Let's create a new user and then setup some security.

New User

```
# login first
mkdfideloper
# Create password
# Skip extra field
# Set Y to save the new user

# Become new user fideloper
sudo su fideloper

# Head to home directory
cd ~/
# See the file path
pwd # /home/ubuntu
```

Setup SSH Key Authentication

We can re-use the SSH key we created to allow us to log in as user root.

On our Mac, we can get the public key into our clipboard again:

```
# On our host (Macintosh):
cat ~/.ssh/id_sfh_start.pub | pbcopy
```

Then over in the server, add that public key to user fideloper's authorized_keys file:

```
# Logged in as user fideloper
cd ~
mkdir .ssh
vim .ssh/authorized_keys
# Paste in the public key
```

Disallow Root Login

First, we want user fideloper to be able to use sudo commands, so we don't need the root user to perform administrative tasks.

Sudo user

We can do this easily in Ubuntu by adding the user fideloper to the group sudo or admin (More explanation on that within the video).

```
# Append (-a) secondary group (-G) "admin" to user "fideloper"
usermod -aG admin fideloper
```

Then log out, and log back in as user fideloper and you'll be able to use sudocommands.

Next, let's secure our server further and disallow root login.

Configure SSH

Now that user fideloper can do administrative tasks (things requiring super user access), let's edit the SSH daemon configuration to change this.

We'll do two things:

Disallow password based authentication

Disallow root user login

Do to that, we update the file /etc/ssh/sshd_config and change the following:

```
# Disallow root login over ssh
PermitRootLogin no

# Disallow password authentication
PasswordAuthentication no
```

Then restart the SSH daemon:

```
sudo service ssh restart
```

And you're all set!

reference: https://serversforhackers.com/c/creating-users-and-ssh-security