CPSC 525/625: Principles of Computer Security (F21)
Instructor: Ryan Henry <ryan.henry@ucalgary.ca>

Worksheet 0x05

Unix permissions

```
ryan@mocha:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 59640 Mar 22 2019 /usr/bin/passwd
ryan@mocha:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 11928 Jan 22 10:41 /etc/passwd
ryan@mocha:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 22121 Jan 27 14:59 /etc/shadow
ryan@mocha:~$ ls -l /usr/bin/sudo
-rwsr-xr-x 1 root root 149080 Oct 10 12:32 /usr/bin/sudo
ryan@mocha:~$ ls -l /bin/su
-rwsr-xr-x 1 root root 44664 Mar 22 2019 /bin/su
ryan@mocha:~$ ls -l /etc/sudoers
-r--r----- 1 root root 755 Jan 17 2018 /etc/sudoers
```

(a) The above output is copy-pasted from a real session on mocha. Which the following files do you think *you* have permissions to read? How about to write? And to execute?

(b) Come up with the best justification you can think of for why each of these files has the permissions that it does.

(c) Join a breakout room with 2 or 3 other students. Including yourself, who's in your breakout room?:

1.

2.

3.

4.

As a group, try to think of any potential security vulnerabilities that might be introduced by setting permissions on these files in this way? **I'm not looking for concrete attacks; rather I'm curious where you would start *looking* for vulnerabilities in light of the information contained above.**

(d) Designate a member of your breakout group to do the following: By the end of today (whatever day we get to this in lecture, that is), post a followup to my Piazza posting that includes your group's responses to prompt 2(c). [And please comment on/critique/discuss the ideas given by other groups by replying to their followups!]