SYS300: LAB 2: Buffer Overflow

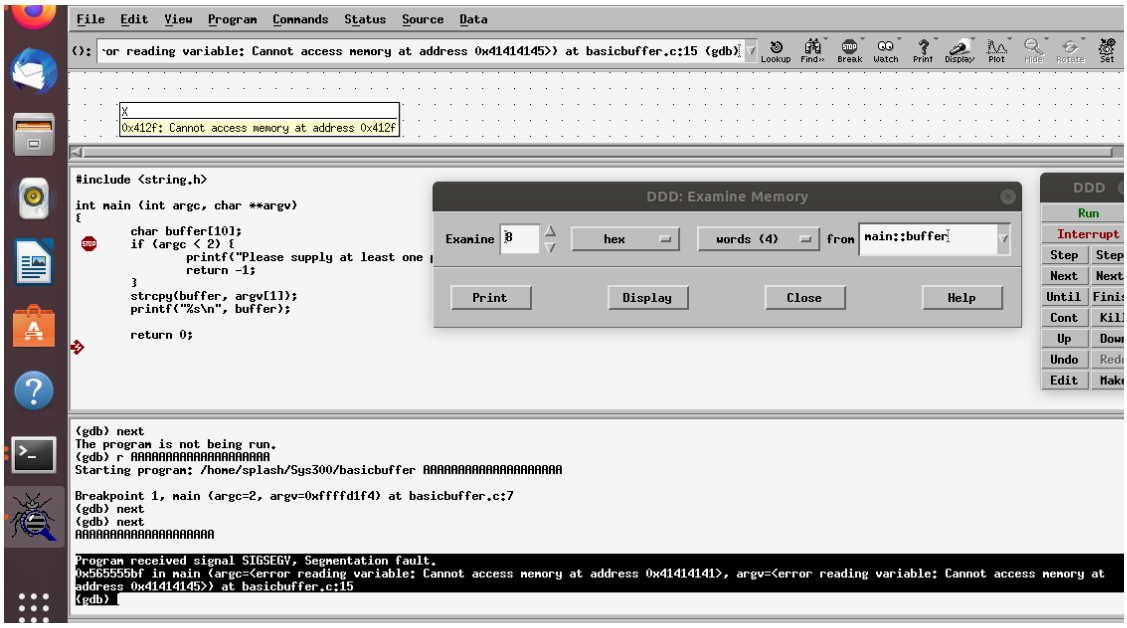
Lab notes:

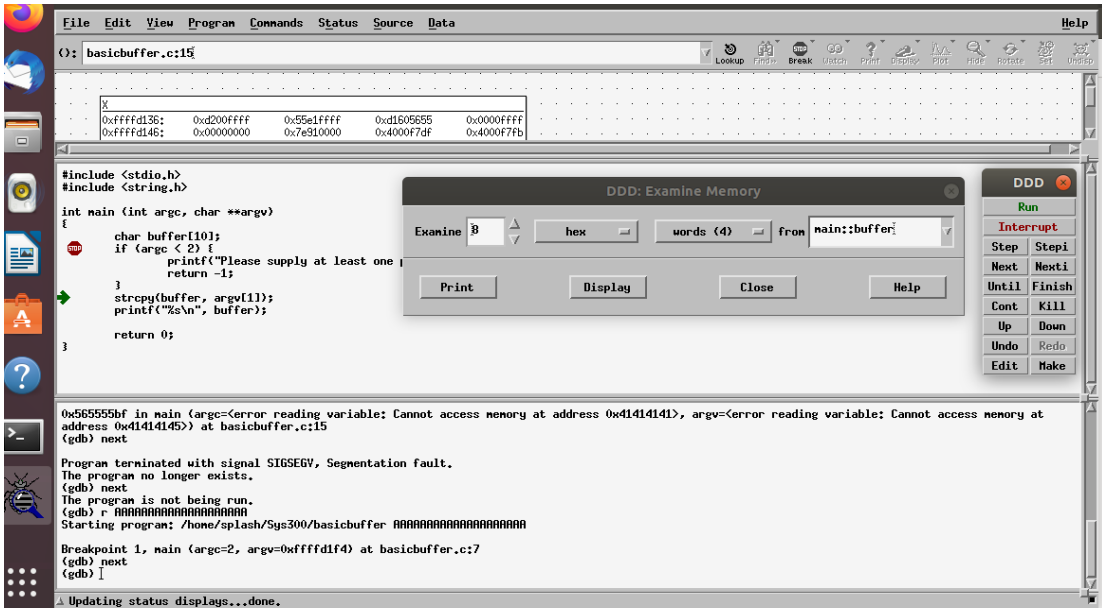
- Successfully installed ddd for graphical view of gdb
- When running the program after command “gcc -m32 -ggdb basicbuffer.c -o basicbuffer”
    - Inputs 10 or less yield a printed out input
    - 11 or more yields stack smashing

- When running the program after command “gcc -fno-stack-protector -m32 -ggdb basicbuffer.c -o basicbuffer”
    - 9 or less reprints input
    - 10 or more yields a segmentation fault

- In gdb, I was able to see:
    - Stack smashing detected at 10 A’s input and it would terminate
    - However, inputs of 30+ would yield “argc=<error reading variable: Cannot access memory at address 0x41414141>”...showing that the memory location was actually the hex of A and the program quit because that memory was inaccessible.
    - When I tried 11 A’s,I get a segmentation fault, but no argc error with 41’s
    - Each time I add a number, the 41’s would start to appear (i.e. 0x00000041, 0x00004141)

- The ddd program worked well and was able to see the break arrow when too many A’s were typed in (as well as the gdb command line segmentation fault error at the bottom)




File Edit View Program Commands Status Source Data Help
(): basicbuffer.c:15
Lookup Finish Break Watch Print Display Plot Hide Rotate Set Unset
X
0xffffd136: 0xd200ffff 0x55e1ffff 0xd1605655 0x0000ffff
0xffffd146: 0x00000000 0x7e910000 0x4000f7df 0x4000f7fb
#include <stdio.h>
#include <string.h>
int main (int argc, char **argv)
{
char buffer[10];
if (argc < 2) {
printf("Please supply at least one
return -1;
}
strcpy(buffer, argv[1]);
printf("%s\n", buffer);
return 0;
}
DDD: Examine Memory
Examine 8
hex
words (4)
from main::buffer
Print
Display
Close
Help
DDD
Run
Interrupt
Step Stepi
Next Nexti
Until Finish
Cont Kill
Up Down
Undo Redo
Edit Make
0x565555bf in main (argc=<error reading variable: Cannot access memory at address 0x41414141>, argv=<error reading variable: Cannot access memory at address 0x41414145>) at basicbuffer.c:15
(gdb) next
Program terminated with signal SIGSEGV, Segmentation fault.
The program no longer exists.
(gdb) next
The program is not being run.
(gdb) r AAAAAAAAAAAAAAAAAAAA
Starting program: /home/splash/Sys300/basicbuffer AAAAAAAAAAAAAAAAAAAA
Breakpoint 1, main (argc=2, argv=0xffffd1f4) at basicbuffer.c:7
(gdb) next
(gdb)
Updating status displays...done.