Lab4: Adding Users and Groups

1. **Michael Scott, Dwight Schrute, Jim Halpert, and your own personal account must be able to execute all commands as root through sudo on Machines A, B, C, D, and E.**
    a. useradd mscott dschrute jhalpert rowe7280 to all machines
    b. type “visudo”
    c. add lines to end of sudoers file
        i. mscott ALL=ALL
        ii. deschrute ALL=ALL
        iii. jhalpert ALL=ALL
        iv. rowe7280 ALL=ALL
2. **Meredith Palmer must be able to run /etc/init.d/vsftpd restart (not start/stop, just restart) on Machine C and run the chown command without typing her password. She must be able to modify all files under /var/ftp.**
    a. “useradd mpalmer” to machine C
    b. “visudo”
    c. add line to sudoers
        i. mpalmer ALL=NOPASSWD:/etc/init.d/vsftpd restart,NOPASSWD:/bin/chown
    d. “chgrp -R mpalmer /var/ftp”
    e. “chmod 775 -R /var/ftp”

3. **Pam Beesly, Kelly Kapoor, and Andy Bernand should be allowed to restart the httpd daemon on Machine B through sudo. They should be prompted for their password when attempting to do so.**
    a. “visudo”
    b. “useradd pbeesly kkapoor abernand”
    c. “visudo”
    d. add lines to sudoers
        i. pbeesly ALL=/etc/init.d/httpd restart
        ii. kkapoor ALL=/etc/init.d/httpd restart
        iii. abernand ALL=/etc/init.d/httpd restart
4. **Pam Beesly, Kelly Kapoor, and Andy Bernand should be able to modify all files under /var/www/html on Machine B without affecting the ability of the user apache to read them.**
    a. “useradd” all users to machine B
    b. “groupadd www” => group for Pam, Kelly, and Andy
    c. “useradd -a -G www pbeesly” => add all three to secondary group www
    d. “chmod 775 /var/www/*” => change permissions on www directory to meet specifications
    e. “chgrp -R www /var/www/” => put the www group in charge of all files under www/
5. **A directory under /var/www/html called employees should be created on Machine B, with one folder inside it for each employee,**

/var/www/html/employees/pbeesly for example. Only that employee, Pam Beesly, Kelly Kapoor, and Andy Bernand can create additional files and folders within it. The user apache should be able to read all files and folders.

a. “mkdir /var/www/html/employees”
b. “chgrp -R www /var/www/html/employees” => make sure Pam, Andy, and Kelly can access other user’s home directories
c. “chown user /home/user” => make sure each user owns their own home directory
d. “chmod -R 775 employees”

6. **The home directories on Machine E under /home should have the appropriate owners assigned to them, with the permissions such that the owner and the group have the ability to read and write all files, but everybody else is denied.**
    a. “useradd” missing users
    b. “rm -rf /home/user” users that are not listed in writeup
    c. “chown user userdirectory/” => change ownership of home directories to specific user
    d. “chgrp primaryusergroup userdirectory/” => changer group ownership of home directories to primary user group
7. **At least 3 secondary groups must be created, one for managers, the sales team, and the accounting team, using the naming scheme of your choice**

and the appropriate users should be added to those groups. You'll likely need to create a few additional groups on top of the minimal to meet the other requirements of this lab.

a. "groupadd" necessary secondary groups according to job list in lab writeup
b. "usermod -a -G usergroup user" => add users to their particular working groups

8. **A shared directory on the file server should be created for each secondary group you created under /home, and permissions should be such that only the group can read, write, and modify files. New files and folders created under the shared directories should retain the group ID of the parent directory, not that of the user that creates them.**
    a. "mkdir /home/group" => make directories for all new user groups
    b. "chgrp group groupdirectory/" => make all groups owners of their own directories
    c. "chmod 2770 groupdirectory/" => change permissions of directory and make sure new files created will inherit proper group name
9. **The umask is set on all machines, except for B, so that when new files are created the owner can read, write, and execute, the group can read and write, and everyone else has no access.**
    a. On all machines
        i. "vi /etc/profile" => edit where default umask is set
        ii. Change umask from 002 to 017 according to task specifications

10. **Please submit a copy of your password policy document that at a minimal describes: good practices for passwords, brief educational materials on how to pick a good password, and the specific complexity and expiration policy you decided for Dunder Mifflin. Please also submit a brief explanation as to why you selected your specific policy. Your password complexity and expiration policy is enabled for all users, and on all servers.**
    a. “cd /etc/pam.d/”
    b. “rm system-auth” => removes symbolic link
    c. “cp -a system-auth-ac system-auth-local”
    d. “ln -s system-auth-local system-auth”
    e. edit system-auth file and add lines to pam-cracklib.so
        i. minlen=12 => make sure there are minimum of 12 chars in the passwd
        ii. minclass=4 => make sure the password has all 4 character classes
    f. edit /etc/default/useradd and /etc/login.defs to change the minimum days the password needs to change to 30 days
    g. edit all users in /etc/shadow so that the 30 day policy takes effect
        i. in vi
            1. “:beginninglinenumber,&s/99999/30/”

11. Password Policy Explanation:

    a. I chose the policy I did because I think that it allows for the most secure possible password for each user.

12. **The UIDs / GIDs for the users and groups you create must be consistent across all servers.**
    a. Checkmate!