Table of Contents

File Permissions Lab

1. Manage File Security from the Command Line

In this lab, you create a collaborative directory for pre-existing users.

1. On the server system become the `root` user.

   ```
   [student@server1 ~]$ su -
   Password:r3dh@t1!
   ```

2. Create a shared group, `ateam`, with two new users, `andy` and `alice`. Set the password for these accounts to `password`.

   ```
   [root@server1 ~]# groupadd ateam
   [root@server1 ~]# useradd andy
   [root@server1 ~]# useradd alice
   [root@server1 ~]# usermod andy -aG ateam
   [root@server1 ~]# usermod alice -aG ateam
   [root@server1 ~]# passwd andy
   [root@server1 ~]# passwd alice
   ```

3. Create a directory in `/home` called `ateam-text`.

   ```
   [root@server1 ~]# mkdir /home/ateam-text
   ```

4. Change the group ownership of the `ateam-text` directory to `ateam`.

```
[root@server1 ~]# chown :ateam /home/ateam-text
```

5. Ensure the permissions of `ateam-text` allows group members to create and delete files.

```
[root@server1 ~]# chmod g+w /home/ateam-text
```

6. Ensure the permissions of `ateam-text` forbids others from accessing its files.

```
[root@server1 ~]# chmod 770 /home/ateam-text
[root@server1 ~]# ls -ld /home/ateam-text
drwxrwx---.  1 root ateam 6 Jan 23 12:0 /home/ateam-text
```

7. Exit the root shell and switch to the user `andy` with the password `password`.

```
[root@server1 ~]# exit
[student@server1 ~]$ su - andy
Password:password
```

8. Navigate to the `/home/ateam-text` folder (remember to open a terminal window first).

```
[andy@server1 ~]$ cd /home/ateam-text
```

9. Create an empty file called `andyfile3`.

```
[andy@server1 ateam-text]$ touch andyfile3
```

10. Record the default user and group ownership of the new file and its permissions.

```
[andy@server1 ateam-text]$ ls -l andyfile3
-rw-rw-r--.  1 andy andy 0 Jan 23 12:9 andyfile3
```

11. Change the group ownership of the new file to `ateam` and record the new ownership and permissions.

```
[andy@server1 ateam-text]$ chown :ateam andyfile3
[andy@server1 ateam-text]$ ls -l andyfile3
-rw-rw-r--.  1 andy ateam 0 Jan 23 12:9 andyfile3
```

12. Exit the shell and switch to the user `alice` with the password `password`.

```
[andy@server1 ateam-text]$ exit
[student@server1 ~]$ su - alice
Password:password
```

13. Navigate to the `/home/ateam-text` folder.

```
[alice@server1 ~]$ cd /home/ateam-text
```

14. Determine `alice`'s privileges to access and/or modify `andyfile3`.

```
[alice@server1 ateam-text]$ echo "text" >> andyfile3
[alice@server1 ateam-text]$ cat andyfile3
text
```

---

2. Control New File Permissions and Ownership

In this lab, you control default permissions on new files using the `umask` command and `setgid` permission.

1. Log in as `alice` on your `server1.example.com` virtual machine and open a window with a `Bash` prompt. Use the `umask` command without arguments to display `alice`'s default `umask` value.

```
[alice@server1 ~]$ umask
0002
```

2. Create a new directory `/tmp/shared` and a new file `/tmp/shared/defaults` to see how the default `umask` affects permissions.

```
[alice@server1 ~]$ mkdir /tmp/shared
[alice@server1 ~]$ ls -ld /tmp/shared
drwxrwxr-x. 2 alice alice 6 Jan 26 18:3 /tmp/shared
[alice@server1 ~]$ touch /tmp/shared/defaults
[alice@server1 ~]$ ls -l /tmp/shared/defaults
-rw-rw-r--. 1 alice alice 0 Jan 26 18:3 /tmp/shared/defaults
```

3. Change the group ownership of `/tmp/shared` to `ateam` and record the new ownership and permissions.

```
[alice@server1 ~]$ chown :ateam /tmp/shared
[alice@server1 ~]$ ls -ld /tmp/shared
drwxrwxr-x. 2 alice ateam 21 Jan 26 18:3 /tmp/shared
```

4. Create a new file in `/tmp/shared` and record the ownership and permissions.

```
[alice@server1 ~]$ touch /tmp/shared/alice3
[alice@server1 ~]$ ls -l /tmp/shared/alice3
-rw-rw-r--. 1 alice alice 0 Jan 26 18:6 /tmp/shared/alice3
```

5. Ensure the permissions of `/tmp/shared` cause files created in that directory to inherit the group ownership of `ateam`.

```
[alice@server1 ~]$ chmod g+s /tmp/shared
[alice@server1 ~]$ ls -ld /tmp/shared
drwxrwsr-x. 2 alice ateam 34 Jan 26 18:6 /tmp/shared
[alice@server1 ~]$ touch /tmp/shared/alice4
[alice@server1 ~]$ ls -l /tmp/shared/alice4
-rw-rw-r--. 1 alice ateam 0 Jan 26 18:8 /tmp/shared/alice4
```

6. Change the `umask` for `alice` such that new files are created with read-only access for the group and no access for other users. Create a new file and record the ownership and permissions.

```
[alice@server1 ~]$ umask 027
[alice@server1 ~]$ touch /tmp/shared/alice5
[alice@server1 ~]$ ls -l /tmp/shared/alice5
-rw-r-----. 1 alice ateam 0 Jan 26 18:8 /tmp/shared/alice5
```

7. Open a new Bash shell as `alice` and view the umask.

```
[alice@server1 ~]$ bash
[alice@server1 ~]$ umask
0002
```

8. Change the default `umask` for `alice` to prohibit all access for users not in their group.

```
[alice@server1 ~]$ echo "umask 007" >> ~/.bashrc
[alice@server1 ~]$ cat ~/.bashrc
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
    . /etc/bashrc
fi

# Uncomment the following line if you don't like systemctl's auto-paging
feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions
umask 007
```

9. Log out and back in to `server1.example.com` as `alice` and confirm that the `umask` changes you made are persistent.

```
[alice@server1 ~]$ exit
[alice@server1 ~]$ logout
[student@server1 ~]$ su - alice
[alice@server1 ~]$ umask
0007
```