1. Start the RH Academy Lab VMs.
2. Log onto to workstation as user student, password = student
3. Switch to root as follows: **su –**
   1. Password is **redhat**
4. Run **less -N /etc/sudoers**
   1. The less command opens sudoers and allows the up/down arrows to navigate
   2. -N shows line numbers
5. Down arrow until lines 100 and 107 are both showing.

|  |
| --- |
| **Take a screenshot of the sudoers file that includes lines 100 – 107 – paste here** |

1. Notice that the user root on all hosts using all users can run all commands ‘root ALL=(ALL) ALL’
   1. Notice that the same is true of the wheel group
   2. Any user that is a member of the wheel group can run commands as any other user (including the super user) using sudo
2. Type **q** to exit
3. Now let’s see who is a member of the wheel group. Run **less -N /etc/group** and look for the wheel group (on mine, it’s on line 11).

|  |
| --- |
| **Take a screenshot of the content of wheel, making sure that the entry for wheel shows – paste here** |

1. Notice that the wheel group, (x in place of possible password), gid = 10, has student as a member
   1. So, as long as we’re logged on as this user, when we need to run commands requiring root privileges:
      1. We don’t need to switch to root (su -)
      2. We can just append sudo to the command (superuser do)
2. Type **q** to exit
3. Run **exit** to exit out of root’s logon and back to your regular user
4. Create a user named Gertrude with the following command: **useradd Gertrude**
5. You see that you need super user privilege
6. Run the command again as **sudo useradd Gertrude**
   1. You will need to provide the password to user student, which is student
7. Give Gertrude the password of Password01 by running **sudo passwd Gertrude**
   1. Make the new password Password01
8. Look for Gertrude in /etc/passwd by running **less -N /etc/passwd**
   1. You don’t have to sudo when viewing passwd because any user can view this file
9. Arrow down to the bottom to see the entry for Gertrude
10. Notice the following:
    1. Gertrude’s uid is 1003 (unless you’ve created users before this), as is the gid of Gertrude’s primary group
    2. Gertrude’s home directory is /home/Gertrude
    3. When Gertrude logs on, the shell will be bash
11. Type **q** to exit
12. The user Gertrude was at the bottom of passwd’s list because that account was the last one created. What if that wasn’t the case? Is there an easier way to just get the information from passwd that we need without having to manually search? Yes there is.
13. Use grep to display lines in the passwd file that contain the string Gertrude by running
    1. **grep Gertrude /etc/passwd**

|  |
| --- |
| **Take a screenshot of the output of the above instruction’s grep command – paste here** |

1. Verify that Gertrude’s password was set by seeing if there is an entry for Gertrude in the shadow file.
   1. **sudo grep Gertrude /etc/shadow** provide the password for student (if requested)

|  |
| --- |
| **Take a screenshot of the output of the above instruction’s grep command – paste here** |

1. Switch to user Gertrude by running **su – Gertrude** provide the password of **Password01**
2. Run **pwd** to verify that your path of working directory is Gertrude’s home directory
3. Create a file by running **touch GertrudeFile**
4. Run **ls -l** Verify that Gertrude and the Gertrude group own the file named GertrudeFile
5. Run **exit** to return back to your student user’s environment
6. Remember that you’re logged on as student now. Run **ls -l /home/Gertrude/**
   1. Notice that you don’t have permission to access
7. root can access anything. Up arrow to bring the previous command back, and append a sudo to it:
   1. **sudo ls -l /home/Gertrude/**

|  |
| --- |
| **Take a screenshot of the output of the above instruction’s ls -l command – paste here** |

1. Copy the /home/Gertrude/GertrudeFile to your home directory, and renaming it, by running the following:
   1. **sudo cp /home/Gertrude/GertrudeFile ~/studentGertrudeFile**
2. Run **ls -l studentGertrudeFile**

|  |
| --- |
| **Take a screenshot of the output of the above instruction’s ls -l command – paste here** |

1. Recall that the file copied (/home/Gertrude/GertrudeFile) was owned by Gertrude. But /home/student /studentGertrudeFile is owned by root, not you
   1. The cp command was run as root, so the owner of the copied file is root
2. Now, lock Gertrude’s account by running **sudo usermod -L Gertrude**
3. Verify by running **sudo grep Gertrude /etc/shadow**

|  |
| --- |
| **Take a screenshot of the output of the above instruction’s grep command – paste here** |

1. Notice the exclamation point after the user name 
   1. This exclamation point is the sign of a locked account
2. Now unlock the Gertrude account by running **sudo usermod -U Gertrude**
3. Verify the unlocking by running (or up arrowing to rerun) **sudo grep Gertrude /etc/shadow**

|  |
| --- |
| **Take a screenshot of the output of the above instruction’s grep command – paste here** |

1. If the account is unlocked, there will no longer be an exclamation point after the user name
2. Now, create a new group named myNewGroup by running **sudo groupadd myNewGroup**
3. Verify that the group exists by running **less /etc/group** and arrowing to the bottom
   1. You could have also just used grep if you were only interested in seeing myNewGroup info
4. Type **q** to exit
5. Change the name of this group to LabGroup by running **sudo groupmod -n LabGroup myNewGroup**
6. Verify with grep - **grep LabGroup /etc/group**
7. Add Gertrude to LabGroup by running **sudo gpasswd -a Gertrude LabGroup**
8. Also add the student user to LabGroup. **sudo gpasswd -a student LabGroup**
9. Verify the membership by rerunning **grep LabGroup /etc/group**
10. Remove student and Gertrude from LabGroup. Run the following:
    1. **sudo gpasswd -d student LabGroup**
    2. **sudo gpasswd -d Gertrude LabGroup**  (you can up arrow the previous command and edit it)
11. Add those users back to the group, but this time with a single command:
    1. **sudo gpasswd -M student,Gertrude LabGroup**
12. Verify the membership by rerunning **grep LabGroup /etc/group**

|  |
| --- |
| **Take a screenshot of the output of the above instruction’s grep command – paste here** |

1. Finally, remove LabGroup with the following command: **sudo groupdel LabGroup**
2. Now, do the specified Guided Exercises from Chapter 6 of Red Hat Academy. Take the requested history screenshots and paste to the document as well.
3. Guided Exercise: **Gain Superuser Access -** chapter 6, section 4

|  |
| --- |
| **Take a screenshot of the output of the history command – paste here** |

1. Guided Exercise: **Manage Local User Accounts -** chapter 6, section 6

|  |
| --- |
| **Before exiting: Take a screenshot of the output of the history command – paste her****e** |

1. Guided Exercise: **Manage Local Group Accounts** - chapter 6, section 8

|  |
| --- |
| **Before exiting: Take a screenshot of the output of the history command – paste here** |

1. Guided Exercise: **Manage User Passwords -** chapter 6, section 10

|  |
| --- |
| **Before exiting: Take a screenshot of the output of the history command – paste here** |

Upload the document of screenshots to Canvas