SUPRISE TEST!

=> Login to root user on server-a using redhat as the password

1) Create a file named redhat.txt
-> having the following content
"This is RedHat Enterprise Version 9"
2) Create a hardlink name /tmp/rhel-backup of /root/redhat.txt
-> Edit the hardlink, with following content
"This is the Latest Version"
3) Create a softlink of name /root/tmp-backup of /tmp
=> Move to student user on server-a
4) Create the follwing Directory: /home/student/Documents/project_plans
-> Create two empty files in the ~/Documents/project_plans directory:
season1_project_plan.pdf and season2_project_plan.pdf
-> Create a total of 12 files with names tv_seasonX_episodeY.ogg. Replace X with the
season number and Y with that season's episode, for two seasons of six episodes each.
-> move all files of tv_season1 to ~/Documents/project_plans/season1
-> move all files of tv_season2 to ~/Documents/project_plans/season1
-> Seems like you don't require season1_project_plan.pdf and season2_project_plan.pdf, please remove them
-> The name of project_plan dir needs to be chnaged with Upcoming_Project-plan
5) Configuring ssh for devops user on serverb
=> Login to Root user on Server-a
-> Configure public and private keys at default locations
-> Do not provide the passphrase
-> share the public key with devops user on serverb
-> Try connecting with devops on serverb, it should not prompt for password
6) Configuring ssh for student user on serverb
=> Generate ssh keys from root user on server-a, the file that stores the keys shall be named as /root/.ssh/student-key
-> Give RedHat as the passphrase to secure the keys
-> Share the public key with student user in server-b
-> Try connection to student@serverb , it shal prompt for passpharase
-> To avaoid shoulder surfing, pls generate the agent process for this newly generated key.
-> Change configuration on server-b such that no one can loginto it's root user account

Perform below questions from root user on servera

7)Managing users and Groups
-> Add a group named managers.
-> Add a user alice who belongs to managers as a secondary group.
-> Add a user vince also belongs to managers as a secondary group.
-> Add a user susan who does not have access to an interactive shell on system and who not a member of managers.
-> The users alice, vince, susan has password " sestiver "
8) Modifying user and group features
-> Alice primary group should be wheel
-> Groupid of managers should be 6060

-> All the members of managers group should be able to run any command as sudo, without requring the password
9) Working on the password policies
-> Configure the password policy for alice, such that:
-> she has to change the password every 30days.
-> she is warned 3 days before password expiry
-> Her accound expires after 120 days of creation
-> Configure Global password policies such that
-> All newly added users cannot change password of 3 days.
-> All newly added users must change their password every 15 days
-> All newly added users should be warned 5 days before their password expires
-> Confirm the above changes by adding natasha user
10) Output Redirection
-> Save a time stamp for later reference at /tmp/saved-timestamp
-> In the same file add number of days passed in 2023 after the following line "The Number of days passed in 2023 are".
11) Managing File Permissions
-> Create a directory called /home/Managers.
-> Change the group ownership of /home/Managers to managers group that you previously created.
-> Set permission such that user owner and group has the full access on the directory but others does not have any access.
-> Any files created in the future inside /home/Managers should by default get group ownership of managers group.
-> Verify the same by creating files in /home/Managers by vince(is member of managers) and student(not a member)
- Configure the umask for user alice such that:
- Any files created by alice should have permission set to "r--r--r--"
- Any Directories created by alice should have permission set to "r-xr-xr-x"
12) Process
-> Find out load avg on your CPU.
-> Find out number of CPUs.
13) Service Managment
-> Stop and Disable your firewalld.service
-> Verify by service status
14) Configuring rsyslog
-> Configure rsyslog on servera to log all messages with the debug priority, or higher, for any service into the new /var/log/messages-debug log file by adding the rsyslog configuration file /etc/rsyslog.d/debug.conf.
15) Network Time Protocol
-> Make sure servera uses 'classroom.example.com' as the NTP server