

SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software
Curso 2019-20

Práctica [1]. Administración de la seguridad en Linux.

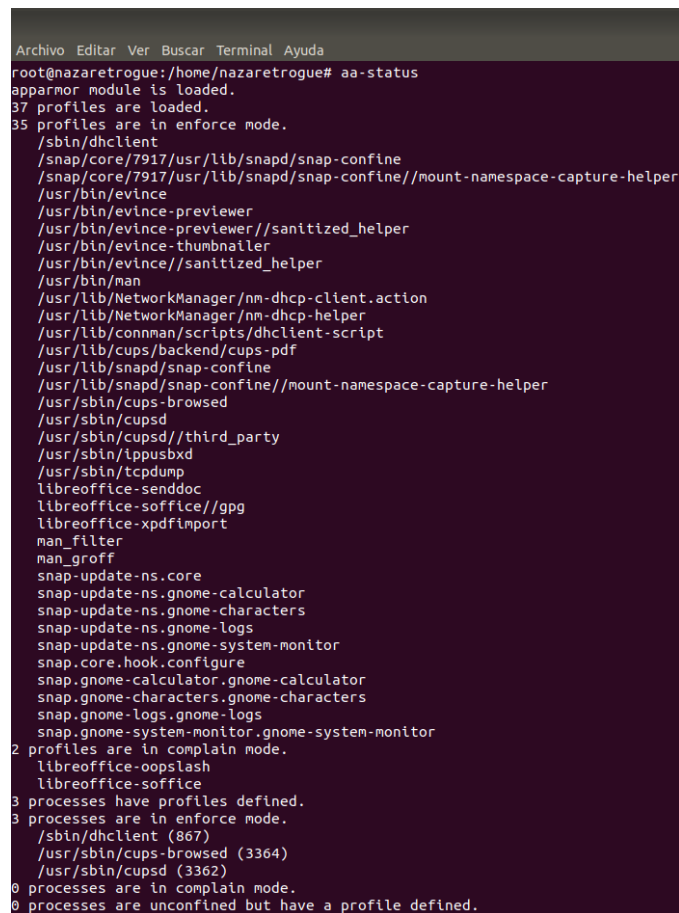
Sesión [3]. AppArmor

Autor¹: Nazaret Román Guerrero

Ejercicio 1.

Determinar los perfiles activos en la distribución Linux de tu equipo. Elige uno de los perfiles y analiza/comenta sus características.

Para mostrar todos los perfiles activos en el sistema, hay que utilizar la orden `aa-status`; la salida muestra lo siguiente:



```
Archivo Editar Ver Buscar Terminal Ayuda
root@nazaretroque:/home/nazaretroque# aa-status
apparmor module is loaded.
37 profiles are loaded.
35 profiles are in enforce mode.
/sbin/dhclient
/snap/core/7917/usr/lib/snapd/snap-confine
/snap/core/7917/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/usr/bin/evince
/usr/bin/evince-previewer
/usr/bin/evince-previewer//sanitized_helper
/usr/bin/evince-thumbnailer
/usr/bin/evince//sanitized_helper
/usr/bin/man
/usr/lib/NetworkManager/nm-dhcp-client.action
/usr/lib/NetworkManager/nm-dhcp-helper
/usr/lib/connman/scripts/dhclient-script
/usr/lib/cups/backend/cups-pdf
/usr/lib/snapd/snap-confine
/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/usr/sbin/cups-browsed
/usr/sbin/cupsd
/usr/sbin/cupsd//third_party
/usr/sbin/ippusbxd
/usr/sbin/tcpdump
libreoffice-senddoc
libreoffice-soffice//gpg
libreoffice-xpdfimport
man_filter
man_groff
snap-update-ns.core
snap-update-ns.gnome-calculator
snap-update-ns.gnome-characters
snap-update-ns.gnome-logs
snap-update-ns.gnome-system-monitor
snap.core.hook.configure
snap.gnome-calculator.gnome-calculator
snap.gnome-characters.gnome-characters
snap.gnome-logs.gnome-logs
snap.gnome-system-monitor.gnome-system-monitor
2 profiles are in complain mode.
libreoffice-oopslash
libreoffice-soffice
3 processes have profiles defined.
3 processes are in enforce mode.
/sbin/dhclient (867)
/usr/sbin/cups-browsed (3364)
/usr/sbin/cupsd (3362)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
```

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 ...”

Hay un total de 37 perfiles cargados, 35 de ellos en modo enforcement y 2 en modo complain.

Vamos a analizar uno de perfiles de algún proceso mostrado en la imagen anterior. Concretamente, vamos a analizar el perfil de Bonjour, un demonio que se encarga de buscar las impresoras disponibles y crear una cola para cada una de ellas. El archivo que debemos inspeccionar para ello es el `/etc/apparmor.d/usr.sbin.cups-browsed`.

El archivo muestra lo siguiente:

```
root@nazaretroque:/home/nazaretroque# cat /etc/apparmor.d/usr.sbin.cups-browsed
#include <tunables/global>

/usr/sbin/cups-browsed flags=(attach_disconnected) {
  #include <abstractions/base>
  #include <abstractions/nameservice>
  #include <abstractions/cups-client>
  #include <abstractions/dbus>
  #include <abstractions/p11-kit>

  /etc/cups/cups-browsed.conf r,
  /etc/cups/lpoptions r,
  /etc/cups/ppd/* r,
  /{var/,}run/cups/certs/* r,
  /var/cache/cups/* rw,
  /var/log/cups/* rw,
  /tmp/** rw,

  # Site-specific additions and overrides. See local/README for details.
  #include <local/usr.sbin.cups-browsed>
}
root@nazaretroque:/home/nazaretroque#
```

La primera línea (`#include <tunables/global>`) indica declaraciones de variables pertenecientes a otros ficheros del sistema, lo que permite que las mismas declaraciones formen parte de distintas aplicaciones pero estén en un solo archivo, de forma que no haya que incluir cada variable declarada en cada uno de los archivos donde se está usando, ya que dichas variables son utilizadas por muchos perfiles y añadirlas en cada archivo de cada perfil haría aumentar a éstos en tamaño.

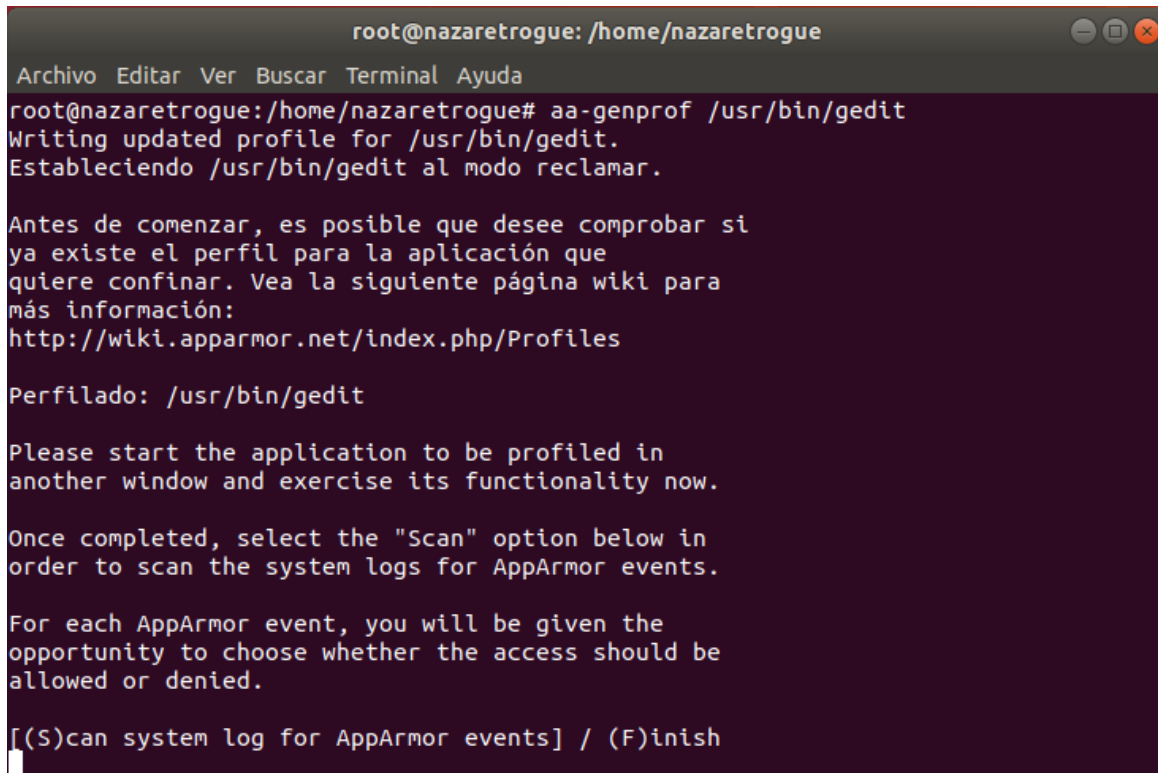
La segunda línea con los sucesivos `includes` se refiere a los path donde está el perfil de apparmor del programa. La bandera `attach_disconnected` significa que debe buscar dichos archivos fuera del espacio de nombres por defecto. Esto reduce el tamaño fichero del perfil de un proceso puesto que toma la información de otro fichero y no es necesario incluirla en él.

Las líneas restantes corresponden a archivos sobre los que el programa tiene ciertos permisos: `r` de lectura, `w` de escritura. O sea, el demonio Bonjour puede leer y escribir en los recursos listados.

Ejercicio 2.

Selecciona un programa de tu distribución que no tenga perfil asociado y crea y activa un perfil con los privilegios que estimes oportunos. Indica cómo se han reflejado éstos en el perfil.

Vamos a crear un perfil para el editor de texto de gedit. Para ello, primero generamos el perfil con la orden `aa-genprof /usr/bin/gedit`:



```
root@nazaretroque: /home/nazaretroque
Archivo Editar Ver Buscar Terminal Ayuda
root@nazaretroque:/home/nazaretroque# aa-genprof /usr/bin/gedit
Writing updated profile for /usr/bin/gedit.
Estableciendo /usr/bin/gedit al modo reclamar.

Antes de comenzar, es posible que desee comprobar si
ya existe el perfil para la aplicación que
quiere confinar. Vea la siguiente página wiki para
más información:
http://wiki.apparmor.net/index.php/Profiles

Perfilado: /usr/bin/gedit

Please start the application to be profiled in
another window and exercise its functionality now.

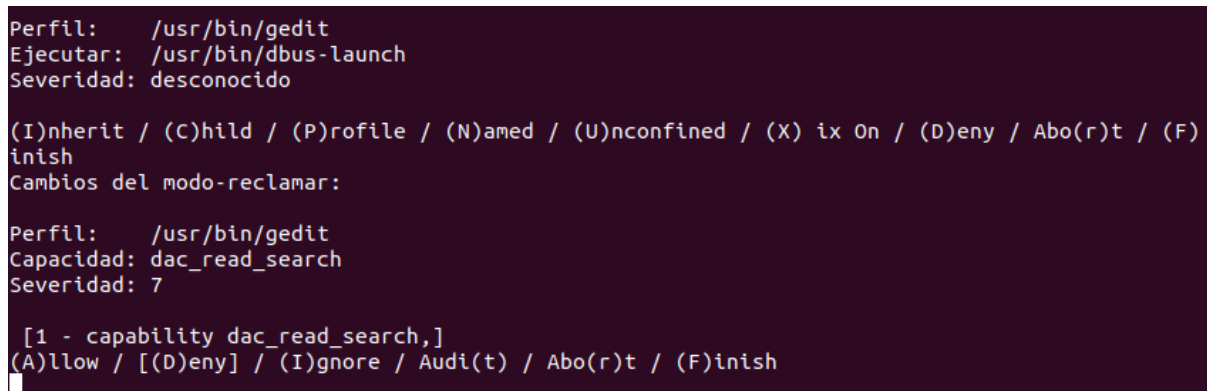
Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.

[(S)can system log for AppArmor events] / (F)inish
```

Una vez hecho esto, abrimos un nuevo terminal y probamos a iniciar la aplicación desde él. Puesto que se abre correctamente, pasamos a darle los permisos. Para ello, volvemos a la terminal que se muestra arriba y pulsamos la tecla S para escanear la aplicación y asignarle sus permisos.

El acceso de ejecución que se le ha dado es el mismo que el del padre, es decir, se pulsa la I para heredar dichos permisos.



```
Perfil: /usr/bin/gedit
Ejecutar: /usr/bin/dbus-launch
Severidad: desconocido

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X)ix On / (D)eny / Abo(r)t / (F)inish
Cambios del modo-reclamar:

Perfil: /usr/bin/gedit
Capacidad: dac_read_search
Severidad: 7

[1 - capability dac_read_search,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

Una vez dado el permiso de ejecución, se nos pregunta por diversos recursos a los que acceder, entre

los que se encuentran por ejemplo el acceso al bus del sistema, necesario para escribir los cambios de los archivos en disco, acceder a directorios del usuario, para poder crear, leer, actualizar y borrar archivos o sobrescribir archivos, necesario para cuando se creen ficheros con el mismo path absoluto. Concretamente estos tres permisos, que pueden resultar peligrosos si alguien entrara en nuestro sistema, han sido permitidos (A, Allow), y se muestran respectivamente en las siguientes imágenes:

- Acceso al bus del sistema:

```
Perfil:      /usr/bin/gedit
Ruta:       /run/dbus/system_bus_socket
Nuevo modo: owner rw
Severidad:  desconocido

[1 - #include <abstractions/dbus-strict>]
2 - owner /run/dbus/system_bus_socket rw,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
Añadiendo #include <abstractions/dbus-strict> al perfil.
```

- Acceso a directorios del usuario:

```
Perfil:      /usr/bin/gedit
Ruta:       /home/nazaretroque/
Nuevo modo: r
Severidad:  4

[1 - /home/*/ r,]
2 - /home/nazaretroque/ r,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
Añadiendo /home/*/ r, al perfil.
```

- Sobreescritura de archivos:

```
Perfil:      /usr/bin/gedit
Capacidad:  dac_override
Severidad:  9

[1 - capability dac_override,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
Añadiendo capability dac_override, al perfil.
```

Una vez establecidos los permisos de cada acción que puede llevar a cabo el proceso, finalizamos con F, guardando los cambios en /usr/bin/gedit:

```
= Changed Local Profiles =

Los siguientes perfiles locales se cambiaron. ¿Quiere guardarlos?

[1 - /usr/bin/gedit]
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean profiles / Abo(r)t
Writing updated profile for /usr/bin/gedit.

Perfilado: /usr/bin/gedit
```

Con esto hemos creado un perfil para un proceso que al principio (como se puede observar en la primera captura del ejercicio 1) no tenía. Todos los permisos que la aplicación pedía han sido

permitidos, puesto que sin accesos a ciertos directorios del sistema o, incluso, a la tabla de archivos del sistema, la aplicación no podría llevar a cabo bien su funcionalidad.