

## Lab 4.6.6 Deleting a User Securely from a Linux System

*From TestOut CompTIA Security+ Course*

In this lab, I will be deleting a user from a hypothetical company's Linux server.

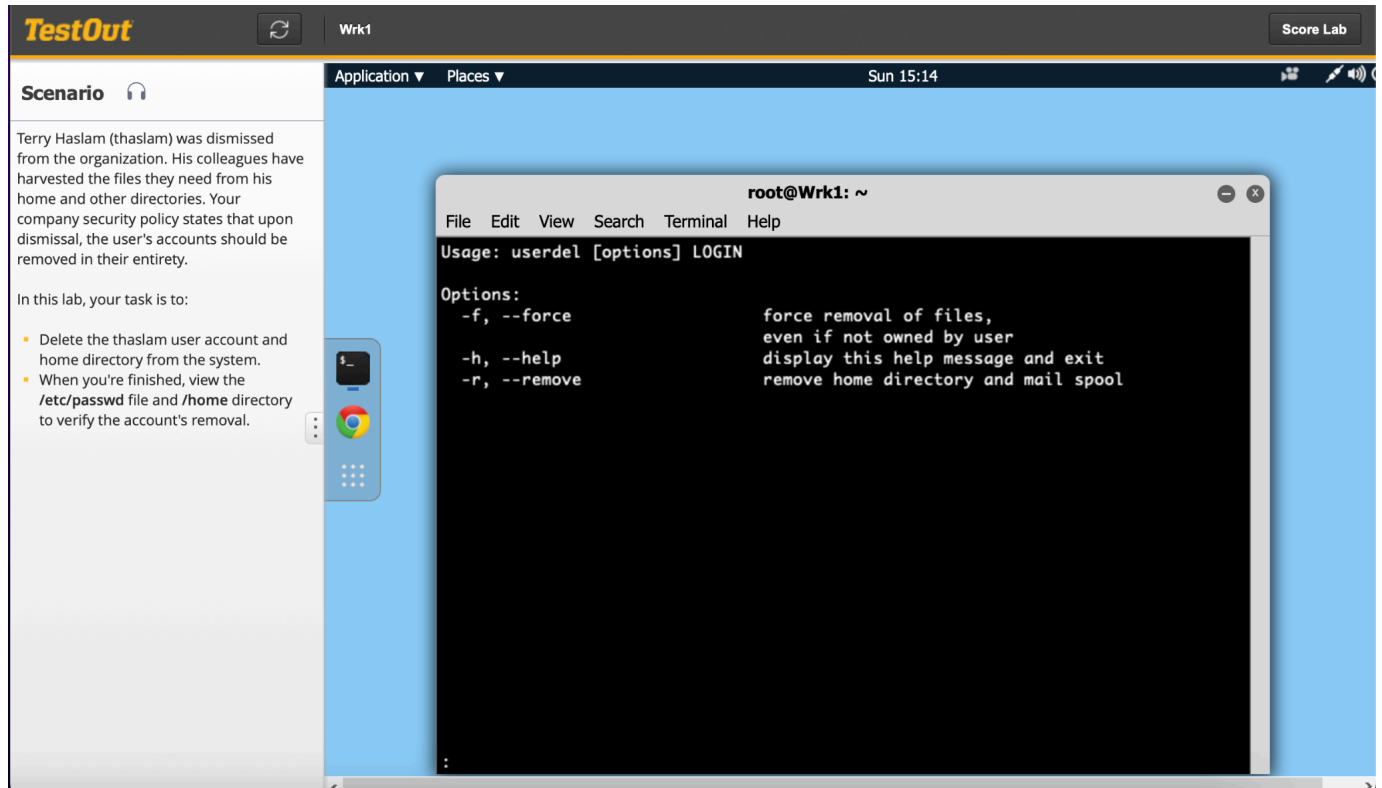
**“The scenario for this lab is as follows:**

**Terry Haslam (thaslam) was dismissed from the organization. His colleagues have harvested the files they need from his home and other directories. Your company security policy states that upon dismissal, the user's accounts should be removed in their entirety.**

**In this lab, your task is to:**

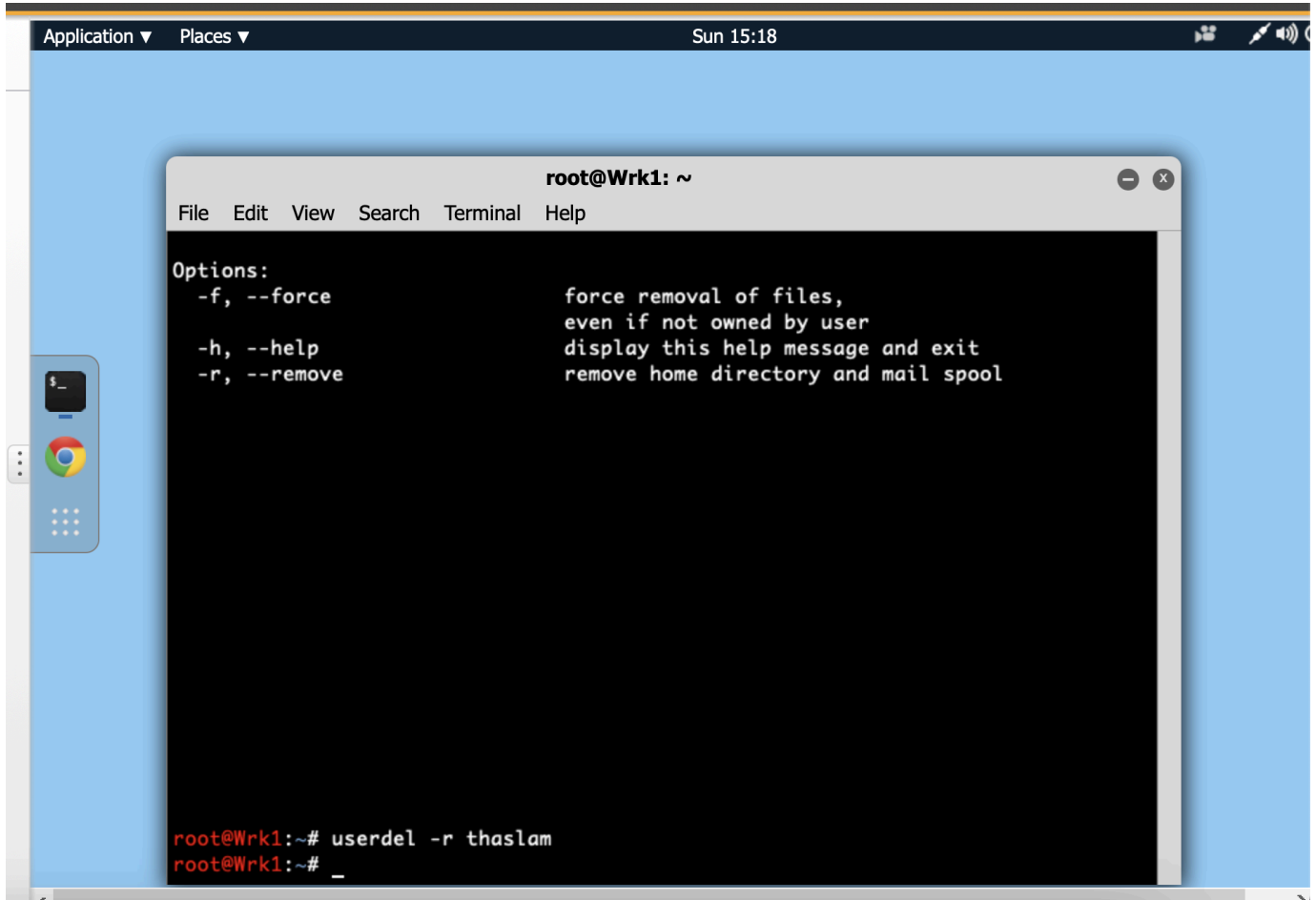
- **Delete the thaslam user account and home directory from the system.**
- **When you're finished, view the /etc/passwd file and /home directory to verify the account's removal.”**

The best of going about this fairly simple task is to utilize the “userdel” binary which is part of almost every GNU/Linux System. To see what we can do with the command , let's query the man page for userdel.



Wow, that's a very simple command! This makes our job much easier! Since our first task states that we should be deleting the thaslam user's /home/thaslam directory, we will want to supply the "-r" flag. The "-f" force flag can be potentially destructive as it states that it will "force removal of files even if not owned by user." We don't need to use it in this case since our colleagues have already harvested all the needed files from the thaslam account.

To delete this user enter in on the command line "userdel -r thaslam"



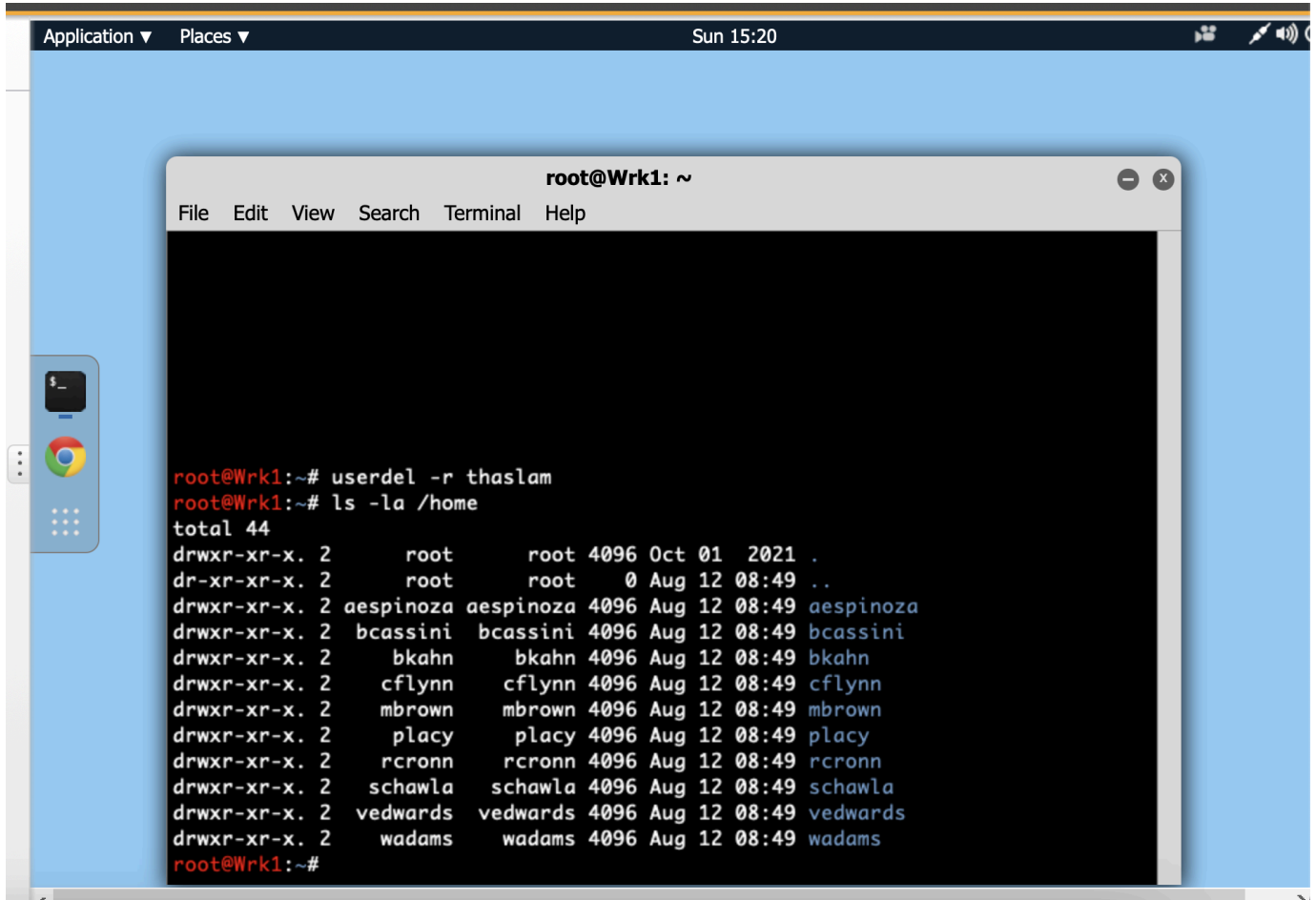
```
root@Wrk1: ~  
File Edit View Search Terminal Help  
Options:  
-f, --force          force removal of files,  
                     even if not owned by user  
-h, --help          display this help message and exit  
-r, --remove        remove home directory and mail spool  
  
root@Wrk1:~# userdel -r thaslam  
root@Wrk1:~# _
```

I know my command was successful because the shell is now prompting to enter another one. To complete the second part of the task which is to verify that the user has been removed from the system. We can know this by checking for the existence of the “thaslam” user in the /home directory as well as the /etc/shadow file. First let’s verify their home directory was deleted by entering “ls -la /home” and looking for the thaslam username.

Robert Carpenter

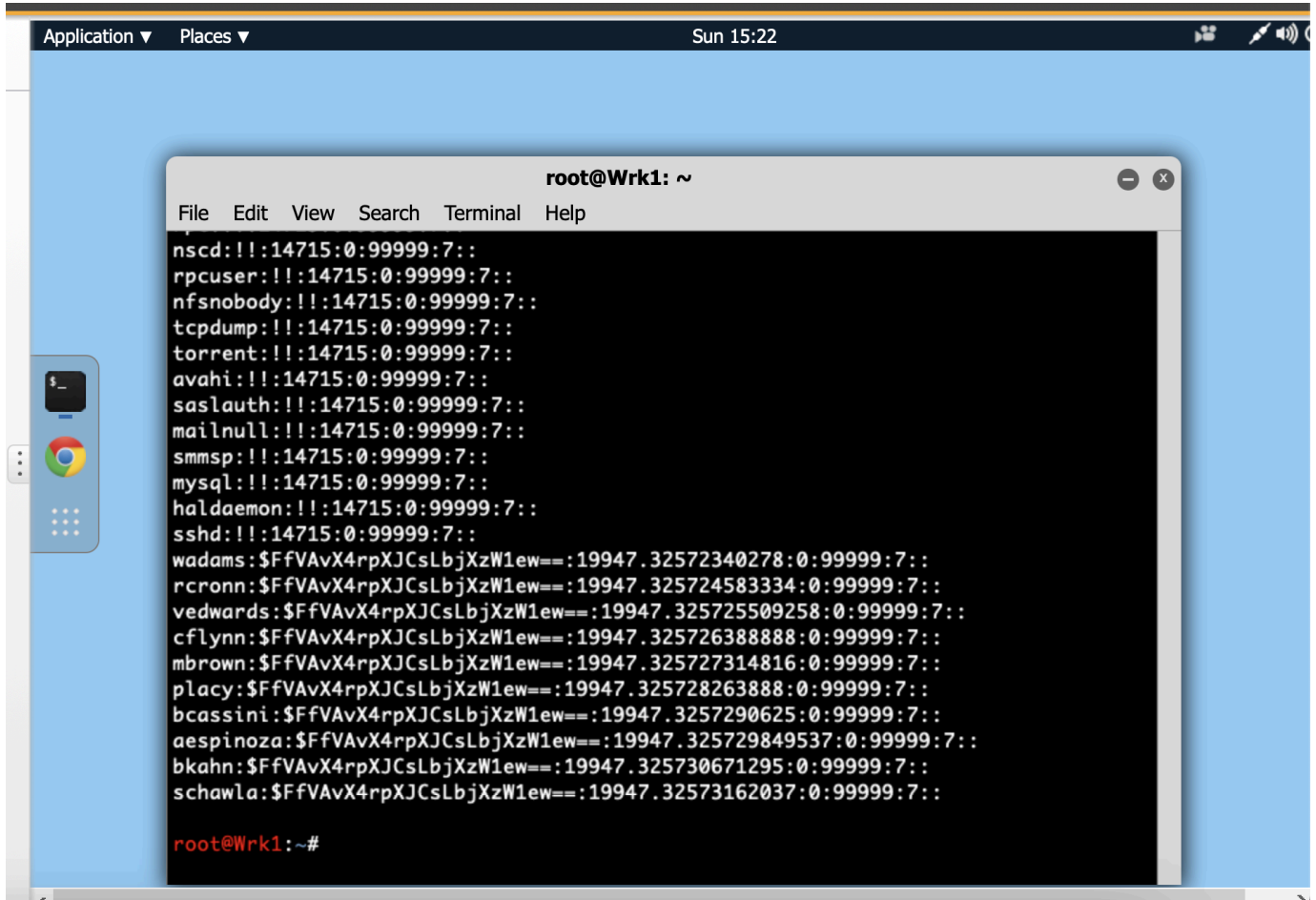
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)

Sun November 17th 2024



```
root@Wrk1: ~  
File Edit View Search Terminal Help  
  
root@Wrk1:~# userdel -r thaslam  
root@Wrk1:~# ls -la /home  
total 44  
drwxr-xr-x. 2 root root 4096 Oct 01 2021 .  
dr-xr-xr-x. 2 root root 0 Aug 12 08:49 ..  
drwxr-xr-x. 2 aespinoza aespinoza 4096 Aug 12 08:49 aespinoza  
drwxr-xr-x. 2 bcassini bcassini 4096 Aug 12 08:49 bcassini  
drwxr-xr-x. 2 bkahn bkahn 4096 Aug 12 08:49 bkahn  
drwxr-xr-x. 2 cflynn cflynn 4096 Aug 12 08:49 cflynn  
drwxr-xr-x. 2 mbrown mbrown 4096 Aug 12 08:49 mbrown  
drwxr-xr-x. 2 placy placy 4096 Aug 12 08:49 placy  
drwxr-xr-x. 2 rcronn rcronn 4096 Aug 12 08:49 rcronn  
drwxr-xr-x. 2 schawla schawla 4096 Aug 12 08:49 schawla  
drwxr-xr-x. 2 vedwards vedwards 4096 Aug 12 08:49 vedwards  
drwxr-xr-x. 2 wadams wadams 4096 Aug 12 08:49 wadams  
root@Wrk1:~#
```

As you can see , their username is not present. Now let's check the /etc/shadow file. Enter "cat /etc/shadow" (we are root so we don't need sudo, although you would want to put sudo in the real world because you never want to run around a Linux system with root privileges ! It's dangerous!)

A screenshot of a terminal window titled "root@Wrk1: ~". The terminal displays a list of system users and their corresponding hashes. The users listed are: nscd, rpcuser, nfsnobody, tcpdump, torrent, avahi, saslauth, mailnull, smmsp, mysql, haldaemon, sshd, wadams, rcronn, vedwards, cflynn, mbrown, placy, bcassini, aespinoza, bkahn, and schawla. Each user is followed by a colon and a long alphanumeric hash. The terminal prompt is "root@Wrk1:~#".

```
root@Wrk1: ~
File Edit View Search Terminal Help
nscd:!!:14715:0:99999:7::
rpcuser:!!:14715:0:99999:7::
nfsnobody:!!:14715:0:99999:7::
tcpdump:!!:14715:0:99999:7::
torrent:!!:14715:0:99999:7::
avahi:!!:14715:0:99999:7::
saslauth:!!:14715:0:99999:7::
mailnull:!!:14715:0:99999:7::
smmsp:!!:14715:0:99999:7::
mysql:!!:14715:0:99999:7::
haldaemon:!!:14715:0:99999:7::
sshd:!!:14715:0:99999:7::
wadams:$FfVAvX4rpXJCslbjXzW1ew==:19947.32572340278:0:99999:7::
rcronn:$FfVAvX4rpXJCslbjXzW1ew==:19947.325724583334:0:99999:7::
vedwards:$FfVAvX4rpXJCslbjXzW1ew==:19947.325725509258:0:99999:7::
cflynn:$FfVAvX4rpXJCslbjXzW1ew==:19947.325726388888:0:99999:7::
mbrown:$FfVAvX4rpXJCslbjXzW1ew==:19947.325727314816:0:99999:7::
placy:$FfVAvX4rpXJCslbjXzW1ew==:19947.325728263888:0:99999:7::
bcassini:$FfVAvX4rpXJCslbjXzW1ew==:19947.3257290625:0:99999:7::
aespinoza:$FfVAvX4rpXJCslbjXzW1ew==:19947.325729849537:0:99999:7::
bkahn:$FfVAvX4rpXJCslbjXzW1ew==:19947.325730671295:0:99999:7::
schawla:$FfVAvX4rpXJCslbjXzW1ew==:19947.32573162037:0:99999:7::
root@Wrk1:~#
```

After parsing through the output I can see that their account no longer exists! We are successful! This will now conclude this lab!

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Sun November 17th 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's tab bar shows several tabs, including 'Learning Platform | C...', 'Lab 4.6.6 Deleting a U...', 'robertmcarpenter/My...', 'List of GNU packages...', and 'userdel command at...'. The TestOut interface has a dark theme. On the left, the 'Scenario' section is visible, containing text about Terry Haslam (thaslam) being dismissed and a list of tasks: 'Delete the thaslam user account and home directory from the system' and 'When you're finished, view the /etc/passwd file and /home directory to verify the account's removal.' The main area shows a 'Lab Report' modal window. The modal has a title 'Lab Report' and a subtitle 'Time Spent: 09:10'. It displays a 'Score: 2/2 (100%)' with a full orange progress bar. Below this, the 'TASK SUMMARY' section is titled 'Required Actions' and lists two items: 'Delete the thaslam user' and 'Delete the thaslam home directory', both marked with green checkmarks. At the bottom of the modal, there is an 'EXPLANATION' section with a speaker icon. The background of the modal shows a terminal window with a command prompt `root@Wrk1:~#` and some output text.

TestOut

Scenario

Terry Haslam (thaslam) was dismissed from the organization. His colleagues have harvested the files they need from his home and other directories. Your company security policy states that upon dismissal, the user's accounts should be removed in their entirety.

In this lab, your task is to:

- Delete the thaslam user account and home directory from the system.
- When you're finished, view the `/etc/passwd` file and `/home` directory to verify the account's removal.

Application ▾ Places ▾ Sun 15:23

Score Lab

### Lab Report

Time Spent: 09:10

**Score: 2/2 (100%)**

TASK SUMMARY

**Required Actions**

- ✓ Delete the thaslam user
- ✓ Delete the thaslam home directory

EXPLANATION

```
bkahn:$FfVAvX4rpXJCslbjXzW1ew==:19947.325730671295:0:99999:7::
schawla:$FfVAvX4rpXJCslbjXzW1ew==:19947.32573162037:0:99999:7::
root@Wrk1:~#
```