Report - CS6570 Assignment 3 - Return Oriented Programming (ROP)

CS18B040 - Raghu Raman

CS18B050 - Aniswar Srivatsa Krishnan

The ROP gadgets we used are as follows:

1) 0x0806c71e : imul eax, edx ; jmp 0x806c57b

2) 0x0805bf42 : pop edx ; ret

3) 0x080672b4 : mov dword ptr [edx], eax ; lea eax, [edx + 1] ; ret

4) 0x080672b6 : lea eax, [edx + 1] ; ret

The gadgets are chained as follows:

1) First the buffer cat\_buf in the function concatenate\_first\_chars() is overflowed to overwrite RA and subsequently place the other gadgets.

2) With the help of gadget 2 and the stack, 5 is placed in edx.

3) With the help of gadget 1 now, 6 is placed in edx.

4) The gadget 1 is used to multiply eax and edx and place the value of 30 in eax

5) We then place 4 in the stack, use gadget to place it in edx and repeat the above procedure to place 120 in eax.

6) Repeating the above procedure with 3 and 2 leads to eax containing the value 6! = 720

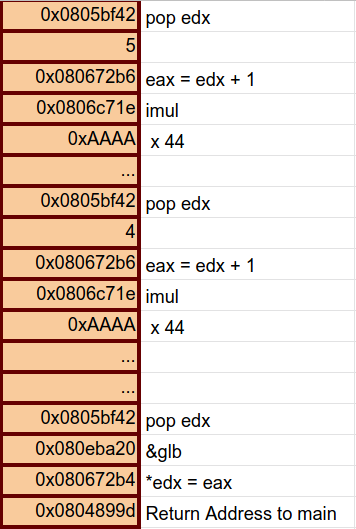
7) The address of the global variable glb 0x080eba20 is placed onto the stack and then loaded into edx using gadget 2.

8) Gadget 3 is then used to load the value of 6! in eax into the variable glb.

9) We then jump to the printf statement inside main function which prints the value of the variable glb.

This prints 720 and completes the required task successfully.

Below is the stack diagram for the reference.



Note: The technique followed for changing glb is also used to change the roll number global variable in the program to our roll numbers