

SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática - Complementos de Ing. del Software

Curso 2018-19

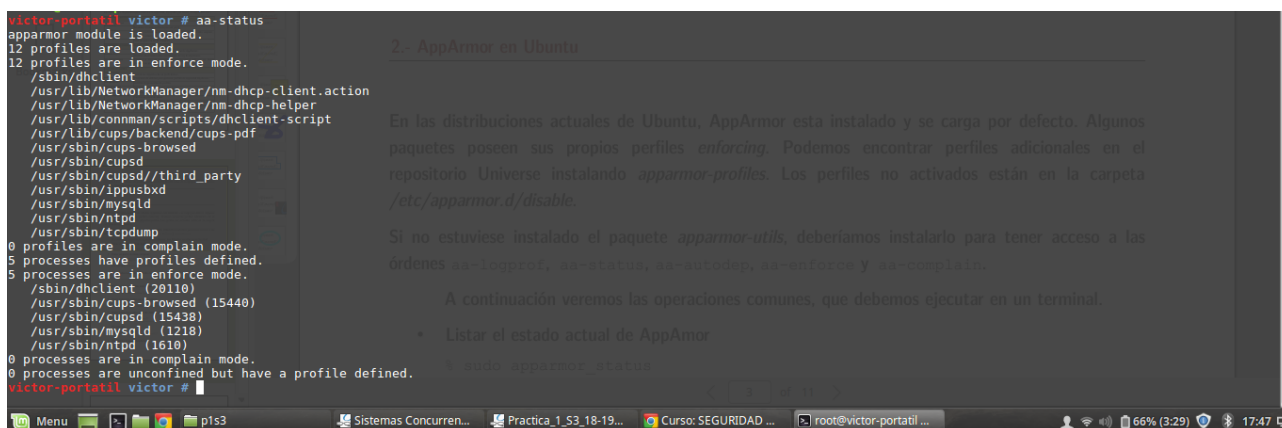
Práctica 1. Administración de la seguridad en Linux

Sesión 3. AppArmor

Autor¹: Víctor García Carrera

Ejercicio 1.

Comenzamos visualizando los perfiles de AppArmor que se encuentran activos en mi sistema. Una primera llamada al comando `aa-status` proporciona la siguiente salida:



```
victor@portatil:~$ aa-status
apparmor module is loaded.
12 profiles are loaded.
12 profiles are in enforce mode.
  /sbin/dhclient
  /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/sbin/cups-browsed
  /usr/sbin/cupsd
  /usr/sbin/cupsd/third_party
  /usr/sbin/ippusbxd
  /usr/sbin/mysqld
  /usr/sbin/ntpd
  /usr/sbin/tcpdump
0 profiles are in complain mode.
5 processes have profiles defined.
5 processes are in enforce mode.
  /sbin/dhclient (20110)
  /usr/sbin/cups-browsed (15440)
  /usr/sbin/cupsd (15438)
  /usr/sbin/mysqld (1218)
  /usr/sbin/ntpd (1610)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
victor@portatil:~$
```

2- AppArmor en Ubuntu

En las distribuciones actuales de Ubuntu, AppArmor está instalado y se carga por defecto. Algunos paquetes poseen sus propios perfiles *enforcing*. Podemos encontrar perfiles adicionales en el repositorio Universe instalando `apparmor-profiles`. Los perfiles no activados están en la carpeta `/etc/apparmor.d/disable`.

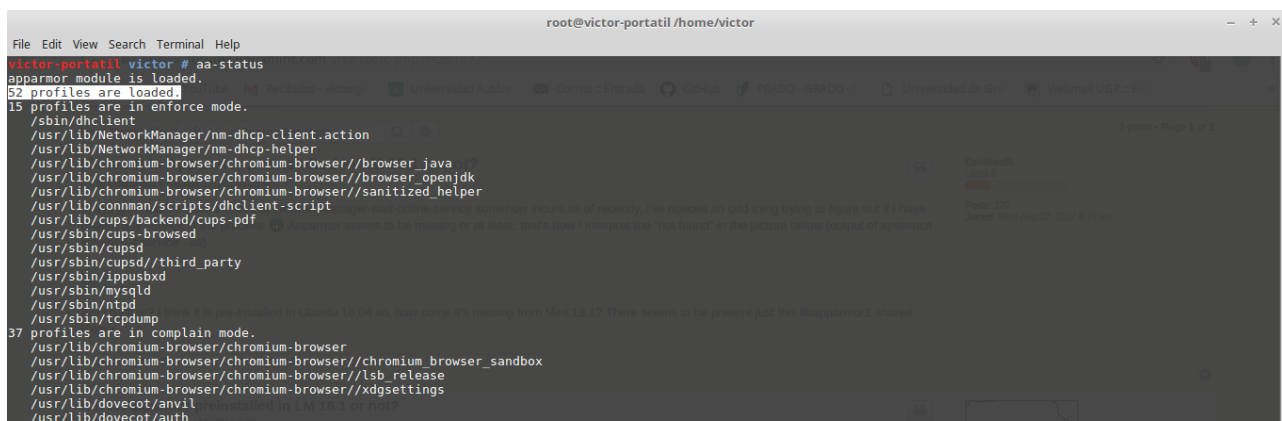
Si no estuviese instalado el paquete `apparmor-utils`, deberíamos instalarlo para tener acceso a los órdenes `aa-logprof`, `aa-status`, `aa-autodep`, `aa-enforce` y `aa-complain`.

A continuación veremos las operaciones comunes, que debemos ejecutar en un terminal.

- Listar el estado actual de AppArmor

```
$ sudo apparmor status
```

Podemos observar que hay 12 perfiles activos, todos ellos en modo enforce (lo que implica que se aplique la política establecida en ese perfil e informe de intentos de violación via `syslog` o `auditd`). Tras descargarme las librerías `apparmor-utils`, `apparmor-profiles` y `apparmor-profiles-extras` una nueva llamada a `aa-status` proporciona esta salida:



```
victor@portatil:~$ aa-status
apparmor module is loaded.
52 profiles are loaded.
15 profiles are in enforce mode.
  /sbin/dhclient
  /usr/lib/NetworkManager/nm-dhcp-client.action
  /usr/lib/NetworkManager/nm-dhcp-helper
  /usr/lib/chromium-browser/chromium-browser//browser_java
  /usr/lib/chromium-browser/chromium-browser//browser_openjdk
  /usr/lib/chromium-browser/chromium-browser//sanitized_helper
  /usr/lib/connman/scripts/dhclient-script
  /usr/lib/cups/backend/cups-pdf
  /usr/sbin/cups-browsed
  /usr/sbin/cupsd
  /usr/sbin/cupsd/third_party
  /usr/sbin/ippusbxd
  /usr/sbin/mysqld
  /usr/sbin/ntpd
  /usr/sbin/tcpdump
37 profiles are in complain mode.
  /usr/lib/chromium-browser/chromium-browser
  /usr/lib/chromium-browser/chromium-browser//chromium_browser_sandbox
  /usr/lib/chromium-browser/chromium-browser//lsb_release
  /usr/lib/chromium-browser/chromium-browser//xdgsettings
  /usr/lib/dovecot/avahi
  /usr/lib/dovecot/auth
```

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 ...”

```
root@victor-portatil /home/victor
File Edit View Search Terminal Help
/usr/lib/dovecot/dovecot-auth
/usr/lib/dovecot/dovecot-lda
/usr/lib/dovecot/dovecot-lda//usr/sbin/sendmail
/usr/lib/dovecot/imap
/usr/lib/dovecot/imap-login
/usr/lib/dovecot/lmtp
/usr/lib/dovecot/lmtp
/usr/lib/dovecot/log
/usr/lib/dovecot/managesieve
/usr/lib/dovecot/managesieve-login
/usr/lib/dovecot/pop3
/usr/lib/dovecot/pop3-login
/usr/lib/dovecot/ssl-params
/usr/sbin/avahi-daemon
/usr/sbin/dnsmasq
/usr/sbin/dnsmasq//libvirt_leaseshelper
/usr/sbin/dovecot
/usr/sbin/identd
/usr/sbin/mdnsd
/usr/sbin/nmbd
/usr/sbin/nsd
/usr/sbin/smbd
/usr/sbin/smbldap-useradd
/usr/sbin/smbldap-useradd//etc/init.d/nsd
/usr/{sbin/traceroute,bin/traceroute.db}
/{usr/,}bin/ping
klogd
syslog-ng
syslogd
8 processes have profiles defined.
5 processes are in enforce mode.
/sbin/dhclient (20110)
/usr/sbin/cups-browsed (15440)
/usr/sbin/cupsd (15438)
/usr/sbin/mysqld (1218)
/usr/sbin/ntpd (1610)
0 processes are in complain mode.
3 processes are unconfined but have a profile defined.
/usr/sbin/avahi-daemon (954)
/usr/sbin/avahi-daemon (1003)
/usr/sbin/dnsmasq (1355)
En este apartado trabajamos con el comando /ls/, que nos permite listar los ficheros
```

A continuación vamos a analizar las características del perfil `{usr/,}bin/ping`. Los perfiles de AppArmor se localizan en el directorio `/etc/apparmor.d/` en forma de simples ficheros de texto. Allí, el perfil de `/bin/ping` se encuentra como el archivo `bin.ping`, el cual visualizamos en un editor de texto con la orden `gedit bin.ping` para poder ver sus características.

```
victor-portatil victor # cd /etc/apparmor.d/
victor-portatil apparmor.d # ls
abstractions  sbin.klogd          usr.lib.dovecot.config  usr.lib.dovecot.log      usr.sbin.cupsd  usr.sbin.nscd
apache2.d    sbin.syslogd        usr.lib.dovecot.deliver  usr.lib.dovecot.managesieve  usr.sbin.dnsmasq  usr.sbin.ntpd
bin.ping     sbin.syslog-ng      usr.lib.dovecot.dict     usr.lib.dovecot.managesieve-login  usr.sbin.dovecot  usr.sbin.rsyslogd
cache        tunables            usr.lib.dovecot.dovecot-auth  usr.lib.dovecot.managesieve  usr.sbin.dovecot  usr.sbin.smbd
disable      usr.bin.chromium-browser  usr.lib.dovecot.dovecot-lda  usr.lib.dovecot.pop3      usr.sbin.identd  usr.sbin.smbldap-useradd
force-complain  usr.bin.firefox      usr.lib.dovecot.dovecot-lda  usr.lib.dovecot.pop3-login  usr.sbin.ippusbxd  usr.sbin.smbd
local        usr.lib.dovecot.anvil  usr.lib.dovecot.imap      usr.lib.dovecot.ssl-params  usr.sbin.mdnsd  usr.sbin.tcpcdump
sbin.dhclient  usr.lib.dovecot.auth  usr.lib.dovecot.imap-login  usr.sbin.avahi-daemon      usr.sbin.mysqld  usr.sbin.traceroute
victor-portatil apparmor.d # vm bin.ping
The program 'vm' is currently not installed. You can install it by typing:
apt install mgetty-voice
victor-portatil apparmor.d # gedit bin.ping
```

```
bin.ping
/etc/apparmor.d
File Edit View Search Tools Documents Help
#
# Copyright (C) 2002-2009 Novell/SUSE
# Copyright (C) 2010 Canonical Ltd.
#
# This program is free software; you can redistribute it and/or
# modify it under the terms of version 2 of the GNU General Public
# License published by the Free Software Foundation.
#
#-----
#include <tunables/global>
/{usr/,}bin/ping flags=(complain) {
#include <abstractions/base>
#include <abstractions/consoles>
#include <abstractions/nameservice>

capability net_raw,
capability setuid,
network inet raw,

/{usr/,}bin/ping mixr,
/etc/modules.conf r,

# Site-specific additions and overrides. See local/README for details.
#include <local/bin.ping>
}
```

La primera línea, `#include <tunables/global>` carga un fichero con definiciones de variables y declaraciones de otros ficheros, lo cual resulta útil para localizar en un único fichero (como el *global*) declaraciones comunes a varios perfiles y aplicaciones.

La línea `{usr,}bin/ping flags=(complain)` establece la ruta al programa en cuestión (al programa al cual se aplica este perfil). Además, establece el modo de este perfil como *complain* (modo en el que no hace cumplir la política pero informa de los intentos de violación).

Las llaves `{}` que siguen a continuación delimitan la región de código donde se pueden incluir declaraciones, subperfiles...

El `#include <abstractions/base>` carga un fichero base con componentes de perfiles de AppArmor para así simplificar estos. Los otros includes realizan tareas similares.

capability net_raw permite a la aplicación acceder a la capacidad de `CAP_NET_RAW` de Posix.1e la cual permite utilizar raw y packet sockets, en el primer caso un socket de comunicación (socket de red) que permite enviar y recibir directamente paquetes IP sin ninguna especificación acerca del protocolo del nivel de transporte, utilizado por ejemplo por aplicaciones como Nmap. En este caso tiene todo el sentido al tratarse de la aplicación de ping que envía paquetes ICMP de solicitud y respuesta para evaluar el estado y diversos parámetros de una red. Los packet sockets son similares a los raw sockets pero en el nivel de enlace (link layer).

capability setuid permite acceder a la capacidad de `CAP_SETUID` de Posix.1e que permite modificar el UID (user ID) de los procesos de forma arbitraria, usado por ejemplo para falsificar el UID al pasar las credenciales del socket a través de sockets de dominio UNIX.

Finalmente, las líneas `{usr,}bin/ping mixr` y `/etc/modules.conf r` proporcionan a la aplicación diversos permisos (lectura, escritura, ejecución) sobre los ficheros especificados a través de su ruta absoluta, en este caso el fichero *ping* que permite `PROT_EXC` con nmap (m), tiene el modo de ejecución heredado (ix) y permite lectura (r), y *modules.conf* con permiso de lectura (r).

Ejercicio 2.

En este apartado vamos a seleccionar la aplicación gedit, editor de texto, y crearemos y activaremos un perfil para la misma. A través del comando `sudo aa-genprof /usr/bin/gedit` entramos en el creador del perfil, que establece que abramos en otra ventana la aplicación en cuestión, hagamos un uso normal de ella y volvamos a esta ventana de creación del perfil donde seleccionamos escanear o Scan para que evalúe las acciones llevadas a cabo registradas en los logs del sistema y nos pregunte acerca de diversas acciones y qué permisos queremos darles. En mi configuración cabe destacar que denegé la utilización de sockets de comunicación (por lo que la aplicación no puede establecer ninguna comunicación de red) y denegé la librería de idioma del inglés de US o United States utilizada para la corrección y sugerencia de palabras. También denegé los permisos de lectura y escritura del archivo creado para probar la aplicación “*pruebagedit*”.

```
victor@victor-portatil /etc/apparmor.d
File Edit View Search Terminal Help
victor@victor-portatil /etc/apparmor.d $ sudo aa-genprof /usr/bin/gedit
Writing updated profile for /usr/bin/gedit.
Setting /usr/bin/gedit to complain mode.

Before you begin, you may wish to check if a profile already exists for the application you wish to confine. See the following wiki page for more information:
http://wiki.apparmor.net/index.php/Profiles

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.

Profiling: /usr/bin/gedit
[(S)can system log for AppArmor events] / (F)inish
Reading log entries from /var/log/syslog.
Updating AppArmor profiles in /etc/apparmor.d
Complain-mode changes:

Profile: /usr/bin/gedit
Network Family: netlink
Socket Type: raw

[1 - #include <abstractions/namespace>]
[2 - network netlink raw,
(A)llow / (D)eny / (I)gnore / Audi(t) / Abo(r)t / (F)inish
Adding deny network netlink raw, to profile.

Profile: /usr/bin/gedit
Path: /etc/fonts/conf.avail/10-antialias.conf
Mode: r
Severity: unknown

[1 - #include <abstractions/fonts>]
[2 - #include <abstractions/gnome>]
[3 - #include <abstractions/kde>]
[4 - #include <abstractions/ubuntu-browsers.d/chromium-browser>]
```

```
victor@victor-portatil /etc/apparmor.d
File Edit View Search Terminal Help

[1 - /home/victor/.config/enchant/en_GB.exc
[2 - /home/*/.config/enchant/en_GB.exc]
[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore

Profile: /usr/bin/gedit
Path: /home/victor/.config/enchant/en_US.dic
Mode: rw
Severity: 6

[1 - /home/victor/.config/enchant/en_US.dic
[2 - /home/*/.config/enchant/en_US.dic]
[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore

Profile: /usr/bin/gedit
Path: /home/victor/.config/enchant/en_US.exc
Mode: rw
Severity: 6

[1 - /home/victor/.config/enchant/en_US.exc
[2 - /home/*/.config/enchant/en_US.exc]
[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore

Profile: /usr/bin/gedit
Path: /home/victor/.config/gedit/accels
Mode: rw
Severity: 6

[1 - /home/victor/.config/gedit/accels
[2 - /home/*/.config/gedit/accels]
[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore
Adding /home/*/.config/gedit/accels rw to profile

Profile: /usr/bin/gedit
Path: /home/victor/.config/gtk-3.0/bookmarks
Mode: r
Severity: 4

[1 - /home/victor/.config/gtk-3.0/bookmarks
[2 - /home/*/.config/gtk-3.0/bookmarks]
[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore
Adding /home/*/.config/gtk-3.0/bookmarks r to profile

Profile: /usr/bin/gedit
Path: /home/victor/.config/user-dirs.dirs
```

```
victor@victor-portatil /etc/apparmor.d

File Edit View Search Terminal Help

1 - /home/victor/.viminfo
[2 - /home/*/.viminfo]
[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore
Adding /home/*/.viminfo r to profile

Profile: /usr/bin/gedit
Path: /home/victor/.xsession-errors
Mode: r
Severity: 4

1 - /home/victor/.xsession-errors
[2 - /home/*/.xsession-errors]
[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore
Adding /home/*/.xsession-errors r to profile

Profile: /usr/bin/gedit
Path: /home/victor/Documents/UGR/scd/practicas/pl1/
Mode: r
Severity: 4

1 - /home/victor/Documents/UGR/scd/practicas/pl1/
[2 - /home/*/Documents/UGR/scd/practicas/pl1/]
[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore
Adding /home/*/Documents/UGR/scd/practicas/pl1/ r to profile

Profile: /usr/bin/gedit
Path: /home/victor/pruebaACL
Mode: r
Severity: 4

1 - /home/victor/pruebaACL
[2 - /home/*/pruebaACL]
[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore
Adding /home/*/pruebaACL r to profile

Profile: /usr/bin/gedit
Path: /home/victor/pruebagedit
Mode: rw
Severity: 6

1 - /home/victor/pruebagedit
[2 - /home/*/pruebagedit]
[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore

```

Tras finalizar la creación del perfil, ya se encuentra activado en modo enforce como comprobamos con una nueva llamada a **aa-status**:

```
victor@victor-portatil /etc/apparmor.d

File Edit View Search Terminal Help

victor@victor-portatil /etc/apparmor.d $ sudo aa-status
[sudo] password for victor:
apparmor module is loaded.
53 profiles are loaded.
16 profiles are in enforce mode.
  /sbin/dhclient
  /usr/bin/gedit
  /usr/lib/NetworkManager/nm-dhcp-client.action
  /usr/lib/NetworkManager/nm-dhcp-helper
  /usr/lib/chromium-browser/chromium-browser//browser_java
  /usr/lib/chromium-browser/chromium-browser//browser_openjdk
  /usr/lib/chromium-browser/chromium-browser//sanitized_helper
  /usr/lib/connman/scripts/dhclient-script
  /usr/lib/cups/backend/cups-pdf
  /usr/sbin/cups-browsed
  /usr/sbin/cupsd
  /usr/sbin/cupsd//third_party
  /usr/sbin/ippusbxd
  /usr/sbin/mysqld
  /usr/sbin/ntpd
  /usr/sbin/tcpdump
37 profiles are in complain mode.
  /usr/lib/chromium-browser/chromium-browser
  /usr/lib/chromium-browser/chromium-browser//chromium_browser_sandbox
  /usr/lib/chromium-browser/chromium-browser//lsb_release
  /usr/lib/chromium-browser/chromium-browser//xdgsettings
  /usr/lib/dovecot/anvil
  /usr/lib/dovecot/auth
  /usr/lib/dovecot/config
  /usr/lib/dovecot/deliver
  /usr/lib/dovecot/dict
  /usr/lib/dovecot/dovecot-auth
  /usr/lib/dovecot/dovecot-lda
  /usr/lib/dovecot/dovecot-lda//usr/sbin/sendmail
  /usr/lib/dovecot/imap
  /usr/lib/dovecot/imap-login
  /usr/lib/dovecot/imap
  /usr/lib/dovecot/log
  /usr/lib/dovecot/managesieve
  /usr/lib/dovecot/managesieve-login
  /usr/lib/dovecot/pop3
  /usr/lib/dovecot/pop3-login
  /usr/lib/dovecot/ssl-params
  /usr/sbin/avahi-daemon
  /usr/sbin/dnsmasq

```

Al intentar abrir cualquier archivo con gedit, compruebo un fallo inesperado: Al haber denegado el socket de comunicación no puede establecer conexión con el servidor y no encuentra los archivos.

```
victor@victor-portatil ~

File Edit View Search Terminal Help

victor@victor-portatil ~ $ gedit
Failed to connect to Mir: Failed to connect to server socket: No such file or directory
Unable to init server: Could not connect: Connection refused

(gedit:4015): Gtk-WARNING **: cannot open display: :0
victor@victor-portatil ~ $
```