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 [4]. **AppAmor.**

Autor[1]: **Matilde Cabrera González**

Ejercicio 4.1

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

```
mati@mati-VirtualBox:~$ sudo aa-status
apparmor module is loaded.
33 profiles are loaded.
33 profiles are in enforce mode.
   /sbin/dhclient
   /snap/core/5548/usr/lib/snapd/snap-confine
   /snap/core/5548/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-thumbnailer//sanitized_helper
   /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
   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
0 profiles are in complain mode.
3 processes have profiles defined.
3 processes are in enforce mode.
   /sbin/dhclient (2769)
   /usr/sbin/cups-browsed (2545)
   /usr/sbin/cupsd (2543)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
mati@mati-VirtualBox:~$
```

[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 ..."

Podemos ver 33 perfiles activos, todos están en modo “enforce”, modo estricto (33 profiles are in enforce mode). 3 de los perfiles activos tienen un proceso definido (3 processes have profiles defined), estos son:
/sbin/dhclient (2769)
/usr/sbin/cups-browsed (2545)
/usr/sbin/cupsd (2543)

Como podemos ver indica la ruta de donde se encuentra el servicio indicado.

Listamos todos los procesos que pueden ejecutar AppArmor con “ps auxZ | grep -v ‘^unconfined’”

```
mati@mati-VirtualBox:~$ ps auxZ | grep -v '^unconfined'
LABEL                          USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
/usr/sbin/cupsd (enforce)      root      2543  0.0  0.1 108204  8724 ?        Ss   12:43   0:00 /usr/sbin/cupsd -l
/usr/sbin/cups-browsed (enforce) root    2545  0.0  0.2 303652 10984 ?        Ssl  12:43   0:00 /usr/sbin/cups-browsed
/sbin/dhclient (enforce)       root      2769  0.0  0.1  25656  6144 ?        S    15:07   0:00 /sbin/dhclient -d -q -sf
 /usr/lib/NetworkManager/nm-dhcp-helper -pf /run/dhclient-enp0s3.pid -lf /var/lib/NetworkManager/dhclient-f3358877-4608-3
f2f-a750-9502853d62d2-enp0s3.lease -cf /var/lib/NetworkManager/dhclient-enp0s3.conf enp0s3
```

Los perfiles de AppArmor se guardan en /etc/apparmor.d/ y contienen una lista de reglas de control de acceso sobre los recursos que pueden utilizar cada programa.

```
mati@mati-VirtualBox:~$ ls /etc/apparmor.d/
abstractions     local           usr.bin.firefox                 usr.sbin.cupsd
cache            sbin.dhclient   usr.bin.man                     usr.sbin.ippusbxd
disable          tunables        usr.lib.snapd.snap-confine.real usr.sbin.rsyslogd
force-complain   usr.bin.evince  usr.sbin.cups-browsed           usr.sbin.tcpdump
```

Rsyslog es el servicio encargado de las anotaciones diarias, de los logs del sistema. AppArmor permite asociar a cada programa un perfil de seguridad y restringir sus capacidades. Rsyslogd debería estar siempre corriendo, aunque en la imagen anterior sala disable.

```
mati@mati-VirtualBox:~$ cat /etc/apparmor.d/usr.sbin.rsyslogd
# Last Modified: Sun Sep 25 08:58:35 2011
#include <tunables/global>

# Debugging the syslogger can be difficult if it can't write to the file
# that the kernel is logging denials to. In these cases, you can do the
# following:
# watch -n 1 'dmesg | tail -5'

/usr/sbin/rsyslogd {
  #include <abstractions/base>
  #include <abstractions/nameservice>

  capability sys_tty_config,
  capability dac_override,
  capability dac_read_search,
  capability setuid,
  capability setgid,
  capability sys_nice,
  capability syslog,

  unix (receive) type=dgram,
  unix (receive) type=stream,
```

```
  £ rsyslog configuration
  /etc/rsyslog.conf r,
  /etc/rsyslog.d/ r,
  /etc/rsyslog.d/** r,
  /{,var/}run/rsyslogd.pid{,.tmp} rwk,
  /var/spool/rsyslog/ r,
  /var/spool/rsyslog/** rwk,

  /usr/lib{,32,64}/{,@{multiarch}/}rsyslog/*.so mr,

  /dev/tty*                       rw,
  /dev/xconsole                   rw,
  @{PROC}/kmsg                    r,

  /dev/log                        rwl,
  /{,var/}run/utmp                rk,
  /var/lib/*/dev/log              rwl,
  /var/spool/postfix/dev/log      rwl,
  /{,var/}run/systemd/notify      w,

  £ 'r' is needed when using imfile
  /var/log/**                     rw,

  £ Add these for mysql support
  £/etc/mysql/my.cnf r,
  £/{,var/}run/mysqld/mysqld.sock rw,

  £ Add thes for postgresql support
  ££include <abstractions/openssl>
  ££include <abstractions/ssl_certs>
  £/{,var/}run/postgresql/.s.PGSQL.*[0-9] rw,

  £ Site-specific additions and overrides. See local/README for details.
  £include <local/usr.sbin.rsyslogd>
}
mati@mati-VirtualBox:~$
```

Llama la atención los permisos rwl, esto indica que varios perfiles están cruzados, es decir, cuando un proceso realiza una operación con un segundo proceso en diferentes perfiles, ambos perfiles tienen que permitir la operación. Entiendo que varios perfiles comparten procesos.
R – leer, w- escribir, k – lock – permiso para bloquear un archivo, vemos rwk, se combinan para determinar el bloqueo exclusivo.

Vemos que contiene varios includes:
Include <tunables/global>

```
mati@mati-VirtualBox:~$ cat /etc/apparmor.d/tunables/global
£ ------------------------------------------------------------------
£
£    Copyright (C) 2006-2009 Novell/SUSE
£    Copyright (C) 2010-2014 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.
£
£ ------------------------------------------------------------------

£ All the tunables definitions that should be available to every profile
£ should be included here

£include <tunables/home>
£include <tunables/multiarch>
£include <tunables/proc>
£include <tunables/alias>
£include <tunables/kernelvars>
£include <tunables/xdg-user-dirs>
```

Include <abstractions/base>

```
mati@mati-VirtualBox:~$ cat /etc/apparmor.d/abstractions/base
£ vim:syntax=apparmor
£ ------------------------------------------------------------------
£
£    Copyright (C) 2002-2009 Novell/SUSE
£    Copyright (C) 2009-2011 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.
£
£ ------------------------------------------------------------------



  £ (Note that the ldd profile has inlined this file; if you make
  £ modifications here, please consider including them in the ldd
  £ profile as well.)

  £ The __canary_death_handler function writes a time-stamped log
  £ message to /dev/log for logging by syslogd. So, /dev/log, timezones,
  £ and localisations of date should be available EVERYWHERE, so
  £ StackGuard, FormatGuard, etc., alerts can be properly logged.
  /dev/log                       w,
  /dev/random                    r,
  /dev/urandom                   r,
  /etc/locale/**                 r,
  /etc/locale.alias              r,
  /etc/localtime                 r,
  /etc/writable/localtime        r,
  /usr/share/locale-bundle/**    r,
  /usr/share/locale-langpack/**  r,
  /usr/share/locale/**           r,
  /usr/share/**/locale/**        r,
  /usr/share/zoneinfo/           r,
  /usr/share/zoneinfo/**         r,
  /usr/share/X11/locale/**       r,
  /run/systemd/journal/dev-log w,
  £ systemd native journal API (see sd_journal_print(4))
  /run/systemd/journal/socket w,
  £ Nested containers and anything using systemd-cat need this. 'r' shouldn't
  £ be required but applications fail without it. journald doesn't leak
  £ anything when reading so this is ok.
  /run/systemd/journal/stdout rw,
```

Establece los permisos, r con lectura, w ejecutables, contiene la base para el resto de programas.

Include <abstractions/nameservice>

Nameservice es igual al anterior, pero para los programas.

Include <abstractions/openssl>

```
mati@mati-VirtualBox:~$ cat /etc/apparmor.d/abstractions/openssl
# ------------------------------------------------------------------
#
#    Copyright (C) 2011 Novell/SUSE
#
#    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.
#
# ------------------------------------------------------------------

  /etc/ssl/openssl.cnf r,
  /usr/share/ssl/openssl.cnf r,
  @{PROC}/sys/crypto/fips_enabled r,
```

Include <abstractions/ssl_certs>

```
mati@mati-VirtualBox:~$ cat /etc/apparmor.d/abstractions/ssl_certs
# ------------------------------------------------------------------
#
#    Copyright (C) 2002-2005 Novell/SUSE
#    Copyright (C) 2010-2011 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.
#
# ------------------------------------------------------------------

  /etc/ssl/ r,
  /etc/ssl/certs/ r,
  /etc/ssl/certs/* r,
  /etc/pki/trust/ r,
  /etc/pki/trust/* r,
  /etc/pki/trust/anchors/ r,
  /etc/pki/trust/anchors/** r,
  /usr/share/ca-certificates/ r,
  /usr/share/ca-certificates/** r,
  /usr/share/ssl/certs/ca-bundle.crt          r,
  /usr/local/share/ca-certificates/ r,
  /usr/local/share/ca-certificates/** r,
  /var/lib/ca-certificates/ r,
  /var/lib/ca-certificates/** r,

  # acmetool
  /var/lib/acme/certs/*/chain r,
  /var/lib/acme/certs/*/cert r,
mati@mati-VirtualBox:~$
```

Ejercicio 4.2

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 estos en el perfil.

He tenido que instalar el paquete de utilidades de apparmor.

```
mati@mati-VirtualBox:~$ aa-genprof vim

No se ha encontrado la orden «aa-genprof», pero se puede instalar con:

sudo apt install apparmor-utils

mati@mati-VirtualBox:~$ sudo apt install apparmor-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  python3-apparmor python3-libapparmor
Paquetes sugeridos:
  vim-addon-manager
```

Vamos a crear un perfil para vim, editor de textos.

```
mati@mati-VirtualBox:~$ sudo aa-genprof /usr/bin/vim
Writing updated profile for /usr/bin/vim.gtk.
Estableciendo /usr/bin/vim.gtk 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/vim.gtk

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
```

Vamos siguiendo las instrucciones de la terminal.

```
[(S)can system log for AppArmor events] / (F)inish
Reading log entries from /var/log/syslog.
Updating AppArmor profiles in /etc/apparmor.d.
Cambios del modo-reclamar:

Perfil:     /usr/bin/vim.gtk
Ruta:       /usr/share/vim/vim80/lang/es/LC_MESSAGES/vim.mo
Nuevo modo: r
Severidad:  3

 [1 - #include <abstractions/evince>]
  2 - /usr/share/vim/vim80/lang/es/LC_MESSAGES/vim.mo r,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)
inish
```

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

Perfil:     /usr/bin/vim.gtk
Ruta:       /home/mati/
Nuevo modo: owner r
Severidad:  4

 [1 - owner /home/*/ r,]
  2 - owner /home/mati/ r,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permi
ssions off / Abo(r)t / (F)inish

Perfil:     /usr/bin/vim.gtk
Ruta:       /home/mati/
Nuevo modo: owner r
Severidad:  4

  1 - owner /home/*/ r,
  2 - owner /home/mati/ r,
 [3 - owner /**/ r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permi
ssions off / Abo(r)t / (F)inish

Perfil:     /usr/bin/vim.gtk
Ruta:       /etc/vim/vimrc
Nuevo modo: r
Severidad:  desconocido

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

Perfil:     /usr/bin/vim.gtk
Ruta:       /etc/vim/gvimrc
Nuevo modo: r
Severidad:  desconocido

 [1 - /etc/vim/gvimrc r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)
inish
```

Vemos los cambios producidos

```
--- /etc/apparmor.d/usr.bin.vim.gtk     2018-10-18 13:01:11.686927605 +0200
+++ /tmp/tmp2ijceekm    2018-10-18 13:09:48.492214733 +0200
@@ -4,7 +4,15 @@
 /usr/bin/vim.gtk flags=(complain) {
   #include <abstractions/base>

+  #include <abstractions/dbus-session-strict>
+  #include <abstractions/evince>
+  #include <abstractions/ubuntu-browsers.d/plugins-common>
+
   /lib/x86_64-linux-gnu/ld-*.so mr,
   /usr/bin/vim.gtk mr,

+  /etc/vim/gvimrc r,
+  /etc/vim/vimrc r,
+  owner /home/*/.ICEauthority r,
+
 }
/tmp/tmptw6iclk7 (END)
```

Lo ponemos en modo complain

```
mati@mati-VirtualBox:~$ sudo aa-complain vim
Estableciendo /usr/bin/vim.gtk al modo reclamar.
```

Compruebo en log el trabajo de hoy

```
Oct 18 12:59:03 mati-VirtualBox sudo:     mati : TTY=pts/0 ; PWD=/home/mati ; USER=root ; COMMAND=/usr/bin/apt install apparmor-utils
Oct 18 12:59:03 mati-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 18 12:59:28 mati-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Oct 18 13:01:08 mati-VirtualBox sudo:     mati : TTY=pts/0 ; PWD=/home/mati ; USER=root ; COMMAND=/usr/sbin/aa-genprof /usr/bin/vim
Oct 18 13:01:08 mati-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 18 13:10:35 mati-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Oct 18 13:13:20 mati-VirtualBox sudo:     mati : TTY=pts/0 ; PWD=/home/mati ; USER=root ; COMMAND=/usr/sbin/aa-complain vim
```

Volvemos a ver los perfiles activos en la distribución y aparecen los cambios. Tenemos vim.gtk

```
2 profiles are in complain mode.
   /usr/bin/vim.gtk
   snap.skype.skype
3 processes have profiles defined.
3 processes are in enforce mode.
   /sbin/dhclient (5453)
   /usr/sbin/cups-browsed (9290)
   /usr/sbin/cupsd (9288)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
```