

## Lab 4.6.8 Changing and Encrypting Password on Behalf of a User on a Linux System

*From TestOut CompTIA Security+ Course*

*Note: This Lab is very similar to the lab I did on 4.6.7 “Changing Password of Admin/Root Account.”*

In this lab, I will be changing the password for a given user on a Linux system.

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

**Salman Chawla (schawla) forgot his password and needs access to the resources on his computer. You are logged on as wadams. The password for the root account is 1worm4b8.**

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

- 1. Change the password for the schawla user account to G20oly04 (0 is a zero).**
- 2. Make sure the password is encrypted in the shadow file.”**

After reading this scenario I first see that in the requested Step #2 of this Lab, they would like us to make sure that the password we change is encrypted. In this case we know NOT TO USE the “usermod -p” command because although this command can change the password for a given user, it doesn’t store the password in encrypted format.

Instead, we’ll opt for the “passwd” binary to change the password for this user. Since the lab states we are logged in as the “wadams” account , and it doesn’t clarify if that account is an admin or part of the sudoers file (or even if the sudo binary is installed on this system!)

We can elevate privileges using the “su” command (which I believe stands for Super User). We can also pass “su” the -c flag which states for the shell to execute

Robert Carpenter

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

Sun November 17th 2024

the command we supply after -c as root. Alternatively we can just elevate the entire shell and login as root by just passing "su." Since it's not good practice to stay logged in as root other than for executing one command, we'll use that method.

Just to be sure let's query the man pages for passwd and su.

```
wadams@Wrk1: ~  
File Edit View Search Terminal Help  
Usage: su [OPTION]... [-] [USER [ARG]...]  
Change the effective user id and group id to that of USER.  
  
-, -l, --login           make the shell a login shell  
-c, --command=COMMAND    pass a single COMMAND to the shell with -c  
--session-command=COMMAND pass a single COMMAND to the shell with -c  
                        and do not create a new session  
-f, --fast               pass -f to the shell (for csh or tcsh)  
-m, --preserve-environment do not reset environment variables  
-p                       same as -m  
-s, --shell=SHELL        run SHELL if /etc/shells allows it  
--help                  display this help and exit  
--version                output version information and exit  
  
A mere - implies -l.  If USER not given, assume root.  
  
Report su bugs to bug-coreutils@gnu.org  
GNU coreutils home page: <http://www.gnu.org/software/coreutils/>  
General help using GNU software: <http://www.gnu.org/gethelp/>  
For complete documentation, run: info coreutils 'su invocation'
```

```
wadams@Wrk1: ~  
File Edit View Search Terminal Help  
Usage: passwd [options] [LOGIN]  
-k, --keep-tokens      keep non-expired authentication tokens  
-d, --delete           delete the password for the named account (root only)  
-l, --lock             lock the named account (root only)  
-u, --unlock          unlock the named account (root only)  
-f, --force           force operation  
-x, --maximum=DAYS    maximum password lifetime (root only)  
-n, --minimum=DAYS    minimum password lifetime (root only)  
-w, --warning=DAYS    number of days warning users receives before  
                      password expiration (root only)  
-i, --inactive=DAYS   number of days after password expiration when an  
                      account becomes disabled (root only)  
-S, --status          report password status on the named account (root  
                      only)  
--stdin              read new tokens from stdin (root only)  
  
Help options:  
-?, --help            Show this help message  
--usage              Display brief usage message
```

Based off what we see from the output I know the command I will need to enter to get this all done in one sweep is: `su -c "passwd schawla"`

1. Su = Super User
2. -c = COMMAND (pass a single command to the shell)
3. "Passwd schawla" (nested argument which gets executing after the su binary is called. We wrap this command in Quotes because it gets passed as a String

```
wadams@Wrk1:~# su -c "passwd schawla"  
Password:  
Changing password for user schawla
```

We see that "su" is asking us for the password. Since su involves the root account we supply the root account password which is given to us in the lab as `1worm4b8`

```
wadams@Wrk1:~# su -c "passwd schawla"
Password:
Changing password for user schawla.
New password: _
```

We now see that the shell is asking us for a new password for schawla. This means that the shell has moved on to the command that we supplied with the -c flag. This is then just becomes entering the requested new password from the lab to G2001y04. Enter in the password then enter it again to confirm.

```
wadams@Wrk1:~# su -c "passwd schawla"
Password:
Changing password for user schawla.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
wadams@Wrk1:~#
```

Finished!

Just kidding not so fast! We must verify that the password has been stored in an encrypted format! The lab asks us to verify the /etc/shadow file (where passwords are stored) for the existence of the password. If what we see in that file doesn't match the password we entered, then we know that the encryption was successful. Passwd command will not store passwords in clear text on the /etc/shadow file.

To query and view the /etc/passwd file, simply pass to the shell: "cat /etc/passwd" (note: we don't need the su command here because I can see the "#" root symbol on my terminal prompt meaning we have elevated privileges already)

```
wadams@Wrk1: ~  
File Edit View Search Terminal Help  
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:$FfVAvX4rpXJCslbjXzW1ew==:19947.325730671295:0:99999:7::  
schawla:$X0zRjiLm8j6yoPh8n6aRxw==:20044.807692488426:0:99999:7::  
wadams@Wrk1:~#
```

Amazing! Now we are finished for real! This now concludes this lab.

Robert Carpenter

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

Sun November 17th 2024

The screenshot shows the TestOut application interface. On the left, the 'Scenario' panel contains the following text: 'Salman Chawla (schawla) forgot his password and needs access to the resources on his computer. You are logged on as wadams. The password for the root account is 1worm4b8. In this lab, your task is to: Change the password for the schawla user account to G20oly04 (0 is a zero). Make sure the password is encrypted in the shadow file.' Below this, a warning icon and text state: 'Do not use the usermod -p command to change the password, as this stores the unencrypted version of the password in the /etc/shadow file.'

The main window displays a 'Lab Report' modal. The modal title is 'Lab Report' with a 'Time Spent: 45:23'. The score is 'Score: 1/1 (100%)' with a full orange progress bar. Under 'TASK SUMMARY', the 'Required Actions' section shows a single item: 'Set the password for user schawla to G20oly04' with a green checkmark. The 'EXPLANATION' section, marked with a headset icon, says 'Complete this lab as follows:'. The background shows a terminal window with the prompt 'wadams@Wrk1:~#'