EPICODE

CYBERSECURITY COURSE

BY MAX ALDROVANDI

17/05/2024

Web-site: https://epicode.com/it

Locality:

Via dei Magazzini Generali,
6 Roma, Lazio 00154, IT

PRACTICE EXERCISE S7/L4

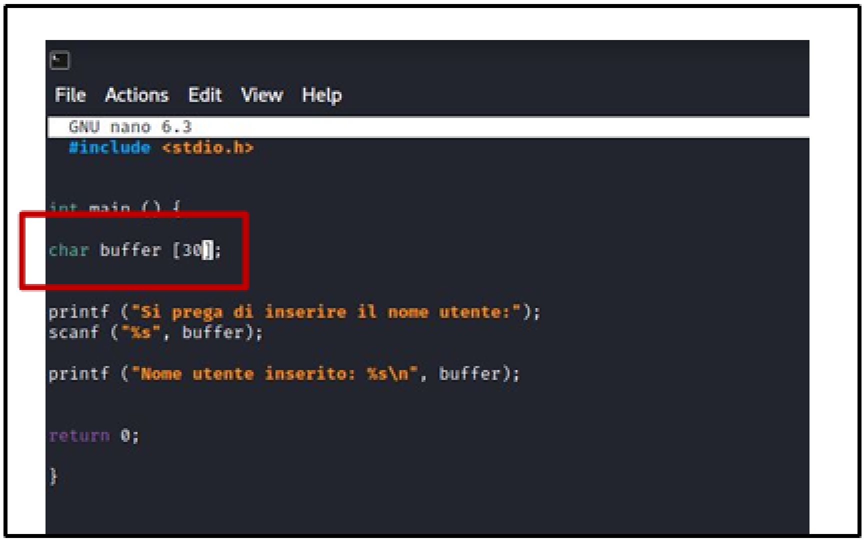
Track:

Modify an example of code in C that is intentionally vulnerable to BOFs, and how to trigger a particular error situation called a "segmentation fault," which is a memory error that occurs when a program inadvertently tries to write to a memory location where it is not allowed to write (such as may be a memory location dedicated to operating system functions).

Solution:

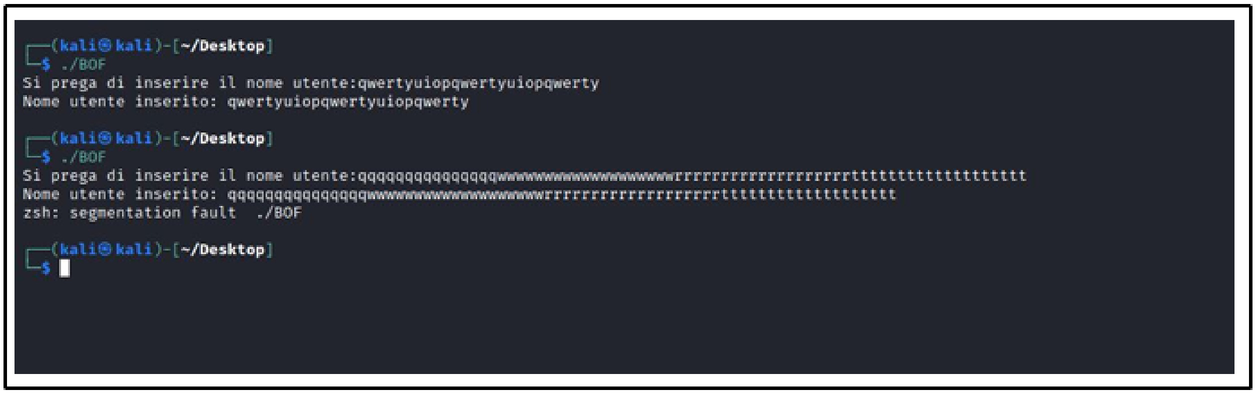
To reproduce the memory error by changing the buffer capacity, we need to perform the following steps:

- Modify the source code of the program so that the variable "buffer" has a capacity of 30 elements, as in the figure:



```
#include <stdio.h>


int main () {

char buffer [30];


printf ("Si prega di inserire il nome utente:");
scanf ("%s", buffer);

printf ("Nome utente inserito: %s\n", buffer);


return 0;

}
```

- Compile the program to generate an executable file downstream of the changes we just introduced with the command: "gcc -g BOF.c -o BOF."
- Run the program again by entering a number of characters greater than 30.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF
Si prega di inserire il nome utente:qwertyuiopqwertyuiopqwerty
Nome utente inserito: qwertyuiopqwertyuiopqwerty

┌──(kali㉿kali)-[~/Desktop]
└─$ ./BOF
Si prega di inserire il nome utente:qqqqqqqqqqqqqqqwwwwwwwwwwwwwwwwwwwrrrrrrrrrrrrrrrrrrrttttttttttttttttttt
Nome utente inserito: qqqqqqqqqqqqqqqwwwwwwwwwwwwwwwwwwwrrrrrrrrrrrrrrrrrrrttttttttttttttttttt
zsh: segmentation fault  ./BOF

┌──(kali㉿kali)-[~/Desktop]
└─$ █
```

With the new modification, by entering a number of characters <30 we have no problem, as you can see in the first example in the figure on the left.

By entering a number of characters >30, we are able to reproduce the segmentation error. This means that we are attempting to write part of our input to a portion of memory that is not accessible.