Andrew Rutherford
CSCI 4113
Lab 5

1. Password Protection Policy Proposal:

   a. Effective immediately, all server passwords must conform to the guidelines and requirements as deployed on the *PAM* module on all servers. They are summarized in the following points:
   b. Passwords may not contain commonly used dictionary based words. All new passwords will be subject to a search against a dictionary. This is to prevent passwords from being brute forced.
   c. Users must not use the same password for various accounts within the Dunder Mifflin network.
   d. Users must not use the same password for any Dunder Mifflin server that is used for any non-Dunder Mifflin activity.
   e. Users must use a password that contains at least 2 uppercase letters.
   f. Users must use a password that contains at least 2 numbers.
   g. Users must use a password that contains at least 1 non-alphanumeric character.
   h. Users will be required to change their password at least once every six months.
   i. User passwords should never be shared with anyone. This includes other employees, non-employees, your supervisor, or even the system administrator.
   j. If you have suspicion that your password may be compromised, you are required to either change your password immediately, or let the systems administrator know immediately.
   k. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

   Email to Jim Halpert:

   Jim,
   After a lengthy discussion with Michael Scott, it was determined that you will not be granted with full administrative access on all servers at this time. This decision was based on the choice and strength (or lack thereof) of server passwords being used. A new password enforcement policy is in the process of being completed. After it is deployed, and a mandatory password reset of all employees is accomplished, we will reassess who will require administrative access to the Dunder Mifflin server network.
   Thank You.

2. On machine C:
   Visudo
   mpalmer ALL=NOPASSWD:/etc/init.d/vsftpd restart,NOPASSWD:/bin/chown

chgrp –R mpalmer /var/ftp
chmod 775 –R /var/ftp

3. On machine B:
   Visudo
   pbeesly ALL=/etc/init.d/httpd restart
   kkapoor ALL=/etc/init.d/httpd restart
   abernard ALL=/etc/init.d/httpd restart

   groupadd web
   usermod –G web pbeesly
   usermod –G web kkapoor
   usermod –G web abernard
   chmod 775 /var/www/*
   chgrp –R web /var/www/
4. On machines A, C, D, and E:
   vi /etc/profile
   Change umask to 007 so user can RWX, group can RWX, others can do nothing
5.
6. On all machines:
   visudo
   mscott ALL=(ALL:ALL) ALL
   dschrute ALL=(ALL:ALL) ALL
   arutherford ALL=(ALL:ALL) ALL
7.
8. On all machines:
   vi /etc/pam.d/system-auth
   password requisite pam_pwquality.so try_first_pass local_users_only retry=5
   authtok_type= minlen=10 ucredit=-2 dcredit=-2 ocredit=-1