SEGURIDAD EN SISTEMAS OPERATIVOS

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

Curso 2017-18

Práctica [1]. Administración de la seguridad en Linux

Sesión [4]. SELinux (Security Enhanced Linux)

Autor[1]: Rubén Calvo Villazán

Ejercicio 1.

Crear un usuario SELinux denominado admin con el rol sysadm_r

Primero creamos el usuario admin en el sistema:

```
$> useradd -m admin # Crea directorio /home
```

Después creamos usuario admin en SELinux con rol sysadm_r:

```
$> semanage user –roles 'sysadm_r' --prefix user –add admin_u
```

Asociamos el usuario creado en SELinux al usuario admin del sistema:

```
$> semanage login –add –seuser admin_u admin
```

Cambiamos contexto de seguridad:

```
$> chcon -R -u admin_u /home/admin/
```

Ejercicio 2.

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

que producen.

Podemos generar un mensaje de error cuando hacemos sudo su y escribimos una contraseña incorrecta. El mensaje de error en este caso es el siguiente:

```
$> /sbin/ausearch -ts recent
```

```
time->Mon Nov 13 22:32:07 2017
```

---

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 ..."

type=USER_AUTH msg=audit(1415055434.297:769): pid=22610 uid=601

auid=406 ses=1

subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

msg='op=PAM:authentication acct="root" exe="/usr/bin/su"

hostname=? addr=? terminal=pts/2 res=failed'

Ejercicio 3.

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

Para ello usamos la orden setenforce, setenforce modifica el modo en el que se

ejecuta SELinux.

Para pasar de estado permisivo a obligatorio debemos ejecutar:

$> setenforce 1

Podemos ver el modo con:

$> sestatus | grep -i mode

Ejercicio 4.

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

vosotros.

El sistema usado es Fedora 20 en VirtualBox, las políticas establecidas son:

Distro:	Policy store name:	MLS?	deny_unknown	unconfined_domains	UBAC?
Fedora 20	targeted	enabled	allowed	si	si