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/man`, 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.man`.

Las compoenntes principales son las siguientes:

- `#include <tunables/global>` carga un archivo que contiene las definiciones de las variables.
- `/usr/bin/man` Ruta absoluta del binario.
- `#include <abstractions/base>` obtiene los componentes de los perfiles de AppArmor para simplifcar el desarrollo de perfiles.
- `{,usr/}` Permite eliminar lineas innecesarias, poniendo los directorios similares dentro de la lista entre lalves. En este caso las opciones son `/bin/bzip2` y `/usr/bin/bzip2`
- `... -> &man_groff` Utiliza el perfil referenciado en la derecha cuando `man` utiliza algun comando de la izquierda.
- `profile ... {` Perfiles secundarios que se ejecutarán cuando estos sean llamados desde el principal. Por ejemplo, mediante el enlace de otro comando desde el perfil principal cuando man lo llame.

Además, despues de la ruta de los comadnos, aparecen letras similares a los permisos de sistemas Linux, estos representan:

- **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`, 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 comoprobaciones de permisos de lecutra 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 personlaizadas para el editor, al ser un archivo inofensivo se puede permitir su uso.