

Lab 4.7.5 Remove a Specific user from a Group on a Linux System

From TestOut CompTIA Security+ Course

In this lab I will be removing a given user from a given group.

The scenario for this lab is as follows:

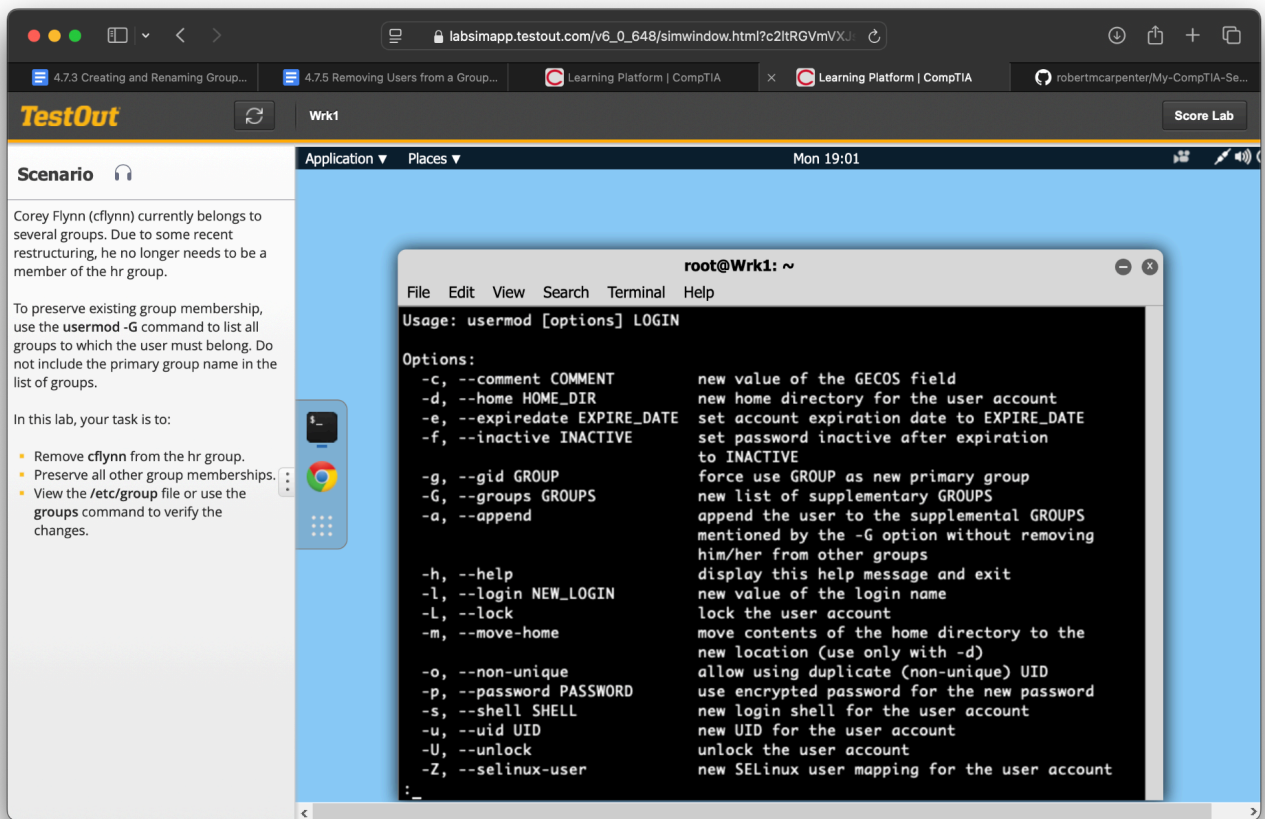
“Corey Flynn (cflynn) currently belongs to several groups. Due to some recent restructuring, he no longer needs to be a member of the hr group.

To preserve existing group membership, use the `usermod -G` command to list all groups to which the user must belong. Do not include the primary group name in the list of groups.

In this lab, your task is to:

1. Remove cflynn from the hr group.
2. Preserve all other group memberships.
3. View the `/etc/group` file or use the `groups` command to verify the changes.”

After reading the scenario I see that they would like me to use the `usermod -G` command to apply these changes. Let's see what that does:



By supplying the `-G` flag it moves the supplied user in the argument to the groups defined and takes them out of the current groups. To see what other groups the cflynn user is apart of we can query the `/etc/group` file by issuing “`cat /etc/group` or `groups`”

```
root@Wrk1: ~  
File Edit View Search Terminal Help  
saslauth:x:493:  
mailnull:x:492:  
smmsp:x:491:  
mysql:x:490:  
haldaemon:x:489:  
sshd:x:488:  
wadams:x:500:  
rcronn:x:501:  
vedwards:x:502:  
cflynn:x:503:  
mbrown:x:504:  
placy:x:505:  
bcassini:x:506:  
aespinoza:x:507:  
bkahn:x:508:  
schawla:x:509:  
mgmt1:x:510:wadams,rcronn,placy,aespinoza,cflynn,mbrown,schawla  
mgmt2:x:511:wadams,rcronn,vedwards,bkahn,schawla  
hr:x:512:wadams,vedwards,placy,cflynn,bcassini,mbrown,schawla  
sales:x:513:bkahn,schawla  
devel:x:514:mbrown  
it:x:515:rcronn,aespinoza,cflynn  
proj:x:516:placy  
  
root@Wrk1:~# _
```

From here we can see that the cflynn user is apart of the MGMT1, HR, and IT groups. Since the usermod -G commands puts that user in the groups we define and removes them from any we don't supply. So in order to remove cflynn from the HR group but keep them in the MGMT1 and IT groups we simply just need to supply those groups to the arguments of the command. Since the HR group is omitted from the command options the usermod command will assign cflynn to those groups and those ONLY. Issuing the command "usermod -G mgmt1,it cflynn" we get:

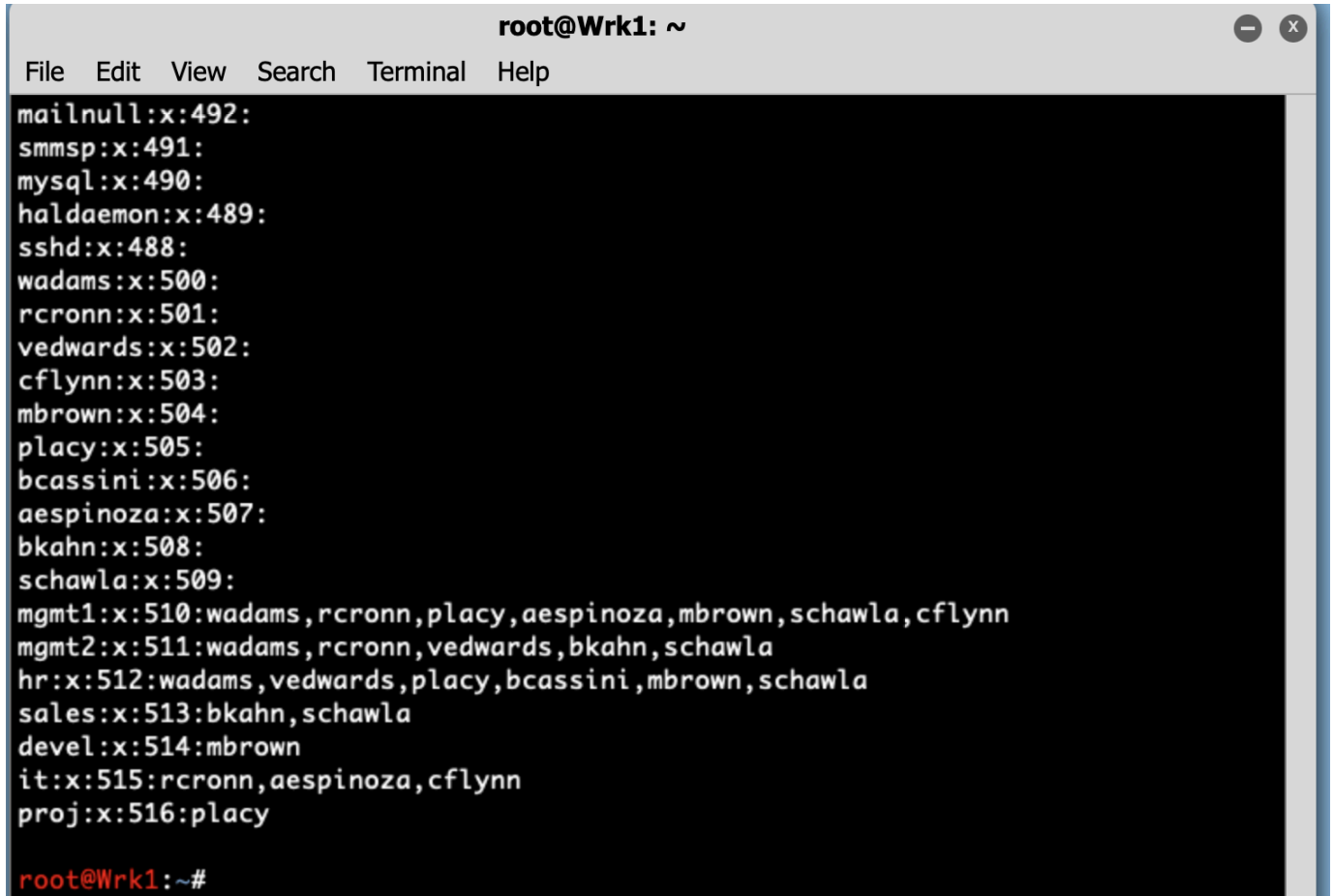
```
root@Wrk1:~# usermod -G mgmt1,it cflynn  
root@Wrk1:~# cat /etc/group  
root@Wrk1:~#
```

Robert Carpenter

github.com/robertmcarpenter

Mon November 18th 2024

To view the changes enter the second command above “cat /etc/group.” This will query the groups file in order for us to see group membership.



```
root@Wrk1: ~
File Edit View Search Terminal Help
mailnull:x:492:
smmsp:x:491:
mysql:x:490:
haldaemon:x:489:
sshd:x:488:
wadams:x:500:
rcronn:x:501:
vedwards:x:502:
cflynn:x:503:
mbrown:x:504:
placy:x:505:
bcassini:x:506:
aespinoza:x:507:
bkahn:x:508:
schawla:x:509:
mgmt1:x:510:wadams,rcronn,placy,aespinoza,mbrown,schawla,cflynn
mgmt2:x:511:wadams,rcronn,vedwards,bkahn,schawla
hr:x:512:wadams,vedwards,placy,bcassini,mbrown,schawla
sales:x:513:bkahn,schawla
devel:x:514:mbrown
it:x:515:rcronn,aespinoza,cflynn
proj:x:516:placy
root@Wrk1:~#
```

Awesome! I can see that the cflynn user is no longer apart of the hr group and has membership still to the other groups they were apart of. Note that this approach is better since sometimes the group file can be quite large and there might be lingering memberships to other groups we don't notice. That way we effectively take them out of EVERY group and then assign them to the groups only we want them to be in.

This now concludes this lab!

Robert Carpenter
github.com/robertmcarpenter
Mon November 18th 2024

The screenshot shows a web browser window with the TestOut interface. The browser's address bar displays `labsimapp.testout.com/v6_0_648/simwindow.html?c2ltRGVmVXJl`. The browser has several tabs open, including '4.7.3 Creating and Renaming Group...', '4.7.5 Removing Users from a Group...', and 'Learning Platform | CompTIA'. The TestOut interface features a sidebar on the left with a 'Scenario' section. The main content area is titled 'Wrk1' and shows a 'Lab Report' modal. The modal displays a score of 3/3 (100%) and a time spent of 42:39. Below the score is a 'TASK SUMMARY' section with 'Required Actions' listed as follows:

- ✓ Remove cflynn from the hr group
- ✓ Keep cflynn as a member of the it group
- ✓ Keep cflynn as a member of the mgmt1 group

The background of the lab interface shows a terminal window with the following output:

```
it:x:515:rcronn,aespinoza,cflynn
proj:x:516:placy
root@Wrk1:~#
```