You are asked to harden a CentOS machine for your company’s new CFO. This computer contains highly sensitive corporate forecasts and SEC-relevant information that may be accessed only by  the CFO himself, the CEO, and the company Treasurer.  You are not sure exactly how to do it, so it will take some research.

After some research on the web, you decide to do the following:

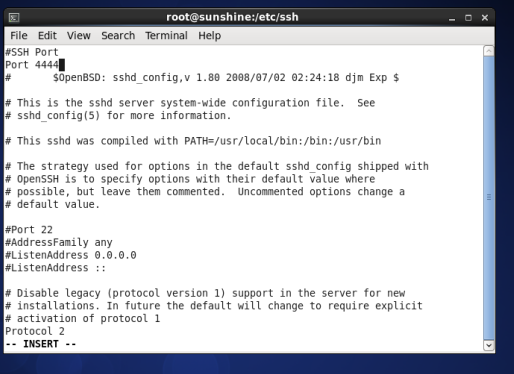
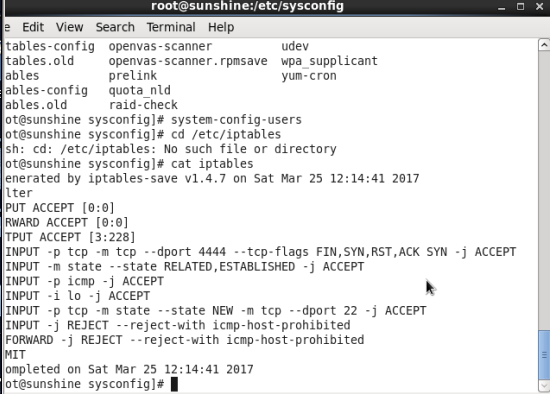
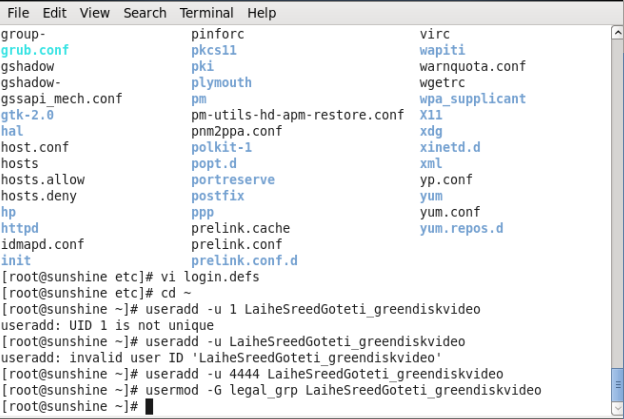
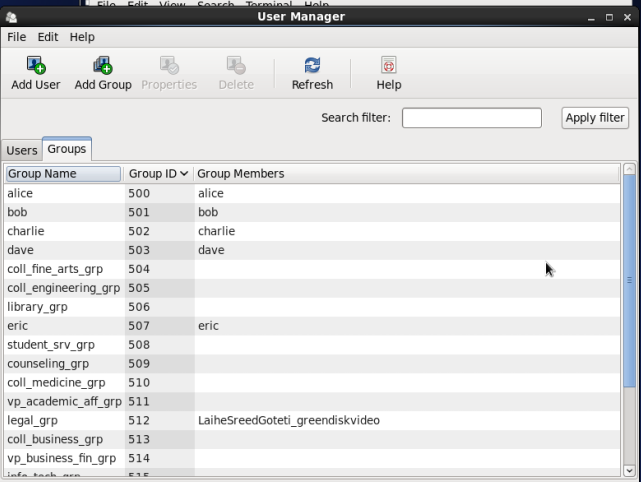
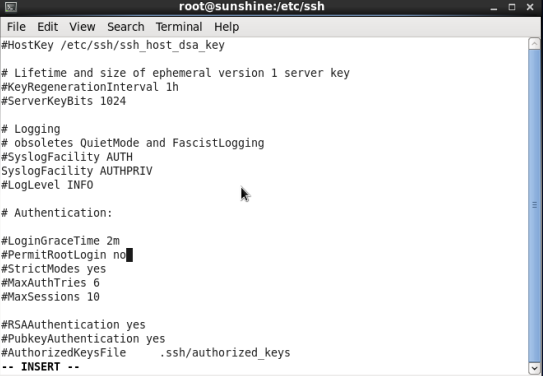
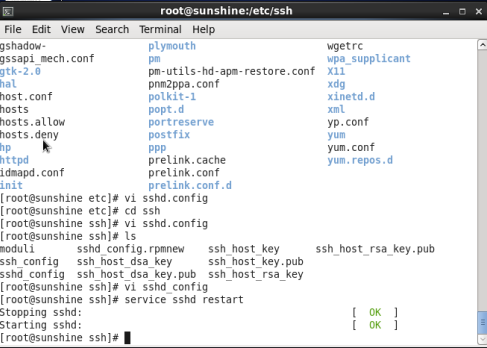
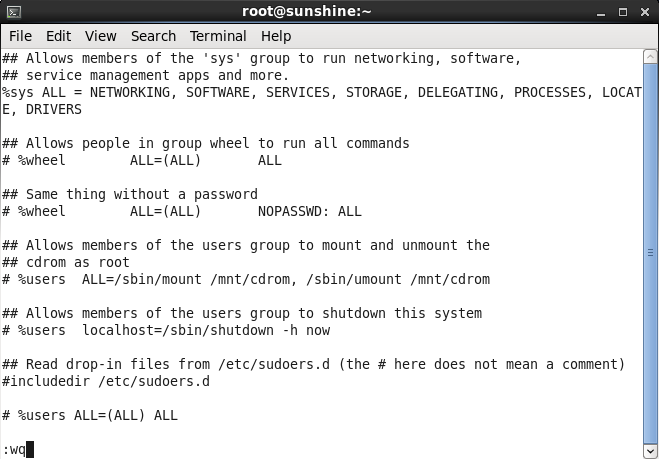
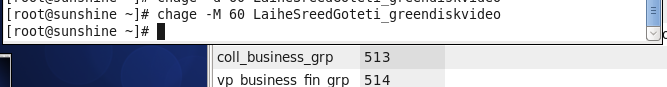
1. [Change the default port for the sshd daemon](https://wiki.centos.org/HowTos/Network/SecuringSSH) from port 22 to port 4444. This minor change will avoid most automated scans to break into the machine using SSH.
2. [Add the CFO’s login id](https://www.centos.org/docs/5/html/Deployment_Guide-en-US/s1-users-tools.html) (<teamfirstnames>\_<company>) to the legal\_grp group.
3. [Disable SSH logins as root](https://wiki.centos.org/HowTos/Network/SecuringSSH), forcing users to use the sudo command instead. This command allows users listed on the wheel group to elevate their privileges and execute commands as the root user.
4. [Change password aging parameters for the user](https://www.centos.org/docs/5/html/Deployment_Guide-en-US/s1-users-tools.html) (<teamfirstnames>\_<company>) to expire in 60 days.
5. [Change password history parameters](https://wiki.centos.org/HowTos/OS_Protection) to remember the last three passwords and password length to a minimum of eight characters.
6. [List the firewall rules](http://www.cyberciti.biz/faq/howto-display-linux-iptables-loaded-rules/) and keep a hard copy.

IN A MS WORD DOCUMENT, SUBMIT THE FOLLOWING:

Screenshots for activities 1-5 showing the exact procedure (the command strings and the file details) you used to implement these changes.  (10 points each).

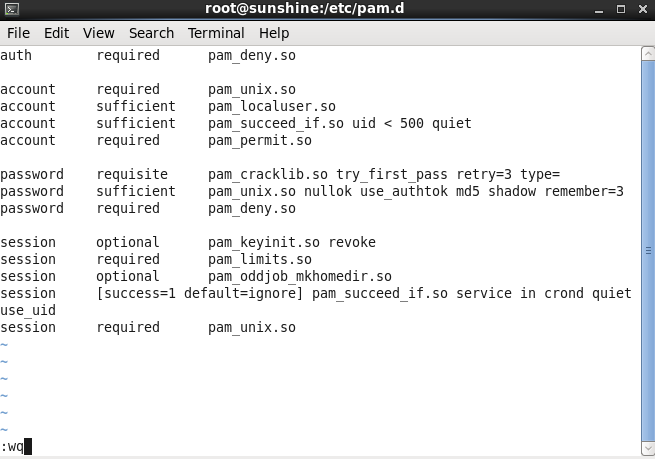
10 points extra credit if you include the firewall rules.

You may find the following configuration files and commands useful:

* sshd\_config
* login.defs
* group
* chage
* system-auth
* iptables
* 
* 
* 
* 
* 
* 
* 
* 

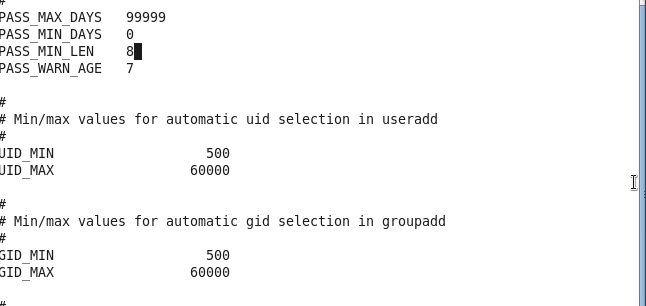
Cd /etc/pam.d

Vi system-auth

* 

cd /etc

Vi login.defs

* 
* 