Práctica 5b - Seguridad Parte 2

Notas >

1. Utilizar un kernel completo (no el compilado en las prácticas 1 y 2).
2. En Debian 12 (Woodworm) utilizar el kernel por defecto 6.1.0 para evitar incompatibilidades con apparmor-utils.
3. Compilar el código C usando el Makefile provisto a fin de deshabilitar algunas medidas de seguridad del compilador y generar un código assembler más simple.
4. Acceda al código necesario para la práctica en el repositorio de la materia.
5. Se recomienda trabajar en una VM ya que como parte de la práctica se van a habilitar y deshabilitar medidas de seguridad, lo que puede generar vulnerabilidades o hacer que determinadas aplicaciones no funcionen.

A - AppArmor

1. Instale las herramientas de espacio de usuario, perfiles por defecto de `app-armor` y `auditd` (necesario para generar perfiles de forma interactiva). `apt install apparmor apparmor-profiles apparmor-utils auditd`

```
so@so:~/codigo-para-practicas$ su
Contraseña:
root@so:/home/so/codigo-para-practicas# apt update
Obj:1 http://deb.debian.org/debian bookworm InRelease
Des:2 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Des:3 http://security.debian.org/debian-security bookworm-security InRelease
[48,0 kB]
Des:4 https://download.docker.com/linux/debian bookworm InRelease [47,0 kB]
Des:5 http://security.debian.org/debian-security bookworm-security/non-free-
firmware Sources [796 B]
Des:6 http://security.debian.org/debian-security bookworm-security/main
Sources [137 kB]
Des:7 http://security.debian.org/debian-security bookworm-security/main
amd64 Packages [265 kB]
Des:8 http://security.debian.org/debian-security bookworm-security/main
Translation-en [160 kB]
Des:9 http://security.debian.org/debian-security bookworm-security/non-free-
firmware amd64 Packages [688 B]
Des:10 https://download.docker.com/linux/debian bookworm/stable amd64
```

```
Packages [41,6 kB]
Descargados 756 kB en 4s (176 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 89 paquetes. Ejecute «apt list --upgradable» para
verlos.
root@so:/home/so/codigo-para-practicas# apt install apparmor apparmor-
profiles apparmor-utils auditd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
apparmor ya está en su versión más reciente (3.0.8-3).
fijado apparmor como instalado manualmente.
Se instalarán los siguientes paquetes adicionales:
  libauparse0 python3-apparmor python3-libapparmor
Paquetes sugeridos:
  vim-addon-manager audispd-plugins
Se instalarán los siguientes paquetes NUEVOS:
  apparmor-profiles apparmor-utils auditd libauparse0 python3-apparmor
python3-libapparmor
0 actualizados, 6 nuevos se instalarán, 0 para eliminar y 89 no
actualizados.
Se necesita descargar 539 kB de archivos.
Se utilizarán 2.269 kB de espacio de disco adicional después de esta
operación.
¿Desea continuar? [S/n] S
Des:1 http://deb.debian.org/debian bookworm/main amd64 libauparse0 amd64
1:3.0.9-1 [61,9 kB]
Des:2 http://deb.debian.org/debian bookworm/main amd64 auditd amd64 1:3.0.9-
1 [218 kB]
Des:3 http://deb.debian.org/debian bookworm/main amd64 apparmor-profiles all
3.0.8-3 [41,7 kB]
Des:4 http://deb.debian.org/debian bookworm/main amd64 python3-libapparmor
amd64 3.0.8-3 [36,4 kB]
Des:5 http://deb.debian.org/debian bookworm/main amd64 python3-apparmor all
3.0.8-3 [87,8 kB]
Des:6 http://deb.debian.org/debian bookworm/main amd64 apparmor-utils all
3.0.8-3 [94,0 kB]
Descargados 539 kB en 0s (1.258 kB/s)
Seleccionando el paquete libauparse0:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 47218 ficheros o directorios instalados
actualmente.)
Preparando para desempaquetar .../0-libauparse0_1%3a3.0.9-1_amd64.deb ...
Desempaquetando libauparse0:amd64 (1:3.0.9-1) ...
Seleccionando el paquete auditd previamente no seleccionado.
```

```
Preparando para desempaquetar .../1-auditd_1%3a3.0.9-1_amd64.deb ...
Desempaquetando auditd (1:3.0.9-1) ...
Seleccionando el paquete apparmor-profiles previamente no seleccionado.
Preparando para desempaquetar .../2-apparmor-profiles_3.0.8-3_all.deb ...
Desempaquetando apparmor-profiles (3.0.8-3) ...
Seleccionando el paquete python3-libapparmor previamente no seleccionado.
Preparando para desempaquetar .../3-python3-libapparmor_3.0.8-3_amd64.deb
...
Desempaquetando python3-libapparmor (3.0.8-3) ...
Seleccionando el paquete python3-apparmor previamente no seleccionado.
Preparando para desempaquetar .../4-python3-apparmor_3.0.8-3_all.deb ...
Desempaquetando python3-apparmor (3.0.8-3) ...
Seleccionando el paquete apparmor-utils previamente no seleccionado.
Preparando para desempaquetar .../5-apparmor-utils_3.0.8-3_all.deb ...
Desempaquetando apparmor-utils (3.0.8-3) ...
Configurando python3-libapparmor (3.0.8-3) ...
Configurando apparmor-profiles (3.0.8-3) ...
Configurando libauparse0:amd64 (1:3.0.9-1) ...
Configurando python3-apparmor (3.0.8-3) ...
Configurando auditd (1:3.0.9-1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/auditd.service →
/lib/systemd/system/auditd.service.
Configurando apparmor-utils (3.0.8-3) ...
Procesando disparadores para man-db (2.11.2-2) ...
Procesando disparadores para libc-bin (2.36-9+deb12u9) ...
```

2. Verifique si apparmor se encuentra habilitado con el comando `aa-enabled`. Si no se encuentra habilitado verifique el kernel que está ejecutando (el kernel de Debian de la VM lo trae habilitado por defecto).

Chequeos para ver si está habilitado

```
so@so:~/codigo-para-practicas$ aa-enabled
S? # que te diga esto indica que no puede determinar con certeza si está
habilitado, asi que vemos otros chequeos
so@so:~/codigo-para-practicas$ cat /sys/module/apparmor/parameters/enabled
Y
so@so:~/codigo-para-practicas$ sudo aa-status
[sudo] contraseña para so:
apparmor module is loaded.
32 profiles are loaded.
11 profiles are in enforce mode.
   /usr/bin/man
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/NetworkManager/nm-dhcp-helper
```

```
   /usr/lib/connman/scripts/dhclient-script
   /{,usr/}sbin/dhclient
   docker-default
   lsb_release
   man_filter
   man_groff
   nvidia_modprobe
   nvidia_modprobe//kmod
21 profiles are in complain mode.
   avahi-daemon
   dnsmasq
   dnsmasq//libvirt_leaseshelper
   identd
   klogd
   mdnsd
   nmbd
   nscd
   php-fpm
   ping
   samba-bgqd
   samba-dcerpcd
   samba-rpcd
   samba-rpcd-classic
   samba-rpcd-spoolss
   smbd
   smbldap-useradd
   smbldap-useradd///etc/init.d/nscd
   syslog-ng
   syslogd
   traceroute
0 profiles are in kill mode.
0 profiles are in unconfined mode.
2 processes have profiles defined.
2 processes are in enforce mode.
   /usr/sbin/dhclient (397) /{,usr/}sbin/dhclient
   /usr/sbin/dhclient (403) /{,usr/}sbin/dhclient
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
0 processes are in mixed mode.
0 processes are in kill mode.
```

3. Utilice la herramienta aa-status para determinar:
    1. ¿Cuántos perfiles se encuentran cargados?
    2. ¿Cuántos procesos y cuáles procesos de tu sistema tienen perfiles definidos?

¿Cuántos perfiles se encuentran cargados?

- Se encuentran cargados 32 perfiles, lo vemos en el código de arriba, específicamente en la línea `32 profiles are loaded.`

¿Cuántos procesos y cuáles procesos de tu sistema tienen perfiles definidos?

- Hay 2 procesos que tienen perfiles definidos, ambos están en modo enforce (se les aplica restricciones activas). Los 2 procesos son:

```
2 processes are in enforce mode.
   /usr/sbin/dhclient (397) /{,usr/}sbin/dhclient
   /usr/sbin/dhclient (403) /{,usr/}sbin/dhclient
```

- Ambos están usando el perfil `/{,usr/}sbin/dhclient`.

4. Detenga y deshabilite el servicio insecure_service creado en la parte 1 de la práctica de forma que no vuelva a iniciarse automáticamente.

```
systemctl stop insecure_service.service
systemctl disable insecure_service.service
```

Deshabilitando todo

```
so@so:~/codigo-para-practicas$ sudo systemctl stop insecure_service.service
so@so:~/codigo-para-practicas$ sudo systemctl disable
insecure_service.service
Removed "/etc/systemd/system/multi-
user.target.wants/insecure_service.service".
```

5. Ejecute `insecure_service` manualmente usando el usuario `root` y verifique que puede acceder libremente al filesystem en http://localhost:8080 (o la IP correspondiente donde se ejecuta el servicio). `/opt/sistemasoperativos/insecure_service`

```
so@so:~/codigo-para-practicas$ sudo /opt/sistemasoperativos/insecure_service
2025/06/03 12:39:56 Servidor iniciado en http://localhost:8080
```

6. Generación de un nuevo profile:
    1. Ejecutar aa-genprof /...
    2. Abrir otra terminal, ejecutar `insecure_service` y navegue el sistema de archivos usando la interfaz web provista por el servicio.

3. Genere un perfil que permita:
    1. Abrir conexiones tcp ipv4
    2. Abrir conexiones tcp ipv6
    3. El perfil debe incluir los siguientes perfiles (y ningún otro):
        1. include <abstractions/base>
        2. include <abstractions/nameservice>
    4. Listar el contenido de / y /proc pero no de otros subdirectorios de /
    5. Ejecutar con los permisos del perfil actual (mrix) los siguientes comandos:
        1. /usr/bin/dash
        2. /usr/bin/ip
        3. /usr/bin/mawk
        4. /usr/bin/ps

Terminal 1

```
so@so:~/codigo-para-practicas$ sudo aa-genprof
/opt/sistemasoperativos/insecure_service
Updating AppArmor profiles in /etc/apparmor.d.

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:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Profiling: /opt/sistemasoperativos/insecure_service

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)inalizar
Reading log entries from /var/log/audit/audit.log.

Perfil:   /opt/sistemasoperativos/insecure_service
Ejecutar: /usr/bin/dash
Severity: desconocido
```

```
(I)nherit / (C)hild / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t
/ (F)inalizar
Complain-mode changes:

Perfil:     /opt/sistemasoperativos/insecure_service
Ruta:       /home/
Modo nuevo: owner r
Severity:   4

 [1 - owner /home/ r,]
(A)llow / [(D)eny] / (I)gnorar / (G)lob / Glob with (E)xtension / (N)uevo /
Audi(t) / (O)wner permissions off / Abo(r)t / (F)inalizar
Añadiendo owner /home/ r, al perfil.

Perfil:     /opt/sistemasoperativos/insecure_service
Ruta:       /
Modo nuevo: owner r
Severity:   desconocido

 [1 - include <abstractions/opencl-pocl>]
  2 - owner / r,
(A)llow / [(D)eny] / (I)gnorar / (G)lob / Glob with (E)xtension / (N)uevo /
Audi(t) / (O)wner permissions off / Abo(r)t / (F)inalizar
Añadiendo include <abstractions/opencl-pocl> al perfil.

Perfil:     /opt/sistemasoperativos/insecure_service
Ruta:       /var/
Modo nuevo: owner r
Severity:   desconocido

 [1 - owner /var/ r,]
(A)llow / [(D)eny] / (I)gnorar / (G)lob / Glob with (E)xtension / (N)uevo /
Audi(t) / (O)wner permissions off / Abo(r)t / (F)inalizar
Añadiendo owner /var/ r, al perfil.

Perfil:     /opt/sistemasoperativos/insecure_service
Ruta:       /var/spool/
Modo nuevo: owner r
Severity:   desconocido

 [1 - owner /var/spool/ r,]
(A)llow / [(D)eny] / (I)gnorar / (G)lob / Glob with (E)xtension / (N)uevo /
Audi(t) / (O)wner permissions off / Abo(r)t / (F)inalizar
Añadiendo owner /var/spool/ r, al perfil.
```

```
Perfil:     /opt/sistemasoperativos/insecure_service
Ruta:       /var/opt/
Modo nuevo: owner r
Severity:   desconocido

 [1 - owner /var/opt/ r,]
(A)llow / [(D)eny] / (I)gnorar / (G)lob / Glob with (E)xtension / (N)uevo /
Audi(t) / (O)wner permissions off / Abo(r)t / (F)inalizar
Añadiendo owner /var/opt/ r, al perfil.

Perfil:     /opt/sistemasoperativos/insecure_service
Ruta:       /etc/ld.so.cache
Modo nuevo: owner r
Severity:   1

 [1 - owner /etc/ld.so.cache r,]
(A)llow / [(D)eny] / (I)gnorar / (G)lob / Glob with (E)xtension / (N)uevo /
Audi(t) / (O)wner permissions off / Abo(r)t / (F)inalizar
Añadiendo owner /etc/ld.so.cache r, al perfil.

= Changed Local Profiles =

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

 [1 - /opt/sistemasoperativos/insecure_service]
(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 /opt/sistemasoperativos/insecure_service.
Profiling: /opt/sistemasoperativos/insecure_service

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)inalizar

Reloaded AppArmor profiles in enforce mode.

Please consider contributing your new profile!
See the following wiki page for more information:
```

```
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Finished generating profile for /opt/sistemasoperativos/insecure_service.
```

Terminal 2

```
so@so:~/codigo-para-practicas/practica5/insecure_service$ sudo
/opt/sistemasoperativos/insecure_service
[sudo] contraseña para so:
2025/06/04 15:30:03 Servidor iniciado en http://localhost:8080
2025/06/04 15:30:08 Browsing path: /, ulr path: /resources/
2025/06/04 15:30:11 Browsing path: /opt, ulr path: /resources/opt
2025/06/04 15:30:14 Browsing path: /, ulr path: /resources/
2025/06/04 15:30:16 Browsing path: /boot, ulr path: /resources/boot
2025/06/04 15:30:18 Browsing path: /, ulr path: /resources/
2025/06/04 15:30:19 Browsing path: /sys, ulr path: /resources/sys
2025/06/04 15:30:23 Browsing path: /, ulr path: /resources/
2025/06/04 15:30:28 Browsing path: /root, ulr path: /resources/root
2025/06/04 15:30:33 Browsing path: /, ulr path: /resources/
2025/06/04 15:30:58 Browsing path: /home, ulr path: /resources/home
2025/06/04 15:31:01 Browsing path: /, ulr path: /resources/
2025/06/04 15:31:03 Browsing path: /, ulr path: /resources/
2025/06/04 15:31:05 Browsing path: /var, ulr path: /resources/var
2025/06/04 15:31:06 Browsing path: /var/spool, ulr path:
/resources/var/spool
2025/06/04 15:31:10 Browsing path: /var/, ulr path: /resources/var/
2025/06/04 15:31:11 Browsing path: /var/, ulr path: /resources/var/
2025/06/04 15:31:14 Browsing path: /var/opt, ulr path: /resources/var/opt
2025/06/04 15:31:15 Browsing path: /var/, ulr path: /resources/var/
2025/06/04 15:31:16 Browsing path: /var/, ulr path: /resources/var/
2025/06/04 15:31:17 Browsing path: /var/, ulr path: /resources/var/
2025/06/04 15:31:19 Browsing path: /, ulr path: /resources/
```

Luego de terminar de ejecutar `aa-genprof` se creó un perfil en `/etc/apparmor.d/opt.sistemasoperativos.insecure_service` que vamos a editar para que cumpla con lo que nos pide, yo usé `sudo vim`:

```
#include <tunables/global>

/opt/sistemasoperativos/insecure_service {
    #include <abstractions/base>
    #include <abstractions/nameservice>
```

```
    # Permisos de red
    network inet tcp, #permite ipv4
    network inet6 tcp, #permite ipv6

    # Permisos de archivos
    / r, #permite leer el directorio raiz
    deny /* r, #deniega leer otros directorios
    /proc/ r, #permite leer /proc
    deny /proc/* r, #deniega leer contenidos de /proc

    # Permisos de ejecución
    /usr/bin/dash ix, #ejecuta con los permisos del perfil actual
    /usr/bin/ip ix,
    /usr/bin/mawk ix,
    /usr/bin/ps ix,

}
```

Luego ejecutamos para recargar el perfil:

```
so@so:~/codigo-para-practicas$ sudo apparmor_parser -r
/etc/apparmor.d/opt.sistemasoperativos.insecure_service
```

7. Habilite el modo enforcing y verifique si funciona (aa-enforcing).

Terminal 1

```
so@so:~/codigo-para-practicas$ sudo aa-enforce
/opt/sistemasoperativos/insecure_service
Setting /opt/sistemasoperativos/insecure_service to enforce mode.
```

Terminal 2

```
so@so:/$ sudo /opt/sistemasoperativos/insecure_service
[sudo] contraseña para so:
2025/06/04 15:50:51 Servidor iniciado en http://localhost:8080
```

8. Si necesita volver a generar un perfil puede usar aa-complain + aa-logprofile o editar el profile a mano y aplicar con apparmor_parser -r

Ayudas >

- Es útil habilitar el modo complain y volver a ejecutar aa-genprof para detectar más acciones y que se agreguen al profile.
- Seguro es necesario ajustar el archivo manualmente ya que aa-genprof no siempre muestra las opciones que necesitamos.
- Verificar que no se agreguen “include” adicionales ya que traen otras reglas que van a cambiar el comportamiento.
- Para permitir acceso a un directorio:
  - /path/terminado/en/barra/ r,
- Para permitir acceso a los subdirectorios:
  - /path/terminado/en/barra/** r,
- Para denegar es lo mismo agregando deny al principio.
- Para permitir listar / pero denegar el resto:
  - / r,
  - deny /* r,
- owner se usa para acceder solo a los recursos de los cuales el proceso es owner. No lo usaremos en esta práctica.
- Siempre verificar que el perfil esté en enforce en las pruebas, si está en complain el proceso podrá acceder a todos los recursos y no estaremos probando el perfil realmente.

Pruebas del nuevo perfil

```
so@so:~/codigo-para-practicas$ sudo aa-exec -p
/opt/sistemasoperativos/insecure_service -- ls /
bin   dev  home        initrd.img.old  lib64       media  opt   root  sbin
sys  usr  vmlinuz
boot  etc  initrd.img  lib            lost+found  mnt    proc  run   srv
tmp  var  vmlinuz.old
so@so:~/codigo-para-practicas$ sudo aa-exec -p
/opt/sistemasoperativos/insecure_service -- ls /home
ls: no se puede abrir el directorio '/home': Permiso denegado
so@so:~/codigo-para-practicas$ sudo aa-exec -p
/opt/sistemasoperativos/insecure_service -- ls /proc
1     1362  17    25    38    48    5945  6177  946        crypto
kallsyms     mtrr           thread-self
10    14    171   254   3840  49    5962  618   961        devices
kcore        net            timer_list
1043  148   18    26    39    5     5963  62    964        diskstats
```

```
keys          pagetypeinfo    tty
1047  149    19     262    4      50     5964   64     970         dma
key-users     partitions      uptime
1067  15     2      275    40     51     5972   640    971         driver
kmsg          pressure        version
1078  152    20     28     41     5139   6      643    989         dynamic_debug
kpagecgroup   schedstat       vmallocinfo
1090  157    202    29     42     52     611    644    acpi        execdomains
kpagecount    self            vmstat
11    158    203    3      43     5276   612    66     asound      fb
kpageflags    slabinfo        zoneinfo
1183  159    21     30     44     53     616    67     buddyinfo   filesystems
loadavg       softirqs
12    16     22     31     441    5426   6167   679    bus         fs
locks         stat
1227  160    2270   33     45     549    6168   72     cgroups     interrupts
meminfo       swaps
1237  161    23     3698   450    55     6173   77     cmdline     iomem
misc          sys
13    162    24     375    462    56     6174   78     consoles    ioports
modules       sysrq-trigger
132   163    242    379    47     5765   6176   945    cpuinfo     irq
mounts        sysvipc
so@so:~/codigo-para-practicas$ sudo aa-exec -p
/opt/sistemasoperativos/insecure_service -- /bin/nc -vz 8.8.8.8 53
dns.google [8.8.8.8] 53 (domain) open
so@so:~/codigo-para-practicas$ sudo aa-exec -p
/opt/sistemasoperativos/insecure_service -- /usr/bin/dash -c "echo
'Funciona'"
Funciona
so@so:~/codigo-para-practicas$ sudo aa-exec -p
/opt/sistemasoperativos/insecure_service -- /usr/bin/ip a show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    link/ether 08:00:27:25:8b:00 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 83603sec preferred_lft 83603sec
    inet6 fe80::a00:27ff:fe25:8b00/64 scope link
       valid_lft forever preferred_lft forever
```

```
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    link/ether 08:00:27:aa:33:8c brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.104/24 brd 192.168.56.255 scope global dynamic enp0s8
       valid_lft 571sec preferred_lft 571sec
    inet6 fe80::a00:27ff:feaa:338c/64 scope link
       valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state
DOWN group default
    link/ether 5a:42:05:4b:75:9c brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
so@so:~/codigo-para-practicas$ sudo aa-exec -p
/opt/sistemasoperativos/insecure_service -- /usr/bin/mawk 'BEGIN {print
"OK"}'
OK
```