Exercise 19.2 SELinux: Contexts

Before starting this exercise verify **SELinux** is enabled and in **enforcing** mode, by editing /etc/selinux/config and rebooting if necessary.

Obviously you can only do this on a system such as **RHEL** where **SELinux** is installed.

1. Install the **httpd** package (if not already present) which provides the **Apache** web server, and then verify that it is working:

```
$ sudo yum install  httpd
$ elinks http:/localhost
```

   (You can also use **lynx** or **firefox** etc. as the browser.)

2. As superuser, create a small file in /var/www/html:

```
$ sudo sh -c "echo file1 > /var/www/html/file1.html"
```

3. Verify you can see it:

```
$ elinks -dump http://localhost/file1.html
file1
```

   Now create another small file in **root**'s home directory and **move** it to /var/www/html. (Do not copy it, move it!) Then try and view it:

```
$ sudo cd /root
$ sudo sh -"echo file2 > file2.html"
$ sudo mv file2.html /var/www.html
$ elinks -dump http://localhost/file2.html
                                   Forbidden

   You don't have permission to access /file2.html on this server.
```

4. Examine the security contexts:

```
$ cd  /var/www/html
$ ls -Z file*html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 file1.html
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 file2.html
```

5. Change the offending context and view again:

```
$ sudo chcon -t admin_home_t file2.html
$ elinks http://localhost/file2.html
file2
```