

SSO Práctica 1 Sesión 2

Andrés Merlo Trujillo

Índice

Ejercicio 1	2
Ejercicio 2	2

Ejercicio 1

Con la orden `aa-status` o la orden `apparmor_status` se pueden ver los perfiles activos en Ubuntu:

Ahora voy a elegir el perfil `/usr/bin/freshclam`, para poder ver el archivo del perfil asociado basta con irse al directorio `/etc/apparmor.d` y el archivo se denomina igual que la ruta absoluta del mismo, pero en vez de usar “/” se utilizan puntos. Por tanto, el archivo deseado es: `/etc/apparmor.d/usr.bin.freshclam`.

Las componentes principales son las siguientes:

- `#include <tunables/global>` Carga un archivo que contiene las definiciones de las variables.
- `/usr/bin/freshclam` Ruta absoluta del binario.
- `#include <abstractions/base>` Obtiene los componentes de los perfiles de AppArmor para simplificar el desarrollo de perfiles.
- `#include <abstractions/namespace>` Incluye las reglas para permitir DNS, LDAP, NIS, SMB, contraseñas de usuarios y grupos, servicios y “lookups” de protocolos
- `#include <abstractions/user-tmp>` Permite acceder a los directorios temporales
- `#include <abstractions/openssl>` Permite acceder a los archivos correspondientes a OpenSSL.
- `{,var/}` Permite eliminar líneas innecesarias, poniendo los directorios similares dentro de la lista entre laves. En este caso las opciones son `/run/clamav/freshclam.pid` y `/var/run/clamav/freshclam.pid`
- `capability ...` Indica las capabilities que tiene permitidas hacer en el sistema. El listado de todas ellas se puede ver usando `man 7 capabilities`.
- `owner archivo` Indica que solo puede acceder al archivo indicado si es el propietario del mismo.
- `deny archivo` Deniega el acceso al archivo indicado.

Además, aparecen variables del tipo “@...”, el valor de estas variables se almacenan en `/etc/apparmor.d/file` donde file es el nombre de la variable. Las que aparecen en este perfil son:

- `@{HOME}`: Lista de todos los `home` de los usuarios, incluido el root.
- `@{PROC}`: Directorio donde `procfs` es montado.

Se puede ver que contiene una lista de archivos y directorios junto con sus permisos, estos son los archivos o directorios a los que puede tener acceso, determinado por los switches que se muestran a continuación:

- **r**: Modo lectura
- **w**: Modo escritura
- **a**: Modo adjuntar (append)
- **k**: Modo de bloqueo de archivo
- **l**: Modo de enlace
- **ux**: Modo de ejecución sin restricciones
- **Ux**: Modo de ejecución sin restricciones. Además, limpia el entorno (scrub the environment)
- **px**: Ejecución discreta del perfil
- **Px**: Modo de ejecución discreta del perfil. Además, limpia el entorno (scrub the environment)
- **ix**: Modo de ejecución heredada
- **m**: Permite `PROT_EXEC` con llamadas a `mmap`
- **Cx**: Permite transiciones a un perfil hijo. Con la C mayúscula se usa “secure exec” de glibc.

Ejercicio 2

Voy a generar un perfil para el programa **nano**, para saber su ruta absoluta se puede usar la orden **which nano**:

Ahora para generar el perfil se ejecuta el comando **aa-genprof /usr/bin/nano**:

Ahora pide que abramos el programa a perfilar y pulsemos en el boton de escanear.

Es recomendable abrir el manual de capabilites para ver que significa cada capability con **man 7 capabilities**.

Esto permite saltarse las comprobaciones de permisos de lectura sobre el archivo y las comprobaciones sobre el directorio de permiso de lectura y ejecucion. Es mejor denegarlo con la tecla "D".

nanorc es un archivo con las configuraciones personalizadas para el editor, al ser un archivo inofensivo se puede permitir su uso.