Questions 1 and 2 cover SUID programs. While doing questions 1 and 2 you should NOT be root.

You must pay particular attention to which user you are when doing the parts of this project. Be sure you are the user you are instructed to be at each step of the project.

As bob: get a copy of `~djv/clogit.c` and compile it (gcc something.c -o binaryfile). Name the compiled version `clogit`. Don't forget to look at it to see what it does. Create a file called `datelog` to be mode 600 and change the `clogit` command to be SUID and executable by everyone (mode 4711).

Login as your account: run clogit.

1) Report: the last two lines in the datelog

Verify security: try doing the same thing by creating (as bob) a shell script that writes to the file using "echo" commands. (Don't be particular about the exact things you echo.) Make the shell script SUID.

Login as your account: run the shell script.

2) Report: what happens.

Examine the `login.defs` file on your machine.

If you want to enable time restrictions on logins, a variable needs to be set and a file needs to be modified.
3) Report the variable and the file name.

If a home directory for a user cannot be found when that user attempts to login, the user may or may not be allowed to complete the login 4) Report the name of the variable that controls this behavior

Make (and test) the following modifications to your `login.defs` file:
a) Log all su activity
b) Limit `su` to `root` to be from the wheel only. To test this, add `bob` to the wheel group (gid 10), but do not add your account, make sure `bob` can su and you cannot.

5) Report: the changes you made and the last line of your su log.

On `cheetah` examine the login history.

6) Report: Ignoring your account, who where the last 3 logins, to what accounts, what hours were they on and where did they login from.

Use iptables to block ssh into your machine from `panther` only. To test this, try to ssh into your machine from both panther and puma.

7) Report: The command you issued.

Clean up: flush all iptables entries.

On cheetah, examine `/usr/local/bin/iptables-rules.sh` to see cheetah's firewall rules.

8) Report: What rule allows established inbound connections (it differs slightly from the lecture notes).