Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024

Lab 4.6.9 Lock and Unlock User accounts on a Linux System

From TestOut CompTIA Security+ Course

In this lab I will be locking and unlocking user accounts on a Linux system. The lab provides a list of users for us to evaluate.

“The scenario for this lab is as follows:

Every seven years, your company provides a six-week sabbatical for every employee. Vera Edwards (vedwards), Corey Flynn (cflynn), and Bhumika Kahn (bkahn) are leaving today. Maggie Brown (mbrown), Brenda Cassini (bcassini), and Arturo Espinoza (aespinoza) are just returning.

The company security policy mandates that user accounts for employees gone for longer than two weeks be disabled.

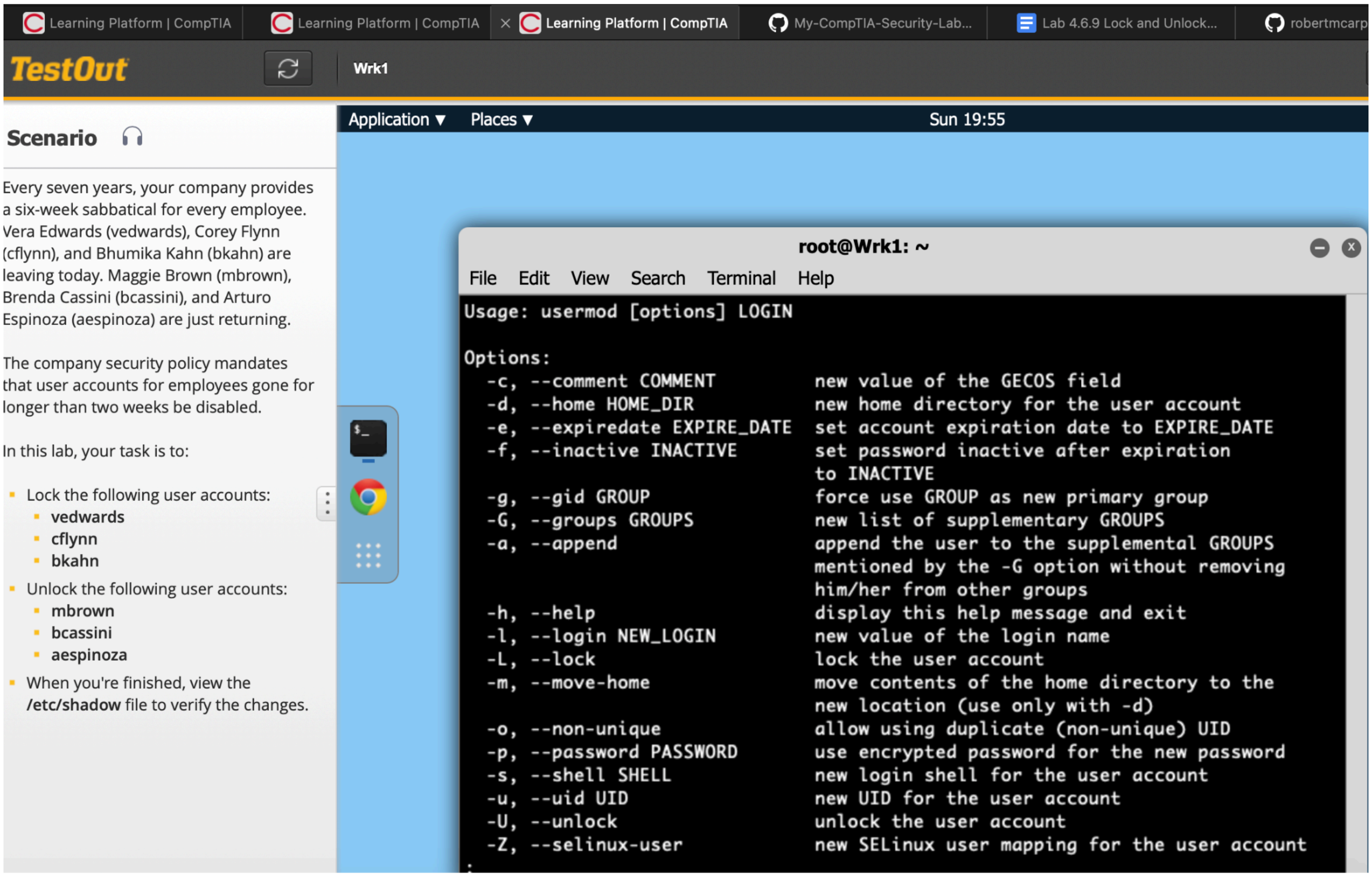
In this lab, your task is to:

- **Lock the following user accounts:**
  - **vedwards**
  - **cflynn**
  - **bkahn**
- **Unlock the following user accounts:**
  - **mbrown**
  - **bcassini**
  - **aespinoza**
- **When you're finished, view the /etc/shadow file to verify the changes.**

To achieve our 1st goal of locking user accounts we can use 2 methods on a Linux systems. “Usermod” and “passwd” both have functions built in that can lock a user account. For the sake of using a different binary for this lab (since we used passwd in the last 2 labs) we’ll go with “usermod.”

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024

Now, how do I know that the usermod command can be used for locking accounts? Simple. Let’s query the man page for usermod to take a look at the arguments we can pass it. Typing “man usermod” we get:


Learning Platform | CompTIA
Learning Platform | CompTIA
Learning Platform | CompTIA
My-CompTIA-Security-Lab...
Lab 4.6.9 Lock and Unlock...
robertmcarp
TestOut
Wrk1
Application ▾
Places ▾
Sun 19:55
root@Wrk1: ~
File
Edit
View
Search
Terminal
Help

Scenario

Every seven years, your company provides a six-week sabbatical for every employee. Vera Edwards (vedwards), Corey Flynn (cflynn), and Bhumika Kahn (bkahn) are leaving today. Maggie Brown (mbrown), Brenda Cassini (bcassini), and Arturo Espinoza (aespinoza) are just returning.

The company security policy mandates that user accounts for employees gone for longer than two weeks be disabled.

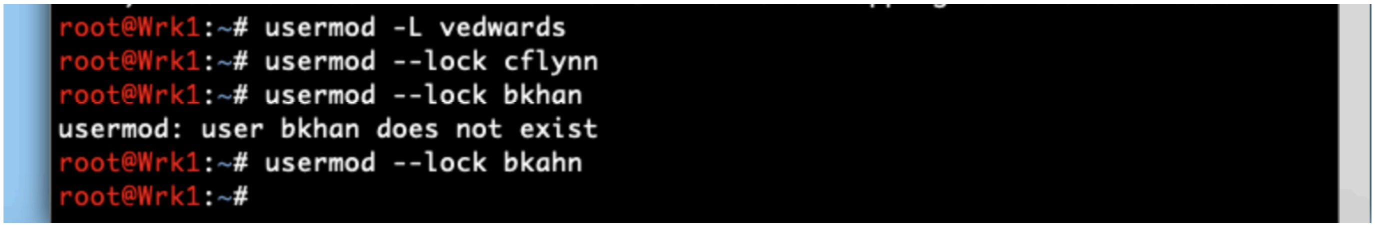
In this lab, your task is to:

- Lock the following user accounts:
  - **vedwards**
  - **cflynn**
  - **bkahn**
- Unlock the following user accounts:
  - **mbrown**
  - **bcassini**
  - **aespinoza**
- When you're finished, view the **/etc/shadow** file to verify the changes.

```
Usage: usermod [options] LOGIN

Options:
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                him/her from other groups
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -Z, --selinux-user            new SELinux user mapping for the user account
```

We can see that the option -L or - -lock (two dashes) can be passed. Either flag works as they are the same thing. Note that in Linux , flags that contain whole words are denoted by a double dash , while flags that are simply just letters are denoted by a single dash. Let’s go ahead and lock the 3 user accounts as requested which are :

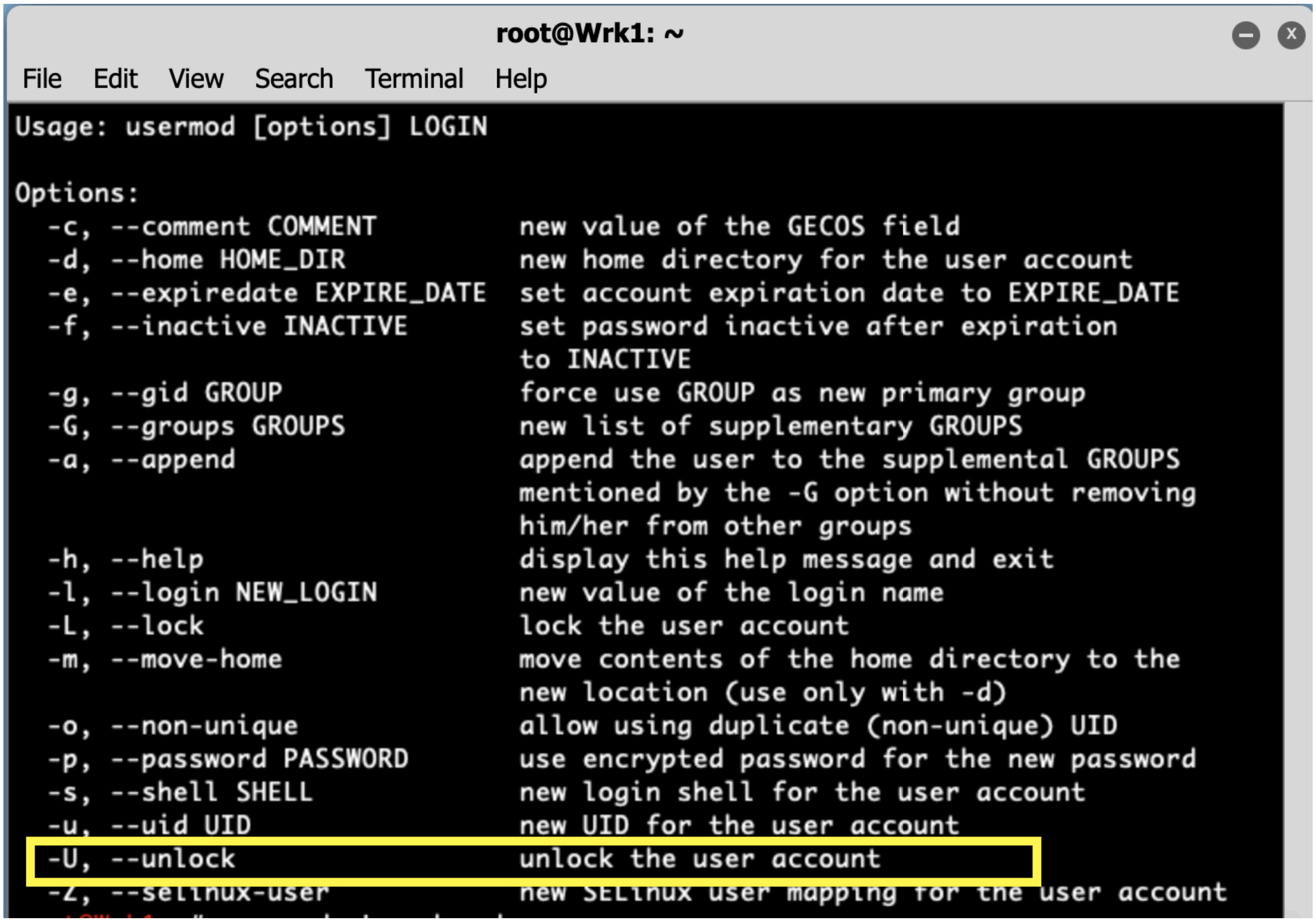


```
root@Wrk1:~# usermod -L vedwards
root@Wrk1:~# usermod --lock cflynn
root@Wrk1:~# usermod --lock bkhan
usermod: user bkhan does not exist
root@Wrk1:~# usermod --lock bkahn
root@Wrk1:~#
```

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024

To demonstrate the abbreviated and full flag names I entered the second command with –lock instead of -L.

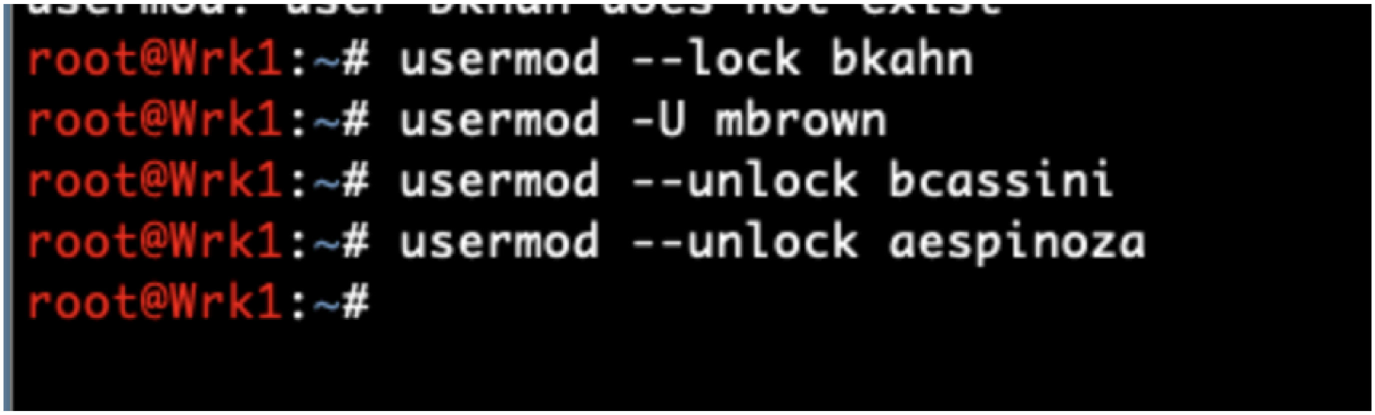
Now that we’ve locked those users now let’s move on to unlocking users which are returning from their 2 week sabbatical. Taking another look at the man page I can see that I can reuse the usermod command but this time, I will need to pass a -U or - - unlock flag to do this.



```
Usage: usermod [options] LOGIN

Options:
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                him/her from other groups
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -Z, --selinux-user            new SELinux user mapping for the user account
```

Since we are root, let’s go ahead and unlock the requested user accounts by passing “usermod -U or –unlock [login]”



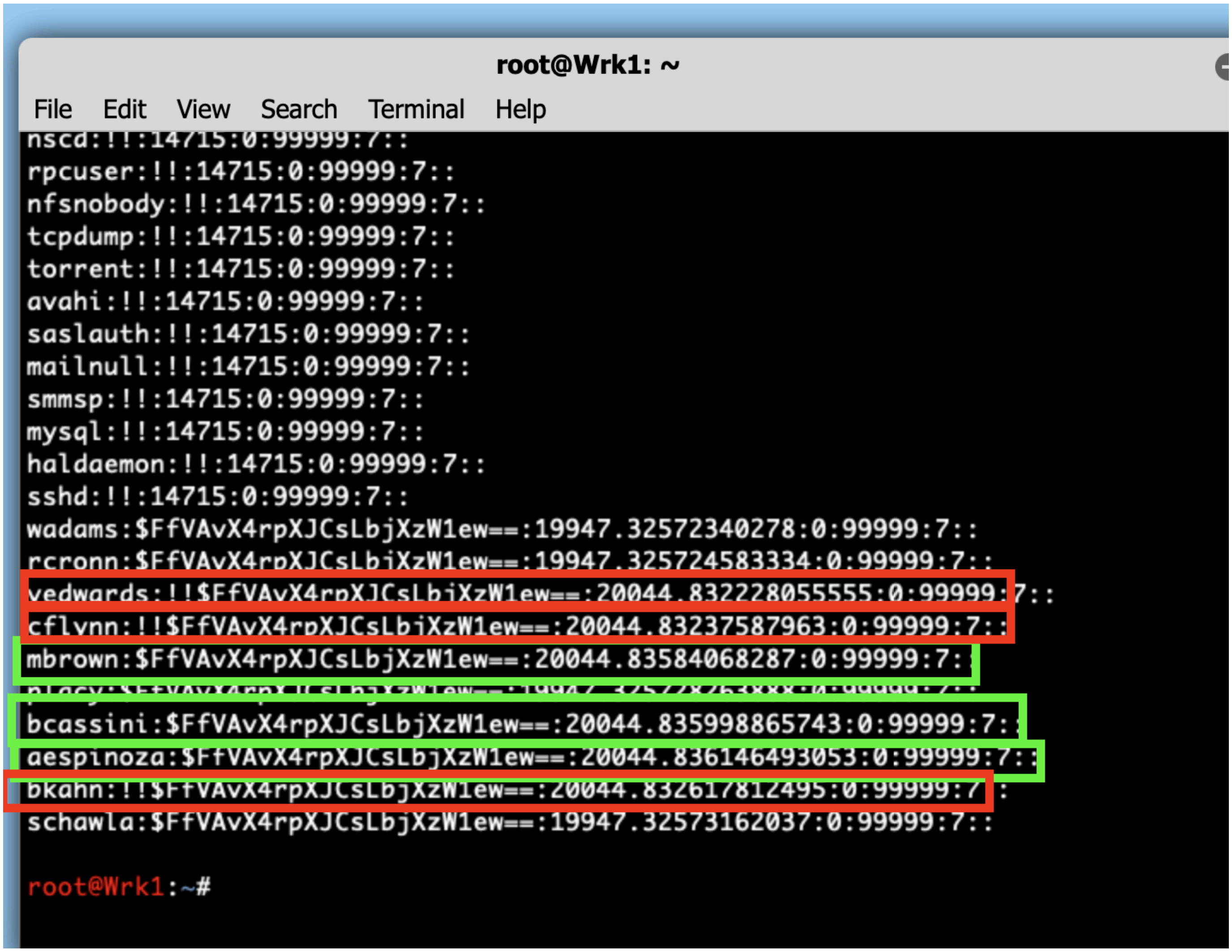
```
usermod: user bkhan does not exist
root@Wrk1:~# usermod --lock bkahn
root@Wrk1:~# usermod -U mbrown
root@Wrk1:~# usermod --unlock bcassini
root@Wrk1:~# usermod --unlock aespinoza
root@Wrk1:~#
```

We can see that the commands were successful because there are no error messages and the shell is prompting us for more input.

Lastly, now that we've locked and unlocked user accounts, let's query the /etc/shadow file to verify that we've done the correct operations on the right accounts. Since we are root simply type: "cat /etc/shadow"

We can see the unlocked accounts in green (which DOES NOT contain "!!") and the locked ones in Red (which DO contain a "!!"). This is how we can tell the status of the account.

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024

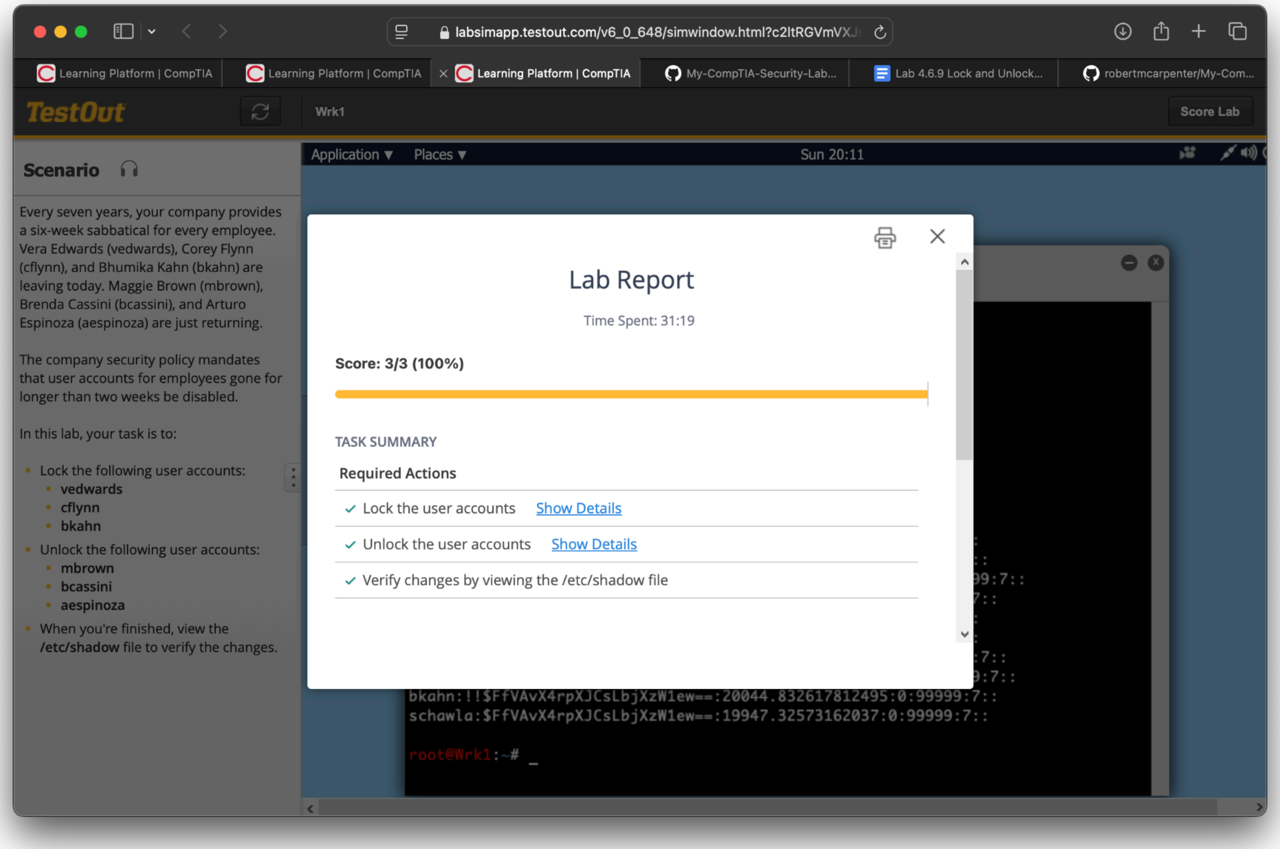


```
nscd:!!:14715:0:99999:7::
rpcuser:!!:14715:0:99999:7::
nfsnobody:!!:14715:0:99999:7::
tcpdump:!!:14715:0:99999:7::
torrent:!!:14715:0:99999:7::
avahi:!!:14715:0:99999:7::
saslauth:!!:14715:0:99999:7::
mailnull:!!:14715:0:99999:7::
smmsp:!!:14715:0:99999:7::
mysql:!!:14715:0:99999:7::
haldaemon:!!:14715:0:99999:7::
sshd:!!:14715:0:99999:7::
wadams:$FfVAvX4rpXJCsLbjXzW1ew==:19947.32572340278:0:99999:7::
rcronn:$FfVAvX4rpXJCsLbjXzW1ew==:19947.325724583334:0:99999:7::
vedwards:!!$FfVAvX4rpXJCsLbjXzW1ew==:20044.832228055555:0:99999:7::
cflynn:!!$FfVAvX4rpXJCsLbjXzW1ew==:20044.83237587963:0:99999:7::
mbrown:$FfVAvX4rpXJCsLbjXzW1ew==:20044.83584068287:0:99999:7::
placy:$FfVAvX4rpXJCsLbjXzW1ew==:19947.325728263888:0:99999:7::
bcassini:$FfVAvX4rpXJCsLbjXzW1ew==:20044.835998865743:0:99999:7::
aespinoza:$FfVAvX4rpXJCsLbjXzW1ew==:20044.836146493053:0:99999:7::
bkahn:!!$FfVAvX4rpXJCsLbjXzW1ew==:20044.832617812495:0:99999:7::
schawla:$FfVAvX4rpXJCsLbjXzW1ew==:19947.32573162037:0:99999:7::

root@Wrk1:~#
```

This now concludes the lab!

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024


labsimapp.testout.com/v6_0_648/simwindow.html?c2ltRGVmVXJ
Learning Platform | CompTIA
Learning Platform | CompTIA
Learning Platform | CompTIA
My-CompTIA-Security-Lab...
Lab 4.6.9 Lock and Unlock...
robertmcarpenter/My-Com...
TestOut
Wrk1
Score Lab
Application ▼
Places ▼
Sun 20:11

Scenario

Every seven years, your company provides a six-week sabbatical for every employee. Vera Edwards (vedwards), Corey Flynn (cflynn), and Bhumika Kahn (bkahn) are leaving today. Maggie Brown (mbrown), Brenda Cassini (bcassini), and Arturo Espinoza (aespinoza) are just returning.

The company security policy mandates that user accounts for employees gone for longer than two weeks be disabled.

In this lab, your task is to:

- Lock the following user accounts:
  - **vedwards**
  - **cflynn**
  - **bkahn**
- Unlock the following user accounts:
  - **mbrown**
  - **bcassini**
  - **aespinoza**
- When you're finished, view the **/etc/shadow** file to verify the changes.

Lab Report

Time Spent: 31:19

Score: 3/3 (100%)

TASK SUMMARY

Required Actions

- ✓ Lock the user accounts Show Details
- ✓ Unlock the user accounts Show Details
- ✓ Verify changes by viewing the /etc/shadow file

```
bkahn:!!$FfVAvX4rpXJCsLbjXzW1ew==:20044.832617812495:0:99999:7::
schawla:$FfVAvX4rpXJCsLbjXzW1ew==:19947.32573162037:0:99999:7::

root@Wrk1:~# _
```