**Skill 4**

**Solution Dt 22-08-2024**

**Perform the below to Set Up Key-Based Authentication for Secure SSH Access**

1. Generating SSH Key Pairs

2. Copying the Public Key to the Remote Server

3. Manually Adding the Public Key (Alternative Method)

4. Configure the SSH Server for Key-Based Authentication

5. Restart the SSH Service

6. Disable Password Authentication

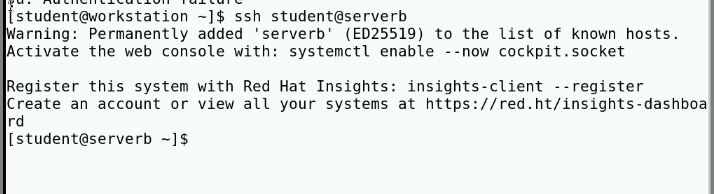
7. Verifying Key-Based SSH Access

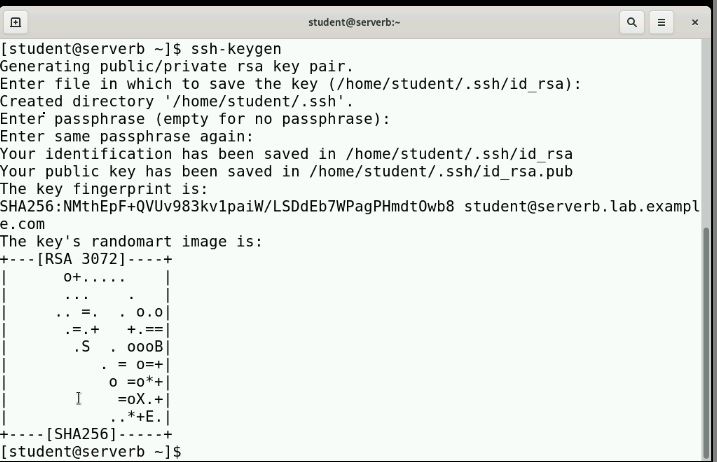
8. Testing with SSH Agent

**Step wise Explanation:**

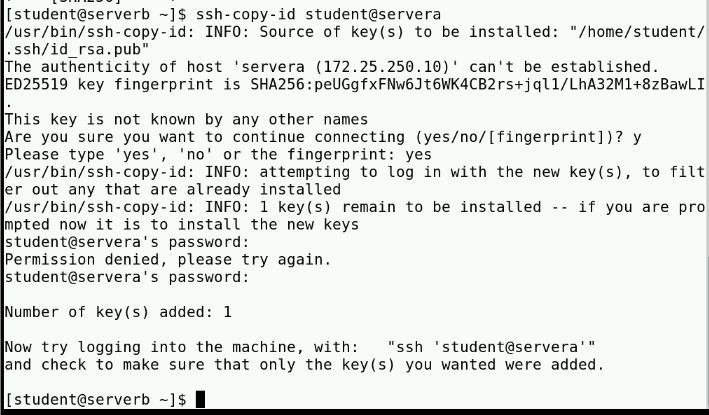
**1. Generating SSH Key Pairs :**

1.1 Switch to the student user on the serverb machine. Use student as the password.

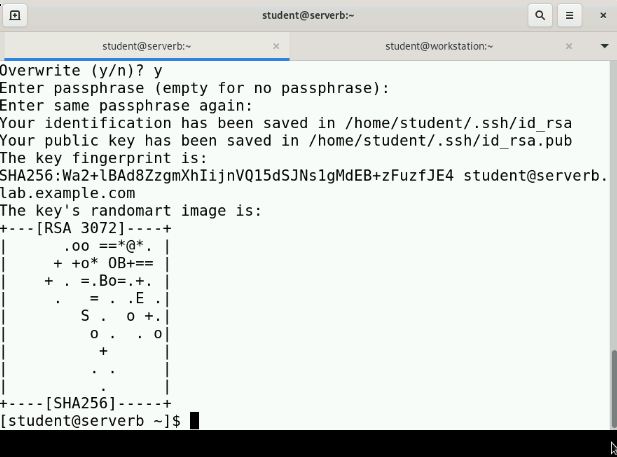
Log in to the serverb machine as the student user.

1.2 Generate a set of SSH keys. Do not enter a passphrase.

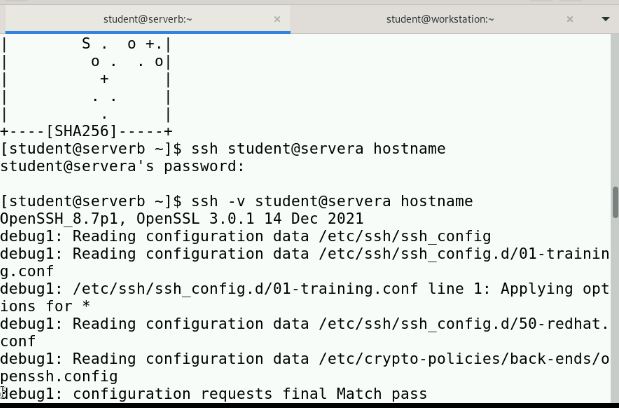
1.3 Send the public key of the SSH key pair to the student user on the servera machine, with student as the password.



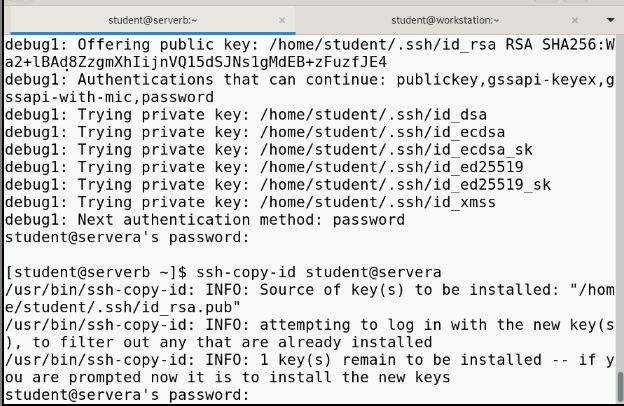
1.4 given null pass -phrase



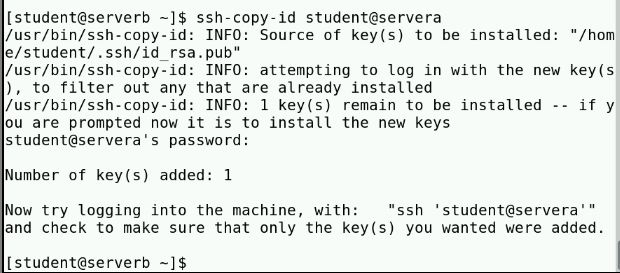
1.5 Execute the hostname command on the servera machine remotely by using the ssh command without accessing the remote interactive shell.

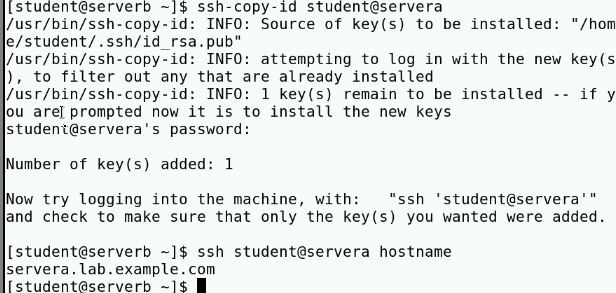


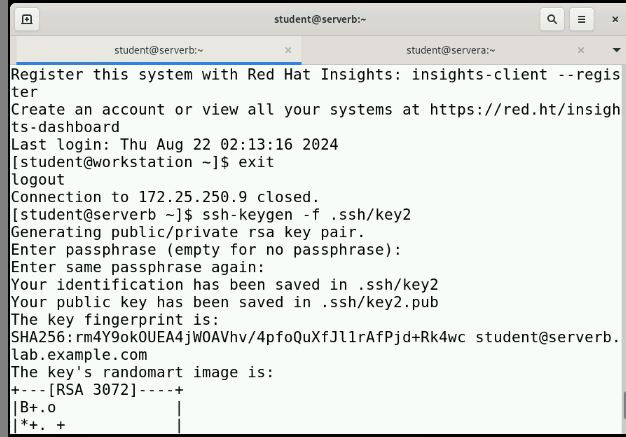
1.6 Generate another set of SSH keys with the default name and without a passphrase, overwriting the previously generated SSH key files. Try to connect to the servera machine by using the new SSH keys. The ssh command asks for a password, because it cannotauthenticate with the SSH key. Run again the ssh command with the -v (verbose) option to verify it.



1.7 Again generate another set of SSH keys with the default name and without a passphrase, overwriting the previously generated SSH key files.



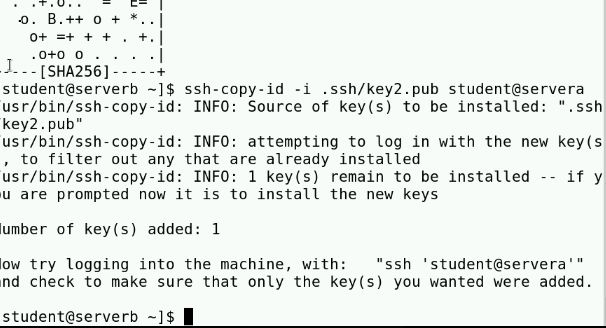




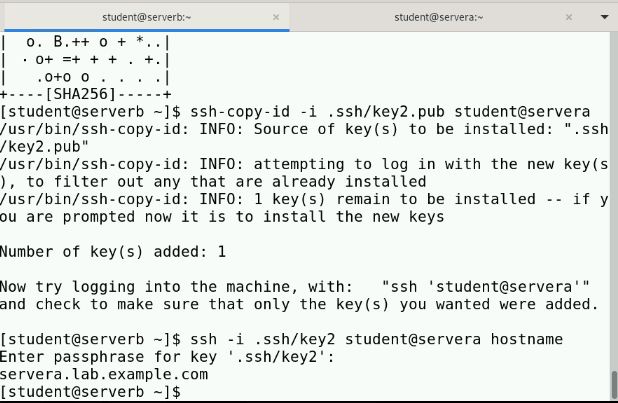
Try to connect to the servera machine by using the new SSH keys. The ssh command asks for a password, because it cannot authenticate with the SSH key.

Press Ctrl+c to exit from the ssh command when it prompts for a password. Run again the ssh command with the -v (verbose) option to verify it. Press again Ctrl+cto exit from the ssh command when it prompts for a password.

1.8 Generate another set of SSH keys with passphrase-protection. Save the key as **/home/student/.ssh/key2**. Use redhatpass as the passphrase of the private key.



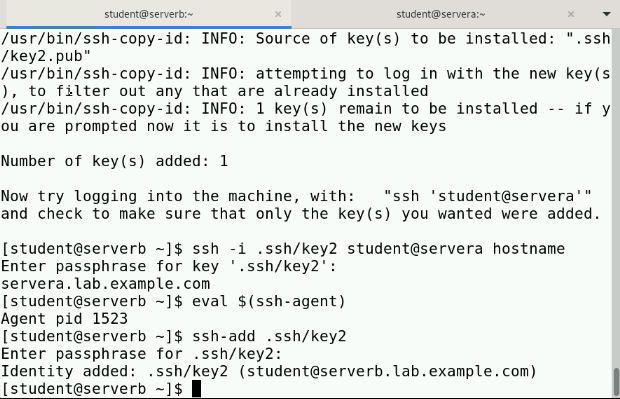
**1.9 Send the public key of the passphrase-protected key pair to the operator1 user on the servera machine. The command does not prompt you for a password because it uses the public key of the passphrase-less private key that you exported to the servera machine in the preceding step.**



**2. Execute the hostname command on the servera machine remotely by using the ssh command. Use the /home/student/.ssh/key2 key as the identity file. Specify redhatpass as the passphrase, which you set for the private key in the preceding step.**

**The command does not prompt you to enter the passphrase interactively.**

**The command starts the ssh-agent program and configures the shell session to use it. Then, you use the ssh-add command to provide the unlocked private key to the ssh-agent program.**

****

**3. Run the ssh-agent program in your Bash shell and add the passphrase-protected private key (/home/student/.ssh/key2) of the SSH key pair to the shell session.**

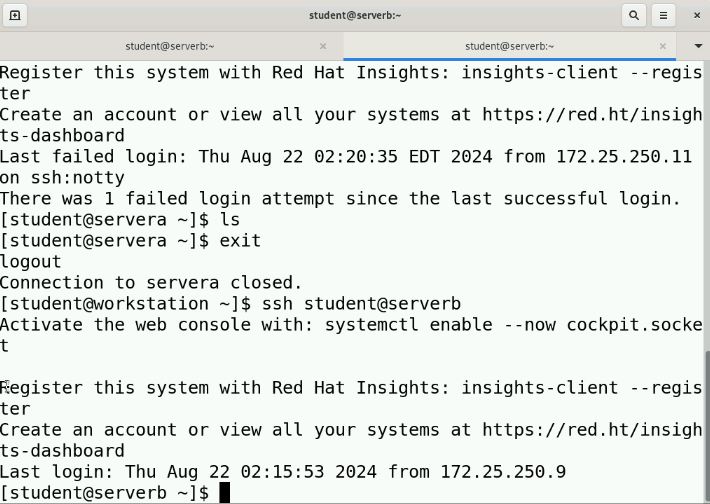
**The command starts the ssh-agent program and configures the shell session to use it. Then, you use the ssh-add command to provide the unlocked private key to the ssh-agent program.**

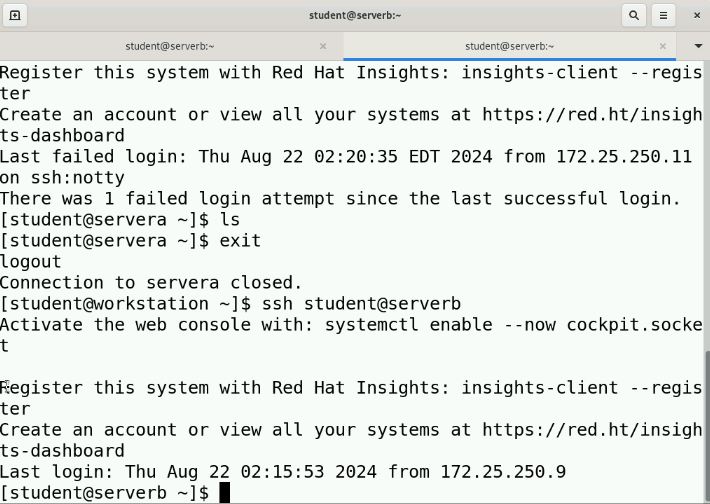
4. Open another terminal on the workstation machine and log in to the serverb machine as the student user.



5. On the serverb machine, switch to the student user and remotely log in to the servera machine. Use the /home/student/.ssh/key2 key as the identity file to

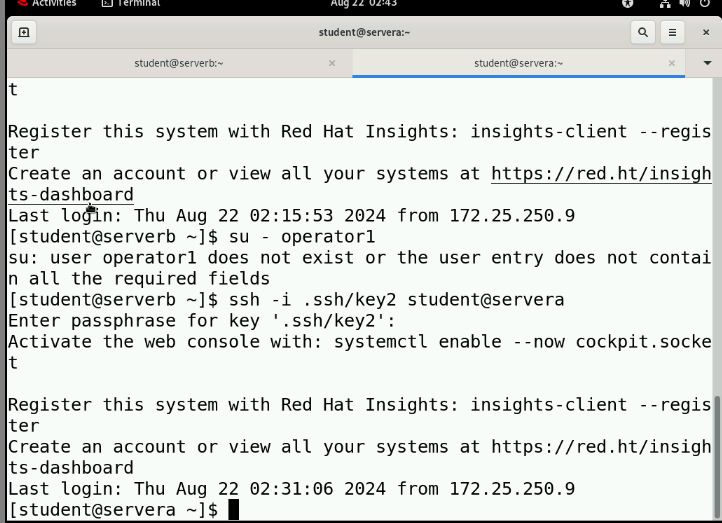
authenticate using the SSH keys.





6. Execute the hostname command on the servera machine remotely without accessing a remote interactive shell. Use the /home/student/.ssh/key2 key as the identity file.

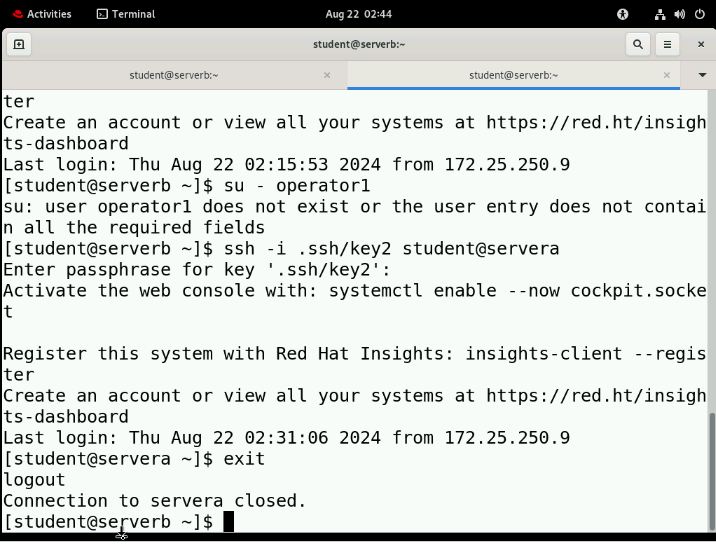
The command does not prompt you to enter the passphrase interactively.



7. Log in to the **servera** machine as the student user.

The command prompts you to enter the passphrase interactively because you do not invoke the SSH connection from the same shell where you started the ssh-agent program.

8. Open another terminal on the workstation machine and log in to the serverb machine as the student user.



9. On the serverb machine, switch to the operator1 user and remotely log in to the servera machine. Use the /home/student/.ssh/key2 key as the identity file to

authenticate using the SSH keys.

10 .Use the su command to switch to the operator1 user. Use student as the password for the operator1 user.

