Exercise 23: Securing your system - Part 1

I. Prepare the environment

II. Perform security administration tasks

1. Login to the CentOS server with student
2. List all the files that is set with SUID and/or SGID and save the output to a file named sug_base.
3. Create a file named danger and set the SUID to that file.
4. Re-do the step 1 and save the output to file named sug_check. Compare the two files to specify the different.
5. Display the resource limits of user student
6. Change the file size limit to 4096 and re-display the resource limits to verify
7. Display all the users that is currently login to the system, and list the current command of the users also.
8. Display the history of log in and out actions of users in the system.
9. Using switch user (su) utility to run the fdisk -l command with root privileges.
10. Configure the sudo utility to allow user student1 to run the fdisk -l command and can view the /var/log/messages with tail command.

Exercise Instructions

I. **Prepare the environment**

II. **Perform security administration tasks**

1. Login to the CentOS server with student
2. List all the files that is set with SUID and/or SGID and save the output to a file named sug_base.
   ```
   $ find / -perm /6000 -type f >sug_base
   ```

3. Create a file named danger and set the SUID to that file.
   ```
   $ touch danger
   $ chmod u+s danger
   ```

4. Re-do the step 1 and save the output to file named sug_check. Compare the two files to specify the different.
   ```
   $ find / -perm /6000 -type f >sug_check
   $ diff sug_base sug_check
   ```

5. Display the resource limits of user student
   ```
   $ ulimit -a
   ```

6. Change the file size limit to 4096 and re-display the resource limits to verify
   ```
   $ ulimit -f 4096
   $ ulimit -a
   ```

7. Display all the users that is currently login to the system, and list the current command of the users also.
   ```
   $ w
   ```

8. Display the history of log in and out actions of users in the system.
   ```
   $ last
   ```

9. Using switch user (su) utility to run the fdisk -l command with root privileges.
   ```
   $ su – root -c “fdisk -l”
   <input 123456 for root password>
   ```

10. Configure the sudo utility to allow user student1 to run the fdisk -l command and can view the /var/log/messages with tail command.
    ```
    $ sudo visudo
    <add the following line>
    student1 ALL=(ALL)  /sbin/fdisk -l, /bin/tail /var/log/messages
    ```