**TP-N7 : Faille OverFlow**

**On considère le programme rédigé en langage C suivant :**

#include <stdio.h>

#include <string.h>

#include <stdlib.h>

int main(void)

{

char buff[15];

int pass = 0;

printf("\n Enter the password : \n");

gets(buff);

if(strcmp(buff, "tmardasri"))

{

printf ("\n Wrong Password \n");

}

else

{

printf ("\n Correct Password \n");

pass = 1;

}

if(pass)

{

/\* Now Give root or admin rights to user\*/

printf ("\n Root privileges given to the user \n");

}

return 0;

} //Fin

Objectif du TP : Cette manipulation a pour objectif de montrer la faille Overflow, d’abord compiler ce programme sous Devc++ et l’exécuter.

1. Donner un mot de passe correcte et constater le résultat.
2. Donner un mot de passe incorrecte et vérifier le résultat.

Problème : En cas de mot de passe incorrect nous allons dépasser la taille prévu pour le mot de passe, et on constate que le programme donner accès à l’application. Cette faille est connue sous le nom de Overflow.

Solution :

1. D’abord vérifier la taille de mot de passe fourni qui ne doit pas dépasser un certain nombre de caractère.
2. Limiter le nombre de tentation à 3 par exemple renouvelable après un délai.