# gCIT 285 - Lab #8: Access Control

## 1: Create an Unprivileged User

Create an unprivileged user named student with a home directory /home/student and shell /bin/bash. Set the password to match your root password.

# useradd -d /home/student -m -s /bin/bash student

# passwd student

Create the group developers, then add the student user to that group and the sudo group.

# groupadd developers

# usermod -G developers,sudo student

Now create a new ssh session and login to the Kali VM as the unprivileged user student from a second terminal. Accept the RSA message.

$ ssh student@your\_Kali\_ip\_address

If you cannot login as student, then you have made a mistake in the student account setup and will need to fix that mistake before proceeding with the lab.



## 2: User Access Control

As the student user, create a temporary directory named t to conduct the exercises in this section.

$ mkdir t && cd t

2.1: What is your user ID? What is your default group ID? What other groups (GIDs) do you belong to (if any)?

$ id

User ID = 1000, group ID = 1000, the other groups I belong to are 27 (sudo) and 1001 (developers)

2.2: Create a test file and check the permissions. List the permissions in both octal and rwx notations. Refer back to the Cybersecurity Resource page for additional information regarding Linux permission values.

$ touch test\_file

$ stat test\_file

0644 and -rw-r--r--

2.3: Create a file named test2 with the following permissions:

* Owner = read, write, execute
* Group = execute
* World = execute
* What commands did you use?

Chmod 711 test2

2.5: Remove all permissions for the file owner from file test2. Leave all group and other permissions unchanged.

* What command did you use? Perform an ls -l to verify your changes
* Screenshot the results below.

Chmod u-rwx

Text

Description automatically generated

2.6: Attempt to view the contents of test2 with the cat command. What error message did you receive?

Cat: test2: permission denied

2.7: Restore the user access permissions test2 had in question 2.3.

* Verify you can view test2 content with cat.
* What commands did you use?

Chmod 711 test2 and then cat test2

2.8: Change the group owner of test2 to the developers group.

* What command did you use?
* Verify the change and provide a screenshot below

Chgrp developers test2

Text

Description automatically generated

2.9: Change the owner of test2 to the root account.

* What command did you use?
* Was an error receive? If so, what was the message.

Sudo chown root test2. There was no error message because of the sudo and entering in a password.

**3: Administrator permissions.**

In the student account terminal, become root using the su command, then change to root's home directory and create a new temporary directory in root's home directory for our experiments.

$ su

# cd ~

# mkdir t && cd t

3.1: How have your user and group identifiers changed by becoming root?

$ id

The root for all of the identifiers equal 0 now, and they all end with (root)

3.2: Create a test file and check the permissions. List the permissions in both octal and rwx notations.

$ touch test\_file2

$ stat test\_file2

0644 and -rw-r--r--

3.3: Create a test file test3 with no access permissions for any user class.

* What commands did you use?
* Verify and screenshot the results below

Chmod 000 tes\_file3

Text

Description automatically generated

3.4: Attempt to view the contents of test3 with the cat command.

* Did this work?
* If not, what error message do you see?
* If it did work, why do you think this is?

Yes, this worked. I think this worked because no matter what the permission is you are currently the root user and can see everything.

Close the terminal to end the session.