Exercise-3: Gaining Access to restricted files

Introduction

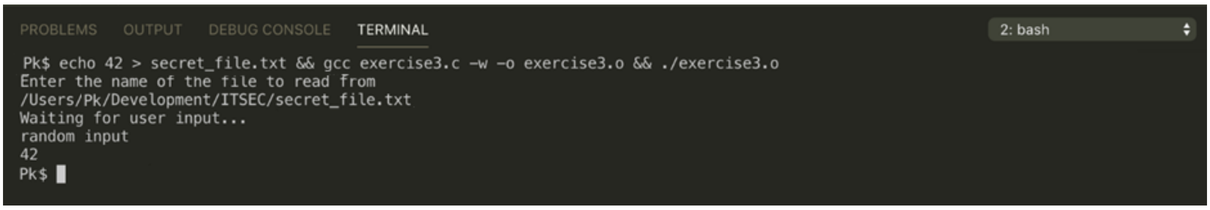
In this exercise, we are asked to read file **secret_file.txt** from a C implementation. This C implementation compares the file name, or a symbolic link of the file name passed. If the filename is matched or the symbolic link is found, then the program exits with access denial.

Source code →

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

char *secret_file = "secret_file.txt";

int linksToSecret(char *fn) {

    char buf[512];

    int count = readlink(fn, buf, sizeof(buf));
    if (count > 0) {
        buf[count] = '\0';
        if (strncmp(buf, secret_file, strlen(secret_file) - 1) == 0) {
            return 1;
        } else {
            return 0;
        }
    }

}

int main() {

    char input[100];
    char fileName[100];
    printf("Enter the name of the file to read from\n");
    fgets(fileName, sizeof(fileName), stdin);

    fileName[strlen(fileName) - 1] = '\0';

    if (strncmp(fileName, secret_file, strlen(secret_file)) == 0 ||
            linksToSecret(fileName) == 1) {
        printf("You are not allowed to access %s or symbolic links to
it!\n", secret_file);
    } else {
        printf("Waiting for user input...\n");
        fgets(input, sizeof(input), stdin);

        FILE *fp = fopen(fileName, "r");
        if (fp != NULL) {
            char ch;
            while ((ch = fgetc(fp)) != EOF)
                printf("%c", ch);
            fclose(fp);
        } else {
            printf("You must provide an existing file you may access!\n");
        }
    }
}
```

Gaining Access to the file

It seems that the access control is implemented by comparing the file name. This check can be easily circumvented by using the complete address of the file.



```
 Pk$ echo 42 > secret_file.txt && gcc exercise3.c -w -o exercise3.o && ./exercise3.o
Enter the name of the file to read from
/Users/Pk/Development/ITSEC/secret_file.txt
Waiting for user input...
random input
42
Pk$ 
```

Mitigation

- Instead of using string compare, we can use string contains for comparing file name to restrict access.

- Use of mature access control techniques.