SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software

Curso 2018-19

Práctica [1]. Administración de la seguridad en Linux

Sesión [4]. SELinux (Security Enhanced Linux)

Autor[1]: Matilde Cabrera González

Ejercicio 2.1.

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

```
[mati@localhost ~]$ useradd -m admin_a
useradd: Permission denied.
useradd: no se pudo bloquear /etc/passwd, inténtelo de nuevo.
[mati@localhost ~]$ sudo -i
[sudo] password for mati:
[root@localhost ~]# useradd -m admin_a
[root@localhost ~]#
```

```
[root@localhost mati]# semanage usr --roles 'sysadm_r' --prefix user -add admin_u
bash: semanage: no se encontró la orden...
¿Quiere instalar el paquete «policycoreutils-python-utils» que proporciona la orden «semanage»? [N/y] y


 * Esperando en cola...
 * Cargando listas de paquetes....
Los siguientes paquetes deben instalarse:
 checkpolicy-2.8-1.fc28.x86_64  SELinux policy compiler
 policycoreutils-python-utils-2.8-1.fc28.noarch SELinux policy core python utilities
 python3-IPy-0.81-21.fc28.noarch        Python 3 module for handling IPv4 and IPv6 Addresses and Networks
 python3-audit-2.8.3-3.fc28.x86_64      Python3 bindings for libaudit
 python3-libsemanage-2.8-2.fc28.x86_64  semanage python 3 bindings for libsemanage
 python3-policycoreutils-2.8-1.fc28.noarch      SELinux policy core python3 interfaces
 python3-setools-4.1.1-9.fc28.x86_64    Policy analysis tools for SELinux
Los siguientes paquetes deben actualizarse:
 libselinux-2.8-1.fc28.x86_64   SELinux library and simple utilities
 libselinux-utils-2.8-1.fc28.x86_64     SELinux libselinux utilies
 libsemanage-2.8-2.fc28.x86_64  SELinux binary policy manipulation library
 libsepol-2.8-1.fc28.x86_64     SELinux binary policy manipulation library
 policycoreutils-2.8-1.fc28.x86_64      SELinux policy core utilities
 python3-libselinux-2.8-1.fc28.x86_64   SELinux python 3 bindings for libselinux
¿Quiere continuar con las modificaciones? [N/y] y


 * Esperando en cola...
 * Esperando autenticación...
 * Esperando en cola...
 * Descargando paquetes...
```

```
[root@localhost mati]# semanage user --roles 'sysadm_r' --prefix admin --add admin
[root@localhost mati]#
```

[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 ~]# semanage login --add --seuser admin admin_a
[root@localhost ~]# chcon -R -u admin /home/admin_a/
[root@localhost ~]# semanage user -l

                Etiquetado MLS/       MLS/
Usuario SELinux  Prefijo    Nivel MCS  Rango MCS                      Roles SELi
nux

admin           admin      s0         s0                            sysadm_r
admin_u         user       s0         s0                            sysadm_r
```

Ejercicio 2.2.

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

Cambio en la configuración al realizar el ejercicio anterior.

```
time->Thu Oct 25 23:54:29 2018
type=CONFIG_CHANGE msg=audit(1540504469.115:82): auid=4294967295 ses=4294967295
subj=system_u:system_r:unconfined_service_t:s0 op=add_rule key=(null) list=1 res
=1
----
```

```
[root@localhost ~]# exit
logout
[mati@localhost ~]$ sudo su
[sudo] password for mati:
Sorry, try again.
[sudo] password for mati:
Sorry, try again.
[sudo] password for mati:
sudo: 3 incorrect password attempts
[mati@localhost ~]$ sudo ausearch -ts recent
[sudo] password for mati:
----
```

```
----
time->Thu Oct 25 23:54:43 2018
type=USER_AUTH msg=audit(1540504483.912:127): pid=837 uid=0 auid=4294967295 ses=
4294967295 subj=system_u:system_r:xdm_t:s0-s0:c0.c1023 msg='op=PAM:authenticatio
n grantors=pam_permit acct="gdm" exe="/usr/libexec/gdm-session-worker" hostname=
localhost.localdomain addr=? terminal=/dev/tty1 res=success'
----
time->Thu Oct 25 23:54:43 2018
type=USER_ACCT msg=audit(1540504483.914:128): pid=837 uid=0 auid=4294967295 ses=
4294967295 subj=system_u:system_r:xdm_t:s0-s0:c0.c1023 msg='op=PAM:accounting gr
antors=pam_permit acct="gdm" exe="/usr/libexec/gdm-session-worker" hostname=loca
lhost.localdomain addr=? terminal=/dev/tty1 res=success'
----
time->Thu Oct 25 23:54:44 2018
type=CRED_ACQ msg=audit(1540504484.005:129): pid=837 uid=0 auid=4294967295 ses=4
294967295 subj=system_u:system_r:xdm_t:s0-s0:c0.c1023 msg='op=PAM:setcred granto
rs=pam_permit acct="gdm" exe="/usr/libexec/gdm-session-worker" hostname=localhos
t.localdomain addr=? terminal=/dev/tty1 res=success'
----
```

Intenté loguearme poniendo la contraseña incorrecta y volví a ejecutar ‘ausearch -ts recent’, he localizado USER_AUTH donde el usuario se intenta identificar sin conseguirlo

Ejercicio 2.3.

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

Tenemos setenforce para cambiar de permisivo a obligatorio, si lo usamos con 0 lo pone a permisivo, si lo ponemos a uno lo dejamos enforcing (obligatorio).

```
[mati@localhost ~]$ getenforce
Enforcing
[mati@localhost ~]$ sudo setenforce 0
[sudo] password for mati:
[mati@localhost ~]$ getenforce
Permissive
```

Ejercicio 2.4.

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

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

```
[mati@localhost ~]$ seinfo
bash: seinfo: no se encontró la orden...
¿Quiere instalar el paquete «setools-console» que proporciona la orden «seinfo»?
 [N/y] y


 * Esperando en cola...
Los siguientes paquetes deben instalarse:
 setools-console-4.1.1-9.fc28.x86_64    Policy analysis command-line tools for S
ELinux
¿Quiere continuar con las modificaciones? [N/y]
```

```
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             31 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             129    Permissions:         450
  Sensitivities:         1    Categories:         1024
  Types:              4852    Attributes:          250
  Users:                10    Roles:                14
  Booleans:            318    Cond. Expr.:         364
  Allow:            107563    Neverallow:            0
  Auditallow:          157    Dontaudit:          9966
  Type_trans:       231039    Type_change:          74
  Type_member:          35    Range_trans:        5986
  Role allow:           39    Role_trans:          422
  Constraints:          67    Validatetrans:         0
  MLS Constrain:        71    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:            105    Portcon:             615
  Netifcon:              0    Nodecon:               0

[mati@localhost ~]$
```

Distribution	Policy store name	MLS?	deny_ unknown	Unconfined domains?	UBAC?
Gentoo	strict	No	denied	No	Yes (configurable)
Fedora 19	minimum	Yes (only s0)	allowed	Yes, but limited	No

Fedora 28 targered enabled allowed yes yes