

SELinux Introduction**Summary**

Investigacion de SELinux Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aequaleam animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguere possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et.

Keywords: Cibersecurity; Linux; Selinux

Contents

1 Introduccion	2
1.1 Que es Selinux	2
1.2 Caracteristicas de Selinux	2
2 Bases de SELinux	3
2.1 Selinux Contexts	3
2.2 Selinux Labels	3
2.3 Selinux Policies	3
3 Casos especiales	3
3.1 Contenedores	3
4 Escenarios	3
4.1 Escenario 1	3
4.2 Escenario 2	3
5 Referencias	3
5.1 Referencia archivos	3
5.2 Referencia archivos de configuracion	3
5.3 Referencia archivos de errores	4
5.4 Referencias comandos	4
5.4.1 Desactivar acciones silenciosas	4
5.4.2 Retiquetar el sistema de archivos	4
5.4.2.1 Grano Grueso	4
5.4.2.2 Grano Fino	5
5.4.3 Monitorizacion Basica SELinux	5
5.4.4 Obtencion de logs de SELinux	6
5.4.5 Lectura de Label o etiquetas (Etiquetas)	6
5.5 Herramientas auxiliares	7
5.5.1 Cockpit	7
5.5.2 Udrca	8
6 Glosario	9
References	9

1 Introduccion

En los sistemas Unix tradicionales, el control de accesos se realiza de forma discrecional Discretionary Access Control (DAC)[1], lo que permite a usuarios y administradores gestionar los permisos sobre archivos y procesos basándose en los identificadores de usuario (UID), de grupo (GID) y otros atributos. Este enfoque flexible puede generar problemas de seguridad, ya que permite a los usuarios manejar los permisos sobre los archivos y recursos que poseen. Por ejemplo, un usuario podría otorgar permisos demasiado amplios a otros usuarios o grupos, lo cual podría permitir el acceso a personas no autorizadas. Adicionalmente podría darse el caso de que se creasen archivos que deberían tener permisos incompatibles debido a quien debe acceder a esos archivos. Para abordar todo esto existe el concepto de Multi-Level Security (MLS)[2]

Security Enhanced Linux (SELinux)[3] se desarrolló para resolver esta problemática mediante la implementación de Mandatory Access Control (MAC)[4], donde las políticas de seguridad son definidas exclusivamente por los administradores del sistema y no pueden ser modificadas ni ignoradas por los usuarios regulares. Además, SELinux sigue una política de “denegación por defecto”, lo que significa que, en ausencia de una regla explícita para una acción, esta será denegada por defecto. Esto contrasta con el modelo DAC, donde un acceso puede ser permitido si no se especifica lo contrario.

En SELinux, todos los objetos y procesos están etiquetados con un Etiqueta que define detalladamente cómo pueden interactuar entre sí. Finalmente, SELinux también aísla los procesos en dominios, lo que impide que un proceso comprometido, como un servidor web, acceda a recursos fuera de su dominio designado. Por lo tanto, SELinux es capaz de mitigar la escalada de privilegios y reducir los riesgos en el sistema, al restringir las acciones que un atacante podría llevar a cabo, limitando su acceso a recursos y otras operaciones que podrían ser posibles en un sistema Unix estándar con DAC en lugar del MAC de SELinux.

1.1 Que es Selinux

SELinux es código que se ejecuta en el espacio de usuario, aprovechando el código de kernel Linux Security Modules (LSM)[5] para proporcionar MAC a través de los recursos del sistema. Los procesos se limitan a dominios, que se pueden considerar como recintos de pruebas. El acceso a objetos del sistema y prestaciones como archivos, colas de mensajes, semáforos, redes, se controla por dominio siguiendo el principio de menor privilegio.

Los directorios y archivos en SELinux se etiquetan con un tipo de dato persistente conocido como Etiqueta que es independiente de los UNIX DAC habituales. Esta capa adicional permite un control más estricto sobre el acceso a los objetos: si un intruso obtiene el control de un proceso propiedad de un usuario, el acceso a todos los archivos propiedad de ese usuario no se otorga automáticamente. El tipo de acceso (lectura, escritura, creación) también puede ser controlado por SELinux. Para una descripción más gráfica y simple se puede referenciar a [6]

1.2 Características de Selinux

- El acceso solo está permitido si existe una regla de política SELinux que lo permita específicamente.
- La política de SELinux está definida administrativamente y se aplica en todo el sistema por SELinux.
- Las decisiones de acceso de SELinux se basan en toda la información disponible, como un usuario de SELinux, rol, tipo y, opcionalmente, un nivel del sistema.
- Mejora de la mitigación para ataques de escalada de privilegios. Los procesos se ejecutan en dominios y, por lo tanto, están separados entre sí. Las reglas de política de SELinux definen cómo los procesos acceden a los archivos y otros procesos.
- SELinux se puede utilizar para hacer cumplir la confidencialidad e integridad de los datos, así como para proteger los procesos de entradas no confiables
- SELinux se ejecuta a nivel de kernel
- SELinux como tal se integra a nivel de kernel a través del framework LSM (Linux Security Modules)
- La aplicación de políticas de SELinux es veloz porque todo, ya está definido por archivos de texto o comandos, transpila a Common Intermediate Language (CIL)[7]

2 Bases de SELinux

Selinux tiene tres modos de operación [Disabled, Permissive, Enforcing]

2.1 Selinux Contexts

2.2 Selinux Labels

2.3 Selinux Policies

Las políticas se guardan en XML en el directorio /var/lib/setroubleshoot/setroubleshoot.xml

3 Casos especiales

3.1 Contenedores

4 Escenarios

4.1 Escenario 1

4.2 Escenario 2

5 Referencias

5.1 Referencia archivos

5.2 Referencia archivos de configuración

- /etc/selinux/config
 - Controla la configuración de SELinux en el sistema.

- grep ^SELINUX= /etc/selinux/config => Permissive||Enforcing
- /sys/fs/selinux/enforce
 - Archivo que indica el estado de selinux
 - cat /sys/fs/selinux/enforce => 0/1
- /sys/fs/selinux
 - Directorio con toda la configuracion de selinux
- /etc/default/grub
 - In grub (/etc/default/grub) GRUB_CMDLINE_LINUX="selinux=0" to disable

5.3 Referencia archivos de errores

- /var/log/audit/*

5.4 Referencias comandos

5.4.1 Desactivar acciones silenciosas

```
1 # -D desactiva mecanismos "don't audit" (bash)
2 semodule -DB
3 # Para volver a activar sirve con reconstruir las politicas
4 semodule -B
```

5.4.2 Retiquetar el sistema de archivos

5.4.2.1 Grano Grueso

```
1 # al reiniciar el sistema reetiqueta el sistema de archivos si selinux detecta este archivo (bash)
2 touch /.autorelabel
```

```
1 # Verifica los contextos de seguridad de los archivos sin realizar cambios. (bash)
2 fixfiles check
3
4 # Restaura el contexto de seguridad de los archivos a sus valores predeterminados.
5 fixfiles restore
6
7 # Pregunta por la eliminacion de /tmp y reetiqueta todos los archivos del sistema de archivos.
8 fixfiles relabel
9
10 # Verifica que todos los archivos tengan el contexto de seguridad correcto.
11 fixfiles verify
12
13 # Reetiqueta todo el sistema
14 fixfiles -F onboot
15
```

```
16 # Estos comandos pueden tener como ultimo parametro la carpeta padre o
    archivo a reetiquetar
17 fixfiles check [folder|file]
```

5.4.2.2 Grano Fino

```
1 # Cambia el contexto de seguridad de un archivo o directorio. (bash)
2 chcon
```

```
1 # Verifica el contexto de seguridad de un archivo utilizando las (bash)
    reglas de política de SELinux.
2 matchpathcon
```

```
1 # Restaura el contexto de seguridad predeterminado de un archivo o (bash)
    directorio.
2 restorecon
```

5.4.3 Monitorizacion Basica SELinux

```
1 # Obtiene el estado actual de cumplimiento de politicas de selinux en (bash)
    el sistema
2 getenforce
3 # Ouput: Enforcing|Permissive
```

```
1 # Obtiene el estado basico de Selinux en el sistema (bash)
2 sestatus
3 # Output:
4 # SELinux status:          enabled
5 # SELinuxfs mount:        /sys/fs/selinux
6 # SELinux root directory:  /etc/selinux
7 # Loaded policy name:      targeted
8 # Current mode:            enforcing
9 # Mode from config file:    enforcing
10 # Policy MLS status:       enabled
11 # Policy deny_unknown status: allowed
12 # Memory protection checking: actual (secure)
13 # Max kernel policy version: 33
```

```
1 # Obtiene el estado basico de los componenetes de las politicas de (bash)
    Selinux en el sistema
2 seinfo
3 # Ouput:
4 # Statistics for policy file: /sys/fs/selinux/policy
5 # Policy Version:           33 (MLS enabled)
6 # Target Policy:            selinux
7 # Handle unknown classes:   allow
8 #   Classes:                134   Permissions:          460
9 #   Sensitivities:           1     Categories:           1024
10 #   Types:                   5266  Attributes:            264
```

11	#	Users:	8	Roles:	15
12	#	Booleans:	365	Cond. Expr.:	398
13	#	Allow:	68070	Neverallow:	0
14	#	Auditallow:	181	Dontaudit:	8830
15	#	Type_trans:	284397	Type_change:	94
16	#	Type_member:	37	Range_trans:	6164
17	#	Role allow:	40	Role_trans:	419
18	#	Constraints:	70	Validatetrans:	0
19	#	MLS Constrains:	72	MLS Val. Tran:	0
20	#	Permissives:	9	Polcap:	6
21	#	Defaults:	7	Typebounds:	0
22	#	Allowxperm:	0	Neverallowxperm:	0
23	#	Auditallowxperm:	0	Dontauditxperm:	0
24	#	Ibendportcon:	0	Ibpkeycon:	0
25	#	Initial SIDs:	27	Fs_use:	35
26	#	Genfscon:	110	Portcon:	665
27	#	Netifcon:	0	Nodecon:	0

5.4.4 Obtencion de logs de SELinux

SELinux setroubleshootd es el proceso que se encarga de gestionar los errores y recomendaciones al usuario de selinux [8]

```
1 # Obtiene los logs relacionados con intentos de accesos no autorizados (bash)
  de recursos
2 journalctl -e -u setroubleshootd
```

```
1 # Obtiene los logs relacionados con intentos de accesos no autorizados (bash)
  de recursos sis usar comando de systemd
2 cat /var/log/audit/audit.log
```

```
1 # Obtiene los ultimos errores lanzados por selinux (bash)
2 ausearch -m avc
3 # En concreto maneja la salida de proceso de auditoria que es la categoria
  en la que esta SELinux
```

5.4.5 Lectura de Etiquetas

```
1 # Obtiene las etiquetas del usuario (bash)
2 id -Z
3 # Output:
4 # unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

```
1 # Obtiene las etiquetas de los archivos (bash)
2 ls -Z
3 # Output:
4 # unconfined_u:object_r:admin_home_t:s0 disk
  unconfined_u:object_r:admin_home_t:s0 podman
  unconfined_u:object_r:admin_home_t:s0 test-secret.asc
```

```

5 # unconfined_u:object_r:admin_home_t:s0 mnt
  unconfined_u:object_r:admin_home_t:s0 test.asc
6 ls -lZ
7 # Output:
8 # total 8
9 # drwxr-xr-x. 3 root root unconfined_u:object_r:admin_home_t:s0 89 Nov 17
  21:38 disk
10 # drwxr-xr-x. 2 root root unconfined_u:object_r:admin_home_t:s0 6 Nov 24
  02:25 mnt
11 # drwxr-xr-x. 3 root root unconfined_u:object_r:admin_home_t:s0 19 Nov 17
  21:40 podman
12 # -rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0 1745 Nov 23
  17:54 test.asc
13 # -rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0 3779 Nov 23
  17:54 test-secret.asc
14

```

```

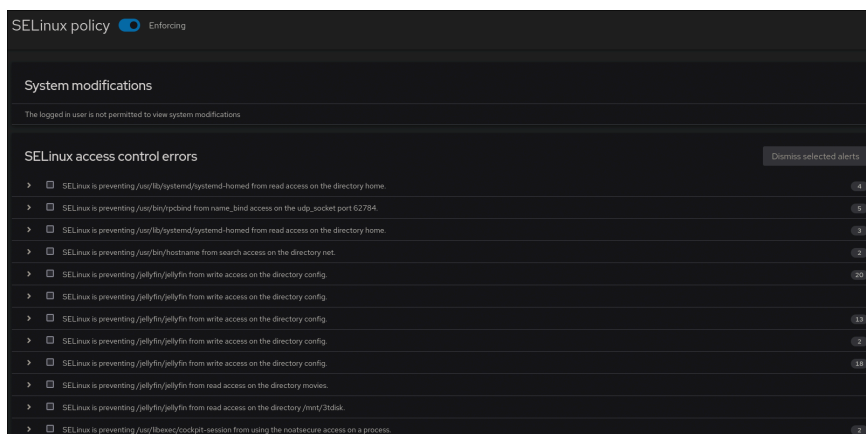
1 # Obtiene las etiquetas de procesos (bash)
2 ps -Z
3 # Output:
4 # LABEL PID TTY TIME CMD
5 # unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 5937 pts/1 00:00:00
  bash
6 # unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 6099 pts/1 00:00:00
  ps


```

5.5 Herramientas auxiliares

5.5.1 Cockpit

Cockpit [9] es una interfaz grafica para servidores, en ella podemos ver diferentes aspectos de un servidor, en este caso las politicas de SELinux que aplica junto a un yaml de ansible para ejecutar esas mismas politicas que han sido modificadas de la base en otros equipos



SELinux policy  Enforcing	
System modifications	
The logged in user is not permitted to view system modifications	
SELinux access control errors	
<input type="checkbox"/> SELinux is preventing /usr/lib/systemd/systemd from read access on the directory home.	4
<input type="checkbox"/> SELinux is preventing /usr/bin/pdftotext from name_bind access on the udp_socket port 62794.	6
<input type="checkbox"/> SELinux is preventing /usr/lib/systemd/systemd from read access on the directory home.	3
<input type="checkbox"/> SELinux is preventing /usr/bin/hotspotd from search access on the directory var.	2
<input type="checkbox"/> SELinux is preventing /usr/bin/pdftotext from write access on the directory config.	20
<input type="checkbox"/> SELinux is preventing /usr/bin/pdftotext from write access on the directory config.	13
<input type="checkbox"/> SELinux is preventing /usr/bin/pdftotext from write access on the directory config.	2
<input type="checkbox"/> SELinux is preventing /usr/bin/pdftotext from write access on the directory config.	15
<input type="checkbox"/> SELinux is preventing /usr/bin/pdftotext from read access on the directory movies.	
<input type="checkbox"/> SELinux is preventing /usr/bin/pdftotext from read access on the directory jms/720iok.	
<input type="checkbox"/> SELinux is preventing /usr/libexec/cryptsetup-session from using the nostore access on a process.	2
<input type="checkbox"/> SELinux is preventing /usr/libexec/cryptsetup-session from using the rlimitinh access on a process.	2
<input type="checkbox"/> SELinux is preventing /usr/libexec/cryptsetup-session from using the sigh access on a process.	2
<input type="checkbox"/> SELinux is preventing /usr/bin/awk_chqsigd from using the nostore access on a process.	3
<input type="checkbox"/> SELinux is preventing /usr/bin/awk_chqsigd from using the rlimitinh access on a process.	3
<input type="checkbox"/> SELinux is preventing /usr/bin/awk_chqsigd from using the sigh access on a process.	3

Cockpit adicionalmente nos muestra de forma sencilla los fallos de acceso y sus formas de permitir ademas de un boton para implementarlas con un solo click

[illegible][illegible]

5.5.2 Udica

6 Glosario

CIL – Common Intermediate Language 3

DAC – Discretionary Access Control 2

LSM – Linux Security Modules: Tambien conocido pero desactualizado MCS o Multilevel Category Security 2

Etiqueta – Label o etiqueta 1, 2, 6

MAC – Mandatory Access Control 2

MLS – Multi-Level Security 2

SELinux – Security Enhanced Linux 2, 6, 7

References

- [1] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Discretionary_access_control
- [2] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Multilevel_security
- [3] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Security-Enhanced_Linux
- [4] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Mandatory_access_control
- [5] Accessed: Nov. 30, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Linux_Security_Modules
- [6] [Online]. Available: https://people.redhat.com/duffy/selinux/selinux-coloring-book_A4-Stapled.pdf
- [7] Accessed: Nov. 30, 2024. [Online]. Available: <https://selinuxproject.org/page/PolicyLanguage>
- [8] Accessed: Nov. 30, 2024. [Online]. Available: <https://linux.die.net/man/8/setroubleshootd>
- [9] Accessed: Nov. 30, 2024. [Online]. Available: <https://github.com/cockpit-project/cockpit>