Exercise 19.1 SELinux: Booleans

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.

RHEL/CentOS systems have had a bug where this lab did not work, but if you have a fully updated system you should be fine.

1. Install the **vsftpd** and **ftp** packages (if not already present).
2. Create a user account **user1** with the password **password**.
3. Change to **user1** account and write some text to a file named `/home/user1/user1file`.
4. Exit the **user1** account and make sure the **ftp** (**vsftpd** by name) service is running.
5. **ftp** to `localhost`, login as `user1`, and try to get `user1file`. It should fail.
   Note this step can fail either at the login, or at the file transfer. The fix for both problems is the same, so it should not affect the exercise. This difference in the behavior is a consequence of differences in the **SELinux** policy.
6. Check `/var/log/messages` to see why. You should see an error from **setroubleshoot**. Run the **sealert** command shown earlier.
7. Fix the error, and now try to **ftp**, login as `user1`, and get `user1file` again. This time it should work.

Solution 19.1

1.
   ```
   $ sudo yum install vsftpd ftp
   ```

2.
   ```
   $ sudo useradd user1
   ```

   ```
   $ sudo passwd user1
   ```

   ```
   Changing password for user user1.
   New password: password
   BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
   Retype new password: password
   passwd: all authentication tokens updated successfully.
   ```

3.
   ```
   $ sudo su - user1
   [user1@rhel7 ~]$ echo ’file created at /home/user1’ > user1file
   [user1@rhel7 ~]$ ls
   user1file
   ```

4.
   ```
   [user1@rhel7 ~]$ exit
   ```

   ```
   $ sudo systemctl status vsftpd.service
   ```

   ```
   vsftpd.service - Vsftpd ftp daemon
      Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled)
      Active: active (running) since Fri 2014-11-21 14:08:14 CET; 32min ago
   ...
   ```

5.
   ```
   $ ftp localhost
   ```

   ```
   Trying ::1...
   Connected to localhost (::1).
   220 (vsFTPd 3.0.2)
   Name (localhost:peter): user1
   331 Please specify the password.
   Password: password
   230 Login successful.
   Remote system type is UNIX.
   ```

```
Using binary mode to transfer files.
ftp> get user1file
local: user1file remote: user1file
229 Entering Extended Passive Mode (|||35032|).
550 Failed to open file.
ftp> quit
221 Goodbye.
```

6.

```
$ tail /var/log/messages
```

```
Nov 21 14:23:26 rhel7 setroubleshoot: SELinux is preventing /usr/sbin/vsftpd from read access on the file .
For complete SELinux messages. run sealert -l 7f8e5e6f-bcee-4c59-9cd1-72b90fb1f462
*****  Plugin catchall_boolean (47.5 confidence) suggests   ******************

If you want to allow ftp to home dir
Then you must tell SELinux about this by enabling the 'ftp_home_dir' boolean.

Do
setsebool -P ftp_home_dir 1
```

Notice that the suggestion to fix the issue can be found at the log file, and it is not even necessary to run **sealert**.

7.

```
$ sudo setsebool -P ftp_home_dir 1
```

```
$ ftp localhost
```

```
Trying ::1...
Connected to localhost (::1).
220 (vsFTPd 3.0.2)
Name (localhost:peter): user1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get user1file
local: user1file remote: user1file
229 Entering Extended Passive Mode (|||18769|).
150 Opening BINARY mode data connection for user1file (28 bytes).
226 Transfer complete.
28 bytes received in 4.2e-05 secs (666.67 Kbytes/sec)
ftp> quit
221 Goodbye.


$ cat user1file
file created at /home/user1
```