

TestOut CompTIA Security + LAB 4.6.4: Create a User account On a Linux System

In this lab, I will be creating a user for the VP of Marketing on a company owned Linux system (hypothetical). The scenario for this lab is as follows:

“The VP of marketing has told you that Paul Denunzio will join the company as a market analyst in two weeks. You need to create a new user account for him. You are logged in as root, so the **sudo** command is unnecessary.

In this lab, your task is to:

- Create the **pdenunzio** user account.
 - Include the full name, **Paul Denunzio**, as a comment for the user account.
- Set **eye8cereal** as the password for the user account.
- When you are finished, view the **/etc/passwd** file to verify the creation of the account.
- Answer the question: What is Paul Denunzio’s User ID (UID) ?”

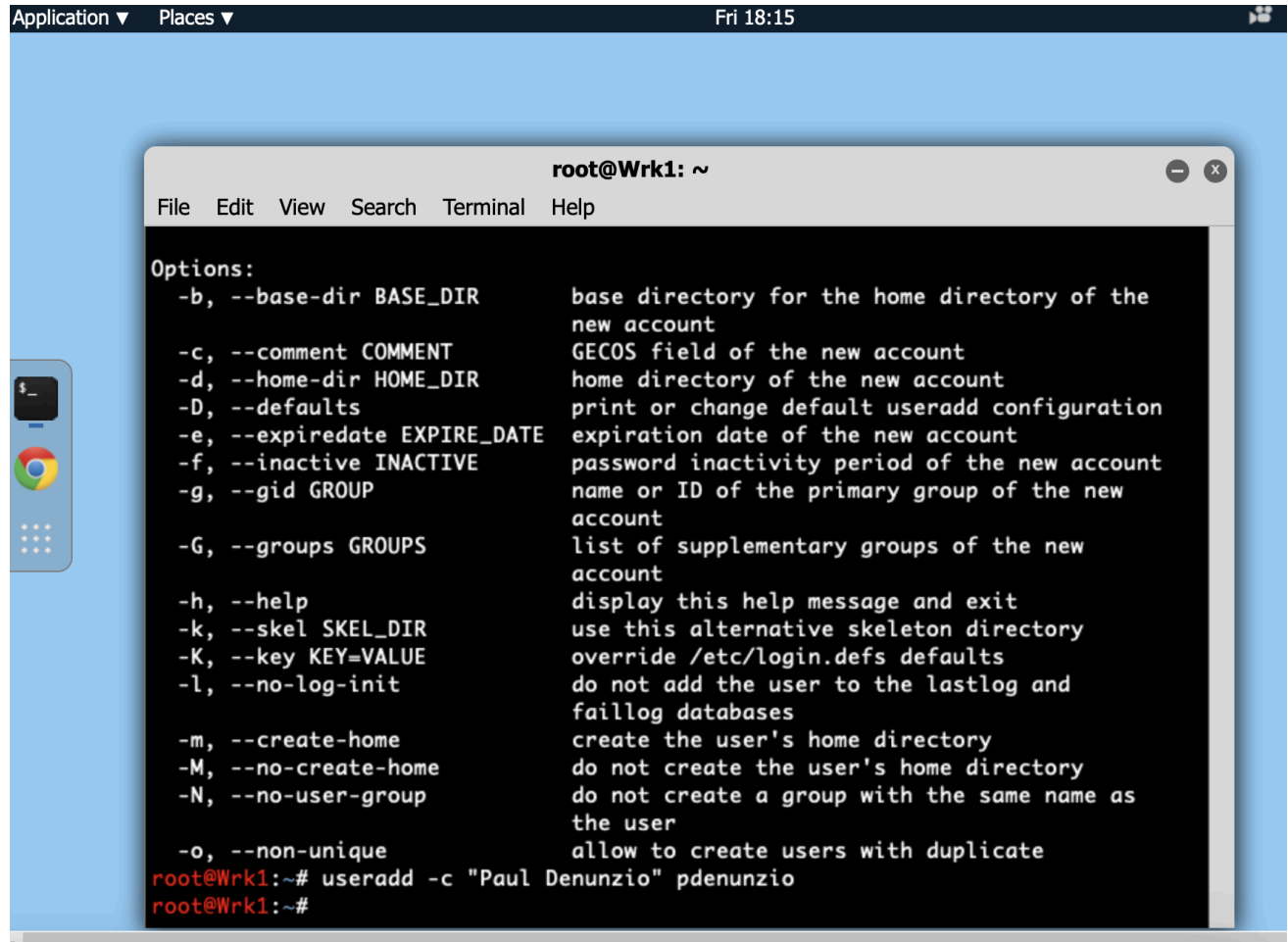
Since this user does not exist on this system we will need to add them. In order to do that GNU/Linux has a built in core util called “useradd” - which as you guessed, adds users to the system! To see what we can do with that command lets type “man useradd” :

The screenshot shows a TestOut lab environment. On the left, a 'Scenario' panel contains the following text: 'The VP of marketing has told you that Paul Denunzio will join the company as a market analyst in two weeks. You need to create a new user account for him.' Below this, a message states: 'You are logged in as root, so the sudo command is unnecessary.' The task instructions are: 'In this lab, your task is to: Create the pdenunzio user account. Include the full name, Paul Denunzio, as a comment for the user account. Set eye8cereal as the password for the user account. When you are finished, view the /etc/passwd file to verify the creation of the account. Answer the question.'

On the right, a terminal window titled 'root@Wrk1: ~' displays the 'Usage: useradd [options] LOGIN' and 'Options:' for the 'useradd' command. The options listed are:

- b, --base-dir BASE_DIR: base directory for the home directory of the new account
- c, --comment COMMENT: GECOS field of the new account
- d, --home-dir HOME_DIR: home directory of the new account
- D, --defaults: print or change default useradd configuration
- e, --expiredate EXPIRE_DATE: expiration date of the new account
- f, --inactive INACTIVE: password inactivity period of the new account
- g, --gid GROUP: name or ID of the primary group of the new account
- G, --groups GROUPS: list of supplementary groups of the new account
- h, --help: display this help message and exit
- k, --skel SKEL_DIR: use this alternative skeleton directory
- K, --key KEY=VALUE: override /etc/login.defs defaults
- l, --no-log-init: do not add the user to the lastlog and faillog databases
- m, --create-home: create the user's home directory
- M, --no-create-home: do not create the user's home directory
- N, --no-user-group: do not create a group with the same name as the user
- o, --non-unique: allow to create users with duplicate

We can see that we can use the “-c” flag to add a comment for this user. In this case we are asked to put their full name in the Comment field.



The screenshot shows a terminal window titled "root@Wrk1: ~" with a menu bar containing "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal displays the "Options:" for the "useradd" command, listing various flags and their descriptions. The options are:

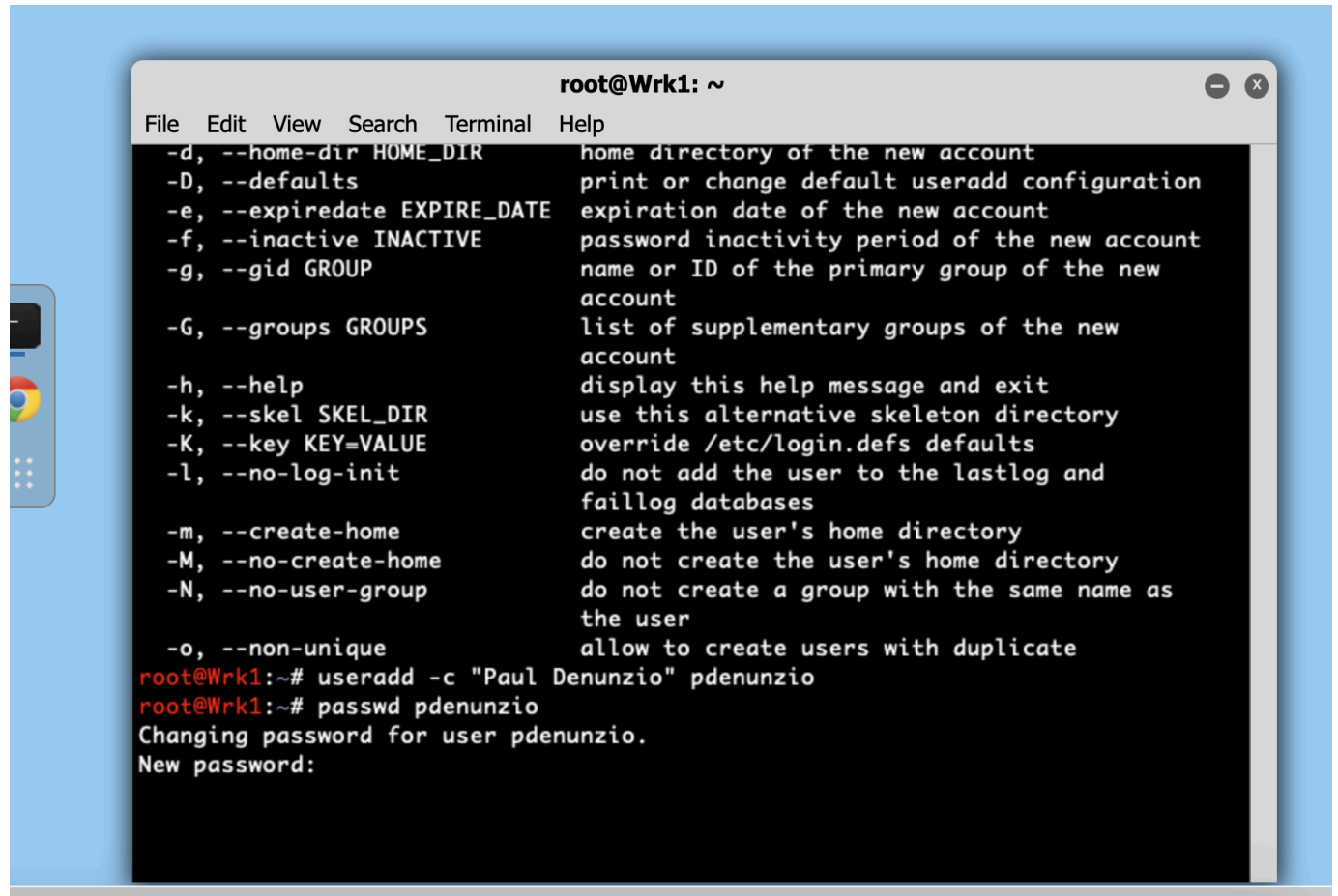
- b, --base-dir BASE_DIR: base directory for the home directory of the new account
- c, --comment COMMENT: GECOS field of the new account
- d, --home-dir HOME_DIR: home directory of the new account
- D, --defaults: print or change default useradd configuration
- e, --expiredate EXPIRE_DATE: expiration date of the new account
- f, --inactive INACTIVE: password inactivity period of the new account
- g, --gid GROUP: name or ID of the primary group of the new account
- G, --groups GROUPS: list of supplementary groups of the new account
- h, --help: display this help message and exit
- k, --skel SKEL_DIR: use this alternative skeleton directory
- K, --key KEY=VALUE: override /etc/login.defs defaults
- l, --no-log-init: do not add the user to the lastlog and faillog databases
- m, --create-home: create the user's home directory
- M, --no-create-home: do not create the user's home directory
- N, --no-user-group: do not create a group with the same name as the user
- o, --non-unique: allow to create users with duplicate

Below the options, the command "useradd -c 'Paul Denunzio' pdenunzio" is executed, and the prompt returns to "root@Wrk1:~#".

Now that we have set this user up in our system, we will need to give them a password. No passwords = a system that's not secure! Just a friendly reminder to ourselves that sometimes security involves extra steps, and if we forget to do that we are giving an attacker the ability to login to this system without authentication.

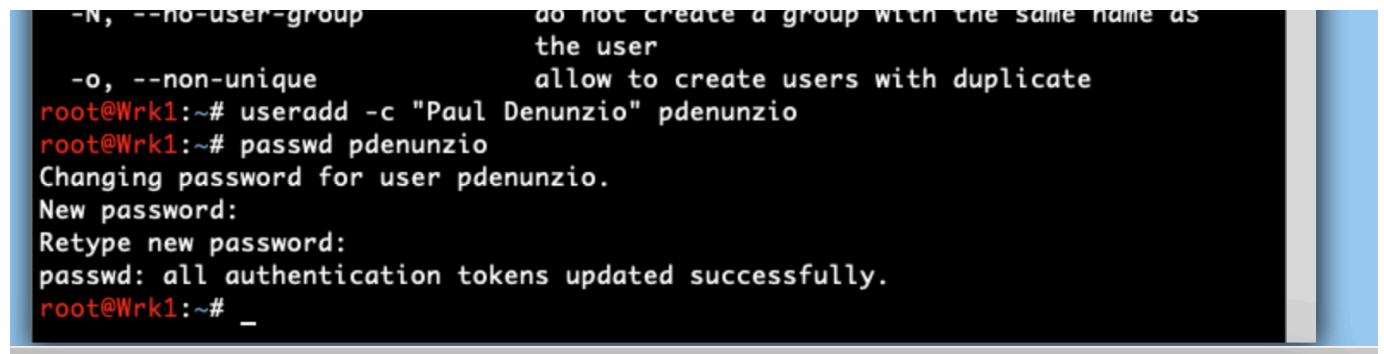
To assign a password to the "pdenunzio" user we use the "passwd" command. Notice that it's spelled differently than the actual word "PASSWORD."

We call the passwd command and supply the user we would like to set the password for:



```
root@Wrk1: ~
File Edit View Search Terminal Help
-d, --home-dir HOME_DIR      home directory of the new account
-D, --defaults               print or change default useradd configuration
-e, --expiredate EXPIRE_DATE expiration date of the new account
-f, --inactive INACTIVE      password inactivity period of the new account
-g, --gid GROUP              name or ID of the primary group of the new
                             account
-G, --groups GROUPS          list of supplementary groups of the new
                             account
-h, --help                   display this help message and exit
-k, --skel SKEL_DIR          use this alternative skeleton directory
-K, --key KEY=VALUE          override /etc/login.defs defaults
-l, --no-log-init             do not add the user to the lastlog and
                             faillog databases
-m, --create-home            create the user's home directory
-M, --no-create-home         do not create the user's home directory
-N, --no-user-group          do not create a group with the same name as
                             the user
-o, --non-unique              allow to create users with duplicate
root@Wrk1:~# useradd -c "Paul Denunzio" pdenunzio
root@Wrk1:~# passwd pdenunzio
Changing password for user pdenunzio.
New password:
```

The Lab calls for us to set a password of “eye8cereal.” On a tangent here, this password is not very secure looking so in the real world you will want a more complex password of long length , various characters, and numbers. We will proceed with this password since it’s just for demonstration purposes:



```
-N, --no-user-group          do not create a group with the same name as
                             the user
-o, --non-unique              allow to create users with duplicate
root@Wrk1:~# useradd -c "Paul Denunzio" pdenunzio
root@Wrk1:~# passwd pdenunzio
Changing password for user pdenunzio.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
root@Wrk1:~# _
```

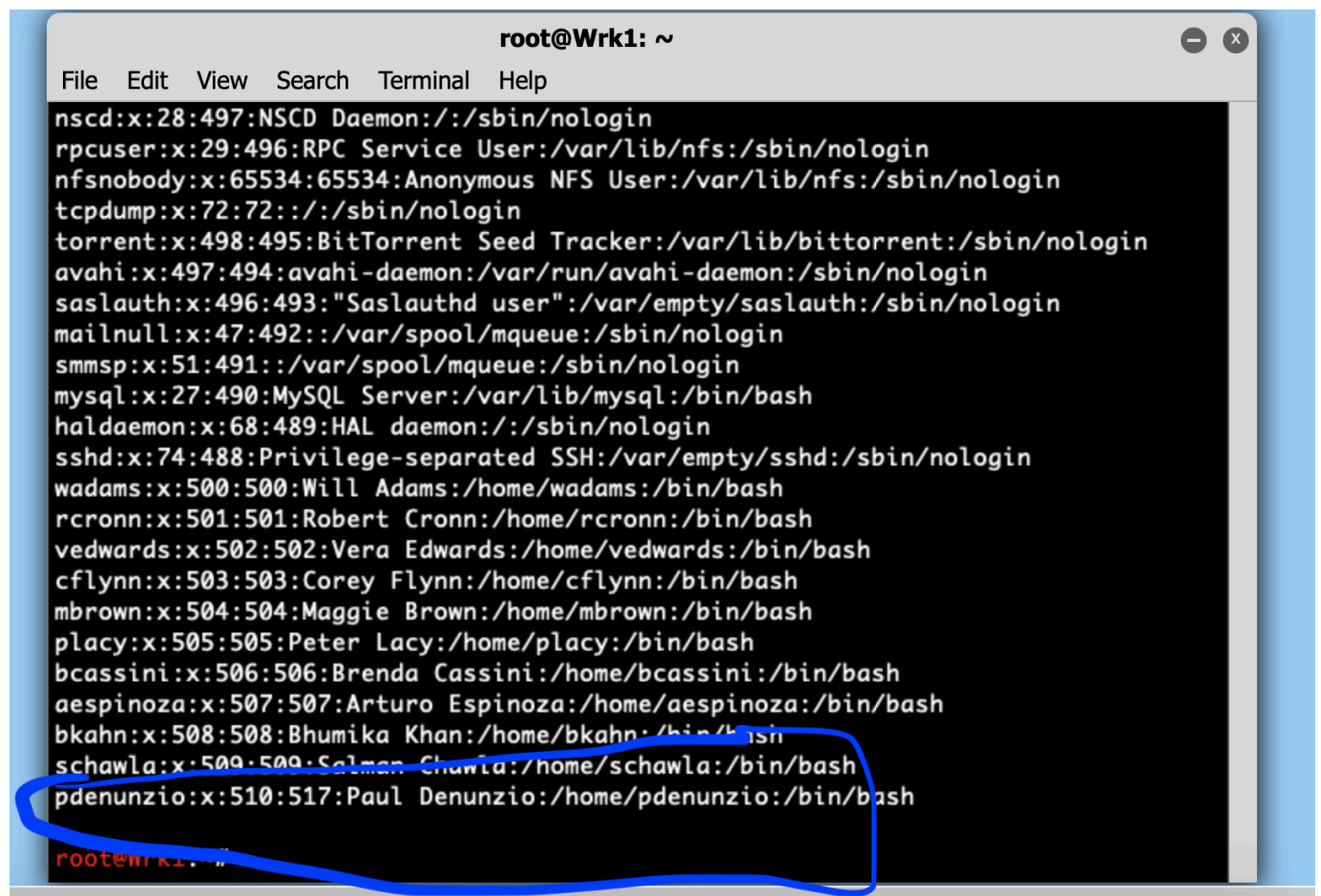
Robert Carpenter

github.com/robertmcarpenter

Fri November 15th 2024

Notice that the password we typed doesn't show up in the terminal. Not even asterisks are present to obscure the password. This is because if an attacker can see the asterisks (*) they can count the length of characters the password is and adjust their attacks accordingly (Example: 8 asterisks would imply a password of 8 characters and the attacker can adjust their Dictionary or Rainbow Tables to a password character length of $n = 8$). This is secure by design! Praise FOSS!

Now that we're done setting the user and password, we will want to query the "/etc/passwd" file to verify that we have added this user to the system. To do that, we will use the "cat" command (which I believe is an acronym for Copy At Terminal) to display the contents of that file. Issuing the "cat /etc/passwd" command we see:

A terminal window titled "root@Wrk1: ~" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal displays the output of the "cat /etc/passwd" command, listing system users and regular users. The entry for "pdenunzio" is circled in blue. The terminal text is as follows:

```
root@Wrk1: ~  
File Edit View Search Terminal Help  
nscd:x:28:497:NSCD Daemon:/:sbin/nologin  
rpcuser:x:29:496:RPC Service User:/var/lib/nfs:/sbin/nologin  
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin  
tcpdump:x:72:72:/:sbin/nologin  
torrent:x:498:495:BitTorrent Seed Tracker:/var/lib/bittorrent:/sbin/nologin  
avahi:x:497:494:avahi-daemon:/var/run/avahi-daemon:/sbin/nologin  
saslauth:x:496:493:"Saslauthd user":/var/empty/saslauth:/sbin/nologin  
mailnull:x:47:492:/:var/spool/mqueue:/sbin/nologin  
smmisp:x:51:491:/:var/spool/mqueue:/sbin/nologin  
mysql:x:27:490:MySQL Server:/var/lib/mysql:/bin/bash  
haldaemon:x:68:489:HAL daemon:/:sbin/nologin  
sshd:x:74:488:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
wadams:x:500:500:Will Adams:/home/wadams:/bin/bash  
rcronn:x:501:501:Robert Cronn:/home/rcronn:/bin/bash  
vedwards:x:502:502:Vera Edwards:/home/vedwards:/bin/bash  
cflynn:x:503:503:Corey Flynn:/home/cflynn:/bin/bash  
mbrown:x:504:504:Maggie Brown:/home/mbrown:/bin/bash  
placy:x:505:505:Peter Lacy:/home/placy:/bin/bash  
bcassini:x:506:506:Brenda Cassini:/home/bcassini:/bin/bash  
aespinoza:x:507:507:Arturo Espinoza:/home/aespinoza:/bin/bash  
bkahn:x:508:508:Bhumika Khan:/home/bkahn:/bin/bash  
schawla:x:509:509:Salman Chawla:/home/schawla:/bin/bash  
pdenunzio:x:510:517:Paul Denunzio:/home/pdenunzio:/bin/bash  
root@Wrk1: ~
```

Robert Carpenter

github.com/robertmcarpenter

Fri November 15th 2024

EXCELLENT ! We have added this user to the System. Now we can answer the final question of the lab which asks:

“What is the user ID for the Paul Denunzio?”

We can see from the output that his UID is 510. This is the answer!

This now concludes this Lab on adding a user to a Linux System.

TestOut Wrk1 Answer Questions

Scenario

The VP of marketing has told you that Paul Denunzio will join the company as a market analyst in two weeks. You need to create a new user account for him.

You are logged in as root, so the **sudo** command is unnecessary.

In this lab, your task is to:

- Create the **pdenunzio** user account.
 - Include the full name, **Paul Denunzio**, as a comment for the user account.
- Set **eye8cereal** as the password for the user account.

When you are finished, view the **/etc/passwd** file to verify the creation of the account.

Answer the question.

Lab Report
Time Spent: 1:28:36

Score: 4/4 (100%)

TASK SUMMARY

Required Actions & Questions

- ✓ Create the pdenunzio user account
- ✓ Add Paul Denunzio as a comment for the user account
- ✓ Set eye8cereal as the password
- ✓ **Q1: What is Paul's user ID?**
Your answer: **510**

bkahn:x:508:508:Bhumika Khan:/home/bkahn:/bin/bash
schawla:x:509:509:Salman Chawla:/home/schawla:/bin/bash
pdenunzio:x:510:517:Paul Denunzio:/home/pdenunzio:/bin/bash

root@Wrk1:~#

Score Lab