Lab

1. Using the useradd command, add accounts for the following users in your system: user1, user2, user3, user4, user5, user6 and user7. Remember to give each user a password.
2. Using the groupadd command, add the following groups to your system.

Group	GID
sales	10000
hr	10001
web	10002

Why should you set GID in this manner instead of allowing the system to set the GID by default?

3. Using the usermod command to add user1 and user2 to the sales secondary group, user3 and user4 to the hr secondary group. User5 and user6 to web secondary group. And add user7 to all secondary groups
4. Login as each user and use id command to verify that they are in the appropriate groups. How else might you verify this information?
5. Create a directory called /depts with a sales, hr, and web directory within the /depts directory.
6. Using the chgrp command, set the group ownership of each directory to the group with the matching name
7. Set the permissions on the /depts directory to 755, and each subdirectory to 770
8. Set the set-gid bit on each departmental directory
9. Use the su command to switch to the user2 account and attempt the following commands:
   touch /depts/sales/user2.txt
   touch /depts/hr/ user2.txt
   touch /depts/web/ user2.txt

   Which of these commands succeeded and which failed? What is the group ownership of the files that were created?
10. Configure sudoers file to allow user3 and user4 to use /bin/mount and /bin/umount commands, while allowing user5 only to use fdisk command.
11. Login by user3 and try to unmount /boot.
12. Login by user4 and remount /boot. Also try to view the partition table using fdisk.
13. Create a directory with permissions rwxrwx---, grant a second group (sales) r-x permissions
14. create a file on that directory and grant read and write to a second group (sales)
15. set the the owning group as the owning group of any newly created file in that directory.
16. Grand your colleagues a collective directory called /opt/research, where they can store generated research results. Only members of group profs and grads should be able to create new files in the directory, and new file should have the following properties:
    - the directory should be owned by root
    - new files should be group owned by group grads

- group profs should automatically have read/write access to new files
- group interns should automatically have read only access to new files
- other users should not be able to access the directory and its contents at all.

1. Change your default SELinux mode to permissive and reboot.
2. After reboot, verify the system is in permissive mode.
3. Change the default SELinux mode to enforcing.
4. Change the current SELinux mode to enforcing.
5. Copy /etc/resolv.conf file to root's home directory.
6. Observe the SELinux context of the intial /etc/resolv.conf
7. Move resolv.conf from root's home directory to /etc/resolv.conf
8. Observe the SELinux of the newly copied /etc/resolv.conf
9. Restore the SELinux context of the newly positioned /etc/resolv.conf
10. Observe the SELinux context of the restored /etc/resolv.conf
11. Configure OpenSSH to allow pulic key-based login credentials
12. Create an SSH key-pair
13. Configure to login without the need of a password.
14. Configure SSH to prevent root logins.
15. Configure logrotate default setting to compress log files when they are rotated.

Bonus

Your boss thinks it’s a great idea to have one central logging server. Satisfy his requirements ☺

Hint:

Set up rsyslogd on the "logging server" machine to accept logging messages from other machines.

On the your "workstation", set up rsyslogd to send messages to the "logging server

Test the new setup by using the logger command on the "workstation" to generate a log message

Does the message appear in the "logging server's" /var/log/messages file?

Why does this message also appear in the "workstation's" /var/log/messages file?

How could you have the message only appear in the "logging server's" files?