Bastille Linux

Bastille Linux es una herramienta de **endurecimiento (hardening)** de sistemas operativos Unix/Linux. Su objetivo es mejorar la seguridad del sistema desactivando servicios innecesarios, aplicando configuraciones seguras y verificando permisos de archivos.

A diferencia de las herramientas de auditoría, Bastille hace **cambios directos** en el sistema para hacerlo más seguro.

Para versiones antiguas. Para las actuales usa **Lynis**

Instalación de Bastille Linux (Vía GitHub)

Paso 1: Instalar dependencias

Bastille es un script de Perl, por lo que necesita el intérprete de Perl, la herramienta git para descargar el código, y el paquete gráfico perl-tk para la interfaz interactiva.

```
# Actualizar la lista de paquetes

sudo apt update



# Instalar git, perl y la librería Tk (necesaria para la interfaz gráfica)

sudo apt install git perl libtk-perl -y

sudo apt install wget unzip -y
```

Paso 2: Clonar el Repositorio

```
# Navegar a una ubicación donde guardar el código (ej. la carpeta de inicio)

cd ~

# Clonar el repositorio de Bastille Linux

git clone https://github.com/discogestalt/bastille-linux.git
```

Paso 3: Instalar Bastille

1. **Navega al directorio clonado:**

```
cd bastille-linux

chmod +x install.sh
```

2. **Ejecuta el script de instalación** con permisos de superusuario:

```
sudo ./install.sh
```

El script debería ejecutarse y preguntarte dónde deseas instalar Bastille (generalmente /usr/local/bastille). Presiona **Enter** para confirmar la ruta por defecto.

Paso 4: Ejecutar Bastille

Una vez finalizada la instalación, ya puedes ejecutar la herramienta de endurecimiento:

Bash

```
sudo bastille
```

Esto iniciará el modo interactivo, que te hará preguntas paso a paso para aplicar las configuraciones de seguridad a tu sistema Ubuntu 24.04.

1. Instalación de Bastille Linux

Bastille está disponible en los repositorios de Ubuntu, lo que simplifica la instalación.

1. **Actualizar el índice de paquetes:**

   ```
   sudo apt update
   sudo add-apt-repository universe
   ```

2. **Instalar Bastille:**

   ```
   sudo apt install bastille -y
   ```

Esto instalará el programa y sus dependencias.

Ubicación Clave

El programa principal se instala en /usr/sbin/bastille y los archivos de configuración están en /etc/bastille/.

2. Puesta en Marcha (El Proceso de Endurecimiento)

El proceso de Bastille es **interactivo** y guiado. Es crucial que preste atención a cada pregunta, ya que sus respuestas determinarán los cambios de seguridad que se aplicarán a su sistema.

Ejecución de la Interfaz

Ejecute Bastille como root o con sudo para iniciar el proceso de endurecimiento:

sudo bastille

Guía del Asistente Interactivo

Bastille lo guiará a través de varias secciones. La herramienta realiza automáticamente una copia de seguridad de los archivos de configuración originales antes de hacer cualquier cambio, lo que permite la reversión.

Sección	**Función**	**Importancia**
I. Archivos y Permisos	Pregunta sobre permisos de archivos sensibles, la eliminación de *set-user-ID* (SUID) inseguros y la restricción del acceso a directorios.	**Alta.** Los permisos incorrectos son una causa común de escalada de privilegios.
II. Cuentas de Usuario	Pregunta si debe deshabilitar cuentas de usuario innecesarias (ej. nobody, sync) y establecer políticas de contraseña.	**Media/Alta.** Reducir la superficie de ataque al eliminar cuentas que no se usan.

Sección	Función	Importancia
III. Dispositivos	Pregunta sobre la desactivación de dispositivos USB, CD-ROM o disquetes para usuarios comunes, previniendo la carga de *malware*.	**Media.** Importante para la seguridad física.
IV. Configuración del Sistema de Archivos	Pregunta sobre la activación de montajes de sistemas de archivos seguros (ej. evitar que los ejecutables se carguen en /tmp).	**Alta.** Protege contra muchos *exploits* que usan directorios temporales.
V. Registro de Logs	Configura el registro de eventos del sistema (syslog) para asegurar que la actividad sea auditada correctamente.	**Alta.** Crucial para la detección de intrusiones posterior al evento.
VI. Red y Firewall	Pregunta sobre la desactivación de servicios de red inseguros (ej. ICMP *redirects*), y la configuración de políticas de *firewall* básicas.	**Alta.** Reduce el riesgo de ataques a la pila TCP/IP.

Proceso Clave:

1. **LEA CADA PREGUNTA:** Bastille presenta una explicación detallada de cada cambio. Si no está seguro, lea la explicación o escoja la opción por defecto (a menudo la más segura).
2. **APLICAR CAMBIOS:** Al final de cada sección, Bastille le preguntará si desea aplicar los cambios sugeridos. Si responde Yes, los cambios se escribirán inmediatamente en los archivos de configuración del sistema.

3. Verificación y Reversión

Después de que Bastille ejecute los cambios, es vital verificar que todo funcione correctamente y saber cómo revertir los cambios si causan problemas.

Verificación

1. Revisar los Logs:

   Los logs del proceso de endurecimiento se guardan en:

   cat /var/log/bastille/bastille.log

   Revise este archivo para confirmar qué cambios se aplicaron y si hubo algún error.

2. Revisar el Archivo de Estado:

   Bastille mantiene un registro de todas las políticas aplicadas.

   cat /etc/bastille/bastille.conf

Reversión de Cambios

Si un cambio aplicado por Bastille rompe la funcionalidad necesaria del sistema, puede revertir la última configuración.

1. **Iniciar el Modo Reversión:**

   sudo bastille -r

   Esto revierte el último conjunto de cambios aplicados volviendo a los archivos de respaldo.

2. Revertir a un Punto Específico:

   Si desea volver a una configuración aún más antigua, puede especificar el número de la versión de configuración.

   sudo bastille -r <versión_anterior>

Advertencia: Bastille es una herramienta poderosa que realiza cambios fundamentales. Siempre úsela primero en un entorno de prueba (como su VirtualBox) antes de aplicarla a un servidor de producción.