SEGURIDAD EN SISTEMAS OPERATIVOS

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

Curso 2017-18

Práctica [1]

Sesión [3]

Autor[1]: Iván Rodríguez Millán.

Ejercicio 1.

Para determinar los perfiles activos de nuestro sistema Linux tenemos la orden:

apparmor_status

Según se nos indica en la propia documentación de Ubuntu: https://help.ubuntu.com/lts/serverguide/apparmor.html

Que en nuestro caso nos da la siguiente información:

apparmor module is loaded.

20 profiles are loaded.

20 profiles are in enforce mode.

/sbin/dhclient

/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/lib/NetworkManager/nm-dhcp-client.action

/usr/lib/connman/scripts/dhclient-script

/usr/lib/cups/backend/cups-pdf

/usr/lib/lightdm/lightdm-guest-session

/usr/lib/lightdm/lightdm-guest-session//chromium

/usr/lib/telepathy/mission-control-5

/usr/lib/telepathy/telepathy-*

/usr/lib/telepathy/telepathy-*//pxgsettings

/usr/lib/telepathy/telepathy-*//sanitized_helper

---

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 ..."

/usr/lib/telepathy/telepathy-ofono

/usr/sbin/cups-browsed

/usr/sbin/cupsd

/usr/sbin/tcpdump

0 profiles are in complain mode.

4 processes have profiles defined.

4 processes are in enforce mode.

/sbin/dhclient (868)

/usr/lib/telepathy/mission-control-5 (2980)

/usr/sbin/cups-browsed (1217)

/usr/sbin/cupsd (3055)

0 processes are in complain mode.

0 processes are unconfined but have a profile defined.

b)

Los perfiles son arhivos de texto plano almacenados en /etc/apparmor.d/ .

En nuestro caso:

```
root@ubuntu:/etc/apparmor.d# ls
abstractions  force-complain        sbin.dhclient  usr.bin.evince    usr.sbin.cups-browsed  usr.sbin.tcpdump
cache         lightdm-guest-session  snap           usr.bin.firefox   usr.sbin.cupsd
disable       local                  tunables       usr.lib.telepathy  usr.sbin.rsyslogd
```

Para analizar sus características escogeremos usr.bin.firefox, que es el perfil que tiene asociado Firefox.

Tenemos lo siguiente:

```
# vim:syntax=apparmor
# Author: Jamie Strandboge <jamie@canonical.com>

# Declare an apparmor variable to help with overrides
@{MOZ_LIBDIR}=/usr/lib/firefox

#include <tunables/global>

# We want to confine the binaries that match:
#  /usr/lib/firefox/firefox
#  /usr/lib/firefox/firefox
# but not:
#  /usr/lib/firefox/firefox.sh
/usr/lib/firefox/firefox{,*[^s][^h]} {
  #include <abstractions/audio>
  #include <abstractions/cups-client>
  # TODO: finetune this for required accesses
  #include <abstractions/dbus>
  #include <abstractions/dbus-accessibility>
  #include <abstractions/dbus-session>
  #include <abstractions/gnome>
  #include <abstractions/ibus>
  #include <abstractions/nameservice>
  #include <abstractions/openssl>
  #include <abstractions/p11-kit>

  # Addons
  #include <abstractions/ubuntu-browsers.d/firefox>

  # for networking
  network inet stream,
  network inet6 stream,
  @{PROC}/[0-9]*/net/if_inet6 r,
  @{PROC}/[0-9]*/net/ipv6_route r,
  @{PROC}/[0-9]*/net/dev r,
```

```
@{PROC}/[0-9]*/net/wireless r,

# should maybe be in abstractions
/etc/ r,
/etc/mime.types r,
/etc/mailcap r,
/etc/xdg/*buntu/applications/defaults.list    r, # for all derivatives
/etc/xfce4/defaults.list r,
/usr/share/xubuntu/applications/defaults.list r,
owner @{HOME}/.local/share/applications/defaults.list r,
owner @{HOME}/.local/share/applications/mimeapps.list r,
owner @{HOME}/.local/share/applications/mimeinfo.cache r,
owner /tmp/** m,
owner /var/tmp/** m,
owner /{,var/}run/shm/shmfd-* rw,
owner /{dev,run}/shm/org.chromium.* rwk,
/tmp/.X[0-9]*-lock r,
/etc/udev/udev.conf r,
# Doesn't seem to be required, but noisy. Maybe allow 'r' for 'b*' if needed.
# Possibly move to an abstraction if anything else needs it.
deny /run/udev/data/** r,

/etc/timezone r,
/etc/wildmidi/wildmidi.cfg r,

# firefox specific
/etc/firefox*/ r,
/etc/firefox*/** r,
/etc/xul-ext/** r,
/etc/xulrunner-2.0*/ r,
/etc/xulrunner-2.0*/** r,
/etc/gre.d/ r,
/etc/gre.d/* r,

# noisy
deny @{MOZ_LIBDIR}/** w,
deny /usr/lib/firefox-addons/** w,
```

```
deny /usr/lib/xulrunner-addons/** w,
deny /usr/lib/xulrunner-*/components/*.tmp w,
deny /.suspended r,
deny /boot/initrd.img* r,
deny /boot/vmlinuz* r,
deny /var/cache/fontconfig/ w,
deny @{HOME}/.local/share/recently-used.xbel r,

# TODO: investigate
deny /usr/bin/gconftool-2 x,

# These are needed when a new user starts firefox and firefox.sh is used
@{MOZ_LIBDIR}/** ixr,
/usr/bin/basename ixr,
/usr/bin/dirname ixr,
/usr/bin/pwd ixr,
/sbin/killall5 ixr,
/bin/which ixr,
/usr/bin/tr ixr,
@{PROC}/ r,
@{PROC}/[0-9]*/cmdline r,
@{PROC}/[0-9]*/mountinfo r,
@{PROC}/[0-9]*/stat r,
owner @{PROC}/[0-9]*/task/[0-9]*/stat r,
@{PROC}/[0-9]*/status r,
@{PROC}/filesystems r,
@{PROC}/sys/vm/overcommit_memory r,
/sys/devices/pci[0-9]*/**/uevent r,
/sys/devices/platform/**/uevent r,
/sys/devices/pci*/**/{busnum,idVendor,idProduct} r,
owner @{HOME}/.thumbnails/*/*.png r,

/etc/mtab r,
/etc/fstab r,

# Needed for the crash reporter
owner @{PROC}/[0-9]*/environ r,
```

```
owner @{PROC}/[0-9]*/auxv r,
/etc/lsb-release r,
/usr/bin/expr ix,
/sys/devices/system/cpu/ r,
/sys/devices/system/cpu/** r,

# about:memory
owner @{PROC}/[0-9]*/statm r,
owner @{PROC}/[0-9]*/smaps r,

# Needed for container to work in xul builds
/usr/lib/xulrunner-*/plugin-container ixr,

# allow access to documentation and other files the user may want to look
# at in /usr and /opt
/usr/ r,
/usr/** r,
/opt/ r,
/opt/** r,

# so browsing directories works
/ r,
/**/ r,

# Default profile allows downloads to ~/Downloads and uploads from ~/Public
owner @{HOME}/ r,
owner @{HOME}/Public/ r,
owner @{HOME}/Public/* r,
owner @{HOME}/Downloads/ r,
owner @{HOME}/Downloads/* rw,

# per-user firefox configuration
owner @{HOME}/.{firefox,mozilla}/ rw,
owner @{HOME}/.{firefox,mozilla}/** rw,
owner @{HOME}/.{firefox,mozilla}/**/*.{db,parentlock,sqlite}* k,
owner @{HOME}/.{firefox,mozilla}/plugins/** rm,
owner @{HOME}/.{firefox,mozilla}/**/plugins/** rm,
```

```
  owner @{HOME}/.gnome2/firefox*-bin-* rw,
  owner @{HOME}/.cache/mozilla/{,firefox/} rw,
  owner @{HOME}/.cache/mozilla/firefox/** rw,
  owner @{HOME}/.cache/mozilla/firefox/**/*.sqlite k,

  #
  # Extensions
  # /usr/share/.../extensions/... is already covered by '/usr/** r', above.
  # Allow 'x' for downloaded extensions, but inherit policy for safety
  owner @{HOME}/.mozilla/**/extensions/** mixr,

  deny @{MOZ_LIBDIR}/update.test w,
  deny /usr/lib/mozilla/extensions/**/ w,
  deny /usr/lib/xulrunner-addons/extensions/**/ w,
  deny /usr/share/mozilla/extensions/**/ w,
  deny /usr/share/mozilla/ w,

  # Miscellaneous (to be abstracted)
  # Ideally these would use a child profile. They are all ELF executables
  # so running with 'Ux', while not ideal, is ok because we will at least
  # benefit from glibc's secure execute.
  /usr/bin/mkfifo Uxr,  # investigate
  /bin/ps Uxr,
  /bin/uname Uxr,

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

En primer lugar tenemos tunnable/global:

root@ubuntu:/etc/apparmor.d# cat tunables/global

#include <tunables/home>

#include <tunables/multiarch>

#include <tunables/proc>

#include <tunables/alias>

#include <tunables/kernelvars>

#include <tunables/xdg-user-dirs>

- Que se dedica a cargar las variables para poder usarlas posteriormente.

  Vemos, de las que nuestro perfil analizado hace uso:

  @{HOME} : Directorio home de todos los usuarios. Similar a /home/*/.

  @{MULTIARCH}: Para dar soporte a múltiples arquitecturas.

  @{PROC}: Es el equivalente a /proc/.

  También en el perfil propio se declara @{MOZ_LIBDIR} que tiene el PATH del directorio de las librerias del Firefox.

Información obtenida de :

http://manpages.ubuntu.com/manpages/trusty/en/man5/apparmor.d.5.html

https://www.suse.com/documentation/sles11/singlehtml/apparmor_quickstart/apparmor_quickstart.html

https://wiki.archlinux.org/index.php/AppArmor

En segundo lugar tenemos abstractions/audio:

```
/dev/admmidi*   rw,
/dev/adsp*      rw,
/dev/aload*     rw,
/dev/amidi*     rw,
/dev/audio*     rw,
/dev/dmfm*      rw,
/dev/dmmidi*    rw,
/dev/dsp*       rw,
/dev/midi*      rw,
/dev/mixer*     rw,
/dev/mpu401data rw,
/dev/mpu401stat rw,
/dev/patmgr*    rw,
/dev/phone*     rw,
/dev/radio*     rw,
/dev/rmidi*     rw,
/dev/sequencer  rw,
/dev/sequencer2 rw,
/dev/smpte*     rw,

/dev/snd/*      rw,
/dev/sound/*    rw,

@{PROC}/asound/** rw,

/usr/share/alsa/** r,
/usr/share/sounds/** r,

owner @{HOME}/.esd_auth r,
owner @{HOME}/.asoundrc r,
/etc/esound/esd.conf r,

# libcanberra
owner @{HOME}/.cache/event-sound-cache.* rwk,
```

 # pulse
/etc/pulse/ r,
/etc/pulse/* r,
/{run,dev}/shm/ r,
owner /{run,dev}/shm/pulse-shm* rwk,
owner @{HOME}/.pulse-cookie rwk,
owner @{HOME}/.pulse/ rw,
owner @{HOME}/.pulse/* rwk,
owner /{,var/}run/user/*/pulse/ rw,
owner /{,var/}run/user/*/pulse/{native,pid} rwk,
owner @{HOME}/.config/pulse/cookie rwk,
owner /tmp/pulse-*/ rw,
owner /tmp/pulse-*/* rw,

 # libgnome2
/etc/sound/ r,
/etc/sound/ r,**

 # openal
/etc/openal/alsoft.conf r,
owner @{HOME}/.alsoftrc r,

Entre otras cosas se pueden visualizar las siguientes características:

- Se dan permisos de escritura y lectura sobre audio*.
- Permisos de lectura sobre sound/r.
- Permisos de mapa de memoria ejecutable (nmap) sobre **/etc/ld.so.cache**

En tercer lugar tenemos abstractions/gnome:

```
#include <abstractions/base>
#include <abstractions/fonts>
#include <abstractions/X>
#include <abstractions/freedesktop.org>
#include <abstractions/xdg-desktop>
#include <abstractions/user-tmp>

  # systemwide gtk defaults
  /etc/gnome/gtkrc*              r,
  /etc/gtk/*                     r,
  /usr/lib{,32,64}/gtk/**        mr,
  /usr/lib/@{multiarch}/gtk/**   mr,
  /usr/share/themes/             r,
  /usr/share/themes/**           r,

  # for gnome 1 applications
  /etc/orbitrc                   r,

  # gtk-2 needed some new rights
  /etc/fonts/*                   r,
  /etc/gtk-*/*                   r,
  /etc/pango/*                   r,
  /usr/lib{,32,64}/pango/**      mr,
  /usr/lib{,32,64}/gtk-*/**      mr,
  /usr/lib{,32,64}/gdk-pixbuf-*/** mr,
  /usr/lib/@{multiarch}/pango/**       mr,
  /usr/lib/@{multiarch}/gtk-*/**       mr,
  /usr/lib/@{multiarch}/gdk-pixbuf-*/** mr,

  # per-user gtk configuration
  owner @{HOME}/.gnome/Gnome           r,
  owner @{HOME}/.gtk                   r,
  owner @{HOME}/.gtkrc                 r,
  owner @{HOME}/.gtkrc-2.0             r,
  owner @{HOME}/.gtk-bookmarks         r,
  owner @{HOME}/.themes/               r,
```

```
owner @{HOME}/.themes/**             r,

# for gtk file dialog
owner @{HOME}/.config/gtk-2.0/**                r,
owner @{HOME}/.config/gtk-2.0/gtkfilechooser.ini* rw,

# from evolution-mail
owner @{HOME}/.gconfd/lock/*                    r,
owner @{HOME}/.gnome/application-info           r,

# per-user font business
owner @{HOME}/.fonts.cache-*    rwl,

# icon caches
/var/cache/**/icon-theme.cache  r,
/usr/share/**/icon-theme.cache  r,

# gnome VFS modules
/etc/gnome-vfs-2.0/modules/ r,
/etc/gnome-vfs-2.0/modules/* r,
/usr/lib/gnome-vfs-2.0/modules/*.so mr,
/usr/lib/@{multiarch}/gnome-vfs-2.0/modules/*.so mr,

# gvfs
/usr/share/gvfs/remote-volume-monitors/  r,
/usr/share/gvfs/remote-volume-monitors/* r,
@{PROC}/@{pid}/mounts                   r,

# printing
/etc/papersize                  r,
/etc/cups/lpoptions             r,
/usr/share/cups/charmaps/**     r,

# holds MIT-MAGIC-COOKIE for gnome
owner /{,var/}run/gdm/auth*/database r,

# mime-types
```

/etc/gnome/defaults.list r,

/usr/share/gnome/applications/ r,

/usr/share/gnome/applications/mimeinfo.cache r,

Entre otras cosas se pueden visualizar las siguientes características:

- Se dan permisos de escritura y lectura sobre **gtkfilechooser.ini***
- Permisos de lectura sobre database
- Permisos de mapa de memoria ejecutable (nmap) sobre **/usr/lib/gnome-vfs-2.0/modules/*.so**

Con respecto al primer fichero del perfil, se habilitan una serie de reglas de red:

- **network inet stream**
- **network inet6 stream**

También establece permisos a una serie de directorios:

- **/etc/firefox*/ r,**
- **/etc/firefox*/** r,**
- **/etc/xul-ext/** r,**
- **/etc/xulrunner-2.0*/ r,**
- **/etc/xulrunner-2.0*/** r,**
- **/etc/gre.d/ r,**
- **/etc/gre.d/* r,**

Ejercicio 2.

En nuestro caso lo que vamos a hacer es establecer un perfil a Apache, el famoso servidor web, y así poder adherir mayor seguridad al sistema.

Para ello nos vamos a crear una serie de directorios, y vamos a hacer que unos sean accesibles y otros no.

mkdir -p /data/www/disponible

mkdir -p /data/www/nodisponible

Una vez tenemos creados los directorios, creamos dentro de ellos un index.html.

nano /data/www/disponible/index.html

nano /data/www/disponible/index.html

Para que apache nos enlace este directorio debemos de modificar algunos de los parámetros que vienen conigurados por defecto:

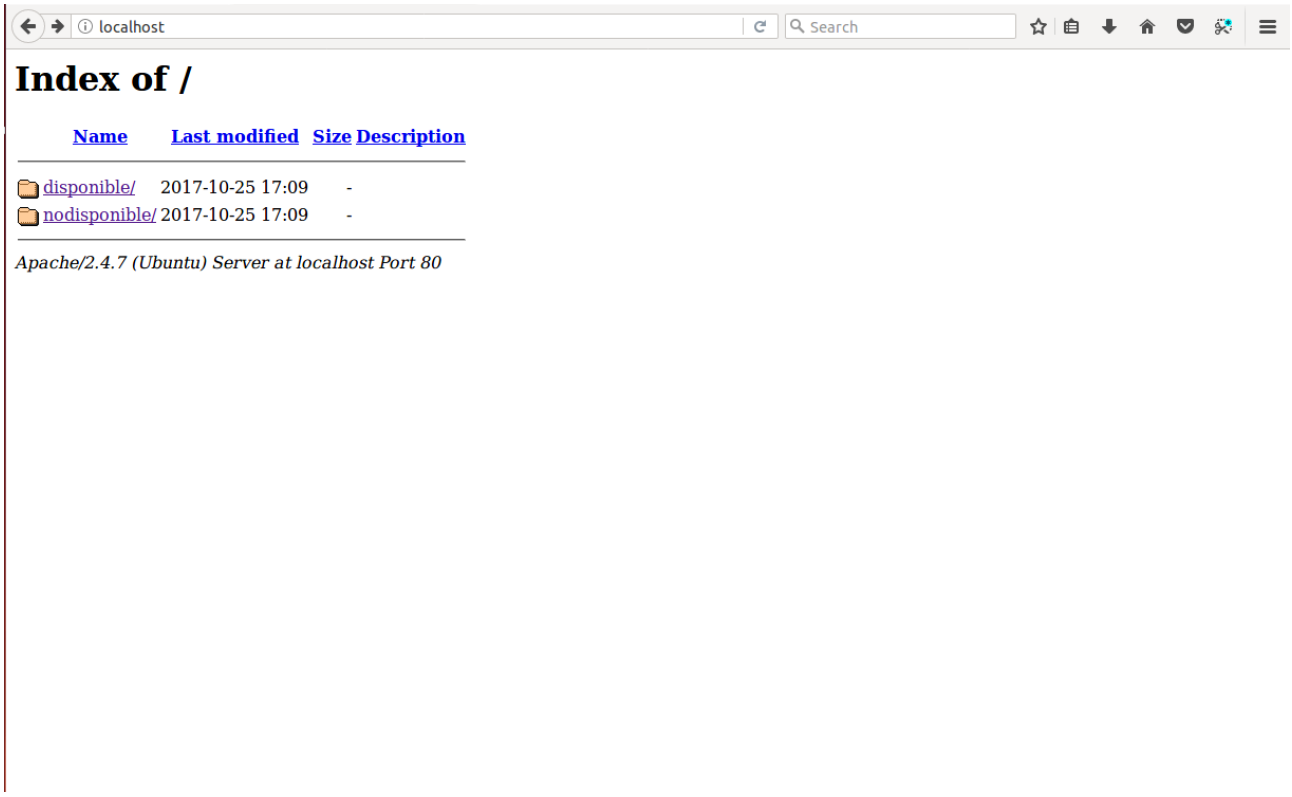
Modificar los siguientes ficheros:

/etc/apache2/apache2.conf

/etc/apache2/sites-available/000-default.conf

/etc/apache2/sites-enabled/000-default.conf

Una vez tenemos enlazado apache para que nos muestre el directorio creado, nos deberá salir algo tal que así:



Una vez llegados a este punto, deberemos instalar:

apt install apparmor-utils

Y ejecutar la siguiente sentencia:

aa-autodep /usr/sbin/apache2

La cuál nos genera el siguiente archivo “usr.sbin.apahe2”:

```
root@ubuntu:/etc/apparmor.d# ls
abstractions  force-complain        sbin.dhclient  usr.bin.evince    usr.sbin.apache2      usr.sbin.rsyslogd
cache         lightdm-guest-session  snap           usr.bin.firefox   usr.sbin.cups-browsed  usr.sbin.tcpdump
disable       local                  tunables       usr.lib.telepathy  usr.sbin.cupsd
```

Que tiene la siguiente información:

```
root@ubuntu:/etc/apparmor.d# cat usr.sbin.apache2
# Last Modified: Wed Oct 25 17:37:53 2017
#include <tunables/global>

/usr/sbin/apache2 flags=(complain) {
  #include <abstractions/base>

  /usr/sbin/apache2 mr,


  ^DEFAULT_URI flags=(complain) {
  }

  ^HANDLING_UNTRUSTED_INPUT flags=(complain) {
  }
}
```

Por ejemplo algo que ya conocemos es tunnables/global y abstractions/base.
También algo acerca de los permisos a /usr/sbin/apache2 nr.

Como se pide en la documentación lo primero que haremos es pasarlo a modo complain.

```
root@ubuntu:/etc/apparmor.d# aa-complain apache2
Setting /usr/sbin/apache2 to complain mode.
```

Y después reiniciaremos apache.

root@ubuntu:/etc/apache2/sites-enabled# aa-logprof
Reading log entries from /var/log/syslog.
Updating AppArmor profiles in /etc/apparmor.d.
Complain-mode changes:

Profile: /usr/sbin/apache2
Network Family: inet6
Socket Type: dgram

[1 - #include <abstractions/nameservice>]
2 - network inet6 dgram,
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
Adding #include <abstractions/nameservice> to profile.

Profile: /usr/sbin/apache2

Path: /etc/apache2/apache2.conf

Mode: r

Severity: 3

1 - #include <abstractions/lightdm>

[2 - /etc/apache2/apache2.conf]

[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore

Adding /etc/apache2/apache2.conf r to profile

Profile: /usr/sbin/apache2

Path: /etc/apache2/mods-available/access_compat.load

Mode: r

Severity: 3

1 - #include <abstractions/lightdm>

[2 - /etc/apache2/mods-available/access_compat.load]

[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore

Adding /etc/apache2/mods-available/access_compat.load r to profile

Profile: /usr/sbin/apache2

Path: /etc/apache2/mods-enabled/

Mode: r

Severity: 3

1 - #include <abstractions/lightdm>

[2 - /etc/apache2/mods-enabled/]

[(A)llow] / (D)eny / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Abo(r)t / (F)inish / (M)ore

Adding /etc/apache2/mods-enabled/ r to profile

Enforce-mode changes:

Profile: /usr/sbin/cupsd

Access mode: send

Signal: term

Peer: unconfined

[1 - signal send set=term peer=unconfined,]

(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish

Adding signal send set=term peer=unconfined, to profile.

= Changed Local Profiles =

The following local profiles were changed. Would you like to save them?

[1 - /usr/sbin/cupsd]

2 - /usr/sbin/apache2

(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean profiles / Abo(r)t

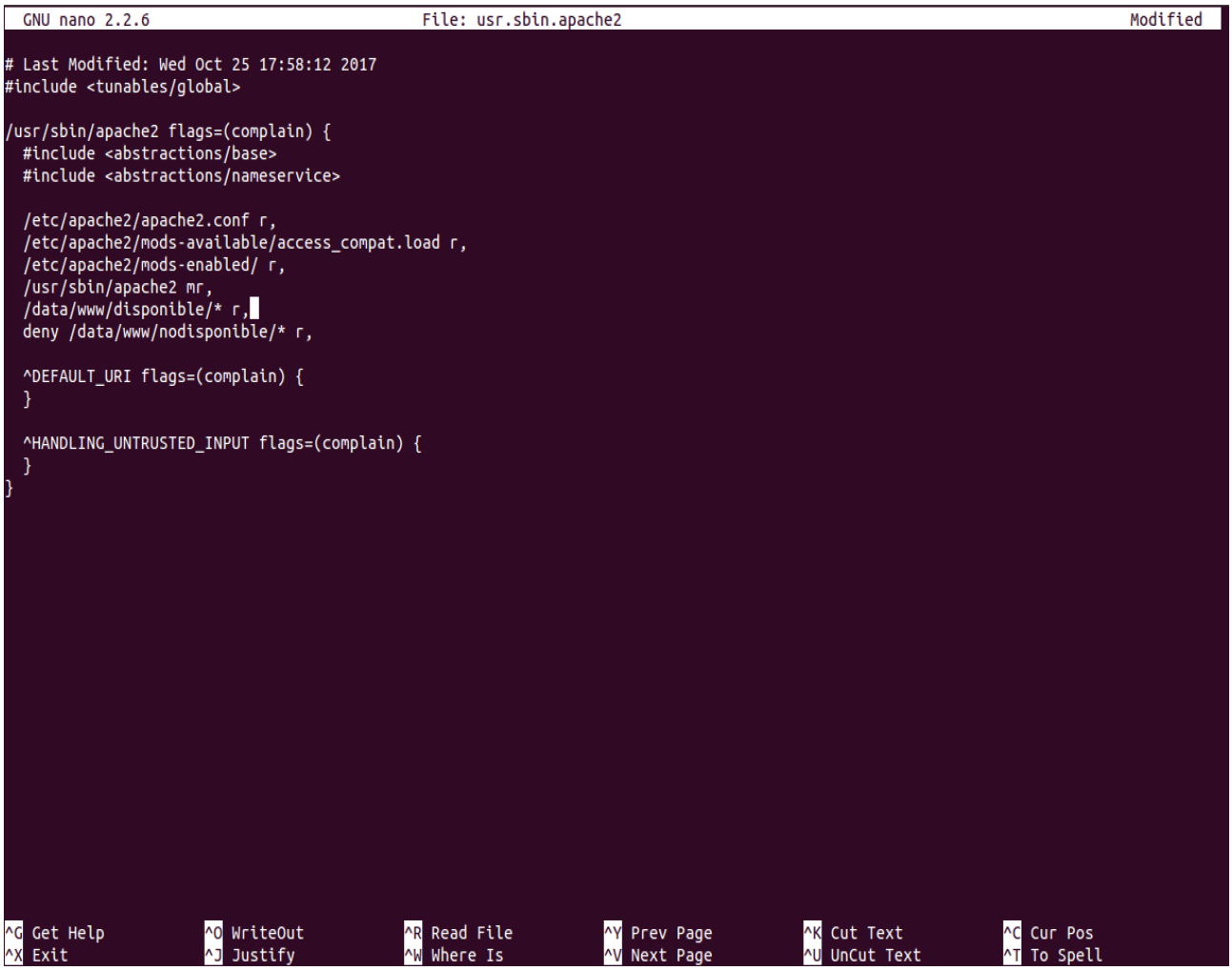
Writing updated profile for /usr/sbin/apache2.

Writing updated profile for /usr/sbin/cupsd.

Ahora podemos volver a mirar el fichero, y veremos que tiene más información, por ejemplo abstractions/nameservice, y también tenemos configuración de más permisos como apache2.conf r, access_compat.load r, etc:

```
root@ubuntu:/etc/apparmor.d# cat usr.sbin.apache2
# Last Modified: Wed Oct 25 17:58:12 2017
#include <tunables/global>

/usr/sbin/apache2 flags=(complain) {
  #include <abstractions/base>
  #include <abstractions/nameservice>

  /etc/apache2/apache2.conf r,
  /etc/apache2/mods-available/access_compat.load r,
  /etc/apache2/mods-enabled/ r,
  /usr/sbin/apache2 mr,


  ^DEFAULT_URI flags=(complain) {
  }

  ^HANDLING_UNTRUSTED_INPUT flags=(complain) {
  }
}
```

Para prohibir el acceso al directorio /data/www/nodisponible y para garantizarlo a /data/www/disponible modificamos el fichero:



Y tras esto lo ponemos en modo Enforce:

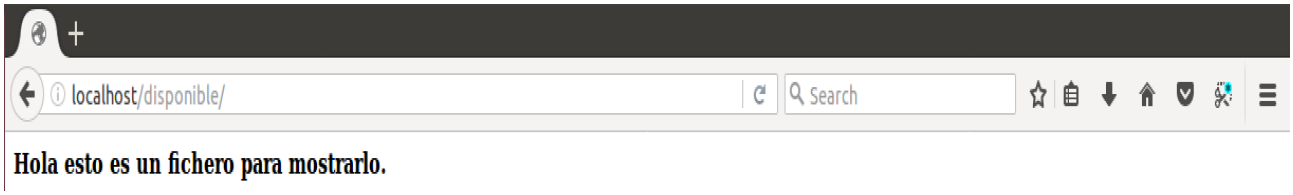
root@ubuntu:/etc/apache2/sites-enabled# aa-enforce apache2
Setting /usr/sbin/apache2 to enforce mode.

Después recargamos todos los perfiles y reiniciamos Apache:

root@ubuntu:/etc/apache2/sites-enabled# invoke-rc.d apparmor reload
*** Reloading AppArmor profiles**
Skipping profile in /etc/apparmor.d/disable: usr.bin.firefox
Skipping profile in /etc/apparmor.d/disable: usr.sbin.rsyslogd
[OK]

Resultado final:

Como vemos podemos acceder al fichero disponible/index.html:



Pero no podemos acceder al fichero nodisponible/index.html: