

---

## PRACTICA 8: SECURITY-ENHANCED LINUX (SELINUX)

---

ADMINISTRACIÓN DE SISTEMAS UNIX/LINUX

ALUMNA:

KARLA ADRIANA ESQUIVEL GUZMÁN

[URLHTTPS://GITHUB.COM/KARLYCAMELO](https://github.com/karlycaramelo)

ERIC GIOVANNI MIGUEL TORRES

[URLHTTPS://GITHUB.COM/ERICGIOVANNI](https://github.com/ERICGIOVANNI)

MARÍA XIMENA LEZAMA HERNÁNDEZ

[URLHTTPS://GITHUB.COM/LEZAMAXI](https://github.com/LEZAMAXI)

GONZALO VAZQUEZ CRUZ

[URLHTTPS://GITHUB.COM/TRUERANDOM](https://github.com/TRUERANDOM)



*UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO*

13/MAYO/2019

1. Al instalar CentOS, por default crea los siguientes usuarios: `sysadm_u`, `system_u`, `xguest_u`, `root`, `guest_u`, `staff_u`, `user_u` y `unconfined_u`. Investiga cuales son las diferencias entre ellos y con que comandos puedo ver que tiene permitido cada uno de ellos.
  - **sysadm\_u**: Usuario SELinux con rol administrativo directo en el sistema asignado. Es utilizado para cuentas de Linux que solo realizan tareas administrativas.
  - **system\_u**: Usuario especial de SELinux destinado a servicios de sistemas. No es utilizado directamente.
  - **xguest\_u**: Se define en la política como un usuario sin privilegios. SELinux evita que los usuarios sin privilegios realicen tareas de administración sin pasar a una función diferente.
  - **root**: El usuario de SELinux destinado para la cuenta de root. Éste es utilizado para la cuenta de root de Linux.
  - **guest\_u**: La descripción de este usuario es la misma que *xguest\_u*.
  - **staff\_u**: Usuario SELinux para operadores que necesitan ejecutar tanto comandos no administrativos (a través del rol `staff_r`) como comandos administrativos (a través del rol `sysadm_r`). Se utiliza para cuentas de Linux utilizadas tanto para el uso del usuario final como para tareas administrativas.
  - **user\_u**: Usuario SELinux para cuentas no privilegiadas.
  - **unconfined\_u**: Usuario de SELinux destinado a usuarios no restringidos. Los usuarios no confinados casi no tienen restricciones en el contexto de SELinux y están destinados a sistemas en los que solo los servicios con acceso a Internet deben ejecutarse confinados (es decir, el almacén de políticas de SELinux dirigido). Se usa para todos los usuarios en un sistema de destino.
2. Al crear un usuario de linux en un sistema con SELinux por default se le asigna un usuario de SELinux. ¿En qué tipo de sistemas convendría los usuarios que tiene por default CentOS? Cambia el usuario por default de SELinux que se asigna en CentOS.

**Respuesta:**

- De acuerdo a lo que sabemos hasta ahora convendría en un sistema en el cual los usuarios necesitan ejecutar las tareas confinadamente.  
“Casi todos los servicios que escuchan en una red, como `sshd` o `httpd`, están confinados en una red. Además, la mayoría de los procesos que se ejecutan como usuario `root` y realizan tareas para los usuarios, como la utilidad `passwd`, están limitados. Cuando un proceso está limitado, se ejecuta en su propio dominio, como

el proceso httpd que se ejecuta en el dominio httpd\_t. Si un atacante compromete un proceso confinado, según la configuración de la política de SELinux, el acceso de un atacante a los recursos y el posible daño que pueden hacer es limitado.”

- El usuario por default de SELinux es **unconfined\_u** lo cambiamos a **system\_u**

```
(root@localhost ~)# semanage login -l
```

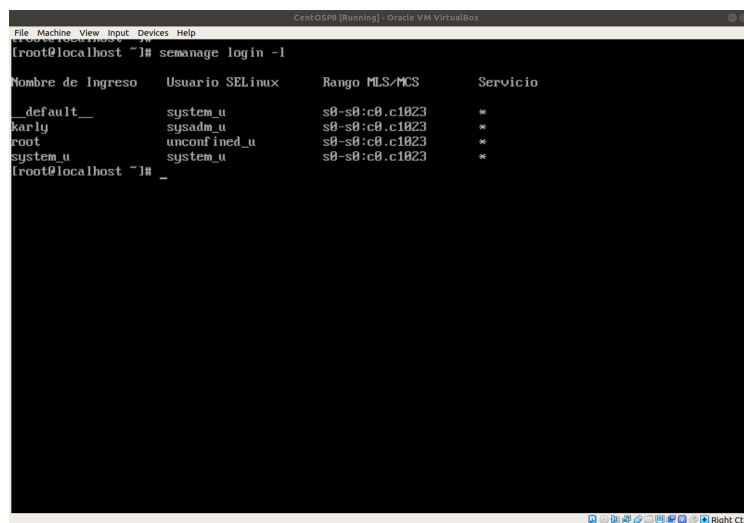
Nombre de Ingreso	Usuario SELinux	Rango MLS/MCS	Servicio
__default__	unconfined_u	s0-s0:c0.c1023	*
karly	sysadm_u	s0-s0:c0.c1023	*
root	unconfined_u	s0-s0:c0.c1023	*
system_u	system_u	s0-s0:c0.c1023	*

```
(root@localhost ~)# _
```

Para cambiar el usuario de SELinux por default, utilizamos el siguiente comando

```
semanage login -a -s system_u __default__
```

Nuevamente escribimos en la terminal **semanage login -l** para que nos muestre la lista de usuarios de SELinux y ya aparece el cambio para el usuario por default.



```
CentOS8 [Running] - Oracle VM VirtualBox
```

```
(root@localhost ~)# semanage login -l
```

Nombre de Ingreso	Usuario SELinux	Rango MLS/MCS	Servicio
__default__	system_u	s0-s0:c0.c1023	*
karly	sysadm_u	s0-s0:c0.c1023	*
root	unconfined_u	s0-s0:c0.c1023	*
system_u	system_u	s0-s0:c0.c1023	*

```
(root@localhost ~)# _
```

3. Investiga el comando auditallow, ¿para qué sirve? ¿Cómo se usa? Da un ejemplo de uso.

- **auditallow**, nos permite controlar la auditoría de los intentos de acceso permitidos. A diferencia del acceso denegado, el acceso permitido no se registra de forma predeterminada. La regla auditallow no permite el acceso; Sólo permite la auditoría de los permisos permitidos. (Registro de los accesos).

- Se utiliza de la siguiente forma:

```
auditallow user_t bin_t : file execute;
```

En este ejemplo auditallow tiene el tipo de origen `user_t`, el tipo de destino `bin_t`, el archivo de clase de objeto y la ejecución de permisos. Esta regla se puede leer como "Permite auditar al `user_t` los archivos de tipo `bin_t`".

4. Crea un usuario tal que solamente pueda tener acceso a su carpeta home. Si el nombre de usuario es `user` entonces se debe agregar un tipo de archivo `user_t` y todos los archivos de dicho usuario deben tener ese tipo.

Se crea el usuario para linux con el comando `useradd`, en este caso para crearlo en SELinux basta simplemente con mapear al usuario llamado `user` al tipo de usuario `user_u` puesto que este tipo cumple con las especificaciones que se piden en este inciso. El comando que se utiliza para el mapeo es el siguiente:

```
semanage login -a -s user_u user
```

Nombre de Ingreso	Usuario SELinux	Rango MLS/MCS	Servicio
<code>_default__</code>	<code>system_u</code>	<code>s0-s0:c0.c1023</code>	<code>*</code>
<code>friend</code>	<code>user_u</code>	<code>s0</code>	<code>*</code>
<code>karly</code>	<code>unconfined_u</code>	<code>s0-s0:c0.c1023</code>	<code>*</code>
<code>root</code>	<code>unconfined_u</code>	<code>s0-s0:c0.c1023</code>	<code>*</code>
<code>system_u</code>	<code>system_u</code>	<code>s0-s0:c0.c1023</code>	<code>*</code>
<code>user</code>	<code>user_u</code>	<code>s0</code>	<code>*</code>

```

[user@localhost ~]$ cd
[user@localhost ~]$ touch file2
[user@localhost ~]$ ls -Z file2
-rw-rw-r--. user user user_u:object_r:user_home_t:s0 file2
[user@localhost ~]$

```

5. Dependiendo de los requerimientos del sistema, a ciertos usuarios, procesos o carpetas pueden tener acceso o no a recursos del sistema. Crea dos reglas de SELinux.

## Referencias

- [1] SELinux by Example: Using Security Enhanced Linux, Frank Mayer, Karl MacMillan, David Caplan, Julio 27, 2006.
- [2] [https://www.systutorials.com/docs/linux/man/8-guest\\_selinux/](https://www.systutorials.com/docs/linux/man/8-guest_selinux/).
- [3] [https://wiki.gentoo.org/wiki/SELinux/Users\\_and\\_logins](https://wiki.gentoo.org/wiki/SELinux/Users_and_logins)

- [4] [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html/security-enhanced\\_linux/index](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security-enhanced_linux/index)
- [5] <https://www.thegeekstuff.com/2017/07/chcon-command-examples/>