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]. AppArmor

Autor[1]: Rubén Calvo Villazán

Ejercicio 1.

Listar todos los perfiles de AppArmor:

```
$> aa-status
```

Listar todos los ejecutables bajo un perfil de AppArmor:

```
$> ps auxZ | grep -v '^unconfined'
```

Los perfiles se guardan en /etc/apparmor.d/ por ejemplo:
usr.lib.libreofficeprogram Correspondiente a libreoffice
apache2.d/ Correspondiente a Apache

Para cargar perfiles:

```
$> cat /etc/apparmor.d/bin.ping | sudo apparmor_parser -a
$> cat /etc/apparmor.d/usr.sbin.traceroute | sudo apparmor_parser -a
$> aa-status
2 profiles are in complain mode.
   /usr/{sbin/traceroute,bin/traceroute.db}
   ping
```

Los perfiles en modo complain no aplican la política pero avisan de los intentos de violación de la misma.

---

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 ..."

Ejercicio 2.

Crear un perfil de AppArmor:

Para crear un perfil usamos

```
$> aa-genprof shutter
```

Creamos un perfil para el programa shutter, un programa de capturas de pantalla.

Seguimos las indicaciones en pantalla eligiendo las opciones correspondientes hasta que la creación finalice.

Después lo ponemos en modo complain:

```
$> a-complain shutter
```

```
Setting /usr/bin/shutter to complain mode.
```

Podemos ver en syslog la creación y cambio de modo del perfil:

```
Oct 22 13:48:51 kali kernel: [ 2758.543353] audit: type=1400 audit(1508672931.156:5): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/bin/shutter" pid=2169 comm="apparmor_parser"
```

```
Oct 22 13:50:04 kali kernel: [ 2832.358905] audit: type=1400 audit(1508673004.972:6): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/usr/bin/shutter" pid=2212 comm="apparmor_parser"
```

```
Oct 22 13:50:40 kali kernel: [ 2868.310303] audit: type=1400 audit(1508673040.923:7): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/usr/bin/shutter" pid=2226 comm="apparmor_parser"
```

Ahora tenemos 3 perfiles en modo complain:

```
$> aa-status
```

```
3 profiles are in complain mode.
   /usr/bin/shutter
   /usr/{sbin/traceroute,bin/traceroute.db}
   ping
```

```
$> cat /etc/apparmor.d/usr.bin.shutter
# Last Modified: Sun Oct 22 13:48:51 2017
#include <tunables/global>

/usr/bin/shutter flags=(complain) {
  #include <abstractions/base>
  #include <abstractions/perl>

  /lib/x86_64-linux-gnu/ld-*.so mr,
  /usr/bin/perl ix,
  /usr/bin/shutter r,

}
```

Al estar en modo complain el perfil no aplica la política pero avisa de los intentos de violación de la misma.