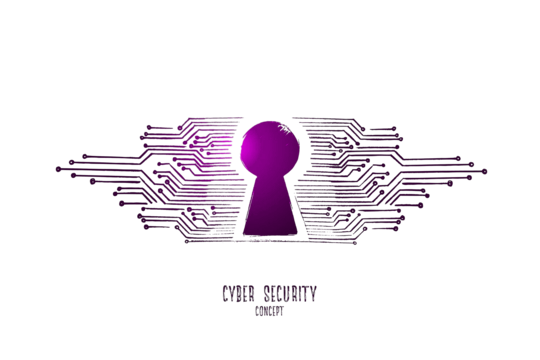
Bastionado de redes 

y sistemas.



**U6\_A1 Kernel Hardening y aislamiento de procesos**

**Francisco Iván Ramírez Ortega**

Curso 2023 - 2024

**IES El Rincón**

Curso de especialización en Ciberseguridad en entornos de las tecnologías de la información.

# Kernel Hardening y aislamiento de procesos

# Introducción

// poner una descripción

# Objetivo

Elaborar un pequeño informe con los pasos necesarios para aislar procesos de sistema

| Herramientas |
| --- |
| * Sistema operativo Linux ( Ubuntu ) . |
|  |

**ÍNDICE**

[**Kernel Hardening y aislamiento de procesos 2**](#_xfpg6pduf6p7)

[**Introducción 2**](#_b9oaw39qdr1r)

[**Objetivo 3**](#_3uoprqr5rx0x)

[**Herramientas 3**](#_wzp689uhopv7)

[**Práctica 3**](#_jwcepppetktp)

[**Bibliografía 4**](#_fxv8jhomw7i7)

| Práctica |
| --- |
| Ajustar parámetros del kernel con **sysctl** |
| El directorio [**/proc**](https://docs.kernel.org/filesystems/proc.html)  un sistema de archivos virtual que proporciona información sobre los procesos del sistema y el kernel. |
| En el directorio /proc encontraremos dos clases de información. |
|  |
| Información sobre procesos de usuario |
| Cada uno de los directorios numerados corresponde con el Process ID (PID) de cada usuario. |
|  |
|  |
| Información sobre qué está haciendo el kernel del sistema operativo |
|  |
| [/proc/sys](https://docs.kernel.org/admin-guide/sysctl/index.html) |
| La carpeta [**/proc/sys**](https://docs.kernel.org/admin-guide/sysctl/index.html) es un tanto especial pues permite al administrador configurar el kernel de sistema. |
|  |
| Se puede editar, sin persistencia, tras reinicios a través de **echo.** |
| Uso de [**sysctl**](http://man.he.net/?topic=sysctl&section=all) |
| **sysctl** se utiliza para modificar parámetros del kernel en tiempo de ejecución.  Los parámetros disponibles son aquellos listados bajo /proc/sys/.  Procfs es necesario para el soporte de sysctl en Linux. Puedes utilizar sysctl tanto para leer como para escribir datos de sysctl. |
| Esta ruta contiene archivos con nombres reconocidos por el sistema y generalmente guardan uno o pocos valores de configuración. sysctl los solamente los edita. |
|  |
| Algunas configuraciones interesantes |
| 1. **net.ipv4.ip\_forward**: Este parámetro controla si se permite o no el reenvío de paquetes entre interfaces en IPv4. Puede ser útil si estás configurando tu sistema como un enrutador. 2. **net.core.somaxconn**: Define el número máximo de conexiones pendientes que el kernel permitirá en un socket de escucha. Puede ser útil para ajustar el rendimiento de servicios que manejan muchas conexiones, como servidores web. 3. **vm.swappiness**: Este valor controla qué tan agresivamente el kernel intercambia datos entre la memoria RAM y el espacio de intercambio (swap). Puede ser útil ajustarlo para optimizar el rendimiento del sistema dependiendo del tipo de carga de trabajo. 4. **fs.file-max**: Define el número máximo de descriptores de archivos que el kernel puede asignar. Puede ser útil aumentar este valor si tu sistema maneja muchas conexiones simultáneas o tiene una gran cantidad de archivos abiertos. 5. **kernel.randomize\_va\_space**: Controla la aleatorización de las direcciones de memoria de los procesos para ayudar a mitigar ciertos tipos de ataques de seguridad, como ataques de desbordamiento de búfer. Es importante tener en cuenta que este valor debe estar configurado adecuadamente para mantener un buen equilibrio entre seguridad y compatibilidad con ciertas aplicaciones. 6. **kernel.panic**: Define el tiempo en segundos antes de que el kernel reinicie automáticamente el sistema después de un pánico del kernel. Puede ser útil ajustar esto en entornos críticos para minimizar el tiempo de inactividad en caso de problemas graves del kernel. |
| Sintaxis |
|  |
| Ejemplos |
| * Muestra todos los archivos editables y sus valores. |
| **sysctl -a** |
| * Mostrar valor del parametro |
| **sysctl kernel.hostname** |
| * Modificar un parámetro temporalmente |
| **sudo sysctl -w net.ipv4.ip\_forward=1** |
| * Modificar un parámetro permanentemente: |
| Agregar el cambio el archivo **/etc/sysctl.conf** en el siguiente formato: |
|  |
| Recargamos la configuración del kernel |
| **sudo sysctl -p** |
| Lynis - Escáner de sistema |
| Instalación |
| **sudo apt install lynis** |
|  |
| Comandos de lynis |
|  |
| Usos frecuentes |
|  |
| Escaneo del sistema |
| Lynis realiza un análisis de seguridad del sistema y nos nos devuelve información referente a: |
| * **Herramientas del sistema:** binarios del sistema * **Arranque y servicios:** cargadores de arranque, servicios de inicio * **kernel**: nivel de ejecución, módulos cargados, configuración del núcleo, volcados principales * **Memoria y procesos:** procesos zombis, procesos en espera de E/S * **Usuarios, grupos y autenticación**: IDs de grupo, sudoers, configuración de PAM, envejecimiento de contraseñas, la máscara predeterminada * Intérpretes de comandos * **Sistemas de archivos:** puntos de montaje, archivos /tmp, sistema de archivos raíz * **Almacenamiento**: USB-storage, firewire ohci * **NFS** * **Software**: servicios de nombres: dominio de búsqueda DNS, BIND * **Puertos y paquetes:** paquetes vulnerables/actualizables, repositorio de seguridad * **Redes**: servidores de nombres, interfaces promiscuas, conexiones * Impresoras y colas: configuración de cups * **Software** de correo **electrónico y mensajería** * **Información sobre firewalls: iptables, pf** * Software de **servidores web: Apache, nginx** * **Soporte SSH**: configuración SSH * **Soporte SNMP** * **Bases de datos**: contraseña de root de MySQL * **Servicios LDAP** * **Información sobre php**: opciones de php * **Soporte Squid** * **Registro y archivos:** demonio Syslog, directorios de registros * **Servicios inseguros:** inetd * **Banners e identificación** * **Tareas programadas**: crontab/cronjob, atd * **Datos de sysstat, auditd** * **Hora y sincronización:** demonio ntp * **Criptografía:** expiración del certificado SSL * **Virtualización** * **Frameworks de seguridad:** AppArmor, SELinux, estado de seguridad * **Escáneres de malware** * **Directorios de inicio**: archivos de historial de comandos del intérprete de comandos |
| **sudo lynis audit system** |
| Puede añadirse una flag para cambiar el tipo de escaneo. Ej: --pentest |
|  |
|  |
|  |
|  |
| Copiamos los valores en un fichero (kernel\_val) |
|  |
| Filtramos los valores diferentes a los por defecto. |
| **grep ‘DIFFERENT’ kernel\_val > kernel\_diff\_val.conf** |
|  |
|  |
| Ahora estaríamos viendo los valores que han sido cambiados de **/proc/sys** |
| Persistir valores editados en /proc/sys |
| La carpeta **/etc/sysctl.d** contiene los archivos que serán leídos en la configuración del sistema. |
| La convención de los nombres **[1-99]-[nombre].conf** se usa para establecer la prioridad con la que los archivos serán leídos. |
|  |
| // Estamos tocando partes críticas del sistema, seguir los pasos teniendo en cuenta que pueden aparecer errores críticos.  Realizar una imagen del sistema puede ayudar a recuperar en caso de fallos. |
| Le cambiamos el nombre para que cumpla la convención de los nombres **[1-99]-[nombre].conf** y lo movemos a la carpeta **/etc/sysctl.c** |
|  |
|  |
| Editamos el archivo, añadiendo los valores entre paréntesis tras un símbolo ‘=’ |
| Antes |
|  |
| Copiamos las líneas que deben tener este aspecto |
| t |
| Las añadimos al archivo **/etc/sysctl.d** |
| Reiniciamos |
| **reboot** |
| En este momento al realizar de nuevo un análisis comprobaremos que los valores aparecerán con el estado “OK”. Lo que significa que los valores se corresponden con los predefinidos, por defecto, del archivo /etc/sysctl.c |
| Aislamiento de procesos |
| Concepto de aislamiento de espacio de nombres. |
| “Namespaces” o espacio de nombres es una característica de seguridad que se introdujo en el Kernel en la versión 2.4.19 en 2002.  Permite a un p**roceso tener sus propios recursos** de un ordenador que **otros procesos no pueden ver.**  Mediante esta tecnología podemos usar productos que la implementen, por ejemplo, algunos exploradores web usan namespaces para crear un sandbox para cada pestaña que abramos.  Docker hace uso de estos Namespace. |
| Objetivo |
| Ejecutar el servidor **apache2** dentro de un sandbox creado con [firejail](http://firejail). |
| Firejail es un programa [SUID](https://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/doc-curso-salamanca-admin-avanzada/html/ch08s06.html) que reduce el riesgo de brechas de seguridad al restringir el entorno de ejecución de aplicaciones no confiables utilizando espacios de nombres de Lin**ux y seccomp-bpf**. Permite que un proceso y todos sus descendientes tengan su propia vista privada de los recursos del kernel compartidos globalmente, como la pila de red, la tabla de procesos y la tabla de montaje. |
| Resulta útil para:   * Aislar la información sensible de los exploradores. * Probar aplicaciones no firmadas, de orígenes desconocidos. |
| Firejail tiene diferentes perfiles de configuración predeterminados para varios programas en Linux. Dichos perfiles pueden definir parámetros como: |
| 1. Las carpetas de nuestro sistema de archivos a las que tendrá acceso el programa que se ejecuta en el sandbox. 2. Los permisos que tendrá el programa sobre ciertos directorios de nuestro sistema operativo. 3. Si los programas tienen acceso al servidor de sonido. 4. Deshabilitar la aceleración 3D de un programa en concreto. 5. Usar unos DNS específicos para un programa usado dentro del sandbox. 6. Determinar si el programa tendrá acceso a Internet. |
|  |
| Instalación |
| **sudo apt-get install firejail** |
| Instalación de la interfaz gráfica |
| **sudo apt-get install firetools** |
| Crear perfil de Firejail |
| En **/etc/firejail** se encuentran los archivos de configuración de los procesos. |
| **sudo nano /etc/firejail/custom.apache.profile** |
|  |
|  |

| Incidencia |
| --- |
|  |
| /etc/firejail/firejail.config |
|  |
|  |

| Bibliografía |
| --- |
| [/proc](https://docs.kernel.org/filesystems/proc.html) |
| [/proc/sys](https://docs.kernel.org/admin-guide/sysctl/index.html) |
| [sysctl](http://man.he.net/?topic=sysctl&section=all) |
| [Firejail](https://firejail.wordpress.com/) |