Project 1b. Create Shared Project Policy and Implement with Access Control.

The learning goals of this assignment are to

1. Learn how to properly implement the security policy of a shared project site using the Unix system access control.
2. Learn how to apply the principle of least privileges in this situation.

The assignment will be graded by the proper access control of the shared directory: which depends on how the users of different roles are allowed with certain privileges:

1. The users not involved in the project will no access to the project directory or files.
2. The basic project members will only have read access to the project directory and files in it.
3. The owner of the project will have read and write access to the project directory.

Assignment Topic:

You are required to create Unix accounts with three different roles and configure the access rights to the project directory with proper Unix access control command.

Setup instructions:

Before you begin, you need to start the instance (virtual machine) which you cloned in your project 1a.

How to submit:

<How a learner submit typically submit the assignment?>

The learner is required to indicate the IP address of the instance they configure for this assignment so that peer reviewers can login and evaluate the setup.

How to realize your assignment:

Step 1. Access your AMI instance.

If you are using a mac or Linux machine, you can use ssh command in the directory containing your instance's private key.

ssh –i cs5910_<yourEmailAddress>_AMILinux_i1.pem ec2-user@<InstancePublicIPAddress>

If you are using a Windows machine, you can download and install putty or bitvise app. Then follow the instruction to setup the private key for the access.

Step 2. Configure SSHD to allow login password access. By default, the AMI Linux is configured to allow access using the private key. Here we change the /etc/ssh/sshd_config configuration file to allow traditional login/password access. The reviewers will be using the remote login/password access to login with different accounts for evaluating the shared project directory access.

Using an editor such as vi to edit the /etc/ssh/sshd_config file, uncomment Line 79 and comment Line 82 to allow the password authentication. The file content should look like the following:

```
# To disable tunneled clear text passwords, change to no here!

PasswordAuthentication yes

# PermitEmptyPasswords no

# EC2 uses keys for remote access

# PasswordAuthentication no
```

Then restart sshd with the following command "*sudo service sshd restart"*

```
[ec2-user@ip-172-31-0-188 ~]$ sudo service sshd restart

Stopping sshd: [ OK ]

Starting sshd: [ OK ]
```

Now with proper login/password, the instance can be assessed and assume the role of a related user.

Step 3. Create First create three additional accounts with usernames p3i (short for public private partnership initiative), csr (for courseraJ) and arm (our project is partial funded Army Reserved) with the following commands:

```
sudo useradd p3i

sudo useradd csr

sudo useradd arm
```

Set the passwords of these three users:

```
sudo passwd p3i

sudo passwd csr

sudo passwd arm
```

Make sure you remember the password.

Verify that you can access your instance with the password of these three accounts. For example, using the following ssh command to login as p3i user.

```
ssh p3i@<yourInstanceIPAddress>
```

Step 4. Carry out the access control exercise related to Principle of Least Privileges.

Here we learn about how to setup **Shared Access Security Policy** follows the **Principle of Least Privileges** and use Unix file system access control command and related **procedures to enforce such access**.

The Shared Access Security Policy to be implemented is :

1. The users not involved in the project will no access to the project directory or files.
2. The basic project members will only have read access to the project directory and files in it.
3. The owner of the project will have read and write access to the project directory.

Step 4a. Define the project owner, project member, and non-project member.

Here we designate p3i as the project owner, arm as a project member, and csr as a non-project member.

Here we implement this policy by requesting ec2-user (with root privilege) to add arm to the p3i group.

While login as ec2-usr, run the following command:

```
sudo usermod -a -G p3i arm
```

You can verify arm has been add to p3i group, by vi /etc/group and see the line like the following

```
p3i:x:502:arm
```

where the armh is shown as a group member of p3i.

Step 4b. Login with p3i and configure the /home/p3i directory will proper shared access.

Login as p3i and create a nsa.txt in its home directory. For example, cat "This is a nsa topsec document."> nsa.txt

ls -al to see that nsa.txt has -rw-rw-r-- privleges where the group can write to it.

```
p3i@ip-172-31-14-30 ~]$ ls -al

total 28

drwx------ 2 p3i p3i 4096 Oct 23 02:48 .
```

```
drwxr-xr-x 6 root root 4096 Oct 23 02:29 ..

-rw-r--r-- 1 p3i p3i 18 Aug 30 19:00 .bash_logout

-rw-r--r-- 1 p3i p3i 193 Aug 30 19:00 .bash_profile

-rw-r--r-- 1 p3i p3i 124 Aug 30 19:00 .bashrc

-rw-rw-r-- 1 p3i p3i 35 Oct 23 02:48 nsa.txt

-rw------- 1 p3i p3i 729 Oct 23 02:48 .viminfo
```

To allow only the owner can write to this file, we run "chmod g-w nsa.txt"

To allow /home/p3i to see by the group not just the owner, we run "chmod g+rx ../p3i"

Step 4c. Verify the configuration actually enforced the Shared Access Security Policy.

First start another terminal window.

Let us first verify csr account does not have access to /home/p3i.

Login to the instance with the csr account.

ssh csr@<InstancePublicIPAddress>

or on Windows system, use bitvise app to login by entering the instance public IP address, username as csr, and changing the initial method to password. Then click "login".

Once login, launch the ls listing directory command try to access the p3i directory. You should get "Permission Denied" message. This verifies that csr cannot access the directory.

ls –al /home/p3i

You shoudl see

```
[csr@ip-172-31-14-30 ~]$ ls -al /home/p3i

ls: cannot open directory /home/p3i: Permission denied
```

Capture the text session of the csr login and the execution results of "ls -al /home/p3i". Save the text session with brief explanation the purpose of this session as csrAccess.txt on your local machine. You will submit this file as the first deliverable of your project 1b.

logout from the csr account by hitting control-d.

Next verify that arm account has read access but no write access to /home/p3i.

Login to the instance with the arm account.

```
ssh arm@<InstancePublicIPAddress>
```

Launch the ls listing directory command try to access the /home/p3i directory. You should see the directory content of /home/p3i. This verifies arm cannot access that directory.

Launch the “more /home/p3i/nsa.txt” command to see the content. You should be able to the current content of the file.

Run "cat 'This is topsec!' > /home/p3i/topsec.txt". This should fail.

Capture the text session of the arm login and the execution results of "ls -al /home/p3i", "more /home/p3i/nsa.txt", and ", and "cat 'This is topsec!' > topsec.txt".

Save the text session with brief explanation the purpose of this session as armAccess.txt on your local machine. You will submit this file as the second deliverable of your project 1b.

Next we verify the owner p3i account can read the directory/file and create new file.

Login the instance with csr account.

```
ssh p3i@<InstancePublicIPAddress>\
```

Try “ls /home/p3i/” and “more nsa.txt” to make sure p3i has read access to the directory and the file.

Try “cat ‘this is topsec’ > topsec.txt” to see if you have write access.

Capture the text session of the p3i login and the execution results of "ls -al /home/p3i", "more /home/p3i/nsa.txt", and ", and "cat 'This is topsec!' > topsec.txt".

Save the text session with brief explanation the purpose of this session as p3iAccess.txt on your local machine. You will submit this file as the third deliverable of your project 1b.

Guidelines for the assignment:

Follow the above steps to complete the assignment. Submit the three text session files as your deliverables for project 1b.