax,%rdx
400b99:       8b 45 f4                mov    -0xc(%rbp),%eax
400b9c:       c1 e8 12                shr    $0x12,%eax
400b9f:       83 e0 3f                and    $0x3f,%eax
400ba2:       89 c0                   mov    %eax,%eax
```

```
400ba4:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bab:       88 02                   mov    %al,(%rdx)
400bad:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bb0:       8d 50 01                lea    0x1(%rax),%edx
400bb3:       89 55 e4                mov    %edx,-0x1c(%rbp)
400bb6:       48 63 d0                movslq %eax,%rdx
400bb9:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400bbd:       48 01 c2                add    %rax,%rdx
400bc0:       8b 45 f4                mov    -0xc(%rbp),%eax
400bc3:       c1 e8 0c                shr    $0xc,%eax
400bc6:       83 e0 3f                and    $0x3f,%eax
400bc9:       89 c0                   mov    %eax,%eax
400bcb:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bd2:       88 02                   mov    %al,(%rdx)
400bd4:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bd7:       8d 50 01                lea    0x1(%rax),%edx
400bda:       89 55 e4                mov    %edx,-0x1c(%rbp)
400bdd:       48 63 d0                movslq %eax,%rdx
400be0:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400be4:       48 01 c2                add    %rax,%rdx
400be7:       8b 45 f4                mov    -0xc(%rbp),%eax
400bea:       c1 e8 06                shr    $0x6,%eax
400bed:       83 e0 3f                and    $0x3f,%eax
400bf0:       89 c0                   mov    %eax,%eax
400bf2:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bf9:       88 02                   mov    %al,(%rdx)
400bfb:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bfe:       8d 50 01                lea    0x1(%rax),%edx
400c01:       89 55 e4                mov    %edx,-0x1c(%rbp)
400c04:       48 63 d0                movslq %eax,%rdx
400c07:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400c0b:       48 01 c2                add    %rax,%rdx
400c0e:       8b 45 f4                mov    -0xc(%rbp),%eax
400c11:       83 e0 3f                and    $0x3f,%eax
400c14:       89 c0                   mov    %eax,%eax
400c16:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400c1d:       88 02                   mov    %al,(%rdx)
400c1f:       8b 45 e0                mov    -0x20(%rbp),%eax
400c22:       48 98                   cltq
400c24:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400c28:       0f 82 b6 fe ff ff       jb     400ae4 <getlogin_r@plt+0x314>
400c2e:       c7 45 e0 00 00 00 00    movl   $0x0,-0x20(%rbp)
400c35:       eb 24                   jmp    400c5b <getlogin_r@plt+0x48b>
400c37:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400c3b:       48 8b 10                mov    (%rax),%rdx
400c3e:       8b 45 e0                mov    -0x20(%rbp),%eax
400c41:       48 98                   cltq
400c43:       48 29 c2                sub    %rax,%rdx
400c46:       48 89 d0                mov    %rdx,%rax
400c49:       48 8d 50 ff             lea    -0x1(%rax),%rdx
400c4d:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400c51:       48 01 d0                add    %rdx,%rax
400c54:       c6 00 3d                movb   $0x3d,(%rax)
```

```
  400c57:       83 45 e0 01             addl   $0x1,-0x20(%rbp)
  400c5b:       48 8b 4d d0             mov    -0x30(%rbp),%rcx
  400c5f:       48 ba ab aa aa aa aa    movabs $0xaaaaaaaaaaaaaaab,%rdx
  400c66:       aa aa aa
  400c69:       48 89 c8                mov    %rcx,%rax
  400c6c:       48 f7 e2                mul    %rdx
  400c6f:       48 d1 ea                shr    %rdx
  400c72:       48 89 d0                mov    %rdx,%rax
  400c75:       48 01 c0                add    %rax,%rax
  400c78:       48 01 d0                add    %rdx,%rax
  400c7b:       48 29 c1                sub    %rax,%rcx
  400c7e:       48 89 ca                mov    %rcx,%rdx
  400c81:       8b 04 95 00 21 60 00    mov    0x602100(,%rdx,4),%eax
  400c88:       3b 45 e0                cmp    -0x20(%rbp),%eax
  400c8b:       7f aa                   jg     400c37 <getlogin_r@plt+0x467>
  400c8d:       48 8b 45 f8             mov    -0x8(%rbp),%rax
  400c91:       c9                      leaveq
  400c92:       c3                      retq
  400c93:       66 2e 0f 1f 84 00 00    nopw   %cs:0x0(%rax,%rax,1)
  400c9a:       00 00 00
  400c9d:       0f 1f 00                nopl   (%rax)
  400ca0:       41 57                   push   %r15
  400ca2:       41 89 ff                mov    %edi,%r15d
  400ca5:       41 56                   push   %r14
  400ca7:       49 89 f6                mov    %rsi,%r14
  400caa:       41 55                   push   %r13
  400cac:       49 89 d5                mov    %rdx,%r13
  400caf:       41 54                   push   %r12
  400cb1:       4c 8d 25 48 11 20 00    lea    0x201148(%rip),%r12        # 601e0
0 <_fini+0x2010ec>
  400cb8:       55                      push   %rbp
  400cb9:       48 8d 2d 48 11 20 00    lea    0x201148(%rip),%rbp        # 601e0
8 <_fini+0x2010f4>
  400cc0:       53                      push   %rbx
  400cc1:       4c 29 e5                sub    %r12,%rbp
  400cc4:       31 db                   xor    %ebx,%ebx
  400cc6:       48 c1 fd 03             sar    $0x3,%rbp
  400cca:       48 83 ec 08             sub    $0x8,%rsp
  400cce:       e8 35 fa ff ff          callq  400708 <_init>
  400cd3:       48 85 ed                test   %rbp,%rbp
  400cd6:       74 1e                   je     400cf6 <getlogin_r@plt+0x526>
  400cd8:       0f 1f 84 00 00 00 00    nopl   0x0(%rax,%rax,1)
  400cdf:       00
  400ce0:       4c 89 ea                mov    %r13,%rdx
  400ce3:       4c 89 f6                mov    %r14,%rsi
  400ce6:       44 89 ff                mov    %r15d,%edi
  400ce9:       41 ff 14 dc             callq  *(%r12,%rbx,8)
  400ced:       48 83 c3 01             add    $0x1,%rbx
  400cf1:       48 39 eb                cmp    %rbp,%rbx
  400cf4:       75 ea                   jne    400ce0 <getlogin_r@plt+0x510>
  400cf6:       48 83 c4 08             add    $0x8,%rsp
  400cfa:       5b                      pop    %rbx
  400cfb:       5d                      pop    %rbp
```

```
  400cfc:       41 5c                   pop    %r12
  400cfe:       41 5d                   pop    %r13
  400d00:       41 5e                   pop    %r14
  400d02:       41 5f                   pop    %r15
  400d04:       c3                      retq
  400d05:       66 66 2e 0f 1f 84 00    data32 nopw %cs:0x0(%rax,%rax,1)
  400d0c:       00 00 00 00
  400d10:       f3 c3                   repz retq

Disassembly of section .fini:

0000000000400d14 <_fini>:
  400d14:       48 83 ec 08             sub    $0x8,%rsp
  400d18:       48 83 c4 08             add    $0x8,%rsp
  400d1c:       c3                      retq
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s 4

Symbol table '.dynsym' contains 19 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMClone
Tab
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND puts@GLIBC_2.2.5 (2)
     3: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND secretoperation
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strlen@GLIBC_2.2.5 (2)
     5: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __stack_chk_fail@GLIBC
_2.4 (3)
     6: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND printf@GLIBC_2.2.5 (2)
     7: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __assert_fail@GLIBC_2.
2.5 (2)
     8: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@GLIB
C_2.2.5 (2)
     9: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND calloc@GLIBC_2.2.5 (2)
    10: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
    11: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND getlogin_r@GLIBC_2.2.5
 (2)
    12: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
    13: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTa
ble
    14: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   24 _edata
    15: 0000000000602110     0 NOTYPE  GLOBAL DEFAULT   25 _end
    16: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   25 __bss_start
    17: 0000000000400708     0 FUNC    GLOBAL DEFAULT   11 _init
    18: 0000000000400d14     0 FUNC    GLOBAL DEFAULT   14 _fini
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -c -fPIC hello.c -o hello.o
gcc: error: hello.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -c -fPIC lib361.c -o lib361.o
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  lib361.c  lib361.o  lib361.so  secrets.txt
```

```
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf lib361.so
Usage: readelf <option(s)> elf-file(s)
 Display information about the contents of ELF format files
 Options are:
  -a --all               Equivalent to: -h -l -S -s -r -d -V -A -I
  -h --file-header       Display the ELF file header
  -l --program-headers   Display the program headers
     --segments          An alias for --program-headers
  -S --section-headers   Display the sections' header
     --sections          An alias for --section-headers
  -g --section-groups    Display the section groups
  -t --section-details   Display the section details
  -e --headers           Equivalent to: -h -l -S
  -s --syms              Display the symbol table
     --symbols           An alias for --syms
  --dyn-syms             Display the dynamic symbol table
  -n --notes             Display the core notes (if present)
  -r --relocs            Display the relocations (if present)
  -u --unwind            Display the unwind info (if present)
  -d --dynamic           Display the dynamic section (if present)
  -V --version-info      Display the version sections (if present)
  -A --arch-specific     Display architecture specific information (if any)
  -c --archive-index     Display the symbol/file index in an archive
  -D --use-dynamic       Use the dynamic section info when displaying symbols
  -x --hex-dump=<number|name>
                         Dump the contents of section <number|name> as bytes
  -p --string-dump=<number|name>
                         Dump the contents of section <number|name> as strings
  -R --relocated-dump=<number|name>
                         Dump the contents of section <number|name> as relocated
bytes
  -w[lLiaprmfFsoRt] or
  --debug-dump[=rawline,=decodedline,=info,=abbrev,=pubnames,=aranges,=macro,=fra
mes,
               =frames-interp,=str,=loc,=Ranges,=pubtypes,
               =gdb_index,=trace_info,=trace_abbrev,=trace_aranges,
               =addr,=cu_index]
                         Display the contents of DWARF2 debug sections
  --dwarf-depth=N        Do not display DIEs at depth N or greater
  --dwarf-start=N        Display DIEs starting with N, at the same depth
                         or deeper
  -I --histogram         Display histogram of bucket list lengths
  -W --wide              Allow output width to exceed 80 characters
  @<file>                Read options from <file>
  -H --help              Display this information
  -v --version           Display the version number of readelf
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s lib361.so

Symbol table '.dynsym' contains 31 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000a10     0 SECTION LOCAL  DEFAULT    9
     2: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMClone
```

```
Tab
     3: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
     4: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
     5: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTa
ble
     6: 0000000000000000     0 FUNC    WEAK   DEFAULT  UND __cxa_finalize@GLIBC_2
.2.5 (2)
     7: 000000000020214c     0 NOTYPE  GLOBAL DEFAULT   24 _edata
     8: 0000000000202158     0 NOTYPE  GLOBAL DEFAULT   25 _end
     9: 000000000020214c     0 NOTYPE  GLOBAL DEFAULT   25 __bss_start
    10: 0000000000000a10     0 FUNC    GLOBAL DEFAULT    9 _init
    11: 0000000000001154     0 FUNC    GLOBAL DEFAULT   12 _fini
    12: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
    13: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND rt__
    14: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND s_start@GLIBC_2.2.5 (2
)
    15: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND terClasses
    16: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND rTMCloneTable@GLIBC_2.
2.5 (2)
    17: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND rtreadelf: Error: bad
dynamic symbol

    18: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND _ITM_deregisterTMClone
Tab@GLIBC_2.2.5 (2)
    19: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND .5@GLIBC_2.2.5 (2)
    20: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND on_start__@GLIBC_2.2.5
 (2)
    21: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND registerTMCloneTable@G
LIBC_2.2.5 (2)
    22: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND sterTMCloneTable
    23: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND eTable@GLIBC_2.2.5 (2)
    24: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND e
    25: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND neTable
    26: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   24 isterClasses
    27: 0000000000602110     0 NOTYPE  GLOBAL DEFAULT   25 egisterTMCloneTable
    28: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   25 asses
    29: 0000000000400708     0 FUNC    GLOBAL DEFAULT   11 _RegisterClasses
    30: 0000000000400d14     0 FUNC    GLOBAL DEFAULT   14 so.6

Symbol table '.symtab' contains 54 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000238     0 SECTION LOCAL  DEFAULT    1
     2: 0000000000000280     0 SECTION LOCAL  DEFAULT    2
     3: 00000000000002f0     0 SECTION LOCAL  DEFAULT    3
     4: 00000000000005d8     0 SECTION LOCAL  DEFAULT    4
     5: 000000000000078a     0 SECTION LOCAL  DEFAULT    5
     6: 00000000000007c8     0 SECTION LOCAL  DEFAULT    6
     7: 0000000000000818     0 SECTION LOCAL  DEFAULT    7
     8: 00000000000008f0     0 SECTION LOCAL  DEFAULT    8
     9: 0000000000000a10     0 SECTION LOCAL  DEFAULT    9
    10: 0000000000000a50     0 SECTION LOCAL  DEFAULT   10
    11: 0000000000000b30     0 SECTION LOCAL  DEFAULT   11
```

```
    12: 0000000000001154     0 SECTION LOCAL  DEFAULT   12
    13: 0000000000001168     0 SECTION LOCAL  DEFAULT   13
    14: 0000000000001227     0 SECTION LOCAL  DEFAULT   14
    15: 0000000000001244     0 SECTION LOCAL  DEFAULT   15
    16: 0000000000001264     0 SECTION LOCAL  DEFAULT   16
    17: 00000000000012a8     0 SECTION LOCAL  DEFAULT   17
    18: 0000000000201c00     0 SECTION LOCAL  DEFAULT   18
    19: 0000000000201c10     0 SECTION LOCAL  DEFAULT   19
    20: 0000000000201c20     0 SECTION LOCAL  DEFAULT   20
    21: 0000000000201c30     0 SECTION LOCAL  DEFAULT   21
    22: 0000000000201fd0     0 SECTION LOCAL  DEFAULT   22
    23: 0000000000202000     0 SECTION LOCAL  DEFAULT   23
    24: 00000000002020a0     0 SECTION LOCAL  DEFAULT   24
    25: 000000000020214c     0 SECTION LOCAL  DEFAULT   25
    26: 0000000000000000     0 SECTION LOCAL  DEFAULT   26
    27: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    28: 0000000000201c20     0 OBJECT  LOCAL  DEFAULT   20 __JCR_LIST__
    29: 0000000000000b30     0 FUNC    LOCAL  DEFAULT   11 deregister_tm_clones
    30: 0000000000000b60     0 FUNC    LOCAL  DEFAULT   11 register_tm_clones
    31: 0000000000000ba0     0 FUNC    LOCAL  DEFAULT   11 __do_global_dtors_aux
    32: 000000000020214c     1 OBJECT  LOCAL  DEFAULT   25 completed.6973
    33: 0000000000201c10     0 OBJECT  LOCAL  DEFAULT   19 __do_global_dtors_aux_
fin
    34: 0000000000000be0     0 FUNC    LOCAL  DEFAULT   11 frame_dummy
    35: 0000000000201c00     0 OBJECT  LOCAL  DEFAULT   18 __frame_dummy_init_arr
ay_
    36: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    37: 0000000000001424     0 OBJECT  LOCAL  DEFAULT   17 __FRAME_END__
    38: 0000000000201c28     0 OBJECT  LOCAL  DEFAULT   20 __JCR_END__
    39: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS
    40: 00000000002020a0     0 OBJECT  LOCAL  DEFAULT   24 __dso_handle
    41: 0000000000201c30     0 OBJECT  LOCAL  DEFAULT   21 _DYNAMIC
    42: 0000000000202150     0 OBJECT  LOCAL  DEFAULT   24 __TMC_END__
    43: 0000000000202000     0 OBJECT  LOCAL  DEFAULT   23 _GLOBAL_OFFSET_TABLE_
    44: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMClone
Tab
    45: 000000000020214c     0 NOTYPE  GLOBAL DEFAULT   24 _edata
    46: 0000000000001154     0 FUNC    GLOBAL DEFAULT   12 _fini
    47: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
    48: 0000000000202158     0 NOTYPE  GLOBAL DEFAULT   25 _end
    49: 000000000020214c     0 NOTYPE  GLOBAL DEFAULT   25 __bss_start
    50: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
    51: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTa
ble
    52: 0000000000000000     0 FUNC    WEAK   DEFAULT  UND __cxa_finalize@@GLIBC_
2.2
    53: 0000000000000a10     0 FUNC    GLOBAL DEFAULT    9 _init
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  lib361.c  lib361.o  lib361.so  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ rm lib361.o lib361.so
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  lib361.c  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o libhello.so -fPIC hello.c
```

```
gcc: error: hello.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -s lib361.so

Symbol table '.dynsym' contains 13 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000548     0 SECTION LOCAL  DEFAULT    9
     2: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMClone
Tab
     3: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
     4: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
     5: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTa
ble
     6: 0000000000000000     0 FUNC    WEAK   DEFAULT  UND __cxa_finalize@GLIBC_2
.2.5 (2)
     7: 0000000000201030     0 NOTYPE  GLOBAL DEFAULT   21 _edata
     8: 0000000000201038     0 NOTYPE  GLOBAL DEFAULT   22 _end
     9: 0000000000201030     0 NOTYPE  GLOBAL DEFAULT   22 __bss_start
    10: 0000000000000548     0 FUNC    GLOBAL DEFAULT    9 _init
    11: 0000000000000685     6 FUNC    GLOBAL DEFAULT   11 secretoperation
    12: 000000000000068c     0 FUNC    GLOBAL DEFAULT   12 _fini

Symbol table '.symtab' contains 53 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000000001c8     0 SECTION LOCAL  DEFAULT    1
     2: 00000000000001f0     0 SECTION LOCAL  DEFAULT    2
     3: 0000000000000230     0 SECTION LOCAL  DEFAULT    3
     4: 0000000000000368     0 SECTION LOCAL  DEFAULT    4
     5: 000000000000041c     0 SECTION LOCAL  DEFAULT    5
     6: 0000000000000438     0 SECTION LOCAL  DEFAULT    6
     7: 0000000000000458     0 SECTION LOCAL  DEFAULT    7
     8: 0000000000000518     0 SECTION LOCAL  DEFAULT    8
     9: 0000000000000548     0 SECTION LOCAL  DEFAULT    9
    10: 0000000000000570     0 SECTION LOCAL  DEFAULT   10
    11: 00000000000005a0     0 SECTION LOCAL  DEFAULT   11
    12: 000000000000068c     0 SECTION LOCAL  DEFAULT   12
    13: 0000000000000698     0 SECTION LOCAL  DEFAULT   13
    14: 00000000000006b8     0 SECTION LOCAL  DEFAULT   14
    15: 0000000000200e00     0 SECTION LOCAL  DEFAULT   15
    16: 0000000000200e08     0 SECTION LOCAL  DEFAULT   16
    17: 0000000000200e10     0 SECTION LOCAL  DEFAULT   17
    18: 0000000000200e18     0 SECTION LOCAL  DEFAULT   18
    19: 0000000000200fd8     0 SECTION LOCAL  DEFAULT   19
    20: 0000000000201000     0 SECTION LOCAL  DEFAULT   20
    21: 0000000000201028     0 SECTION LOCAL  DEFAULT   21
    22: 0000000000201030     0 SECTION LOCAL  DEFAULT   22
    23: 0000000000000000     0 SECTION LOCAL  DEFAULT   23
    24: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    25: 0000000000200e10     0 OBJECT  LOCAL  DEFAULT   17 __JCR_LIST__
```

```
    26: 00000000000005a0     0 FUNC    LOCAL  DEFAULT   11 deregister_tm_clones
    27: 00000000000005d0     0 FUNC    LOCAL  DEFAULT   11 register_tm_clones
    28: 0000000000000610     0 FUNC    LOCAL  DEFAULT   11 __do_global_dtors_aux
    29: 0000000000201030     1 OBJECT  LOCAL  DEFAULT   22 completed.6973
    30: 0000000000200e08     0 OBJECT  LOCAL  DEFAULT   16 __do_global_dtors_aux_
fin
    31: 0000000000000650     0 FUNC    LOCAL  DEFAULT   11 frame_dummy
    32: 0000000000200e00     0 OBJECT  LOCAL  DEFAULT   15 __frame_dummy_init_arr
ay_
    33: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS lib361.c
    34: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    35: 0000000000000718     0 OBJECT  LOCAL  DEFAULT   14 __FRAME_END__
    36: 0000000000200e10     0 OBJECT  LOCAL  DEFAULT   17 __JCR_END__
    37: 0000000000000000     0 FILE    LOCAL  DEFAULT  ABS
    38: 0000000000201028     0 OBJECT  LOCAL  DEFAULT   21 __dso_handle
    39: 0000000000200e18     0 OBJECT  LOCAL  DEFAULT   18 _DYNAMIC
    40: 0000000000201030     0 OBJECT  LOCAL  DEFAULT   21 __TMC_END__
    41: 0000000000201000     0 OBJECT  LOCAL  DEFAULT   20 _GLOBAL_OFFSET_TABLE_
    42: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMClone
Tab
    43: 0000000000201030     0 NOTYPE  GLOBAL DEFAULT   21 _edata
    44: 0000000000000685     6 FUNC    GLOBAL DEFAULT   11 secretoperation
    45: 000000000000068c     0 FUNC    GLOBAL DEFAULT   12 _fini
    46: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
    47: 0000000000201038     0 NOTYPE  GLOBAL DEFAULT   22 _end
    48: 0000000000201030     0 NOTYPE  GLOBAL DEFAULT   22 __bss_start
    49: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
    50: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTa
ble
    51: 0000000000000000     0 FUNC    WEAK   DEFAULT  UND __cxa_finalize@@GLIBC_
2.2
    52: 0000000000000548     0 FUNC    GLOBAL DEFAULT    9 _init
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  lib361.c  lib361.so  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ strings 4
/lib64/ld-linux-x86-64.so.2
lib361.so
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
```

```
_init
secretoperation
_fini
libc.so.6
puts
__stack_chk_fail
__assert_fail
printf
calloc
strlen
getlogin_r
__libc_start_main
_edata
__bss_start
_end
GLIBC_2.4
GLIBC_2.2.5
dH34%(
[]A\A]A^A_
34567890123456789012
%s%s
you win! the secret is:
bangarang
this program tests the implementation of a dynamically linked library.
get_sum.c
result == 10
result == 4
main
;*3$"
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
GCC: (Ubuntu 4.8.4-2ubuntu1~14.04) 4.8.4
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.jcr
.dynamic
```

```
.got
.got.plt
.data
.bss
.comment
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  lib361.c  lib361.so  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
lib361.c: In function ‘secretoperation’:
lib361.c:3:35: error: expected ‘;’ before ‘}’ token
 int secretoperation() { return 10 }
                                   ^
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ strace ./4
execve("./4", ["./4"], [/* 20 vars */]) = 0
brk(0)                                  = 0x1897000
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f76
f1a6c000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=25058, ...}) = 0
mmap(NULL, 25058, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f76f1a65000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/tls/x86_64/lib361.so", O_RDONLY|O_CLOEXEC) = -1 ENOEN
T (No such file or directory)
stat("/lib/x86_64-linux-gnu/tls/x86_64", 0x7fffd5ddb150) = -1 ENOENT (No such fil
e or directory)
open("/lib/x86_64-linux-gnu/tls/lib361.so", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No s
uch file or directory)
stat("/lib/x86_64-linux-gnu/tls", 0x7fffd5ddb150) = -1 ENOENT (No such file or di
```

```
rectory)
open("/lib/x86_64-linux-gnu/x86_64/lib361.so", O_RDONLY|O_CLOEXEC) = -1 ENOENT (N
o such file or directory)
stat("/lib/x86_64-linux-gnu/x86_64", 0x7fffd5ddb150) = -1 ENOENT (No such file or
 directory)
open("/lib/x86_64-linux-gnu/lib361.so", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\240\5\0\0\0\0\0\0"..., 83
2) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=7868, ...}) = 0
mmap(NULL, 2101304, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f7
6f164a000
mprotect(0x7f76f164b000, 2093056, PROT_NONE) = 0
mmap(0x7f76f184a000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWR
ITE, 3, 0) = 0x7f76f184a000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\320\37\2\0\0\0\0\0"..., 8
32) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=1840928, ...}) = 0
mmap(NULL, 3949248, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f7
6f1285000
mprotect(0x7f76f1440000, 2093056, PROT_NONE) = 0
mmap(0x7f76f163f000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYW
RITE, 3, 0x1ba000) = 0x7f76f163f000
mmap(0x7f76f1645000, 17088, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONY
MOUS, -1, 0) = 0x7f76f1645000
close(3)                                = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f76
f1a64000
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f76
f1a62000
arch_prctl(ARCH_SET_FS, 0x7f76f1a62740) = 0
mprotect(0x7f76f163f000, 16384, PROT_READ) = 0
mprotect(0x7f76f184a000, 4096, PROT_READ) = 0
mprotect(0x601000, 4096, PROT_READ)     = 0
mprotect(0x7f76f1a6e000, 4096, PROT_READ) = 0
munmap(0x7f76f1a65000, 25058)           = 0
fstat(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f76
f1a6b000
write(1, "this program tests the implement"..., 71this program tests the implemen
tation of a dynamically linked library.
) = 71
brk(0)                                  = 0x1897000
brk(0x18b8000)                          = 0x18b8000
write(2, "4: get_sum.c:20: main: Assertion"..., 554: get_sum.c:20: main: Assertio
n `result == 4' failed.
) = 55
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f76
f1a6a000
rt_sigprocmask(SIG_UNBLOCK, [ABRT], NULL, 8) = 0
gettid()                                = 22989
```

```
tgkill(22989, 22989, SIGABRT)           = 0
--- SIGABRT {si_signo=SIGABRT, si_code=SI_TKILL, si_pid=22989, si_uid=1000} ---
+++ killed by SIGABRT (core dumped) +++
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
lib361.c:5:1: error: expected identifier or ‘(’ before ‘return’
 return 4;
 ^
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
lib361.c:5:1: error: expected ‘,’ or ‘;’ before ‘int’
 int secretoperation() { return num; }
 ^
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
lib361.c: In function ‘secretoperation’:
lib361.c:5:25: warning: return makes integer from pointer without a cast [enabled
 by default]
 int secretoperation() { return num; }
                         ^
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -d 4

4:     file format elf64-x86-64


Disassembly of section .init:
```

```
0000000000400708 <_init>:
  400708:       48 83 ec 08             sub    $0x8,%rsp
  40070c:       48 8b 05 e5 18 20 00    mov    0x2018e5(%rip),%rax        # 601ff
8 <_fini+0x2012e4>
  400713:       48 85 c0                test   %rax,%rax
  400716:       74 05                   je     40071d <_init+0x15>
  400718:       e8 a3 00 00 00          callq  4007c0 <__gmon_start__@plt>
  40071d:       48 83 c4 08             add    $0x8,%rsp
  400721:       c3                      retq

Disassembly of section .plt:

0000000000400730 <puts@plt-0x10>:
  400730:       ff 35 d2 18 20 00       pushq  0x2018d2(%rip)        # 602008 <_f
ini+0x2012f4>
  400736:       ff 25 d4 18 20 00       jmpq   *0x2018d4(%rip)        # 602010 <_
fini+0x2012fc>
  40073c:       0f 1f 40 00             nopl   0x0(%rax)

0000000000400740 <puts@plt>:
  400740:       ff 25 d2 18 20 00       jmpq   *0x2018d2(%rip)        # 602018 <_
fini+0x201304>
  400746:       68 00 00 00 00          pushq  $0x0
  40074b:       e9 e0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400750 <secretoperation@plt>:
  400750:       ff 25 ca 18 20 00       jmpq   *0x2018ca(%rip)        # 602020 <_
fini+0x20130c>
  400756:       68 01 00 00 00          pushq  $0x1
  40075b:       e9 d0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400760 <strlen@plt>:
  400760:       ff 25 c2 18 20 00       jmpq   *0x2018c2(%rip)        # 602028 <_
fini+0x201314>
  400766:       68 02 00 00 00          pushq  $0x2
  40076b:       e9 c0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400770 <__stack_chk_fail@plt>:
  400770:       ff 25 ba 18 20 00       jmpq   *0x2018ba(%rip)        # 602030 <_
fini+0x20131c>
  400776:       68 03 00 00 00          pushq  $0x3
  40077b:       e9 b0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400780 <printf@plt>:
  400780:       ff 25 b2 18 20 00       jmpq   *0x2018b2(%rip)        # 602038 <_
fini+0x201324>
  400786:       68 04 00 00 00          pushq  $0x4
  40078b:       e9 a0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400790 <__assert_fail@plt>:
  400790:       ff 25 aa 18 20 00       jmpq   *0x2018aa(%rip)        # 602040 <_
fini+0x20132c>
```

```
  400796:       68 05 00 00 00          pushq  $0x5
  40079b:       e9 90 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007a0 <__libc_start_main@plt>:
  4007a0:       ff 25 a2 18 20 00       jmpq   *0x2018a2(%rip)        # 602048 <_
fini+0x201334>
  4007a6:       68 06 00 00 00          pushq  $0x6
  4007ab:       e9 80 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007b0 <calloc@plt>:
  4007b0:       ff 25 9a 18 20 00       jmpq   *0x20189a(%rip)        # 602050 <_
fini+0x20133c>
  4007b6:       68 07 00 00 00          pushq  $0x7
  4007bb:       e9 70 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007c0 <__gmon_start__@plt>:
  4007c0:       ff 25 92 18 20 00       jmpq   *0x201892(%rip)        # 602058 <_
fini+0x201344>
  4007c6:       68 08 00 00 00          pushq  $0x8
  4007cb:       e9 60 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007d0 <getlogin_r@plt>:
  4007d0:       ff 25 8a 18 20 00       jmpq   *0x20188a(%rip)        # 602060 <_
fini+0x20134c>
  4007d6:       68 09 00 00 00          pushq  $0x9
  4007db:       e9 50 ff ff ff          jmpq   400730 <_init+0x28>

Disassembly of section .text:

00000000004007e0 <.text>:
  4007e0:       31 ed                   xor    %ebp,%ebp
  4007e2:       49 89 d1                mov    %rdx,%r9
  4007e5:       5e                      pop    %rsi
  4007e6:       48 89 e2                mov    %rsp,%rdx
  4007e9:       48 83 e4 f0             and    $0xfffffffffffffff0,%rsp
  4007ed:       50                      push   %rax
  4007ee:       54                      push   %rsp
  4007ef:       49 c7 c0 10 0d 40 00    mov    $0x400d10,%r8
  4007f6:       48 c7 c1 a0 0c 40 00    mov    $0x400ca0,%rcx
  4007fd:       48 c7 c7 cd 08 40 00    mov    $0x4008cd,%rdi
  400804:       e8 97 ff ff ff          callq  4007a0 <__libc_start_main@plt>
  400809:       f4                      hlt
  40080a:       66 0f 1f 44 00 00       nopw   0x0(%rax,%rax,1)
  400810:       b8 17 21 60 00          mov    $0x602117,%eax
  400815:       55                      push   %rbp
  400816:       48 2d 10 21 60 00       sub    $0x602110,%rax
  40081c:       48 83 f8 0e             cmp    $0xe,%rax
  400820:       48 89 e5                mov    %rsp,%rbp
  400823:       77 02                   ja     400827 <getlogin_r@plt+0x57>
  400825:       5d                      pop    %rbp
  400826:       c3                      retq
  400827:       b8 00 00 00 00          mov    $0x0,%eax
  40082c:       48 85 c0                test   %rax,%rax
```

```
  40082f:       74 f4                   je     400825 <getlogin_r@plt+0x55>
  400831:       5d                      pop    %rbp
  400832:       bf 10 21 60 00          mov    $0x602110,%edi
  400837:       ff e0                   jmpq   *%rax
  400839:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400840:       b8 10 21 60 00          mov    $0x602110,%eax
  400845:       55                      push   %rbp
  400846:       48 2d 10 21 60 00       sub    $0x602110,%rax
  40084c:       48 c1 f8 03             sar    $0x3,%rax
  400850:       48 89 e5                mov    %rsp,%rbp
  400853:       48 89 c2                mov    %rax,%rdx
  400856:       48 c1 ea 3f             shr    $0x3f,%rdx
  40085a:       48 01 d0                add    %rdx,%rax
  40085d:       48 d1 f8                sar    %rax
  400860:       75 02                   jne    400864 <getlogin_r@plt+0x94>
  400862:       5d                      pop    %rbp
  400863:       c3                      retq
  400864:       ba 00 00 00 00          mov    $0x0,%edx
  400869:       48 85 d2                test   %rdx,%rdx
  40086c:       74 f4                   je     400862 <getlogin_r@plt+0x92>
  40086e:       5d                      pop    %rbp
  40086f:       48 89 c6                mov    %rax,%rsi
  400872:       bf 10 21 60 00          mov    $0x602110,%edi
  400877:       ff e2                   jmpq   *%rdx
  400879:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400880:       80 3d 85 18 20 00 00    cmpb   $0x0,0x201885(%rip)        # 60210
c <_edata>
  400887:       75 11                   jne    40089a <getlogin_r@plt+0xca>
  400889:       55                      push   %rbp
  40088a:       48 89 e5                mov    %rsp,%rbp
  40088d:       e8 7e ff ff ff          callq  400810 <getlogin_r@plt+0x40>
  400892:       5d                      pop    %rbp
  400893:       c6 05 72 18 20 00 01    movb   $0x1,0x201872(%rip)        # 60210
c <_edata>
  40089a:       f3 c3                   repz retq
  40089c:       0f 1f 40 00             nopl   0x0(%rax)
  4008a0:       48 83 3d 68 15 20 00    cmpq   $0x0,0x201568(%rip)        # 601e1
0 <_fini+0x2010fc>
  4008a7:       00
  4008a8:       74 1e                   je     4008c8 <getlogin_r@plt+0xf8>
  4008aa:       b8 00 00 00 00          mov    $0x0,%eax
  4008af:       48 85 c0                test   %rax,%rax
  4008b2:       74 14                   je     4008c8 <getlogin_r@plt+0xf8>
  4008b4:       55                      push   %rbp
  4008b5:       bf 10 1e 60 00          mov    $0x601e10,%edi
  4008ba:       48 89 e5                mov    %rsp,%rbp
  4008bd:       ff d0                   callq  *%rax
  4008bf:       5d                      pop    %rbp
  4008c0:       e9 7b ff ff ff          jmpq   400840 <getlogin_r@plt+0x70>
  4008c5:       0f 1f 00                nopl   (%rax)
  4008c8:       e9 73 ff ff ff          jmpq   400840 <getlogin_r@plt+0x70>
  4008cd:       55                      push   %rbp
  4008ce:       48 89 e5                mov    %rsp,%rbp
```

```
  4008d1:       48 83 ec 10             sub    $0x10,%rsp
  4008d5:       c7 45 f4 01 00 00 00    movl   $0x1,-0xc(%rbp)
  4008dc:       c7 45 f8 02 00 00 00    movl   $0x2,-0x8(%rbp)
  4008e3:       c7 45 fc 00 00 00 00    movl   $0x0,-0x4(%rbp)
  4008ea:       bf 70 0d 40 00          mov    $0x400d70,%edi
  4008ef:       e8 4c fe ff ff          callq  400740 <puts@plt>
  4008f4:       be 06 00 00 00          mov    $0x6,%esi
  4008f9:       bf 03 00 00 00          mov    $0x3,%edi
  4008fe:       e8 4d fe ff ff          callq  400750 <secretoperation@plt>
  400903:       89 45 fc                mov    %eax,-0x4(%rbp)
  400906:       83 7d fc 0a             cmpl   $0xa,-0x4(%rbp)
  40090a:       74 19                   je     400925 <getlogin_r@plt+0x155>
  40090c:       b9 da 0d 40 00          mov    $0x400dda,%ecx
  400911:       ba 12 00 00 00          mov    $0x12,%edx
  400916:       be b7 0d 40 00          mov    $0x400db7,%esi
  40091b:       bf c1 0d 40 00          mov    $0x400dc1,%edi
  400920:       e8 6b fe ff ff          callq  400790 <__assert_fail@plt>
  400925:       8b 55 f8                mov    -0x8(%rbp),%edx
  400928:       8b 45 f4                mov    -0xc(%rbp),%eax
  40092b:       89 d6                   mov    %edx,%esi
  40092d:       89 c7                   mov    %eax,%edi
  40092f:       e8 1c fe ff ff          callq  400750 <secretoperation@plt>
  400934:       89 45 fc                mov    %eax,-0x4(%rbp)
  400937:       83 7d fc 04             cmpl   $0x4,-0x4(%rbp)
  40093b:       74 19                   je     400956 <getlogin_r@plt+0x186>
  40093d:       b9 da 0d 40 00          mov    $0x400dda,%ecx
  400942:       ba 14 00 00 00          mov    $0x14,%edx
  400947:       be b7 0d 40 00          mov    $0x400db7,%esi
  40094c:       bf ce 0d 40 00          mov    $0x400dce,%edi
  400951:       e8 3a fe ff ff          callq  400790 <__assert_fail@plt>
  400956:       48 8b 05 33 17 20 00    mov    0x201733(%rip),%rax        # 60209
0 <_fini+0x20137c>
  40095d:       48 89 c7                mov    %rax,%rdi
  400960:       e8 28 00 00 00          callq  40098d <getlogin_r@plt+0x1bd>
  400965:       48 89 c2                mov    %rax,%rdx
  400968:       48 8b 0d 31 17 20 00    mov    0x201731(%rip),%rcx        # 6020a
0 <_fini+0x20138c>
  40096f:       48 8b 05 22 17 20 00    mov    0x201722(%rip),%rax        # 60209
8 <_fini+0x201384>
  400976:       48 89 ce                mov    %rcx,%rsi
  400979:       48 89 c7                mov    %rax,%rdi
  40097c:       b8 00 00 00 00          mov    $0x0,%eax
  400981:       e8 fa fd ff ff          callq  400780 <printf@plt>
  400986:       b8 00 00 00 00          mov    $0x0,%eax
  40098b:       c9                      leaveq
  40098c:       c3                      retq
  40098d:       55                      push   %rbp
  40098e:       48 89 e5                mov    %rsp,%rbp
  400991:       53                      push   %rbx
  400992:       48 81 ec 38 04 00 00    sub    $0x438,%rsp
  400999:       48 89 bd c8 fb ff ff    mov    %rdi,-0x438(%rbp)
  4009a0:       64 48 8b 04 25 28 00    mov    %fs:0x28,%rax
  4009a7:       00 00
```

```
4009a9:       48 89 45 e8             mov    %rax,-0x18(%rbp)
4009ad:       31 c0                   xor    %eax,%eax
4009af:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
4009b6:       be 00 04 00 00          mov    $0x400,%esi
4009bb:       48 89 c7                mov    %rax,%rdi
4009be:       e8 0d fe ff ff          callq  4007d0 <getlogin_r@plt>
4009c3:       c7 85 d4 fb ff ff 00    movl   $0x0,-0x42c(%rbp)
4009ca:       00 00 00
4009cd:       eb 3e                   jmp    400a0d <getlogin_r@plt+0x23d>
4009cf:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
4009d5:       48 98                   cltq
4009d7:       0f b6 94 05 e0 fb ff    movzbl -0x420(%rbp,%rax,1),%edx
4009de:       ff
4009df:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
4009e5:       48 63 c8                movslq %eax,%rcx
4009e8:       48 8b 85 c8 fb ff ff    mov    -0x438(%rbp),%rax
4009ef:       48 01 c8                add    %rcx,%rax
4009f2:       0f b6 00                movzbl (%rax),%eax
4009f5:       31 c2                   xor    %eax,%edx
4009f7:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
4009fd:       48 98                   cltq
4009ff:       88 94 05 e0 fb ff ff    mov    %dl,-0x420(%rbp,%rax,1)
400a06:       83 85 d4 fb ff ff 01    addl   $0x1,-0x42c(%rbp)
400a0d:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
400a13:       48 63 d8                movslq %eax,%rbx
400a16:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
400a1d:       48 89 c7                mov    %rax,%rdi
400a20:       e8 3b fd ff ff          callq  400760 <strlen@plt>
400a25:       48 39 c3                cmp    %rax,%rbx
400a28:       72 a5                   jb     4009cf <getlogin_r@plt+0x1ff>
400a2a:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
400a30:       48 63 c8                movslq %eax,%rcx
400a33:       48 8d 95 d8 fb ff ff    lea    -0x428(%rbp),%rdx
400a3a:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
400a41:       48 89 ce                mov    %rcx,%rsi
400a44:       48 89 c7                mov    %rax,%rdi
400a47:       e8 1e 00 00 00          callq  400a6a <getlogin_r@plt+0x29a>
400a4c:       48 8b 75 e8             mov    -0x18(%rbp),%rsi
400a50:       64 48 33 34 25 28 00    xor    %fs:0x28,%rsi
400a57:       00 00
400a59:       74 05                   je     400a60 <getlogin_r@plt+0x290>
400a5b:       e8 10 fd ff ff          callq  400770 <__stack_chk_fail@plt>
400a60:       48 81 c4 38 04 00 00    add    $0x438,%rsp
400a67:       5b                      pop    %rbx
400a68:       5d                      pop    %rbp
400a69:       c3                      retq
400a6a:       55                      push   %rbp
400a6b:       48 89 e5                mov    %rsp,%rbp
400a6e:       48 83 ec 40             sub    $0x40,%rsp
400a72:       48 89 7d d8             mov    %rdi,-0x28(%rbp)
400a76:       48 89 75 d0             mov    %rsi,-0x30(%rbp)
400a7a:       48 89 55 c8             mov    %rdx,-0x38(%rbp)
400a7e:       48 8b 45 d0             mov    -0x30(%rbp),%rax
```

```
400a82:       48 83 c0 02             add    $0x2,%rax
400a86:       48 ba ab aa aa aa aa    movabs $0xaaaaaaaaaaaaaaab,%rdx
400a8d:       aa aa aa
400a90:       48 f7 e2                mul    %rdx
400a93:       48 89 d0                mov    %rdx,%rax
400a96:       48 d1 e8                shr    %rax
400a99:       48 8d 14 85 00 00 00    lea    0x0(,%rax,4),%rdx
400aa0:       00
400aa1:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400aa5:       48 89 10                mov    %rdx,(%rax)
400aa8:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400aac:       48 8b 00                mov    (%rax),%rax
400aaf:       be 01 00 00 00          mov    $0x1,%esi
400ab4:       48 89 c7                mov    %rax,%rdi
400ab7:       e8 f4 fc ff ff          callq  4007b0 <calloc@plt>
400abc:       48 89 45 f8             mov    %rax,-0x8(%rbp)
400ac0:       48 83 7d f8 00          cmpq   $0x0,-0x8(%rbp)
400ac5:       75 0a                   jne    400ad1 <getlogin_r@plt+0x301>
400ac7:       b8 00 00 00 00          mov    $0x0,%eax
400acc:       e9 c0 01 00 00          jmpq   400c91 <getlogin_r@plt+0x4c1>
400ad1:       c7 45 e0 00 00 00 00    movl   $0x0,-0x20(%rbp)
400ad8:       c7 45 e4 00 00 00 00    movl   $0x0,-0x1c(%rbp)
400adf:       e9 3b 01 00 00          jmpq   400c1f <getlogin_r@plt+0x44f>
400ae4:       8b 45 e0                mov    -0x20(%rbp),%eax
400ae7:       48 98                   cltq
400ae9:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400aed:       73 1b                   jae    400b0a <getlogin_r@plt+0x33a>
400aef:       8b 45 e0                mov    -0x20(%rbp),%eax
400af2:       8d 50 01                lea    0x1(%rax),%edx
400af5:       89 55 e0                mov    %edx,-0x20(%rbp)
400af8:       48 63 d0                movslq %eax,%rdx
400afb:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400aff:       48 01 d0                add    %rdx,%rax
400b02:       0f b6 00                movzbl (%rax),%eax
400b05:       0f b6 c0                movzbl %al,%eax
400b08:       eb 05                   jmp    400b0f <getlogin_r@plt+0x33f>
400b0a:       b8 00 00 00 00          mov    $0x0,%eax
400b0f:       89 45 e8                mov    %eax,-0x18(%rbp)
400b12:       8b 45 e0                mov    -0x20(%rbp),%eax
400b15:       48 98                   cltq
400b17:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400b1b:       73 1b                   jae    400b38 <getlogin_r@plt+0x368>
400b1d:       8b 45 e0                mov    -0x20(%rbp),%eax
400b20:       8d 50 01                lea    0x1(%rax),%edx
400b23:       89 55 e0                mov    %edx,-0x20(%rbp)
400b26:       48 63 d0                movslq %eax,%rdx
400b29:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400b2d:       48 01 d0                add    %rdx,%rax
400b30:       0f b6 00                movzbl (%rax),%eax
400b33:       0f b6 c0                movzbl %al,%eax
400b36:       eb 05                   jmp    400b3d <getlogin_r@plt+0x36d>
400b38:       b8 00 00 00 00          mov    $0x0,%eax
400b3d:       89 45 ec                mov    %eax,-0x14(%rbp)
```

```
400b40:       8b 45 e0                mov    -0x20(%rbp),%eax
400b43:       48 98                   cltq
400b45:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400b49:       73 1b                   jae    400b66 <getlogin_r@plt+0x396>
400b4b:       8b 45 e0                mov    -0x20(%rbp),%eax
400b4e:       8d 50 01                lea    0x1(%rax),%edx
400b51:       89 55 e0                mov    %edx,-0x20(%rbp)
400b54:       48 63 d0                movslq %eax,%rdx
400b57:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400b5b:       48 01 d0                add    %rdx,%rax
400b5e:       0f b6 00                movzbl (%rax),%eax
400b61:       0f b6 c0                movzbl %al,%eax
400b64:       eb 05                   jmp    400b6b <getlogin_r@plt+0x39b>
400b66:       b8 00 00 00 00          mov    $0x0,%eax
400b6b:       89 45 f0                mov    %eax,-0x10(%rbp)
400b6e:       8b 45 e8                mov    -0x18(%rbp),%eax
400b71:       c1 e0 10                shl    $0x10,%eax
400b74:       89 c2                   mov    %eax,%edx
400b76:       8b 45 ec                mov    -0x14(%rbp),%eax
400b79:       c1 e0 08                shl    $0x8,%eax
400b7c:       01 c2                   add    %eax,%edx
400b7e:       8b 45 f0                mov    -0x10(%rbp),%eax
400b81:       01 d0                   add    %edx,%eax
400b83:       89 45 f4                mov    %eax,-0xc(%rbp)
400b86:       8b 45 e4                mov    -0x1c(%rbp),%eax
400b89:       8d 50 01                lea    0x1(%rax),%edx
400b8c:       89 55 e4                mov    %edx,-0x1c(%rbp)
400b8f:       48 63 d0                movslq %eax,%rdx
400b92:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400b96:       48 01 c2                add    %rax,%rdx
400b99:       8b 45 f4                mov    -0xc(%rbp),%eax
400b9c:       c1 e8 12                shr    $0x12,%eax
400b9f:       83 e0 3f                and    $0x3f,%eax
400ba2:       89 c0                   mov    %eax,%eax
400ba4:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bab:       88 02                   mov    %al,(%rdx)
400bad:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bb0:       8d 50 01                lea    0x1(%rax),%edx
400bb3:       89 55 e4                mov    %edx,-0x1c(%rbp)
400bb6:       48 63 d0                movslq %eax,%rdx
400bb9:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400bbd:       48 01 c2                add    %rax,%rdx
400bc0:       8b 45 f4                mov    -0xc(%rbp),%eax
400bc3:       c1 e8 0c                shr    $0xc,%eax
400bc6:       83 e0 3f                and    $0x3f,%eax
400bc9:       89 c0                   mov    %eax,%eax
400bcb:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bd2:       88 02                   mov    %al,(%rdx)
400bd4:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bd7:       8d 50 01                lea    0x1(%rax),%edx
400bda:       89 55 e4                mov    %edx,-0x1c(%rbp)
400bdd:       48 63 d0                movslq %eax,%rdx
400be0:       48 8b 45 f8             mov    -0x8(%rbp),%rax
```

```
400be4:       48 01 c2                add    %rax,%rdx
400be7:       8b 45 f4                mov    -0xc(%rbp),%eax
400bea:       c1 e8 06                shr    $0x6,%eax
400bed:       83 e0 3f                and    $0x3f,%eax
400bf0:       89 c0                   mov    %eax,%eax
400bf2:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bf9:       88 02                   mov    %al,(%rdx)
400bfb:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bfe:       8d 50 01                lea    0x1(%rax),%edx
400c01:       89 55 e4                mov    %edx,-0x1c(%rbp)
400c04:       48 63 d0                movslq %eax,%rdx
400c07:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400c0b:       48 01 c2                add    %rax,%rdx
400c0e:       8b 45 f4                mov    -0xc(%rbp),%eax
400c11:       83 e0 3f                and    $0x3f,%eax
400c14:       89 c0                   mov    %eax,%eax
400c16:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400c1d:       88 02                   mov    %al,(%rdx)
400c1f:       8b 45 e0                mov    -0x20(%rbp),%eax
400c22:       48 98                   cltq
400c24:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400c28:       0f 82 b6 fe ff ff       jb     400ae4 <getlogin_r@plt+0x314>
400c2e:       c7 45 e0 00 00 00 00    movl   $0x0,-0x20(%rbp)
400c35:       eb 24                   jmp    400c5b <getlogin_r@plt+0x48b>
400c37:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400c3b:       48 8b 10                mov    (%rax),%rdx
400c3e:       8b 45 e0                mov    -0x20(%rbp),%eax
400c41:       48 98                   cltq
400c43:       48 29 c2                sub    %rax,%rdx
400c46:       48 89 d0                mov    %rdx,%rax
400c49:       48 8d 50 ff             lea    -0x1(%rax),%rdx
400c4d:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400c51:       48 01 d0                add    %rdx,%rax
400c54:       c6 00 3d                movb   $0x3d,(%rax)
400c57:       83 45 e0 01             addl   $0x1,-0x20(%rbp)
400c5b:       48 8b 4d d0             mov    -0x30(%rbp),%rcx
400c5f:       48 ba ab aa aa aa aa    movabs $0xaaaaaaaaaaaaaaab,%rdx
400c66:       aa aa aa
400c69:       48 89 c8                mov    %rcx,%rax
400c6c:       48 f7 e2                mul    %rdx
400c6f:       48 d1 ea                shr    %rdx
400c72:       48 89 d0                mov    %rdx,%rax
400c75:       48 01 c0                add    %rax,%rax
400c78:       48 01 d0                add    %rdx,%rax
400c7b:       48 29 c1                sub    %rax,%rcx
400c7e:       48 89 ca                mov    %rcx,%rdx
400c81:       8b 04 95 00 21 60 00    mov    0x602100(,%rdx,4),%eax
400c88:       3b 45 e0                cmp    -0x20(%rbp),%eax
400c8b:       7f aa                   jg     400c37 <getlogin_r@plt+0x467>
400c8d:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400c91:       c9                      leaveq
400c92:       c3                      retq
400c93:       66 2e 0f 1f 84 00 00    nopw   %cs:0x0(%rax,%rax,1)
```

```
  400c9a:       00 00 00
  400c9d:       0f 1f 00                nopl   (%rax)
  400ca0:       41 57                   push   %r15
  400ca2:       41 89 ff                mov    %edi,%r15d
  400ca5:       41 56                   push   %r14
  400ca7:       49 89 f6                mov    %rsi,%r14
  400caa:       41 55                   push   %r13
  400cac:       49 89 d5                mov    %rdx,%r13
  400caf:       41 54                   push   %r12
  400cb1:       4c 8d 25 48 11 20 00    lea    0x201148(%rip),%r12        # 601e0
0 <_fini+0x2010ec>
  400cb8:       55                      push   %rbp
  400cb9:       48 8d 2d 48 11 20 00    lea    0x201148(%rip),%rbp        # 601e0
8 <_fini+0x2010f4>
  400cc0:       53                      push   %rbx
  400cc1:       4c 29 e5                sub    %r12,%rbp
  400cc4:       31 db                   xor    %ebx,%ebx
  400cc6:       48 c1 fd 03             sar    $0x3,%rbp
  400cca:       48 83 ec 08             sub    $0x8,%rsp
  400cce:       e8 35 fa ff ff          callq  400708 <_init>
  400cd3:       48 85 ed                test   %rbp,%rbp
  400cd6:       74 1e                   je     400cf6 <getlogin_r@plt+0x526>
  400cd8:       0f 1f 84 00 00 00 00    nopl   0x0(%rax,%rax,1)
  400cdf:       00
  400ce0:       4c 89 ea                mov    %r13,%rdx
  400ce3:       4c 89 f6                mov    %r14,%rsi
  400ce6:       44 89 ff                mov    %r15d,%edi
  400ce9:       41 ff 14 dc             callq  *(%r12,%rbx,8)
  400ced:       48 83 c3 01             add    $0x1,%rbx
  400cf1:       48 39 eb                cmp    %rbp,%rbx
  400cf4:       75 ea                   jne    400ce0 <getlogin_r@plt+0x510>
  400cf6:       48 83 c4 08             add    $0x8,%rsp
  400cfa:       5b                      pop    %rbx
  400cfb:       5d                      pop    %rbp
  400cfc:       41 5c                   pop    %r12
  400cfe:       41 5d                   pop    %r13
  400d00:       41 5e                   pop    %r14
  400d02:       41 5f                   pop    %r15
  400d04:       c3                      retq
  400d05:       66 66 2e 0f 1f 84 00    data32 nopw %cs:0x0(%rax,%rax,1)
  400d0c:       00 00 00 00
  400d10:       f3 c3                   repz retq

Disassembly of section .fini:

0000000000400d14 <_fini>:
  400d14:       48 83 ec 08             sub    $0x8,%rsp
  400d18:       48 83 c4 08             add    $0x8,%rsp
  400d1c:       c3                      retq
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ scanelf result 4
 TYPE   FILE
ET_EXEC 4
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ scanelf --name result 4
```

```
scanelf: Unknown option '' or argument missing
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ scanelf -name result 4
 TYPE    PAX   PERM ENDIAN STK/REL/PTL TEXTREL RPATH NEEDED BIND FILE
ET_EXEC PeMRxS 0775 LE RW- R-- RW-    -      -   lib361.so,libc.so.6 LAZY 4
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ clear

Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ strings 4
/lib64/ld-linux-x86-64.so.2
lib361.so
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
_init
secretoperation
_fini
libc.so.6
puts
__stack_chk_fail
__assert_fail
printf
calloc
strlen
getlogin_r
__libc_start_main
_edata
__bss_start
_end
GLIBC_2.4
GLIBC_2.2.5
dH34%(
[]A\A]A^A_
34567890123456789012
%s%s
you win! the secret is:
bangarang
this program tests the implementation of a dynamically linked library.
get_sum.c
result == 10
result == 4
main
;*3$"
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
GCC: (Ubuntu 4.8.4-2ubuntu1~14.04) 4.8.4
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
```

```
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.jcr
.dynamic
.got
.got.plt
.data
.bss
.comment
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gdb 4
GNU gdb (Ubuntu 7.7.1-0ubuntu5~14.04.2) 7.7.1
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from 4...(no debugging symbols found)...done.
(gdb) disas
No frame selected.
(gdb) r
Starting program: /home/Dpate85/dpate85/hw2/puzzles/4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.

Program received signal SIGABRT, Aborted.
```

```
0x00007ffff7849cc9 in __GI_raise (sig=sig@entry=6)
    at ../nptl/sysdeps/unix/sysv/linux/raise.c:56
56      ../nptl/sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) b main
Function "main" not defined.
Make breakpoint pending on future shared library load? (y or [n]) n
(gdb) quit
A debugging session is active.

        Inferior 1 [process 23157] will be killed.

Quit anyway? (y or n) y
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ clear

Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ strings 4
/lib64/ld-linux-x86-64.so.2
lib361.so
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
_init
secretoperation
_fini
libc.so.6
puts
__stack_chk_fail
__assert_fail
printf
calloc
strlen
getlogin_r
__libc_start_main
_edata
__bss_start
_end
GLIBC_2.4
GLIBC_2.2.5
dH34%(
[]A\A]A^A_
34567890123456789012
%s%s
you win! the secret is:
bangarang
this program tests the implementation of a dynamically linked library.
get_sum.c
result == 10
result == 4
main
;*3$"
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
GCC: (Ubuntu 4.8.4-2ubuntu1~14.04) 4.8.4
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
```

```
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.jcr
.dynamic
.got
.got.plt
.data
.bss
.comment
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ readelf -a 4
ELF Header:
  Magic:   7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF64
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Advanced Micro Devices X86-64
  Version:                           0x1
  Entry point address:               0x4007e0
  Start of program headers:          64 (bytes into file)
  Start of section headers:          8792 (bytes into file)
  Flags:                             0x0
  Size of this header:               64 (bytes)
  Size of program headers:           56 (bytes)
  Number of program headers:         9
  Size of section headers:           64 (bytes)
  Number of section headers:         28
  Section header string table index: 27

Section Headers:
  [Nr] Name              Type             Address           Offset
       Size              EntSize          Flags  Link  Info  Align
  [ 0]                   NULL             0000000000000000  00000000
       0000000000000000  0000000000000000           0     0     0
```

```
[ 1] .interp           PROGBITS         0000000000400238  00000238
     000000000000001c  0000000000000000   A       0     0     1
[ 2] .note.ABI-tag     NOTE             0000000000400254  00000254
     0000000000000020  0000000000000000   A       0     0     4
[ 3] .note.gnu.build-i NOTE             0000000000400274  00000274
     0000000000000024  0000000000000000   A       0     0     4
[ 4] .gnu.hash         GNU_HASH         0000000000400298  00000298
     0000000000000038  0000000000000000   A       5     0     8
[ 5] .dynsym           DYNSYM           00000000004002d0  000002d0
     00000000000001c8  0000000000000018   A       6     1     8
[ 6] .dynstr           STRTAB           0000000000400498  00000498
     000000000000010e  0000000000000000   A       0     0     1
[ 7] .gnu.version      VERSYM           00000000004005a6  000005a6
     0000000000000026  0000000000000002   A       5     0     2
[ 8] .gnu.version_r    VERNEED          00000000004005d0  000005d0
     0000000000000030  0000000000000000   A       6     1     8
[ 9] .rela.dyn         RELA             0000000000400600  00000600
     0000000000000018  0000000000000018   A       5     0     8
[10] .rela.plt         RELA             0000000000400618  00000618
     00000000000000f0  0000000000000018   A       5    12     8
[11] .init             PROGBITS         0000000000400708  00000708
     000000000000001a  0000000000000000  AX       0     0     4
[12] .plt              PROGBITS         0000000000400730  00000730
     00000000000000b0  0000000000000010  AX       0     0     16
[13] .text             PROGBITS         00000000004007e0  000007e0
     0000000000000532  0000000000000000  AX       0     0     16
[14] .fini             PROGBITS         0000000000400d14  00000d14
     0000000000000009  0000000000000000  AX       0     0     4
[15] .rodata           PROGBITS         0000000000400d20  00000d20
     00000000000000bf  0000000000000000   A       0     0     8
[16] .eh_frame_hdr     PROGBITS         0000000000400de0  00000de0
     0000000000000044  0000000000000000   A       0     0     4
[17] .eh_frame         PROGBITS         0000000000400e28  00000e28
     000000000000013c  0000000000000000   A       0     0     8
[18] .init_array       INIT_ARRAY       0000000000601e00  00001e00
     0000000000000008  0000000000000000  WA       0     0     8
[19] .fini_array       FINI_ARRAY       0000000000601e08  00001e08
     0000000000000008  0000000000000000  WA       0     0     8
[20] .jcr              PROGBITS         0000000000601e10  00001e10
     0000000000000008  0000000000000000  WA       0     0     8
[21] .dynamic          DYNAMIC          0000000000601e18  00001e18
     00000000000001e0  0000000000000010  WA       6     0     8
[22] .got              PROGBITS         0000000000601ff8  00001ff8
     0000000000000008  0000000000000008  WA       0     0     8
[23] .got.plt          PROGBITS         0000000000602000  00002000
     0000000000000068  0000000000000008  WA       0     0     8
[24] .data             PROGBITS         0000000000602080  00002080
     000000000000008c  0000000000000000  WA       0     0     32
[25] .bss              NOBITS           000000000060210c  0000210c
     0000000000000004  0000000000000000  WA       0     0     1
[26] .comment          PROGBITS         0000000000000000  0000210c
     000000000000004d  0000000000000001  MS       0     0     1
[27] .shstrtab         STRTAB           0000000000000000  00002159
```

```
       00000000000000f8  0000000000000000           0     0     1
Key to Flags:
  W (write), A (alloc), X (execute), M (merge), S (strings), l (large)
  I (info), L (link order), G (group), T (TLS), E (exclude), x (unknown)
  O (extra OS processing required) o (OS specific), p (processor specific)

There are no section groups in this file.

Program Headers:
  Type           Offset             VirtAddr           PhysAddr
                 FileSiz            MemSiz              Flags  Align
  PHDR           0x0000000000000040 0x0000000000400040 0x0000000000400040
                 0x00000000000001f8 0x00000000000001f8  R E    8
  INTERP         0x0000000000000238 0x0000000000400238 0x0000000000400238
                 0x000000000000001c 0x000000000000001c  R      1
      [Requesting program interpreter: /lib64/ld-linux-x86-64.so.2]
  LOAD           0x0000000000000000 0x0000000000400000 0x0000000000400000
                 0x0000000000000f64 0x0000000000000f64  R E    200000
  LOAD           0x0000000000001e00 0x0000000000601e00 0x0000000000601e00
                 0x000000000000030c 0x0000000000000310  RW     200000
  DYNAMIC        0x0000000000001e18 0x0000000000601e18 0x0000000000601e18
                 0x00000000000001e0 0x00000000000001e0  RW     8
  NOTE           0x0000000000000254 0x0000000000400254 0x0000000000400254
                 0x0000000000000044 0x0000000000000044  R      4
  GNU_EH_FRAME   0x0000000000000de0 0x0000000000400de0 0x0000000000400de0
                 0x0000000000000044 0x0000000000000044  R      4
  GNU_STACK      0x0000000000000000 0x0000000000000000 0x0000000000000000
                 0x0000000000000000 0x0000000000000000  RW     10
  GNU_RELRO      0x0000000000001e00 0x0000000000601e00 0x0000000000601e00
                 0x0000000000000200 0x0000000000000200  R      1

 Section to Segment mapping:
  Segment Sections...
   00
   01     .interp
   02     .interp .note.ABI-tag .note.gnu.build-id .gnu.hash .dynsym .dynstr .gnu
.version .gnu.version_r .rela.dyn .rela.plt .init .plt .text .fini .rodata .eh_fr
ame_hdr .eh_frame
   03     .init_array .fini_array .jcr .dynamic .got .got.plt .data .bss
   04     .dynamic
   05     .note.ABI-tag .note.gnu.build-id
   06     .eh_frame_hdr
   07
   08     .init_array .fini_array .jcr .dynamic .got

Dynamic section at offset 0x1e18 contains 25 entries:
  Tag        Type                         Name/Value
 0x0000000000000001 (NEEDED)             Shared library: [lib361.so]
 0x0000000000000001 (NEEDED)             Shared library: [libc.so.6]
 0x000000000000000c (INIT)               0x400708
 0x000000000000000d (FINI)               0x400d14
 0x0000000000000019 (INIT_ARRAY)         0x601e00
 0x000000000000001b (INIT_ARRAYSZ)       8 (bytes)
```

```
 0x000000000000001a (FINI_ARRAY)         0x601e08
 0x000000000000001c (FINI_ARRAYSZ)       8 (bytes)
 0x000000006ffffef5 (GNU_HASH)           0x400298
 0x0000000000000005 (STRTAB)             0x400498
 0x0000000000000006 (SYMTAB)             0x4002d0
 0x000000000000000a (STRSZ)              270 (bytes)
 0x000000000000000b (SYMENT)             24 (bytes)
 0x0000000000000015 (DEBUG)              0x0
 0x0000000000000003 (PLTGOT)             0x602000
 0x0000000000000002 (PLTRELSZ)           240 (bytes)
 0x0000000000000014 (PLTREL)             RELA
 0x0000000000000017 (JMPREL)             0x400618
 0x0000000000000007 (RELA)               0x400600
 0x0000000000000008 (RELASZ)             24 (bytes)
 0x0000000000000009 (RELAENT)            24 (bytes)
 0x000000006ffffffe (VERNEED)            0x4005d0
 0x000000006fffffff (VERNEEDNUM)         1
 0x000000006ffffff0 (VERSYM)             0x4005a6
 0x0000000000000000 (NULL)               0x0

Relocation section '.rela.dyn' at offset 0x600 contains 1 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000601ff8  000a00000006 R_X86_64_GLOB_DAT 0000000000000000 __gmon_start__ + 0

Relocation section '.rela.plt' at offset 0x618 contains 10 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
000000602018  000200000007 R_X86_64_JUMP_SLO 0000000000000000 puts + 0
000000602020  000300000007 R_X86_64_JUMP_SLO 0000000000000000 secretoperation + 0
000000602028  000400000007 R_X86_64_JUMP_SLO 0000000000000000 strlen + 0
000000602030  000500000007 R_X86_64_JUMP_SLO 0000000000000000 __stack_chk_fail +
0
000000602038  000600000007 R_X86_64_JUMP_SLO 0000000000000000 printf + 0
000000602040  000700000007 R_X86_64_JUMP_SLO 0000000000000000 __assert_fail + 0
000000602048  000800000007 R_X86_64_JUMP_SLO 0000000000000000 __libc_start_main +
 0
000000602050  000900000007 R_X86_64_JUMP_SLO 0000000000000000 calloc + 0
000000602058  000a00000007 R_X86_64_JUMP_SLO 0000000000000000 __gmon_start__ + 0
000000602060  000b00000007 R_X86_64_JUMP_SLO 0000000000000000 getlogin_r + 0

The decoding of unwind sections for machine type Advanced Micro Devices X86-64 is
 not currently supported.

Symbol table '.dynsym' contains 19 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMClone
Tab
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND puts@GLIBC_2.2.5 (2)
     3: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND secretoperation
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND strlen@GLIBC_2.2.5 (2)
     5: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __stack_chk_fail@GLIBC
_2.4 (3)
     6: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND printf@GLIBC_2.2.5 (2)
```

```
     7: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __assert_fail@GLIBC_2.
2.5 (2)
     8: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@GLIB
C_2.2.5 (2)
     9: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND calloc@GLIBC_2.2.5 (2)
    10: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
    11: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND getlogin_r@GLIBC_2.2.5
 (2)
    12: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _Jv_RegisterClasses
    13: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTa
ble
    14: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   24 _edata
    15: 0000000000602110     0 NOTYPE  GLOBAL DEFAULT   25 _end
    16: 000000000060210c     0 NOTYPE  GLOBAL DEFAULT   25 __bss_start
    17: 0000000000400708     0 FUNC    GLOBAL DEFAULT   11 _init
    18: 0000000000400d14     0 FUNC    GLOBAL DEFAULT   14 _fini

Histogram for `.gnu.hash' bucket list length (total of 3 buckets):
 Length  Number     % of total  Coverage
      0  0          (  0.0%)
      1  1          ( 33.3%)     20.0%
      2  2          ( 66.7%)    100.0%

Version symbols section '.gnu.version' contains 19 entries:
 Addr: 00000000004005a6  Offset: 0x0005a6  Link: 5 (.dynsym)
  000:   0 (*local*)       0 (*local*)       2 (GLIBC_2.2.5)   0 (*local*)
  004:   2 (GLIBC_2.2.5)   3 (GLIBC_2.4)     2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)
  008:   2 (GLIBC_2.2.5)   2 (GLIBC_2.2.5)   0 (*local*)       2 (GLIBC_2.2.5)
  00c:   0 (*local*)       0 (*local*)       1 (*global*)      1 (*global*)
  010:   1 (*global*)      1 (*global*)      1 (*global*)

Version needs section '.gnu.version_r' contains 1 entries:
 Addr: 0x00000000004005d0  Offset: 0x0005d0  Link: 6 (.dynstr)
  000000: Version: 1  File: libc.so.6  Cnt: 2
  0x0010:   Name: GLIBC_2.4  Flags: none  Version: 3
  0x0020:   Name: GLIBC_2.2.5  Flags: none  Version: 2

Displaying notes found at file offset 0x00000254 with length 0x00000020:
  Owner                 Data size       Description
  GNU                  0x00000010       NT_GNU_ABI_TAG (ABI version tag)
    OS: Linux, ABI: 2.6.24

Displaying notes found at file offset 0x00000274 with length 0x00000024:
  Owner                 Data size       Description
  GNU                  0x00000014       NT_GNU_BUILD_ID (unique build ID bitstrin
g)
    Build ID: 516c99c45c7b1cd513589f91ae029c0f1528d553
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
```

```
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ strace ./4
execve("./4", ["./4"], [/* 20 vars */]) = 0
brk(0)                                  = 0x20aa000
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e
4977d000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=25058, ...}) = 0
mmap(NULL, 25058, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f4e49776000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/tls/x86_64/lib361.so", O_RDONLY|O_CLOEXEC) = -1 ENOEN
T (No such file or directory)
stat("/lib/x86_64-linux-gnu/tls/x86_64", 0x7ffd788daf10) = -1 ENOENT (No such fil
e or directory)
open("/lib/x86_64-linux-gnu/tls/lib361.so", O_RDONLY|O_CLOEXEC) = -1 ENOENT (No s
uch file or directory)
stat("/lib/x86_64-linux-gnu/tls", 0x7ffd788daf10) = -1 ENOENT (No such file or di
rectory)
open("/lib/x86_64-linux-gnu/x86_64/lib361.so", O_RDONLY|O_CLOEXEC) = -1 ENOENT (N
o such file or directory)
stat("/lib/x86_64-linux-gnu/x86_64", 0x7ffd788daf10) = -1 ENOENT (No such file or
 directory)
open("/lib/x86_64-linux-gnu/lib361.so", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\240\5\0\0\0\0\0\0"..., 83
2) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=7868, ...}) = 0
mmap(NULL, 2101304, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f4
e4935b000
mprotect(0x7f4e4935c000, 2093056, PROT_NONE) = 0
mmap(0x7f4e4955b000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWR
ITE, 3, 0) = 0x7f4e4955b000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\320\37\2\0\0\0\0\0"..., 8
32) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=1840928, ...}) = 0
mmap(NULL, 3949248, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f4
e48f96000
mprotect(0x7f4e49151000, 2093056, PROT_NONE) = 0
mmap(0x7f4e49350000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYW
RITE, 3, 0x1ba000) = 0x7f4e49350000
mmap(0x7f4e49356000, 17088, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONY
MOUS, -1, 0) = 0x7f4e49356000
close(3)                                = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e
49775000
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e
49773000
arch_prctl(ARCH_SET_FS, 0x7f4e49773740) = 0
```

```
mprotect(0x7f4e49350000, 16384, PROT_READ) = 0
mprotect(0x7f4e4955b000, 4096, PROT_READ) = 0
mprotect(0x601000, 4096, PROT_READ)     = 0
mprotect(0x7f4e4977f000, 4096, PROT_READ) = 0
munmap(0x7f4e49776000, 25058)           = 0
fstat(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e
4977c000
write(1, "this program tests the implement"..., 71this program tests the implemen
tation of a dynamically linked library.
) = 71
brk(0)                                  = 0x20aa000
brk(0x20cb000)                          = 0x20cb000
write(2, "4: get_sum.c:18: main: Assertion"..., 564: get_sum.c:18: main: Assertio
n `result == 10' failed.
) = 56
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f4e
4977b000
rt_sigprocmask(SIG_UNBLOCK, [ABRT], NULL, 8) = 0
gettid()                                = 23254
tgkill(23254, 23254, SIGABRT)           = 0
--- SIGABRT {si_signo=SIGABRT, si_code=SI_TKILL, si_pid=23254, si_uid=1000} ---
+++ killed by SIGABRT (core dumped) +++
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -d 4

4:     file format elf64-x86-64


Disassembly of section .init:

0000000000400708 <_init>:
  400708:       48 83 ec 08             sub    $0x8,%rsp
  40070c:       48 8b 05 e5 18 20 00    mov    0x2018e5(%rip),%rax        # 601ff
8 <_fini+0x2012e4>
  400713:       48 85 c0                test   %rax,%rax
  400716:       74 05                   je     40071d <_init+0x15>
  400718:       e8 a3 00 00 00          callq  4007c0 <__gmon_start__@plt>
  40071d:       48 83 c4 08             add    $0x8,%rsp
  400721:       c3                      retq

Disassembly of section .plt:

0000000000400730 <puts@plt-0x10>:
  400730:       ff 35 d2 18 20 00       pushq  0x2018d2(%rip)        # 602008 <_f
ini+0x2012f4>
  400736:       ff 25 d4 18 20 00       jmpq   *0x2018d4(%rip)        # 602010 <_
fini+0x2012fc>
  40073c:       0f 1f 40 00             nopl   0x0(%rax)

0000000000400740 <puts@plt>:
  400740:       ff 25 d2 18 20 00       jmpq   *0x2018d2(%rip)        # 602018 <_
fini+0x201304>
```

```
  400746:       68 00 00 00 00          pushq  $0x0
  40074b:       e9 e0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400750 <secretoperation@plt>:
  400750:       ff 25 ca 18 20 00       jmpq   *0x2018ca(%rip)        # 602020 <_
fini+0x20130c>
  400756:       68 01 00 00 00          pushq  $0x1
  40075b:       e9 d0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400760 <strlen@plt>:
  400760:       ff 25 c2 18 20 00       jmpq   *0x2018c2(%rip)        # 602028 <_
fini+0x201314>
  400766:       68 02 00 00 00          pushq  $0x2
  40076b:       e9 c0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400770 <__stack_chk_fail@plt>:
  400770:       ff 25 ba 18 20 00       jmpq   *0x2018ba(%rip)        # 602030 <_
fini+0x20131c>
  400776:       68 03 00 00 00          pushq  $0x3
  40077b:       e9 b0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400780 <printf@plt>:
  400780:       ff 25 b2 18 20 00       jmpq   *0x2018b2(%rip)        # 602038 <_
fini+0x201324>
  400786:       68 04 00 00 00          pushq  $0x4
  40078b:       e9 a0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400790 <__assert_fail@plt>:
  400790:       ff 25 aa 18 20 00       jmpq   *0x2018aa(%rip)        # 602040 <_
fini+0x20132c>
  400796:       68 05 00 00 00          pushq  $0x5
  40079b:       e9 90 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007a0 <__libc_start_main@plt>:
  4007a0:       ff 25 a2 18 20 00       jmpq   *0x2018a2(%rip)        # 602048 <_
fini+0x201334>
  4007a6:       68 06 00 00 00          pushq  $0x6
  4007ab:       e9 80 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007b0 <calloc@plt>:
  4007b0:       ff 25 9a 18 20 00       jmpq   *0x20189a(%rip)        # 602050 <_
fini+0x20133c>
  4007b6:       68 07 00 00 00          pushq  $0x7
  4007bb:       e9 70 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007c0 <__gmon_start__@plt>:
  4007c0:       ff 25 92 18 20 00       jmpq   *0x201892(%rip)        # 602058 <_
fini+0x201344>
  4007c6:       68 08 00 00 00          pushq  $0x8
  4007cb:       e9 60 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007d0 <getlogin_r@plt>:
  4007d0:       ff 25 8a 18 20 00       jmpq   *0x20188a(%rip)        # 602060 <_
```

```
fini+0x20134c>
  4007d6:       68 09 00 00 00          pushq  $0x9
  4007db:       e9 50 ff ff ff          jmpq   400730 <_init+0x28>

Disassembly of section .text:

00000000004007e0 <.text>:
  4007e0:       31 ed                   xor    %ebp,%ebp
  4007e2:       49 89 d1                mov    %rdx,%r9
  4007e5:       5e                      pop    %rsi
  4007e6:       48 89 e2                mov    %rsp,%rdx
  4007e9:       48 83 e4 f0             and    $0xfffffffffffffff0,%rsp
  4007ed:       50                      push   %rax
  4007ee:       54                      push   %rsp
  4007ef:       49 c7 c0 10 0d 40 00    mov    $0x400d10,%r8
  4007f6:       48 c7 c1 a0 0c 40 00    mov    $0x400ca0,%rcx
  4007fd:       48 c7 c7 cd 08 40 00    mov    $0x4008cd,%rdi
  400804:       e8 97 ff ff ff          callq  4007a0 <__libc_start_main@plt>
  400809:       f4                      hlt
  40080a:       66 0f 1f 44 00 00       nopw   0x0(%rax,%rax,1)
  400810:       b8 17 21 60 00          mov    $0x602117,%eax
  400815:       55                      push   %rbp
  400816:       48 2d 10 21 60 00       sub    $0x602110,%rax
  40081c:       48 83 f8 0e             cmp    $0xe,%rax
  400820:       48 89 e5                mov    %rsp,%rbp
  400823:       77 02                   ja     400827 <getlogin_r@plt+0x57>
  400825:       5d                      pop    %rbp
  400826:       c3                      retq
  400827:       b8 00 00 00 00          mov    $0x0,%eax
  40082c:       48 85 c0                test   %rax,%rax
  40082f:       74 f4                   je     400825 <getlogin_r@plt+0x55>
  400831:       5d                      pop    %rbp
  400832:       bf 10 21 60 00          mov    $0x602110,%edi
  400837:       ff e0                   jmpq   *%rax
  400839:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400840:       b8 10 21 60 00          mov    $0x602110,%eax
  400845:       55                      push   %rbp
  400846:       48 2d 10 21 60 00       sub    $0x602110,%rax
  40084c:       48 c1 f8 03             sar    $0x3,%rax
  400850:       48 89 e5                mov    %rsp,%rbp
  400853:       48 89 c2                mov    %rax,%rdx
  400856:       48 c1 ea 3f             shr    $0x3f,%rdx
  40085a:       48 01 d0                add    %rdx,%rax
  40085d:       48 d1 f8                sar    %rax
  400860:       75 02                   jne    400864 <getlogin_r@plt+0x94>
  400862:       5d                      pop    %rbp
  400863:       c3                      retq
  400864:       ba 00 00 00 00          mov    $0x0,%edx
  400869:       48 85 d2                test   %rdx,%rdx
  40086c:       74 f4                   je     400862 <getlogin_r@plt+0x92>
  40086e:       5d                      pop    %rbp
  40086f:       48 89 c6                mov    %rax,%rsi
  400872:       bf 10 21 60 00          mov    $0x602110,%edi
```

```
  400877:       ff e2                   jmpq   *%rdx
  400879:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400880:       80 3d 85 18 20 00 00    cmpb   $0x0,0x201885(%rip)        # 60210
c <_edata>
  400887:       75 11                   jne    40089a <getlogin_r@plt+0xca>
  400889:       55                      push   %rbp
  40088a:       48 89 e5                mov    %rsp,%rbp
  40088d:       e8 7e ff ff ff          callq  400810 <getlogin_r@plt+0x40>
  400892:       5d                      pop    %rbp
  400893:       c6 05 72 18 20 00 01    movb   $0x1,0x201872(%rip)        # 60210
c <_edata>
  40089a:       f3 c3                   repz retq
  40089c:       0f 1f 40 00             nopl   0x0(%rax)
  4008a0:       48 83 3d 68 15 20 00    cmpq   $0x0,0x201568(%rip)        # 601e1
0 <_fini+0x2010fc>
  4008a7:       00
  4008a8:       74 1e                   je     4008c8 <getlogin_r@plt+0xf8>
  4008aa:       b8 00 00 00 00          mov    $0x0,%eax
  4008af:       48 85 c0                test   %rax,%rax
  4008b2:       74 14                   je     4008c8 <getlogin_r@plt+0xf8>
  4008b4:       55                      push   %rbp
  4008b5:       bf 10 1e 60 00          mov    $0x601e10,%edi
  4008ba:       48 89 e5                mov    %rsp,%rbp
  4008bd:       ff d0                   callq  *%rax
  4008bf:       5d                      pop    %rbp
  4008c0:       e9 7b ff ff ff          jmpq   400840 <getlogin_r@plt+0x70>
  4008c5:       0f 1f 00                nopl   (%rax)
  4008c8:       e9 73 ff ff ff          jmpq   400840 <getlogin_r@plt+0x70>
  4008cd:       55                      push   %rbp
  4008ce:       48 89 e5                mov    %rsp,%rbp
  4008d1:       48 83 ec 10             sub    $0x10,%rsp
  4008d5:       c7 45 f4 01 00 00 00    movl   $0x1,-0xc(%rbp)
  4008dc:       c7 45 f8 02 00 00 00    movl   $0x2,-0x8(%rbp)
  4008e3:       c7 45 fc 00 00 00 00    movl   $0x0,-0x4(%rbp)
  4008ea:       bf 70 0d 40 00          mov    $0x400d70,%edi
  4008ef:       e8 4c fe ff ff          callq  400740 <puts@plt>
  4008f4:       be 06 00 00 00          mov    $0x6,%esi
  4008f9:       bf 03 00 00 00          mov    $0x3,%edi
  4008fe:       e8 4d fe ff ff          callq  400750 <secretoperation@plt>
  400903:       89 45 fc                mov    %eax,-0x4(%rbp)
  400906:       83 7d fc 0a             cmpl   $0xa,-0x4(%rbp)
  40090a:       74 19                   je     400925 <getlogin_r@plt+0x155>
  40090c:       b9 da 0d 40 00          mov    $0x400dda,%ecx
  400911:       ba 12 00 00 00          mov    $0x12,%edx
  400916:       be b7 0d 40 00          mov    $0x400db7,%esi
  40091b:       bf c1 0d 40 00          mov    $0x400dc1,%edi
  400920:       e8 6b fe ff ff          callq  400790 <__assert_fail@plt>
  400925:       8b 55 f8                mov    -0x8(%rbp),%edx
  400928:       8b 45 f4                mov    -0xc(%rbp),%eax
  40092b:       89 d6                   mov    %edx,%esi
  40092d:       89 c7                   mov    %eax,%edi
  40092f:       e8 1c fe ff ff          callq  400750 <secretoperation@plt>
  400934:       89 45 fc                mov    %eax,-0x4(%rbp)
```

```
  400937:       83 7d fc 04             cmpl   $0x4,-0x4(%rbp)
  40093b:       74 19                   je     400956 <getlogin_r@plt+0x186>
  40093d:       b9 da 0d 40 00          mov    $0x400dda,%ecx
  400942:       ba 14 00 00 00          mov    $0x14,%edx
  400947:       be b7 0d 40 00          mov    $0x400db7,%esi
  40094c:       bf ce 0d 40 00          mov    $0x400dce,%edi
  400951:       e8 3a fe ff ff          callq  400790 <__assert_fail@plt>
  400956:       48 8b 05 33 17 20 00    mov    0x201733(%rip),%rax        # 60209
0 <_fini+0x20137c>
  40095d:       48 89 c7                mov    %rax,%rdi
  400960:       e8 28 00 00 00          callq  40098d <getlogin_r@plt+0x1bd>
  400965:       48 89 c2                mov    %rax,%rdx
  400968:       48 8b 0d 31 17 20 00    mov    0x201731(%rip),%rcx        # 6020a
0 <_fini+0x20138c>
  40096f:       48 8b 05 22 17 20 00    mov    0x201722(%rip),%rax        # 60209
8 <_fini+0x201384>
  400976:       48 89 ce                mov    %rcx,%rsi
  400979:       48 89 c7                mov    %rax,%rdi
  40097c:       b8 00 00 00 00          mov    $0x0,%eax
  400981:       e8 fa fd ff ff          callq  400780 <printf@plt>
  400986:       b8 00 00 00 00          mov    $0x0,%eax
  40098b:       c9                      leaveq
  40098c:       c3                      retq
  40098d:       55                      push   %rbp
  40098e:       48 89 e5                mov    %rsp,%rbp
  400991:       53                      push   %rbx
  400992:       48 81 ec 38 04 00 00    sub    $0x438,%rsp
  400999:       48 89 bd c8 fb ff ff    mov    %rdi,-0x438(%rbp)
  4009a0:       64 48 8b 04 25 28 00    mov    %fs:0x28,%rax
  4009a7:       00 00
  4009a9:       48 89 45 e8             mov    %rax,-0x18(%rbp)
  4009ad:       31 c0                   xor    %eax,%eax
  4009af:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
  4009b6:       be 00 04 00 00          mov    $0x400,%esi
  4009bb:       48 89 c7                mov    %rax,%rdi
  4009be:       e8 0d fe ff ff          callq  4007d0 <getlogin_r@plt>
  4009c3:       c7 85 d4 fb ff ff 00    movl   $0x0,-0x42c(%rbp)
  4009ca:       00 00 00
  4009cd:       eb 3e                   jmp    400a0d <getlogin_r@plt+0x23d>
  4009cf:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  4009d5:       48 98                   cltq
  4009d7:       0f b6 94 05 e0 fb ff    movzbl -0x420(%rbp,%rax,1),%edx
  4009de:       ff
  4009df:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  4009e5:       48 63 c8                movslq %eax,%rcx
  4009e8:       48 8b 85 c8 fb ff ff    mov    -0x438(%rbp),%rax
  4009ef:       48 01 c8                add    %rcx,%rax
  4009f2:       0f b6 00                movzbl (%rax),%eax
  4009f5:       31 c2                   xor    %eax,%edx
  4009f7:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  4009fd:       48 98                   cltq
  4009ff:       88 94 05 e0 fb ff ff    mov    %dl,-0x420(%rbp,%rax,1)
  400a06:       83 85 d4 fb ff ff 01    addl   $0x1,-0x42c(%rbp)
```

```
400a0d:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
400a13:       48 63 d8                movslq %eax,%rbx
400a16:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
400a1d:       48 89 c7                mov    %rax,%rdi
400a20:       e8 3b fd ff ff          callq  400760 <strlen@plt>
400a25:       48 39 c3                cmp    %rax,%rbx
400a28:       72 a5                   jb     4009cf <getlogin_r@plt+0x1ff>
400a2a:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
400a30:       48 63 c8                movslq %eax,%rcx
400a33:       48 8d 95 d8 fb ff ff    lea    -0x428(%rbp),%rdx
400a3a:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
400a41:       48 89 ce                mov    %rcx,%rsi
400a44:       48 89 c7                mov    %rax,%rdi
400a47:       e8 1e 00 00 00          callq  400a6a <getlogin_r@plt+0x29a>
400a4c:       48 8b 75 e8             mov    -0x18(%rbp),%rsi
400a50:       64 48 33 34 25 28 00    xor    %fs:0x28,%rsi
400a57:       00 00
400a59:       74 05                   je     400a60 <getlogin_r@plt+0x290>
400a5b:       e8 10 fd ff ff          callq  400770 <__stack_chk_fail@plt>
400a60:       48 81 c4 38 04 00 00    add    $0x438,%rsp
400a67:       5b                      pop    %rbx
400a68:       5d                      pop    %rbp
400a69:       c3                      retq
400a6a:       55                      push   %rbp
400a6b:       48 89 e5                mov    %rsp,%rbp
400a6e:       48 83 ec 40             sub    $0x40,%rsp
400a72:       48 89 7d d8             mov    %rdi,-0x28(%rbp)
400a76:       48 89 75 d0             mov    %rsi,-0x30(%rbp)
400a7a:       48 89 55 c8             mov    %rdx,-0x38(%rbp)
400a7e:       48 8b 45 d0             mov    -0x30(%rbp),%rax
400a82:       48 83 c0 02             add    $0x2,%rax
400a86:       48 ba ab aa aa aa aa    movabs $0xaaaaaaaaaaaaaaab,%rdx
400a8d:       aa aa aa
400a90:       48 f7 e2                mul    %rdx
400a93:       48 89 d0                mov    %rdx,%rax
400a96:       48 d1 e8                shr    %rax
400a99:       48 8d 14 85 00 00 00    lea    0x0(,%rax,4),%rdx
400aa0:       00
400aa1:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400aa5:       48 89 10                mov    %rdx,(%rax)
400aa8:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400aac:       48 8b 00                mov    (%rax),%rax
400aaf:       be 01 00 00 00          mov    $0x1,%esi
400ab4:       48 89 c7                mov    %rax,%rdi
400ab7:       e8 f4 fc ff ff          callq  4007b0 <calloc@plt>
400abc:       48 89 45 f8             mov    %rax,-0x8(%rbp)
400ac0:       48 83 7d f8 00          cmpq   $0x0,-0x8(%rbp)
400ac5:       75 0a                   jne    400ad1 <getlogin_r@plt+0x301>
400ac7:       b8 00 00 00 00          mov    $0x0,%eax
400acc:       e9 c0 01 00 00          jmpq   400c91 <getlogin_r@plt+0x4c1>
400ad1:       c7 45 e0 00 00 00 00    movl   $0x0,-0x20(%rbp)
400ad8:       c7 45 e4 00 00 00 00    movl   $0x0,-0x1c(%rbp)
400adf:       e9 3b 01 00 00          jmpq   400c1f <getlogin_r@plt+0x44f>
```

```
400ae4:       8b 45 e0                mov    -0x20(%rbp),%eax
400ae7:       48 98                   cltq
400ae9:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400aed:       73 1b                   jae    400b0a <getlogin_r@plt+0x33a>
400aef:       8b 45 e0                mov    -0x20(%rbp),%eax
400af2:       8d 50 01                lea    0x1(%rax),%edx
400af5:       89 55 e0                mov    %edx,-0x20(%rbp)
400af8:       48 63 d0                movslq %eax,%rdx
400afb:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400aff:       48 01 d0                add    %rdx,%rax
400b02:       0f b6 00                movzbl (%rax),%eax
400b05:       0f b6 c0                movzbl %al,%eax
400b08:       eb 05                   jmp    400b0f <getlogin_r@plt+0x33f>
400b0a:       b8 00 00 00 00          mov    $0x0,%eax
400b0f:       89 45 e8                mov    %eax,-0x18(%rbp)
400b12:       8b 45 e0                mov    -0x20(%rbp),%eax
400b15:       48 98                   cltq
400b17:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400b1b:       73 1b                   jae    400b38 <getlogin_r@plt+0x368>
400b1d:       8b 45 e0                mov    -0x20(%rbp),%eax
400b20:       8d 50 01                lea    0x1(%rax),%edx
400b23:       89 55 e0                mov    %edx,-0x20(%rbp)
400b26:       48 63 d0                movslq %eax,%rdx
400b29:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400b2d:       48 01 d0                add    %rdx,%rax
400b30:       0f b6 00                movzbl (%rax),%eax
400b33:       0f b6 c0                movzbl %al,%eax
400b36:       eb 05                   jmp    400b3d <getlogin_r@plt+0x36d>
400b38:       b8 00 00 00 00          mov    $0x0,%eax
400b3d:       89 45 ec                mov    %eax,-0x14(%rbp)
400b40:       8b 45 e0                mov    -0x20(%rbp),%eax
400b43:       48 98                   cltq
400b45:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400b49:       73 1b                   jae    400b66 <getlogin_r@plt+0x396>
400b4b:       8b 45 e0                mov    -0x20(%rbp),%eax
400b4e:       8d 50 01                lea    0x1(%rax),%edx
400b51:       89 55 e0                mov    %edx,-0x20(%rbp)
400b54:       48 63 d0                movslq %eax,%rdx
400b57:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400b5b:       48 01 d0                add    %rdx,%rax
400b5e:       0f b6 00                movzbl (%rax),%eax
400b61:       0f b6 c0                movzbl %al,%eax
400b64:       eb 05                   jmp    400b6b <getlogin_r@plt+0x39b>
400b66:       b8 00 00 00 00          mov    $0x0,%eax
400b6b:       89 45 f0                mov    %eax,-0x10(%rbp)
400b6e:       8b 45 e8                mov    -0x18(%rbp),%eax
400b71:       c1 e0 10                shl    $0x10,%eax
400b74:       89 c2                   mov    %eax,%edx
400b76:       8b 45 ec                mov    -0x14(%rbp),%eax
400b79:       c1 e0 08                shl    $0x8,%eax
400b7c:       01 c2                   add    %eax,%edx
400b7e:       8b 45 f0                mov    -0x10(%rbp),%eax
400b81:       01 d0                   add    %edx,%eax
```

```
400b83:       89 45 f4                mov    %eax,-0xc(%rbp)
400b86:       8b 45 e4                mov    -0x1c(%rbp),%eax
400b89:       8d 50 01                lea    0x1(%rax),%edx
400b8c:       89 55 e4                mov    %edx,-0x1c(%rbp)
400b8f:       48 63 d0                movslq %eax,%rdx
400b92:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400b96:       48 01 c2                add    %rax,%rdx
400b99:       8b 45 f4                mov    -0xc(%rbp),%eax
400b9c:       c1 e8 12                shr    $0x12,%eax
400b9f:       83 e0 3f                and    $0x3f,%eax
400ba2:       89 c0                   mov    %eax,%eax
400ba4:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bab:       88 02                   mov    %al,(%rdx)
400bad:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bb0:       8d 50 01                lea    0x1(%rax),%edx
400bb3:       89 55 e4                mov    %edx,-0x1c(%rbp)
400bb6:       48 63 d0                movslq %eax,%rdx
400bb9:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400bbd:       48 01 c2                add    %rax,%rdx
400bc0:       8b 45 f4                mov    -0xc(%rbp),%eax
400bc3:       c1 e8 0c                shr    $0xc,%eax
400bc6:       83 e0 3f                and    $0x3f,%eax
400bc9:       89 c0                   mov    %eax,%eax
400bcb:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bd2:       88 02                   mov    %al,(%rdx)
400bd4:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bd7:       8d 50 01                lea    0x1(%rax),%edx
400bda:       89 55 e4                mov    %edx,-0x1c(%rbp)
400bdd:       48 63 d0                movslq %eax,%rdx
400be0:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400be4:       48 01 c2                add    %rax,%rdx
400be7:       8b 45 f4                mov    -0xc(%rbp),%eax
400bea:       c1 e8 06                shr    $0x6,%eax
400bed:       83 e0 3f                and    $0x3f,%eax
400bf0:       89 c0                   mov    %eax,%eax
400bf2:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bf9:       88 02                   mov    %al,(%rdx)
400bfb:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bfe:       8d 50 01                lea    0x1(%rax),%edx
400c01:       89 55 e4                mov    %edx,-0x1c(%rbp)
400c04:       48 63 d0                movslq %eax,%rdx
400c07:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400c0b:       48 01 c2                add    %rax,%rdx
400c0e:       8b 45 f4                mov    -0xc(%rbp),%eax
400c11:       83 e0 3f                and    $0x3f,%eax
400c14:       89 c0                   mov    %eax,%eax
400c16:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400c1d:       88 02                   mov    %al,(%rdx)
400c1f:       8b 45 e0                mov    -0x20(%rbp),%eax
400c22:       48 98                   cltq
400c24:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400c28:       0f 82 b6 fe ff ff       jb     400ae4 <getlogin_r@plt+0x314>
400c2e:       c7 45 e0 00 00 00 00    movl   $0x0,-0x20(%rbp)
```

```
  400c35:       eb 24                   jmp    400c5b <getlogin_r@plt+0x48b>
  400c37:       48 8b 45 c8             mov    -0x38(%rbp),%rax
  400c3b:       48 8b 10                mov    (%rax),%rdx
  400c3e:       8b 45 e0                mov    -0x20(%rbp),%eax
  400c41:       48 98                   cltq
  400c43:       48 29 c2                sub    %rax,%rdx
  400c46:       48 89 d0                mov    %rdx,%rax
  400c49:       48 8d 50 ff             lea    -0x1(%rax),%rdx
  400c4d:       48 8b 45 f8             mov    -0x8(%rbp),%rax
  400c51:       48 01 d0                add    %rdx,%rax
  400c54:       c6 00 3d                movb   $0x3d,(%rax)
  400c57:       83 45 e0 01             addl   $0x1,-0x20(%rbp)
  400c5b:       48 8b 4d d0             mov    -0x30(%rbp),%rcx
  400c5f:       48 ba ab aa aa aa aa    movabs $0xaaaaaaaaaaaaaaab,%rdx
  400c66:       aa aa aa
  400c69:       48 89 c8                mov    %rcx,%rax
  400c6c:       48 f7 e2                mul    %rdx
  400c6f:       48 d1 ea                shr    %rdx
  400c72:       48 89 d0                mov    %rdx,%rax
  400c75:       48 01 c0                add    %rax,%rax
  400c78:       48 01 d0                add    %rdx,%rax
  400c7b:       48 29 c1                sub    %rax,%rcx
  400c7e:       48 89 ca                mov    %rcx,%rdx
  400c81:       8b 04 95 00 21 60 00    mov    0x602100(,%rdx,4),%eax
  400c88:       3b 45 e0                cmp    -0x20(%rbp),%eax
  400c8b:       7f aa                   jg     400c37 <getlogin_r@plt+0x467>
  400c8d:       48 8b 45 f8             mov    -0x8(%rbp),%rax
  400c91:       c9                      leaveq
  400c92:       c3                      retq
  400c93:       66 2e 0f 1f 84 00 00    nopw   %cs:0x0(%rax,%rax,1)
  400c9a:       00 00 00
  400c9d:       0f 1f 00                nopl   (%rax)
  400ca0:       41 57                   push   %r15
  400ca2:       41 89 ff                mov    %edi,%r15d
  400ca5:       41 56                   push   %r14
  400ca7:       49 89 f6                mov    %rsi,%r14
  400caa:       41 55                   push   %r13
  400cac:       49 89 d5                mov    %rdx,%r13
  400caf:       41 54                   push   %r12
  400cb1:       4c 8d 25 48 11 20 00    lea    0x201148(%rip),%r12        # 601e0
0 <_fini+0x2010ec>
  400cb8:       55                      push   %rbp
  400cb9:       48 8d 2d 48 11 20 00    lea    0x201148(%rip),%rbp        # 601e0
8 <_fini+0x2010f4>
  400cc0:       53                      push   %rbx
  400cc1:       4c 29 e5                sub    %r12,%rbp
  400cc4:       31 db                   xor    %ebx,%ebx
  400cc6:       48 c1 fd 03             sar    $0x3,%rbp
  400cca:       48 83 ec 08             sub    $0x8,%rsp
  400cce:       e8 35 fa ff ff          callq  400708 <_init>
  400cd3:       48 85 ed                test   %rbp,%rbp
  400cd6:       74 1e                   je     400cf6 <getlogin_r@plt+0x526>
  400cd8:       0f 1f 84 00 00 00 00    nopl   0x0(%rax,%rax,1)
```

```
  400cdf:       00
  400ce0:       4c 89 ea                mov    %r13,%rdx
  400ce3:       4c 89 f6                mov    %r14,%rsi
  400ce6:       44 89 ff                mov    %r15d,%edi
  400ce9:       41 ff 14 dc             callq  *(%r12,%rbx,8)
  400ced:       48 83 c3 01             add    $0x1,%rbx
  400cf1:       48 39 eb                cmp    %rbp,%rbx
  400cf4:       75 ea                   jne    400ce0 <getlogin_r@plt+0x510>
  400cf6:       48 83 c4 08             add    $0x8,%rsp
  400cfa:       5b                      pop    %rbx
  400cfb:       5d                      pop    %rbp
  400cfc:       41 5c                   pop    %r12
  400cfe:       41 5d                   pop    %r13
  400d00:       41 5e                   pop    %r14
  400d02:       41 5f                   pop    %r15
  400d04:       c3                      retq
  400d05:       66 66 2e 0f 1f 84 00    data32 nopw %cs:0x0(%rax,%rax,1)
  400d0c:       00 00 00 00
  400d10:       f3 c3                   repz retq

Disassembly of section .fini:

0000000000400d14 <_fini>:
  400d14:       48 83 ec 08             sub    $0x8,%rsp
  400d18:       48 83 c4 08             add    $0x8,%rsp
  400d1c:       c3                      retq
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -a 4

4:     file format elf64-x86-64
4

Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -s 4

4:     file format elf64-x86-64

Contents of section .interp:
 400238 2f6c6962 36342f6c 642d6c69 6e75782d  /lib64/ld-linux-
 400248 7838362d 36342e73 6f2e3200           x86-64.so.2.
Contents of section .note.ABI-tag:
 400254 04000000 10000000 01000000 474e5500  ............GNU.
 400264 00000000 02000000 06000000 18000000  ................
Contents of section .note.gnu.build-id:
 400274 04000000 14000000 03000000 474e5500  ............GNU.
 400284 516c99c4 5c7b1cd5 13589f91 ae029c0f  Ql..\{...X......
 400294 1528d553                             .(.S
Contents of section .gnu.hash:
 400298 03000000 0e000000 01000000 06000000  ................
 4002a8 88c02001 00044009 0e000000 10000000  .. ...@.........
 4002b8 12000000 4245d5ec bbe3927c d871581c  ....BE.....|.qX.
 4002c8 b98df10e ebd3ef0e                    ........
Contents of section .dynsym:
 4002d0 00000000 00000000 00000000 00000000  ................
 4002e0 00000000 00000000 0b000000 20000000  ............ ...
```

```
 4002f0 00000000 00000000 00000000 00000000  ................
 400300 8a000000 12000000 00000000 00000000  ................
 400310 00000000 00000000 6a000000 12000000  ........j.......
 400320 00000000 00000000 00000000 00000000  ................
 400330 bc000000 12000000 00000000 00000000  ................
 400340 00000000 00000000 8f000000 12000000  ................
 400350 00000000 00000000 00000000 00000000  ................
 400360 ae000000 12000000 00000000 00000000  ................
 400370 00000000 00000000 a0000000 12000000  ................
 400380 00000000 00000000 00000000 00000000  ................
 400390 ce000000 12000000 00000000 00000000  ................
 4003a0 00000000 00000000 b5000000 12000000  ................
 4003b0 00000000 00000000 00000000 00000000  ................
 4003c0 27000000 20000000 00000000 00000000  '... ............
 4003d0 00000000 00000000 c3000000 12000000  ................
 4003e0 00000000 00000000 00000000 00000000  ................
 4003f0 36000000 20000000 00000000 00000000  6... ............
 400400 00000000 00000000 4a000000 20000000  ........J... ...
 400410 00000000 00000000 00000000 00000000  ................
 400420 e0000000 10001800 0c216000 00000000  .........!`.....
 400430 00000000 00000000 f3000000 10001900  ................
 400440 10216000 00000000 00000000 00000000  .!`.............
 400450 e7000000 10001900 0c216000 00000000  .........!`.....
 400460 00000000 00000000 64000000 12000b00  ........d.......
 400470 08074000 00000000 00000000 00000000  ..@.............
 400480 7a000000 12000e00 140d4000 00000000  z.........@.....
 400490 00000000 00000000                    ........
Contents of section .dynstr:
 400498 006c6962 3336312e 736f005f 49544d5f  .lib361.so._ITM_
 4004a8 64657265 67697374 6572544d 436c6f6e  deregisterTMClon
 4004b8 65546162 6c65005f 5f676d6f 6e5f7374  eTable.__gmon_st
 4004c8 6172745f 5f005f4a 765f5265 67697374  art__._Jv_Regist
 4004d8 6572436c 61737365 73005f49 544d5f72  erClasses._ITM_r
 4004e8 65676973 74657254 4d436c6f 6e655461  egisterTMCloneTa
 4004f8 626c6500 5f696e69 74007365 63726574  ble._init.secret
 400508 6f706572 6174696f 6e005f66 696e6900  operation._fini.
 400518 6c696263 2e736f2e 36007075 7473005f  libc.so.6.puts._
 400528 5f737461 636b5f63 686b5f66 61696c00  _stack_chk_fail.
 400538 5f5f6173 73657274 5f666169 6c007072  __assert_fail.pr
 400548 696e7466 0063616c 6c6f6300 7374726c  intf.calloc.strl
 400558 656e0067 65746c6f 67696e5f 72005f5f  en.getlogin_r.__
 400568 6c696263 5f737461 72745f6d 61696e00  libc_start_main.
 400578 5f656461 7461005f 5f627373 5f737461  _edata.__bss_sta
 400588 7274005f 656e6400 474c4942 435f322e  rt._end.GLIBC_2.
 400598 3400474c 4942435f 322e322e 3500      4.GLIBC_2.2.5.
Contents of section .gnu.version:
 4005a6 00000000 02000000 02000300 02000200  ................
 4005b6 02000200 00000200 00000000 01000100  ................
 4005c6 01000100 0100                        ......
Contents of section .gnu.version_r:
 4005d0 01000200 80000000 10000000 00000000  ................
 4005e0 1469690d 00000300 f8000000 10000000  .ii.............
 4005f0 751a6909 00000200 02010000 00000000  u.i.............
```

```
Contents of section .rela.dyn:
 400600 f81f6000 00000000 06000000 0a000000  ..`.............
 400610 00000000 00000000                    ........
Contents of section .rela.plt:
 400618 18206000 00000000 07000000 02000000  . `.............
 400628 00000000 00000000 20206000 00000000  ........  `.....
 400638 07000000 03000000 00000000 00000000  ................
 400648 28206000 00000000 07000000 04000000  ( `.............
 400658 00000000 00000000 30206000 00000000  ........0 `.....
 400668 07000000 05000000 00000000 00000000  ................
 400678 38206000 00000000 07000000 06000000  8 `.............
 400688 00000000 00000000 40206000 00000000  ........@ `.....
 400698 07000000 07000000 00000000 00000000  ................
 4006a8 48206000 00000000 07000000 08000000  H `.............
 4006b8 00000000 00000000 50206000 00000000  ........P `.....
 4006c8 07000000 09000000 00000000 00000000  ................
 4006d8 58206000 00000000 07000000 0a000000  X `.............
 4006e8 00000000 00000000 60206000 00000000  ........` `.....
 4006f8 07000000 0b000000 00000000 00000000  ................
Contents of section .init:
 400708 4883ec08 488b05e5 18200048 85c07405  H...H.... .H..t.
 400718 e8a30000 004883c4 08c3               .....H....
Contents of section .plt:
 400730 ff35d218 2000ff25 d4182000 0f1f4000  .5.. ..%.. ...@.
 400740 ff25d218 20006800 000000e9 e0ffffff  .%.. .h.........
 400750 ff25ca18 20006801 000000e9 d0ffffff  .%.. .h.........
 400760 ff25c218 20006802 000000e9 c0ffffff  .%.. .h.........
 400770 ff25ba18 20006803 000000e9 b0ffffff  .%.. .h.........
 400780 ff25b218 20006804 000000e9 a0ffffff  .%.. .h.........
 400790 ff25aa18 20006805 000000e9 90ffffff  .%.. .h.........
 4007a0 ff25a218 20006806 000000e9 80ffffff  .%.. .h.........
 4007b0 ff259a18 20006807 000000e9 70ffffff  .%.. .h.....p...
 4007c0 ff259218 20006808 000000e9 60ffffff  .%.. .h.....`...
 4007d0 ff258a18 20006809 000000e9 50ffffff  .%.. .h.....P...
Contents of section .text:
 4007e0 31ed4989 d15e4889 e24883e4 f0505449  1.I..^H..H...PTI
 4007f0 c7c0100d 400048c7 c1a00c40 0048c7c7  ....@.H....@.H..
 400800 cd084000 e897ffff fff4660f 1f440000  ..@.......f..D..
 400810 b8172160 0055482d 10216000 4883f80e  ..!`.UH-.!`.H...
 400820 4889e577 025dc3b8 00000000 4885c074  H..w.].......H..t
 400830 f45dbf10 216000ff e00f1f80 00000000  .]..!`..........
 400840 b8102160 0055482d 10216000 48c1f803  ..!`.UH-.!`.H...
 400850 4889e548 89c248c1 ea3f4801 d048d1f8  H..H..H..?H..H..
 400860 75025dc3 ba000000 004885d2 74f45d48  u.].......H..t.]H
 400870 89c6bf10 216000ff e20f1f80 00000000  ....!`..........
 400880 803d8518 20000075 11554889 e5e87eff  .=.. ..u.UH...~.
 400890 ffff5dc6 05721820 0001f3c3 0f1f4000  ..]..r. .......@.
 4008a0 48833d68 15200000 741eb800 00000048  H.=h. ..t......H
 4008b0 85c07414 55bf101e 60004889 e5ffd05d  ..t.U...`.H....]
 4008c0 e97bffff ff0f1f00 e973ffff ff554889  .{.......s...UH.
 4008d0 e54883ec 10c745f4 01000000 c745f802  .H....E......E..
 4008e0 000000c7 45fc0000 0000bf70 0d4000e8  ....E......p.@..
 4008f0 4cfeffff be060000 00bf0300 0000e84d  L..............M
```

```
400900 fefffff89 45fc837d fc0a7419 b9da0d40  ....E..}..t....@
400910 00ba1200 0000beb7 0d4000bf c10d4000  .........@....@.
400920 e86bfeff ff8b55f8 8b45f489 d689c7e8  .k....U..E......
400930 1cfeffff 8945fc83 7dfc0474 19b9da0d  .....E..}..t....
400940 4000ba14 000000be b70d4000 bfce0d40  @.........@....@
400950 00e83afe ffff488b 05331720 004889c7  ..:...H..3. .H..
400960 e8280000 004889c2 488b0d31 17200048  .(...H..H..1. .H
400970 8b052217 20004889 ce4889c7 b8000000  ..". .H..H......
400980 00e8fafd ffffb800 000000c9 c3554889  .............UH.
400990 e5534881 ec380400 004889bd c8fbffff  .SH..8...H......
4009a0 64488b04 25280000 00488945 e831c048  dH..%(...H.E.1.H
4009b0 8d85e0fb ffffbe00 04000048 89c7e80d  ...........H....
4009c0 fefffc7 85d4fbff ff000000 00eb3e8b  ..............>.
4009d0 85d4fbff ff48980f b69405e0 fbffff8b  .....H..........
4009e0 85d4fbff ff4863c8 488b85c8 fbffff48  .....Hc.H......H
4009f0 01c80fb6 0031c28b 85d4fbff ff489888  .....1.......H..
400a00 9405e0fb ffff8385 d4fbffff 018b85d4  ................
400a10 fbffff48 63d8488d 85e0fbff ff4889c7  ...Hc.H......H..
400a20 e83bfdff ff4839c3 72a58b85 d4fbffff  .;...H9.r.......
400a30 4863c848 8d95d8fb ffff488d 85e0fbff  Hc.H......H.....
400a40 ff4889ce 4889c7e8 1e000000 488b75e8  .H..H.......H.u.
400a50 64483334 25280000 007405e8 10fdffff  dH34%(...t......
400a60 4881c438 0400005b 5dc35548 89e54883  H..8...[].UH..H.
400a70 ec404889 7dd84889 75d04889 55c8488b  .@H.}.H.u.H.U.H.
400a80 45d04883 c00248ba abaaaaaa aaaaaaaa  E.H...H.........
400a90 48f7e248 89d048d1 e8488d14 85000000  H..H..H..H......
400aa0 00488b45 c8488910 488b45c8 488b00be  .H.E.H..H.E.H...
400ab0 01000000 4889c7e8 f4fcffff 488945f8  ....H.......H.E.
400ac0 48837df8 00750ab8 00000000 e9c00100  H.}..u..........
400ad0 00c745e0 00000000 c745e400 000000e9  ..E......E......
400ae0 3b010000 8b45e048 98483b45 d0731b8b  ;....E.H.H;E.s..
400af0 45e08d50 018955e0 4863d048 8b45d848  E..P..U.Hc.H.E.H
400b00 01d00fb6 000fb6c0 eb05b800 00000089  ................
400b10 45e88b45 e0489848 3b45d073 1b8b45e0  E..E.H.H;E.s..E.
400b20 8d500189 55e04863 d0488b45 d84801d0  .P..U.Hc.H.E.H..
400b30 0fb6000f b6c0eb05 b8000000 008945ec  ..............E.
400b40 8b45e048 98483b45 d0731b8b 45e08d50  .E.H.H;E.s..E..P
400b50 018955e0 4863d048 8b45d848 01d00fb6  ..U.Hc.H.E.H....
400b60 000fb6c0 eb05b800 00000089 45f08b45  ............E..E
400b70 e8c1e010 89c28b45 ecc1e008 01c28b45  .......E.......E
400b80 f001d089 45f48b45 e48d5001 8955e448  ....E..E..P..U.H
400b90 63d0488b 45f84801 c28b45f4 c1e81283  c.H.E.H...E.....
400ba0 e03f89c0 0fb680c0 20600088 028b45e4  .?...... `....E.
400bb0 8d500189 55e44863 d0488b45 f84801c2  .P..U.Hc.H.E.H..
400bc0 8b45f4c1 e80c83e0 3f89c00f b680c020  .E......?...... 
400bd0 60008802 8b45e48d 50018955 e44863d0  `....E..P..U.Hc.
400be0 488b45f8 4801c28b 45f4c1e8 0683e03f  H.E.H...E......?
400bf0 89c00fb6 80c02060 0088028b 45e48d50  ...... `....E..P
400c00 018955e4 4863d048 8b45f848 01c28b45  ..U.Hc.H.E.H...E
400c10 f483e03f 89c00fb6 80c02060 0088028b  ...?...... `....
400c20 45e04898 483b45d0 0f82b6fe ffffc745  E.H.H;E........E
400c30 e0000000 00eb2448 8b45c848 8b108b45  ......$H.E.H...E
400c40 e0489848 29c24889 d0488d50 ff488b45  .H.H).H..H.P.H.E
```

```
 400c50 f84801d0 c6003d83 45e00148 8b4dd048  .H....=.E..H.M.H
 400c60 baabaaaa aaaaaaaa aa4889c8 48f7e248  .........H..H..H
 400c70 d1ea4889 d04801c0 4801d048 29c14889  ..H..H..H..H).H.
 400c80 ca8b0495 00216000 3b45e07f aa488b45  .....!`.;E...H.E
 400c90 f8c9c366 2e0f1f84 00000000 000f1f00  ...f............
 400ca0 41574189 ff415649 89f64155 4989d541  AWA..AVI..AUI..A
 400cb0 544c8d25 48112000 55488d2d 48112000  TL.%H. .UH.-H. .
 400cc0 534c29e5 31db48c1 fd034883 ec08e835  SL).1.H...H....5
 400cd0 fafffff48 85ed741e 0f1f8400 00000000  ...H..t.........
 400ce0 4c89ea4c 89f64489 ff41ff14 dc4883c3  L..L..D..A...H..
 400cf0 014839eb 75ea4883 c4085b5d 415c415d  .H9.u.H...[]A\A]
 400d00 415e415f c366662e 0f1f8400 00000000  A^A_.ff.........
 400d10 f3c3                                 ..
Contents of section .fini:
 400d14 4883ec08 4883c408 c3                 H...H....
Contents of section .rodata:
 400d20 01000200 00000000 33343536 37383930  ........34567890
 400d30 31323334 35363738 39303132 00257325  123456789012.%s%
 400d40 730a0000 00000000 796f7520 77696e21  s.......you win!
 400d50 20746865 20736563 72657420 69733a0a   the secret is:.
 400d60 0062616e 67617261 6e670000 00000000  .bangarang......
 400d70 74686973 2070726f 6772616d 20746573  this program tes
 400d80 74732074 68652069 6d706c65 6d656e74  ts the implement
 400d90 6174696f 6e206f66 20612064 796e616d  ation of a dynam
 400da0 6963616c 6c79206c 696e6b65 64206c69  ically linked li
 400db0 62726172 792e0067 65745f73 756d2e63  brary..get_sum.c
 400dc0 00726573 756c7420 3d3d2031 30007265  .result == 10.re
 400dd0 73756c74 203d3d20 34006d61 696e00    sult == 4.main.
Contents of section .eh_frame_hdr:
 400de0 011b033b 44000000 07000000 50f9ffff  ...;D.......P...
 400df0 90000000 00faffff 60000000 edfaffff  ........`.......
 400e00 b8000000 adfbffff d8000000 8afcffff  ................
 400e10 00010000 c0feffff 20010000 30ffffff  ........ ...0...
 400e20 68010000                             h...
Contents of section .eh_frame:
 400e28 14000000 00000000 017a5200 01781001  .........zR..x..
 400e38 1b0c0708 90010710 14000000 1c000000  ................
 400e48 98f9ffff 2a000000 00000000 00000000  ....*...........
 400e58 14000000 00000000 017a5200 01781001  .........zR..x..
 400e68 1b0c0708 90010000 24000000 1c000000  ........$.......
 400e78 b8f8ffff b0000000 000e1046 0e184a0f  ...........F..J.
 400e88 0b770880 003f1a3b 2a332422 00000000  .w...?.;*3$"....
 400e98 1c000000 44000000 2dfaffff c0000000  ....D...-.......
 400ea8 00410e10 8602430d 0602bb0c 07080000  .A....C.........
 400eb8 24000000 64000000 cdfaffff dd000000  $...d...........
 400ec8 00410e10 8602430d 06488303 02d00c07  .A....C..H......
 400ed8 08000000 00000000 1c000000 8c000000  ................
 400ee8 82fbffff 29020000 00410e10 8602430d  ....)....A....C.
 400ef8 06032402 0c070800 44000000 ac000000  ..$.....D.......
 400f08 98fdffff 65000000 00420e10 8f02450e  ....e....B....E.
 400f18 188e0345 0e208d04 450e288c 05480e30  ...E. ..E.(..H.0
 400f28 8606480e 3883074d 0e406c0e 38410e30  ..H.8..M.@l.8A.0
 400f38 410e2842 0e20420e 18420e10 420e0800  A.(B. B..B..B...
```

```
 400f48 14000000 f4000000 c0fdffff 02000000  ................
 400f58 00000000 00000000 00000000           ............
Contents of section .init_array:
 601e00 a0084000 00000000                    ..@.....
Contents of section .fini_array:
 601e08 80084000 00000000                    ..@.....
Contents of section .jcr:
 601e10 00000000 00000000                    ........
Contents of section .dynamic:
 601e18 01000000 00000000 01000000 00000000  ................
 601e28 01000000 00000000 80000000 00000000  ................
 601e38 0c000000 00000000 08074000 00000000  ..........@.....
 601e48 0d000000 00000000 140d4000 00000000  ..........@.....
 601e58 19000000 00000000 001e6000 00000000  ..........`.....
 601e68 1b000000 00000000 08000000 00000000  ................
 601e78 1a000000 00000000 081e6000 00000000  ..........`.....
 601e88 1c000000 00000000 08000000 00000000  ................
 601e98 f5feff6f 00000000 98024000 00000000  ...o......@.....
 601ea8 05000000 00000000 98044000 00000000  ..........@.....
 601eb8 06000000 00000000 d0024000 00000000  ..........@.....
 601ec8 0a000000 00000000 0e010000 00000000  ................
 601ed8 0b000000 00000000 18000000 00000000  ................
 601ee8 15000000 00000000 00000000 00000000  ................
 601ef8 03000000 00000000 00206000 00000000  ......... `.....
 601f08 02000000 00000000 f0000000 00000000  ................
 601f18 14000000 00000000 07000000 00000000  ................
 601f28 17000000 00000000 18064000 00000000  ..........@.....
 601f38 07000000 00000000 00064000 00000000  ..........@.....
 601f48 08000000 00000000 18000000 00000000  ................
 601f58 09000000 00000000 18000000 00000000  ................
 601f68 fefffff6f 00000000 d0054000 00000000  ...o......@.....
 601f78 ffffff6f 00000000 01000000 00000000  ...o............
 601f88 f0ffff6f 00000000 a6054000 00000000  ...o......@.....
 601f98 00000000 00000000 00000000 00000000  ................
 601fa8 00000000 00000000 00000000 00000000  ................
 601fb8 00000000 00000000 00000000 00000000  ................
 601fc8 00000000 00000000 00000000 00000000  ................
 601fd8 00000000 00000000 00000000 00000000  ................
 601fe8 00000000 00000000 00000000 00000000  ................
Contents of section .got:
 601ff8 00000000 00000000                    ........
Contents of section .got.plt:
 602000 181e6000 00000000 00000000 00000000  ..`.............
 602010 00000000 00000000 46074000 00000000  ........F.@.....
 602020 56074000 00000000 66074000 00000000  V.@.....f.@.....
 602030 76074000 00000000 86074000 00000000  v.@.......@.....
 602040 96074000 00000000 a6074000 00000000  ..@.......@.....
 602050 b6074000 00000000 c6074000 00000000  ..@.......@.....
 602060 d6074000 00000000                    ..@.....
Contents of section .data:
 602080 00000000 00000000 00000000 00000000  ................
 602090 280d4000 00000000 3d0d4000 00000000  (.@.....=.@.....
 6020a0 480d4000 00000000 00000000 00000000  H.@.............
```

```
 6020b0 00000000 00000000 00000000 00000000  ................
 6020c0 41424344 45464748 494a4b4c 4d4e4f50  ABCDEFGHIJKLMNOP
 6020d0 51525354 55565758 595a6162 63646566  QRSTUVWXYZabcdef
 6020e0 6768696a 6b6c6d6e 6f707172 73747576  ghijklmnopqrstuv
 6020f0 7778797a 30313233 34353637 38392b2f  wxyz0123456789+/
 602100 00000000 02000000 01000000           ............
Contents of section .comment:
 0000 4743433a 20285562 756e7475 20342e38  GCC: (Ubuntu 4.8
 0010 2e342d32 7562756e 7475317e 31342e30  .4-2ubuntu1~14.0
 0020 34292034 2e382e34 00474343 3a202855  4) 4.8.4.GCC: (U
 0030 62756e74 7520342e 382e322d 31397562  buntu 4.8.2-19ub
 0040 756e7475 31292034 2e382e32 00        untu1) 4.8.2.
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -S 4

4:     file format elf64-x86-64


Disassembly of section .init:

0000000000400708 <_init>:
  400708:       48 83 ec 08             sub    $0x8,%rsp
  40070c:       48 8b 05 e5 18 20 00    mov    0x2018e5(%rip),%rax        # 601ff
8 <_fini+0x2012e4>
  400713:       48 85 c0                test   %rax,%rax
  400716:       74 05                   je     40071d <_init+0x15>
  400718:       e8 a3 00 00 00          callq  4007c0 <__gmon_start__@plt>
  40071d:       48 83 c4 08             add    $0x8,%rsp
  400721:       c3                      retq

Disassembly of section .plt:

0000000000400730 <puts@plt-0x10>:
  400730:       ff 35 d2 18 20 00       pushq  0x2018d2(%rip)        # 602008 <_f
ini+0x2012f4>
  400736:       ff 25 d4 18 20 00       jmpq   *0x2018d4(%rip)        # 602010 <_
fini+0x2012fc>
  40073c:       0f 1f 40 00             nopl   0x0(%rax)

0000000000400740 <puts@plt>:
  400740:       ff 25 d2 18 20 00       jmpq   *0x2018d2(%rip)        # 602018 <_
fini+0x201304>
  400746:       68 00 00 00 00          pushq  $0x0
  40074b:       e9 e0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400750 <secretoperation@plt>:
  400750:       ff 25 ca 18 20 00       jmpq   *0x2018ca(%rip)        # 602020 <_
fini+0x20130c>
  400756:       68 01 00 00 00          pushq  $0x1
  40075b:       e9 d0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400760 <strlen@plt>:
  400760:       ff 25 c2 18 20 00       jmpq   *0x2018c2(%rip)        # 602028 <_
fini+0x201314>
```

```
  400766:       68 02 00 00 00          pushq  $0x2
  40076b:       e9 c0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400770 <__stack_chk_fail@plt>:
  400770:       ff 25 ba 18 20 00       jmpq   *0x2018ba(%rip)        # 602030 <_
fini+0x20131c>
  400776:       68 03 00 00 00          pushq  $0x3
  40077b:       e9 b0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400780 <printf@plt>:
  400780:       ff 25 b2 18 20 00       jmpq   *0x2018b2(%rip)        # 602038 <_
fini+0x201324>
  400786:       68 04 00 00 00          pushq  $0x4
  40078b:       e9 a0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400790 <__assert_fail@plt>:
  400790:       ff 25 aa 18 20 00       jmpq   *0x2018aa(%rip)        # 602040 <_
fini+0x20132c>
  400796:       68 05 00 00 00          pushq  $0x5
  40079b:       e9 90 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007a0 <__libc_start_main@plt>:
  4007a0:       ff 25 a2 18 20 00       jmpq   *0x2018a2(%rip)        # 602048 <_
fini+0x201334>
  4007a6:       68 06 00 00 00          pushq  $0x6
  4007ab:       e9 80 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007b0 <calloc@plt>:
  4007b0:       ff 25 9a 18 20 00       jmpq   *0x20189a(%rip)        # 602050 <_
fini+0x20133c>
  4007b6:       68 07 00 00 00          pushq  $0x7
  4007bb:       e9 70 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007c0 <__gmon_start__@plt>:
  4007c0:       ff 25 92 18 20 00       jmpq   *0x201892(%rip)        # 602058 <_
fini+0x201344>
  4007c6:       68 08 00 00 00          pushq  $0x8
  4007cb:       e9 60 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007d0 <getlogin_r@plt>:
  4007d0:       ff 25 8a 18 20 00       jmpq   *0x20188a(%rip)        # 602060 <_
fini+0x20134c>
  4007d6:       68 09 00 00 00          pushq  $0x9
  4007db:       e9 50 ff ff ff          jmpq   400730 <_init+0x28>

Disassembly of section .text:

00000000004007e0 <.text>:
  4007e0:       31 ed                   xor    %ebp,%ebp
  4007e2:       49 89 d1                mov    %rdx,%r9
  4007e5:       5e                      pop    %rsi
  4007e6:       48 89 e2                mov    %rsp,%rdx
  4007e9:       48 83 e4 f0             and    $0xfffffffffffffff0,%rsp
```

```
  4007ed:       50                      push   %rax
  4007ee:       54                      push   %rsp
  4007ef:       49 c7 c0 10 0d 40 00    mov    $0x400d10,%r8
  4007f6:       48 c7 c1 a0 0c 40 00    mov    $0x400ca0,%rcx
  4007fd:       48 c7 c7 cd 08 40 00    mov    $0x4008cd,%rdi
  400804:       e8 97 ff ff ff          callq  4007a0 <__libc_start_main@plt>
  400809:       f4                      hlt
  40080a:       66 0f 1f 44 00 00       nopw   0x0(%rax,%rax,1)
  400810:       b8 17 21 60 00          mov    $0x602117,%eax
  400815:       55                      push   %rbp
  400816:       48 2d 10 21 60 00       sub    $0x602110,%rax
  40081c:       48 83 f8 0e             cmp    $0xe,%rax
  400820:       48 89 e5                mov    %rsp,%rbp
  400823:       77 02                   ja     400827 <getlogin_r@plt+0x57>
  400825:       5d                      pop    %rbp
  400826:       c3                      retq
  400827:       b8 00 00 00 00          mov    $0x0,%eax
  40082c:       48 85 c0                test   %rax,%rax
  40082f:       74 f4                   je     400825 <getlogin_r@plt+0x55>
  400831:       5d                      pop    %rbp
  400832:       bf 10 21 60 00          mov    $0x602110,%edi
  400837:       ff e0                   jmpq   *%rax
  400839:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400840:       b8 10 21 60 00          mov    $0x602110,%eax
  400845:       55                      push   %rbp
  400846:       48 2d 10 21 60 00       sub    $0x602110,%rax
  40084c:       48 c1 f8 03             sar    $0x3,%rax
  400850:       48 89 e5                mov    %rsp,%rbp
  400853:       48 89 c2                mov    %rax,%rdx
  400856:       48 c1 ea 3f             shr    $0x3f,%rdx
  40085a:       48 01 d0                add    %rdx,%rax
  40085d:       48 d1 f8                sar    %rax
  400860:       75 02                   jne    400864 <getlogin_r@plt+0x94>
  400862:       5d                      pop    %rbp
  400863:       c3                      retq
  400864:       ba 00 00 00 00          mov    $0x0,%edx
  400869:       48 85 d2                test   %rdx,%rdx
  40086c:       74 f4                   je     400862 <getlogin_r@plt+0x92>
  40086e:       5d                      pop    %rbp
  40086f:       48 89 c6                mov    %rax,%rsi
  400872:       bf 10 21 60 00          mov    $0x602110,%edi
  400877:       ff e2                   jmpq   *%rdx
  400879:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400880:       80 3d 85 18 20 00 00    cmpb   $0x0,0x201885(%rip)        # 60210
c <_edata>
  400887:       75 11                   jne    40089a <getlogin_r@plt+0xca>
  400889:       55                      push   %rbp
  40088a:       48 89 e5                mov    %rsp,%rbp
  40088d:       e8 7e ff ff ff          callq  400810 <getlogin_r@plt+0x40>
  400892:       5d                      pop    %rbp
  400893:       c6 05 72 18 20 00 01    movb   $0x1,0x201872(%rip)        # 60210
c <_edata>
  40089a:       f3 c3                   repz retq
```

```
  40089c:       0f 1f 40 00             nopl   0x0(%rax)
  4008a0:       48 83 3d 68 15 20 00    cmpq   $0x0,0x201568(%rip)        # 601e1
0 <_fini+0x2010fc>
  4008a7:       00
  4008a8:       74 1e                   je     4008c8 <getlogin_r@plt+0xf8>
  4008aa:       b8 00 00 00 00          mov    $0x0,%eax
  4008af:       48 85 c0                test   %rax,%rax
  4008b2:       74 14                   je     4008c8 <getlogin_r@plt+0xf8>
  4008b4:       55                      push   %rbp
  4008b5:       bf 10 1e 60 00          mov    $0x601e10,%edi
  4008ba:       48 89 e5                mov    %rsp,%rbp
  4008bd:       ff d0                   callq  *%rax
  4008bf:       5d                      pop    %rbp
  4008c0:       e9 7b ff ff ff          jmpq   400840 <getlogin_r@plt+0x70>
  4008c5:       0f 1f 00                nopl   (%rax)
  4008c8:       e9 73 ff ff ff          jmpq   400840 <getlogin_r@plt+0x70>
  4008cd:       55                      push   %rbp
  4008ce:       48 89 e5                mov    %rsp,%rbp
  4008d1:       48 83 ec 10             sub    $0x10,%rsp
  4008d5:       c7 45 f4 01 00 00 00    movl   $0x1,-0xc(%rbp)
  4008dc:       c7 45 f8 02 00 00 00    movl   $0x2,-0x8(%rbp)
  4008e3:       c7 45 fc 00 00 00 00    movl   $0x0,-0x4(%rbp)
  4008ea:       bf 70 0d 40 00          mov    $0x400d70,%edi
  4008ef:       e8 4c fe ff ff          callq  400740 <puts@plt>
  4008f4:       be 06 00 00 00          mov    $0x6,%esi
  4008f9:       bf 03 00 00 00          mov    $0x3,%edi
  4008fe:       e8 4d fe ff ff          callq  400750 <secretoperation@plt>
  400903:       89 45 fc                mov    %eax,-0x4(%rbp)
  400906:       83 7d fc 0a             cmpl   $0xa,-0x4(%rbp)
  40090a:       74 19                   je     400925 <getlogin_r@plt+0x155>
  40090c:       b9 da 0d 40 00          mov    $0x400dda,%ecx
  400911:       ba 12 00 00 00          mov    $0x12,%edx
  400916:       be b7 0d 40 00          mov    $0x400db7,%esi
  40091b:       bf c1 0d 40 00          mov    $0x400dc1,%edi
  400920:       e8 6b fe ff ff          callq  400790 <__assert_fail@plt>
  400925:       8b 55 f8                mov    -0x8(%rbp),%edx
  400928:       8b 45 f4                mov    -0xc(%rbp),%eax
  40092b:       89 d6                   mov    %edx,%esi
  40092d:       89 c7                   mov    %eax,%edi
  40092f:       e8 1c fe ff ff          callq  400750 <secretoperation@plt>
  400934:       89 45 fc                mov    %eax,-0x4(%rbp)
  400937:       83 7d fc 04             cmpl   $0x4,-0x4(%rbp)
  40093b:       74 19                   je     400956 <getlogin_r@plt+0x186>
  40093d:       b9 da 0d 40 00          mov    $0x400dda,%ecx
  400942:       ba 14 00 00 00          mov    $0x14,%edx
  400947:       be b7 0d 40 00          mov    $0x400db7,%esi
  40094c:       bf ce 0d 40 00          mov    $0x400dce,%edi
  400951:       e8 3a fe ff ff          callq  400790 <__assert_fail@plt>
  400956:       48 8b 05 33 17 20 00    mov    0x201733(%rip),%rax        # 60209
0 <_fini+0x20137c>
  40095d:       48 89 c7                mov    %rax,%rdi
  400960:       e8 28 00 00 00          callq  40098d <getlogin_r@plt+0x1bd>
  400965:       48 89 c2                mov    %rax,%rdx
```

```
  400968:       48 8b 0d 31 17 20 00    mov    0x201731(%rip),%rcx        # 6020a
0 <_fini+0x20138c>
  40096f:       48 8b 05 22 17 20 00    mov    0x201722(%rip),%rax        # 60209
8 <_fini+0x201384>
  400976:       48 89 ce                mov    %rcx,%rsi
  400979:       48 89 c7                mov    %rax,%rdi
  40097c:       b8 00 00 00 00          mov    $0x0,%eax
  400981:       e8 fa fd ff ff          callq  400780 <printf@plt>
  400986:       b8 00 00 00 00          mov    $0x0,%eax
  40098b:       c9                      leaveq
  40098c:       c3                      retq
  40098d:       55                      push   %rbp
  40098e:       48 89 e5                mov    %rsp,%rbp
  400991:       53                      push   %rbx
  400992:       48 81 ec 38 04 00 00    sub    $0x438,%rsp
  400999:       48 89 bd c8 fb ff ff    mov    %rdi,-0x438(%rbp)
  4009a0:       64 48 8b 04 25 28 00    mov    %fs:0x28,%rax
  4009a7:       00 00
  4009a9:       48 89 45 e8             mov    %rax,-0x18(%rbp)
  4009ad:       31 c0                   xor    %eax,%eax
  4009af:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
  4009b6:       be 00 04 00 00          mov    $0x400,%esi
  4009bb:       48 89 c7                mov    %rax,%rdi
  4009be:       e8 0d fe ff ff          callq  4007d0 <getlogin_r@plt>
  4009c3:       c7 85 d4 fb ff ff 00    movl   $0x0,-0x42c(%rbp)
  4009ca:       00 00 00
  4009cd:       eb 3e                   jmp    400a0d <getlogin_r@plt+0x23d>
  4009cf:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  4009d5:       48 98                   cltq
  4009d7:       0f b6 94 05 e0 fb ff    movzbl -0x420(%rbp,%rax,1),%edx
  4009de:       ff
  4009df:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  4009e5:       48 63 c8                movslq %eax,%rcx
  4009e8:       48 8b 85 c8 fb ff ff    mov    -0x438(%rbp),%rax
  4009ef:       48 01 c8                add    %rcx,%rax
  4009f2:       0f b6 00                movzbl (%rax),%eax
  4009f5:       31 c2                   xor    %eax,%edx
  4009f7:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  4009fd:       48 98                   cltq
  4009ff:       88 94 05 e0 fb ff ff    mov    %dl,-0x420(%rbp,%rax,1)
  400a06:       83 85 d4 fb ff ff 01    addl   $0x1,-0x42c(%rbp)
  400a0d:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  400a13:       48 63 d8                movslq %eax,%rbx
  400a16:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
  400a1d:       48 89 c7                mov    %rax,%rdi
  400a20:       e8 3b fd ff ff          callq  400760 <strlen@plt>
  400a25:       48 39 c3                cmp    %rax,%rbx
  400a28:       72 a5                   jb     4009cf <getlogin_r@plt+0x1ff>
  400a2a:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  400a30:       48 63 c8                movslq %eax,%rcx
  400a33:       48 8d 95 d8 fb ff ff    lea    -0x428(%rbp),%rdx
  400a3a:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
  400a41:       48 89 ce                mov    %rcx,%rsi
```

```
400a44:       48 89 c7                mov    %rax,%rdi
400a47:       e8 1e 00 00 00          callq  400a6a <getlogin_r@plt+0x29a>
400a4c:       48 8b 75 e8             mov    -0x18(%rbp),%rsi
400a50:       64 48 33 34 25 28 00    xor    %fs:0x28,%rsi
400a57:       00 00
400a59:       74 05                   je     400a60 <getlogin_r@plt+0x290>
400a5b:       e8 10 fd ff ff          callq  400770 <__stack_chk_fail@plt>
400a60:       48 81 c4 38 04 00 00    add    $0x438,%rsp
400a67:       5b                      pop    %rbx
400a68:       5d                      pop    %rbp
400a69:       c3                      retq
400a6a:       55                      push   %rbp
400a6b:       48 89 e5                mov    %rsp,%rbp
400a6e:       48 83 ec 40             sub    $0x40,%rsp
400a72:       48 89 7d d8             mov    %rdi,-0x28(%rbp)
400a76:       48 89 75 d0             mov    %rsi,-0x30(%rbp)
400a7a:       48 89 55 c8             mov    %rdx,-0x38(%rbp)
400a7e:       48 8b 45 d0             mov    -0x30(%rbp),%rax
400a82:       48 83 c0 02             add    $0x2,%rax
400a86:       48 ba ab aa aa aa aa    movabs $0xaaaaaaaaaaaaaaab,%rdx
400a8d:       aa aa aa
400a90:       48 f7 e2                mul    %rdx
400a93:       48 89 d0                mov    %rdx,%rax
400a96:       48 d1 e8                shr    %rax
400a99:       48 8d 14 85 00 00 00    lea    0x0(,%rax,4),%rdx
400aa0:       00
400aa1:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400aa5:       48 89 10                mov    %rdx,(%rax)
400aa8:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400aac:       48 8b 00                mov    (%rax),%rax
400aaf:       be 01 00 00 00          mov    $0x1,%esi
400ab4:       48 89 c7                mov    %rax,%rdi
400ab7:       e8 f4 fc ff ff          callq  4007b0 <calloc@plt>
400abc:       48 89 45 f8             mov    %rax,-0x8(%rbp)
400ac0:       48 83 7d f8 00          cmpq   $0x0,-0x8(%rbp)
400ac5:       75 0a                   jne    400ad1 <getlogin_r@plt+0x301>
400ac7:       b8 00 00 00 00          mov    $0x0,%eax
400acc:       e9 c0 01 00 00          jmpq   400c91 <getlogin_r@plt+0x4c1>
400ad1:       c7 45 e0 00 00 00 00    movl   $0x0,-0x20(%rbp)
400ad8:       c7 45 e4 00 00 00 00    movl   $0x0,-0x1c(%rbp)
400adf:       e9 3b 01 00 00          jmpq   400c1f <getlogin_r@plt+0x44f>
400ae4:       8b 45 e0                mov    -0x20(%rbp),%eax
400ae7:       48 98                   cltq
400ae9:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400aed:       73 1b                   jae    400b0a <getlogin_r@plt+0x33a>
400aef:       8b 45 e0                mov    -0x20(%rbp),%eax
400af2:       8d 50 01                lea    0x1(%rax),%edx
400af5:       89 55 e0                mov    %edx,-0x20(%rbp)
400af8:       48 63 d0                movslq %eax,%rdx
400afb:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400aff:       48 01 d0                add    %rdx,%rax
400b02:       0f b6 00                movzbl (%rax),%eax
400b05:       0f b6 c0                movzbl %al,%eax
```

```
400b08:       eb 05                   jmp    400b0f <getlogin_r@plt+0x33f>
400b0a:       b8 00 00 00 00          mov    $0x0,%eax
400b0f:       89 45 e8                mov    %eax,-0x18(%rbp)
400b12:       8b 45 e0                mov    -0x20(%rbp),%eax
400b15:       48 98                   cltq
400b17:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400b1b:       73 1b                   jae    400b38 <getlogin_r@plt+0x368>
400b1d:       8b 45 e0                mov    -0x20(%rbp),%eax
400b20:       8d 50 01                lea    0x1(%rax),%edx
400b23:       89 55 e0                mov    %edx,-0x20(%rbp)
400b26:       48 63 d0                movslq %eax,%rdx
400b29:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400b2d:       48 01 d0                add    %rdx,%rax
400b30:       0f b6 00                movzbl (%rax),%eax
400b33:       0f b6 c0                movzbl %al,%eax
400b36:       eb 05                   jmp    400b3d <getlogin_r@plt+0x36d>
400b38:       b8 00 00 00 00          mov    $0x0,%eax
400b3d:       89 45 ec                mov    %eax,-0x14(%rbp)
400b40:       8b 45 e0                mov    -0x20(%rbp),%eax
400b43:       48 98                   cltq
400b45:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400b49:       73 1b                   jae    400b66 <getlogin_r@plt+0x396>
400b4b:       8b 45 e0                mov    -0x20(%rbp),%eax
400b4e:       8d 50 01                lea    0x1(%rax),%edx
400b51:       89 55 e0                mov    %edx,-0x20(%rbp)
400b54:       48 63 d0                movslq %eax,%rdx
400b57:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400b5b:       48 01 d0                add    %rdx,%rax
400b5e:       0f b6 00                movzbl (%rax),%eax
400b61:       0f b6 c0                movzbl %al,%eax
400b64:       eb 05                   jmp    400b6b <getlogin_r@plt+0x39b>
400b66:       b8 00 00 00 00          mov    $0x0,%eax
400b6b:       89 45 f0                mov    %eax,-0x10(%rbp)
400b6e:       8b 45 e8                mov    -0x18(%rbp),%eax
400b71:       c1 e0 10                shl    $0x10,%eax
400b74:       89 c2                   mov    %eax,%edx
400b76:       8b 45 ec                mov    -0x14(%rbp),%eax
400b79:       c1 e0 08                shl    $0x8,%eax
400b7c:       01 c2                   add    %eax,%edx
400b7e:       8b 45 f0                mov    -0x10(%rbp),%eax
400b81:       01 d0                   add    %edx,%eax
400b83:       89 45 f4                mov    %eax,-0xc(%rbp)
400b86:       8b 45 e4                mov    -0x1c(%rbp),%eax
400b89:       8d 50 01                lea    0x1(%rax),%edx
400b8c:       89 55 e4                mov    %edx,-0x1c(%rbp)
400b8f:       48 63 d0                movslq %eax,%rdx
400b92:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400b96:       48 01 c2                add    %rax,%rdx
400b99:       8b 45 f4                mov    -0xc(%rbp),%eax
400b9c:       c1 e8 12                shr    $0x12,%eax
400b9f:       83 e0 3f                and    $0x3f,%eax
400ba2:       89 c0                   mov    %eax,%eax
400ba4:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
```

```
400bab:       88 02                   mov    %al,(%rdx)
400bad:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bb0:       8d 50 01                lea    0x1(%rax),%edx
400bb3:       89 55 e4                mov    %edx,-0x1c(%rbp)
400bb6:       48 63 d0                movslq %eax,%rdx
400bb9:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400bbd:       48 01 c2                add    %rax,%rdx
400bc0:       8b 45 f4                mov    -0xc(%rbp),%eax
400bc3:       c1 e8 0c                shr    $0xc,%eax
400bc6:       83 e0 3f                and    $0x3f,%eax
400bc9:       89 c0                   mov    %eax,%eax
400bcb:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bd2:       88 02                   mov    %al,(%rdx)
400bd4:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bd7:       8d 50 01                lea    0x1(%rax),%edx
400bda:       89 55 e4                mov    %edx,-0x1c(%rbp)
400bdd:       48 63 d0                movslq %eax,%rdx
400be0:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400be4:       48 01 c2                add    %rax,%rdx
400be7:       8b 45 f4                mov    -0xc(%rbp),%eax
400bea:       c1 e8 06                shr    $0x6,%eax
400bed:       83 e0 3f                and    $0x3f,%eax
400bf0:       89 c0                   mov    %eax,%eax
400bf2:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bf9:       88 02                   mov    %al,(%rdx)
400bfb:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bfe:       8d 50 01                lea    0x1(%rax),%edx
400c01:       89 55 e4                mov    %edx,-0x1c(%rbp)
400c04:       48 63 d0                movslq %eax,%rdx
400c07:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400c0b:       48 01 c2                add    %rax,%rdx
400c0e:       8b 45 f4                mov    -0xc(%rbp),%eax
400c11:       83 e0 3f                and    $0x3f,%eax
400c14:       89 c0                   mov    %eax,%eax
400c16:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400c1d:       88 02                   mov    %al,(%rdx)
400c1f:       8b 45 e0                mov    -0x20(%rbp),%eax
400c22:       48 98                   cltq
400c24:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400c28:       0f 82 b6 fe ff ff       jb     400ae4 <getlogin_r@plt+0x314>
400c2e:       c7 45 e0 00 00 00 00    movl   $0x0,-0x20(%rbp)
400c35:       eb 24                   jmp    400c5b <getlogin_r@plt+0x48b>
400c37:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400c3b:       48 8b 10                mov    (%rax),%rdx
400c3e:       8b 45 e0                mov    -0x20(%rbp),%eax
400c41:       48 98                   cltq
400c43:       48 29 c2                sub    %rax,%rdx
400c46:       48 89 d0                mov    %rdx,%rax
400c49:       48 8d 50 ff             lea    -0x1(%rax),%rdx
400c4d:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400c51:       48 01 d0                add    %rdx,%rax
400c54:       c6 00 3d                movb   $0x3d,(%rax)
400c57:       83 45 e0 01             addl   $0x1,-0x20(%rbp)
```

```
  400c5b:       48 8b 4d d0             mov    -0x30(%rbp),%rcx
  400c5f:       48 ba ab aa aa aa aa    movabs $0xaaaaaaaaaaaaaaab,%rdx
  400c66:       aa aa aa
  400c69:       48 89 c8                mov    %rcx,%rax
  400c6c:       48 f7 e2                mul    %rdx
  400c6f:       48 d1 ea                shr    %rdx
  400c72:       48 89 d0                mov    %rdx,%rax
  400c75:       48 01 c0                add    %rax,%rax
  400c78:       48 01 d0                add    %rdx,%rax
  400c7b:       48 29 c1                sub    %rax,%rcx
  400c7e:       48 89 ca                mov    %rcx,%rdx
  400c81:       8b 04 95 00 21 60 00    mov    0x602100(,%rdx,4),%eax
  400c88:       3b 45 e0                cmp    -0x20(%rbp),%eax
  400c8b:       7f aa                   jg     400c37 <getlogin_r@plt+0x467>
  400c8d:       48 8b 45 f8             mov    -0x8(%rbp),%rax
  400c91:       c9                      leaveq
  400c92:       c3                      retq
  400c93:       66 2e 0f 1f 84 00 00    nopw   %cs:0x0(%rax,%rax,1)
  400c9a:       00 00 00
  400c9d:       0f 1f 00                nopl   (%rax)
  400ca0:       41 57                   push   %r15
  400ca2:       41 89 ff                mov    %edi,%r15d
  400ca5:       41 56                   push   %r14
  400ca7:       49 89 f6                mov    %rsi,%r14
  400caa:       41 55                   push   %r13
  400cac:       49 89 d5                mov    %rdx,%r13
  400caf:       41 54                   push   %r12
  400cb1:       4c 8d 25 48 11 20 00    lea    0x201148(%rip),%r12        # 601e0
0 <_fini+0x2010ec>
  400cb8:       55                      push   %rbp
  400cb9:       48 8d 2d 48 11 20 00    lea    0x201148(%rip),%rbp        # 601e0
8 <_fini+0x2010f4>
  400cc0:       53                      push   %rbx
  400cc1:       4c 29 e5                sub    %r12,%rbp
  400cc4:       31 db                   xor    %ebx,%ebx
  400cc6:       48 c1 fd 03             sar    $0x3,%rbp
  400cca:       48 83 ec 08             sub    $0x8,%rsp
  400cce:       e8 35 fa ff ff          callq  400708 <_init>
  400cd3:       48 85 ed                test   %rbp,%rbp
  400cd6:       74 1e                   je     400cf6 <getlogin_r@plt+0x526>
  400cd8:       0f 1f 84 00 00 00 00    nopl   0x0(%rax,%rax,1)
  400cdf:       00
  400ce0:       4c 89 ea                mov    %r13,%rdx
  400ce3:       4c 89 f6                mov    %r14,%rsi
  400ce6:       44 89 ff                mov    %r15d,%edi
  400ce9:       41 ff 14 dc             callq  *(%r12,%rbx,8)
  400ced:       48 83 c3 01             add    $0x1,%rbx
  400cf1:       48 39 eb                cmp    %rbp,%rbx
  400cf4:       75 ea                   jne    400ce0 <getlogin_r@plt+0x510>
  400cf6:       48 83 c4 08             add    $0x8,%rsp
  400cfa:       5b                      pop    %rbx
  400cfb:       5d                      pop    %rbp
  400cfc:       41 5c                   pop    %r12
```

```
  400cfe:       41 5d                   pop    %r13
  400d00:       41 5e                   pop    %r14
  400d02:       41 5f                   pop    %r15
  400d04:       c3                      retq
  400d05:       66 66 2e 0f 1f 84 00    data32 nopw %cs:0x0(%rax,%rax,1)
  400d0c:       00 00 00 00
  400d10:       f3 c3                   repz retq

Disassembly of section .fini:

0000000000400d14 <_fini>:
  400d14:       48 83 ec 08             sub    $0x8,%rsp
  400d18:       48 83 c4 08             add    $0x8,%rsp
  400d1c:       c3                      retq
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ vi lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:18: main: Assertion `result == 10' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ sudo cp lib361.so /lib/x86_64-linux-gnu/
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objcopy --redefine-sym old=new 4
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  lib361.c  lib361.so  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ rm 4
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cd
Dpate85@Dhrumil:~$ cd dpate85
Dpate85@Dhrumil:~/dpate85$ ;s
-bash: syntax error near unexpected token `;'
Dpate85@Dhrumil:~/dpate85$ ls
hw1  hw2  README.md
Dpate85@Dhrumil:~/dpate85$ cd ..
Dpate85@Dhrumil:~$ cd public
Dpate85@Dhrumil:~/public$ ls
hw1  hw2
Dpate85@Dhrumil:~/public$ cd hw2
Dpate85@Dhrumil:~/public/hw2$ ls
puzzles
Dpate85@Dhrumil:~/public/hw2$ cd puzzles
Dpate85@Dhrumil:~/public/hw2/puzzles$ ls
0  1  2  3  4
Dpate85@Dhrumil:~/public/hw2/puzzles$ cp -r ~/public/hw2/puzzles/4 ~/dpate85/hw2/
puzzles/
Dpate85@Dhrumil:~/public/hw2/puzzles$ cd
Dpate85@Dhrumil:~$ ls
```

```
dpate85  public
Dpate85@Dhrumil:~$ cd dpate85
Dpate85@Dhrumil:~/dpate85$ ls
hw1  hw2  README.md
Dpate85@Dhrumil:~/dpate85$ cd hw2
Dpate85@Dhrumil:~/dpate85/hw2$ ls
puzzles
Dpate85@Dhrumil:~/dpate85/hw2$ cd puzzles
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  lib361.c  lib361.so  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cd dpate85
-bash: cd: dpate85: No such file or directory
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  lib361.c  lib361.so  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cd
Dpate85@Dhrumil:~$ ls
dpate85  public
Dpate85@Dhrumil:~$ cd ..
Dpate85@Dhrumil:/home$ ls
Dpate85
Dpate85@Dhrumil:/home$ cd ..
Dpate85@Dhrumil:/$ ls
bin   dev  home        initrd.img.old  lib64       media  opt   root  sbin  sys
usr  vmlinuz
boot  etc  initrd.img  lib             lost+found  mnt    proc  run   srv   tmp
var  vmlinuz.old
Dpate85@Dhrumil:/$ cd usr
Dpate85@Dhrumil:/usr$ ls
bin  games  include  lib  local  sbin  share  src
Dpate85@Dhrumil:/usr$ cd local
Dpate85@Dhrumil:/usr/local$ ls
bin  etc  games  include  lib  man  sbin  share  src
Dpate85@Dhrumil:/usr/local$ cd lib
Dpate85@Dhrumil:/usr/local/lib$ ls
python2.7  python3.4
Dpate85@Dhrumil:/usr/local/lib$ vi lib361.c
Dpate85@Dhrumil:/usr/local/lib$ sudo vi lib361.c
Dpate85@Dhrumil:/usr/local/lib$ gcc -shared -o lib361.so -fPIC lib361.c
/usr/bin/ld: cannot open output file lib361.so: Permission denied
collect2: error: ld returned 1 exit status
Dpate85@Dhrumil:/usr/local/lib$ ls
lib361.c  python2.7  python3.4
Dpate85@Dhrumil:/usr/local/lib$ sudo gcc -shared -o lib361.so -fPIC lib361.c
Dpate85@Dhrumil:/usr/local/lib$ ls
lib361.c  lib361.so  python2.7  python3.4
Dpate85@Dhrumil:/usr/local/lib$ cd
Dpate85@Dhrumil:~$ ls
dpate85  public
Dpate85@Dhrumil:~$ cd dpate85
```

```
Dpate85@Dhrumil:~/dpate85$ ls
hw1  hw2  README.md
Dpate85@Dhrumil:~/dpate85$ cd hw2
Dpate85@Dhrumil:~/dpate85/hw2$ ls
puzzles
Dpate85@Dhrumil:~/dpate85/hw2$ cd puzzles
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  lib361.c  lib361.so  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cd
Dpate85@Dhrumil:~$ ls
dpate85  public
Dpate85@Dhrumil:~$ cd ..
Dpate85@Dhrumil:/home$ ls
Dpate85
Dpate85@Dhrumil:/home$ cd .
Dpate85@Dhrumil:/home$ cd ..
Dpate85@Dhrumil:/$ ls
bin   dev  home        initrd.img.old  lib64       media  opt   root  sbin  sys
usr  vmlinuz
boot  etc  initrd.img  lib             lost+found  mnt    proc  run   srv   tmp
var  vmlinuz.old
Dpate85@Dhrumil:/$ cd etc
Dpate85@Dhrumil:/etc$ ls
acpi                    groff            mime.types              rmt
adduser.conf            group            mke2fs.conf             rpc
adjtime                 group-           modprobe.d              rsyslog.conf
alternatives            grub.d           modules                 rsyslog.d
apm                     gshadow          mtab                    samba
apparmor                gshadow-         nanorc                  screenrc
apparmor.d              hdparm.conf      network                 securetty
apport                  host.conf        networks                security
apt                     hostname         newt                    selinux
at.deny                 hosts            nologin                 services
bash.bashrc             hosts.allow      nscd.conf               sgml
bash_completion         hosts.deny       nsswitch.conf           shadow
bash_completion.d       init             opt                     shadow-
bindresvport.blacklist  init.d           os-release              shells
blkid.conf              initramfs-tools  overlayroot.conf        skel
blkid.tab               inputrc          overlayroot.local.conf  ssh
byobu                   insserv          pam.conf                ssl
ca-certificates         insserv.conf     pam.d                   subgid
ca-certificates.conf    insserv.conf.d   passwd                  subgid-
calendar                iproute2         passwd-                 subuid
chatscripts             issue            perl                    subuid-
cloud                   issue.net        pm                      sudoers
console-setup           kbd              polkit-1                sudoers.d
cron.d                  kernel           pollinate               sysctl.conf
cron.daily              kernel-img.conf  popularity-contest.conf  sysctl.d
cron.hourly             landscape        ppp                     systemd
```

```
cron.monthly            ldap              profile                 terminfo
crontab                 ld.so.cache       profile.d               timezone
cron.weekly             ld.so.conf        protocols               ucf.conf
crypttab                ld.so.conf.d      python                  udev
dbus-1                  legal             python2.7               ufw
debconf.conf            libaudit.conf     python3                 updatedb.conf
debian_version          libnl-3           python3.4               update-manager
default                 locale.alias      rc0.d                   update-motd.d
deluser.conf            localtime         rc1.d                   update-notifier
depmod.d                logcheck          rc2.d                   upstart-xsessio
ns
dhcp                    login.defs        rc3.d                   vim
dpkg                    logrotate.conf    rc4.d                   vmware-tools
ec2_version             logrotate.d       rc5.d                   vtrgb
environment             lsb-release       rc6.d                   w3m
fonts                   ltrace.conf       rc.local                waagent.conf
fstab                   magic             rcS.d                   wgetrc
fstab.d                 magic.mime        request-key.conf        X11
fuse.conf               mailcap           request-key.d           xdg
gai.conf                mailcap.order     resolvconf              xml
gdb                     manpath.config    resolv.conf             zsh_command_not
_found
Dpate85@Dhrumil:/etc$ ls *.conf
adduser.conf          gai.conf         libaudit.conf   overlayroot.conf         r
syslog.conf
blkid.conf            hdparm.conf      logrotate.conf  overlayroot.local.conf   s
ysctl.conf
ca-certificates.conf  host.conf        ltrace.conf     pam.conf                 u
cf.conf
debconf.conf          insserv.conf     mke2fs.conf     popularity-contest.conf  u
pdatedb.conf
deluser.conf          kernel-img.conf  nscd.conf       request-key.conf         w
aagent.conf
fuse.conf             ld.so.conf       nsswitch.conf   resolv.conf
Dpate85@Dhrumil:/etc$ sudo vi ls.do.conf
Dpate85@Dhrumil:/etc$ sudo vi ls.so.conf
Dpate85@Dhrumil:/etc$ sudo vi ld.so.conf
Dpate85@Dhrumil:/etc$ cd
Dpate85@Dhrumil:~$ cd dpate85
Dpate85@Dhrumil:~/dpate85$ ls
hw1  hw2  README.md
Dpate85@Dhrumil:~/dpate85$ cd hw2
Dpate85@Dhrumil:~/dpate85/hw2$ ls
puzzles
Dpate85@Dhrumil:~/dpate85/hw2$ cd puzzles
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ls
0  1  2  3  4  howto.txt  iamspecial  lib361.c  lib361.so  secrets.txt
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ./4
this program tests the implementation of a dynamically linked library.
4: get_sum.c:20: main: Assertion `result == 4' failed.
Aborted (core dumped)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -s 4
```

```
4:     file format elf64-x86-64

Contents of section .interp:
 400238 2f6c6962 36342f6c 642d6c69 6e75782d  /lib64/ld-linux-
 400248 7838362d 36342e73 6f2e3200           x86-64.so.2.
Contents of section .note.ABI-tag:
 400254 04000000 10000000 01000000 474e5500  ............GNU.
 400264 00000000 02000000 06000000 18000000  ................
Contents of section .note.gnu.build-id:
 400274 04000000 14000000 03000000 474e5500  ............GNU.
 400284 516c99c4 5c7b1cd5 13589f91 ae029c0f  Ql..\{...X......
 400294 1528d553                             .(.S
Contents of section .gnu.hash:
 400298 03000000 0e000000 01000000 06000000  ................
 4002a8 88c02001 00044009 0e000000 10000000  .. ...@.........
 4002b8 12000000 4245d5ec bbe3927c d871581c  ....BE.....|.qX.
 4002c8 b98df10e ebd3ef0e                    ........
Contents of section .dynsym:
 4002d0 00000000 00000000 00000000 00000000  ................
 4002e0 00000000 00000000 0b000000 20000000  ............ ...
 4002f0 00000000 00000000 00000000 00000000  ................
 400300 8a000000 12000000 00000000 00000000  ................
 400310 00000000 00000000 6a000000 12000000  ........j.......
 400320 00000000 00000000 00000000 00000000  ................
 400330 bc000000 12000000 00000000 00000000  ................
 400340 00000000 00000000 8f000000 12000000  ................
 400350 00000000 00000000 00000000 00000000  ................
 400360 ae000000 12000000 00000000 00000000  ................
 400370 00000000 00000000 a0000000 12000000  ................
 400380 00000000 00000000 00000000 00000000  ................
 400390 ce000000 12000000 00000000 00000000  ................
 4003a0 00000000 00000000 b5000000 12000000  ................
 4003b0 00000000 00000000 00000000 00000000  ................
 4003c0 27000000 20000000 00000000 00000000  '... ...........
 4003d0 00000000 00000000 c3000000 12000000  ................
 4003e0 00000000 00000000 00000000 00000000  ................
 4003f0 36000000 20000000 00000000 00000000  6... ...........
 400400 00000000 00000000 4a000000 20000000  ........J... ...
 400410 00000000 00000000 00000000 00000000  ................
 400420 e0000000 10001800 0c216000 00000000  .........!`.....
 400430 00000000 00000000 f3000000 10001900  ................
 400440 10216000 00000000 00000000 00000000  .!`.............
 400450 e7000000 10001900 0c216000 00000000  .........!`.....
 400460 00000000 00000000 64000000 12000b00  ........d.......
 400470 08074000 00000000 00000000 00000000  ..@.............
 400480 7a000000 12000e00 140d4000 00000000  z.........@.....
 400490 00000000 00000000                    ........
Contents of section .dynstr:
 400498 006c6962 3336312e 736f005f 49544d5f  .lib361.so._ITM_
 4004a8 64657265 67697374 6572544d 436c6f6e  deregisterTMClon
 4004b8 65546162 6c65005f 5f676d6f 6e5f7374  eTable.__gmon_st
 4004c8 6172745f 5f005f4a 765f5265 67697374  art__._Jv_Regist
 4004d8 6572436c 61737365 73005f49 544d5f72  erClasses._ITM_r
```

```
 4004e8 65676973 74657254 4d436c6f 6e655461  egisterTMCloneTa
 4004f8 626c6500 5f696e69 74007365 63726574  ble._init.secret
 400508 6f706572 6174696f 6e005f66 696e6900  operation._fini.
 400518 6c696263 2e736f2e 36007075 7473005f  libc.so.6.puts._
 400528 5f737461 636b5f63 686b5f66 61696c00  _stack_chk_fail.
 400538 5f5f6173 73657274 5f666169 6c007072  __assert_fail.pr
 400548 696e7466 0063616c 6c6f6300 7374726c  intf.calloc.strl
 400558 656e0067 65746c6f 67696e5f 72005f5f  en.getlogin_r.__
 400568 6c696263 5f737461 72745f6d 61696e00  libc_start_main.
 400578 5f656461 7461005f 5f627373 5f737461  _edata.__bss_sta
 400588 7274005f 656e6400 474c4942 435f322e  rt._end.GLIBC_2.
 400598 3400474c 4942435f 322e322e 3500      4.GLIBC_2.2.5.
Contents of section .gnu.version:
 4005a6 00000000 02000000 02000300 02000200  ................
 4005b6 02000200 00000200 00000000 01000100  ................
 4005c6 01000100 0100                        ......
Contents of section .gnu.version_r:
 4005d0 01000200 80000000 10000000 00000000  ................
 4005e0 1469690d 00000300 f8000000 10000000  .ii.............
 4005f0 751a6909 00000200 02010000 00000000  u.i.............
Contents of section .rela.dyn:
 400600 f81f6000 00000000 06000000 0a000000  ..`.............
 400610 00000000 00000000                    ........
Contents of section .rela.plt:
 400618 18206000 00000000 07000000 02000000  . `.............
 400628 00000000 00000000 20206000 00000000  ........  `.....
 400638 07000000 03000000 00000000 00000000  ................
 400648 28206000 00000000 07000000 04000000  ( `.............
 400658 00000000 00000000 30206000 00000000  ........0 `.....
 400668 07000000 05000000 00000000 00000000  ................
 400678 38206000 00000000 07000000 06000000  8 `.............
 400688 00000000 00000000 40206000 00000000  ........@ `.....
 400698 07000000 07000000 00000000 00000000  ................
 4006a8 48206000 00000000 07000000 08000000  H `.............
 4006b8 00000000 00000000 50206000 00000000  ........P `.....
 4006c8 07000000 09000000 00000000 00000000  ................
 4006d8 58206000 00000000 07000000 0a000000  X `.............
 4006e8 00000000 00000000 60206000 00000000  ........` `.....
 4006f8 07000000 0b000000 00000000 00000000  ................
Contents of section .init:
 400708 4883ec08 488b05e5 18200048 85c07405  H...H.... .H..t.
 400718 e8a30000 004883c4 08c3               .....H....
Contents of section .plt:
 400730 ff35d218 2000ff25 d4182000 0f1f4000  .5.. ..%.. ...@.
 400740 ff25d218 20006800 000000e9 e0ffffff  .%.. .h.........
 400750 ff25ca18 20006801 000000e9 d0ffffff  .%.. .h.........
 400760 ff25c218 20006802 000000e9 c0ffffff  .%.. .h.........
 400770 ff25ba18 20006803 000000e9 b0ffffff  .%.. .h.........
 400780 ff25b218 20006804 000000e9 a0ffffff  .%.. .h.........
 400790 ff25aa18 20006805 000000e9 90ffffff  .%.. .h.........
 4007a0 ff25a218 20006806 000000e9 80ffffff  .%.. .h.........
 4007b0 ff259a18 20006807 000000e9 70ffffff  .%.. .h.....p...
 4007c0 ff259218 20006808 000000e9 60ffffff  .%.. .h.....`...
```

```
 4007d0 ff258a18 20006809 000000e9 50ffffff  .%.. .h.....P...
Contents of section .text:
 4007e0 31ed4989 d15e4889 e24883e4 f0505449  1.I..^H..H...PTI
 4007f0 c7c0100d 400048c7 c1a00c40 0048c7c7  ....@.H....@.H..
 400800 cd084000 e897ffff fff4660f 1f440000  ..@.......f..D..
 400810 b8172160 0055482d 10216000 4883f80e  ..!`.UH-.!`.H...
 400820 4889e577 025dc3b8 00000000 4885c074  H..w.].......H..t
 400830 f45dbf10 216000ff e00f1f80 00000000  .]..!`..........
 400840 b8102160 0055482d 10216000 48c1f803  ..!`.UH-.!`.H...
 400850 4889e548 89c248c1 ea3f4801 d048d1f8  H..H..H..?H..H..
 400860 75025dc3 ba000000 004885d2 74f45d48  u.].......H..t.]H
 400870 89c6bf10 216000ff e20f1f80 00000000  ....!`..........
 400880 803d8518 20000075 11554889 e5e87eff  .=.. ..u.UH...~.
 400890 ffff5dc6 05721820 0001f3c3 0f1f4000  ..]..r. ......@.
 4008a0 48833d68 15200000 741eb800 00000048  H.=h. ..t......H
 4008b0 85c07414 55bf101e 60004889 e5ffd05d  ..t.U...`.H....]
 4008c0 e97bffff ff0f1f00 e973ffff ff554889  .{.......s...UH.
 4008d0 e54883ec 10c745f4 01000000 c745f802  .H....E......E..
 4008e0 000000c7 45fc0000 0000bf70 0d4000e8  ....E......p.@..
 4008f0 4cfeffff be060000 00bf0300 0000e84d  L.............M
 400900 fefffff89 45fc837d fc0a7419 b9da0d40  ....E..}..t....@
 400910 00ba1200 0000beb7 0d4000bf c10d4000  .........@....@.
 400920 e86bfeff ff8b55f8 8b45f489 d689c7e8  .k....U..E......
 400930 1cfeffff 8945fc83 7dfc0474 19b9da0d  .....E..}..t....
 400940 4000ba14 000000be b70d4000 bfce0d40  @.........@....@
 400950 00e83afe ffff488b 05331720 004889c7  ..:...H..3. .H..
 400960 e8280000 004889c2 488b0d31 17200048  .(...H..H..1. .H
 400970 8b052217 20004889 ce4889c7 b8000000  ..". .H..H......
 400980 00e8fafd ffffb800 000000c9 c3554889  .............UH.
 400990 e5534881 ec380400 004889bd c8fbffff  .SH..8...H......
 4009a0 64488b04 25280000 00488945 e831c048  dH..%(...H.E.1.H
 4009b0 8d85e0fb ffffbe00 04000048 89c7e80d  ...........H....
 4009c0 fefffc7 85d4fbff ff000000 00eb3e8b  ..............>.
 4009d0 85d4fbff ff48980f b69405e0 fbffff8b  .....H..........
 4009e0 85d4fbff ff4863c8 488b85c8 fbffff48  .....Hc.H......H
 4009f0 01c80fb6 0031c28b 85d4fbff ff489888  .....1.......H..
 400a00 9405e0fb ffff8385 d4fbffff 018b85d4  ................
 400a10 fbffff48 63d8488d 85e0fbff ff4889c7  ...Hc.H......H..
 400a20 e83bfdff ff4839c3 72a58b85 d4fbffff  .;...H9.r.......
 400a30 4863c848 8d95d8fb ffff488d 85e0fbff  Hc.H......H.....
 400a40 ff4889ce 4889c7e8 1e000000 488b75e8  .H..H.......H.u.
 400a50 64483334 25280000 007405e8 10fdffff  dH34%(...t......
 400a60 4881c438 0400005b 5dc35548 89e54883  H..8...[].UH..H.
 400a70 ec404889 7dd84889 75d04889 55c8488b  .@H.}.H.u.H.U.H.
 400a80 45d04883 c00248ba abaaaaaa aaaaaaaa  E.H...H.........
 400a90 48f7e248 89d048d1 e8488d14 85000000  H..H..H..H......
 400aa0 00488b45 c8488910 488b45c8 488b00be  .H.E.H..H.E.H...
 400ab0 01000000 4889c7e8 f4fcffff 488945f8  ....H.......H.E.
 400ac0 48837df8 00750ab8 00000000 e9c00100  H.}..u..........
 400ad0 00c745e0 00000000 c745e400 000000e9  ..E......E......
 400ae0 3b010000 8b45e048 98483b45 d0731b8b  ;....E.H.H;E.s..
 400af0 45e08d50 018955e0 4863d048 8b45d848  E..P..U.Hc.H.E.H
 400b00 01d00fb6 000fb6c0 eb05b800 00000089  ................
```

```
 400b10 45e88b45 e0489848 3b45d073 1b8b45e0  E..E.H.H;E.s..E.
 400b20 8d500189 55e04863 d0488b45 d84801d0  .P..U.Hc.H.E.H..
 400b30 0fb6000f b6c0eb05 b8000000 008945ec  ..............E.
 400b40 8b45e048 98483b45 d0731b8b 45e08d50  .E.H.H;E.s..E..P
 400b50 018955e0 4863d048 8b45d848 01d00fb6  ..U.Hc.H.E.H....
 400b60 000fb6c0 eb05b800 00000089 45f08b45  ............E..E
 400b70 e8c1e010 89c28b45 ecc1e008 01c28b45  .......E.......E
 400b80 f001d089 45f48b45 e48d5001 8955e448  ....E..E..P..U.H
 400b90 63d0488b 45f84801 c28b45f4 c1e81283  c.H.E.H...E.....
 400ba0 e03f89c0 0fb680c0 20600088 028b45e4  .?...... `....E.
 400bb0 8d500189 55e44863 d0488b45 f84801c2  .P..U.Hc.H.E.H..
 400bc0 8b45f4c1 e80c83e0 3f89c00f b680c020  .E......?......
 400bd0 60008802 8b45e48d 50018955 e44863d0  `....E..P..U.Hc.
 400be0 488b45f8 4801c28b 45f4c1e8 0683e03f  H.E.H...E......?
 400bf0 89c00fb6 80c02060 0088028b 45e48d50  ...... `....E..P
 400c00 018955e4 4863d048 8b45f848 01c28b45  ..U.Hc.H.E.H...E
 400c10 f483e03f 89c00fb6 80c02060 0088028b  ...?...... `....
 400c20 45e04898 483b45d0 0f82b6fe ffffc745  E.H.H;E........E
 400c30 e0000000 00eb2448 8b45c848 8b108b45  ......$H.E.H...E
 400c40 e0489848 29c24889 d0488d50 ff488b45  .H.H).H..H.P.H.E
 400c50 f84801d0 c6003d83 45e00148 8b4dd048  .H....=.E..H.M.H
 400c60 baabaaaa aaaaaaaa aa4889c8 48f7e248  .........H..H..H
 400c70 d1ea4889 d04801c0 4801d048 29c14889  ..H..H..H..H).H.
 400c80 ca8b0495 00216000 3b45e07f aa488b45  .....!`.;E...H.E
 400c90 f8c9c366 2e0f1f84 00000000 000f1f00  ...f............
 400ca0 41574189 ff415649 89f64155 4989d541  AWA..AVI..AUI..A
 400cb0 544c8d25 48112000 55488d2d 48112000  TL.%H. .UH.-H. .
 400cc0 534c29e5 31db48c1 fd034883 ec08e835  SL).1.H...H....5
 400cd0 fafffff48 85ed741e 0f1f8400 00000000  ...H..t.........
 400ce0 4c89ea4c 89f64489 ff41ff14 dc4883c3  L..L..D..A...H..
 400cf0 014839eb 75ea4883 c4085b5d 415c415d  .H9.u.H...[]A\A]
 400d00 415e415f c366662e 0f1f8400 00000000  A^A_.ff.........
 400d10 f3c3                                 ..
Contents of section .fini:
 400d14 4883ec08 4883c408 c3                 H...H....
Contents of section .rodata:
 400d20 01000200 00000000 33343536 37383930  ........34567890
 400d30 31323334 35363738 39303132 00257325  123456789012.%s%
 400d40 730a0000 00000000 796f7520 77696e21  s.......you win!
 400d50 20746865 20736563 72657420 69733a0a   the secret is:.
 400d60 0062616e 67617261 6e670000 00000000  .bangarang......
 400d70 74686973 2070726f 6772616d 20746573  this program tes
 400d80 74732074 68652069 6d706c65 6d656e74  ts the implement
 400d90 6174696f 6e206f66 20612064 796e616d  ation of a dynam
 400da0 6963616c 6c79206c 696e6b65 64206c69  ically linked li
 400db0 62726172 792e0067 65745f73 756d2e63  brary..get_sum.c
 400dc0 00726573 756c7420 3d3d2031 30007265  .result == 10.re
 400dd0 73756c74 203d3d20 34006d61 696e00    sult == 4.main.
Contents of section .eh_frame_hdr:
 400de0 011b033b 44000000 07000000 50f9ffff  ...;D.......P...
 400df0 90000000 00faffff 60000000 edfaffff  ........`.......
 400e00 b8000000 adfbffff d8000000 8afcffff  ................
 400e10 00010000 c0feffff 20010000 30ffffff  ........ ...0...
```

```
 400e20 68010000                             h...
Contents of section .eh_frame:
 400e28 14000000 00000000 017a5200 01781001  .........zR..x..
 400e38 1b0c0708 90010710 14000000 1c000000  ................
 400e48 98f9ffff 2a000000 00000000 00000000  ....*...........
 400e58 14000000 00000000 017a5200 01781001  .........zR..x..
 400e68 1b0c0708 90010000 24000000 1c000000  ........$.......
 400e78 b8f8ffff b0000000 000e1046 0e184a0f  ...........F..J.
 400e88 0b770880 003f1a3b 2a332422 00000000  .w...?.;*3$"....
 400e98 1c000000 44000000 2dfaffff c0000000  ....D...-.......
 400ea8 00410e10 8602430d 0602bb0c 07080000  .A....C.........
 400eb8 24000000 64000000 cdfaffff dd000000  $...d...........
 400ec8 00410e10 8602430d 06488303 02d00c07  .A....C..H......
 400ed8 08000000 00000000 1c000000 8c000000  ................
 400ee8 82fbffff 29020000 00410e10 8602430d  ....)....A....C.
 400ef8 06032402 0c070800 44000000 ac000000  ..$.....D.......
 400f08 98fdffff 65000000 00420e10 8f02450e  ....e....B....E.
 400f18 188e0345 0e208d04 450e288c 05480e30  ...E. ..E.(..H.0
 400f28 8606480e 3883074d 0e406c0e 38410e30  ..H.8..M.@l.8A.0
 400f38 410e2842 0e20420e 18420e10 420e0800  A.(B. B..B..B...
 400f48 14000000 f4000000 c0fdffff 02000000  ................
 400f58 00000000 00000000 00000000           ............
Contents of section .init_array:
 601e00 a0084000 00000000                    ..@.....
Contents of section .fini_array:
 601e08 80084000 00000000                    ..@.....
Contents of section .jcr:
 601e10 00000000 00000000                    ........
Contents of section .dynamic:
 601e18 01000000 00000000 01000000 00000000  ................
 601e28 01000000 00000000 80000000 00000000  ................
 601e38 0c000000 00000000 08074000 00000000  ..........@.....
 601e48 0d000000 00000000 140d4000 00000000  ..........@.....
 601e58 19000000 00000000 001e6000 00000000  ..........`.....
 601e68 1b000000 00000000 08000000 00000000  ................
 601e78 1a000000 00000000 081e6000 00000000  ..........`.....
 601e88 1c000000 00000000 08000000 00000000  ................
 601e98 f5feff6f 00000000 98024000 00000000  ...o......@.....
 601ea8 05000000 00000000 98044000 00000000  ..........@.....
 601eb8 06000000 00000000 d0024000 00000000  ..........@.....
 601ec8 0a000000 00000000 0e010000 00000000  ................
 601ed8 0b000000 00000000 18000000 00000000  ................
 601ee8 15000000 00000000 00000000 00000000  ................
 601ef8 03000000 00000000 00206000 00000000  ......... `.....
 601f08 02000000 00000000 f0000000 00000000  ................
 601f18 14000000 00000000 07000000 00000000  ................
 601f28 17000000 00000000 18064000 00000000  ..........@.....
 601f38 07000000 00000000 00064000 00000000  ..........@.....
 601f48 08000000 00000000 18000000 00000000  ................
 601f58 09000000 00000000 18000000 00000000  ................
 601f68 fefffff6f 00000000 d0054000 00000000  ...o......@.....
 601f78 ffffff6f 00000000 01000000 00000000  ...o............
 601f88 f0ffff6f 00000000 a6054000 00000000  ...o......@.....
```

```
 601f98 00000000 00000000 00000000 00000000  ................
 601fa8 00000000 00000000 00000000 00000000  ................
 601fb8 00000000 00000000 00000000 00000000  ................
 601fc8 00000000 00000000 00000000 00000000  ................
 601fd8 00000000 00000000 00000000 00000000  ................
 601fe8 00000000 00000000 00000000 00000000  ................
Contents of section .got:
 601ff8 00000000 00000000                    ........
Contents of section .got.plt:
 602000 181e6000 00000000 00000000 00000000  ..`.............
 602010 00000000 00000000 46074000 00000000  ........F.@.....
 602020 56074000 00000000 66074000 00000000  V.@.....f.@.....
 602030 76074000 00000000 86074000 00000000  v.@.......@.....
 602040 96074000 00000000 a6074000 00000000  ..@.......@.....
 602050 b6074000 00000000 c6074000 00000000  ..@.......@.....
 602060 d6074000 00000000                    ..@.....
Contents of section .data:
 602080 00000000 00000000 00000000 00000000  ................
 602090 280d4000 00000000 3d0d4000 00000000  (.@.....=.@.....
 6020a0 480d4000 00000000 00000000 00000000  H.@.............
 6020b0 00000000 00000000 00000000 00000000  ................
 6020c0 41424344 45464748 494a4b4c 4d4e4f50  ABCDEFGHIJKLMNOP
 6020d0 51525354 55565758 595a6162 63646566  QRSTUVWXYZabcdef
 6020e0 6768696a 6b6c6d6e 6f707172 73747576  ghijklmnopqrstuv
 6020f0 7778797a 30313233 34353637 38392b2f  wxyz0123456789+/
 602100 00000000 02000000 01000000           ............
Contents of section .comment:
 0000 4743433a 20285562 756e7475 20342e38  GCC: (Ubuntu 4.8
 0010 2e342d32 7562756e 7475317e 31342e30  .4-2ubuntu1~14.0
 0020 34292034 2e382e34 00474343 3a202855  4) 4.8.4.GCC: (U
 0030 62756e74 7520342e 382e322d 31397562  buntu 4.8.2-19ub
 0040 756e7475 31292034 2e382e32 00        untu1) 4.8.2.
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ objdump -S 4

4:     file format elf64-x86-64


Disassembly of section .init:

0000000000400708 <_init>:
  400708:       48 83 ec 08             sub    $0x8,%rsp
  40070c:       48 8b 05 e5 18 20 00    mov    0x2018e5(%rip),%rax        # 601ff
8 <_fini+0x2012e4>
  400713:       48 85 c0                test   %rax,%rax
  400716:       74 05                   je     40071d <_init+0x15>
  400718:       e8 a3 00 00 00          callq  4007c0 <__gmon_start__@plt>
  40071d:       48 83 c4 08             add    $0x8,%rsp
  400721:       c3                      retq

Disassembly of section .plt:

0000000000400730 <puts@plt-0x10>:
  400730:       ff 35 d2 18 20 00       pushq  0x2018d2(%rip)        # 602008 <_f
```

```
ini+0x2012f4>
  400736:       ff 25 d4 18 20 00       jmpq   *0x2018d4(%rip)        # 602010 <_
fini+0x2012fc>
  40073c:       0f 1f 40 00             nopl   0x0(%rax)

0000000000400740 <puts@plt>:
  400740:       ff 25 d2 18 20 00       jmpq   *0x2018d2(%rip)        # 602018 <_
fini+0x201304>
  400746:       68 00 00 00 00          pushq  $0x0
  40074b:       e9 e0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400750 <secretoperation@plt>:
  400750:       ff 25 ca 18 20 00       jmpq   *0x2018ca(%rip)        # 602020 <_
fini+0x20130c>
  400756:       68 01 00 00 00          pushq  $0x1
  40075b:       e9 d0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400760 <strlen@plt>:
  400760:       ff 25 c2 18 20 00       jmpq   *0x2018c2(%rip)        # 602028 <_
fini+0x201314>
  400766:       68 02 00 00 00          pushq  $0x2
  40076b:       e9 c0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400770 <__stack_chk_fail@plt>:
  400770:       ff 25 ba 18 20 00       jmpq   *0x2018ba(%rip)        # 602030 <_
fini+0x20131c>
  400776:       68 03 00 00 00          pushq  $0x3
  40077b:       e9 b0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400780 <printf@plt>:
  400780:       ff 25 b2 18 20 00       jmpq   *0x2018b2(%rip)        # 602038 <_
fini+0x201324>
  400786:       68 04 00 00 00          pushq  $0x4
  40078b:       e9 a0 ff ff ff          jmpq   400730 <_init+0x28>

0000000000400790 <__assert_fail@plt>:
  400790:       ff 25 aa 18 20 00       jmpq   *0x2018aa(%rip)        # 602040 <_
fini+0x20132c>
  400796:       68 05 00 00 00          pushq  $0x5
  40079b:       e9 90 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007a0 <__libc_start_main@plt>:
  4007a0:       ff 25 a2 18 20 00       jmpq   *0x2018a2(%rip)        # 602048 <_
fini+0x201334>
  4007a6:       68 06 00 00 00          pushq  $0x6
  4007ab:       e9 80 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007b0 <calloc@plt>:
  4007b0:       ff 25 9a 18 20 00       jmpq   *0x20189a(%rip)        # 602050 <_
fini+0x20133c>
  4007b6:       68 07 00 00 00          pushq  $0x7
  4007bb:       e9 70 ff ff ff          jmpq   400730 <_init+0x28>
```

```
00000000004007c0 <__gmon_start__@plt>:
  4007c0:       ff 25 92 18 20 00       jmpq   *0x201892(%rip)        # 602058 <_
fini+0x201344>
  4007c6:       68 08 00 00 00          pushq  $0x8
  4007cb:       e9 60 ff ff ff          jmpq   400730 <_init+0x28>

00000000004007d0 <getlogin_r@plt>:
  4007d0:       ff 25 8a 18 20 00       jmpq   *0x20188a(%rip)        # 602060 <_
fini+0x20134c>
  4007d6:       68 09 00 00 00          pushq  $0x9
  4007db:       e9 50 ff ff ff          jmpq   400730 <_init+0x28>

Disassembly of section .text:

00000000004007e0 <.text>:
  4007e0:       31 ed                   xor    %ebp,%ebp
  4007e2:       49 89 d1                mov    %rdx,%r9
  4007e5:       5e                      pop    %rsi
  4007e6:       48 89 e2                mov    %rsp,%rdx
  4007e9:       48 83 e4 f0             and    $0xfffffffffffffff0,%rsp
  4007ed:       50                      push   %rax
  4007ee:       54                      push   %rsp
  4007ef:       49 c7 c0 10 0d 40 00    mov    $0x400d10,%r8
  4007f6:       48 c7 c1 a0 0c 40 00    mov    $0x400ca0,%rcx
  4007fd:       48 c7 c7 cd 08 40 00    mov    $0x4008cd,%rdi
  400804:       e8 97 ff ff ff          callq  4007a0 <__libc_start_main@plt>
  400809:       f4                      hlt
  40080a:       66 0f 1f 44 00 00       nopw   0x0(%rax,%rax,1)
  400810:       b8 17 21 60 00          mov    $0x602117,%eax
  400815:       55                      push   %rbp
  400816:       48 2d 10 21 60 00       sub    $0x602110,%rax
  40081c:       48 83 f8 0e             cmp    $0xe,%rax
  400820:       48 89 e5                mov    %rsp,%rbp
  400823:       77 02                   ja     400827 <getlogin_r@plt+0x57>
  400825:       5d                      pop    %rbp
  400826:       c3                      retq
  400827:       b8 00 00 00 00          mov    $0x0,%eax
  40082c:       48 85 c0                test   %rax,%rax
  40082f:       74 f4                   je     400825 <getlogin_r@plt+0x55>
  400831:       5d                      pop    %rbp
  400832:       bf 10 21 60 00          mov    $0x602110,%edi
  400837:       ff e0                   jmpq   *%rax
  400839:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400840:       b8 10 21 60 00          mov    $0x602110,%eax
  400845:       55                      push   %rbp
  400846:       48 2d 10 21 60 00       sub    $0x602110,%rax
  40084c:       48 c1 f8 03             sar    $0x3,%rax
  400850:       48 89 e5                mov    %rsp,%rbp
  400853:       48 89 c2                mov    %rax,%rdx
  400856:       48 c1 ea 3f             shr    $0x3f,%rdx
  40085a:       48 01 d0                add    %rdx,%rax
  40085d:       48 d1 f8                sar    %rax
  400860:       75 02                   jne    400864 <getlogin_r@plt+0x94>
```

```
  400862:       5d                      pop    %rbp
  400863:       c3                      retq
  400864:       ba 00 00 00 00          mov    $0x0,%edx
  400869:       48 85 d2                test   %rdx,%rdx
  40086c:       74 f4                   je     400862 <getlogin_r@plt+0x92>
  40086e:       5d                      pop    %rbp
  40086f:       48 89 c6                mov    %rax,%rsi
  400872:       bf 10 21 60 00          mov    $0x602110,%edi
  400877:       ff e2                   jmpq   *%rdx
  400879:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
  400880:       80 3d 85 18 20 00 00    cmpb   $0x0,0x201885(%rip)        # 60210
c <_edata>
  400887:       75 11                   jne    40089a <getlogin_r@plt+0xca>
  400889:       55                      push   %rbp
  40088a:       48 89 e5                mov    %rsp,%rbp
  40088d:       e8 7e ff ff ff          callq  400810 <getlogin_r@plt+0x40>
  400892:       5d                      pop    %rbp
  400893:       c6 05 72 18 20 00 01    movb   $0x1,0x201872(%rip)        # 60210
c <_edata>
  40089a:       f3 c3                   repz retq
  40089c:       0f 1f 40 00             nopl   0x0(%rax)
  4008a0:       48 83 3d 68 15 20 00    cmpq   $0x0,0x201568(%rip)        # 601e1
0 <_fini+0x2010fc>
  4008a7:       00
  4008a8:       74 1e                   je     4008c8 <getlogin_r@plt+0xf8>
  4008aa:       b8 00 00 00 00          mov    $0x0,%eax
  4008af:       48 85 c0                test   %rax,%rax
  4008b2:       74 14                   je     4008c8 <getlogin_r@plt+0xf8>
  4008b4:       55                      push   %rbp
  4008b5:       bf 10 1e 60 00          mov    $0x601e10,%edi
  4008ba:       48 89 e5                mov    %rsp,%rbp
  4008bd:       ff d0                   callq  *%rax
  4008bf:       5d                      pop    %rbp
  4008c0:       e9 7b ff ff ff          jmpq   400840 <getlogin_r@plt+0x70>
  4008c5:       0f 1f 00                nopl   (%rax)
  4008c8:       e9 73 ff ff ff          jmpq   400840 <getlogin_r@plt+0x70>
  4008cd:       55                      push   %rbp
  4008ce:       48 89 e5                mov    %rsp,%rbp
  4008d1:       48 83 ec 10             sub    $0x10,%rsp
  4008d5:       c7 45 f4 01 00 00 00    movl   $0x1,-0xc(%rbp)
  4008dc:       c7 45 f8 02 00 00 00    movl   $0x2,-0x8(%rbp)
  4008e3:       c7 45 fc 00 00 00 00    movl   $0x0,-0x4(%rbp)
  4008ea:       bf 70 0d 40 00          mov    $0x400d70,%edi
  4008ef:       e8 4c fe ff ff          callq  400740 <puts@plt>
  4008f4:       be 06 00 00 00          mov    $0x6,%esi
  4008f9:       bf 03 00 00 00          mov    $0x3,%edi
  4008fe:       e8 4d fe ff ff          callq  400750 <secretoperation@plt>
  400903:       89 45 fc                mov    %eax,-0x4(%rbp)
  400906:       83 7d fc 0a             cmpl   $0xa,-0x4(%rbp)
  40090a:       74 19                   je     400925 <getlogin_r@plt+0x155>
  40090c:       b9 da 0d 40 00          mov    $0x400dda,%ecx
  400911:       ba 12 00 00 00          mov    $0x12,%edx
  400916:       be b7 0d 40 00          mov    $0x400db7,%esi
```

```
  40091b:       bf c1 0d 40 00          mov    $0x400dc1,%edi
  400920:       e8 6b fe ff ff          callq  400790 <__assert_fail@plt>
  400925:       8b 55 f8                mov    -0x8(%rbp),%edx
  400928:       8b 45 f4                mov    -0xc(%rbp),%eax
  40092b:       89 d6                   mov    %edx,%esi
  40092d:       89 c7                   mov    %eax,%edi
  40092f:       e8 1c fe ff ff          callq  400750 <secretoperation@plt>
  400934:       89 45 fc                mov    %eax,-0x4(%rbp)
  400937:       83 7d fc 04             cmpl   $0x4,-0x4(%rbp)
  40093b:       74 19                   je     400956 <getlogin_r@plt+0x186>
  40093d:       b9 da 0d 40 00          mov    $0x400dda,%ecx
  400942:       ba 14 00 00 00          mov    $0x14,%edx
  400947:       be b7 0d 40 00          mov    $0x400db7,%esi
  40094c:       bf ce 0d 40 00          mov    $0x400dce,%edi
  400951:       e8 3a fe ff ff          callq  400790 <__assert_fail@plt>
  400956:       48 8b 05 33 17 20 00    mov    0x201733(%rip),%rax        # 60209
0 <_fini+0x20137c>
  40095d:       48 89 c7                mov    %rax,%rdi
  400960:       e8 28 00 00 00          callq  40098d <getlogin_r@plt+0x1bd>
  400965:       48 89 c2                mov    %rax,%rdx
  400968:       48 8b 0d 31 17 20 00    mov    0x201731(%rip),%rcx        # 6020a
0 <_fini+0x20138c>
  40096f:       48 8b 05 22 17 20 00    mov    0x201722(%rip),%rax        # 60209
8 <_fini+0x201384>
  400976:       48 89 ce                mov    %rcx,%rsi
  400979:       48 89 c7                mov    %rax,%rdi
  40097c:       b8 00 00 00 00          mov    $0x0,%eax
  400981:       e8 fa fd ff ff          callq  400780 <printf@plt>
  400986:       b8 00 00 00 00          mov    $0x0,%eax
  40098b:       c9                      leaveq
  40098c:       c3                      retq
  40098d:       55                      push   %rbp
  40098e:       48 89 e5                mov    %rsp,%rbp
  400991:       53                      push   %rbx
  400992:       48 81 ec 38 04 00 00    sub    $0x438,%rsp
  400999:       48 89 bd c8 fb ff ff    mov    %rdi,-0x438(%rbp)
  4009a0:       64 48 8b 04 25 28 00    mov    %fs:0x28,%rax
  4009a7:       00 00
  4009a9:       48 89 45 e8             mov    %rax,-0x18(%rbp)
  4009ad:       31 c0                   xor    %eax,%eax
  4009af:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
  4009b6:       be 00 04 00 00          mov    $0x400,%esi
  4009bb:       48 89 c7                mov    %rax,%rdi
  4009be:       e8 0d fe ff ff          callq  4007d0 <getlogin_r@plt>
  4009c3:       c7 85 d4 fb ff ff 00    movl   $0x0,-0x42c(%rbp)
  4009ca:       00 00 00
  4009cd:       eb 3e                   jmp    400a0d <getlogin_r@plt+0x23d>
  4009cf:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  4009d5:       48 98                   cltq
  4009d7:       0f b6 94 05 e0 fb ff    movzbl -0x420(%rbp,%rax,1),%edx
  4009de:       ff
  4009df:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
  4009e5:       48 63 c8                movslq %eax,%rcx
```

```
4009e8:       48 8b 85 c8 fb ff ff    mov    -0x438(%rbp),%rax
4009ef:       48 01 c8                add    %rcx,%rax
4009f2:       0f b6 00                movzbl (%rax),%eax
4009f5:       31 c2                   xor    %eax,%edx
4009f7:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
4009fd:       48 98                   cltq
4009ff:       88 94 05 e0 fb ff ff    mov    %dl,-0x420(%rbp,%rax,1)
400a06:       83 85 d4 fb ff ff 01    addl   $0x1,-0x42c(%rbp)
400a0d:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
400a13:       48 63 d8                movslq %eax,%rbx
400a16:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
400a1d:       48 89 c7                mov    %rax,%rdi
400a20:       e8 3b fd ff ff          callq  400760 <strlen@plt>
400a25:       48 39 c3                cmp    %rax,%rbx
400a28:       72 a5                   jb     4009cf <getlogin_r@plt+0x1ff>
400a2a:       8b 85 d4 fb ff ff       mov    -0x42c(%rbp),%eax
400a30:       48 63 c8                movslq %eax,%rcx
400a33:       48 8d 95 d8 fb ff ff    lea    -0x428(%rbp),%rdx
400a3a:       48 8d 85 e0 fb ff ff    lea    -0x420(%rbp),%rax
400a41:       48 89 ce                mov    %rcx,%rsi
400a44:       48 89 c7                mov    %rax,%rdi
400a47:       e8 1e 00 00 00          callq  400a6a <getlogin_r@plt+0x29a>
400a4c:       48 8b 75 e8             mov    -0x18(%rbp),%rsi
400a50:       64 48 33 34 25 28 00    xor    %fs:0x28,%rsi
400a57:       00 00
400a59:       74 05                   je     400a60 <getlogin_r@plt+0x290>
400a5b:       e8 10 fd ff ff          callq  400770 <__stack_chk_fail@plt>
400a60:       48 81 c4 38 04 00 00    add    $0x438,%rsp
400a67:       5b                      pop    %rbx
400a68:       5d                      pop    %rbp
400a69:       c3                      retq
400a6a:       55                      push   %rbp
400a6b:       48 89 e5                mov    %rsp,%rbp
400a6e:       48 83 ec 40             sub    $0x40,%rsp
400a72:       48 89 7d d8             mov    %rdi,-0x28(%rbp)
400a76:       48 89 75 d0             mov    %rsi,-0x30(%rbp)
400a7a:       48 89 55 c8             mov    %rdx,-0x38(%rbp)
400a7e:       48 8b 45 d0             mov    -0x30(%rbp),%rax
400a82:       48 83 c0 02             add    $0x2,%rax
400a86:       48 ba ab aa aa aa aa    movabs $0xaaaaaaaaaaaaaaab,%rdx
400a8d:       aa aa aa
400a90:       48 f7 e2                mul    %rdx
400a93:       48 89 d0                mov    %rdx,%rax
400a96:       48 d1 e8                shr    %rax
400a99:       48 8d 14 85 00 00 00    lea    0x0(,%rax,4),%rdx
400aa0:       00
400aa1:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400aa5:       48 89 10                mov    %rdx,(%rax)
400aa8:       48 8b 45 c8             mov    -0x38(%rbp),%rax
400aac:       48 8b 00                mov    (%rax),%rax
400aaf:       be 01 00 00 00          mov    $0x1,%esi
400ab4:       48 89 c7                mov    %rax,%rdi
400ab7:       e8 f4 fc ff ff          callq  4007b0 <calloc@plt>
```

```
400abc:       48 89 45 f8             mov    %rax,-0x8(%rbp)
400ac0:       48 83 7d f8 00          cmpq   $0x0,-0x8(%rbp)
400ac5:       75 0a                   jne    400ad1 <getlogin_r@plt+0x301>
400ac7:       b8 00 00 00 00          mov    $0x0,%eax
400acc:       e9 c0 01 00 00          jmpq   400c91 <getlogin_r@plt+0x4c1>
400ad1:       c7 45 e0 00 00 00 00    movl   $0x0,-0x20(%rbp)
400ad8:       c7 45 e4 00 00 00 00    movl   $0x0,-0x1c(%rbp)
400adf:       e9 3b 01 00 00          jmpq   400c1f <getlogin_r@plt+0x44f>
400ae4:       8b 45 e0                mov    -0x20(%rbp),%eax
400ae7:       48 98                   cltq
400ae9:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400aed:       73 1b                   jae    400b0a <getlogin_r@plt+0x33a>
400aef:       8b 45 e0                mov    -0x20(%rbp),%eax
400af2:       8d 50 01                lea    0x1(%rax),%edx
400af5:       89 55 e0                mov    %edx,-0x20(%rbp)
400af8:       48 63 d0                movslq %eax,%rdx
400afb:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400aff:       48 01 d0                add    %rdx,%rax
400b02:       0f b6 00                movzbl (%rax),%eax
400b05:       0f b6 c0                movzbl %al,%eax
400b08:       eb 05                   jmp    400b0f <getlogin_r@plt+0x33f>
400b0a:       b8 00 00 00 00          mov    $0x0,%eax
400b0f:       89 45 e8                mov    %eax,-0x18(%rbp)
400b12:       8b 45 e0                mov    -0x20(%rbp),%eax
400b15:       48 98                   cltq
400b17:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400b1b:       73 1b                   jae    400b38 <getlogin_r@plt+0x368>
400b1d:       8b 45 e0                mov    -0x20(%rbp),%eax
400b20:       8d 50 01                lea    0x1(%rax),%edx
400b23:       89 55 e0                mov    %edx,-0x20(%rbp)
400b26:       48 63 d0                movslq %eax,%rdx
400b29:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400b2d:       48 01 d0                add    %rdx,%rax
400b30:       0f b6 00                movzbl (%rax),%eax
400b33:       0f b6 c0                movzbl %al,%eax
400b36:       eb 05                   jmp    400b3d <getlogin_r@plt+0x36d>
400b38:       b8 00 00 00 00          mov    $0x0,%eax
400b3d:       89 45 ec                mov    %eax,-0x14(%rbp)
400b40:       8b 45 e0                mov    -0x20(%rbp),%eax
400b43:       48 98                   cltq
400b45:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
400b49:       73 1b                   jae    400b66 <getlogin_r@plt+0x396>
400b4b:       8b 45 e0                mov    -0x20(%rbp),%eax
400b4e:       8d 50 01                lea    0x1(%rax),%edx
400b51:       89 55 e0                mov    %edx,-0x20(%rbp)
400b54:       48 63 d0                movslq %eax,%rdx
400b57:       48 8b 45 d8             mov    -0x28(%rbp),%rax
400b5b:       48 01 d0                add    %rdx,%rax
400b5e:       0f b6 00                movzbl (%rax),%eax
400b61:       0f b6 c0                movzbl %al,%eax
400b64:       eb 05                   jmp    400b6b <getlogin_r@plt+0x39b>
400b66:       b8 00 00 00 00          mov    $0x0,%eax
400b6b:       89 45 f0                mov    %eax,-0x10(%rbp)
```

```
400b6e:       8b 45 e8                mov    -0x18(%rbp),%eax
400b71:       c1 e0 10                shl    $0x10,%eax
400b74:       89 c2                   mov    %eax,%edx
400b76:       8b 45 ec                mov    -0x14(%rbp),%eax
400b79:       c1 e0 08                shl    $0x8,%eax
400b7c:       01 c2                   add    %eax,%edx
400b7e:       8b 45 f0                mov    -0x10(%rbp),%eax
400b81:       01 d0                   add    %edx,%eax
400b83:       89 45 f4                mov    %eax,-0xc(%rbp)
400b86:       8b 45 e4                mov    -0x1c(%rbp),%eax
400b89:       8d 50 01                lea    0x1(%rax),%edx
400b8c:       89 55 e4                mov    %edx,-0x1c(%rbp)
400b8f:       48 63 d0                movslq %eax,%rdx
400b92:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400b96:       48 01 c2                add    %rax,%rdx
400b99:       8b 45 f4                mov    -0xc(%rbp),%eax
400b9c:       c1 e8 12                shr    $0x12,%eax
400b9f:       83 e0 3f                and    $0x3f,%eax
400ba2:       89 c0                   mov    %eax,%eax
400ba4:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bab:       88 02                   mov    %al,(%rdx)
400bad:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bb0:       8d 50 01                lea    0x1(%rax),%edx
400bb3:       89 55 e4                mov    %edx,-0x1c(%rbp)
400bb6:       48 63 d0                movslq %eax,%rdx
400bb9:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400bbd:       48 01 c2                add    %rax,%rdx
400bc0:       8b 45 f4                mov    -0xc(%rbp),%eax
400bc3:       c1 e8 0c                shr    $0xc,%eax
400bc6:       83 e0 3f                and    $0x3f,%eax
400bc9:       89 c0                   mov    %eax,%eax
400bcb:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bd2:       88 02                   mov    %al,(%rdx)
400bd4:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bd7:       8d 50 01                lea    0x1(%rax),%edx
400bda:       89 55 e4                mov    %edx,-0x1c(%rbp)
400bdd:       48 63 d0                movslq %eax,%rdx
400be0:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400be4:       48 01 c2                add    %rax,%rdx
400be7:       8b 45 f4                mov    -0xc(%rbp),%eax
400bea:       c1 e8 06                shr    $0x6,%eax
400bed:       83 e0 3f                and    $0x3f,%eax
400bf0:       89 c0                   mov    %eax,%eax
400bf2:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
400bf9:       88 02                   mov    %al,(%rdx)
400bfb:       8b 45 e4                mov    -0x1c(%rbp),%eax
400bfe:       8d 50 01                lea    0x1(%rax),%edx
400c01:       89 55 e4                mov    %edx,-0x1c(%rbp)
400c04:       48 63 d0                movslq %eax,%rdx
400c07:       48 8b 45 f8             mov    -0x8(%rbp),%rax
400c0b:       48 01 c2                add    %rax,%rdx
400c0e:       8b 45 f4                mov    -0xc(%rbp),%eax
400c11:       83 e0 3f                and    $0x3f,%eax
```

```
  400c14:       89 c0                   mov    %eax,%eax
  400c16:       0f b6 80 c0 20 60 00    movzbl 0x6020c0(%rax),%eax
  400c1d:       88 02                   mov    %al,(%rdx)
  400c1f:       8b 45 e0                mov    -0x20(%rbp),%eax
  400c22:       48 98                   cltq
  400c24:       48 3b 45 d0             cmp    -0x30(%rbp),%rax
  400c28:       0f 82 b6 fe ff ff       jb     400ae4 <getlogin_r@plt+0x314>
  400c2e:       c7 45 e0 00 00 00 00    movl   $0x0,-0x20(%rbp)
  400c35:       eb 24                   jmp    400c5b <getlogin_r@plt+0x48b>
  400c37:       48 8b 45 c8             mov    -0x38(%rbp),%rax
  400c3b:       48 8b 10                mov    (%rax),%rdx
  400c3e:       8b 45 e0                mov    -0x20(%rbp),%eax
  400c41:       48 98                   cltq
  400c43:       48 29 c2                sub    %rax,%rdx
  400c46:       48 89 d0                mov    %rdx,%rax
  400c49:       48 8d 50 ff             lea    -0x1(%rax),%rdx
  400c4d:       48 8b 45 f8             mov    -0x8(%rbp),%rax
  400c51:       48 01 d0                add    %rdx,%rax
  400c54:       c6 00 3d                movb   $0x3d,(%rax)
  400c57:       83 45 e0 01             addl   $0x1,-0x20(%rbp)
  400c5b:       48 8b 4d d0             mov    -0x30(%rbp),%rcx
  400c5f:       48 ba ab aa aa aa aa    movabs $0xaaaaaaaaaaaaaaab,%rdx
  400c66:       aa aa aa
  400c69:       48 89 c8                mov    %rcx,%rax
  400c6c:       48 f7 e2                mul    %rdx
  400c6f:       48 d1 ea                shr    %rdx
  400c72:       48 89 d0                mov    %rdx,%rax
  400c75:       48 01 c0                add    %rax,%rax
  400c78:       48 01 d0                add    %rdx,%rax
  400c7b:       48 29 c1                sub    %rax,%rcx
  400c7e:       48 89 ca                mov    %rcx,%rdx
  400c81:       8b 04 95 00 21 60 00    mov    0x602100(,%rdx,4),%eax
  400c88:       3b 45 e0                cmp    -0x20(%rbp),%eax
  400c8b:       7f aa                   jg     400c37 <getlogin_r@plt+0x467>
  400c8d:       48 8b 45 f8             mov    -0x8(%rbp),%rax
  400c91:       c9                      leaveq
  400c92:       c3                      retq
  400c93:       66 2e 0f 1f 84 00 00    nopw   %cs:0x0(%rax,%rax,1)
  400c9a:       00 00 00
  400c9d:       0f 1f 00                nopl   (%rax)
  400ca0:       41 57                   push   %r15
  400ca2:       41 89 ff                mov    %edi,%r15d
  400ca5:       41 56                   push   %r14
  400ca7:       49 89 f6                mov    %rsi,%r14
  400caa:       41 55                   push   %r13
  400cac:       49 89 d5                mov    %rdx,%r13
  400caf:       41 54                   push   %r12
  400cb1:       4c 8d 25 48 11 20 00    lea    0x201148(%rip),%r12        # 601e0
0 <_fini+0x2010ec>
  400cb8:       55                      push   %rbp
  400cb9:       48 8d 2d 48 11 20 00    lea    0x201148(%rip),%rbp        # 601e0
8 <_fini+0x2010f4>
  400cc0:       53                      push   %rbx
```

```
  400cc1:       4c 29 e5                sub    %r12,%rbp
  400cc4:       31 db                   xor    %ebx,%ebx
  400cc6:       48 c1 fd 03             sar    $0x3,%rbp
  400cca:       48 83 ec 08             sub    $0x8,%rsp
  400cce:       e8 35 fa ff ff          callq  400708 <_init>
  400cd3:       48 85 ed                test   %rbp,%rbp
  400cd6:       74 1e                   je     400cf6 <getlogin_r@plt+0x526>
  400cd8:       0f 1f 84 00 00 00 00    nopl   0x0(%rax,%rax,1)
  400cdf:       00
  400ce0:       4c 89 ea                mov    %r13,%rdx
  400ce3:       4c 89 f6                mov    %r14,%rsi
  400ce6:       44 89 ff                mov    %r15d,%edi
  400ce9:       41 ff 14 dc             callq  *(%r12,%rbx,8)
  400ced:       48 83 c3 01             add    $0x1,%rbx
  400cf1:       48 39 eb                cmp    %rbp,%rbx
  400cf4:       75 ea                   jne    400ce0 <getlogin_r@plt+0x510>
  400cf6:       48 83 c4 08             add    $0x8,%rsp
  400cfa:       5b                      pop    %rbx
  400cfb:       5d                      pop    %rbp
  400cfc:       41 5c                   pop    %r12
  400cfe:       41 5d                   pop    %r13
  400d00:       41 5e                   pop    %r14
  400d02:       41 5f                   pop    %r15
  400d04:       c3                      retq
  400d05:       66 66 2e 0f 1f 84 00    data32 nopw %cs:0x0(%rax,%rax,1)
  400d0c:       00 00 00 00
  400d10:       f3 c3                   repz retq

Disassembly of section .fini:

0000000000400d14 <_fini>:
  400d14:       48 83 ec 08             sub    $0x8,%rsp
  400d18:       48 83 c4 08             add    $0x8,%rsp
  400d1c:       c3                      retq
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ ldd 4
        linux-vdso.so.1 =>  (0x00007fff137cd000)
        lib361.so => /lib/x86_64-linux-gnu/lib361.so (0x00007f353cbc1000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f353c7fc000)
        /lib64/ld-linux-x86-64.so.2 (0x000055eda9ef7000)
Dpate85@Dhrumil:~/dpate85/hw2/puzzles$ cd
Dpate85@Dhrumil:~$ cd ..
Dpate85@Dhrumil:/home$ cd ..
Dpate85@Dhrumil:/$ cd usr
Dpate85@Dhrumil:/usr$ cd local
Dpate85@Dhrumil:/usr/local$ cd lib
Dpate85@Dhrumil:/usr/local/lib$ ls
lib361.c  lib361.so  python2.7  python3.4
Dpate85@Dhrumil:/usr/local/lib$ sudo rm lib361.c lib361.so
Dpate85@Dhrumil:/usr/local/lib$ ls
python2.7  python3.4
Dpate85@Dhrumil:/usr/local/lib$ cd ..
Dpate85@Dhrumil:/usr/local$ cd ..
Dpate85@Dhrumil:/usr$ cd ..
```