Lab 4: Access Controls

1. **Dunder Mifflin Password Policy:**

Email to Jim

To: Jim Halpert

From: Elijah Berumen

Subject: Administrative Server Access Request

Hi Jim,

I'm reaching out to you in regards to your request for administrative server access. Unfortunately at this time we are unable to fulfill this request due to a recently implemented password protection policy at Dunder Mifflin. The password protection stipulations are as follows:

- Passwords must not be shared with anyone, including supervisors and coworkers.
- Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.
- Passwords may be stored only in "password managers" authorized by the organization.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Lastly we recommend creating a password that utilizes a unique combination of passphrases, upper/lower case, numbers, and symbols. Please avoid using common words and number combos such as "123" and refrain from using the company name. Thank you for your understanding.

Best,

Elijah Berumen

IT Systems Administrator

Dunder-Mifflin

2. Meredith Palmer on Machine C
    - a. Added the following line to etc/sudoers using visudo -f
        - i. Mpalmer ALL=NOPASSWD: /bin/systemctl restart vsftpd
    - b. Ran the following commands to change the group membership of /var/ftp/ and all of its contents (recursively with -R parameter) to the user’s owngroup, as well as change access permissions of /var/ftp/, respectively
        - i. Chgrp mpalmer /var/ftp/ -R
        - ii. Chmod 775 /var/ftp/ -R

3. Pam, Kelly, Andy on Machine B
    - a. We need to add a line to /etc/sudoers using visudo -f to edit, for each of the 3 users to be able to restart http daemon(aka: httpd)
        - i. pbeesly ALL= /bin/systemctl restart httpd
        - ii. kkapoor ALL= /bin/systemctl restart httpd
        - iii. abernard ALL= /bin/systemctl restart httpd
    - b. All 3 must be able to modify all files under /var/www/dundermifflin/ without affecting apache’s read ability as follows. We do this by making an additional group that won’t be either the user groups but a specific one for them. Lowercase -g parameter is for primary groups and we want secondary(G)
        - i. Groupadd dmiff
        - ii. Usermod -aG dmiff pbeesly
        - iii. Usermod -aG dmiff kkapoor
        - iv. Usermod -aG dmiff abernard
    - c. We change the permissions for /var/www/dundermifflin to allow modification by the users and then make sure we put the proper group ownership
        - i. Chmod 775 /var/www/dundermifflin/ -R
        - ii. Chgrp dmiff /var/www/dundermifflin/ -R
4. Default umask
    - a. We want 770 permissions so we set the default umask within /etc/profile to 007 to allow the Owner and Group to read, write, and execute and nothing for Others.

        i. We change this on machines A, C, D, and E

5. Using pam_access we explicitly allow root to ssh, as well as specified users to connect to the following machines as follows:

    First we add pam_access.so to /etc/pam.d/login

    Now we add the following to /etc/security/access.conf

    a. Machine A:
        i. + : root : ALL
        ii. + : dschrute : ALL
        iii. + : eberumen : ALL
        iv. + : mscott : ALL
        v. - : ALL : ALL
    b. Machine B:
        i. + : root : ALL
        ii. + : dschrute : ALL
        iii. + : eberumen : ALL
        iv. + : pbeesly : ALL
        v. + : kkapoor : ALL
        vi. + : abernard : ALL
        vii. + : mscott : ALL
        viii. - : ALL : ALL
    c. Machine C:
        i. + : root : ALL
        ii. + : dschrute : ALL
        iii. + : eberumen : ALL
        iv. + : mpalmer : ALL
        v. + : mscott : ALL
        vi. - : ALL : ALL
    d. Machine D:
        i. + : root : ALL
        ii. + : dschrute : ALL
        iii. + : eberumen : ALL
        iv. + : mscott : ALL
        v. - : ALL : ALL
    e. Machine E: All users(No entries)

6. Sudo access per machine
   a. Machine A
      i. Usermod -aG wheel dschrute
      ii. Usermod -aG wheel eberumen
   b. Machine B
      i. Usermod -aG wheel dschrute
      ii. Usermod -aG wheel eberumen
   c. Machine C
      i. Usermod -aG wheel dschrute
      ii. Usermod -aG wheel eberumen
   d. Machine D
      i. Usermod -aG wheel dschrute
      ii. Usermod -aG wheel eberumen
   e. Machine E
      i. Usermod -aG wheel dschrute
      ii. Usermod -aG wheel eberumen

7. Michael Scott server shutdown permission
   a. In /etc/sudoers in all machines we add the following line
      i. Mscott ALL= /sbin/poweroff, /sbin/halt

8. Password enforcement: 10 char long, 2 digits, 2 uppercase, and 1 non alphanumeric character
   a. Authconfig --passminlen=10 --update # This command is the same as editing pwquality.conf
   b. Dcredit = -2
   c. Ucredit = -2
   d. Ocredit = -1