1. Create a kickstart file (need to add some parameters)
    a. Kickstart meet the following objectives
    b. Set the root password to "password"
    c. Use http installation "url=http://server1.example.com/pub/rhel-7.0/dvd"
    d. Install base package group
    e. Create 200M /boot
    f. Create 200M swap
    g. Use the rest of the drive for /

2. Verify kickstart file syntax using the appropriate command.
3. Make your kickstart file accessible via http from either server1 or station1.
4. On Station1 download http://server1/pub/materials/shakespeare.txt using http.
5. Get a count of the number of times the word "the" is used in the file, direct your output to ~/count.info
6. Determine the number of lines in shakepeare.txt that contain with the word "Valentine", direct your output to ~/count.info while preserving the existing information in the file.
7. Create a one time task on station1 to determine who is logged in at current time plus 5 minutes, and direct the output to ~/logged-in.info
8. Create a recurring task on station1 to post the system time to ~/sys-time.info every 5 minutes. After 5 iterations, you can stop the task from running.
9. Configure your station1 to purge all temp files older than 2 days.
10. Display the nice levels of all running processes on station1, redirect the output to ~/nice.info
11. Determine the ACL's are on your home folder, direct the output to ~/acl.info
12. Create the folder /share on station1, set the default ACL on /shares so that student has rwx to everything in the folder
13. Determine the current status of selinux, direct the output to ~/selinux.info
14. Generate a list of all selinux booleans for ftp, direct the output to ~/selinux.info
15. Determine the selinux context of /var/www/html, direct the out output to ~/web-selinux.info
16. Configure station1 to use LDAP/TLS and kerberos for user authentication with a domain of example.com
    a. You will need to use the cert.pem file located at http://server1.example.com/pub/materials/
17. Configure station1 to automount /home/server1 when the ldap user guest01 logs in
18. Configure the 2nd hard drive on station 1 with two 250M partitions each with an XFS file system
    a. Mount the two partitions to /data1 and /data2
    b. Setup both partitions so that they are mounted at boot using the UUID
19. Create a 3rd partition on the second hard drive on station 1 that is 250M
    a. Configure the partition to be used as swap and mounted at boot
20. On each of the 3 remaining disks on station1, create a 200M partition.
    a. Use the 3 newly created partitions to create an Logical Volume named LVM01
    b. Format the volume with XFS and set it up to mount at boot using the UUID to /LVM-Data
    c. Review your logical volume details, redirect your output to ~/volume.info
21. Create two more 200M partitions on any drive with enough space on station1
22. Extend your current logical volume using both of the newly created partitions

23. Extend the filesystem to include all of the space in your logical volume.
24. Discover all of the NFS mounts on server1 from station1, redirect your results to ~/nfs.info
25. mount the second nfs share from server1 to /media on the station1
26. ensure the exports is available automatically when needed without putting the share in the fstab
27. mount the secure nfs share titles nfssecure to /mnt on station1, make the mount persistent across reboots
28. Discover all of the samba shares available on server1, direct your output to ~/samba.txt
29. setup the public share to automatically mount when needed without using fstab
30. mount the server1 share titled restricted to a folder called data on station 1, make the mount persistent across reboots
31. Setup grub to boot the system to a single user cli only mode
32. Use grub to change the root password
33. configure a firewall on station 1 to allow port 443, nfs, 8080, http, cifs shares and dns.