Network Security
Homework Assignment 3

CS5285
2016 Fall

Problem 0:

In this homework assignment, you will exploit simple software vulnerabilities in C programs. In order to ensure that everyone uses the same platform, the programs will be running on a virtual machine. As your 0th task, please

- download and install Oracle VM Virtualbox (https://www.virtualbox.org/),
- download the virtual machine from Blackboard and import it into Virtualbox,
- start the virtual machine.

After a couple of seconds, you should see a text-based Ubuntu Linux login screen. Enter `user` for the username and `password` for the password.[1]

In your home directory, you will find (type `ls –lt` to list the contents of the directory) five programs: `problem1`, …, `problem5`. You can launch `problemX` by typing `./problemX`. Attached to this assignment description, you will find the corresponding C source files: `problem1.c`, …, `problem5.c`. Please note that you will not have to compile these files, you will need them only for finding vulnerabilities.

For each problem, you will have to read the contents of a secret file:

```
/home/netsec/secret1.txt
…
/home/netsec/secret5.txt
```

You will be able to read the contents of each file by finding and exploiting a vulnerability in the corresponding program. Note that each file contains a simple, one-sentence message.

As your solution, please submit for each problem

- contents of the secret file
- short description of how you would fix this vulnerability (you only have to fix the vulnerability that you have exploited, not any other one).

Happy hacking!

[1] If you would like to login using SSH, please see instructions at the end of this file. This is completely optional.

Problem 1 (2 point): Buffer Overflow

- Exploit the buffer overflow vulnerability! Note that you will not have to inject code or change the return address.
- Describe briefly how you would change line 29 of the source file (only that line) to fix this vulnerability!

Problem 2 (1 point): Integer Overflow

- Exploit the integer overflow vulnerability!
- Describe briefly how you would fix this vulnerability in the source file!

Problem 3 (2 point): Format String Reading

- Exploit the format string vulnerability! Hints:
  - use a lot of `%d` to find out where things are on the stack,
  - the secret is on the heap, not the stack,
  - you will only need to read using the vulnerability.
- Describe briefly how you would change line 24 of the source file (only that line) to fix this vulnerability!

Problem 4 (1 points): Filenames and Symbolic Links

- Exploit the vulnerability! Hint: you can create a symbolic link by typing `ln –s targetfile linkfile`.
- Describe briefly how you would fix this vulnerability in the source file!

Problem 5 (2 point): Format String Writing

- Exploit the format string vulnerability by changing your "`authorization_level`"! Hint: use a lot of `%d` to find out where things are on the stack.
- Describe briefly how you would fix this vulnerability in the source file!

SSH

If you would like to login to the virtual machine using SSH,

- open Preferences in VirtualBox, and select Network / Host-only Networks
- click "Add new host-only network", select the new network, and click "Edit the selected host-only network"
- make sure that the IPv4 network mask is 255.255.255.0 and the IPv4 address is 192.168.56.1 (or any other address in that range except for 192.168.56.2, which is used by the virtual machine)
- select the virtual machine and click Setting, and select Network / Adapter 1
- enable Adapter 1, attach it to "Host-only Adapter", and select the host-only adapter that you have just created.

After this, you should be able to login to the virtual machine using SSH with the same suer once it is up and running.