

# 哈尔滨工业大学

# 实验报告

## 实 验（五）

题 目 LinkLab

链接

专 业 计算机类

学 号 1190501614

班 级 19030006

学 生 cgh

指 导 教 师 史先俊

实 验 地 点 G709

实 验 日 期 2021.05.26

计算机科学与技术学院

# 目 录

<b>第 1 章 实验基本信息</b> .....	<b>4 -</b>
1.1 实验目的.....	4 -
1.2 实验环境与工具 .....	4 -
1.2.1 硬件环境.....	4 -
1.2.2 软件环境.....	4 -
1.2.3 开发工具.....	4 -
1.3 实验预习.....	4 -
<b>第 2 章 实验预习</b> .....	<b>5 -</b>
2.1 请按顺序写出 ELF 格式的可执行目标文件的各类信息（5 分） .....	5 -
2.2 请按照内存地址从低到高的顺序，写出 LINUX 下 X64 内存映像。（5 分） -	5 -
内核虚存区 .....	5 -
用户栈.....	5 -
栈->向下 .....	5 -
共享库内存映射区域.....	5 -
堆->向上 .....	5 -
运行时堆 .....	6 -
读写数据段 .....	6 -
只读代码段 .....	6 -
未使用 .....	6 -
2.3 请运行“LINKADDRESS -U 学号 姓名”按地址循序写出各符号的地址、空间。 并按照 LINUX 下 X64 内存映像标出其所属各区。.....	6 -
（5 分） .....	6 -
所属区.....	6 -
各符号的地址、空间.....	6 -
只读代码段 .....	6 -
读写段.....	6 -
运行时堆 .....	6 -
共享库内存映射区域.....	6 -
用户栈.....	6 -
2.4 请按顺序写出 LINKADDRESS 从开始执行到 MAIN 前/后执行的子程序的名字。 (GCC 与 OBJDUMP/GDB/EDB)（5 分） .....	9 -
<b>第 3 章 各阶段的原理与方法</b> .....	<b>10 -</b>
3.1 阶段 1 的分析 .....	10 -
3.2 阶段 2 的分析.....	11 -
3.3 阶段 3 的分析.....	12 -

3.4 阶段 4 的分析.....	- 14 -
3.5 阶段 5 的分析.....	- 14 -
<b>第 4 章 总结.....</b>	<b>- 15 -</b>
4.1 请总结本次实验的收获.....	- 15 -
4.2 请给出对本次实验内容的建议 .....	- 15 -
<b>参考文献.....</b>	<b>- 16 -</b>

## 第 1 章 实验基本信息

### 1.1 实验目的

理解链接的作用与工作步骤

掌握 ELF 结构、符号解析与重定位的工作过程

熟练使用 Linux 工具完成 ELF 分析与修改

### 1.2 实验环境与工具

#### 1.2.1 硬件环境

X64 CPU; 2GHz; 2G RAM; 256GHD Disk 以上

#### 1.2.2 软件环境

Windows7 64 位以上; VirtualBox/Vmware 11 以上; Ubuntu 16.04 LTS 64 位/优麒麟 64 位;

#### 1.2.3 开发工具

Visual Studio 2010 64 位以上; GDB/OBJDUMP; DDD/EDB 等

### 1.3 实验预习

上实验课前, 必须认真预习实验指导书(PPT 或 PDF)了解实验的目的、实验环境与软硬件工具、实验操作步骤, 复习与实验有关的理论知识。请按顺序写出 ELF 格式的可执行目标文件的各类信息。请按照内存地址从低到高的顺序, 写出 Linux 下 X64 内存映像。请运行“LinkAddress -u 学号 姓名”按地址顺序写出各符号的地址、空间。并按照 Linux 下 X64 内存映像标出其所属各区。请按顺序写出 LinkAddress 从开始执行到 main 前/后执行的子程序的名字。(gcc 与 objdump/GDB/EDB)

## 第 2 章 实验预习

### 2.1 请按顺序写出 ELF 格式的可执行目标文件的各类信息 (5 分)

ELF 头

段头部表：页面大小，虚拟内存段

.init: 初始化

.text: 代码段

.rodata: 只读数据，跳转表

.data: 已初始化全局变量

.bss: 未初始化全局变量

.symtab: 符号表

.rel.text: 可重定位代码

.rel.data: 可重定位数据

.debug: 调试信息

节头表：每个节的偏移量

### 2.2 请按照内存地址从低到高的顺序, 写出 Linux 下 X64 内存映像。 (5 分)





2.3 请运行“LinkAddress -u 学号 姓名” 按地址循序写出各符号的地址、空间。并按照 Linux 下 X64 内存映像标出其所属各区。

(5 分)

所属区	各符号的地址、空间
只读代码段	show_pointer 0x565ce235 1448927797 useless 0x565ce21d 1448927773 main 0x565ce26b 1448927851
读写段	big array 0x965d10e0 2522681568 huge array 0x565d10e0 1448939744 global 0x565d1020 1448939552 p2 0x991175b0 2568058288
运行时堆	p1 0xe7d1b010 3889278992 p3 0xe7cfa010 3889143824 p4 0xa7cf9010 2815397904 p5 (nil) 0
共享库内存映射区域	exit 0xf7d54170 4157948272 printf 0xf7d70340 4158063424 malloc 0xf7da2df0 4158270960 free 0xf7da3420 4158272544 strcpy 0xf7db7090 4158353552
用户栈	argc 0xff8d8a50 4287466064 argv 0xff8d8ae4 4287466212 argv[0] ff8da290 argv[1] ff8da295 argv[2] ff8da298 argv[3] ff8da2a3

	<pre> argv[0]    0xff8da290 4287472272 ./ld argv[1]    0xff8da295 4287472277 -u argv[2]    0xff8da298 4287472280 1190501614 argv[3]    0xff8da2a3 4287472291 陈广焕  env 0xff8d8af8 4287466232 env[0]     *env 0xff8da2ad 4287472301 SHELL=/bin/bash env[1]     *env 0xff8da2bd 4287472317 SESSION_MANAGER=local/ubuntu:0/tmp/.ICE-unix/1759,unix/ubuntu:/tmp/.ICE-unix/1759 env[2]     *env 0xff8da30f 4287472399 QT_ACCESSIBILITY=1 env[3]     *env 0xff8da322 4287472418 COLORTERM=truecolor env[4]     *env 0xff8da336 4287472438 XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg env[5]     *env 0xff8da363 4287472483 XDG_MENU_PREFIX=gnome- env[6]     *env 0xff8da37a 4287472506 GNOME_DESKTOP_SESSION_ID=this-is-deprecated env[7]     *env 0xff8da3a6 4287472550 GTK_IM_MODULE=fcitx env[8]     *env 0xff8da3ba 4287472570 LANGUAGE=en_US:en env[9]     *env 0xff8da3cc 4287472588 QT4_IM_MODULE=fcitx env[10]    *env 0xff8da3e0 4287472608 LC_ADDRESS=zh_CN.UTF-8 env[11]    *env 0xff8da3f7 4287472631 GNOME_SHELL_SESSION_MODE=ubuntu env[12]    *env 0xff8da417 4287472663 LC_NAME=zh_CN.UTF-8 env[13]    *env 0xff8da42b 4287472683 SSH_AUTH_SOCK=/run/user/1000/keyring/ssh env[14]    *env 0xff8da454 4287472724 XMODIFIERS=@im=fcitx env[15]    *env 0xff8da469 4287472745 DESKTOP_SESSION=ubuntu env[16]    *env 0xff8da480 4287472768 LC_MONETARY=zh_CN.UTF-8 env[17]    *env 0xff8da498 4287472792 SSH_AGENT_PID=1704 env[18]    *env 0xff8da4ab 4287472811 GTK_MODULES=gail:atk-bridge env[19]    *env 0xff8da4c7 4287472839 DBUS_STARTER_BUS_TYPE=session env[20]    *env 0xff8da4e5 4287472869 PWD=/home/cgh1190501614/Desktop/hitcs env[21]    *env 0xff8da50c 4287472908 LOGNAME=cgh1190501614 env[22]    *env 0xff8da522 4287472930 XDG_SESSION_DESKTOP=ubuntu env[23]    *env 0xff8da53d 4287472957 XDG_SESSION_TYPE=x11 env[24]    *env 0xff8da552 4287472978 GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1 env[25]    *env 0xff8da586 4287473030 XAUTHORITY=/run/user/1000/gdm/Xauthority </pre>
--	---

env[26]	*env 0xff8da5af 4287473071
WINDOWPATH=2	
env[27]	*env 0xff8da5bc 4287473084
HOME=/home/cgh1190501614	
env[28]	*env 0xff8da5d5 4287473109
USERNAME=cgh1190501614	
env[29]	*env 0xff8da5ec 4287473132
IM_CONFIG_PHASE=1	
env[30]	*env 0xff8da5fe 4287473150
LC_PAPER=zh_CN.UTF-8	
env[31]	*env 0xff8da613 4287473171
LANG=en_US.UTF-8	
env[32]	*env 0xff8da624 4287473188
env[33]	*env 0xff8dac06 4287474694
XDG_CURRENT_DESKTOP=ubuntu:GNOME	
env[34]	*env 0xff8dac27 4287474727
VTE_VERSION=6003	
env[35]	*env 0xff8dac38 4287474744
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/5190ed5e_3258_4451_988b_c5375cce976f	
env[36]	*env 0xff8dac8e 4287474830
INVOCATION_ID=c78680a158ad4aa28a5eccb51782abcb	
env[37]	*env 0xff8dacbd 4287474877
MANAGERPID=1525	
env[38]	*env 0xff8daccd 4287474893
CLUTTER_IM_MODULE=fcitx	
env[39]	*env 0xff8dace5 4287474917
LESSCLOSE=/usr/bin/lesspipe %s %s	
env[40]	*env 0xff8dad07 4287474951
XDG_SESSION_CLASS=user	
env[41]	*env 0xff8dad1e 4287474974
TERM=xterm-256color	
env[42]	*env 0xff8dad32 4287474994
LC_IDENTIFICATION=zh_CN.UTF-8	
env[43]	*env 0xff8dad50 4287475024
LESSOPEN=  /usr/bin/lesspipe %s	
env[44]	*env 0xff8dad70 4287475056
USER=cgh1190501614	
env[45]	*env 0xff8dad83 4287475075
GNOME_TERMINAL_SERVICE=:1.258	
env[46]	*env 0xff8dada1 4287475105
DISPLAY=:0	
env[47]	*env 0xff8dadac 4287475116
SHLVL=1	
env[48]	*env 0xff8dadb4 4287475124
LC_TELEPHONE=zh_CN.UTF-8	
env[49]	*env 0xff8dadcd 4287475149
QT_IM_MODULE=fcitx	
env[50]	*env 0xff8dade0 4287475168
LC_MEASUREMENT=zh_CN.UTF-8	
env[51]	*env 0xff8dadfb 4287475195
DBUS_STARTER_ADDRESS=unix:path=/run/user/1000/bus, guid=dd3e6bcf777747da481d4af160ad9ff7	
env[52]	*env 0xff8dae53 4287475283
PAPERSIZE=a4	
env[53]	*env 0xff8dae60 4287475296
XDG_RUNTIME_DIR=/run/user/1000	
env[54]	*env 0xff8dae7f 4287475327
LC_TIME=zh_CN.UTF-8	
env[55]	*env 0xff8dae93 4287475347
JOURNAL_STREAM=8:50492	
env[56]	*env 0xff8daeea 4287475370
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share:/usr/share:/var/lib/snapd/desktop	
env[57]	*env 0xff8daeff 4287475455



	PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin env[58] *env 0xff8daf67 4287475559 GDMSSESSION=ubuntu env[59] *env 0xff8daf79 4287475577 DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus, guid=dd3e6bcf777747da481d4af160ad9ff7 env[60] *env 0xff8dafd5 4287475669 LC_NUMERIC=zh_CN.UTF-8 env[61] *env 0xff8dafec 4287475692
--	---

2.4 请按顺序写出 LinkAddress 从开始执行到 main 前/后执行的子程序的名字。(gcc 与 objdump/GDB/EDB) (5 分)

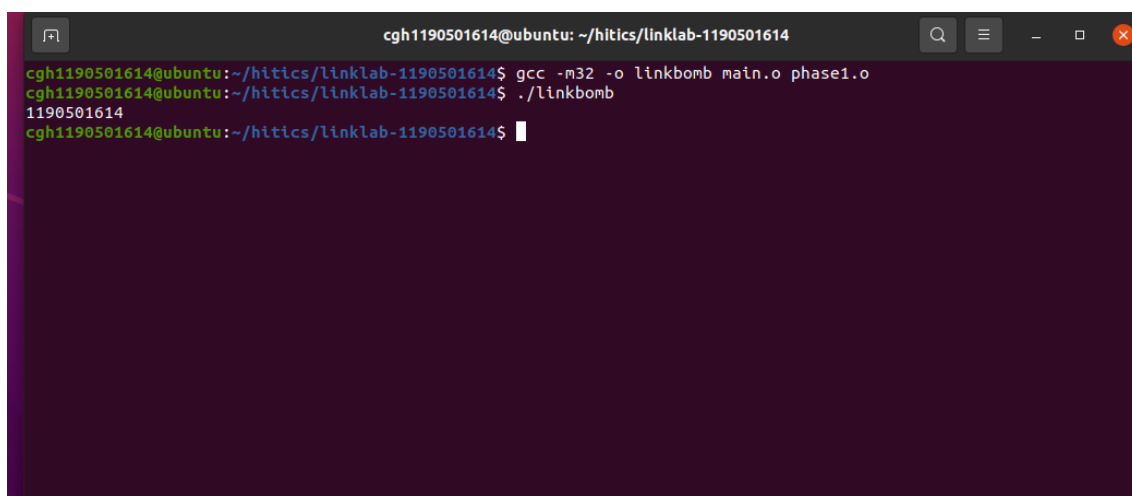
执行时间	子程序名
Main 函数之前	_init free@plt puts@plt __stack_chk_fail@plt printf@plt __libc_start_main@plt malloc@plt exit@plt _start _tm_clones register_tm_clones _do_global_dtors_aux frame_dummy show_pointer useless
Main 函数之后	__libc_csu_init __libc_csu_fini

## 第 3 章 各阶段的原理与方法

每阶段 40 分，phases.o 20 分，分析 20 分，总分不超过 80 分

### 3.1 阶段 1 的分析

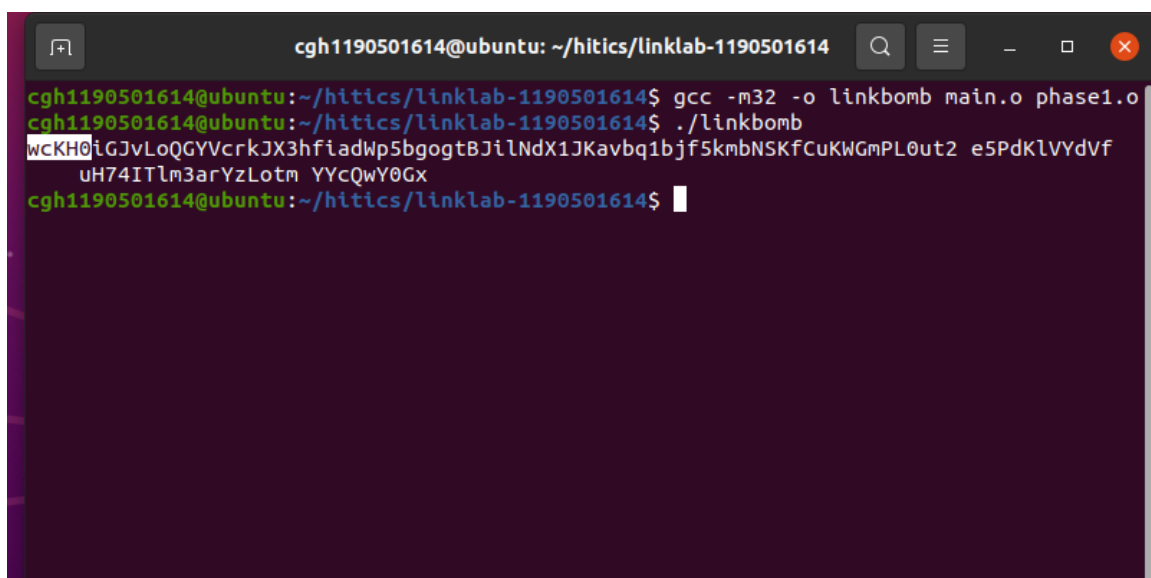
程序运行结果截图：



```
cgh1190501614@ubuntu: ~/hitics/linklab-1190501614
cgh1190501614@ubuntu:~/hitics/linklab-1190501614$ gcc -m32 -o linkbomb main.o phase1.o
cgh1190501614@ubuntu:~/hitics/linklab-1190501614$ ./linkbomb
1190501614
cgh1190501614@ubuntu:~/hitics/linklab-1190501614$
```

分析与设计的过程：

首先将未修改 phase1.o 和 main.o 链接看输出的字符串



```
cgh1190501614@ubuntu: ~/hitics/linklab-1190501614
cgh1190501614@ubuntu:~/hitics/linklab-1190501614$ gcc -m32 -o linkbomb main.o phase1.o
cgh1190501614@ubuntu:~/hitics/linklab-1190501614$ ./linkbomb
wCKH0iGJvLoQGYVcrkJX3hfiadWp5bgogtBJiLNdX1JKavbq1bjf5kmbNSKFCuKWGmPL0ut2 e5PdKlVYdVf
uH74ITlm3arYzLotm YYcQwY0Gx
cgh1190501614@ubuntu:~/hitics/linklab-1190501614$
```



查看偏移量

```

cgh1190501614@ubuntu: ~/Desktop/hitics/linklab-1190501614
Section Headers:
[Nr] Name                Type           Addr      Off      Size    ES Flg Lk Inf AL
[ 0]                      NULL          00000000 000000 000000 00  0  0  0
[ 1] .text                 PROGBITS      00000000 000034 00005e 00  AX  0  0  1
[ 2] .rel.text            REL           00000000 00025c 000018 08  I 12  1  4
[ 3] .data                 PROGBITS      00000000 000094 000004 00  WA  0  0  4
[ 4] .rel.data            REL           00000000 000274 000008 08  I 12  3  4
[ 5] .bss                  NOBITS        00000000 000098 000000 00  WA  0  0  1
[ 6] .rodata               PROGBITS      00000000 000098 00000b 00  A  0  0  1
[ 7] .comment              PROGBITS      00000000 0000a3 00002d 01  MS  0  0  1
[ 8] .note.GNU-stack       PROGBITS      00000000 0000d0 000000 00  0  0  1
[ 9] .note.gnu.property    NOTE          00000000 0000d0 00001c 00  A  0  0  4
[10] .eh_frame             PROGBITS      00000000 0000ec 000058 00  A  0  0  4
[11] .rel.eh_frame         REL           00000000 00027c 000010 08  I 12 10  4
[12] .symtab               SYMTAB        00000000 000144 0000f0 10  13 11  4
[13] .strtab               STRTAB        00000000 000234 000028 00  0  0  1
[14] .shstrtab             STRTAB        00000000 00028c 000076 00  0  0  1
Key to Flags:
W (write), A (alloc), X (execute), M (merge), S (strings), I (info),
L (link order), O (extra OS processing required), G (group), T (TLS),
C (compressed), x (unknown), o (OS specific), E (exclude),
p (processor specific)
cgh1190501614@ubuntu:~/Desktop/hitics/linklab-1190501614$

```

编写插入指令

```

cgh1190501614@ubuntu:~/Desktop$ gcc -m32 -c ph2.c -o ph2.o
cgh1190501614@ubuntu:~/Desktop$ objdump -d ph2.o

ph2.o:      file format elf32-i386

Disassembly of section .text:

00000000 <.text>:
0:  83 ec 20                sub    $0x20,%esp
3:  c7 45 e8 31 31 39 30    movl   $0x30393131,-0x18(%ebp)
a:  c7 45 ec 35 30 31 36    movl   $0x36313035,-0x14(%ebp)
11: c7 45 f0 31 34 00 00    movl   $0x3431,-0x10(%ebp)
18: 8d 45 e8                lea     -0x18(%ebp),%eax
1b: 89 45 e0                mov     %eax,-0x20(%ebp)
1e: e8 a2 ff ff ff         call    0xffffffffc5
23: 83 c4 20                add     $0x20,%esp
cgh1190501614@ubuntu:~/Desktop$

```

修改后链接即可

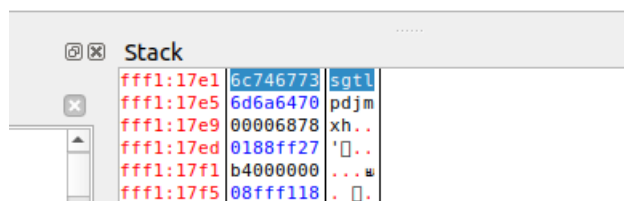
### 3.3 阶段 3 的分析

程序运行结果截图:

```
cgh1190501614@ubuntu: ~/Desktop/hitics/linklab-1190501614
cgh1190501614@ubuntu:~/Desktop/hitics/linklab-1190501614$ ./linkbomb3
1190501614
cgh1190501614@ubuntu:~/Desktop/hitics/linklab-1190501614$
```

分析与设计的过程:

用 edb 调试, 找到数组 cookie 中的字母为 sgtlpdjmxxh



查看需要构造的数组的符号名

```
cgh1190501614@ubuntu: ~/Desktop/hitics/linklab-1190501614
cgh1190501614@ubuntu:~/Desktop/hitics/linklab-1190501614$ readelf -s phase3.o

Symbol table '.syntab' contains 14 entries:
   Num:  Value  Size Type    Bind   Vis      Ndx Name
   ---:  ---:  ---:  ---:    ---:  ---:      ---:
   0: 00000000      0 NOTYPE  LOCAL  DEFAULT  UND
   1: 00000000      0 FILE    LOCAL  DEFAULT  ABS phase3.c
   2: 00000000      0 SECTION LOCAL  DEFAULT    1
   3: 00000000      0 SECTION LOCAL  DEFAULT    3
   4: 00000000      0 SECTION LOCAL  DEFAULT    5
   5: 00000000      0 SECTION LOCAL  DEFAULT    7
   6: 00000000      0 SECTION LOCAL  DEFAULT    8
   7: 00000000      0 SECTION LOCAL  DEFAULT    9
   8: 00000000      0 SECTION LOCAL  DEFAULT    6
   9: 00000020    256 OBJECT  GLOBAL  DEFAULT  COM zWtbeoxlAq
  10: 00000000    135 FUNC    GLOBAL  DEFAULT    1 do_phase
  11: 00000000      0 NOTYPE  GLOBAL  DEFAULT  UND putchar
  12: 00000000      0 NOTYPE  GLOBAL  DEFAULT  UND __stack_chk_fail
  13: 00000000      4 OBJECT  GLOBAL  DEFAULT    3 phase
cgh1190501614@ubuntu:~/Desktop/hitics/linklab-1190501614$
```



## 第 4 章 总结

### 4.1 请总结本次实验的收获

更加熟练掌握 readelf 等工具  
对汇编代码的认识更加深刻

### 4.2 请给出对本次实验内容的建议

无

## 参考文献