CSCI4113
LAB4 Notes

Milan Formanek

February 28, 2019

1.

For Meredith to be able to run the systemctl restart vsftpd, the line
mpalmer ALL = NOPASSWD: /bin/systemctl restart vsftpd
is added to the file /etc/sudoers on Machine C. This will allow Meredith to run the sudo systemctl restart vsftpd command.

To allow Meredith to read and write /var/ftp we run the following commands. First we add mpalmer to the group ftp, then we own /var/ftp with the ftp group and finally we set the group to rwx on the folder.

```
[root@machinec ~]# usermod -a -G ftp mpalmer
[root@machinec ~]# chown -R :ftp /var/ftp
[root@machinec ~]# chmod -R 775 /var/ftp
```

2.

In order for Pam, Kelly and Andy to be able to restart the httpd deamon the following 2 lines are added to /etc/sudoers Machine B
User_Alias HTTPD = pbeesly, kkapoor, abernard
HTTPD ALL = NOPASSWD: /usr/sbin/apachectl restart
This will add Pam Kelly and Andy under the alias HTTPD to the sudoers white list.

```
[root@machineb ~]# chmod -R 757 /var/www/dundermifflin/
```

Setting the directory rwx for everyone allows for Pam, Kelly and Andy to access the /var/www/dundermifflin directory. Not the most secure but since everyone else will be locked out of logging into machine B, I think this is fine.

3.

To get the desired effect the default umask has to be set to 007. In order to do this the /etc/profile file is modified changing both umask lines to umask 007. This is done on

Machines A,C,D and E.

4.

To restrict user access we will first modify the /etc/ssh/sshd_config and file, by adding the line
UsePAM yes
Then we modify /etc/pam.d/system-auth and /etc/pam.d/password-auth by adding the line below to both files.
account required pam_access.so
This is done on Machines A-D. The final step is modifying the /etc/security/access.conf. This has to be done according to what users need access on the individual machines. For Machines A and D only users root, mformanek, dschrute, mscott need access. For Machine B it's root, mformanek, dschrute, mscott, pbeesly, kkapoor, abernard and for Machine C it's users root, mformanek, dschrute, mscott, mpalmer. This done by adding the following lines to the /etc/security/access.conf file.
+:[USERS_ALLOWED]:ALL
-:ALL:ALL

5.

Only the root, mformanek and dschrute accounts should be able to run all commands with sudo. To do this the allow people in wheel group to run all commands without password line has to be uncommented in /etc/sudoers file. After that the admin accounts have to be added to the wheel group using the commands below.

```
[root@machinea ~]# usermod -aG wheel mformanek
[root@machinea ~]# usermod -aG wheel dschrute
```

This has to be done for all Machines A-E.

6.

To allow user mscott to shutdown machines with at least 2 hour notice and cancel pending shutdowns the following lines are added to the /etc/sudoers on Machines A-E.
mscott ALL = NOPASSWD: /usr/sbin/shutdown -c
mscott ALL = NOPASSWD: /usr/sbin/shutdown +[2-9][0-9][0-9]*
mscott ALL = NOPASSWD: /usr/sbin/shutdown +[1-2][2-9][0-9]*
mscott ALL = NOPASSWD: /usr/sbin/shutdown +1[0-9][0-9][0-9]*

7.

To enforce the new password rules 2 files have to be modified on Machines A-E. First, in /etc/login.defs the line PASS_MIN_LEN has to be set to 10. Second in the file /etc/pam.d/system-auth the ucredit=-2 dcredit=-1 and minlen=10 parameters have to be added to the line password requisite pam_pwquality.so. This will set the requirement for all passwords to have 2 upper case letters, 2 digits and 1 special character of minimum length 10.

8. Email to Jim

Dear Jim,
I was unfortunately unable to grant you the right you requested due to our company policy. I would need written permission from M.Scott for you to gain admin rights. I have also reset you password, in the future please refrain from giving your password out to anyone (including me).

Regards,

DM Admin

M Formanek

P.S. I hope we are still on for the weekend bbq!

9. Purposed password policy

1.1 Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to Dunder Mifflin systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1.2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

1.3 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Dunder Mifflin facility, has access to the Dunder Mifflin network, or stores any nonpublic Dunder Mifflin information.

1.4 Policy

1.4.1 Password Creation

All user-level and system-level passwords must conform to the Password Construction Guidelines.
Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.
User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommend that some form of multi-factor authentication is used for any privileged accounts.

1.4.2 Password Change

Passwords should be changed only when there is reason to believe a password has been compromised.
Password cracking or guessing may be performed on a periodic or random basis by the Amin Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

1.4.3 Password Protection

Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Dunder Mifflin information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
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.

1.4.4 Password Construction Guidelines.

All passwords have to be at least 10 characters long and include at least 2 upper case letters, 2 numbers and 1 special character.

1.4.5 Multi-Factor Authentication

Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

1.5 Policy Compliance

1.5.1 Compliance Measurement

The Admin team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

1.5.2 Exceptions

Any exception to the policy must be approved in writing by the Admin Team and Manager in advance.

1.5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.