Password Auditing Lab

Yay! Password auditing. Know that this is very important for CyberPatriot and can easily get you points in the early rounds, and a few points in the later rounds. Also note that to complete this lab, you should know all the basic commands (e.g. ls, cd, nano, sudo, etc.), so if you do not know, please refer to the previous slides or ask the instructor for help. Remember that you need to remember all of these commands for competition in order to complete all the tasks quickly and not waste time on searching up commands!

Instructions: Follow the following steps to see if you know how to apply password auditing principles to a real Linux system.

1. Run `sudo apt install libpam-cracklib` to install the PAM cracklib module
   **Do not worry about what this command does yet, as we will be going over packages later*
2. Change the password for user `Kay` to `AS3cureP4ssw0rd`
3. Lock root password
4. Open `/etc/login.defs` and configure password min, max, and warning ages
5. Open `/etc/pam.d/common-auth` and setup the configuration
6. Open `/etc/pam.d/common-password` and setup the configuration
   **For these two file configurations you may refer back to the slides and copy+paste the configuration (however, you should try to somewhat remember the simpler file configurations, like for login.defs)*
   Test out how your configurations affect changing passwords. You may need to make new accounts to test password changes because of your login.defs config.
   - ***Change one option at a time. For example, test to see if you can make a password with only lowercase characters. Then, change the config to check for various characters.***
7. Manually change the password age for user `Jay` to maximum `30`, minimum `14`, and warn `7`
8. Edit the sudoers file (make sure you do it the correct way) and add a line (this is the tricky part) to disable password authentication for commands for the user `user`
   a. Hint (highlight text to see hint):
9. Exit your terminal session and start a new one, then run the command to open the sudoers file again
   a. Notice how it does not prompt you for a password (if you did the previous step right)
10. Remove the line you added to the sudoers file, save, and exit

Good job! You are done :)