Lab 19.1: SELinux

Antes de comenzar este ejercicio verifique que **SELinux** esté instalado y en modo **enforcing**. Edite /etc/selinux/config y reinicie si es necesario.

Obviamente solo puede hacer esto en un sistema que tiene **SELinux** instalado. En este ejemplo estamos usando **RHEL**.

1. Instale los paquetes **vsftpd** y **ftp**.
2. Cree una cuenta **user1** con la contraseña **password**.
3. Cámbiese a la cuenta **user1** y escriba algún texto en un archivo llamado /home/user1/user1file.
4. Salga de la cuenta **user1** y asegúrese que el servicio **ftp** (el nombre del servicio es **vsftpd**) esté en ejecución.
5. Haga **ftp** al `localhost`, conéctese como `user1` e intente obtener user1file. Esto debería fallar.

   Tenga en cuenta que esto podría fallar ya sea al conectarse a la cuenta o al transferir el archivo. La solución a ambos problemas es el mismo, por lo cual el ejercicio no se verá afectado. Las diferencias en el comportamiento son una consecuencia de las diferencias en las políticas de **SELinux**.
6. Verifique /var/log/messages para determinar porqué. Usted debería ver un error relativo a **setroubleshoot**. Ejecute el comando **sealert** mostrado anteriormente.
7. Resuelva el problema e intente de nuevo hacer **ftp**, conectarse como `user1` y obtener el archivo user1file. Esta vez debería funcionar.

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
```

