



Práctica 3: Apparmor

Curso 2017-2018

1. Sistemas de control de acceso

Existen dos modelos básicos de control de acceso: DAC (Discretional Access Control) y MAC (Mandatory Access Control) que podrás encontrar bien explicados en *Tipos de Control de acceso*

2. Introducción a Apparmor

AppArmor ofrece tecnología de inmunización, configura una serie de perfiles de aplicación por defecto para proteger los servicios estándar de Linux. Como en anteriores prácticas vamos a recurrir a la información que ya está publicada en la Web. En este caso no vamos a utilizar un único guión como referencia, sino que iremos sacando una cosas de un lado y otras de otro. Aunque vamos a seguir principalmente una versión en castellano disponible en *Guía Novell AppArmor*. Otros enlaces de interés son los siguientes:

- Ayudas para trabajar bajo Ubuntu. *AppArmor en Ubuntu*:
- *Más de AppArmor*:

De entre toda esta información debería quedarte claro:

1. DAC versus MAC
2. Concepto de perfil
3. Algunos elementos de un perfil: el documento Quick Referencia podrá ayudarte.
 - Tipo de reglas: capabilities(capacidades), paths (vías) e #includes.
 - Permisos de ficheros
 - deny, audit
 - Perfiles específicos
4. Modos de funcionamiento de AppArmor: complain (modo aprendizaje) y enforce (modo aplicación).
5. Gestión de la propia aplicación AppArmor:
`$ sudo service apparmor {start | stop| restart | recache | reload| force-reload| status }`



3. Ejemplo Apparmor

Para probar alguna de las características de AppArmor vamos a plantearnos lo siguiente

1. Instala el paquete *apparmor-utils*
2. Crea una copia del comando *cp* que encontrarás en */bin* y llámala *mi_cp*
3. Crea un perfil para tu nuevo comando mediante *aa-genprof*. Ponte en modo escucha y abre otro terminal crea un par de directorios *d1* y *d2*, crea un fichero *f1* en *d1* y cópialo al directorio *d2* mediante *mi_cp*. Cambia de terminal y observa qué muestra *aa-genprof*. Finaliza la ejecución de *aa-genprof* y comprueba que se ha creado un perfil para *mi_cp* en el directorio correspondiente.
4. Modifica el nuevo perfil para hacer copias desde el directorio *d2* al *d1*, pero no al revés.
5. Comprueba que todo funciona como has establecido.