WIIT 7780 Lab 5: Understanding Basic Security Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 1**

Sign into your Ubuntu Desktop with credentials provided by your Instructor

Exercise 1: Viewing Account & Group Configuration Files

1. Open a Terminal window
2. At the prompt, type **less /etc/passwd** and press Enter. View the /etc/passwd file and pick a standard user account to use in this exercise. Record the account’s username: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
3. Press **q** to quit the less utility.
4. Type **grep *Username* /etc/passwd** and press Enter. Don’t actually type *Username*, but instead enter the account username you recorded in step #4. You should see *Username*’s record in the /etc/passwd file.
5. Record the *Username* account’s data information for each field:  
     
   a) username: \_\_\_\_\_\_  
     
   b) password: \_\_\_\_\_  
     
   c) UID: \_\_\_\_\_  
     
   d) GID: \_\_\_\_  
     
   e) Full Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   f) Home Directory:\_\_\_\_\_\_\_\_\_\_\_\_  
     
   g) Default Shell \_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   There are seven data fields in each /etc/passwd record. The fields are separated by colons (:). Note: The password is an x because the passwords are not stored in this file. Also note that the “Full Name” field is also called the “Comment” field.

Exercise 1: Viewing Account & Group Configuration Files (continued)

1. Type **sudo** **grep *Username* /etc/shadow** and press Enter. Don’t actually type *Username*, but instead enter the account username you recorded in step #4. You should see *Username*’s record in the /etc/shadow file.
2. Record the *Username* account’s data information for each field:  
     
   a) Username: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   b) Password: (Don’t record this one.)  
     
   c) Last modified: \_\_\_\_\_\_\_\_\_\_\_\_  
     
   d) Min days: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   e) Max days:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   f) Days warn:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   g) Disabled days \_\_\_\_\_\_\_\_\_\_\_\_  
     
   h) Expire \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   There are eight active data fields in each /etc/shadow record. The fields are separated by colons (:). The password displayed is actually a salted hash and not a plain text password. Note: Many of the fields may be blank.
3. Type **grep *Username* /etc/group** and press Enter. Don’t actually type *Username*, but instead enter the account username you recorded in step #4. You should see *Username*’s record in the /etc/group file.
4. Record the group’s data information for each field. (Pick one group, if *Username* is in more than one group.)  
     
   a) Group (aka Group Name): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   b) Password: \_\_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   c) GID: \_\_\_\_\_\_\_\_\_\_\_\_  
     
   d) Users: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (It’s okay if there are no users to list.)  
     
   There are four data fields in each /etc/group record. The fields are separated by colons. Note: The password is an x because the passwords are not stored in this file.
5. Type **exit** and press Enter to log out of the root user account.

Exercise 2: Using Account Tools to Discover Your Identity

1. Open a Terminal window
2. Type **whoami** and press Enter. You should see displayed the standard user account’s name you just logged into.
3. Type **who am i** and press Enter. Notice the information is similar to the information displayed in the preceding step.
4. Type **id** and press Enter. This command shows a lot more additional information than the whoami command.
5. Record the additional information that the id command displays below:
6. Try out the different options available with the id command from Table 12.1 in the book (or tutorial).

Exercise 3: Using Account Tools to Discover Who is Online

1. Open a Terminal window
2. Type **whoami** and press Enter. You should see root displayed.
3. Type **who** and press Enter. Who is logged on to your Linux system? Record the usernames below:  
   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   The who command shows who is currently logged on to your Linux system.
4. Type **who -q** and press Enter. Notice that you are given summary information of what usernames are currently accessing the system.
5. Type **w** and press Enter. There is quite a lot of information displayed here. Notice that this is a display of who is online and gives you greater detail than the who command did.
6. Type **exit** to log out of the root account.