

SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software
Curso 2019-20

Práctica [1]. Administración de la seguridad en Linux.

Sesión [4]. SELinux (Security Enhanced Linux)

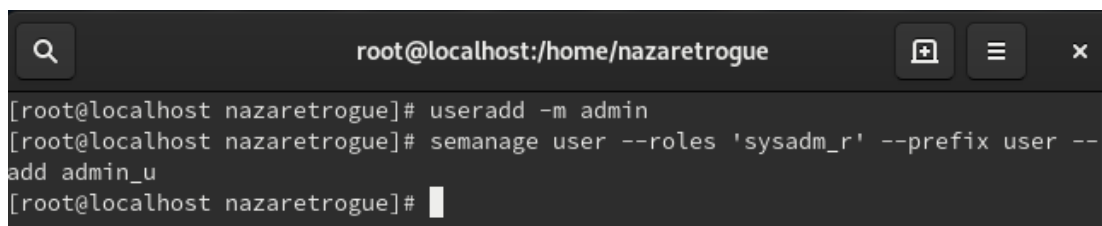
Autor¹: Nazaret Román Guerrero

Ejercicio 1.

Crear un usuario SELinux denominado `admin` con el rol `sysadm_r`.

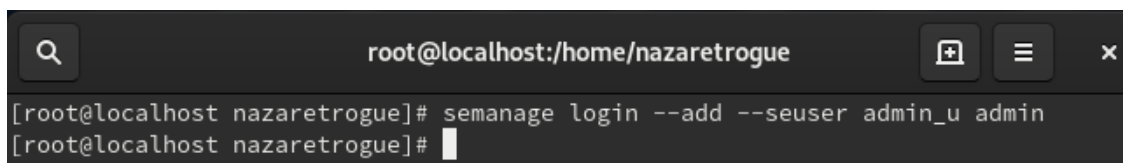
Para dar el rol a un usuario, primero es necesario crear a dicho usuario. Para eso, utilizamos el comando `useradd -m admin`, que crea un usuario de nombre `admin` y crea un `/home` si no está creado (opción `-m`).

Una vez creado, se le da el rol de `sysadm_r` al usuario `admin_u` en SELinux, tal y como se ve en el segundo comando de la siguiente imagen:



```
root@localhost:/home/nazaretroque
[root@localhost nazaretroque]# useradd -m admin
[root@localhost nazaretroque]# semanage user --roles 'sysadm_r' --prefix user --add admin_u
[root@localhost nazaretroque]#
```

Después de esto, asignamos el usuario creado en SELinux con el comando anterior con el usuario del sistema que hemos creado antes, tal y como se muestra a continuación.



```
root@localhost:/home/nazaretroque
[root@localhost nazaretroque]# semanage login --add --seuser admin_u admin
[root@localhost nazaretroque]#
```

Una vez asignado el usuario, el damos una contraseña al usuario `admin` del sistema con el uso de la orden `passwd`.

1 Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la “Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada” esto “conllevará la calificación numérica de cero ... independientemente del resto de calificaciones que el estudiante hubiera obtenido ...”

```
root@localhost:/home/nazaretroque

[root@localhost nazaretroque]# passwd admin
Cambiando la contraseña del usuario admin.
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: todos los tokens de autenticación se actualizaron exitosamente.
[root@localhost nazaretroque]#
```

Por último, establecemos el contexto de seguridad del home, de manera recursiva (opción -R) y para el usuario admin_u (indicado con la opción -u).

```
root@localhost:/home/nazaretroque

[root@localhost nazaretroque]# chcon -R -u admin_u /home/admin/
[root@localhost nazaretroque]#
```

Una vez completados estos pasos, vamos a comprobar si en efecto el usuario que hemos creado tiene el rol que hemos decidido asignarle. Para ello utilizamos el comando `semanage user -l`, que lista todos los usuarios con el prefijo que tiene cada uno y el rol (o roles) que tienen en SELinux. Como se puede observar, el usuario admin_u es un usuario cuyo rol es sysadm_r, por lo que la configuración del usuario es correcta.

```
root@localhost:/home/nazaretroque

[root@localhost nazaretroque]# semanage user -l
```

Usuario SELinux	Etiquetado Prefijo	MLS/ Nivel MCS	MLS/ Rango MCS	Roles SELinux
admin_u	user	s0	s0	sysadm_r

Ejercicio 2.

Localiza algunos mensajes de los logs de tu sistema, o genera alguno, y describe la denegación que producen.

Para ver los logs, lo primero que debemos hacer es saber si auditd está funcionando para saber donde tendremos que buscar el archivo de log. Para ello, utilizamos `systemctl` y comprobamos si está habilitado y escuchando fallos que se produzcan el sistema, tal y como se puede observar en la imagen de abajo.

Como podemos comprobar, está activo y habilitado (recuadros rojos). Por tanto, para ver los log necesitamos saber dónde se están registrando. Para ello, buscamos en el archivo `/etc/audit/auditd.conf`, que nos dice que todos los logs se están registran en el archivo `/var/log/audit/audit.log`.

```
root@localhost:/home/nazaretroque

[root@localhost nazaretroque]# systemctl status auditd.service
● auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2019-10-26 14:42:57 CEST; 2h 11min ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Process: 728 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
   Process: 735 ExecStartPost=/sbin/auditd --load (code=exited, status=0/SUCCESS)
  Main PID: 730 (auditd)
    Tasks: 2 (limit: 2352)
   Memory: 3.2M
    CGroup: /system.slice/auditd.service
            └─730 /sbin/auditd

oct 26 14:42:56 localhost.localdomain systemd[1]: Starting Security Auditing Service...
oct 26 14:42:56 localhost.localdomain auditd[730]: No plugins found, not dispatching events
oct 26 14:42:56 localhost.localdomain auditd[730]: Init complete, auditd 3.0 listening for events (startup state)
oct 26 14:42:57 localhost.localdomain augenrules[735]: /sbin/augenrules: No change
oct 26 14:42:57 localhost.localdomain augenrules[735]: No rules
oct 26 14:42:57 localhost.localdomain systemd[1]: Started Security Auditing Service.
[root@localhost nazaretroque]#
```

Sabiendo el archivo, hacemos un cat mostrando aquellas líneas donde el resultado haya sido un fallo (res=failed). La primera que aparece es la que se muestra en la imagen; analicemos qué significa.

```
root@localhost:/home/nazaretroque

[root@localhost nazaretroque]# cat /var/log/audit/audit.log | grep failed
type=SERVICE_STOP msg=audit(1570793523.864:333): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=rngd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=failed'
UID="root" AUID="unset"
```

Este log quiere decir que ha fallado el proceso con pid 1, que intentaba parar un servicio (type=SERVICE_STOP) mediante systemd (comm="systemd", que ejecuta el programa que hay en exe="/usr/lib/systemd/systemd") y cuya etiqueta de ejecución es system_u:system_r:init_t:s0.

Es decir, el demonio que se encarga del control de los procesos del sistema (systemd) ha intentado parar un servicio pero no ha tenido éxito, motivo por el cual se ha visto reflejado en los logs como una operación cuyo resultado ha sido failed.

Ejercicio 3.

Indicar la orden que debemos ejecutar para pasar de un estado permisivo a uno obligatorio.

Por defecto, la política viene en modo enforcing, de manera que para hacer el ejercicio, la he cambiado a permissive y así poder mostrar el funcionamiento. Cambiar de permissive a enforcing se puede hacer de varias maneras:

- Si pretendemos establecer la política de enforcing de manera temporal, podemos utilizar dos formas:
 - Utilizando la palabra Enforcing junto con el comando setenforce, tal y como se muestra en la siguiente imagen.

```
root@localhost:/home/nazaretroque

[root@localhost nazaretroque]# getenforce
Permissive
[root@localhost nazaretroque]# setenforce Enforcing
[root@localhost nazaretroque]# getenforce
Enforcing
[root@localhost nazaretroque]#
```

- Utilizando el número 1 (valor booleano 1, true) junto con el comando setenforce, como se puede observar debajo.

```
root@localhost:/home/nazaretroque

[root@localhost nazaretroque]# getenforce
Permissive
[root@localhost nazaretroque]# setenforce 1
[root@localhost nazaretroque]# getenforce
Enforcing
[root@localhost nazaretroque]#
```

- Si pretendemos que la política se establezca en modo enforcing de manera permanente y se mantenga tras reiniciar la máquina, debemos modificar el archivo /etc/selinux/config. Como he mencionado antes, por defecto la política establecida es enforcing, por eso en el archivo de configuración aparece en modo enforcing como se puede observar abajo. Si se desea poner en modo permissive, solo tenemos que cambiarlo tal y como indica el propio archivo.

```
root@localhost:/home/nazaretroque

[root@localhost nazaretroque]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Ejercicio 4.

Completar la tabla anterior para la distribución de Linux que esté usando cada uno de vosotros.

El sistema operativo que estoy utilizando es Fedora 30.

Para extraer la información necesaria para completar la tabla, es necesario instalar en el sistema el paquete setools que contiene seinfo y sestatus, dos utilidades que muestran información sobre la política de SELinux.

La información se ha extraído de la siguiente forma:

- Policy store name: cuarta línea de sestatus.
- MLS: séptima línea de sestatus y segunda línea de seinfo.
- deny_unknown: octava línea de sestatus.
- Unconfined domains: comando seinfo -tunconfined_t.
- UBAC: comando seinfo -aubac_constrained_type -x.

La información que se muestra en la imagen está pasada a forma de tabla:

Fedora 30				
Policy store name	MLS	deny_unknown	unconfined domains	UBAC
targeted	Sí, enabled	Sí, allowed	Sí	No

```
root@localhost:/home/nazaretroque

[root@localhost nazaretroque]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 131   Permissions:          457
Sensitivities:           1     Categories:           1024
Types:                   4916  Attributes:           249
Users:                   9     Roles:                14
Booleans:                326   Cond. Expr.:         372
Allow:                   111656 Neverallow:            0
Auditallow:              159   Dontaudit:           10246
Type_trans:              238392 Type_change:           87
Type_member:              35   Range_trans:         6015
Role allow:              39    Role_trans:          424
Constraints:              72   Validatetrans:        0
MLS Constrain:           72    MLS Val. Tran:       0
Permissives:              0    Polcap:               5
Defaults:                 7    Typebounds:           0
Allowxperm:               0    Neverallowxperm:      0
Auditallowxperm:         0    Dontauditxperm:       0
Initial SIDs:             27    Fs_use:               33
Genfscon:                 106   Portcon:              627
Netifcon:                  0    Nodecon:              0

[root@localhost nazaretroque]# sestatus
SELinux status:           enabled
SELinuxfs mount:          /sys/fs/selinux
SELinux root directory:   /etc/selinux
Loaded policy name:        targeted
Current mode:              enforcing
Mode from config file:    enforcing
Policy MLS status:         enabled
Policy deny_unknown status: allowed
Memory protection checking: actual (secure)
Max kernel policy version: 31

[root@localhost nazaretroque]# seinfo -tunconfined_t

Types: 1
    unconfined_t

[root@localhost nazaretroque]# seinfo -aubac_constrained_type -x

Type Attributes: 0
[root@localhost nazaretroque]#
```