SELinux: Hero Edition

Fedora México

Alex Callejas
Senior Technical Support Engineer | Red Hat
Junio, 2019

About me

Alex Callejas
Senior Technical Support Engineer @Red Hat

@dark_axl

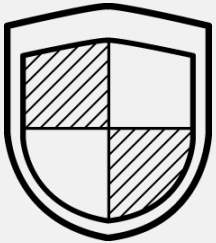
/rootzilopochtli

www.rootzilopochtli.com

Geek by nature, Linux by choice, Fedora of course!

Ver en YouTube

Security



Hardening

Compliance

Policy

SysAdmin's Apocalypse

SELINUX

SELinux

Security Enhanced Linux

- Creado por la NSA como un conjunto de parches para el kernel de Linux que utiliza los Linux Security Modules (LSM)
- Liberado por la NSA bajo la GNU Public License (GPL) en el 2000
- Adoptado por el kernel de Linux en 2003
- Es un ejemplo de Control de Acceso Mandatorio (MAC:Mandatory Access Control)
    - Acceso regido por políticas, no por propiedad

¿Como funciona SELinux?

Conceptos básicos

- SELinux es un sistema de **ETIQUETADO**, lo que significa que cada proceso tiene una **ETIQUETA**. Cada archivo, directorio y objeto del sistema tiene una **ETIQUETA**. Las políticas controlan el acceso entre los procesos etiquetados y los objetos etiquetados. El kernel hace cumplir estas reglas.
- Los dos conceptos más importantes son: ***Labeling*** (archivos, procesos, puertos, etc.) y ***Type enforcement*** (que aísla los procesos entre sí según su tipo).
- El formato de etiquetas es: `user:role:type:level` (*opcional*)

¿Como funciona SELinux?

Ejemplo práctico

Apache Web Server

- Binario: **/usr/sbin/httpd** → `httpd_exec_t`
- Archivos de configuración: **/etc/httpd** → `httpd_config_t`
- Logs: **/var/log/httpd** → `httpd_log_t`
- Directorio de contenido: **/var/www/html** → `httpd_sys_content_t`
- Startup script: **/usr/lib/systemd/system/httpd.service** → `httpd_unit_file_d`
- Proceso: **/usr/sbin/httpd -DFOREGROUND** → `httpd_t`
- Puertos: **80/tcp**, **443/tcp** → `httpd_t` `http_port_t`

Un proceso que se ejecuta en el contexto ***httpd_t*** sólo puede interactuar con objetos con la etiqueta ***httpd_something_t***.

¿Como funciona SELinux?

Conceptos básicos

- Archivo de configuración: **`/etc/selinux/config`**
- Comprobar si SELinux está habilitado: **`# getenforce`**
- Temporalmente deshabilitar/habilitar SELinux: **`# setenforce [1|0]`**
- Status tool: **`# sestatus`**
- Re-etiquetar todo el sistema: **`# touch /.autorelabel`** y **`# reboot`**

¿Qué trata de decirme SELinux?

Troubleshooting

Existen 4 causas principales de errores en SELinux:

- Etiquetado
- SELinux necesita saber
- La aplicación y/o la política de SELinux pueden tener bugs
- Tu información puede estar COMPROMETIDA

¿Qué trata de decirme SELinux?

Troubleshooting

Labeling problem: Los archivos en `/srv/myweb` no están etiquetados correctamente y no se pueden acceder

- Si conoces la etiqueta correcta:
  - `# semanage fcontext -a -t httpd_sys_content_t '/srv/myweb(/.*)?'`
- Si conoces un archivo con la etiqueta equivalente:
  - `# semanage fcontext -a -e /srv/myweb /var/www`
- Restaurar el contexto (para ambos casos):
  - `# restorecon -vR /srv/myweb`

¿Qué trata de decirme SELinux?

Troubleshooting

Labeling problem: Si un archivo se mueve, en lugar de copiarlo, mantiene su contexto original, para solucionarlo:

- Cambiar el contexto a la etiqueta correcta:
  - `# chcon -t httpd_system_content_t /var/www/html/index.html`
- Cambiar el contexto con una etiqueta de referencia:
  - `# chcon --reference /var/www/html/ /var/www/html/index.html`
- Restaurar el contexto (para ambos casos):
  - `# restorecon -vR /var/www/html/`

¿Qué trata de decirme SELinux?

Troubleshooting

SELinux needs to know:

- El Web Server (HTTPD) va a escuchar peticiones por el puerto 8585
  - `# semanage port -a -t http_port_t -p tcp 8585`
- El Web Server (HTTPD) va a enviar correo:
  - `# setsebool -P httpd_can_sendmail 1`

¿Qué trata de decirme SELinux?

Troubleshooting

SELinux needs to know [*Booleans*]

Los *booleanos* permiten modificar partes de las políticas de SELinux en tiempo de ejecución, sin necesidad de re-escribir la política:

- Para ver todos los booleanos: `# getsebool -a`
- Revisar la descripción de cada uno: `# semanage boolean -l`
- Encender/apagar booleano: `# setsebool [boolean] [1|0]`
  - Para hacerlo permanente: `# setsebool -P httpd_can_sendmail 1`

¿Qué trata de decirme SELinux?

Troubleshooting

SELinux Policy/App bugs:

- Rutas inusuales en el código
- Configuraciones
- Redirección del stdout
- File descriptors filtrados
- Memoria ejecutable
- Librerías mal construidas

SELINUX IS A LABELING SYSTEM

¿Qué trata de decirme SELinux?

Troubleshooting

Tu información puede estar COMPROMETIDA

- Si las herramientas no diferencian contextos
- Si tienes dominios confinados que intentan:
  - Cargar módulos de kernel
  - Apagar el modo enforcing de SELinux
  - Escribir a **`etc_t/shadow_t`**
  - Modificar reglas de **`iptables`**
- Tu información puede estar en **PELIGRO**

SELINUX IS A LABELING SYSTEM

¿Qué trata de decirme SELinux?

Troubleshooting tools & tips

- Instala setroubleshoot:
  - **`# dnf -y install setroubleshoot setroubleshoot-server`**
  - Reinicia el servicio audit después de instalarlo
- Usa **`journalctl`** para listar todos los logs relacionados con **`setroubleshoot`**:
  - **`# journalctl -t setroubleshoot --since=19:20`**

SELinux en la vida real

Ejemplo práctico

```
[root@vmtest01 ~]# vi ~/index.html
[root@vmtest01 ~]#
[root@vmtest01 ~]# cat ~/index.html
Hola Mundillo!
[root@vmtest01 ~]# mv ~/index.html /var/www/html/
[root@vmtest01 ~]#
[root@vmtest01 ~]# wget localhost
--2019-06-16 20:49:22--  http://localhost/
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2019-06-16 20:49:22 ERROR 403: Forbidden.

[root@vmtest01 ~]#
```

SELinux en la vida real

Ejemplo práctico

```
[root@vmtest01 ~]# tail /var/log/httpd/error_log
[Tue Jun 16 20:49:22.387701 2019] [core:error] [pid 555:tid 139880684480256]
(13)Permission denied: [client ::1:54922] AH00035: access to /index.html denied
(filesystem path '/var/www/html/index.html') because search permissions are
missing on a component of the path
[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

SELinux en la vida real

Ejemplo práctico

```
[root@vmtest01 ~]# ausearch -m avc -ts recent
time->Tue Jun 16 20:49:22 2019
type=AVC msg=audit(1555447762.387:114): avc:  denied  { getattr } for  pid=555
comm="httpd" path="/var/www/html/index.html" dev="vda1" ino=3207
scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file permissive=0
----
time->Tue Jun 16 20:49:22 2019
type=AVC msg=audit(1555447762.387:115): avc:  denied  { getattr } for  pid=555
comm="httpd" path="/var/www/html/index.html" dev="vda1" ino=3207
scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file permissive=0
[root@vmtest01 ~]#
```

SELinux en la vida real

Ejemplo práctico

```
[root@vmtest01 ~]# journalctl -f -t setroubleshoot
-- Logs begin at Mon 2019-06-08 20:49:18 UTC. --
Jun 16 20:49:22 vmtest01.mx.redhat.lab setroubleshoot[1539]: failed to retrieve
rpm info for /var/www/html/index.html
Jun 16 20:49:22 vmtest01.mx.redhat.lab setroubleshoot[1539]: SELinux is
preventing httpd from getattr access on the file /var/www/html/index.html. For
complete SELinux messages run: sealert -l 4cc11a34-9f9f-49c2-ba0f-0dc9a848ee38
Jun 16 20:49:22 vmtest01.mx.redhat.lab setroubleshoot[1539]: failed to retrieve
rpm info for /var/www/html/index.html
Jun 16 20:49:22 vmtest01.mx.redhat.lab setroubleshoot[1539]: SELinux is
preventing httpd from getattr access on the file /var/www/html/index.html. For
complete SELinux messages run: sealert -l 4cc11a34-9f9f-49c2-ba0f-0dc9a848ee38
[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

SELinux en la vida real

Ejemplo práctico

```
[root@vmtest01 ~]# ls -Z /var/www/html/index.html
unconfined_u:object_r:admin_home_t:s0 /var/www/html/index.html
[root@vmtest01 ~]#
[root@vmtest01 ~]# restorecon -v /var/www/html/index.html
Relabeled /var/www/html/index.html from unconfined_u:object_r:admin_home_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0
[root@vmtest01 ~]#
[root@vmtest01 ~]# ls -Z /var/www/html/index.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/index.html
[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

SELinux en la vida real

Ejemplo práctico

```
[root@vmtest01 ~]# wget localhost
--2019-06-16 21:23:15--  http://localhost/
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15 [text/html]
Saving to: ‘index.html’

index.html
100%[======================================================>]  15  --.-KB/s    in 0s


2019-06-16 21:23:15 (2.82 MB/s) - ‘index.html’ saved [15/15]

[root@vmtest01 ~]#
```

SELinux en la vida real

Troubleshooting

SELinux registra información en todos los logs:

- **/var/log/httpd/error_log**
- **/var/log/audit/audit.log**
- **/var/log/messages** [journalctl]
- **/var/lib/setroubleshoot/setroubleshoot_database.xml**

SELinux en la vida real

Troubleshooting

Pero eso es lo que siempre enseñas...

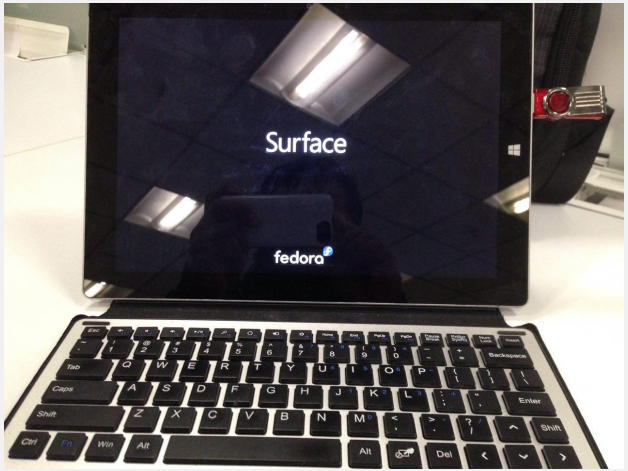
SELINUX IS A LABELING SYSTEM

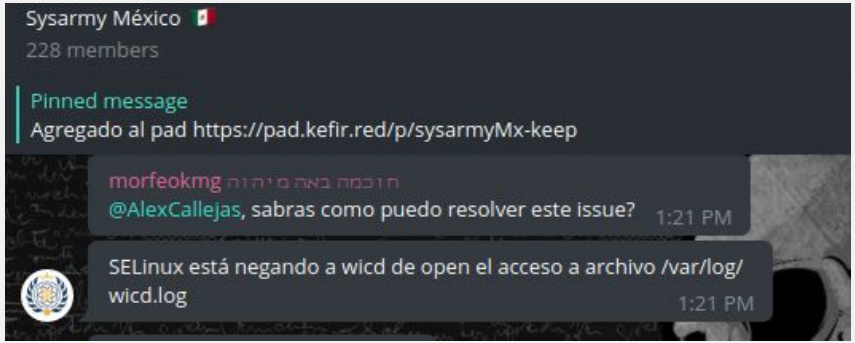
SELinux en la vida real

Ejemplo práctico

Microsoft Surface con Fedora 30

- `wicd en lugar de NetworkManager`





SELINUX IS A LABELING SYSTEM

SELinux en la vida real
Ejemplo práctico

```
[root@vmtest01 ~]# grep denied audit.log | cut -d { -f2 | sort -n | uniq -u
 create } for  pid=2670 comm="wicd" scontext=system_u:system_r:NetworkManager_t:s0
tcontext=system_u:system_r:NetworkManager_t:s0 tclass=appletalk_socket permissive=1
 create } for  pid=2670 comm="wicd" scontext=system_u:system_r:NetworkManager_t:s0
tcontext=system_u:system_r:NetworkManager_t:s0 tclass=ax25_socket permissive=1
 ioctl } for  pid=2670 comm="wicd" path="socket:[52681]" dev="sockfs" ino=52681 ioctlcmd=0x8b01
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=system_u:system_r:NetworkManager_t:s0 tclass=ax25_socket
permissive=1
 ioctl } for  pid=2670 comm="wicd" path="socket:[52684]" dev="sockfs" ino=52684 ioctlcmd=0x8b01
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=system_u:system_r:NetworkManager_t:s0 tclass=appletalk_socket
permissive=1
 setattr } for  pid=2214 comm="wicd" name="dhclient.conf.template" dev="dm-0" ino=437068
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=unconfined_u:object_r:etc_t:s0 tclass=file permissive=0
 setattr } for  pid=2280 comm="wicd" name="dhclient.conf.template" dev="dm-0" ino=437068
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=unconfined_u:object_r:etc_t:s0 tclass=file permissive=0
 setattr } for  pid=2573 comm="wicd" name="dhclient.conf.template" dev="dm-0" ino=437068
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=unconfined_u:object_r:etc_t:s0 tclass=file permissive=0
 setattr } for  pid=2670 comm="wicd" name="dhclient.conf.template" dev="dm-0" ino=437068
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=unconfined_u:object_r:etc_t:s0 tclass=file permissive=1
 setattr } for  pid=859 comm="wicd" name="dhclient.conf.template" dev="dm-0" ino=437068
scontext=system_u:system_r:NetworkManager_t:s0 tcontext=unconfined_u:object_r:etc_t:s0 tclass=file permissive=0
[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

SELinux en la vida real

Ejemplo práctico

```
[root@vmtest01 ~]# ausearch  -c 'wicd' -if audit.log | audit2allow -M my_wicd
******************** IMPORTANT ***********************
To make this policy package active, execute:

semodule -i my_wicd.pp

[root@vmtest01 ~]#
[root@vmtest01 ~]# cat my_wicd.te

module my_wicd 1.0;

require {
        type NetworkManager_t;
        type etc_t;
        class ipx_socket create;
        class ax25_socket { create ioctl };
        class appletalk_socket { create ioctl };
        class file setattr;
}

#============= NetworkManager_t ==============
allow NetworkManager_t etc_t:file setattr;
allow NetworkManager_t self:appletalk_socket { create ioctl };
allow NetworkManager_t self:ax25_socket { create ioctl };
allow NetworkManager_t self:ipx_socket create;
[root@vmtest01 ~]#
```

SELINUX IS A LABELING SYSTEM

SELinux en la vida real

Ejemplo práctico

```
[root@vmtest01 ~]# dnf -y install selinux-policy-devel

[root@vmtest01 ~]# vi my_wicd.te

[root@vmtest01 ~]#  make -f /usr/share/selinux/devel/Makefile my_wicd.pp
Compiling targeted my_wicd module
Creating targeted my_wicd.pp policy package
rm tmp/my_wicd.mod tmp/my_wicd.mod.fc
[root@vmtest01 ~]#
```

SELinux and Containers

Demo

```
[root@vmtest01 ~]# id
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@vmtest01 ~]# id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@vmtest01 ~]# runcon -r system_r -t openshift_t -l s0:c0,c1 /bin/sh
sh-4.4# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:system_r:openshift_t:s0:c0,c1
sh-4.4# id -Z
unconfined_u:system_r:openshift_t:s0:c0,c1
sh-4.4# cat /etc/shadow
cat: /etc/shadow: Permission denied
sh-4.4#
sh-4.4# touch /virus
touch: cannot touch '/virus': Permission denied
sh-4.4#
sh-4.4# exit
exit
[root@vmtest01 ~]#
```

SELinux and Containers: https://danwalsh.livejournal.com/78643.html

Referencias

SELinux Docs

- **SELinux Guide**
  - https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index
- **Fedora Project SELinux Docs**
  - https://fedoraproject.org/wiki/SELinux
- **Dan Walsh's Blog**
  - https://danwalsh.livejournal.com/
- **A SysAdmin's guide to SELinux: 42 answers to the big questions**
  - https://opensource.com/article/18/7/sysadmin-guide-selinux
- **A sysadmin's handy cheat sheet for SELinux**
  - https://opensource.com/article/18/8/cheat-sheet-selinux

stopdisablingselinux.com

redhat.

fedora

Gracias!

fedoracommunity.org/latam

https://t.me/fedoralat

https://t.me/fedoramexico