Bomb 实验相关内容

柴云鹏
ypchai@ruc.edu.cn

实验内容和要求

- 拆弹！
  - 可执行文件 bomb 包括 6 道密码，必须全都解开；输错密码会导致炸弹爆炸；
  - 此外还包含一个隐藏关！
  - 注意：在线系统随机生成密码，每个人的都不相同；
  - 方法：反汇编、 GDB 调试（ Linux 环境）；
  - 实验报告：详细求解密码的过程

内容讲解

- **Linux 服务器登录和基本操作**
- gcc, make file 使用方法
- gdb 使用方法

Linux 服务器登录和基本操作

- 登录工具（windows)： putty.exe
  - 协议： ssh 协议（端口 22 ）
- 本机与服务器文件互传： psftp.exe
  - open <domain>
  - lcd XXX (改变本机目录）
  - get xxx (从服务器下载文件)
  - put xxx (从本机上传文件)

Linux 服务器登录和基本操作

- Linux 常用命令
  - ls; ll; pwd;cd; mkdir; chmod
  - cp; mv; rm –fr ./XXX
  - vi; vim
  - df; top; free
  - tar (z)xvf …; tar zcvf …; gzip …; unzip …
  - find; grep
  - ifconfig; ping

内容讲解

- Linux 服务器登录和基本操作
- **gcc, make file 使用方法**
- gdb 使用方法

gcc, make file 使用方法

- gcc (–O1) –o p p1.c p2.c
  - C 预处理器，扩展源代码（ #include, #define ）
  - 编译器，生成汇编代码 p1.s ， p2.s
  - 汇编器，生成目标代码 p1.o ， p2.o
  - 链接器，生成可执行代码文件 p
  - 优化级别 1~3 ，越高优化度越高

gcc, make file 使用方法

- gcc (–O1) -S code.c
  - -S: 产生汇编文件 code.s ，不做进一步的工作
- gcc (–O1) –c code.c
  - -c ：编译并汇编，产生目标代码文件 code.o
- gcc –Wall hw.c
  - 给出 warning
- gcc –g hw.c
  - 支持 debug

gcc, make file 使用方法

- 反汇编器（ disassembler ）
  - 根据目标代码（二进制）内容，生成汇编代码
  - objdump –d code.o

```
0000000000400595 <sumstore>:
  400595:  53                   push   %rbx
  400596:  48 89 d3             mov    %rdx,%rbx
  400599:  e8 f2 ff ff ff       callq  400590 <plus>
  40059e:  48 89 03             mov    %rax,(%rbx)
  4005a1:  5b                   pop    %rbx
  4005a2:  c3                   retq
```

  - objdump –s –d bomb （打印所有段，包括常量等）

Makefile

- 集成编译链接的工具（类似批处理）
- Make 即可进行所有工作
- 文件 Makefile 或 makefile 内容：

```
hw: hw.o helper.o
gcc –o hw hw.o helper.o –lm （链接库 m ）
hw.o: hw.c
gcc –O –Wall –c hw.c
helper.o: helper.c
gcc –O –Wall –c helper.c
clean:
rm –f hw.o helper.o hw
```

更标准的 Makefile 写法

```
# specify all source files here
SRCS = hw.c helper.c
# specify target here (name of executable)
TARG = hw
# specify compiler, compiler flags, and needed libs
CC = gcc
OPTS = -Wall –O
LIBS = -lm

#this translates .c files in src list to .o's
OBJS = $(SRCS:.c=.o)

# all is not really needed, but is used to generate the target
All: $(TARG)
# this generates the target executable
$(TARG): $(OBJS)
        $(CC) –o $(TARG) $(OBJS) $(LIBS)
# this is a generic rule for .o files
%.o: %.c
        $(CC) $(OPTS) –c $< -o $@
# and finally, a clean line
clean:
        rm –f $(OBJS) $(TARG)
```

内容讲解

- Linux 服务器登录和基本操作
- gcc, make file 使用方法
- **gdb 使用方法**

gdb 使用方法

- GDB 是什么?
  - GDB 是一个由 GNU 开源组织发布的、 UNIX/ LINUX 操作系统下的、基于命令行的、功能强大的程序调试工具。 对于一名 Linux 下工作的 c/c++ 程序员， gdb 是必不可少的工具。

gdb 使用方法

- 一般来说， GDB 主要帮忙你完成下面四个方面的功能：
  - 1 、启动你的程序，可以按照你的自定义的要求随心所欲的运行程序。
  - 2 、可让被调试的程序在你所指定的调置的断点处停住。（断点可以是条件表达式）
  - 3 、当程序被停住时，可以检查此时你的程序中所发生的事。
  - 4 、动态的改变你程序的执行环境。

gdb 使用方法

显示当前源码： list [linenum]	l
搜索字符串： search str	
设置断点： break linenum|func 设置在某个程序某个函数的断点： break program:func	b
查看断点： info break	Info b
删除断点： delete break	d 断点号
运行调试 | 重启调试： run	r
输出变量 / 表达式信息： print [变量 / 表达式]	p
单步调试： next	n
跟入函数调试： step	s
执行到下一断点： continue	c
退出调试： quit	q

gdb 使用方法

- Buggy.c

```
#include <stdio.h>

Struct Data {
        int x;
};

Int main (int argc, char *argv[]) {
        struct Data *p = NULL;
        printf("%d\n", p->x);
}
```

- >gdb buggy
- (gdb)run

-> segmentation fault

- (gdb) print p

1= (Data *) 0x0

- (gdb) break main

gdb 使用方法

- set args 可指定运行时参数
  - set args 10 20 30 40 50
- show args 命令可以查看设置好的运行参数。

gdb 调试汇编程序

- 显示寄存器的值
  - (gdb) print $rbp
- 要执行到下一行
  - (gdb) nexti
- 进入函数调用（汇编指令是 call）
  - (gdb) stepi
- 直接运行到这个函数结束
  - (gdb) finish
- 任意汇编指令上添加断点
  - (gdb) break *0x400486

Gdb 查看内存

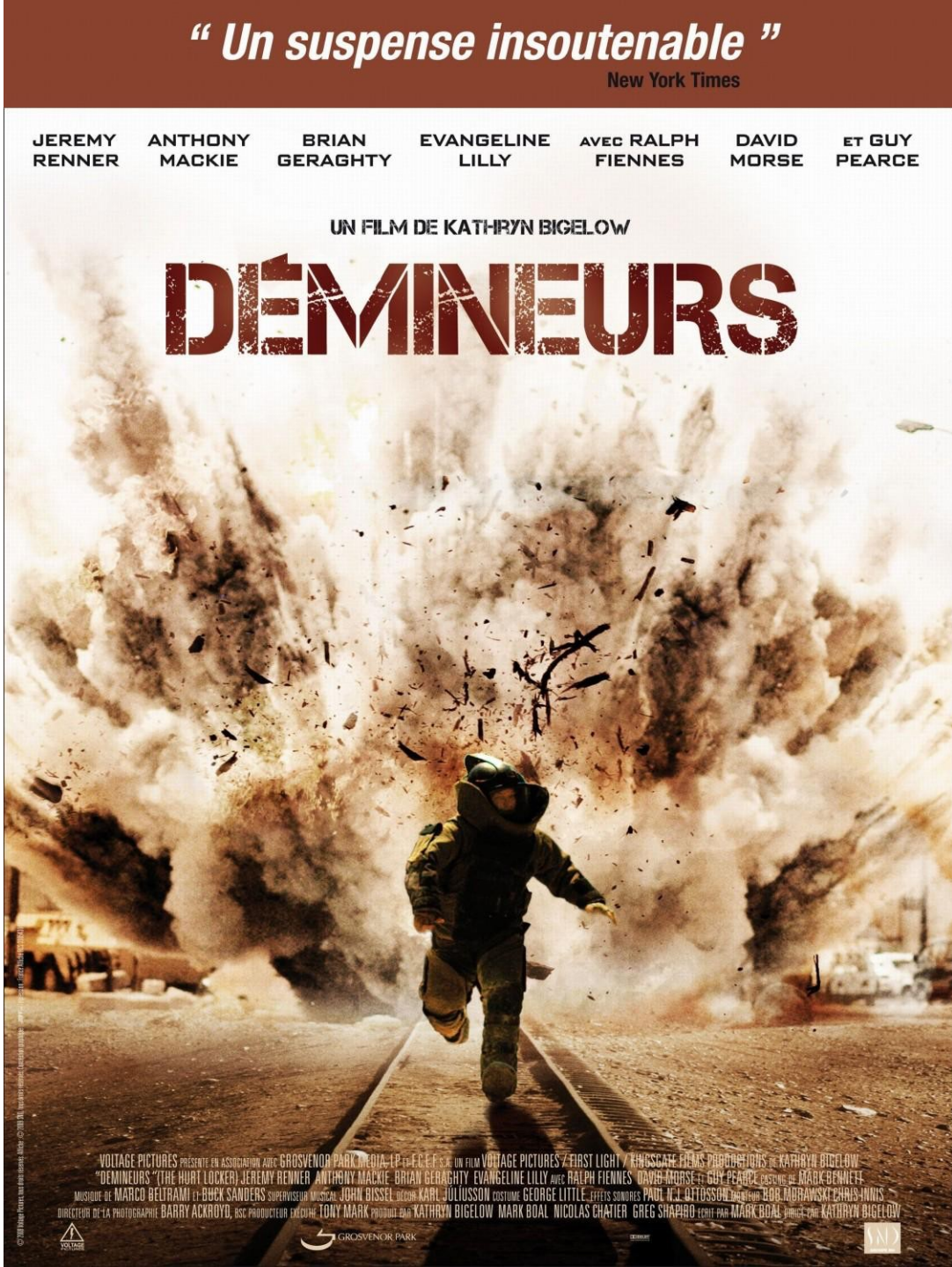
- x /nfu
  - x 是 examine 的缩写
  - **n 表示要显示的内存单元的个数**
  - **f 表示显示方式，可取如下值**
    - x 按十六进制格式显示变量。
    - d 按十进制格式显示变量。
    - u 按十进制格式显示无符号整型。
    - o 按八进制格式显示变量。
    - t 按二进制格式显示变量。
    - a 按十六进制格式显示变量。
    - i 指令地址格式
    - c 按字符格式显示变量。
    - f 按浮点数格式显示变量。
  - **u 表示一个地址单元的长度**
    - b 表示单字节，
    - h 表示双字节，
    - w 表示四字节，
    - g 表示八字节

- 举例
  - x/3uh buf
  - 表示从内存地址 buf 读取内容，
  - h 表示以双字节为一个单位，
  - 3 表示三个单位，
  - u 表示按十六进制显示

GDB 调试正在运行进程

- ps 获得进程号（ pid ）
- gdb attach pid

ENJOY IT!


“ Un suspense insoutenable ”
New York Times
JEREMY RENNER
ANTHONY MACKIE
BRIAN GERAGHTY
EVANGELINE LILLY
AVEC RALPH FIENNES
DAVID MORSE
ET GUY PEARCE
UN FILM DE KATHRYN BIGELOW
DÉMINEURS