

Tarea 1.4: Creación de un Shell Restringido

Descripción de la tarea

En esta tarea guiada vamos a crear un shell restringido para limitar las acciones que puede realizar un determinado usuario. El ejercicio comienza suponiendo que tenemos un usuario llamado "carmela", que puedes crear previamente con el modo gráfico, o bien con el comando interactivo `adduser` o con el comando de bajo nivel `useradd`.

Se recomienda tener abiertas dos terminales: una para que el administrador pueda realizar sus operaciones y otra para comprobar con el usuario `carmela` que dichas operaciones surten efecto.

Pasos de la tarea

1. En la terminal de administrador, edita `/etc/passwd` para que el shell por defecto de `carmela` sea `/bin/rbash` en lugar de `/bin/bash`.
2. En la terminal de `carmela`, inicia sesión como `carmela` ejecutando:

```
sudo -u carmela -i
```

3. En la terminal de `carmela`, verifica que:
 - Eres `carmela` con `whoami`.
 - Estás en `/home/carmela` con `pwd`.
 - Usas un bash restringido con `ps`.
 - El autocompletado con la tecla tabulador ya no funciona y no puedes cambiar de directorio con `cd`.
 - Comandos como `ps` y `ls` siguen funcionando.
 - `echo $PATH` muestra rutas como `/usr/bin`, `/bin`, etc. Esto debe corregirse en el siguiente paso.
4. En la terminal de administrador, ubícate en `/home/carmela` y crea un directorio `bin`:

```
cd /home/carmela
sudo mkdir bin
```

5. En la terminal de administrador, edita el archivo `.profile` con permisos de `sudo`:

```
sudo nano .profile
```

Añade al final la línea:

```
PATH="$HOME/bin"
```

6. En la terminal de **carmela**, sal del shell con **exit** y vuelve a entrar con **sudo -u carmela -i**. Verifica que ya no puedes ejecutar ningún comando como **ls** o **ps**.
7. En la terminal de administrador, crea enlaces simbólicos para permitir que **carmela** use ciertos comandos:

```
sudo ln -s /bin/ls /home/carmela/bin/ls
sudo ln -s /bin/rm /home/carmela/bin/rm
sudo ln -s /bin/vi /home/carmela/bin/vi
sudo ln -s /bin/nano /home/carmela/bin/nano
```

8. En la terminal de **carmela**, verifica que puedes ejecutar estos comandos, pero no **ps**.
9. En la terminal de **carmela**, ejecuta **ls -lisa** y verifica que los archivos de inicio (.profile, .bashrc, etc.) siguen siendo propiedad de **carmela**.
10. En la terminal de administrador, cambia el dueño y grupo de estos archivos a **root**:

```
sudo chown root:root .profile
sudo chown root:root .bashrc
```

Verifica que **carmela** no puede modificarlos.

11. En la terminal de **carmela**, intenta eliminar **.profile** con **rm .profile**. Si puedes hacerlo, sal y vuelve a entrar con **sudo -u carmela -i**, y comprueba que ahora **ps** vuelve a funcionar.
12. En la terminal de administrador, restaura **.profile** con la copia de seguridad que hayas hecho previamente.
13. Como **carmela** tiene permisos de escritura en **/home/carmela**, puede eliminar archivos. Para corregir esto, en la terminal de administrador ejecuta:

```
sudo chown root:root /home/carmela
sudo chmod +t /home/carmela
```

Verifica con **ls -lisa /home** que los permisos sean **drwxr-xr-t** y el dueño **root:root**.

14. En la terminal de **carmela**, intenta borrar **.profile**. Verás que ahora no puedes.
15. En la terminal de **carmela**, intenta crear un archivo (**nano prueba**). Verás que tampoco puedes porque no tienes permisos de escritura en tu directorio.
16. Para solucionar esto, hay dos alternativas:
 - Opción 1:

```
sudo chown root:carmela /home/carmela
sudo chmod 1775 /home/carmela
```

Si **carmela** aún puede borrar **.profile**, esta opción no es válida y deberás restaurar la copia de seguridad.

- Opción 2:

```
sudo chown root:root /home/carmela
sudo chmod 1755 /home/carmela
sudo setfacl -m "u:carmela:rwx" /home/carmela
```

Verifica con `getfacl /home/carmela` que la ACL está activa y con `ls -lisa /home` que hay un `+` al final de los permisos.

17. En la terminal de `carmela`, prueba que puedes crear archivos pero no modificar ni eliminar `.profile`.

Evidencias de la tarea

- Capturas de pantalla donde se muestre:
 1. En la terminal del administrador:
 - El dueño y permisos del directorio `/home/carmela`.
 - El dueño y permisos de los archivos dentro de `/home/carmela`.
 - Que las ACLs están activadas.
 2. En la terminal de `carmela`:
 - Que puede ejecutar `ls`.
 - Que no puede ejecutar `ps`.
 - Que no puede borrar `.profile`.

Indicadores de logro

- El dueño y permisos del directorio `/home/carmela` están correctamente establecidos.
- El dueño y permisos de los archivos de configuración en `/home/carmela` están correctamente establecidos.
- El usuario `carmela` puede ejecutar `ls`.
- El usuario `carmela` no puede ejecutar `ps`.
- El usuario `carmela` no puede borrar `.profile`.

Criterios de corrección

- La tarea se considerará "Apta" si se cumplen todas las condiciones establecidas en los indicadores de logro.

Peso en la calificación

- **Peso en la calificación final:** 25 puntos.
- **Peso en el tema correspondiente:** 25%.