IntroSec HW6

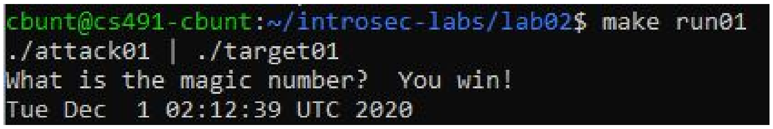
Name: *Carl Bunt* ***Class:*** *CS491 - Intro to Security*

Prof Karen Karavanic

04 DEC 2020
Portland State University

Target 01:

When decompiled I found `movl $0xe032e6e,-0x4(%ebp)` just before it was compared with `%eax` which was the hex of **235089518**.

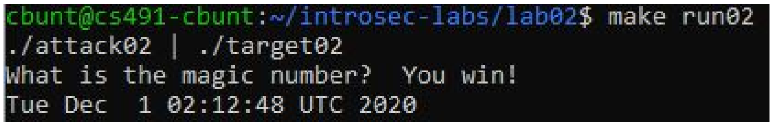


```
cbunt@cs491-cbunt:~/introsec-labs/lab02$ make run01
./attack01 | ./target01
What is the magic number?  You win!
Tue Dec  1 02:12:39 UTC 2020
```

Figure 1: **Attack01: Success**

Target 02:

When decompiled I found `cmp %eax,0x8(%ebp)`. The val in `%eax` at that is struction was **1410972340**.

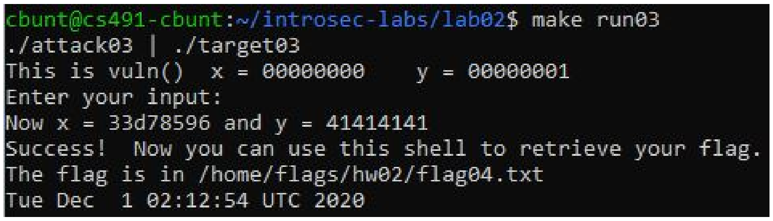


```
cbunt@cs491-cbunt:~/introsec-labs/lab02$ make run02
./attack02 | ./target02
What is the magic number?  You win!
Tue Dec  1 02:12:48 UTC 2020
```

Figure 2: **Attack02: Success**

Target 03:

When decompiled I found `cmpl $0x33d78596,-0xc(%ebp)`. I needed to overflow the char[16] buffer and the 4 int32 so I pushed 20 `A`'s then `0x96`, `0x85`, `0xD7`, `0x33` to writ the value into `x`.



```
cbunt@cs491-cbunt:~/introsec-labs/lab02$ make run03
./attack03 | ./target03
This is vuln()  x = 00000000    y = 00000001
Enter your input:
Now x = 33d78596 and y = 41414141
Success!  Now you can use this shell to retrieve your flag.
The flag is in /home/flags/hw02/flag04.txt
Tue Dec  1 02:12:54 UTC 2020
```

Figure 3: **Attack03: Success**