Lab 2 Report – Exploring Unix Logs  
CS3670

**Your Name Here**

1. With respect to the log file named /var/log/messages, what permissions are given to regular users?

TBD

1. In /var/log/secure what wording is used to indicate a failed login attempt?

TBD

1. Referring to Item #2 above, describe a real-world situation where this information would be very useful.

TBD

1. In /var/log/secure what wording is used to indicate that you entered a password as the username?

TBD

1. In /var/log/secure what wording is used to indicate that you raised your privileges with the su command?

TBD

1. In your own words, describe the functionality that is provided by the –t option of the last command.

TBD

1. What rule in the syslog configuration file will match the record you sent with logger (i.e., a facility of “user” and a priority of “info”)?

TBD

1. What rule did you add to put debug messages (and only debug messages) into /var/log/mydebug?

TBD

1. How did you test the new debug rule?

TBD

1. What command(s) did you use to change the permissions on logger so that only the root user and the root group can execute it?

TBD

1. Looking at all the active rules in rsyslog.conf, what action(s) would rsyslog take if a record were received from the kernel with a priority of emerg?

TBD

1. Looking at all the active rules in rsyslog.conf, what action(s) would rsyslog take if a record were received from a mail facility with a priority of notice?

TBD

1. Looking at all the active rules in rsyslog.conf, what action(s) would rsyslog take if a record were received from a local6 facility with a priority of err?

TBD

1. Describe any extra experimentation or exploration you performed.

TBD

1. What did you learn from this lab assignment?

TBD

1. How could this assignment be improved?

TBD