Module File Permissions

How to Start Module:

- Before starting the module, Run the <module_script_name> to configure the environment and then <module_script_name> to verify you have done the work correctly
    1. Open a Terminal Window
    2. Clone the GitHub repo (If you have already downloaded Github Repo, skip Step2) (https://github.com/milodigwe/Linux_Essentials_m2itech)
        - From the command line type:

          git clone https://github.com/milodigwe/Linux_Essentials_m2itech
    3. Once repository is cloned, navigate to the Hands_On Folder and find the script named: **file_perm.sh**
    4. Run the navigating_and_working_the_file_system.sh script: This will configure the environment for the hands-on module
        - **sh ./ file_perm.sh**
        - The script will ask you for your public IP of your instance (which you can find in your aws console) and your key_pair (which you downloaded and assigned to instance during the ec2 creation process) to log into your instance.
    5. Once the script is finished it will provide you with an output on how to log into the system.
        - Should look like: ssh -i <path to key pair> ec2-user@<ip address>
    6. Once logged in to the instance, Perform the required tasks below.

7. To verify that you have performed the task correctly. You will need to run the **file_perm.sh_check.sh** script located in /home/ec2-user directory.
    - **file_perm.sh_check.sh** You must score a 100% to pass this module.
8. Please Note * Terminate or Stop your instance when not using it.

HAPPY LEARNING!!!

Questions:

To run these commands become root by typing:
sudo su - or enter sudo before each command.

Lab1: Create a file called example.txt in /home/ec2-user directory. Make this file readable, writeable, and executable for the user and group but not for the others. Others should not be able read, write, or execute this file.

```
[ec2-user@ip-172-31-27-40 ~]$ touch example.txt
[ec2-user@ip-172-31-27-40 ~]$ chmod 770 example.txt
```

Lab 2: Create a user called linux_user, with the uid of 2000

```
[ec2-user@ip-172-31-27-40 ~]$ sudo useradd -u 2000 linux_user
[ec2-user@ip-172-31-27-40 ~]$ id linux_user
uid=2000(linux_user) gid=2000(linux_user) groups=2000(linux_user)
```

Lab 3: Create a group called linux group, with a group id of 2001
Add user linux_user to the linux_group as the secondary group.

```
[ec2-user@ip-172-31-27-40 ~]$ sudo groupadd -g 2001 linux_group
[ec2-user@ip-172-31-27-40 ~]$ id linux_user
uid=2000(linux_user) gid=2000(linux_user) groups=2000(linux_user),2001(linux_group)
```

```
[ec2-user@ip-172-31-27-40 ~]$ sudo usermod -aG linux_group linux_user
[ec2-user@ip-172-31-27-40 ~]$ id linux_user
 uid=2000(linux_user) gid=2000(linux_user) groups=2000(linux_user),2001(linux_group)
```

```
[ec2-user@ip-172-31-27-40 ~]$ sudo cat /etc/group | grep linux
linux_user:x:2000:
linux_group:x:2001:linux_user
[ec2-user@ip-172-31-27-40 ~]$
```

Lab 4: Create a file called temp_file in the /tmp directory. Change the ownership to linux_user and group ownership to linux_group of the file temp_file. Make sure this directory is readable and writeable and executable by the user, group and executable by others.

```
[ec2-user@ip-172-31-27-40 ~]$ cd /tmp/
[ec2-user@ip-172-31-27-40 tmp]$ touch temp_file
[ec2-user@ip-172-31-27-40 tmp]$ sudo chmod 777 temp_file
[ec2-user@ip-172-31-27-40 tmp]$
```

```
[ec2-user@ip-172-31-27-40 tmp]$ sudo chown linux_user:linux_group temp_file
```

Lab 5: Create an expiration date for linux_user account to expire June 30th, 2030

```
[ec2-user@ip-172-31-27-40 tmp]$ sudo chage -l linux_user
Last password change                                    : Jun 29, 2024
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
[ec2-user@ip-172-31-27-40 tmp]$ sudo chage -E ^Cinux_user
[ec2-user@ip-172-31-27-40 tmp]$ man chage
[ec2-user@ip-172-31-27-40 tmp]$ sudo chage -l linux_user
Last password change                                    : Jun 29, 2024
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
[ec2-user@ip-172-31-27-40 tmp]$ sudo chage -E 2030-06-30 linux_user
[ec2-user@ip-172-31-27-40 tmp]$ sudo chage -l linux_user
Last password change                                    : Jun 29, 2024
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : Jun 30, 2030
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
[ec2-user@ip-172-31-27-40 tmp]$ ls
```

Check Script:

```
[ec2-user@ip-172-31-20-29 ~]$ sh ./file_perm_check.sh
1. Checking if example.txt has the correct permissions. PASS
PASS

2. Checking if linux_user exist and has the correct uid. PASS
PASS

3. Checking if linux_group exist and has the correct guid. PASS
PASS

4. Checking if User linux_user is a member of supplementary group linux_group. PASS
PASS

5. Checking if File /tmp/temp_file exists and has the correct permissions, owner, and group. PASS
6. Checking if linux_user has the correct account expiration date of June 30th, 2030. PASS
PASS

Score: 6 / 6
Your score is 100%, You have passed this module!!

Number of Correct : 6 / Number of Fail : 0 PASS
```