Summary:

You have created accounts and removed root access for all D-M employees. Now they have started complaining to you and Michael Scott that they can no longer do things that they once could. Michael Scott wants you to address these issues as soon as possible so that everyone calms down. You've received these emails so far:

From: Meredith Palmer
I can log in to my account on our ftp server, but I can no longer restart vsftp as I used to using the systemctl restart vsftpd thingy or modify any files under /var/ftp/. I have supplier lists I need to update today. Please fix it now!!!!

From: Pam Beesly
I just wanted to let you know that neither Kelly Kapoor, Andy Bernard, nor I can update the website anymore. We have some changes to make soon so it would be wonderful if we could be granted access to modify the files on our web server under /var/www/dundermifflin/ and restart httpd like we used to! Thank you very much for your help!

From: Dwight Schrute
Your clever attempt to gain control of our Linux systems has worked, but only temporarily. Michael Scott will confirm that I must be granted administrative access on all servers. Please grant me access today, or else.

From: Jim Halpert
Hey, quick question… can you grant me full administrative access on all of the servers? In the event that you are out of town I might need to access employee files or help them out with other things. My password is Dund3rMifflin if that makes it easier for you.

After checking with Michael Scott for permission to grant access you proceed with all except Jim Halpert. Include in your submission the email you sent to Jim denying his access request.

Also, since you've set up accounts for employees you've noticed that they are not taking password security as seriously as they should, especially after reading Jim's email. You have concluded that allowing all employees to log in to every server might be a bad idea.

Michael has agreed to let you enforce a password policy. He wants you to write a document defining the password requirements (feel free to use this template as a starting place). He has also agreed that you may limit server access to only those who need it, as long as he retains the ability to shut the servers down.

Prerequisites

Please complete last weeks reading and all prior labs before starting this lab. You are strongly advised to familiarize yourself with the commands involved on your own virtual machine before trying this on the production machines. The system uptime portion of your grade will suffer if you accidentally take down any production machine for an extended period of time.

Use of puppet for this lab is optional - if you decide to use it then you are required to submit your manifests. You may also use these community puppet modules to manage sudo and pam_access.

Submission Requirements

1. Please submit your lab notes as a pdf,including the password protection policy you propose for our D-M branch office, and your e-mail to Jim.
2. Meredith Palmer must be able to run systemctl restart vsftpd (not start/stop, just restart) on Machine C. She must be able to read and modify all files and folders under /var/ftp/.
3. Pam Beesly, Kelly Kapoor, and Andy Bernard must be allowed to restart the http daemon (not start/stop, just restart) on machine B through sudo, and modify all files under /var/www/dundermifflin/ without affecting the user apache's ability to read them.
4. The default umask must be adjusted on machines A, C, D, and E so that when new directories are created the owner can read, write, and execute, the group can read, write and execute, and others have no access. You need to do either the reading from the prior homework or some independent research to identify how to do this.
5. Access on each server should be restricted such that only users who need to are allowed to log in. The one exception is all users should be allowed to log in on machine E. Access restriction should be imposed using pam_access so that the /etc/passwd and /etc/shadow files stay consistent across all machines. IMPORTANT: You must explicitly allow root access via SSH. While it is certainly more secure to disallow direct access to root remotely, access to root must be maintained so we can grade your machines.

6. Sudo access to all commands, on all machines, should be granted to responsible users who have specifically requested it. This includes your own personal account.
7. Michael Scott should be allowed to shut all servers down with no less than 2 hours notice to other users (see man shutdown). He should be limited to shutting them down, not restarting. He should also be allowed to cancel a pending shutdown.
8. Password changes must be enforced on all servers such that pam ensures that new passwords are at least 10 characters long, and contain at least 2 digits, 2 uppercase, and 1 non alphanumeric character.