Cyber Defense Club @ UI

Date: 11/01/16

Start Time: 7:00 PM

End Time: 8:32 PM

1. Happenings
   1. Hannah Talked About Buffer Overflows
   2. When you call a function, you push parameters, the return address, the saved frame pointer, and then push local variables onto the stack
   3. Looked at Hannah’s Exploit Program

#include <stdlib.h>

#include <unistd.h>

#include <stdio.h>

int main(int argc, char \*\*argv)

{

volatile int modified;

char buffer[64];

modified = 0;

gets(buffer);

if(modified != 0) {

printf("you have changed the 'modified' variable\n");

} else {

printf("Try again?\n");

}

}

* 1. Another Exploit Program

#include <stdlib.h>

#include <unistd.h>

#include <stdio.h>

#include <string.h>

int main(int argc, char \*\*argv)

{

volatile int modified;

char buffer[64];

if(argc == 1) {

errx(1, "please specify an argument\n");

}

modified = 0;

strcpy(buffer, argv[1]);

if(modified == 0x61626364) {

printf("you have correctly got the variable to the right value\n");

} else {

printf("Try again, you got 0x%08x\n", modified);

}

}

* 1. Go through rest of examples at: <https://exploit-exercises.com/protostar/>
  2. Accomplished A LOT!
  3. Thanks Hannah for presenting and finding us things to use!