Student CTF
Summer Term 2013

Raphael Ernst

Assignment Sheet 1

Information about this sheet:

- Release date: Tuesday, May 21st, 2013
- Discussion in group: Tuesday, May 28th, 2013

Exercise 1: C Memory Problems / Exploitation

Consider the following C program.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#define BLOCK_SIZE 4

int retVal;
char memoryBlock1[BLOCK_SIZE];
int val;
char memoryBlock2[BLOCK_SIZE];

int sampleFn(char* input) {
   char memoryBlock3[BLOCK_SIZE];
   int retVal = 42;

   memcpy(memoryBlock3,input,strlen(input));

   return retVal;
}

int main(int argc, char* argv[]) {
   retVal = 23;
   val = 21;

   if(argc != 3) {
      printf("Expecting two parameters...\n");
      return retVal;
   }
```

```
    printf("%s %d\n",argv[1],strlen(argv[1]));
    printf("retVal: %d\n",(int)&retVal);
    printf("memoryBlock1: %d\n",(int)memoryBlock1);
    printf("memoryBlock1[1]: %d\n",(int)&memoryBlock1[1]);
    printf("memoryBlock1[2]: %d\n",(int)&memoryBlock1[2]);
    printf("val: %d\n",(int)&val);
    printf("memoryBlock2: %d\n",(int)memoryBlock2);

    memcpy(memoryBlock1,argv[1],strlen(argv[1]));
    printf("Result:\n");
    printf("sampleFn: %d\n",sampleFn(argv[2]));
    printf("retVal: %d\n",retVal);
    printf("val: %d\n",val);

    return retVal;
}
```

The program takes two arguments. Try to reach the following goals and describe your solution (Input, Compiler flags/options, Operation System, etc.):

- Crash the program
- Change the return value to a random value $\neq 23$
- Change the value of *val* to a random value $\neq 21$
- Change the return value of the *sampleFn* to a random value $\neq 42$
- Change the return value to 17
- Change the return value of the *sampleFn* to 21
- Prevent the execution of the *sampleFn*
- Run your own code