Brent Turner

CSC 495

Lab 1

Buffer Overflow

TARGET 1: (target1.c found at the bottom)

A buffer Overflow is present when, if the exploit exists, a piece of memory, a buffer, is given more data to which it can hold, and then proceeds to fill that data in other places of the buffer, that are most defiantly not intended, to the point where, if the code is present, the hacker can get the program to move to a specific return address in the code.

Objective

The objective is to perform a buffer overflow on a program that looks to see if a password is valid, but in a very poor way. The program being exploitable allows the "hacker" to enter a password with shell code to bypass the successful login check. The overflow is made when the entered text exceeds the designated size of the buffer, and, once the entered text reaches the high memory address, the "hacker" can input shell code in order to direct to the return address of a successful login.

1 & 2

Parameters: None

return address: 0x000005bc (successfulLogin) 4bytes

0x000005e7 (incorrectPasswordError) – 4bytes

local variable:

usersPassword – (size of 8 * size of pointer 4) = 32 bytes

password – (size of 8 * size of pointer 4) = 32 bytes

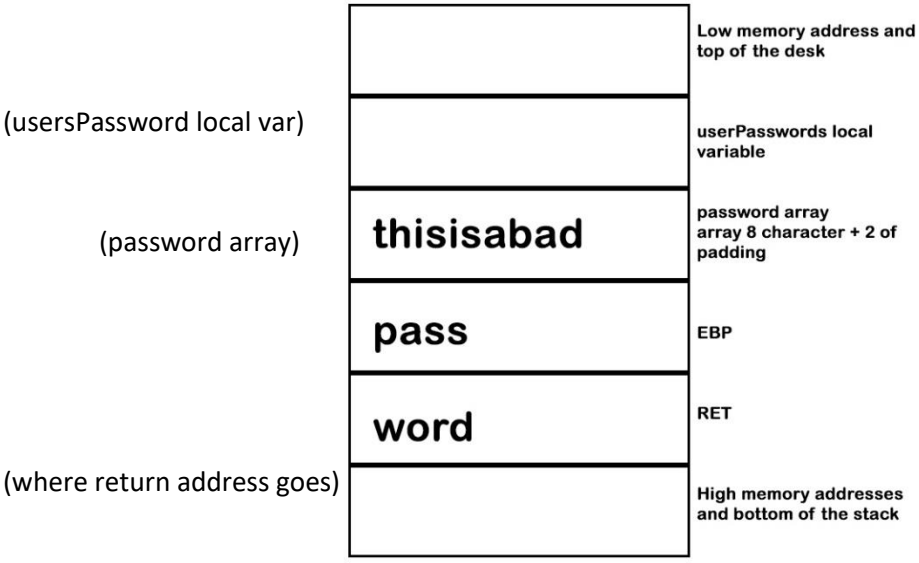
3

To get the overflow buffer one must type in 18 characters then the shell code

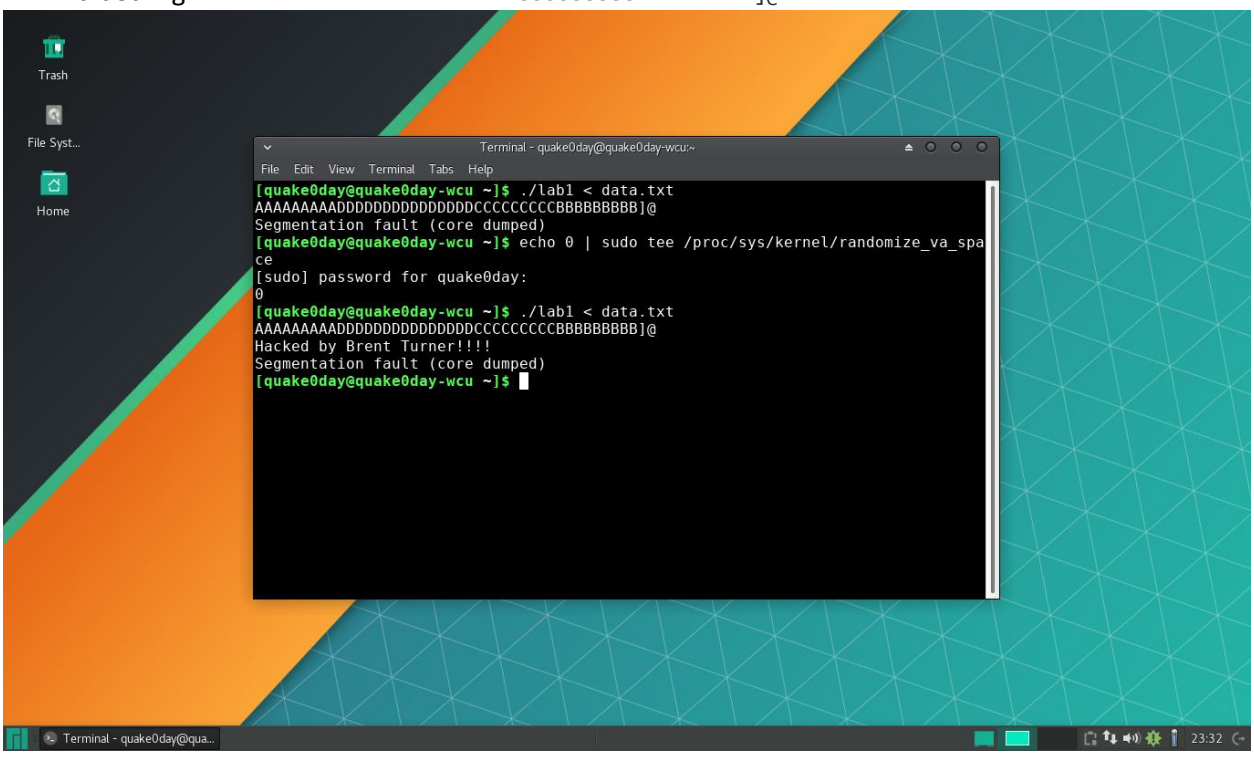
(8 (array size) + 2 (padding) + 4 (size of EBP) + 4 (size of RET)) These are the base 18 characters and then the shell code can proceed

4

The overflow direction is down words to get access to memory address



DATA.txt String: AAAAAAAAADDDDDDDDDDDDDDDCCCCCCCCCCBBBBBBBBB]@



Target1.c

```c
#include<stdio.h>

                    #include <string.h>
                    void successfulLogin();
```

```c
void incorrectPasswordError();


main()
{
    //need to make a buffer/stack in order to overflow
    char password[8];
    char usersPassword[8] = "secret99";
    gets(password);


    if(password == usersPassword)
    {
        successfulLogin();
    }
    else
    {
        incorrectPasswordError();
    }
}


void successfulLogin()
{
    printf("You password is correct, You have now logged in");
}


void incorrectPasswordError()
{
    printf("The entered password was incorrect, please try again");
}
```