Advanced Unix Programming
Assignment-7
Vijesh Ghandare – 111403013

Q1.1.“The child “exec” call inherits the file descriptors of parent if Close_on_exec is not set“. Demonstrate with an example.

main program:

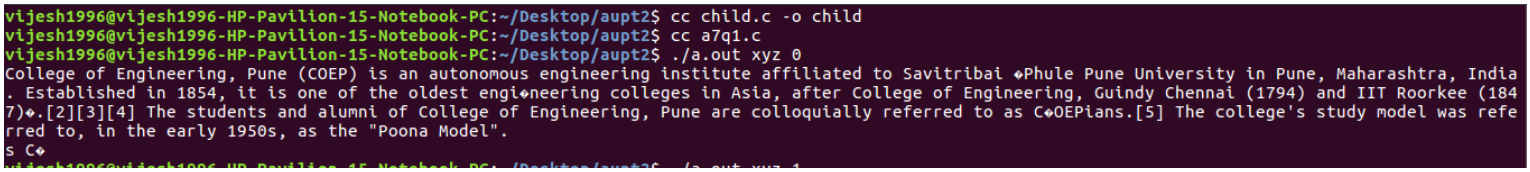
```c
#include<stdio.h>
#include<stdlib.h>
#include <unistd.h>
#include <fcntl.h>
#include <sys/types.h>
#include <sys/wait.h>
int main(int argc, char **argv){
    int fd, pid;
    char buf[10];
    fd = open(argv[1], O_RDWR);
    sprintf(buf, "%d", fd);
    char *const parmList[] = {"./child",buf, NULL}; /*parameter list for exec*/
    fcntl(fd, F_SETFD, atoi(argv[2]));              /*set and unset of CLOS_ON_EXEC*/
    pid = fork();
    if(pid == 0) {
        execvp("./child",parmList);
    }
    wait(NULL);
    return 0;
}
```

child program:

```c
#include<stdio.h>
#include<stdlib.h>
#include <unistd.h>
int main (int argc, char **argv){
    char buf [100];
    int fd = atoi(argv[1]);
    if(read(fd,buf,100) > 0){
        printf("%s",buf);
        while(read(fd,buf,100)){
            printf("%s", buf);
        }
    }
    else{
        printf("Read failed in child..!!!\n");
    }
    return 0;
}
```

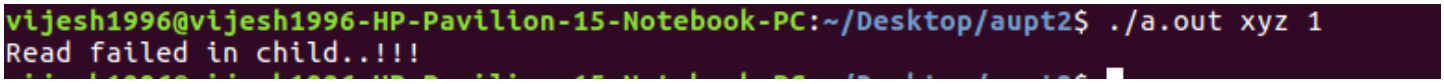
OUTPUTS:

***Case 1: Close_on_exec is not Set.**



In this case first argument to the code is filename and second is Close_on_exec flag. So, it is "zero" in this case and file is read by the child program successfully this shows that "fd" is inherited by child from the parent.

***Case 2: Close_on_exec is set.**



Close_on_exec is "set" and "fd" not inherited by child , hence read failed in child.

Q2.Write a program that takes a file name as an argument, opens the file, reads it and closes the file.The file should contain a string with the name of another application (e.g., 'ls' or 'ps' or any of your own applications) and the program forks a new process that executes the application named in the file.

Program:

```c
#include<stdio.h>
#include<stdlib.h>
#include<sys/types.h>
#include<sys/stat.h>
#include<fcntl.h>
#include<string.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/wait.h>
#define MAX_ARGS 64
int main(int argc, char **argv){
    int j;
    char buff[255];
    char *params[MAX_ARGS];
    char **next = params;
    int fd = open(argv[1],O_RDONLY);
    if(fd <= 0){
        printf("Open failed..!!!\n");
        return 0;
    }
    read(fd,buff,255);
    close(fd);
    char *token = strtok(buff," \n");
    while(token != NULL){
        *next++ = token;
        token = strtok(NULL," \n");
    }
    *next = NULL;
    pid_t pid;
    if ((pid = fork()) == -1)
        perror("fork() error");
     else if (pid == 0) {
        execvp(params[0],params);
        printf("Return not expected. Must be an execvp() error.\n");
     }
     wait(NULL);
    return 0;
}
```

OUTPUTS:
Output1: for “ls” command

```
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/aupt2$ cat commandFile.txt
ls -l
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/aupt2$ cc a7q2.c
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/aupt2$ ./a.out commandFile.txt
total 112
-rw-rw-r-- 1 vijesh1996 vijesh1996   484 Oct 10 09:11 a7q1.c
-rw-rw-r-- 1 vijesh1996 vijesh1996   801 Oct 10 09:29 a7q2.c
-rw-rw-r-- 1 vijesh1996 vijesh1996   458 Oct  7 20:33 a7q3.c
-rwxrwxr-x 1 vijesh1996 vijesh1996  9072 Oct 10 09:29 a.out
-rwxrwxr-x 1 vijesh1996 vijesh1996  8872 Oct 10 09:23 child
-rw-rw-r-- 1 vijesh1996 vijesh1996   316 Oct 10 09:23 child.c
-rw-rw-r-- 1 vijesh1996 vijesh1996     6 Oct 10 09:28 commandFile.txt
-rw-rw-r-- 1 vijesh1996 vijesh1996 20185 Oct  4 21:37 LAB7.pdf
-rw-rw-r-- 1 vijesh1996 vijesh1996   368 Oct  7 16:34 ls.c
-rwxrwxr-x 1 vijesh1996 vijesh1996  8800 Oct  4 17:10 main
-rw-rw-r-- 1 vijesh1996 vijesh1996   240 Oct  7 18:43 main.c
-rwxrwxr-x 1 vijesh1996 vijesh1996  8752 Oct  7 18:42 my
-rw-rw-r-- 1 vijesh1996 vijesh1996   350 Oct  7 20:41 my.c
-rwxrwxr-x 1 vijesh1996 vijesh1996    17 Oct  4 17:13 script
-rw-rw-r-- 1 vijesh1996 vijesh1996   497 Oct 10 09:21 xyz
-rw-rw-r-- 1 vijesh1996 vijesh1996    24 Oct  7 18:29 xyz1
```

Output2: for “ps” command

```
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/aupt2$ cat commandFile.txt
ps
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/aupt2$ ./a.out commandFile.txt
  PID TTY          TIME CMD
 2457 pts/2    00:00:00 bash
 3362 pts/2    00:00:00 a.out
 3363 pts/2    00:00:00 ps
```

Q3: Implement cat < hw.txt > hw-copy.txt

Program:

```c
#include<stdio.h>
#include<unistd.h>
#include <sys/types.h>
#include <sys/wait.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <errno.h>
int main(int argc,char **argv){
    int fdr = open(argv[1],O_RDONLY);
    int fdw = open(argv[2],O_WRONLY | O_CREAT | O_TRUNC,0777);
    pid_t pid = fork();
    if(pid == 0){
        dup2(fdr,0);
        dup2(fdw,1);
        execl("/bin/sh","sh","-c","cat",(char*)0);
        _exit(127);
    }
    if(waitpid(pid,NULL,0) != pid)
        return errno;
    return 0;
}
```

OUTPUTS:

***Initial Contents of File1 and File2**

```
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/aupt2$ cat file1
College of Engineering, Pune (COEP) is an autonomous engineering institute affiliated to Savitribai Phule Pune University in Pune, Maharashtra, India.
 Established in 1854, it is one of the oldest engineering colleges in Asia, after College of Engineering, Guindy Chennai (1794) and IIT Roorkee (1847)
.[2][3][4] The students and alumni of College of Engineering, Pune are colloquially referred to as COEPians.[5] The college's study model was referred
 to, in the early 1950s, as the "Poona Model".
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/aupt2$ cat file2
```

***Contents of File1 and File2 after program execution:**

```
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/aupt2$ cc a7q3.c
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/aupt2$ ./a.out file1 file2
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/aupt2$ cat file1
College of Engineering, Pune (COEP) is an autonomous engineering institute affiliated to Savitribai Phule Pune University in Pune, Maharashtra, India.
 Established in 1854, it is one of the oldest engineering colleges in Asia, after College of Engineering, Guindy Chennai (1794) and IIT Roorkee (1847)
.[2][3][4] The students and alumni of College of Engineering, Pune are colloquially referred to as COEPians.[5] The college's study model was referred
 to, in the early 1950s, as the "Poona Model".
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/aupt2$ cat file2
College of Engineering, Pune (COEP) is an autonomous engineering institute affiliated to Savitribai Phule Pune University in Pune, Maharashtra, India.
 Established in 1854, it is one of the oldest engineering colleges in Asia, after College of Engineering, Guindy Chennai (1794) and IIT Roorkee (1847)
.[2][3][4] The students and alumni of College of Engineering, Pune are colloquially referred to as COEPians.[5] The college's study model was referred
 to, in the early 1950s, as the "Poona Model".
```

---

4. Bob works for an auditing agency needs to be able to read all the files in the system. The system admin has to protect the integrity of the system and should not allow Bob to modify or delete any file. Write a special SETUID program for the admin so that he can gave the executable permission of it to Bob. This program requires Bob to type a file name at the command line and then it will run /bin/cat to display the specified file. Can Bob compromise the integrity (by adding/modifying/deleting files) of this system? How?

CODE:

a7q4.c

```c
#include <string.h>
#include <stdio.h>
#include <stdlib.h>
#include<unistd.h>
#include <sys/types.h>

int main(int argc, char *argv[]) {
    char *buffer[3];
    if(setuid(1000) == -1)
        printf("error");
    buffer[0] = "/bin/cat"; buffer[1] = argv[1]; buffer[2] = 0;
    if(execve(buffer[0], buffer, 0) < 0) {
        printf("exec error\n");
        return 0;
    }
    return 0;
}
```

OUTPUTS:

***Initial Permissions: When owner is user**

```
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/AUP/Lab7/que4$ cc a7q4.c -o a7q4
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/AUP/Lab7/que4$ ls -l
total 20
-rwxrwxr-x 1 vijesh1996 vijesh1996 8816 Oct 25 08:47 a7q4
-rw-rw-r-- 1 vijesh1996 vijesh1996  353 Oct 12 21:47 a7q4.c
-rwx------ 1 vijesh1996 vijesh1996   10 Oct 10 16:23 xyz1
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/AUP/Lab7/que4$ chmod u+s a7q4
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~/AUP/Lab7/que4$ ls -l
total 20
-rwsrwxr-x 1 vijesh1996 vijesh1996 8816 Oct 25 08:47 a7q4
-rw-rw-r-- 1 vijesh1996 vijesh1996  353 Oct 12 21:47 a7q4.c
-rwx------ 1 vijesh1996 vijesh1996   10 Oct 10 16:23 xyz1
```

***Copying files from owner to temp user:**

```
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~$ sudo cp -p /home/vijesh1996/AUP/Lab7/que4/a7q4 /home/temp/Desktop/que4/
[sudo] password for vijesh1996:
```

```
vijesh1996@vijesh1996-HP-Pavilion-15-Notebook-PC:~$ sudo cp -p /home/vijesh1996/AUP/Lab7/que4/xyz1 /home/temp/Desktop/que4/
```

***Final outputs: when files executed by temp user**

```
temp@vijesh1996-HP-Pavilion-15-Notebook-PC:~$ cd Desktop/que4/
temp@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/que4$ ls -l
total 16
-rwsrwxr-x 1 vijesh1996 vijesh1996 8816 Oct 25 08:47 a7q4
-rwx------ 1 vijesh1996 vijesh1996   10 Oct 10 16:23 xyz1
temp@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/que4$ cat xyz1
cat: xyz1: Permission denied
temp@vijesh1996-HP-Pavilion-15-Notebook-PC:~/Desktop/que4$ ./a7q4 xyz1
Hello all
```