To limit logins using the PAM module, I first enabled the /etc/security/access.conf on all machines by typing in the command: account required pam\_access.so to the following files:

* Redhat
  + /etc/pam.d/system-auth
  + /etc/pam.d/password-auth
* Debian
  + /etc/pam.d/login
  + /etc/pam.d/sshd

Then I edited the /etc/security/access.conf according to specific conditions in the assignment:

* +:root loch1722 mscott dschrute : ALL 🡪 This allowed for these users to access the machine and was applied to all machines
* +: (All dunder Mifflin usernames) : ALL 🡪 This allowed for all the users at Dunder Mifflin to access machine E
* +:pbeesly abernard kkapoor : ALL 🡪 This allowed for these users to access machines C and D
* +:(accounting) : ALL 🡪 This allowed for users in the accounting group to access machine F
* -:ALL:ALL 🡪 This was put at the end of every access.conf file as to not allow access to anyone else but specified above

To set the password policy, I went into /etc/security/pwquality.conf and edited the file to add the policy:

* Minlen = 10 🡪 Min of 10 characters
* Dcredit = -2 🡪 Must be at least 2 digits
* Ucredit = -2 🡪 Must be at least 2 uppercase letters
* Ocredit = -1 🡪 Must be at least 1 non-alphanumeric character
* Lcredit = 0 🡪 Lowercase letters do not carry any credit

This is how I set up everything so specific users can login to specific machines and there is a password policy on every machine.

Time spent on assignment:

6 hours.