- Please read all the handouts
- Modify your /etc/motd file to include a security message and verify it works
- If you are working in a corporate environment then check the security protocol with your datacenter technician as to whether there are security at datacenter, floor, cage, rack and server level
- List all packages in your Linux system and go through as many as you can. Identify which ones are not needed and before you delete them make sure you take a snapshot or backup of your server
- Run yum utility command to remove orphan packages from your server. This utility should be run as a cronjob to delete packages on a schedule and to meet the audit requirement
- Update your system by running the yum update command
- Look for services in your system that are not used and stop and disable them
- Build a new system by separating disk partition such as
    - /usr = 2G
    - /var = 2G
    - /home = 2G
    - / = rest of the space
- Disable Ctrl+Alt+Del function in your Linux machine and also from the GUI
- Make sure all your physical system console passwords do not have the default passwords. If they do then go ahead and change them
- Check all your Linux servers and make sure they are running either NTP or Chronyd and they are configured to synchronize with the correct master NTP server
- Try locking down cron for one of test user in your Linux machine for practice. Also if you are in corporate environment then consult with your manager to lock down cronjobs for everyone except root
- Try changing your SSH port to 1110 and see if it prevents you from logging in using port 22
- Try enforcing and disabling SELinux through /etc/selinux/config file
- Also for practice purpose turn ON or OFF a few SELinux booleans