# Report
# CS6570 Assignment 3 - ROP

CS18B040 R Raghu Raman
CS18B050 Aniswar Srivatsa Krishnan

March 10, 2021

## 1 Gadgets

The ROP gadgets we used are as follows:

- 0x0806c71e : imul eax, edx ; jmp 0x806c57b
- 0x0805bf42 : pop edx ; ret
- 0x080672b4 : mov dword ptr [edx], eax ; lea eax, [edx + 1] ; ret
- 0x080672b6 : lea eax, [edx + 1] ; ret

## 2 Exploit

The gadgets are chained as follows:

- First the buffer cat_buf in the function concatenate_first_chars() is overflowed to overwrite RA and subsequently place the other gadgets.
- With the help of gadget 2 and the stack, 5 is placed in edx.
- With the help of gadget 1 now, 6 is placed in edx.
- The gadget 1 is used to multiply eax and edx and place the value of 30 in eax
- We then place 4 in the stack, use gadget to place it in edx and repeat the above procedure to place 120 in eax.
- Repeating the above procedure with 3 and 2 leads to eax containing the value 6! = 720
- The address of the global variable glb 0x080eba20 is placed onto the stack and then loaded into edx using gadget 2.
- Gadget 3 is then used to load the value of 6! in eax into the variable glb.
- 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.

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

## 3 Stack

| | |
|---|---|
| 0x0805bf42 | pop edx |
| 5 | |
| 0x080672b6 | eax = edx + 1 |
| 0x0806c71e | imul |
| 0xAAAA | x 44 |
| ... | |
| 0x0805bf42 | pop edx |
| 4 | |
| 0x080672b6 | eax = edx + 1 |
| 0x0806c71e | imul |
| 0xAAAA | x 44 |
| ... | |
| ... | |
| 0x0805bf42 | pop edx |
| 0x080eba20 | &glb |
| 0x080672b4 | *edx = eax |
| 0x0804899d | Return Address to main |

Figure 1: Stack Contents