Assignment 5, Fall 2015
CS 4630, Defense Against the Dark Arts
Incursus Format Sententiam

Purpose
To learn how format string vulnerabilities can be exploited.

Due Date
This assignment is due on Wednesday, 10/21/2015, at 10:00am

Prerequisites to Review
1. Review the "Format String Vulnerability" slides.
2. Review the website: http://www.infond.fr/2010/07/tutorial-exploitation-format-string.html
3. Another resource is Ször.

Assignment Details
1. This assignment must be completed using the Ubuntu 12.04 LTS OS you installed on your VM. This environment is where we will test your submitted code. It is possible, due to the sensitivity of vulnerabilities to the operating environment, that exploit code developed for one environment will work not correctly in a slightly different environment.

2. Download the files format_string_vulnerability.bin and format_string_vulnerability.c. You must use format_string_vulnerability.bin. Do not recompile and use a different version. Again, it is possible, due to the sensitivity of vulnerabilities to the operating environment, that exploit code developed for one executable will work not correctly for a slightly different executable.

3. This program has a format string vulnerability that you can exploit to give yourself a better grade than the default, which is an "D". Your goal is to give yourself a grade of "A".

4. As before, you should write a program that generates the malicious input. This program can be written using C, perl, python or any language of your choice. Here are two sample runs that demonstrate the sample runs of the program.
   Assume the file name.txt contains two lines where each line has the name Ron Weasley.

```
$ ./format_string_vulnerability.bin <name.txt
Ron Weasley
Thank you, Ron Weasley.
I recommend that you get a grade of D on this assignment.
$
```

   Now we generate an attack string by running a shell script attack_format_string.sh and running the program.

```
$ ./attack_format_string.sh >grade.txt
$ ./format_string_vulnerability.bin <grade.txt
(?0 Tp ` ? ?? ? @ ? H ?d 1073859552 1073856500 1073945512
Thank you, Ron Weasley.
```

```
I recommend that you get a grade of A on this assignment.
$
```

5. You must use the executable provide to you via the Collab. Notice the garbled output before the “Thank you, Ron Weasley” message. This output is being generated by the format string that is being passed to function vulnerable() . This type of output is a downside of a format string attack.

Items to Submit

1. You should submit your attack string file. It must be called grade.txt