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

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."**

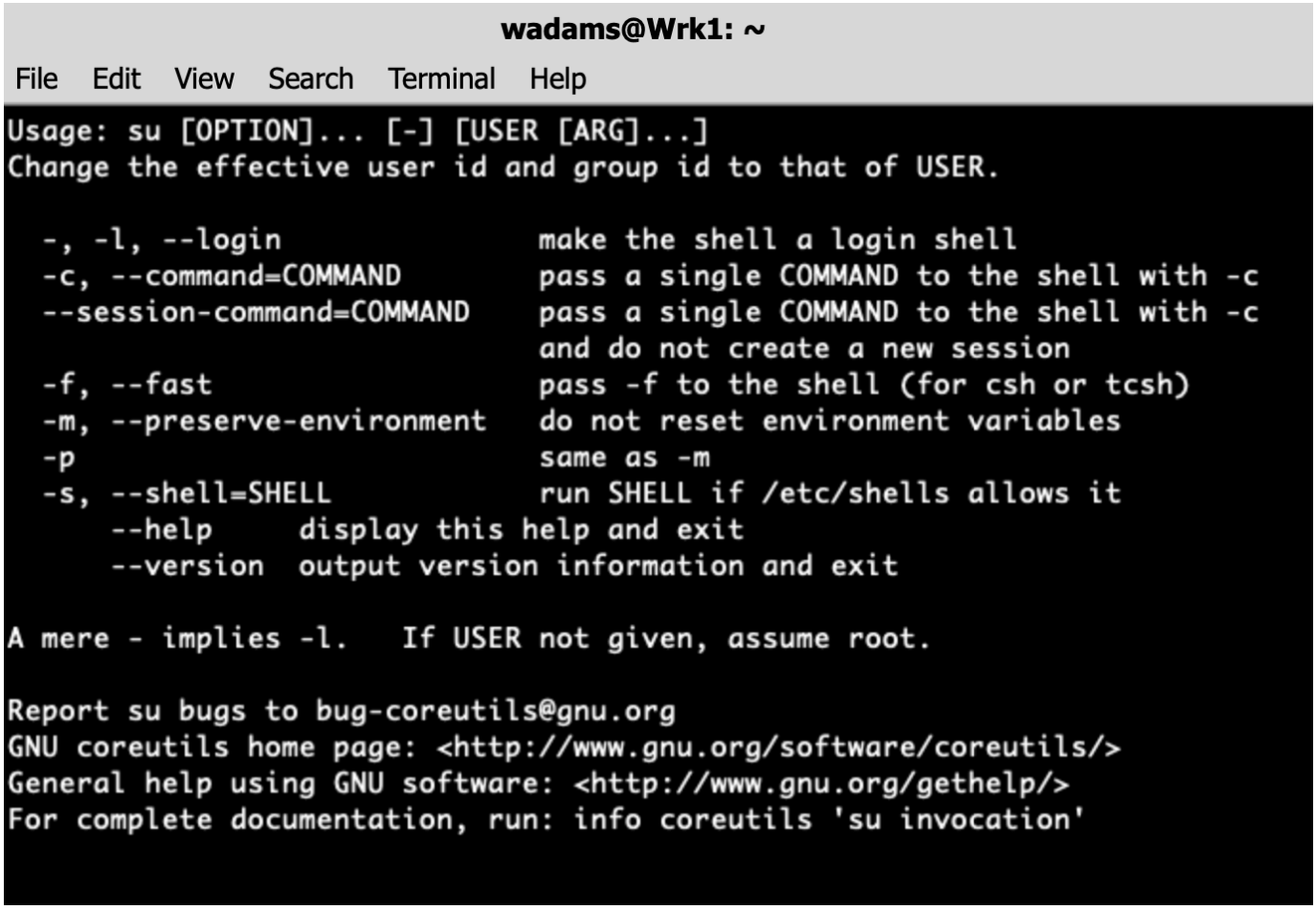
After reading this scenario I first see that in the requested Step #2 of this Lab, they would like us to make sure that the password we change is encrypted. In this case we know NOT TO USE the "usermod -p" command because although this command can change the password for a given user, it doesn't store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

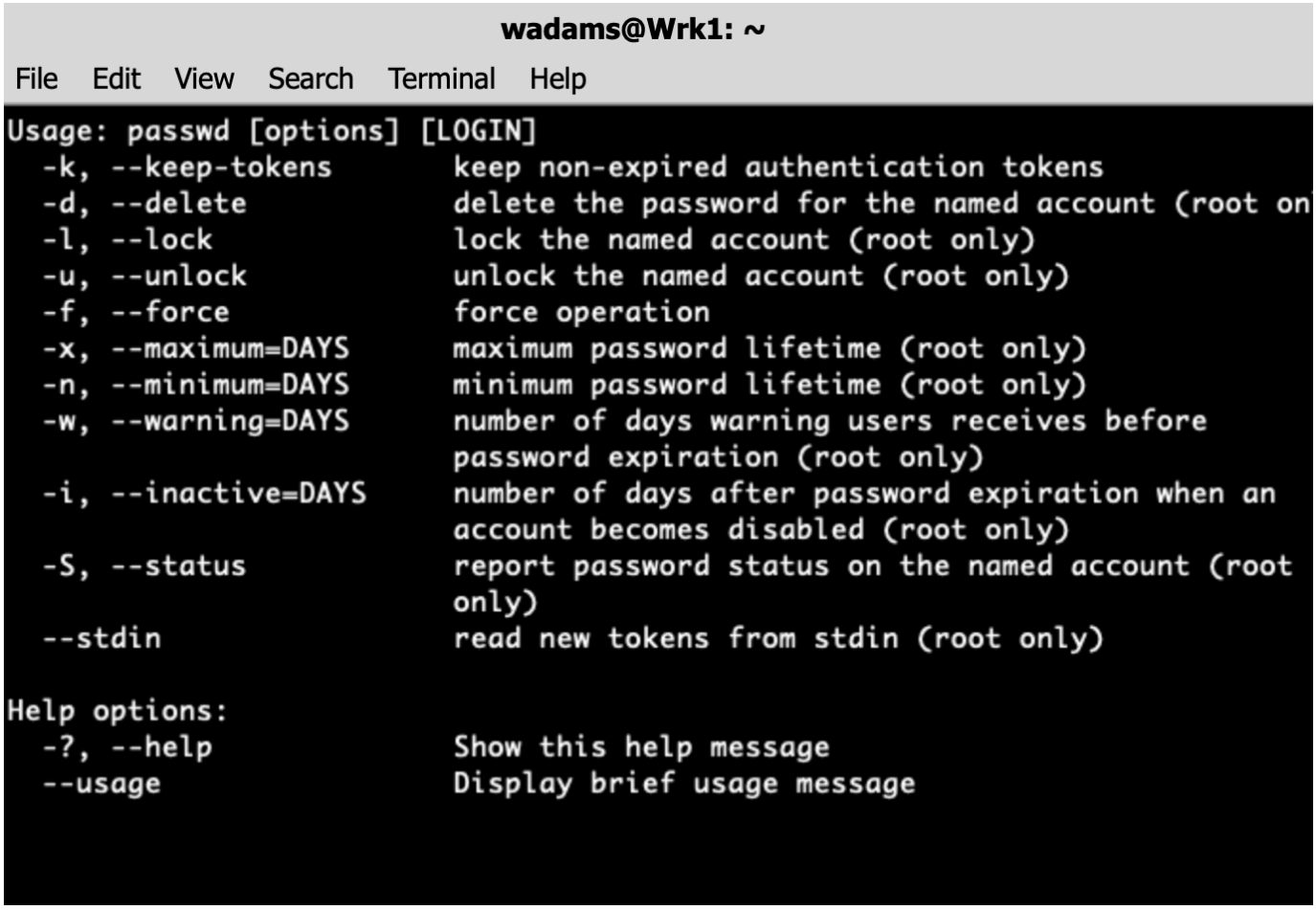
We can elevate privileges using the "su" command (which I believe stands for Super User). We can also pass "su" the -c flag which states for the shell to execute

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.

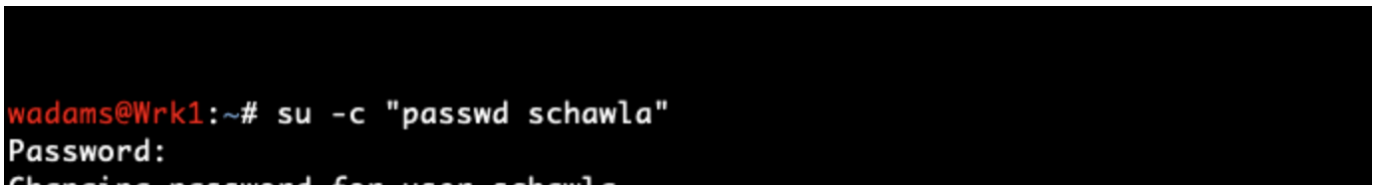


Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



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



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**

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

```
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 **G20oly04.** Enter in the password then enter it again to confirm.

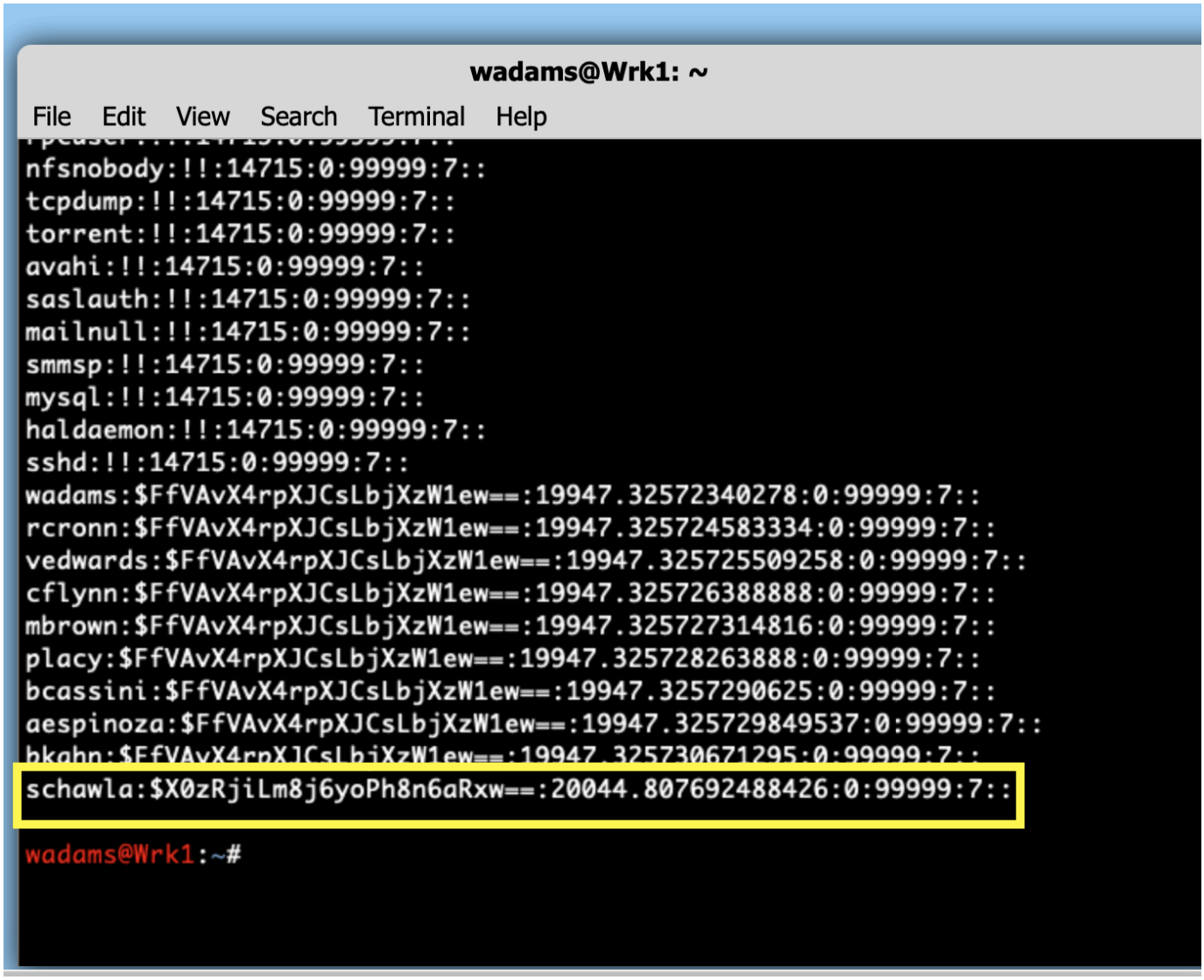
```
wadams@Wrk1:~# su -c "passwd schawla"
Password:
Changing password for user schawla.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
wadams@Wrk1:~#
```

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/shadow" (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)

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



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

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