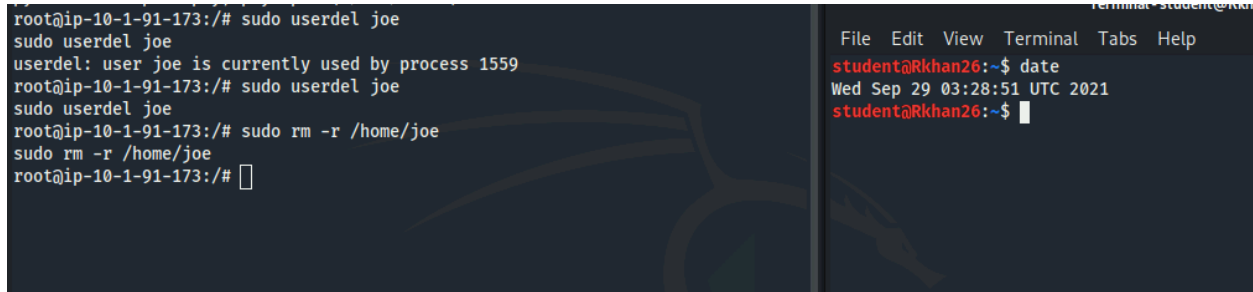


Roozah Khan

Laboratory Exercise 3-9 – Cleaning up

Task 1: Remove the user account you created

A screenshot of a terminal window showing the process of removing a user named 'joe'. The terminal is running as root on a machine with IP 10-1-91-173. The commands executed are: 'sudo userdel joe', which returns 'userdel: user joe is currently used by process 1559', followed by another 'sudo userdel joe'. Then, 'sudo rm -r /home/joe' is run to remove the user's home directory. The prompt returns to root@ip-10-1-91-173:/. On the right, a separate terminal window titled 'Terminal - student@Rkhan26: ~' shows the user 'student@Rkhan26' running 'date', which outputs 'Wed Sep 29 03:28:51 UTC 2021'.

```
root@ip-10-1-91-173:/# sudo userdel joe
sudo userdel joe
userdel: user joe is currently used by process 1559
root@ip-10-1-91-173:/# sudo userdel joe
sudo userdel joe
root@ip-10-1-91-173:/# sudo rm -r /home/joe
sudo rm -r /home/joe
root@ip-10-1-91-173:/#
```

```
student@Rkhan26:~$ date
Wed Sep 29 03:28:51 UTC 2021
student@Rkhan26:~$
```

I deleted the user joe using the sudo userdel command and sudo rm -r /home/joe to completely remove joe user.

Task 2: Remove the student account from the sudo group

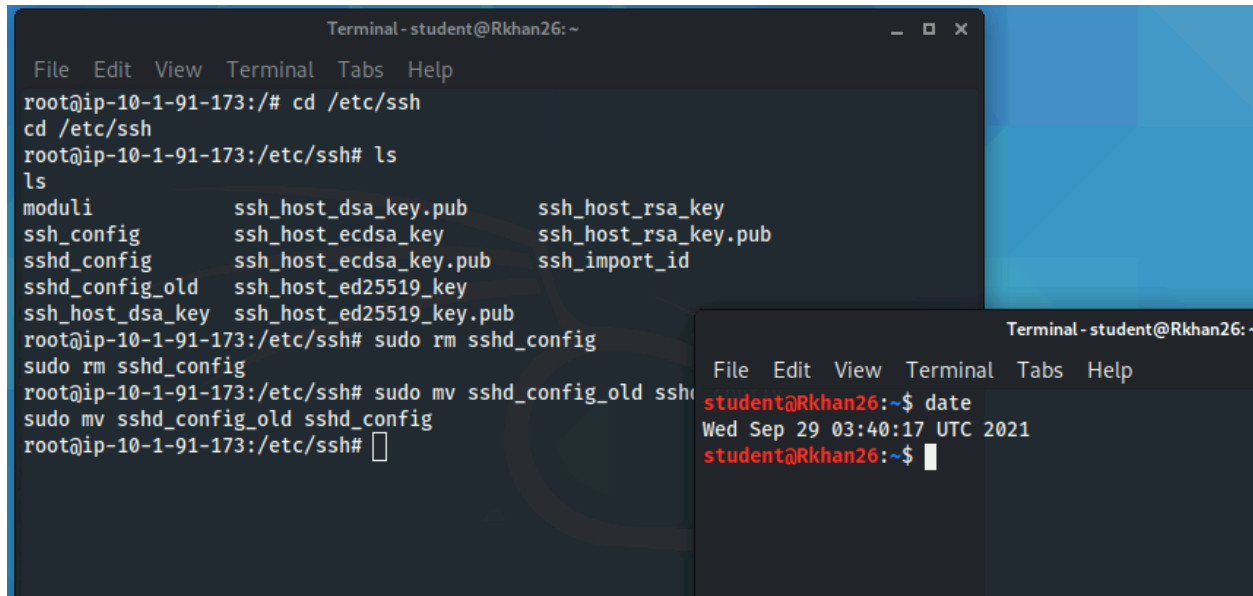
A screenshot of a terminal window showing the removal of the 'student' user from the 'sudo' group. The terminal is running as root on a machine with IP 10-1-91-173. The commands executed are: 'sudo gpasswd -d student sudo', which returns 'Removing user student from group sudo'. The prompt returns to root@ip-10-1-91-173:/. On the right, a separate terminal window titled 'Terminal - student@Rkhan26: ~' shows the user 'student@Rkhan26' running 'date', which outputs 'Wed Sep 29 03:29:55 UTC 2021'.

```
root@ip-10-1-91-173:/# sudo gpasswd -d student sudo
sudo gpasswd -d student sudo
Removing user student from group sudo
root@ip-10-1-91-173:/#
```

```
student@Rkhan26:~$ date
Wed Sep 29 03:29:55 UTC 2021
student@Rkhan26:~$
```

I removed the user student from the sudo group.

Task 3: Put the original sshd_config file back



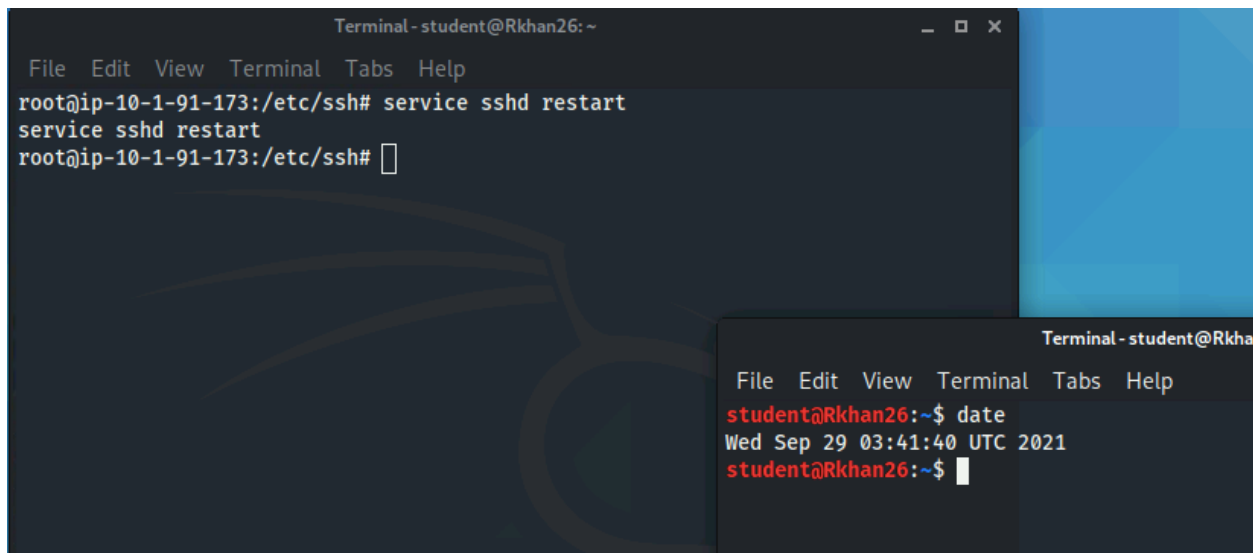
The screenshot shows a terminal window titled 'Terminal - student@Rkhan26: ~'. The user is root at ip-10-1-91-173. They navigate to /etc/ssh and list files. Then they remove the modified sshd_config and rename the original sshd_config_old back to sshd_config. A second terminal window shows the date command output.

```
Terminal - student@Rkhan26: ~
File Edit View Terminal Tabs Help
root@ip-10-1-91-173:/# cd /etc/ssh
cd /etc/ssh
root@ip-10-1-91-173:/etc/ssh# ls
ls
moduli                ssh_host_dsa_key.pub    ssh_host_rsa_key
ssh_config             ssh_host_ecdsa_key      ssh_host_rsa_key.pub
sshd_config            ssh_host_ecdsa_key.pub  ssh_import_id
sshd_config_old        ssh_host_ed25519_key
ssh_host_dsa_key        ssh_host_ed25519_key.pub
root@ip-10-1-91-173:/etc/ssh# sudo rm sshd_config
sudo rm sshd_config
root@ip-10-1-91-173:/etc/ssh# sudo mv sshd_config_old sshd_config
sudo mv sshd_config_old sshd_config
root@ip-10-1-91-173:/etc/ssh#
```

```
Terminal - student@Rkhan26: ~
File Edit View Terminal Tabs Help
student@Rkhan26:~$ date
Wed Sep 29 03:40:17 UTC 2021
student@Rkhan26:~$
```

I put the original sshd_config back to where it was by changing into the ssh directory and then removing the modified sshd_config file and then renaming the original file back to its original name.

Task 4: Restart the ssh server



The screenshot shows a terminal window titled 'Terminal - student@Rkhan26: ~'. The user is root at ip-10-1-91-173. They run the command 'service sshd restart'. A second terminal window shows the date command output.

```
Terminal - student@Rkhan26: ~
File Edit View Terminal Tabs Help
root@ip-10-1-91-173:/etc/ssh# service sshd restart
service sshd restart
root@ip-10-1-91-173:/etc/ssh#
```

```
Terminal - student@Rkhan26: ~
File Edit View Terminal Tabs Help
student@Rkhan26:~$ date
Wed Sep 29 03:41:40 UTC 2021
student@Rkhan26:~$
```

After that I restarted the sshd service on the target system.

Task 5: Backout of the backdoor

```
$ exit
Connection to 10.1.91.173 closed.
student@Rkhan26:~$
```

```
File Edit View Terminal Tabs Help
student@Rkhan26:~$ date
Wed Sep 29 03:42:35 UTC 2021
student@Rkhan26:~$
```

I exited out the session.