

Práctica 5 - Seguridad - Parte 2

D - AppArmor

1. Instale las herramientas de espacio de usuario, perfiles por defecto de apparmor y auditd (necesario para generar perfiles de forma interactiva).

..

```
apt install apparmor apparmor-profiles apparmor-utils auditd
```

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).

```
root@so:/home/so# aa-enabled  
S?
```

No sabe si esta habilitado.

```
root@so:/home/so# cat /sys/module/apparmor/parameters/enabled  
Y
```

De esta forma estaría habilitado.

3. Utilice la herramienta aa-status para determinar:

Antes de arrancar, a mi no me andaba el comando así que hice esto:

```
root@so:/home/so# apt update  
Obj:1 http://deb.debian.org/debian bookworm InRelease  
Des:2 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]  
Des:3 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]  
Des:4 http://security.debian.org/debian-security bookworm-security/main Sources [137  
kB]  
Des:5 http://security.debian.org/debian-security bookworm-security/main amd64 Packages  
[265 kB]  
Descargados 505 kB en 1s (544 kB/s)  
Leyendo lista de paquetes... Hecho
```

```

Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 79 paquetes. Ejecute «apt list --upgradable» para verlos.
root@so:/home/so# 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).
apparmor-profiles ya está en su versión más reciente (3.0.8-3).
apparmor-utils ya está en su versión más reciente (3.0.8-3).
auditd ya está en su versión más reciente (1:3.0.9-1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 79 no actualizados.
root@so:/home/so# aa-status
bash: aa-status: orden no encontrada
root@so:/home/so# systemctl status apparmor
● apparmor.service - Load AppArmor profiles
   Loaded: loaded (/lib/systemd/system/apparmor.service; enabled; preset: enabled)
   Active: active (exited) since Tue 2025-06-03 13:24:09 -03; 10min ago
     Docs: man:apparmor(7)
           https://gitlab.com/apparmor/apparmor/wikis/home/
  Main PID: 250 (code=exited, status=0/SUCCESS)
    CPU: 112ms

jun 03 13:24:09 so systemd[1]: Starting apparmor.service - Load AppArmor profiles...
jun 03 13:24:09 so apparmor.systemd[250]: Restarting AppArmor
jun 03 13:24:09 so apparmor.systemd[250]: Reloading AppArmor profiles
jun 03 13:24:09 so systemd[1]: Finished apparmor.service - Load AppArmor profiles.
root@so:/home/so# find / -name aa-status 2>/dev/null
/usr/sbin/aa-status

```

aa-status esta pero no lo encuentra. Así que:

```

root@so:/home/so# /usr/sbin/aa-status
apparmor module is loaded.
31 profiles are loaded.
10 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
  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 (388) /{,usr/}sbin/dhclient
  /usr/sbin/dhclient (390) /{,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.

```

a. ¿Cuántos perfiles se encuentran cargados?

31

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

```

2 processes are in enforce mode.
  /usr/sbin/dhclient (388) /{,usr/}sbin/dhclient
  /usr/sbin/dhclient (390) /{,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
```

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).

6. Generación de un nuevo profile:

a. Ejecutar `aa-genprof` /...

```
root@so:/home/so/codigo-para-practicas/practica5# /usr/sbin/aa-genprof
insecure_service/
Updating AppArmor profiles in /etc/apparmor.d.
Writing updated profile for /home/so/codigo-para-practicas/practica5/insecure_service.
Estableciendo /home/so/codigo-para-practicas/practica5/insecure_service al modo
reclamar.
```

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: /home/so/codigo-para-practicas/practica5/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
Setting /home/so/codigo-para-practicas/practica5/insecure_service to enforce mode.

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 /home/so/codigo-para-  
practicas/practica5/insecure_service.
```

b. Abrir otra terminal, ejecutar `insecure_service` y navegue el sistema de archivos usando la interfaz web provista por el servicio.

c. Genere un perfil que permita:

i. Abrir conexiones tcp ipv4

ii. Abrir conexiones tcp ipv6

iii. Listar el contenido de `/` y `/proc` iv. Ejecutar dash con los permisos del perfil actual (ix)

```
root@so:/home/so/codigo-para-practicas/practica5/insecure_service# cat  
/etc/apparmor.d/home.so.codigo-para-practicas.practica5.insecure_service  
#include <tunables/global>  
  
/home/so/codigo-para-practicas/practica5/insecure_service/insecure_service {  
  
    # Permisos de red  
    network inet tcp,  
    network inet6 tcp,  
  
    # Acceso a directorios  
    / r,  
    /proc/ r,  
    /proc/* r,  
  
    # Ejecución de dash  
    /usr/bin/dash ix,  
}
```

Si lo debugueamos tira:

```
root@so:/home/so/codigo-para-practicas/practica5/insecure_service#  
/usr/sbin/apparmor_parser --debug /etc/apparmor.d/home.so.codigo-para-  
practicas.practica5.insecure_service  
----- Debugging built structures -----  
Name: /home/so/codigo-para-  
practicas/practica5/insecure_service/insecure_service  
Mode:  
Network: inet { stream } inet6 { stream }  
--- Entries ---  
Mode:  r:r      Name:  (/)  
Mode:  r:r      Name:  (/proc/)
```

```
Mode:  r:r      Name:  (/proc/*)
Mode:  x:x      Name:  (/usr/bin/dash)
```

Todo epico debería estar pero vamos a ver que no anda

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

```
root@so:/home/so/codigo-para-practicas/practica5/insecure_service# /usr/sbin/aa-enforce
/home/so/codigo-para-practicas/practica5/insecure_service/insecure_service
Setting /home/so/codigo-para-practicas/practica5/insecure_service/insecure_service to
enforce mode.
```

Recursos

Home

Recursos

Memoria

Directory: /proc

..

fb

fs

bus

dma

irq

net

sys

tty

acpi

keys

kmsg

misc

mtrr

stat

inmem

Network Interfaces

InterfaceIP Address

lo127.0.0.1/8

enp0s3192.168.0.15/24

enp0s8192.168.56.104/24

Processes

PID	User	Name
1	root	systemd
2	root	kthreadd
3	root	rcu_gp
4	root	rcu_par_gp
5	root	slub_flushwq
6	root	netns
8	root	kworker/0:0H-kblockd
10	root	mm_percpu_wq
11	root	rcu_tasks_kthread
12	root	rcu_tasks_rude_kthread
13	root	rcu_tasks_trace_kthread
14	root	ksoftirqd/0
15	root	rcu_preempt
16	root	migration/0
18	root	rcu_hrt/0

Environment Variables

Variable	Value
SHELL	/bin/bash
COLORTERM	truecolor
TERM_PROGRAM_VERSION	1.100.2
LANGUAGE	es_AR:es
PWD	/home/so/codigo-para-practicas/practica5/insecure_service
LOGNAME	so
XDG_SESSION_TYPE	tty
VSCODE_GIT_ASKPASS_NODE	/home/so/.vscode-server/cli/servers/Stable-848b80aeb52026648a8ff9f
MOTD_SHOWN	pam
HOME	/root
LANG	es_AR.UTF-8
LS_COLORS	rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;dist=00;90*:dPKG-old=00;90*:ucf-dist=00;90*:ucf-new=00;90*:ucf-olc
SSL_CERT_DIR	/usr/lib/ssl/certs

Aparentemente estaría entrando a `/proc` pero no verifique si antes no podía.

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