CySec News

2019 SEPTIEMBRE

SANDBOX EN LINUX

INTRODUCCIÓN

En seguridad informática, un Sandbox es un entorno de ejecución restringido y controlado que evita que el software potencialmente malicioso, como el código móvil, acceda a los recursos del sistema, excepto aquellos para los cuales el software está autorizado.

Su principal utilidad es ejecutar programas de forma segura y sin peligro de comprometer el resto del sistema operativo.

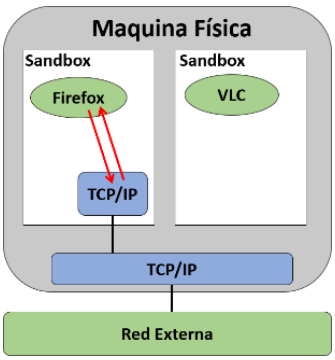

Ilustración 1, Fuente Propia

Firejail Sandbox es un programa que utiliza SUID (Set User ID), los espacios de nombres del kernel Linux (Linux Namespaces) y seccomp-bpf. De esta forma podremos ejecutar cualquier tipo de programa de forma segura en un entorno controlado. Permite que un proceso y todos sus descendientes tengan su propia vista privada de los recursos del núcleo compartidos globalmente, como la pila de red, la tabla de procesos y la tabla de montaje.

Puede proteger cualquier tipo de proceso: servidores, aplicaciones gráficas e incluso sesiones de inicio de sesión de usuario. El software incluye perfiles de seguridad para una gran cantidad de programas Linux: Mozilla Firefox, Chromium, VLC, Transmisión, etc.

SOBRE LOS PERMISOS

Firejail Sandbox tiene un contenedor del sistema de archivos que se crea cuando se inicia y se destruye cuando se cierra. Se basa en el sistema de archivos actual instalado en las computadoras de los usuarios. Solo permite acceder a un pequeño conjunto de archivos y directorios.

Directorio	Descripción
/boot	En lista negra
/bin	Solo lectura
/dev	Solo lectura; similar al directorio de inicio, solo está disponible en el sistema de archivos esqueleto
/etc	Solo lectura, /etc/passwd y /etc group se han modificado para hacer referencia solo al usuario actual
/home	Solo el usuario actual es visible
/lib, /lib32, /lib64	Solo lectura
/proc, /sys	Se vuelve a montar para reflejar el nuevo espacio de nombres PID; solo los procesos iniciados por el programa son visibles
/usr	Solo lectura
/usr/sbin	En lista negra
/var	Solo lectura; similar al directorio de inicio, solo está disponible en el sistema de archivos esqueleto

DEMOSTRACIÓN

ESCENARIO

- El sysadmin ha implementado un Firejail Sanbox como medida de prevención.
- El servidor tiene instalado vim.
- El atacante logra tener acceso mediante un shell al servidor GNU/Linux.

PARTE 1: Implementación de Firejail Sanbox:

- Descargar Firejail Sanbox desde https://sourceforge.net/projects/firejail/files/firejail/
- Luego instalarlo en su equipo GNU/Linux.
- En el directorio /etc/firejail se encuentran los perfiles de seguridad para diferentes aplicaciones. Para nuestro ejemplo usaremos el perfil de seguridad /etc/firejail/vim.profile, agregar la línea: tracelog para activar el registro.
- Configurar el uso de Firejail de forma predeterminada, ejecutar:
- ln -s /usr/bin/firejail /usr/local/bin/vim
- Crear un usuario
- Agregar al usuario a la lista de usuarios permitidos a usar Firejail SandBox
- firecfg --add-users usuario

```
protocol unix,inet,inet6
seccomp
tracelog
```

Ilustración 2, Fuente Propia

PARTE 2: Prueba de funcionamiento de Firejail Sanbox:

- Iniciar sesión en la consola virtual 2 y ejecutar el editor VI.
- Volver a la consola virtual 1 e identificar el PID
- Acceder dentro de sandbox y ejecutar algunos comandos
- Salir del sandbox
- Visualizar el registro:
- tail -f /var/log/messages

```
[root@bacula ~]# firejail --list
1808:jeler::/usr/bin/firejail /bin/vim
[root@bacula ~]#
[root@bacula ~]# firejail --join=1808
Switching to pid 1809, the first child process inside the sandbox
Child process initialized in 18.87 ms
[root@bacula ~]#
[root@bacula ~]# ls /boot
[root@bacula ~]# ls /usr/sbin
[root@bacula ~]# cd /boot
bash: cd: /boot: Permiso denegado
[root@bacula ~]# cat /etc/shadow
[root@bacula ~]# exit
exit
```

Ilustración 3, Fuente Propia

```
Aug 13 06:13:36 bacula firejail[7]: blacklist violation - sandbox 1808, exe ls, syscall opendir, path /boot
Aug 13 06:13:46 bacula firejail[8]: blacklist violation - sandbox 1808, exe ls, syscall opendir, path /usr/sbin
Aug 13 06:13:57 bacula firejail[6]: blacklist violation - sandbox 1808, exe bash, syscall chdir, path /boot
Aug 13 06:13:57 bacula firejail[6]: blacklist violation - sandbox 1808, exe bash, syscall chdir, path /boot
Aug 13 06:14:11 bacula firejail[9]: blacklist violation - sandbox 1808, exe cat, syscall open, path /etc/shadow
```

Ilustración 4, Fuente Propia

CONCLUSIÓN

Firejail Sandbox permite enjaular las aplicaciones incrementando el nivel de seguridad y reduciendo la superficie de ataque

FUENTE DE REFERENCIA

- Firejail: https://firejail.wordpress.com/
- Sandbox: https://csrc.nist.gov/glossary/term/Sandbox

Contribuidor

Jeler Vásquez: Profesional en gestión de proyectos TI y mejoras de procesos, colaborando en ventas, consultoría y capacitación. Especialista en implementación, administración, optimización y seguridad de redes.

LinkedIn: https://www.linkedin.com/in/jeler-vásquez-cobos-a058a92a/

Recursos LCW

LinkedIn	https://www.linkedin.com/company/cysecbywomen/
Facebook	https://www.facebook.com/CySecByWomen/
Twitter	@cysecbywomen