

Practical Exercise 11-1: managing User Access

This Practical Exercise will take students through the practice of setting age limits on passwords as well as configuring sudo to allow a standard user to kill a process.

Open VirtualBox and start the openSUSE VM. Run snapshot 17-1 for the correctly configured environment. To run snapshot 17-1:

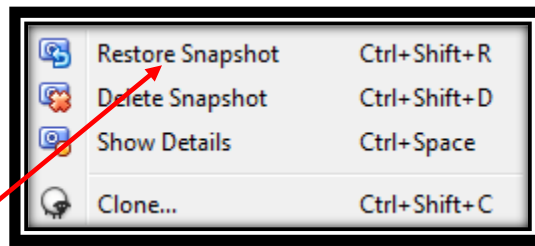
1. Open the Oracle VM VirtualBox manager by double clicking this icon on your desktop:



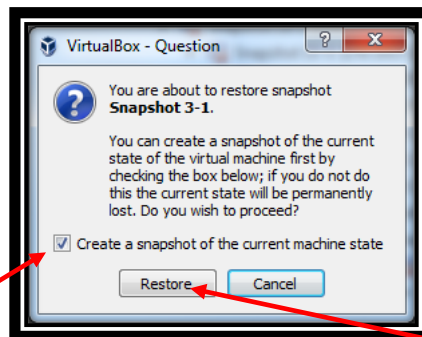
2. Click "Snapshots" in the top right of the Oracle VM Virtualbox Manager.



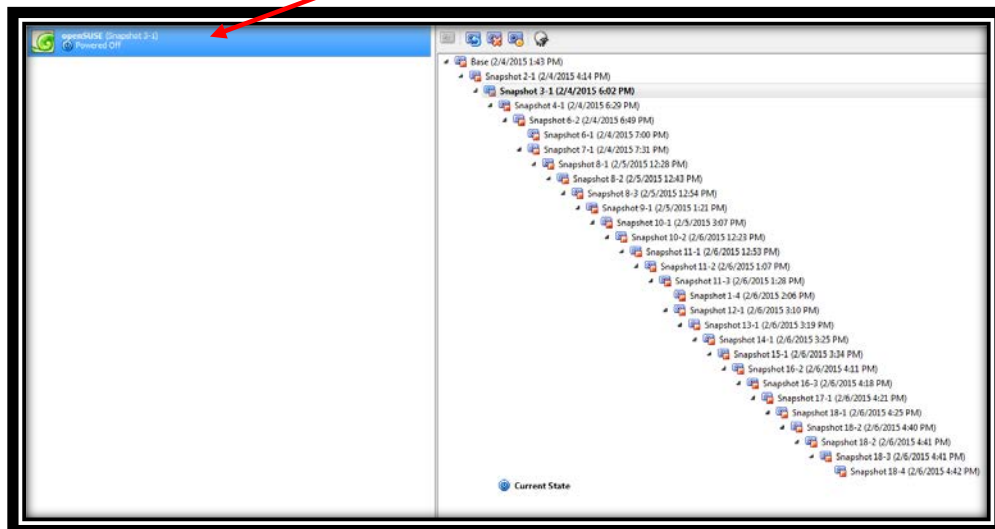
3. In the right side box populated with snapshots scroll up and find the one titled "Snapshot 17-1" and right click on it. The following box should appear:



4. Select "Restore Snapshot" and the following pop-up should appear:



5. Uncheck the "Create a Snapshot of the current machine state" box and then click the "Restore" button. If the pop up box does not have the check box, just click "Restore."
6. You should now see in the left box the openSUSE (Snapshot 17-1) with a status of "Powered Off." Power it on by double clicking it.



7. A separate window should open and you should see the openSUSE Linux OS booting.

8. Press **CTRL+ALT+F1** and login with the username: **root** and password: **student**.
9. Practice configuring age limits by completing the following:
 - a. Use the cat or less utility to view the /etc/passwd file. Identify a user on the system that you want to configure password age limits for.
 - b. Set the minimum password age to three days, the maximum password age to 60 days, and the number of warning days before expiration to seven by entering **chage -m 3 -M 60 -W 7 username** at the shell prompt.
10. Configure sudo to allow a user on your system to kill processes as the root user by doing the following:
 - a. Identify a user on your system to whom you want to grant the ability to kill processes as root.
 - b. As your root user, enter **visudo** at the shell prompt. You should see the /etc/sudoers file loaded in the vi text editor.
 - c. Press **INS**.
 - d. Scroll down to the lines shown in the example that follows and **comment them out by inserting a # character at the beginning of each one**.

Defaults targetpw # ask for the password of the target user i.e. root
ALL ALL=(ALL) ALL # WARNING! Only use this together with 'Defaults targetpw'!

- e. Add the following lines to the end of the sudoers file:

```
User_Alias PWRUSRS = your_user  
Cmnd_Alias KILLPROCS = /bin/kill, /usr/bin/killall  
Host_Alias MYHSTS = openSUSE  
PWRUSRS MYHSTS = (root) KILLPROCS
```

- f. Press **ESC** and then enter **:exit** to save the changes to the sudoers file.
- g. Run **top** at the shell prompt as your root user.

- h. Open a new terminal session, **CTRL-ALT-F2**, and (as your standard user) enter **ps –elf | grep top**. You should see a top process running that is owned by the root user.
- i. Kill that process as your standard user by entering **sudo killall top**.
- j. When prompted, enter your user's password (**student**).
- k. Enter **ps –elf | grep top** at the shell prompt again. You should see that the top process that was owned by the root user has been killed.

--End of Practical Exercise--