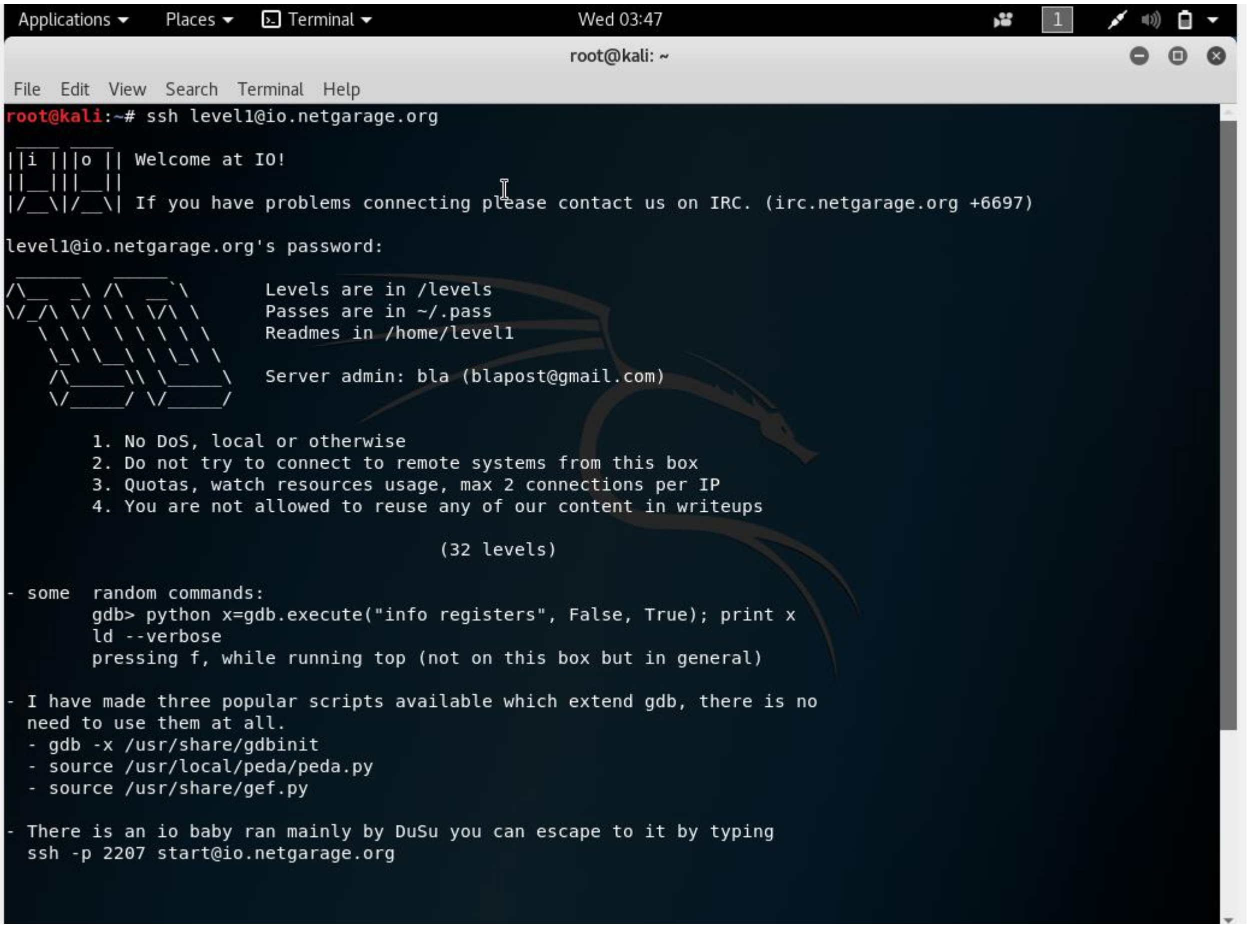
IT16149090

Abeysingha M.H

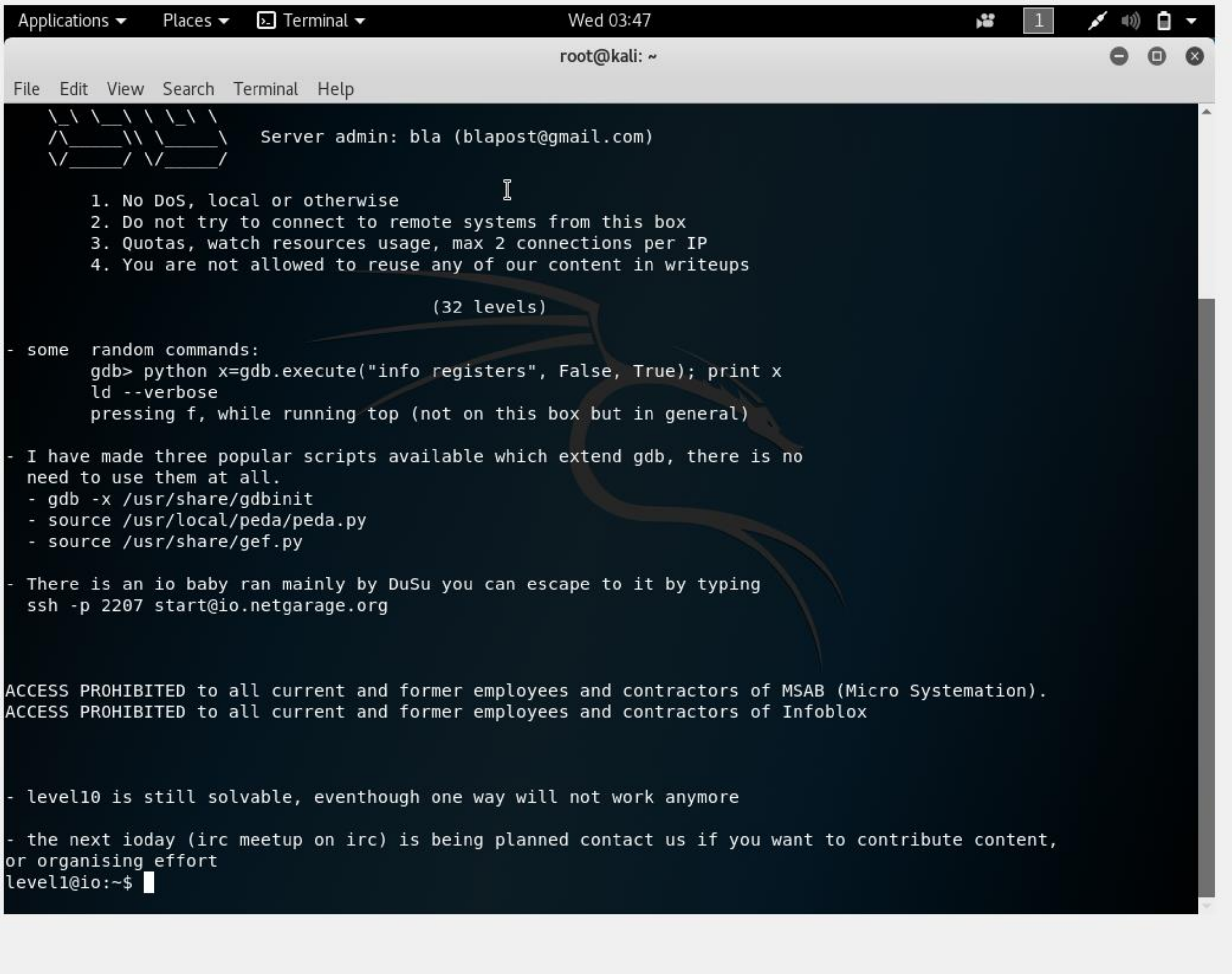
IO wargame

You have to use an ssh client to connect to the game.

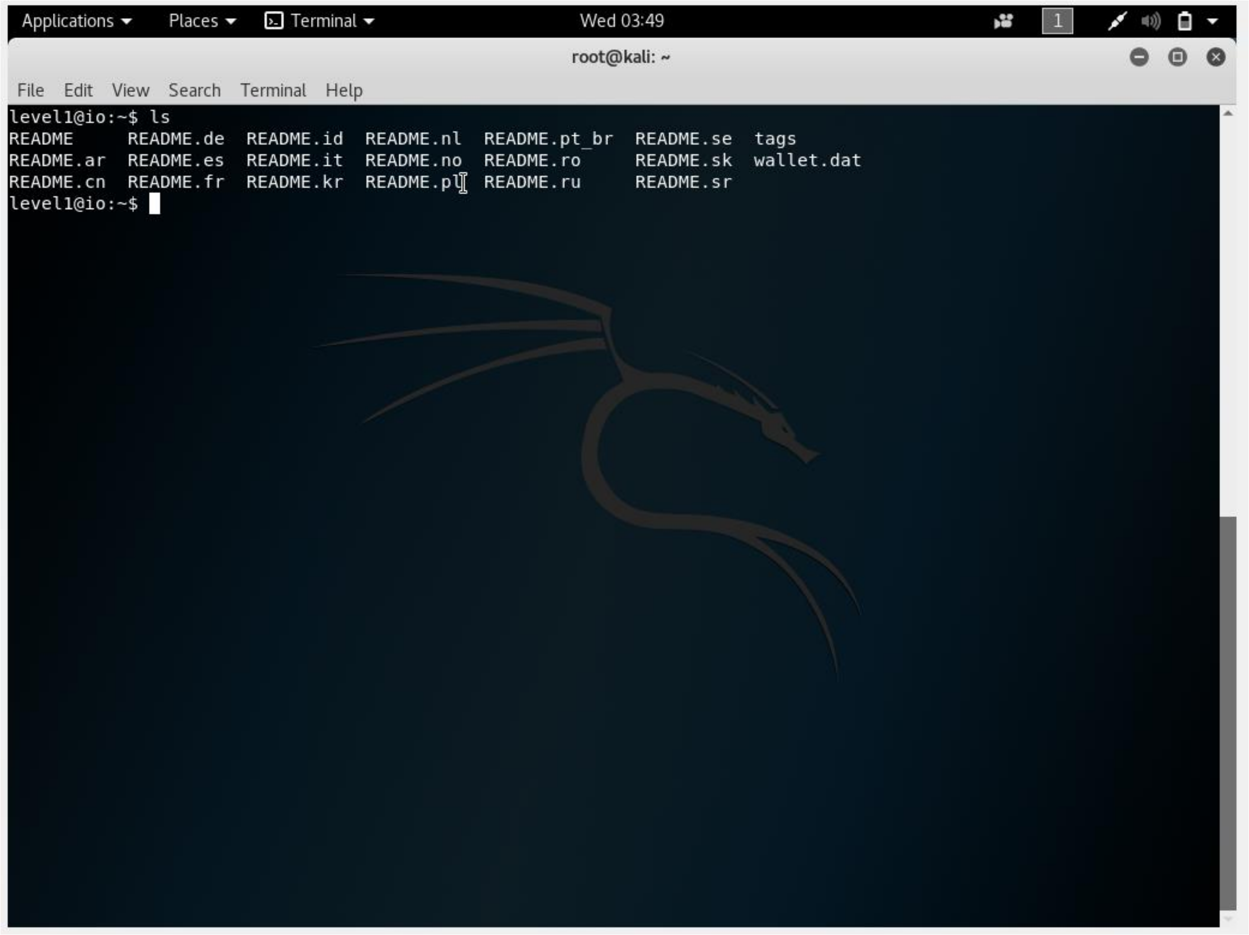
```
ssh level1@io.netgarage.org
password: level1
```



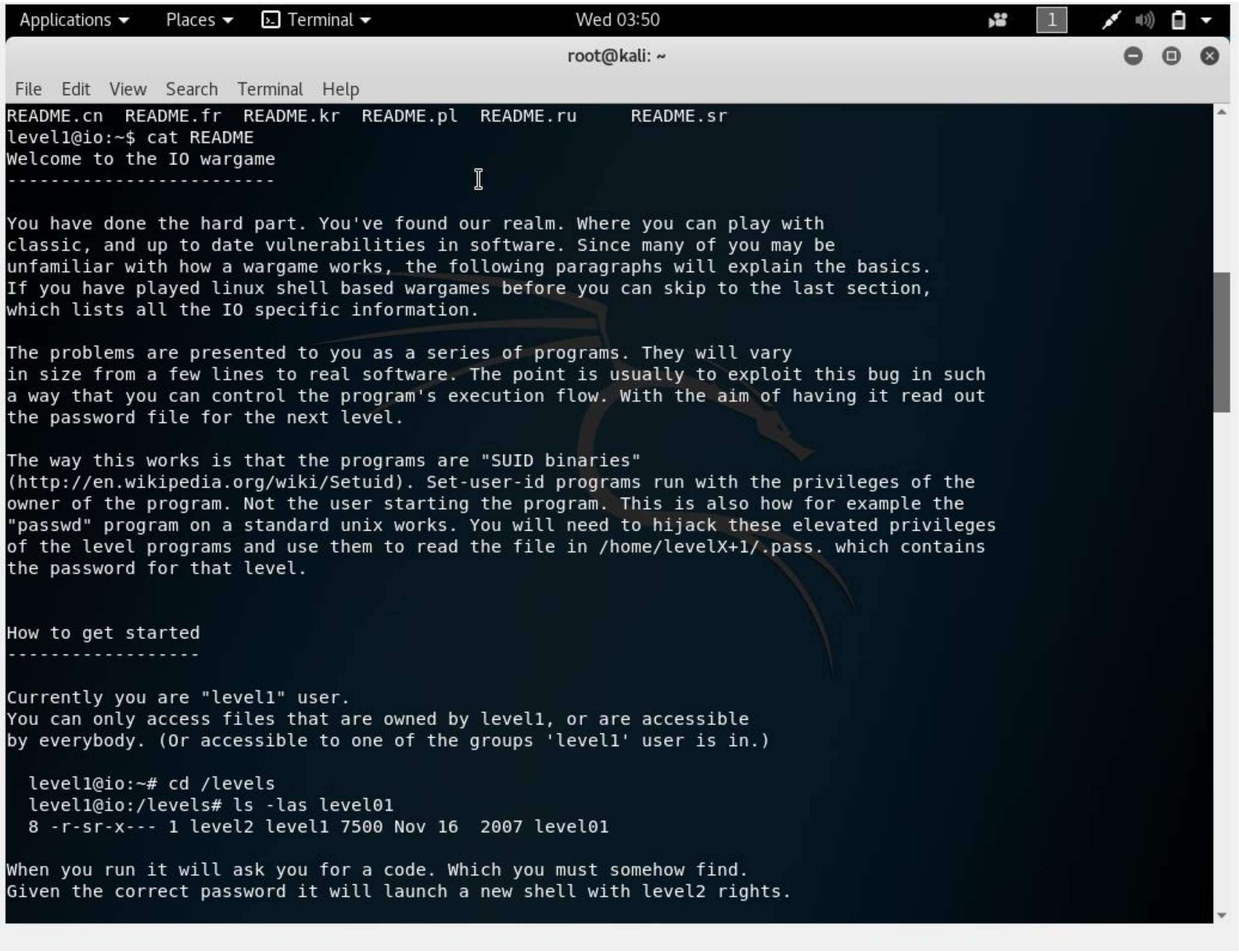
```
root@kali:~# ssh level1@io.netgarage.org
 ____ ____
||i |||o || Welcome at IO!
||__|||__||
|/__\|/__\| If you have problems connecting please contact us on IRC. (irc.netgarage.org +6697)

level1@io.netgarage.org's password:
 ______   _____
/\__  _\ /\  __`\       Levels are in /levels
\/_/\ \/ \ \ \/\ \      Passes are in ~/.pass
   \ \ \  \ \ \ \ \     Readmes in /home/level1
    \_\ \__\ \ \_\ \
    /\_____\\ \_____\   Server admin: bla (blapost@gmail.com)
    \/_____/ \/_____/

        1. No DoS, local or otherwise
        2. Do not try to connect to remote systems from this box
        3. Quotas, watch resources usage, max 2 connections per IP
        4. You are not allowed to reuse any of our content in writeups

                                        (32 levels)

- some  random commands:
        gdb> python x=gdb.execute("info registers", False, True); print x
        ld --verbose
        pressing f, while running top (not on this box but in general)

- I have made three popular scripts available which extend gdb, there is no
  need to use them at all.
  - gdb -x /usr/share/gdbinit
  - source /usr/local/peda/peda.py
  - source /usr/share/gef.py

- There is an io baby ran mainly by DuSu you can escape to it by typing
  ssh -p 2207 start@io.netgarage.org
```



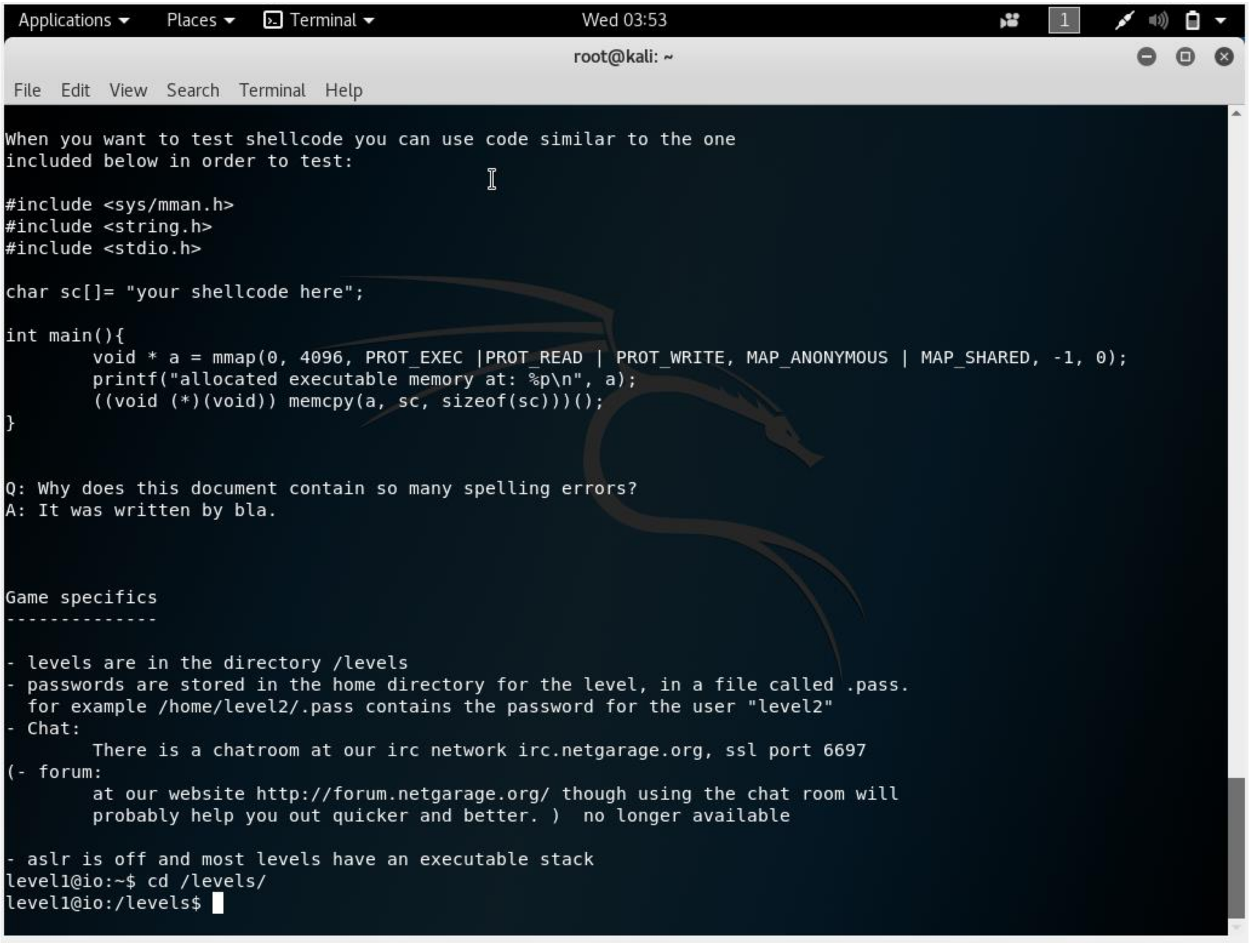
```
    \_\ \__\ \ \_\ \
    /\_____\\ \_____\   Server admin: bla (blapost@gmail.com)
    \/_____/ \/_____/

        1. No DoS, local or otherwise
        2. Do not try to connect to remote systems from this box
        3. Quotas, watch resources usage, max 2 connections per IP
        4. You are not allowed to reuse any of our content in writeups

                                        (32 levels)

- some  random commands:
        gdb> python x=gdb.execute("info registers", False, True); print x
        ld --verbose
        pressing f, while running top (not on this box but in general)

- I have made three popular scripts available which extend gdb, there is no
  need to use them at all.
  - gdb -x /usr/share/gdbinit
  - source /usr/local/peda/peda.py
  - source /usr/share/gef.py

- There is an io baby ran mainly by DuSu you can escape to it by typing
  ssh -p 2207 start@io.netgarage.org



ACCESS PROHIBITED to all current and former employees and contractors of MSAB (Micro Systemation).
ACCESS PROHIBITED to all current and former employees and contractors of Infoblox



- level10 is still solvable, eventhough one way will not work anymore

- the next ioday (irc meetup on irc) is being planned contact us if you want to contribute content,
or organising effort
level1@io:~$ 
```



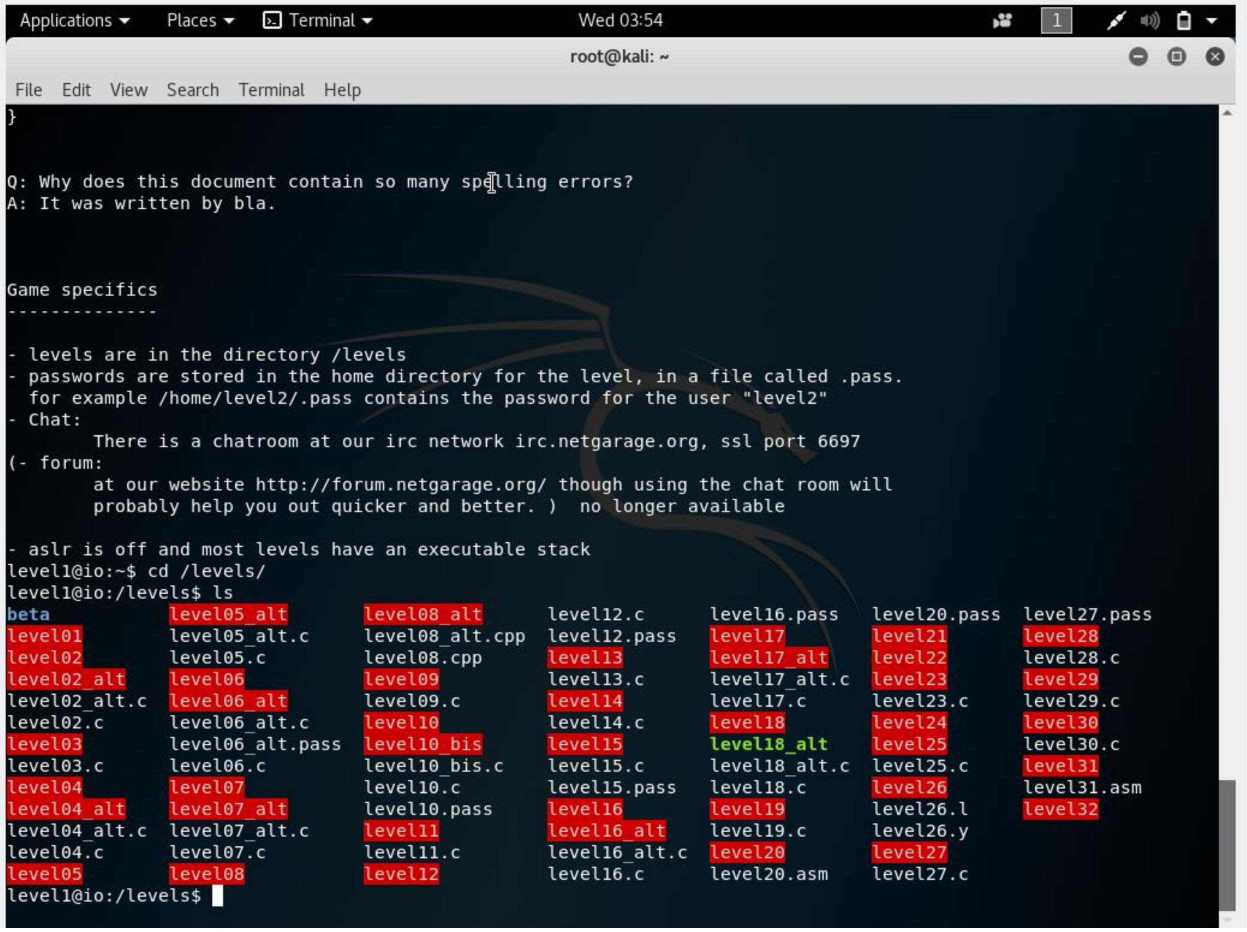
```
level1@io:~$ ls
README     README.de  README.id  README.nl  README.pt_br  README.se  tags
README.ar  README.es  README.it  README.no  README.ro     README.sk  wallet.dat
README.cn  README.fr  README.kr  README.pl  README.ru     README.sr
level1@io:~$ 
```



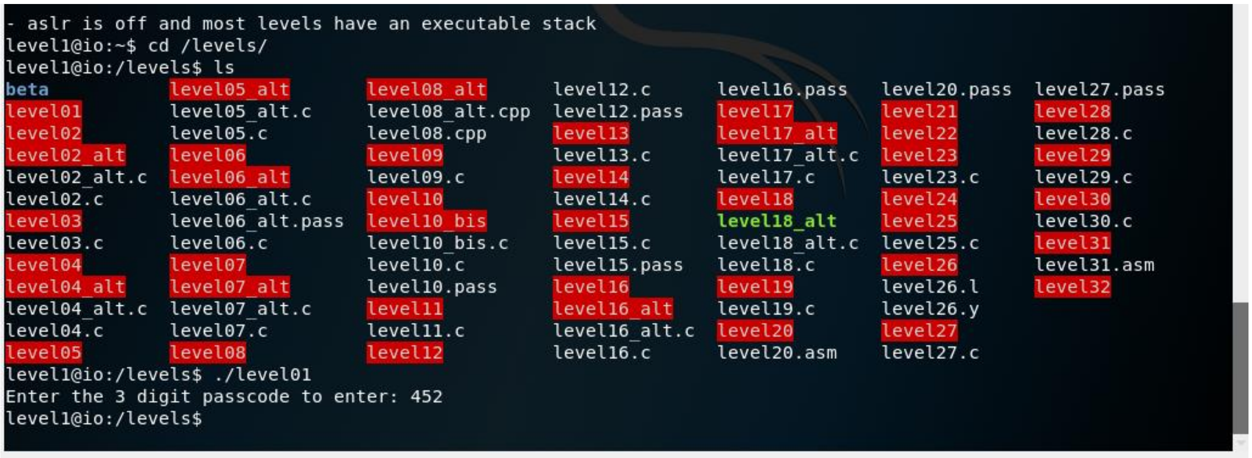
```
README.cn  README.fr  README.kr  README.pl  README.ru     README.sr
level1@io:~$ cat README
Welcome to the IO wargame
-------------------------

You have done the hard part. You've found our realm. Where you can play with
classic, and up to date vulnerabilities in software. Since many of you may be
unfamiliar with how a wargame works, the following paragraphs will explain the basics.
If you have played linux shell based wargames before you can skip to the last section,
which lists all the IO specific information.

The problems are presented to you as a series of programs. They will vary
in size from a few lines to real software. The point is usually to exploit this bug in such
a way that you can control the program's execution flow. With the aim of having it read out
the password file for the next level.

The way this works is that the programs are "SUID binaries"
(http://en.wikipedia.org/wiki/Setuid). Set-user-id programs run with the privileges of the
owner of the program. Not the user starting the program. This is also how for example the
"passwd" program on a standard unix works. You will need to hijack these elevated privileges
of the level programs and use them to read the file in /home/levelX+1/.pass. which contains
the password for that level.


How to get started
------------------

Currently you are "level1" user.
You can only access files that are owned by level1, or are accessible
by everybody. (Or accessible to one of the groups 'level1' user is in.)

  level1@io:~# cd /levels
  level1@io:/levels# ls -las level01
  8 -r-sr-x--- 1 level2 level1 7500 Nov 16  2007 level01

When you run it will ask you for a code. Which you must somehow find.
Given the correct password it will launch a new shell with level2 rights.
```



```
When you want to test shellcode you can use code similar to the one
included below in order to test:

#include <sys/mman.h>
#include <string.h>
#include <stdio.h>

char sc[]= "your shellcode here";

int main(){
        void * a = mmap(0, 4096, PROT_EXEC |PROT_READ | PROT_WRITE, MAP_ANONYMOUS | MAP_SHARED, -1, 0);
        printf("allocated executable memory at: %p\n", a);
        ((void (*)(void)) memcpy(a, sc, sizeof(sc)))();
}


Q: Why does this document contain so many spelling errors?
A: It was written by bla.



Game specifics
--------------

- levels are in the directory /levels
- passwords are stored in the home directory for the level, in a file called .pass.
  for example /home/level2/.pass contains the password for the user "level2"
- Chat:
        There is a chatroom at our irc network irc.netgarage.org, ssl port 6697
(- forum:
        at our website http://forum.netgarage.org/ though using the chat room will
        probably help you out quicker and better. )  no longer available

- aslr is off and most levels have an executable stack
level1@io:~$ cd /levels/
level1@io:/levels$ 
```

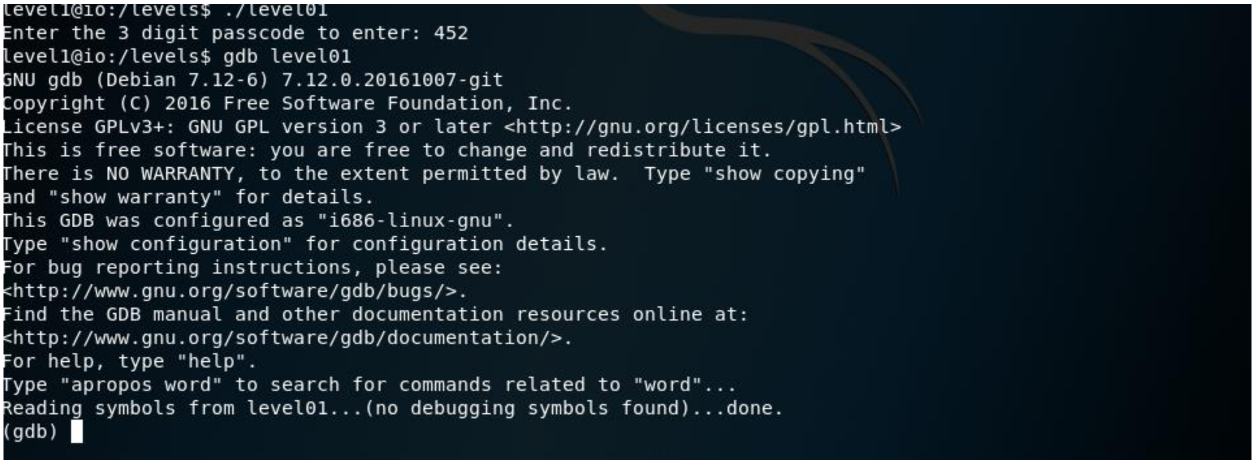


```
}


Q: Why does this document contain so many spelling errors?
A: It was written by bla.



Game specifics
--------------

- levels are in the directory /levels
- passwords are stored in the home directory for the level, in a file called .pass.
  for example /home/level2/.pass contains the password for the user "level2"
- Chat:
        There is a chatroom at our irc network irc.netgarage.org, ssl port 6697
(- forum:
        at our website http://forum.netgarage.org/ though using the chat room will
        probably help you out quicker and better. )  no longer available

- aslr is off and most levels have an executable stack
level1@io:~$ cd /levels/
level1@io:/levels$ ls
beta           level05_alt       level08_alt      level12.c      level16.pass   level20.pass  level27.pass
level01        level05_alt.c     level08_alt.cpp  level12.pass   level17        level21       level28
level02        level05.c         level08.cpp      level13        level17_alt    level22       level28.c
level02_alt    level06           level09          level13.c      level17_alt.c  level23       level29
level02_alt.c  level06_alt       level09.c        level14        level17.c      level23.c     level29.c
level02.c      level06_alt.c     level10          level14.c      level18        level24       level30
level03        level06_alt.pass  level10_bis      level15        level18_alt    level25       level30.c
level03.c      level06.c         level10_bis.c    level15.c      level18_alt.c  level25.c     level31
level04        level07           level10.c        level15.pass   level18.c      level26       level31.asm
level04_alt    level07_alt       level10.pass     level16        level19        level26.l     level32
level04_alt.c  level07_alt.c     level11          level16_alt    level19.c      level26.y
level04.c      level07.c         level11.c        level16_alt.c  level20        level27
level05        level08           level12          level16.c      level20.asm    level27.c
level1@io:/levels$ 
```

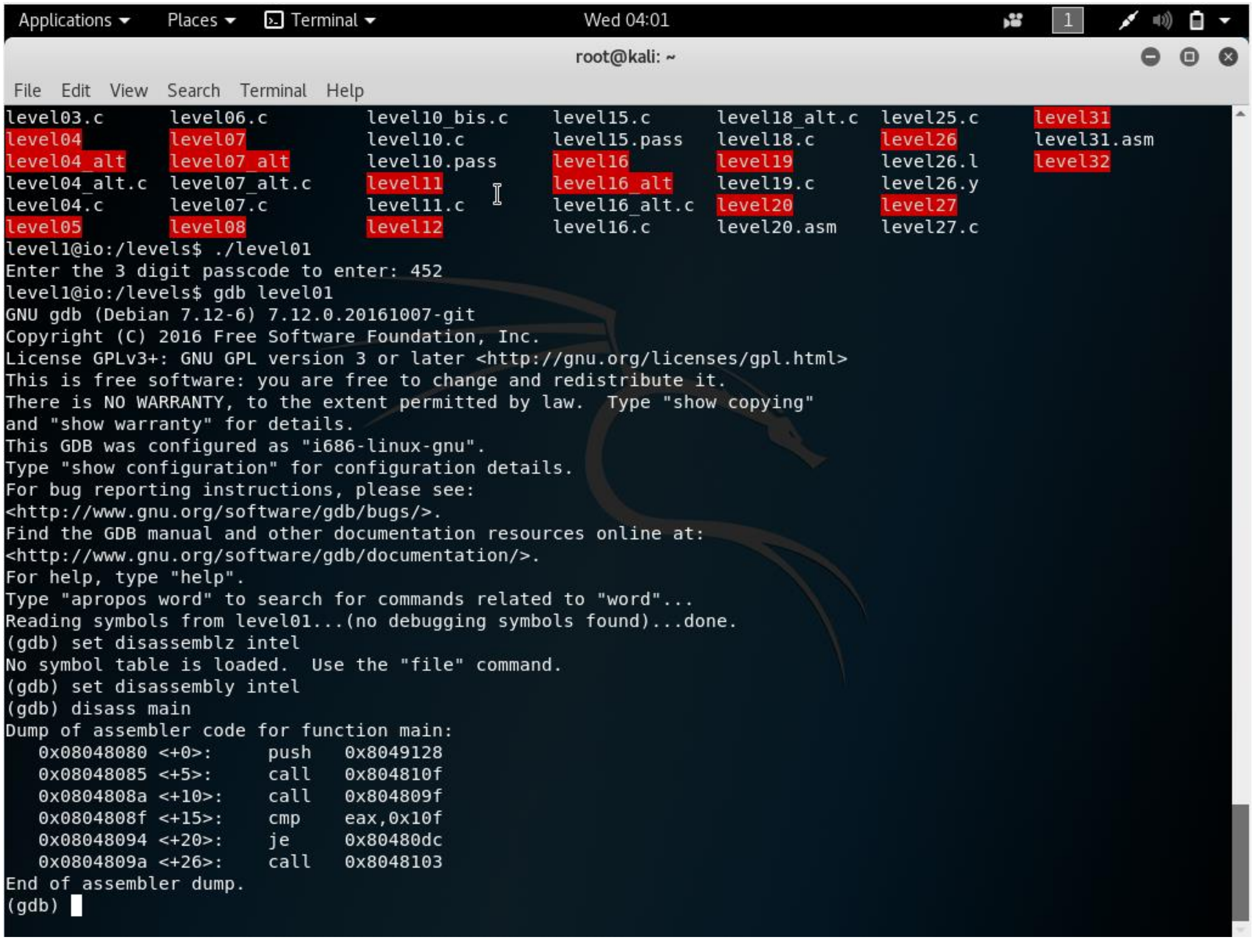


```
- aslr is off and most levels have an executable stack
level1@io:~$ cd /levels/
level1@io:/levels$ ls
beta           level05_alt       level08_alt      level12.c      level16.pass   level20.pass  level27.pass
level01        level05_alt.c     level08_alt.cpp  level12.pass   level17        level21       level28
level02        level05.c         level08.cpp      level13        level17_alt    level22       level28.c
level02_alt    level06           level09          level13.c      level17_alt.c  level23       level29
level02_alt.c  level06_alt       level09.c        level14        level17.c      level23.c     level29.c
level02.c      level06_alt.c     level10          level14.c      level18        level24       level30
level03        level06_alt.pass  level10_bis      level15        level18_alt    level25       level30.c
level03.c      level06.c         level10_bis.c    level15.c      level18_alt.c  level25.c     level31
level04        level07           level10.c        level15.pass   level18.c      level26       level31.asm
level04_alt    level07_alt       level10.pass     level16        level19        level26.l     level32
level04_alt.c  level07_alt.c     level11          level16_alt    level19.c      level26.y
level04.c      level07.c         level11.c        level16_alt.c  level20        level27
level05        level08           level12          level16.c      level20.asm    level27.c
```

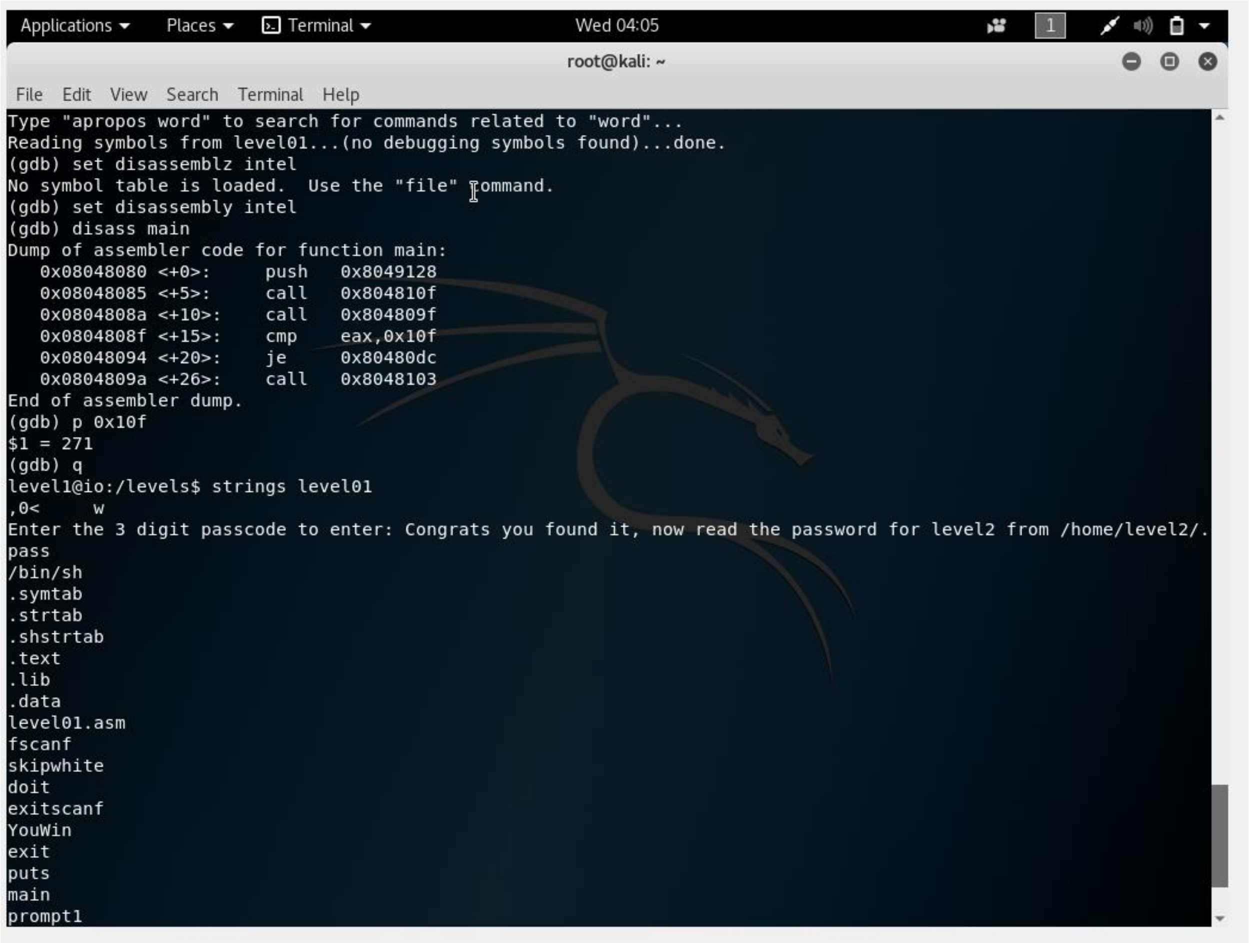
```
level1@io:/levels$ ./level01
Enter the 3 digit passcode to enter: 452
level1@io:/levels$
```



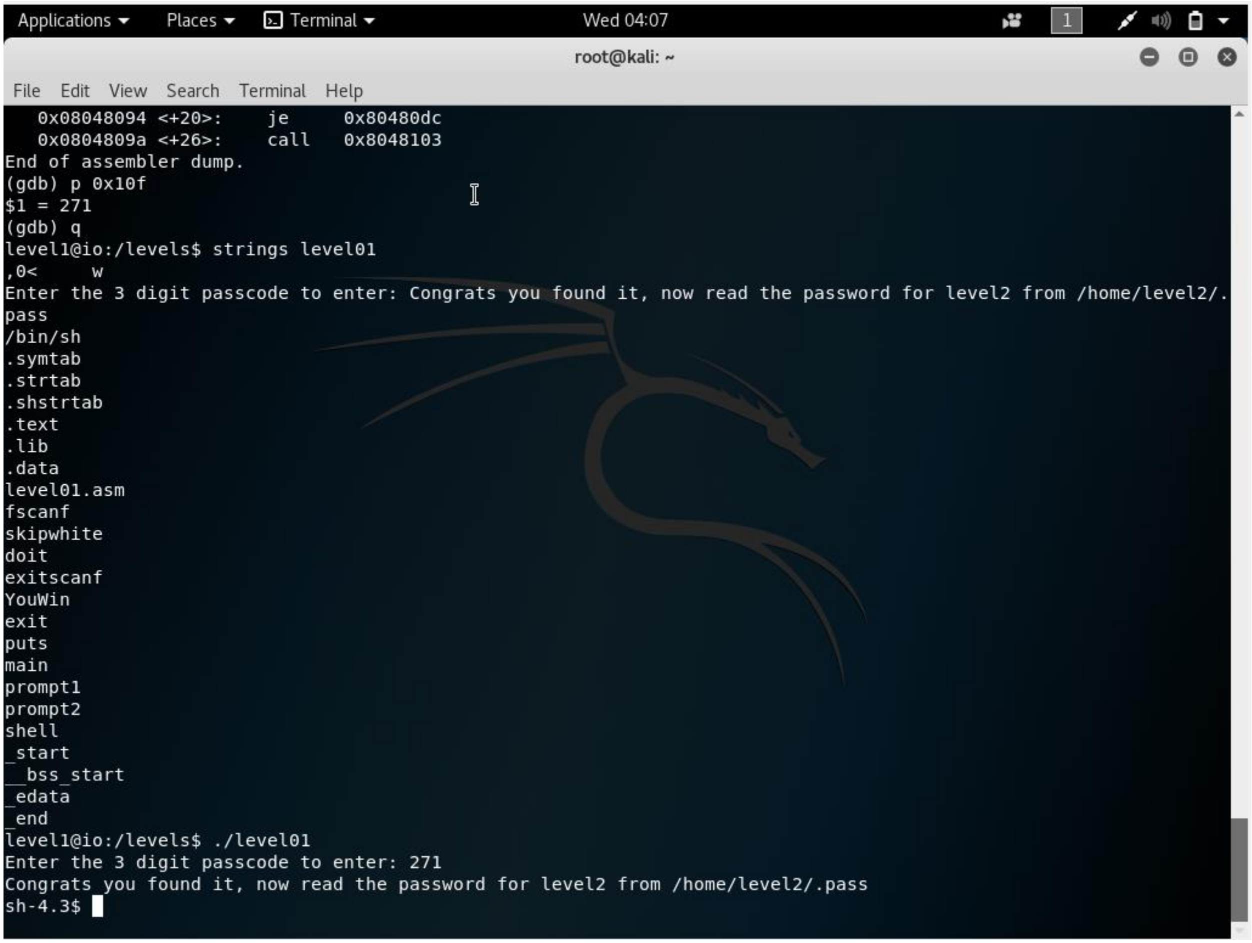
```
level1@io:/levels$ ./level01
Enter the 3 digit passcode to enter: 452
level1@io:/levels$ gdb level01
GNU gdb (Debian 7.12-6) 7.12.0.20161007-git
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you 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 "i686-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 level01...(no debugging symbols found)...done.
(gdb) 
```



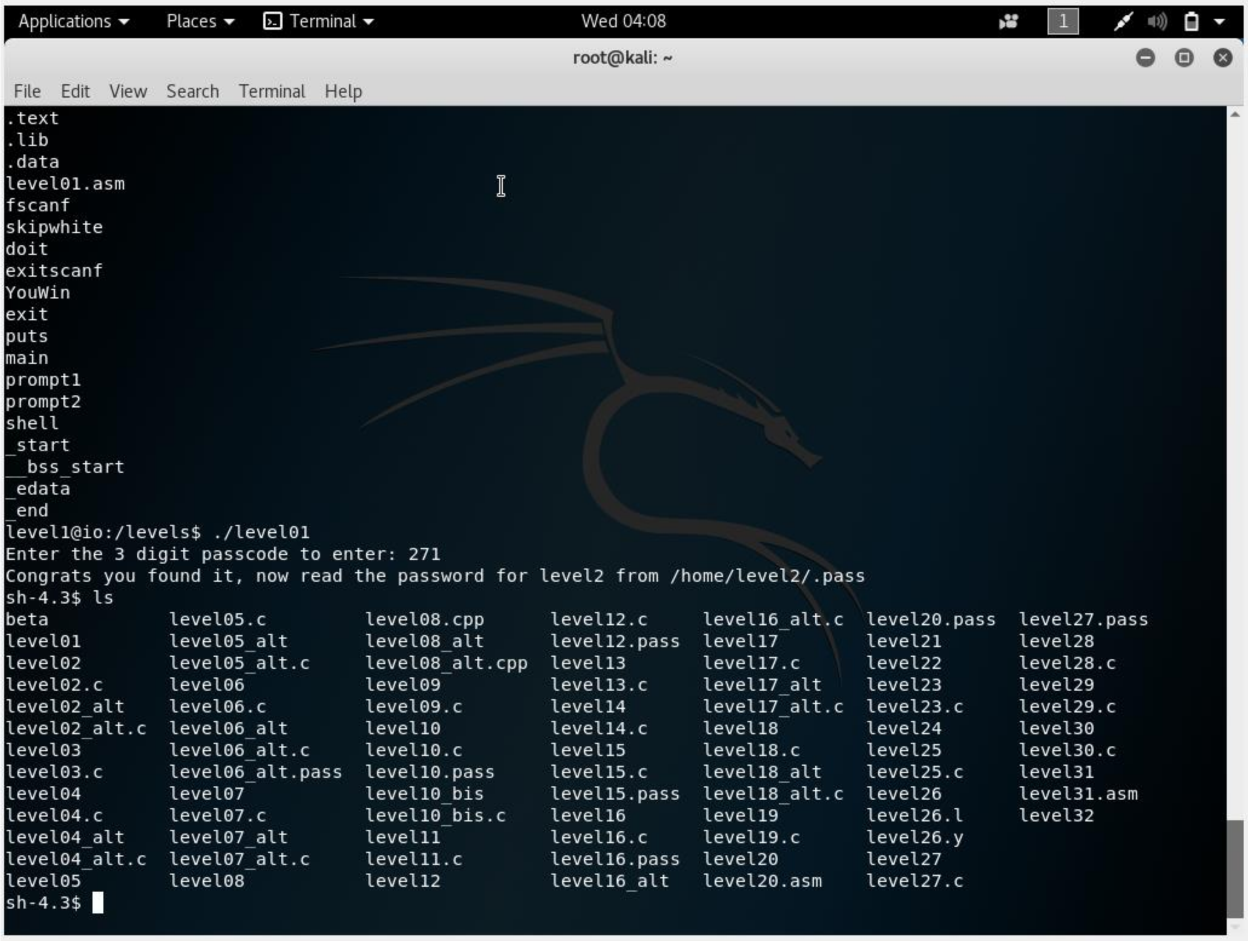
```
level03.c      level06.c      level10_bis.c   level15.c       level18_alt.c  level25.c   level31
level04        level07        level10.c       level15.pass    level18.c      level26     level31.asm
level04_alt    level07_alt    level10.pass    level16         level19        level26.l   level32
level04_alt.c  level07_alt.c  level11         level16_alt     level19.c      level26.y
level04.c      level07.c      level11.c       level16_alt.c   level20        level27
level05        level08        level12         level16.c       level20.asm    level27.c
level1@io:/levels$ ./level01
Enter the 3 digit passcode to enter: 452
level1@io:/levels$ gdb level01
GNU gdb (Debian 7.12-6) 7.12.0.20161007-git
Copyright (C) 2016 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 "i686-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 level01...(no debugging symbols found)...done.
(gdb) set disassemblz intel
No symbol table is loaded.  Use the "file" command.
(gdb) set disassembly intel
(gdb) disass main
Dump of assembler code for function main:
   0x08048080 <+0>:     push   0x8049128
   0x08048085 <+5>:     call   0x804810f
   0x0804808a <+10>:    call   0x804809f
   0x0804808f <+15>:    cmp    eax,0x10f
   0x08048094 <+20>:    je     0x80480dc
   0x0804809a <+26>:    call   0x8048103
End of assembler dump.
(gdb) 
```



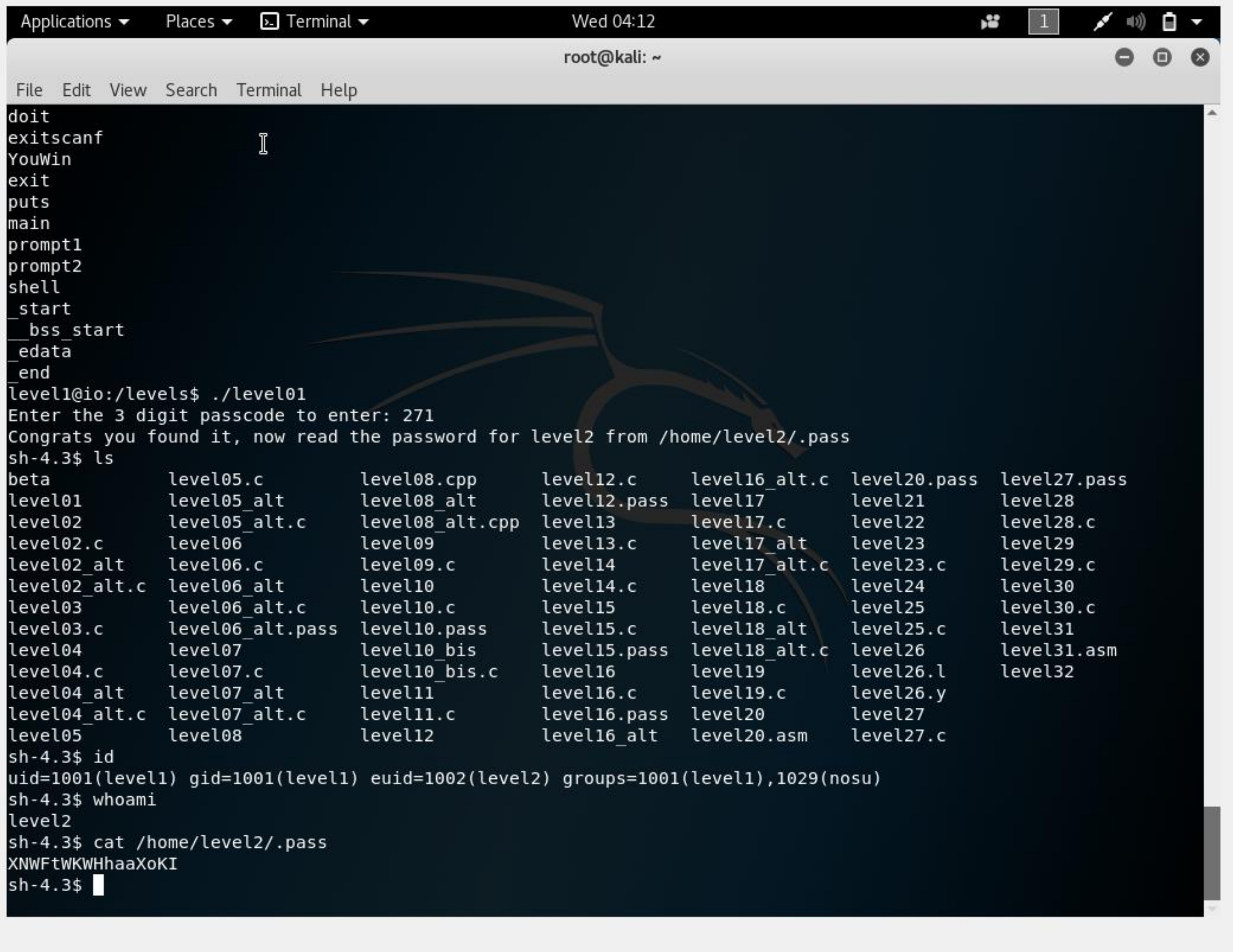
```
Type "apropos word" to search for commands related to "word"...
Reading symbols from level01...(no debugging symbols found)...done.
(gdb) set disassemblz intel
No symbol table is loaded.  Use the "file" command.
(gdb) set disassembly intel
(gdb) disass main
Dump of assembler code for function main:
   0x08048080 <+0>:     push   0x8049128
   0x08048085 <+5>:     call   0x804810f
   0x0804808a <+10>:    call   0x804809f
   0x0804808f <+15>:    cmp    eax,0x10f
   0x08048094 <+20>:    je     0x80480dc
   0x0804809a <+26>:    call   0x8048103
End of assembler dump.
(gdb) p 0x10f
$1 = 271
(gdb) q
level1@io:/levels$ strings level01
,0<     w
Enter the 3 digit passcode to enter: Congrats you found it, now read the password for level2 from /home/level2/.
pass
/bin/sh
.symtab
.strtab
.shstrtab
.text
.lib
.data
level01.asm
fscanf
skipwhite
doit
exitscanf
YouWin
exit
puts
main
prompt1
```



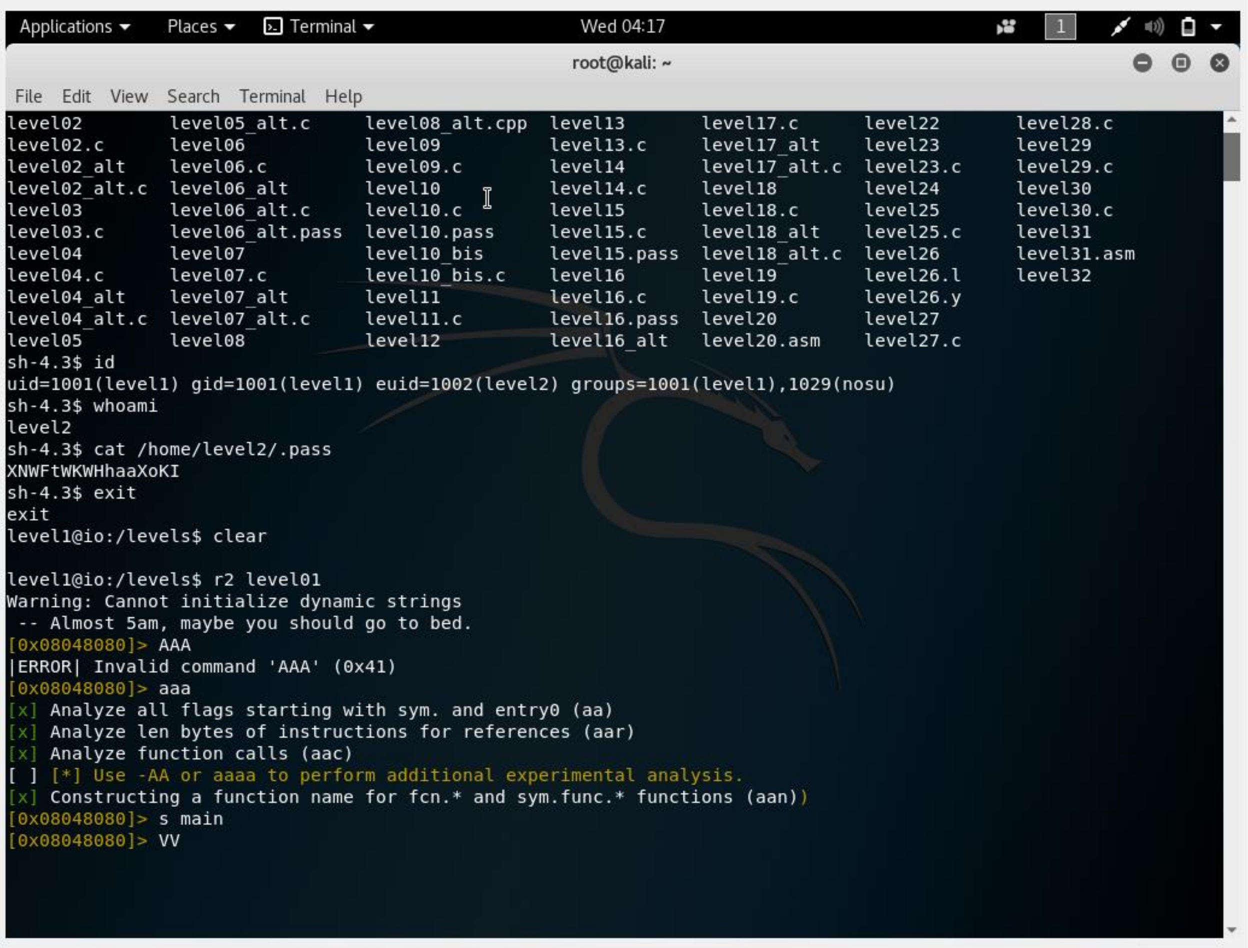
```
   0x08048094 <+20>:    je     0x80480dc
   0x0804809a <+26>:    call   0x8048103
End of assembler dump.
(gdb) p 0x10f
$1 = 271
(gdb) q
level1@io:/levels$ strings level01
,0<     w
Enter the 3 digit passcode to enter: Congrats you found it, now read the password for level2 from /home/level2/.
pass
/bin/sh
.symtab
.strtab
.shstrtab
.text
.lib
.data
level01.asm
fscanf
skipwhite
doit
exitscanf
YouWin
exit
puts
main
prompt1
prompt2
shell
_start
__bss_start
_edata
_end
level1@io:/levels$ ./level01
Enter the 3 digit passcode to enter: 271
Congrats you found it, now read the password for level2 from /home/level2/.pass
sh-4.3$ 
```



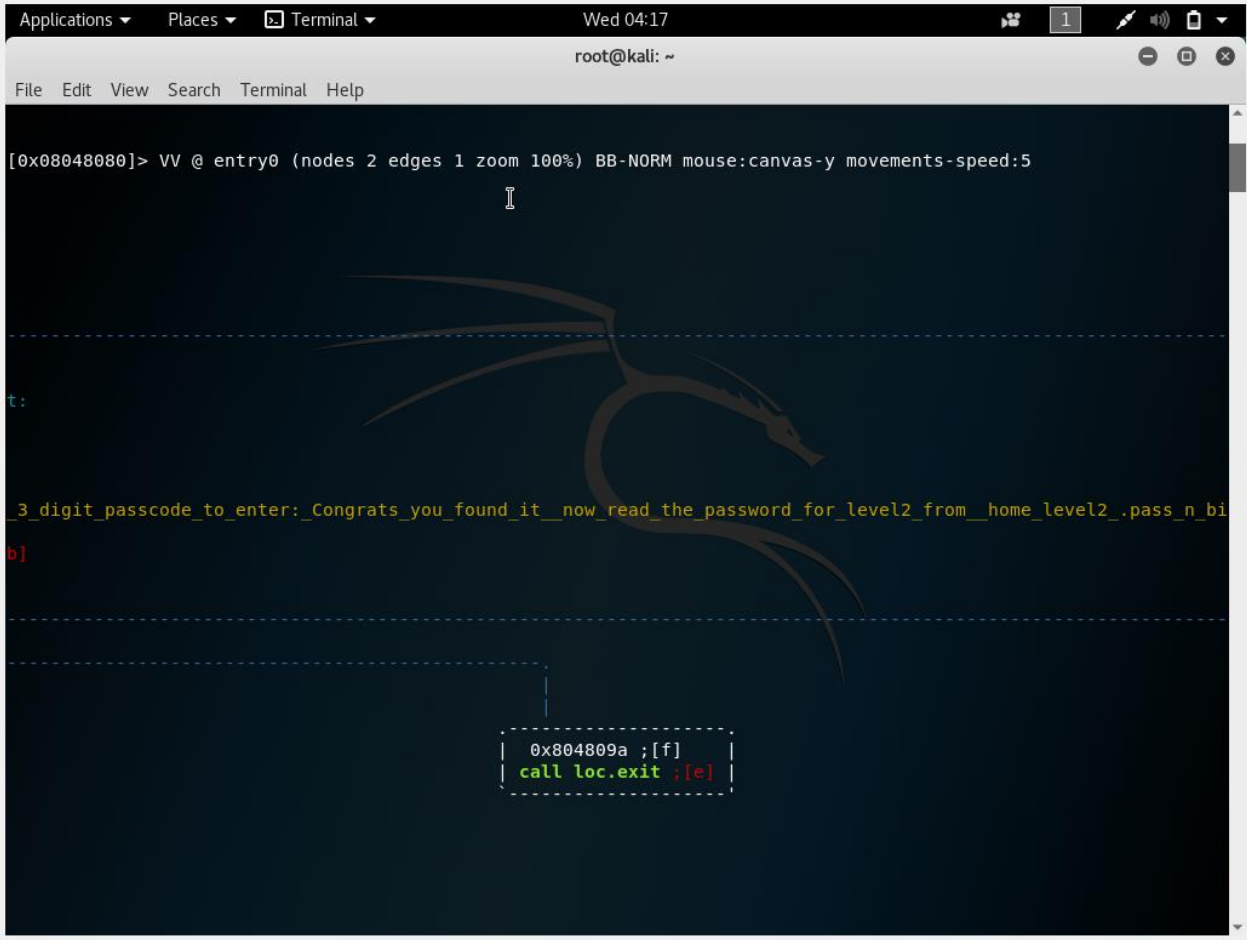
```
.text
.lib
.data
level01.asm
fscanf
skipwhite
doit
exitscanf
YouWin
exit
puts
main
prompt1
prompt2
shell
_start
__bss_start
_edata
_end
level1@io:/levels$ ./level01
Enter the 3 digit passcode to enter: 271
Congrats you found it, now read the password for level2 from /home/level2/.pass
sh-4.3$ ls
beta           level05.c         level08.cpp      level12.c     level16_alt.c  level20.pass  level27.pass
level01        level05_alt       level08_alt      level12.pass  level17        level21       level28
level02        level05_alt.c     level08_alt.cpp  level13       level17.c      level22       level28.c
level02.c      level06           level09          level13.c     level17_alt    level23       level29
level02_alt    level06.c         level09.c        level14       level17_alt.c  level23.c     level29.c
level02_alt.c  level06_alt       level10          level14.c     level18        level24       level30
level03        level06_alt.c     level10.c        level15       level18.c      level25       level30.c
level03.c      level06_alt.pass  level10.pass     level15.c     level18_alt    level25.c     level31
level04        level07           level10_bis      level15.pass  level18_alt.c  level26       level31.asm
level04.c      level07.c         level10_bis.c    level16       level19        level26.l     level32
level04_alt    level07_alt       level11          level16.c     level19.c      level26.y
level04_alt.c  level07_alt.c     level11.c        level16.pass  level20        level27
level05        level08           level12          level16_alt   level20.asm    level27.c
sh-4.3$ 
```



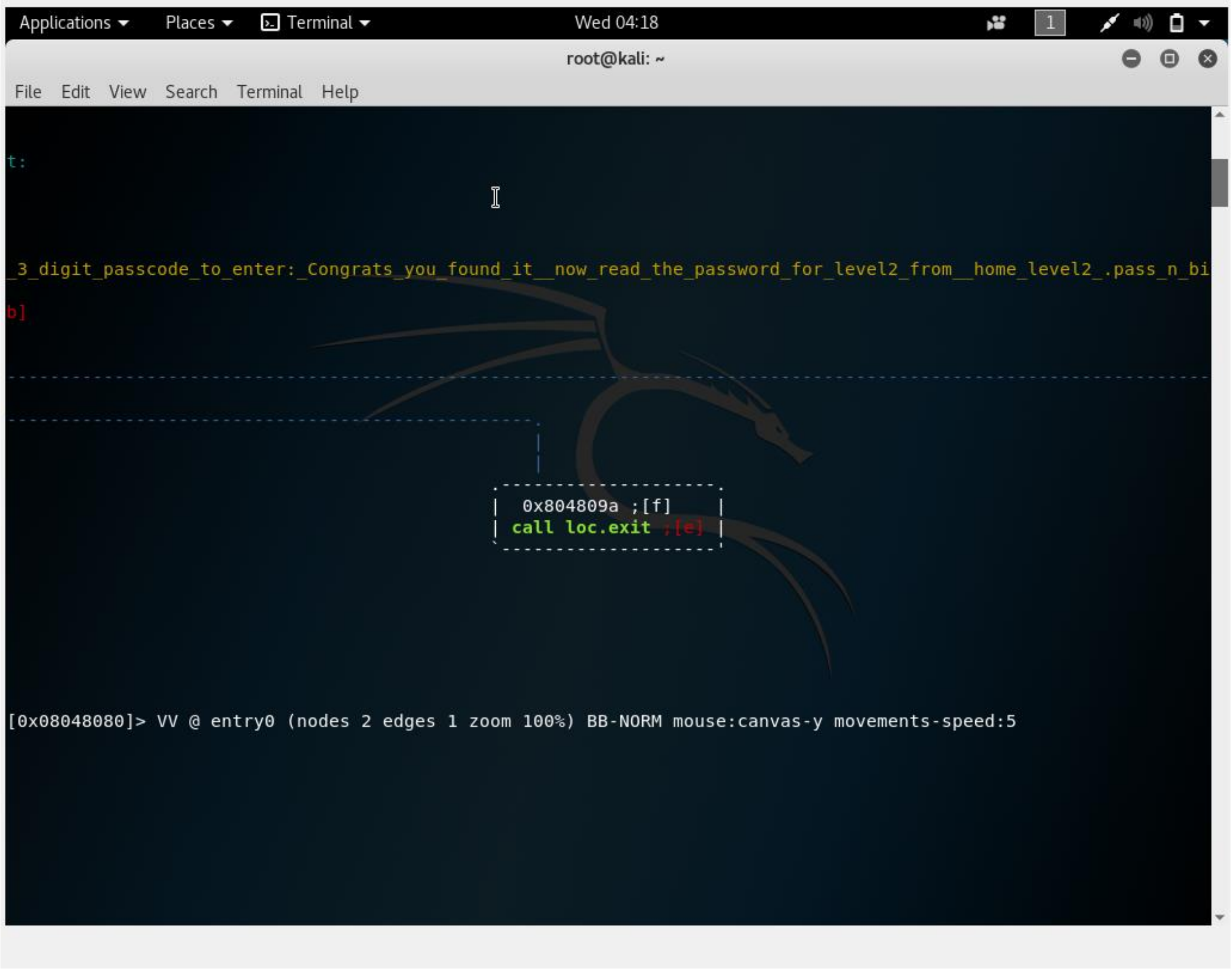
```
doit
exitscanf
YouWin
exit
puts
main
prompt1
prompt2
shell
_start
__bss_start
_edata
_end
level1@io:/levels$ ./level01
Enter the 3 digit passcode to enter: 271
Congrats you found it, now read the password for level2 from /home/level2/.pass
sh-4.3$ ls
beta           level05.c         level08.cpp      level12.c     level16_alt.c  level20.pass  level27.pass
level01        level05_alt       level08_alt      level12.pass  level17        level21       level28
level02        level05_alt.c     level08_alt.cpp  level13       level17.c      level22       level28.c
level02.c      level06           level09          level13.c     level17_alt    level23       level29
level02_alt    level06.c         level09.c        level14       level17_alt.c  level23.c     level29.c
level02_alt.c  level06_alt       level10          level14.c     level18        level24       level30
level03        level06_alt.c     level10.c        level15       level18.c      level25       level30.c
level03.c      level06_alt.pass  level10.pass     level15.c     level18_alt    level25.c     level31
level04        level07           level10_bis      level15.pass  level18_alt.c  level26       level31.asm
level04.c      level07.c         level10_bis.c    level16       level19        level26.l     level32
level04_alt    level07_alt       level11          level16.c     level19.c      level26.y
level04_alt.c  level07_alt.c     level11.c        level16.pass  level20        level27
level05        level08           level12          level16_alt   level20.asm    level27.c
sh-4.3$ id
uid=1001(level1) gid=1001(level1) euid=1002(level2) groups=1001(level1),1029(nosu)
sh-4.3$ whoami
level2
sh-4.3$ cat /home/level2/.pass
XNWFtWKWHhaaXoKI
sh-4.3$ 
```



```
level02        level05_alt.c     level08_alt.cpp  level13       level17.c      level22       level28.c
level02.c      level06           level09          level13.c     level17_alt    level23       level29
level02_alt    level06.c         level09.c        level14       level17_alt.c  level23.c     level29.c
level02_alt.c  level06_alt       level10          level14.c     level18        level24       level30
level03        level06_alt.c     level10.c        level15       level18.c      level25       level30.c
level03.c      level06_alt.pass  level10.pass     level15.c     level18_alt    level25.c     level31
level04        level07           level10_bis      level15.pass  level18_alt.c  level26       level31.asm
level04.c      level07.c         level10_bis.c    level16       level19        level26.l     level32
level04_alt    level07_alt       level11          level16.c     level19.c      level26.y
level04_alt.c  level07_alt.c     level11.c        level16.pass  level20        level27
level05        level08           level12          level16_alt   level20.asm    level27.c
sh-4.3$ id
uid=1001(level1) gid=1001(level1) euid=1002(level2) groups=1001(level1),1029(nosu)
sh-4.3$ whoami
level2
sh-4.3$ cat /home/level2/.pass
XNWFtWKWHhaaXoKI
sh-4.3$ exit
exit
level1@io:/levels$ clear

level1@io:/levels$ r2 level01
Warning: Cannot initialize dynamic strings
 -- Almost 5am, maybe you should go to bed.
[0x08048080]> AAA
|ERROR| Invalid command 'AAA' (0x41)
[0x08048080]> aaa
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze len bytes of instructions for references (aar)
[x] Analyze function calls (aac)
[ ] [*] Use -AA or aaaa to perform additional experimental analysis.
[x] Constructing a function name for fcn.* and sym.func.* functions (aan))
[0x08048080]> s main
[0x08048080]> VV
```



```
[0x08048080]> VV @ entry0 (nodes 2 edges 1 zoom 100%) BB-NORM mouse:canvas-y movements-speed:5



----------------------------------------------------------------------------------------------------------------

t:


_3_digit_passcode_to_enter:_Congrats_you_found_it__now_read_the_password_for_level2_from__home_level2_.pass_n_bi

b]

----------------------------------------------------------------------------------------------------------------

-------------------------------------------------.
                                                 |
                                                 |
                                             .---------------------.
                                             |  0x804809a ;[f]     |
                                             | call loc.exit ;[e]  |
                                             `---------------------'
```



```
t:

_3_digit_passcode_to_enter:_Congrats_you_found_it__now_read_the_password_for_level2_from__home_level2_.pass_n_bi

b]

----------------------------------------------------------------------------------------------------------------

------------------------------------------------.
                                                |
                                                |
                                            .---------------------.
                                            |  0x804809a ;[f]     |
                                            | call loc.exit ;[e]  |
                                            `---------------------'


[0x08048080]> VV @ entry0 (nodes 2 edges 1 zoom 100%) BB-NORM mouse:canvas-y movements-speed:5
```

Github link :