**Lab-2. Authentication & Access Control**

**Submission:**

You will compose a lab report that documents each step you take, including screenshots to illustrate the effects of commands you type, and describing your observations.

Contents

[**Lab 2.1. Password policies (OS: MS Windows)** 1](#_Toc50964002)

[**Lab 2.2. Ubuntu** 5](#_Toc50964003)

# **Lab 2.1. Password policies (OS: MS Windows)**

In this lab, you will learn how to modify the following:

* The local security policy
* The **Minimum password length** password policy
* The **Do not display username in logon screen** security option
* The **account lockout threshold** account lockout policy
* The **Reset accout lockout counter** accout lockout policy
* **Activity 1: (Create a new user)**
* Log on to the system as Admin (leave password blank).
* Click Start 🡪Control Panel 🡪 Users Accounts
* Click Create a New Account
* **Activity 2: (Password Policy Settings for Length)**

***Step One:***

(1.) Continuing in **Control Panel 🡪 Administrative Tools 🡪 Local Security Policy.**

(2.) Expand **Account Policies**.

(3.) Click on the **Password Policy** option.

\*\*IMPORTANT\*\* Make sure all values (except maximum password age) is either **0 or Disabled**

(4.) Double-click **Minimum password length**.

(5.) In the **Minimum password length properties** window, change the value from 0 to 9.

(6.) Click **OK**.

(7.) Close **ALL** windows and log off as **Admin**.

***Step Two:***

(1.) Log on as **User1** (use password created in Activity 1.)

(2.) **Start 🡪 Control Panel 🡪** (switch to Classic View if necessary) **User Accounts**.

(3.) Click **Change password**…, for **User1**.

(4.) Type in the following information that's bold:

Old Password: **user1**

New Password: **password**

Confirm New Password: **password**

\*\*CLICK Change Password\*\*

(5.) You will receive a message.

QUESTION? What is the message you received? (Write this message down.)\*

(6.) Try assigning **password1** as the new password.

QUESTION? Was password1 successful?

(7.) Close **ALL** windows and Log off as **user1**

* **Activity 3: (Password Policy Settings for Complexity)**

***Step One:***

(1.) Log on to the system as an **Admin** (leave password blank).

(2.) Click **Start 🡪 Control Panel 🡪 Administrative Tools 🡪 Local Security Policy**.

(3.) Expand **Account Policies** (if not already).

(4.) Click on the **Password Policy** option.

(5.) Double-click **Passwords must meet complexity requirements**.

(6.) Click the **Enable** radio button.

(7.) Click **OK**.

(8.) Close **ALL** windows and log off as **Admin**.

***Step Two:***

(1.) Log on as **User1** (password is set as password1.)

(2.) **Start🡪 Control Panel 🡪 User Accounts.**

(3.) Click **Change my password**…, for **User1**.

(4.) Type in the following information that is in bold:

Old Password: **password1**

New Password: **password**

Confirm New Password: **password**

\*\*CLICK Change Password\*\*

(5.) You will receive a message.

QUESTION? What is the message you received? (Write this message down.)\*

(6.) Try assigning Password1 as the new password. (Was this successful?)

Note: the old password is still password1.

(7.) Close ALL windows and log off as user1.

QUESTION? List all possible settings that can be configured for the Windows Local Password Policy. For each, define and explain why each setting is an important aspect of the Local Password Policy.

* **Activity 4: (Setting an Account Lockout Policy)**

***Step One:***

(1.) Log on to the system as an **Admin** (leave password blank).

(2.) Click **Start 🡪 Control Panel 🡪 Administrative Tools 🡪 Local Security Policy**.

(3.) Expand **Account Policies** (if not already).

(4.) Click **Account Lockout Policy**.

\*\*IMPORTANT\*\* Make sure the value for **Account lockout threshold** is 0.

(5.) Double-click **Account lockout threshold**.

(6.) In the **Account lockout threshold properties** window, change the invalid logon attempts to **3**.

(7.) Click **OK**.

(8.) You will be prompted with the Suggested Value Changes window.

(9.) Click **OK** to accept default settings.

(10.) Close **ALL** windows and log off as **Admin**.

***Step Two:***

(1.) Log on as user1, OMITTING THE PASSWORD three times.

(2.) Log on a fourth time.

(3.) You will receive a message.

QUESTION? What is the message you received? (Write this message down.)\*

4. Click **OK**.

***Step Three: (Unlocking a user account as an Administrator.)***

(1.) Log on to the system as an **Admin** (leave password blank).

(2.) Click **Start 🡪 Control Panel 🡪 Administrative Tools 🡪 Computer Management**.

(3.) Expand **Local Users and Groups**.

(4.) Click **Users**.

(5.) Double click on the name of the user who is locked out, **user1**.

(6.) Uncheck the option that says **Account is locked out**.

(7.) Click the **OK** button.

(8.) Close **ALL** open windows.

***Step Four: (Removing user1 account)***

(1.) Click **Start🡪 Control Panel 🡪 Users Accounts**

(2.) Click on **user1**.

(3.) Click the **Delete Account** button, which will remove user.

(4.) Click **Delete files**.

(5.) Click **Delete Account**.

(6.) Close **ALL** windows and log off the machine.

QUESTION? List all possible settings that can be configured for the Windows **Account Lockout Policy**. For each, define and explain why each setting is an important aspect of the **Account Lockout Policy**.

# **Lab 2.2. Ubuntu**

In this lab, you will be conducting host security practices using the Linux command line. You will be performing the following tasks:

1. Adding Groups, Users and Passwords

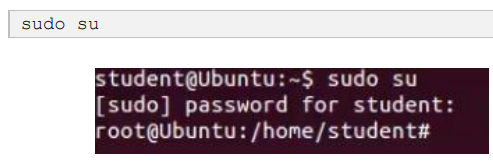
2. Permissions

LAB GUIDE:

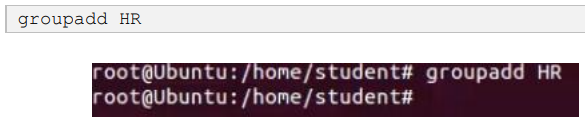
1. Open a new Terminal window by clicking on the Terminal icon located on the left menu pane:



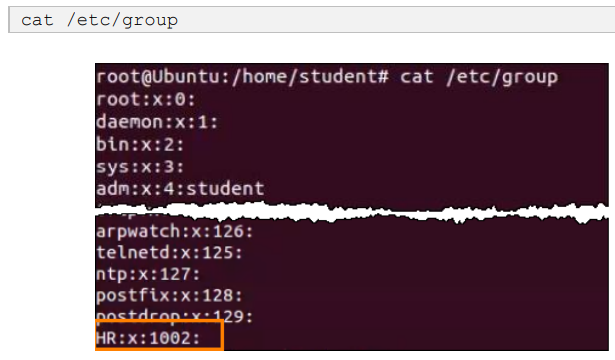
1. Escalate privileges to the root level by typing the command below followed by pressing Enter.



1. When prompted for a password, enter the password…..
2. Add a new group named HR



1. Verify the new group has been added to the group file list.

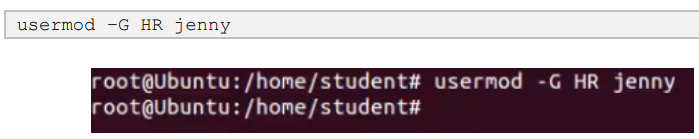


The new group HR will be added to the bottom of the /etc/group file with a group ID of 1002.

1. Add a new user named **jenny**.



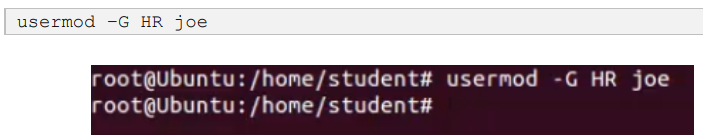
1. Place the user jenny in the newly created HR group.



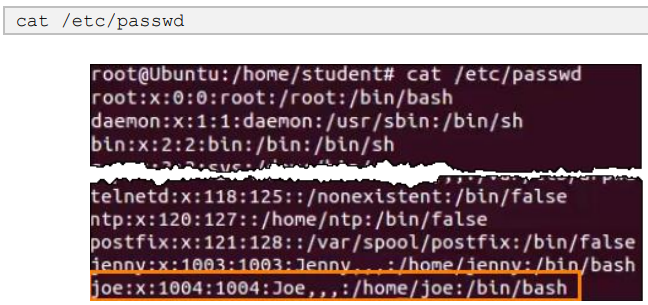
1. Add another new user named joe



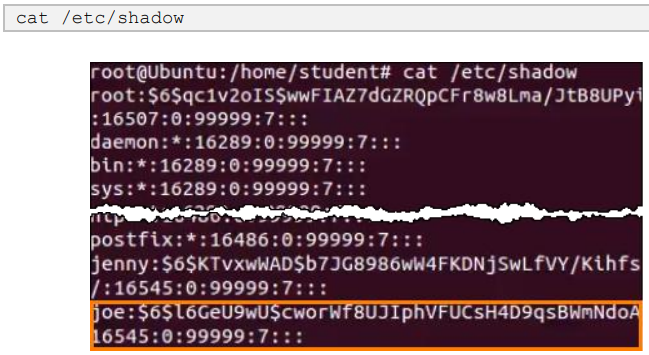
1. Place the user joe in the HR group



1. . Verify the newly created users in the passwd file

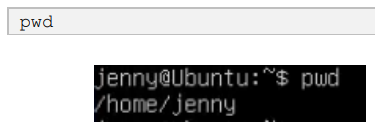


1. View the created users in the shadow file

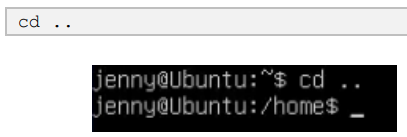


**Permissions 1:**

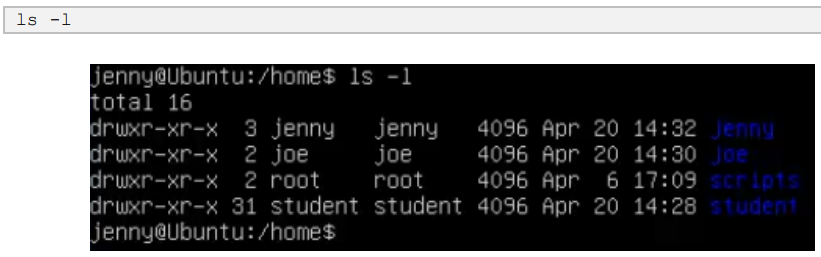
1. **Logon as jenny user**
2. View your present directory

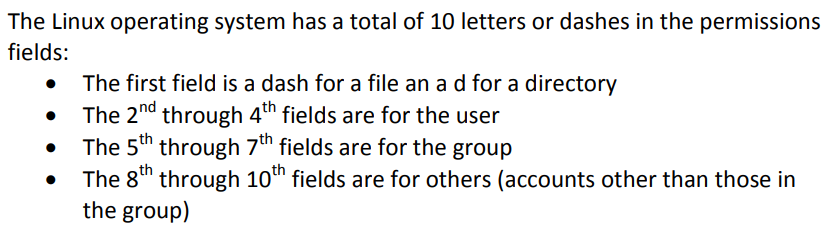


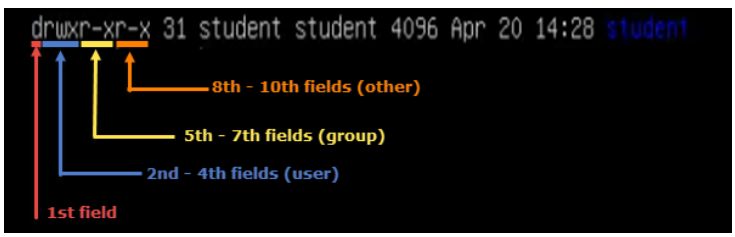
1. Go back one directory level to the /home directory



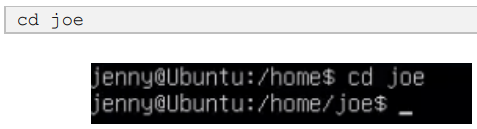
1. List all directories and their permissions.





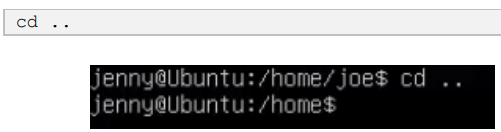


1. Enter Joe’s folder as Jenny by typing the command below.



*Notice that we are able to go into Joe’s home folder.*

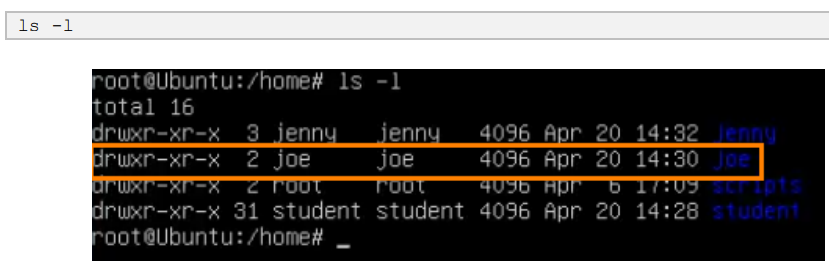
1. Change back up one directory level.



1. Press and hold CTRL+ALT+F2 to switch to another Terminal session (tty2).
2. Login as the user root
3. Change to the /home directory.

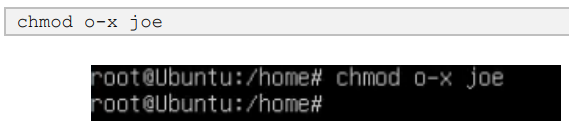


1. . List all current directories with their permissions

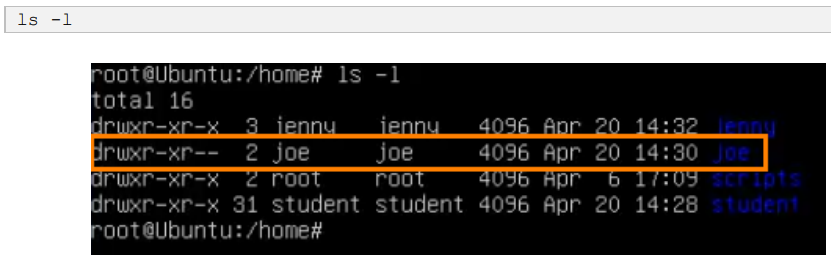


*Take note of the “other” field for Joe’s folder, notice that it is currently set with an x, which makes it available to execute for “other” users.*

1. Change the “other” permission on joe’s folder by making it non-executable.

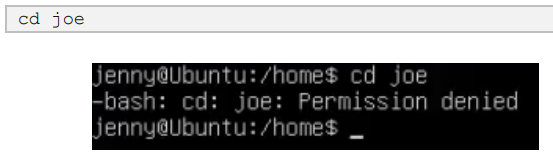


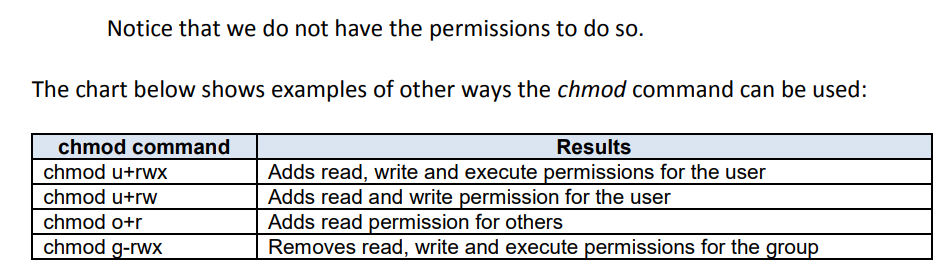
1. . List the directories once more with their respective permissions.



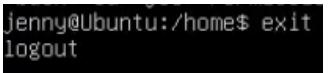
Notice now that there are two dashes in the “others” field for joe’s folder.

1. . Press and hold CTRL+ALT+F1 to switch back to the other Terminal session (tty1). Make sure you are viewing the following command prompt: jenny@Ubuntu:/home$.
2. Now that we switched to jenny’s Terminal session, attempt to go into joe’s folder once more.



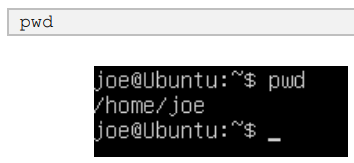


1. Type exit followed by pressing Enter to logout of the Terminal session.

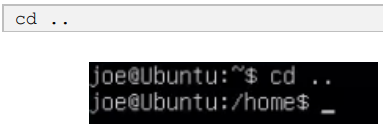


**Permission 2:**

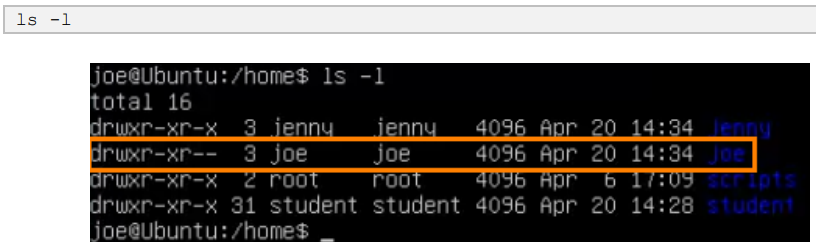
1. Login as the user joe
2. Print your current working directory



1. Go back one directory level to the /home directory.



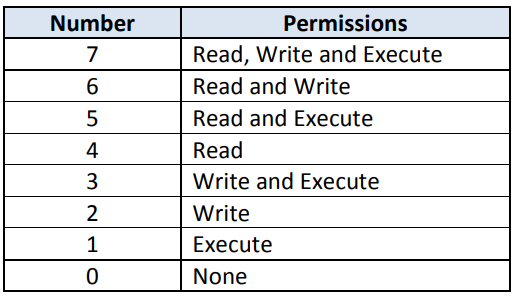
1. List all directories and their permissions in the current working directory



Notice that Joe’s folder is set so that “others” are not able to access the folder.

The other way of assigning permissions besides using symbolic permissions is the use of absolute permissions. Absolute permissions use a three digit octal number to represent the permissions for owner, group and other.

The table below outlines each absolute value and its corresponding permissions:



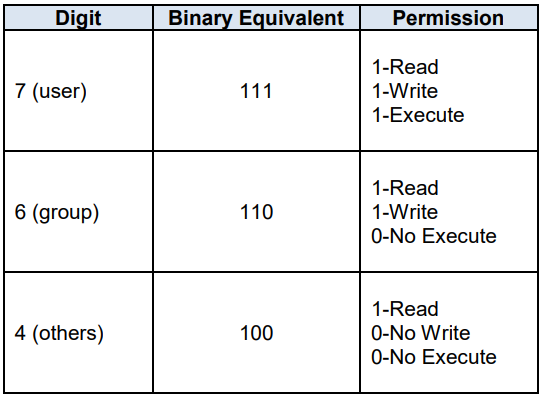
By typing the command, chmod 764 , the examplefile will be assigned the follow permissions:

• The user will get Read, Write and Execute permissions

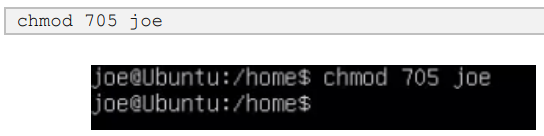
• The group will get Read and Write permissions

• Others will get Read Access

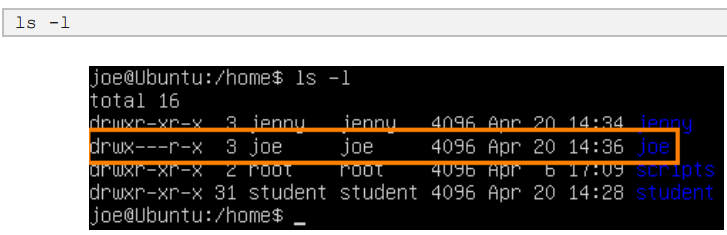
Breakdown of how 764 represents these permissions:



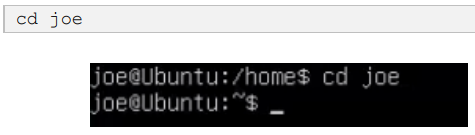
1. Modify the “others” field for Joe’s folder so that others will be able read and execute but not write while still maintaining the “user” field to read, write, and execute.



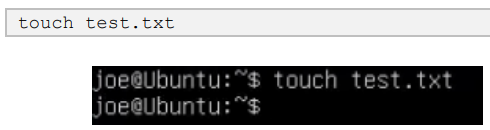
1. List the file permissions of the current directory to see that the absolute changes were made.



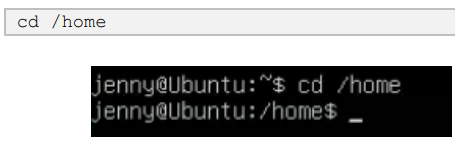
1. Change to the /home/joe directory.



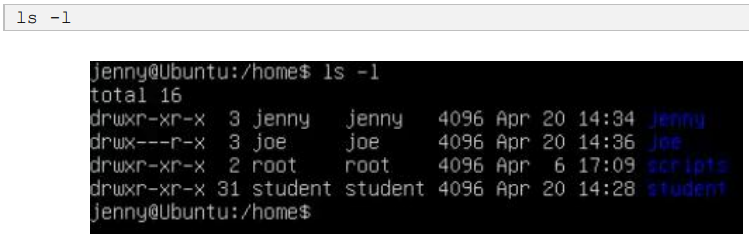
1. Create a simple text file named test.txt



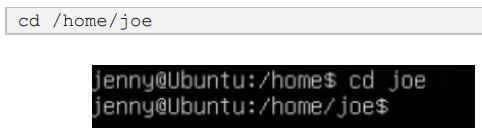
1. Type exit followed by pressing Enter to log out of Joe’s session
2. While on the tty1 Terminal, log back in as jenny
3. Change to the /home directory.



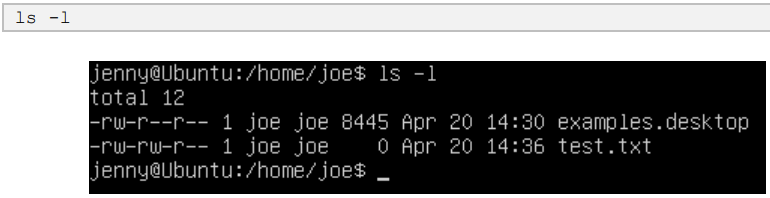
1. List all directories with their respective permissions.



1. Change to the /home/joe directory.

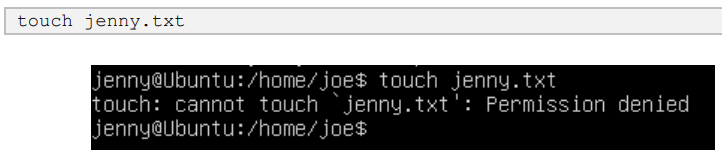


1. List all files in the current directory.



Notice that we are able to enter Joe’s folder and read the files within the directory. We are able to see the test.txt file.

1. Attempt to create a file



Notice we do not have permission to create the file.