CS 378 - Spring 2016	Assignment 1 - Capture the Flag
System Security (Freshman Research Initiative)	Due: Jan 27^{th} at 11:59pm

Preamble

Step 1: Read and understand the Universitys rules on plagiarism:
`http://deanofstudents.utexas.edu/sjs/acadint_plagiarism.php`

If you have any questions about academic dishonesty or plagiarism,
please post to the Piazza page (privately, if you wish).
`https://piazza.com/utexas/spring2016/cs378/home`

Step 2: Post a private note on Piazza to let us know if you have read
and understood the Universitys rules on plagiarism.

Assignment Objectives

To help you get acclimated with Linux, scripting, and problem solving, we have designed a capture-the-flag challenge. You may ask questions about the lab assignment on Piazza; however, please be careful to not post solutions or hints. If you're uncertain whether your question should be made public, send a private note through Piazza to the instructors.

Lab tasks

Task 1: Set up the Virtual Machine. The lab comes packaged as a Virtual Machine Disk (VMDK) file. You will need an application that supports virtualization, such as VMWare or VirtualBox, to play through the challenges. We recommend using VirtualBox since it is free and the challenge was built and tested in VirtualBox. There are several resources on the Internet to help you setup the Virtual Machine. Contact us if you have any issues with the setup.

Tip: Since passwords to each level are relatively long, you may soon become tired of typing. Unfortunately, copy/paste will not work in the VM. However, you can use the `sshpass` command. A minor quirk about `sshpass` is that you first have to attempt logging in using the regular `ssh` command (and failing, because of an incorrect password). Alternatively, you could try setting up the VM so that you can `ssh` from the host machine.

Tip: While playing, you should back up important files. Please note that if you do not create backups and you corrupt or delete your flag file, you might need to redownload and reinstall the virtual machine.

Task 2: Capture the Flag! To start, please use the credentials **user:**`level0` **pass:**`level0`. Your home directory will contain a flag or a hint. The flag is usually (but not always) named *flag*. Your goal is to find the random 128-bit (32 character) MD5 hash that we've hidden and use it to access the next level. You can `ssh` or `su` into the next level by using this hash as the password. For example, say *hypothetically* that the hash you found in `level0` was `75da1e6b17ae0fb3452baabdb5ccd448`. This hash is also the password for `level1`! Everytime you find a flag, you may use it to login to the next level. There are 10 levels and 10 corresponding users (level1, . . . , level10). Please keep track of your solutions, commands and scripts to each level and their respective flags.

Submission

You should submit a detailed lab report to describe what you have done and what you have observed, including screenshots and any code you may have written. Please write your lab reports in LaTeX. Lab reports must be submitted to Canvas in PDF format.

To earn extra credit, you can provide explanations, observations or workarounds to the challenges. We encourage you to investigate further and deeper. Good luck, have fun! This assignment is due Wednesday, January 27^{th} at 11:59pm.