The LinUx Hardening System

Hernán Cortés

Daisy González

Jorge Montes

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

La primera opción y el mejor ejemplo

TLUHS surge para automatizar el proceso de Hardening en servidores Linux

¿Qué es Hardening?

Hardening es empleado para referirse a un conjunto de métodos, buenas prácticas, configuraciones y administración de los servicios de una máquina para **minimizar las vulnerabilidades de su sistema operativo**

Problemática actual

En el momento los **procesos de Hardening de plataformas Linux son tediosos y requieren de una gran inversión en tiempo** debido a que no existe una herramienta que automatice el proceso

Motivación

- El Hardening de plataformas es una de las necesidades actuales en las organizaciones
- La tendencia de hoy en día es preservar la información en servidores Linux

Objetivos

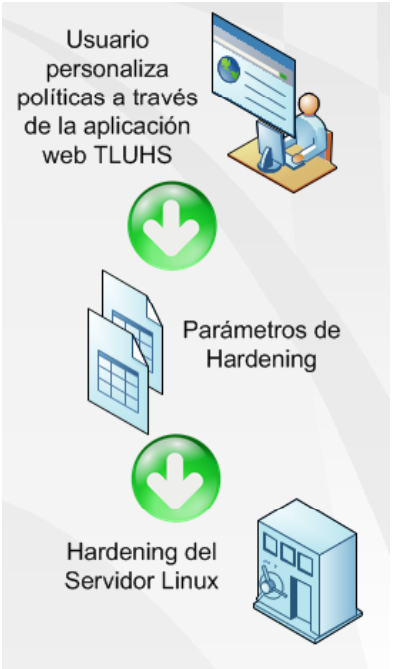
- Desarrollar una herramienta que preste el **servicio de Hardening de servidores Linux**
- **Administrar políticas de seguridad** de la información
- Generar un **backup de la configuración** del servidor antes del aseguramiento, asegurando su **integridad con MD5**

TLUHS es una aplicación web, multi-usuario y multi-servidor que permite administra el proceso de Hardening

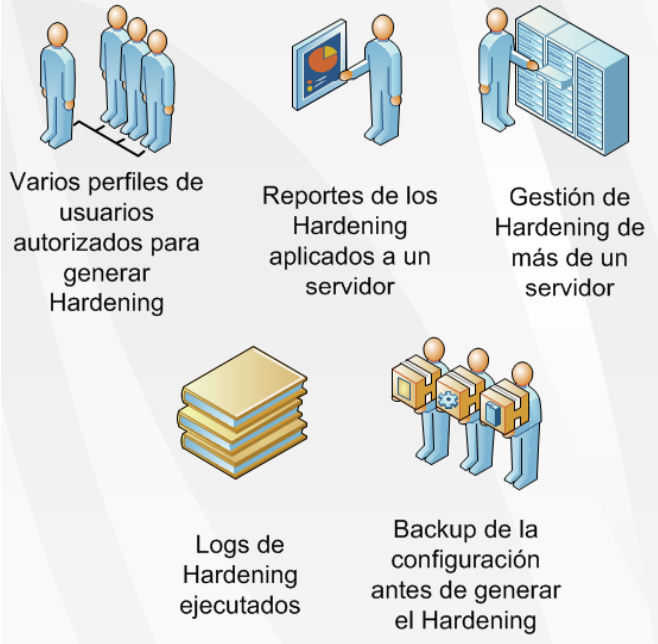
Alcance

TLUHS genera scripts automatizados para cuatros distribuciones de Linux

Proceso



Reportes

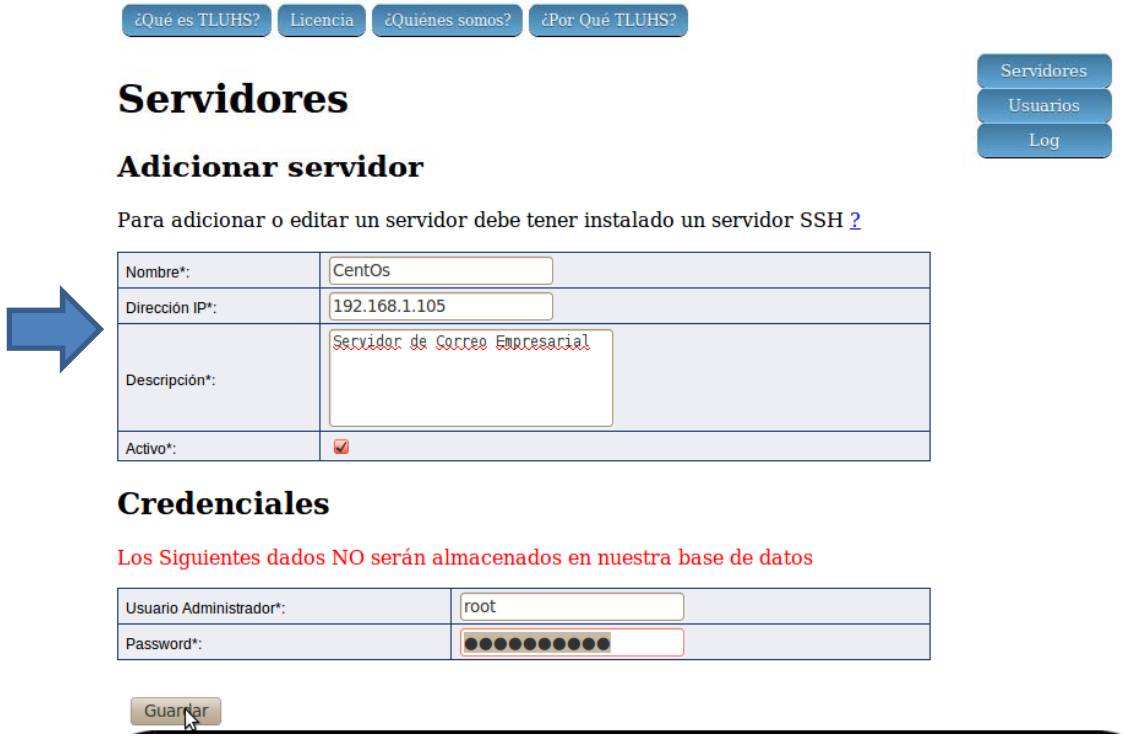


TLUHS es diferente a cualquier aplicación de Hardening existente

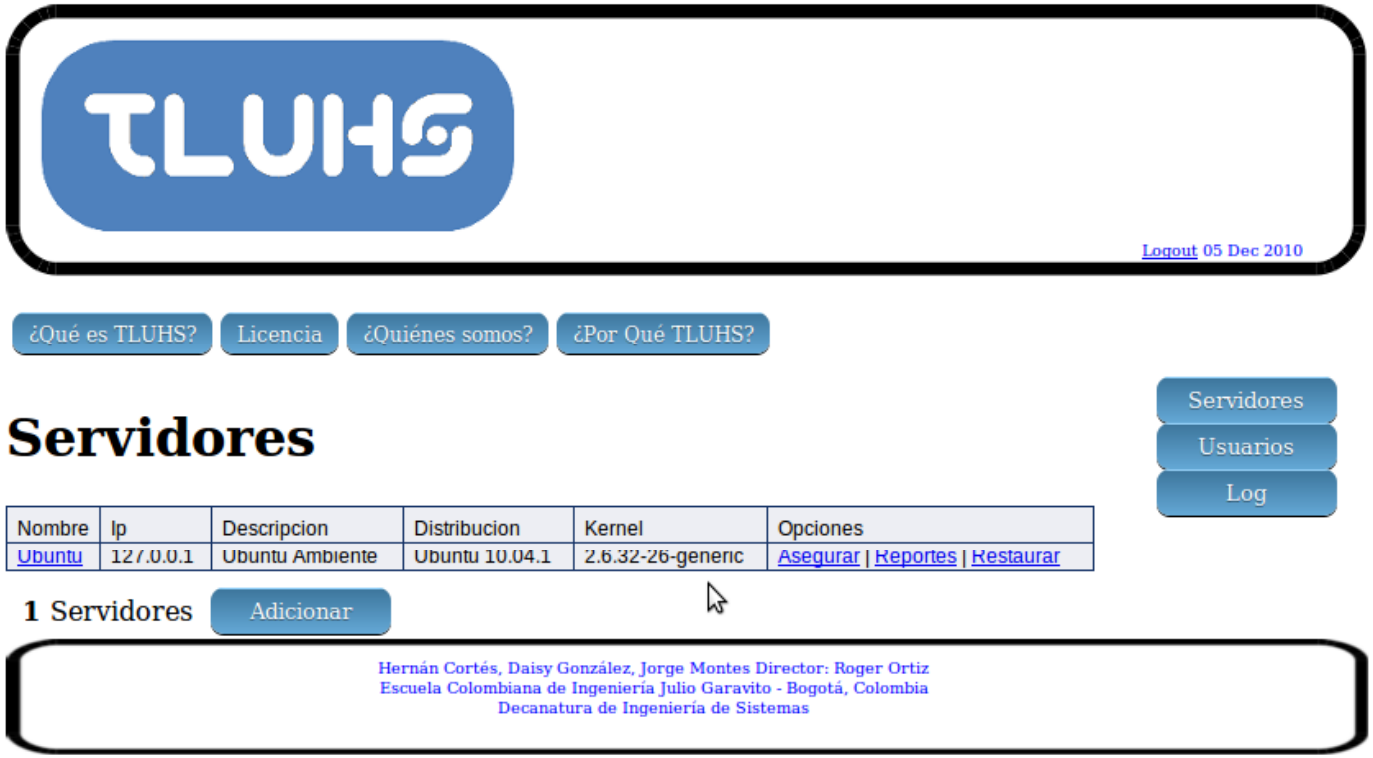
A diferencia de las aplicaciones desarrolladas para automatizar parcial o totalmente el proceso de Hardening de servidores Linux, TLUHS sobresale porque:

- Está enfocado en recomendar al usuario las mejores prácticas de seguridad para que el mismo las aplique alineándolas con las políticas de seguridad definidas en su organización
- Es una aplicación web orientada a facilitar la administración y ejecución del proceso de Hardening
- Permite la creación de uno o más usuarios con diferentes permisos de acceso para ejecutar y administrar el proceso
- Permite almacenar, recuperar y ejecutar copias de seguridad antes del proceso de Hardening. Las copias de seguridad son almacenadas localmente en el servidor y en la base de datos de TLUHS como respaldo adicional
- Almacena la información de más de un servidor, permitiendo la administración centralizada de los mismos
- Alimenta un log de acciones ejecutadas sobre los servidores
- Permite generar y consultar reportes de los procesos asociados a un servidor con el fin de recopilar y detallar el Hardening ejecutado en cualquier momento del tiempo

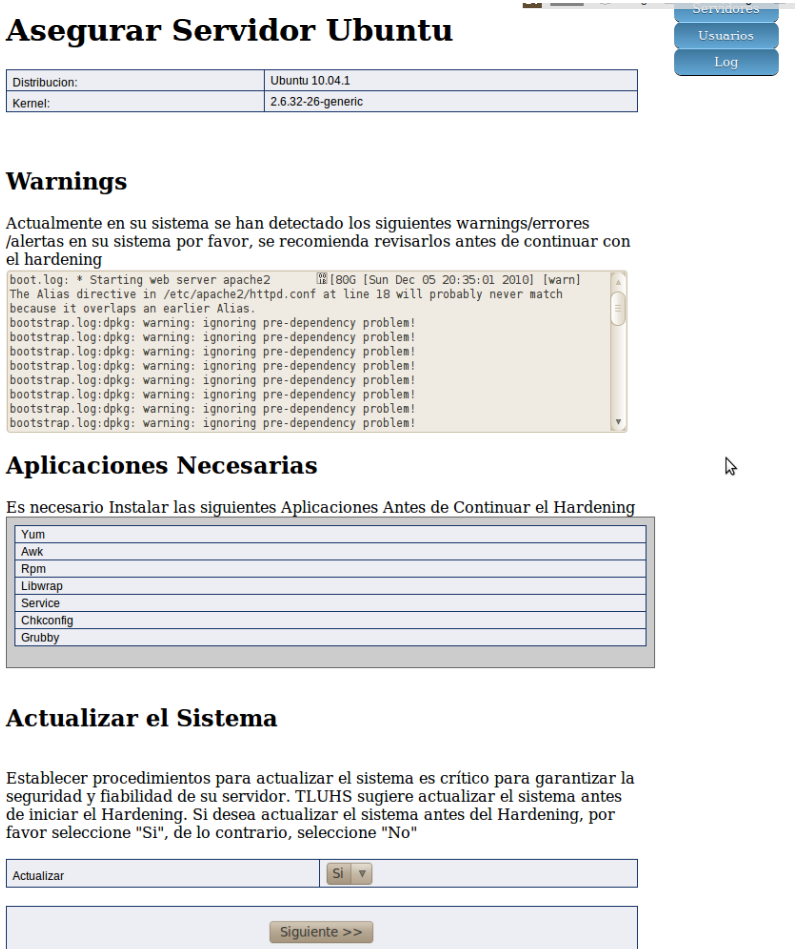
El usuario puede adicionar un servidor para administrar el proceso de Hardening



Una vez adicionado el servidor, el usuario puede consultar sus reportes, asegurarlo o restaurar un backup

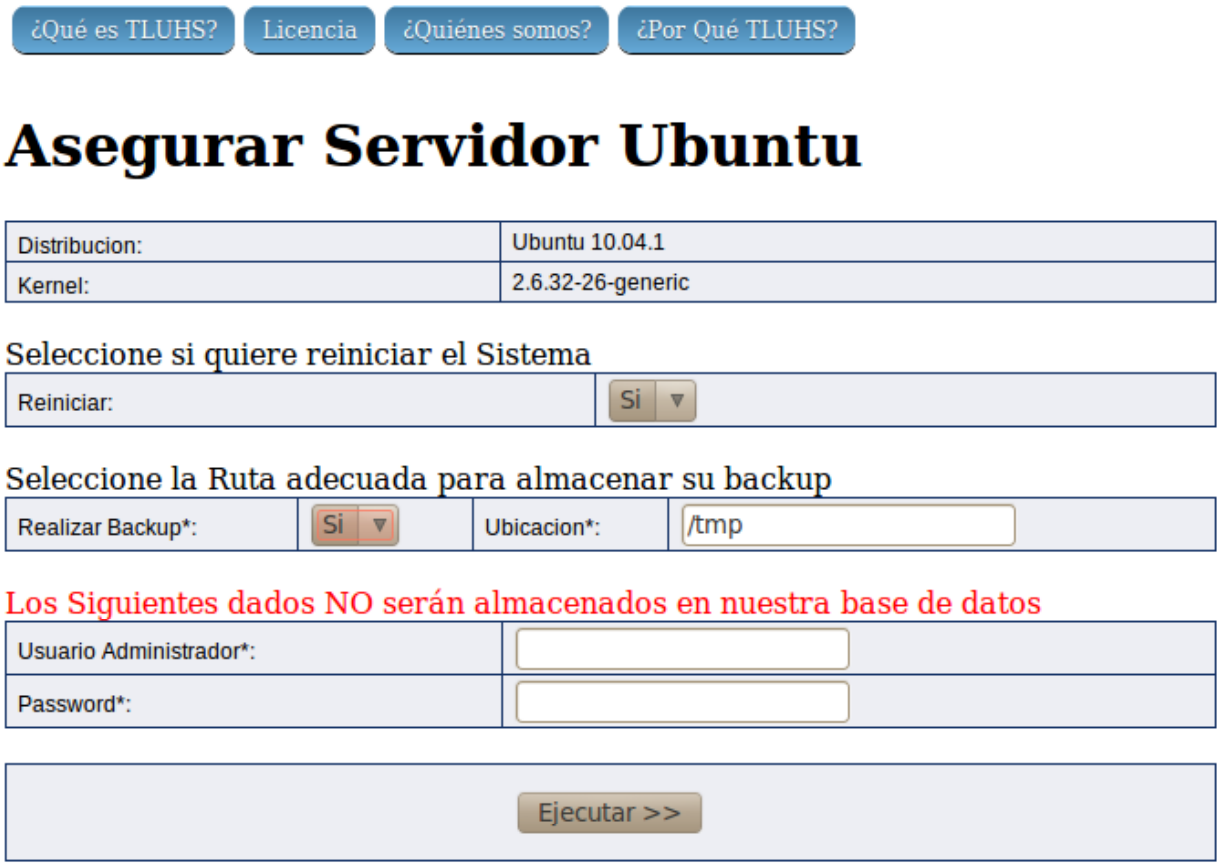


Antes de asegurar el servidor, el usuario debe solucionar problemas, instalar aplicaciones y actualizar el SO

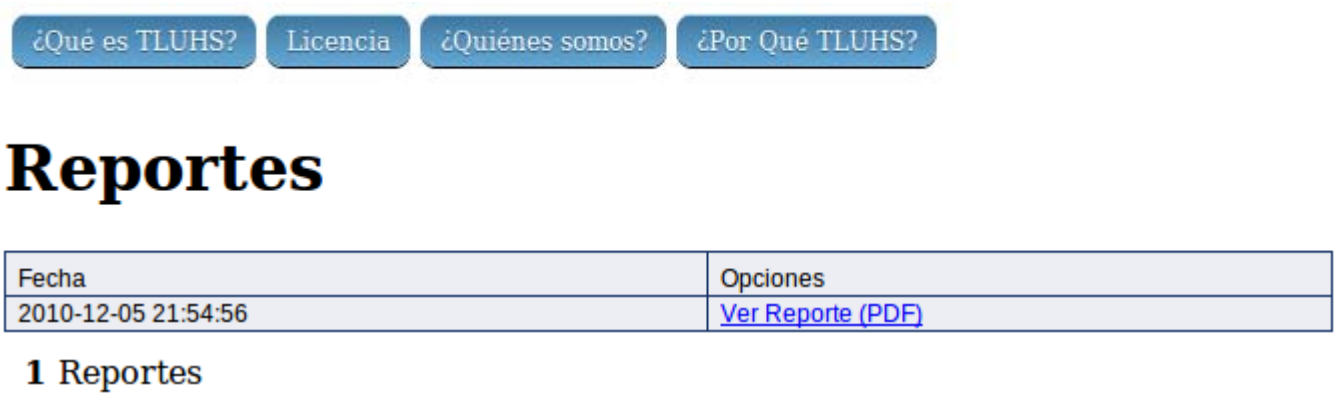


El usuario selecciona las políticas que desea aplicar y configura sus parámetros

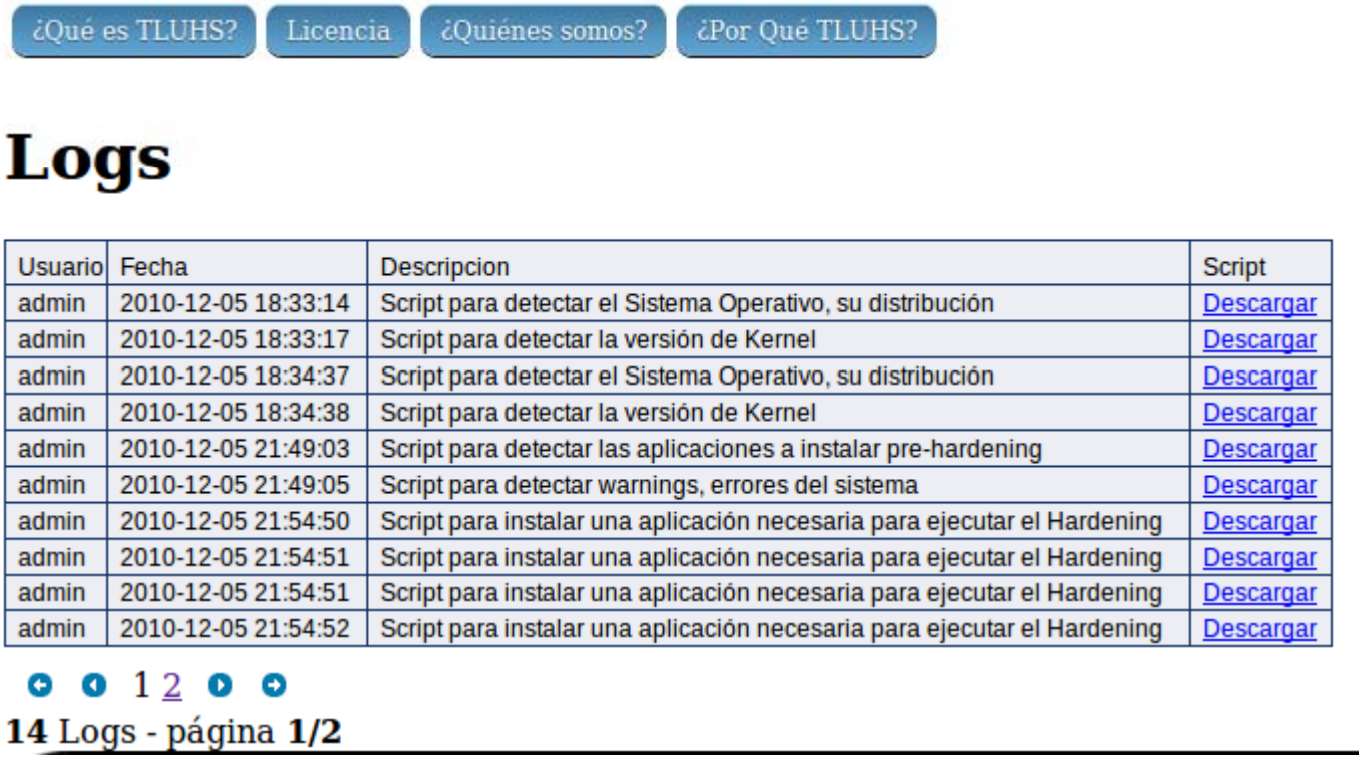
Al finalizar el proceso de Hardening, el usuario puede decidir reiniciar el sistema o generar un backup



El usuario puede consultar los reportes de un servidor



El usuario puede consultar el log de acciones ejecutadas para un servidor



Referencias

1. Seguridad informática. [En línea] http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n [Consultado el 17 de febrero de 2010]
2. Bastille [en línea] http://www.bastille-unix.org/ [Consultado el 17 de febrero de 2010]
3. [3] Seguridad con Bastille. [En línea] http://beta.redeslinux.com/manuales/seguridad/bastille.pdf [Consultado el 17 de febrero de 2010]