# SSO Práctica 1 Sesión 2

Andrés Merlo Trujillo

## Índice

# 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 compoenntes 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 simplifcar el desarrollo de perfiles.
- `#include <abstractions/nameservice>` Incluye las reglas para permitri DNS, LDAP, NIS, SMB, contraseñas de usuarios y grupos, serivicos 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 lineas innecesarias, poniendo los directorios similares dentro de la lista entre lalves. 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 capabilites`.
- `owner archivo` Indica que solo puede accder 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 continuacion:

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

# Ejercicio 2

Voy a generar un perfil para el programa `nano`, la característica principal que voy a añadir es prohibirle el acceso a un archivo denominado `/root/archivoProhibido` el cual contiene los siguiente:

, 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.

A continuacion apareceran distintos archivos y capabilities relacionadas a las que debemos dar acceso o no.

Al ser el archivo de configuracion de nano, es recomendable deshabilitar los permisos de propietario, para que los demas usuarios puedan usarlo y permitirlo.

Ademas, aparece la opción de denegar el acceso a `/etc/passwd`, tras varias modificaciones he llegado a la conclusion de que es necesario para que detecte los usuarios que no sean root, por lo que hay que ponerle el mismo ajuste que a `/etc/nanorc`.

Finalmente, el archivo generado por defecto es el siguiente:

Como se puede ver, va a prohibir el acceso a cualuqier directorio.

Si se quiere que se permita acceso a los directorios `/home` y `/root`, pero prohibiendo el acceso a `/root/archivoProhibido` se debe poner lo siguiente:

Ahora, haciendo `systemctl reload apparmor` se recargan todos los perfiles.

Como se puede ver, si hago `nano /root/prueba` permite la creacion del archivo.

Sin embargo, si intento hacer `nano /root/archivoProhibido` no permite ni visualizarlo: