**21CY682 – Secure Coding lab - I**

**Assignment Topic: Users and Groups**

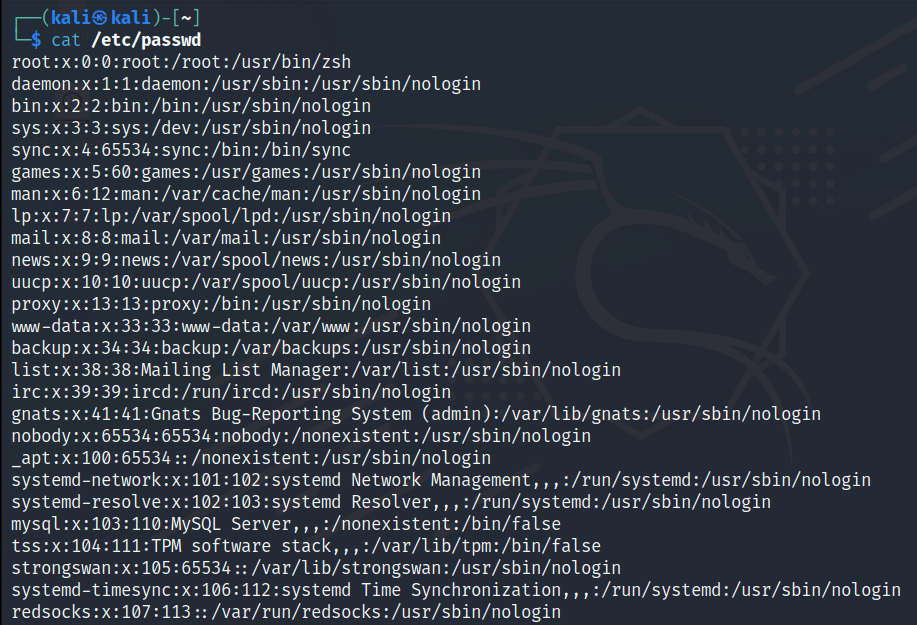
**Register Number: CYS22005**

**Date: 23/10/2022**

**Name: B.Shebu**

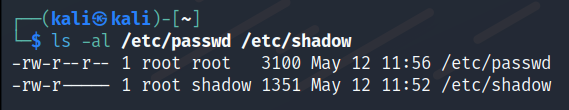
**PROCEDURE -**

**1. /etc/passwd**



The /etc/passwd file contains information about what users are present in the system

**2. ls –al /etc/passwd /etc/shadow**

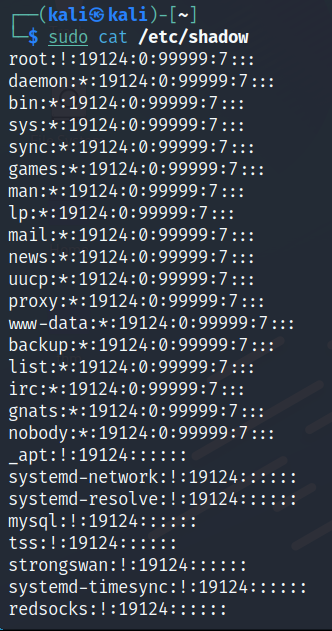


Now by using ls –al command we can see that both the files are owned by root and we have read permissions to only the passwd file.

The passwd file contains the user information, user’s home directory & also the default shell used by the user. Whereas the shadow file contains the value of x in the passwdfile which is the password hash of the user account.

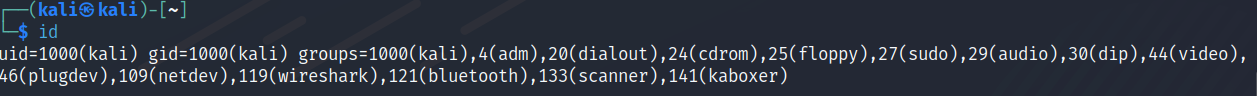
**3. sudo cat /etc/shadow**

As a normal user we cant cat the contents of the shadow files since it is owned by root for security reasons. So we need to use the sudo command to view the contents



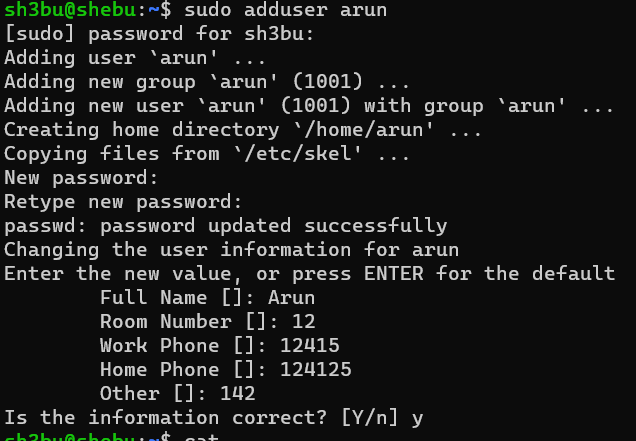
**4. id**

The id command show the userid, groupid and what groups the current user is a part of .



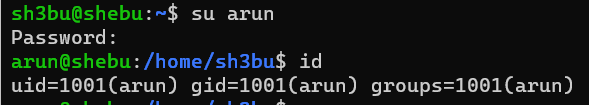
**5.sudo adduser <username>**

We use the adduser command to create a new user I a linux system. While running this command it will ask for the username, password, default shell to use etc..,

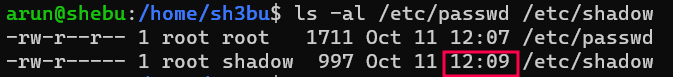


**6. su <user>**

When we need to switch between one user to another we need to use the su command.



**7. List the permissions of shadow file**



Since a new user is created , there was a change made in the shadow file. We can see that the file has been modified by noting the time .

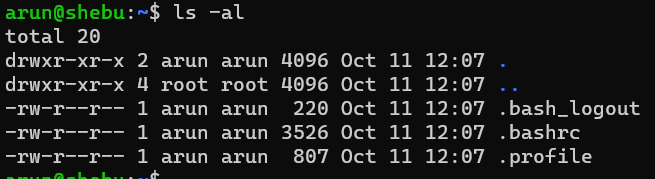
**8. cat /etc/group**

This file shows what users are a part of a particular group.. We just need to add a line in that file to add a user to that particular desired group



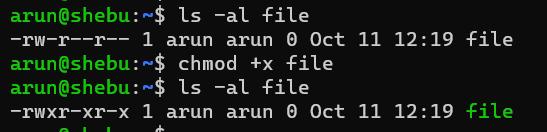
**9. Access control & permissions**

Each file has read,write & execute permissions which is denoted by rwx.



**10 . Change permissions**

We can use the chmod command to add or remove permissions of a file. Below we can see that after giving execute permissons to the file, now we can execute the file since we have enough permissions allocated.



**11. Permission on directories**

Similar to giving permissions to file , we can also give permissions to directories.

R- list contents of a folder

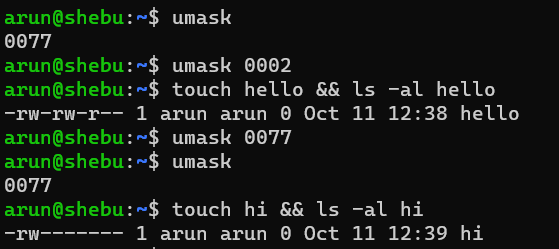
W- Create files/folders in a folder.

X - Enter a folder.



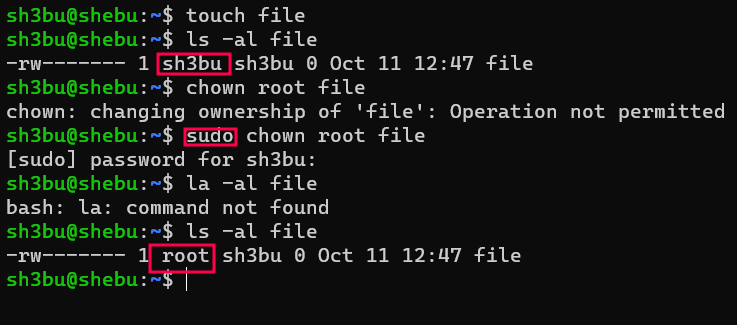
**12. Default Permissions**

By default the OS assigns a set of permissions, in order to change it we need to use the umask command followed by the value for permissions.The next time when a user creates a file, it gets created with the modified permission.



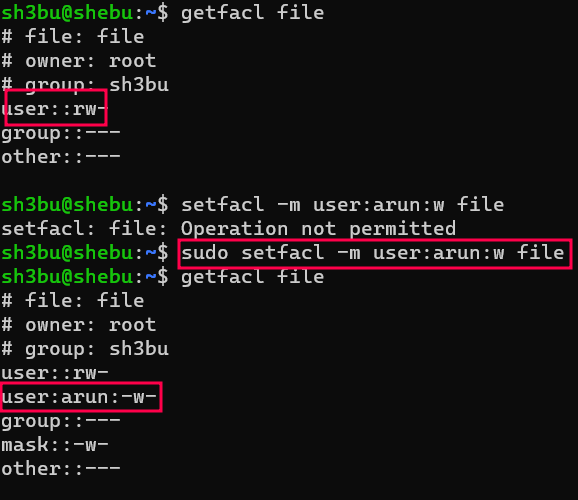
**13. Change ownership**

We can change the ownership of the file using the chown command followed by the name of the user to which the ownership of the file has to be changed.



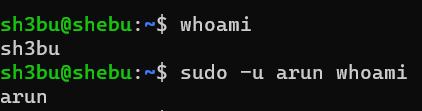
**14. Full Access control list**

Getfacl is a command used to display the name,owner,group and ACL of a file.



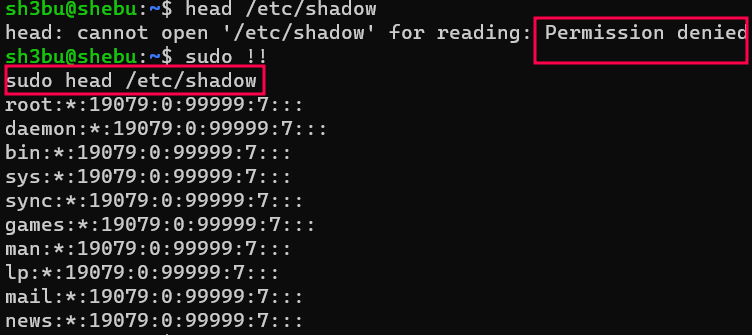
**15. sudo ( run command as another user)**

Some commands like sudo need elevated privileges to be run as normal user. So in this case we use the sudo command.



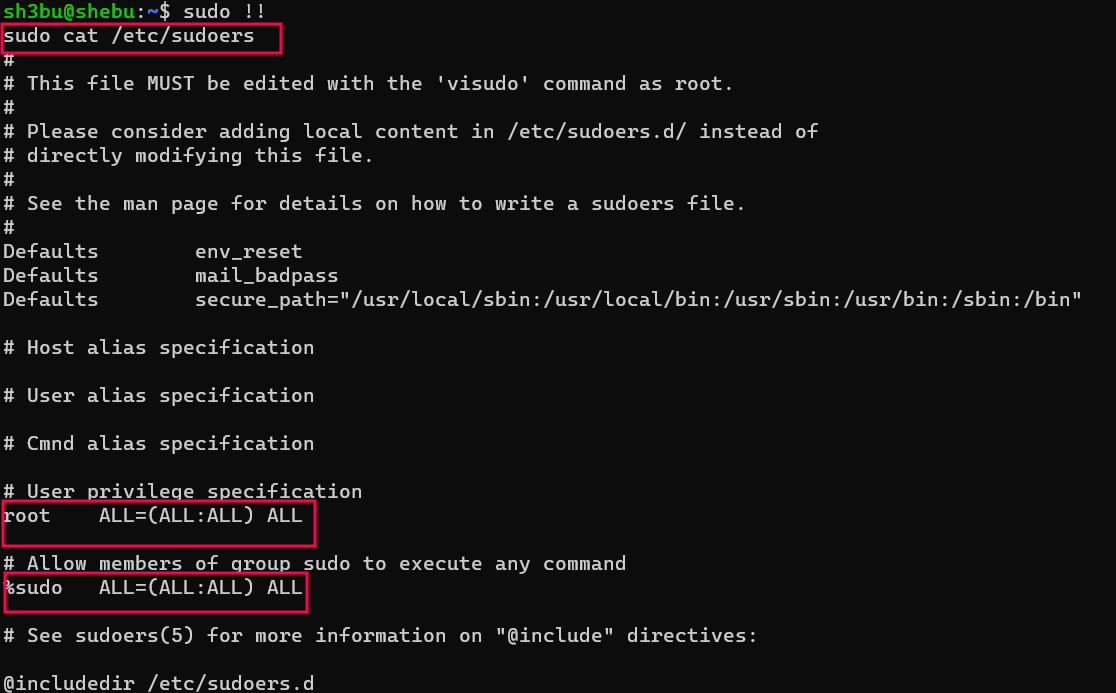
**17.Need for super user privileges**

Some files require sudo privileges (ie) running with userid 0 to read the file. An example of this is /etc/shadow file since it contains sensitive information like password hash of a user.



**18. sudo configuration file**

The sudo configuration file is located at /etc/sudoers .On listing the sudoers file we can see that the root account can run any command with sudo permissions.



Since the user sh3bu is added as a part of sudo group in the /etc/groups file, we can run any command which requires elevated privileges using sudo command.

