

The LinUx Hardening System

Hernán Cortés
Daisy González
Jorge Montes

ACIS X | Jornada de Seguridad Informática

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

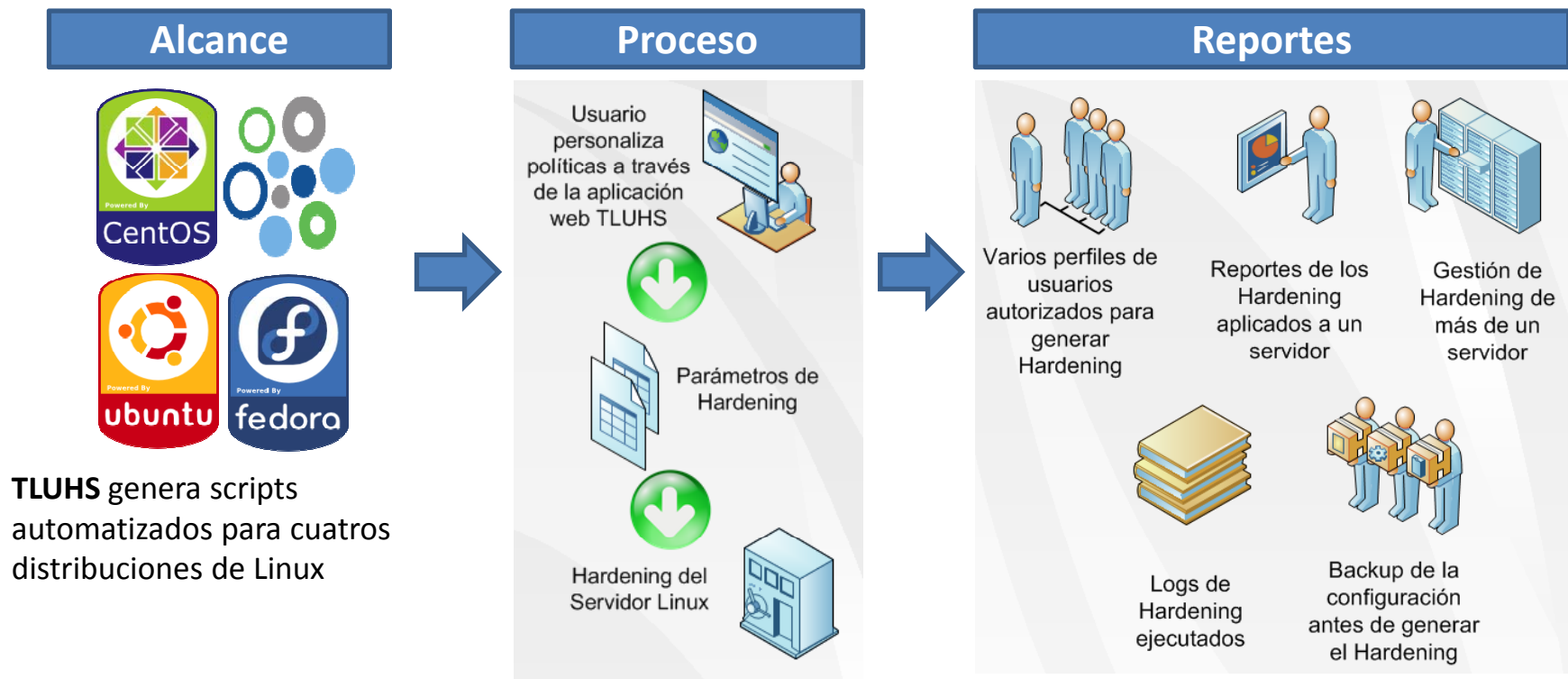


Objetivos

- 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**

ACIS XI Jornada de Seguridad Informática

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



ACIS XI Jornada de Seguridad Informática

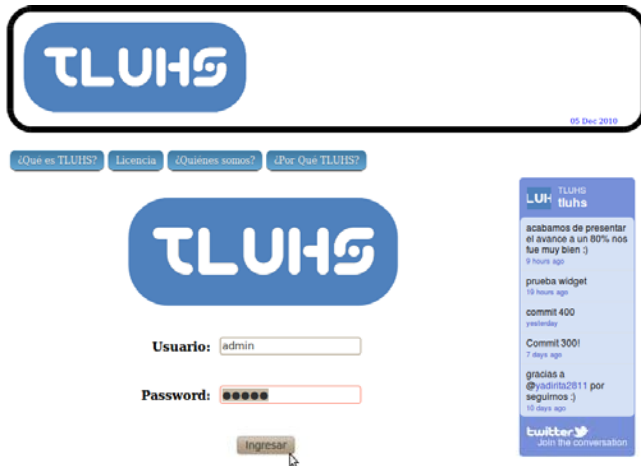
TLUHS es diferente a cualquier aplicación de Hardening existente

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

ACIS XI Jornada de Seguridad Informática

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



[¿Qué es TLUHS?](#) [Licencia](#) [¿Quiénes somos?](#) [¿Por Qué TLUHS?](#)

[Servidores](#)
[Usuarios](#)
[Log](#)

Servidores

Adicionar servidor

Para adicionar o editar un servidor debe tener instalado un servidor SSH [?](#)

Nombre*:	<input type="text" value="CentOs"/>
Dirección IP*:	<input type="text" value="192.168.1.105"/>
Descripción*:	<input type="text" value="Servidor de Correo Empresarial"/>
Activo*:	<input checked="" type="checkbox"/>

Credenciales

Los Sigüientes dados NO serán almacenados en nuestra base de datos

Usuario Administrador*:	<input type="text" value="root"/>
Password*:	<input type="password" value="[redacted]"/>

ACIS XI Jornada de Seguridad Informática

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

Logout 05 Dec 2010

¿Qué es TLUHS? Licencia ¿Quiénes somos? ¿Por Qué TLUHS?

Servidores

Servidores
Usuarios
Log

Nombre	Ip	Descripción	Distribucion	Kernel	Opciones
Ubuntu	127.0.0.1	Ubuntu Ambiente	Ubuntu 10.04.1	2.6.32-26-generic	Asegurar Reportes Restaurar

1 Servidores [Adicionar](#)

Hernán Cortés, Daisy González, Jorge Montes Director: Roger Ortiz
Escuela Colombiana de Ingeniería Julio Garavito - Bogotá, Colombia
Decanatura de Ingeniería de Sistemas

ACIS XI Jornada de Seguridad Informática

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

Asegurar Servidor Ubuntu

Distribucion:	Ubuntu 10.04.1
Kernel:	2.6.32-26-generic

- Servidores
- Usuarios
- Log

Warnings

Actualmente en su sistema se han detectado los siguientes warnings/errores /alertas en su sistema por favor, se recomienda revisarlos antes de continuar con el hardening

```
boot.log: * Starting web server apache2 [80G [Sun Dec 05 20:35:01 2010] [warn]
The Alias directive in /etc/apache2/httpd.conf at line 18 will probably never match
because it overlaps an earlier Alias.
bootstrap.log:dpkg: warning: ignoring pre-dependency problem!
bootstrap.log:dpkg: warning: ignoring pre-dependency problem!
bootstrap.log:dpkg: warning: ignoring pre-dependency problem!
bootstrap.log:dpkg: warning: ignoring pre-dependency problem!
bootstrap.log:dpkg: warning: ignoring pre-dependency problem!
bootstrap.log:dpkg: warning: ignoring pre-dependency problem!
bootstrap.log:dpkg: warning: ignoring pre-dependency problem!
bootstrap.log:dpkg: warning: ignoring pre-dependency problem!
```

Aplicaciones Necesarias

Es necesario Instalar las siguientes Aplicaciones Antes de Continuar el Hardening

Yum
Awk
Rpm
Libwrap
Service
Chkconfig
Grubby

Actualizar el Sistema

Establecer procedimientos para actualizar el sistema es crítico para garantizar la seguridad y fiabilidad de su servidor. TLUHS sugiere actualizar el sistema antes de iniciar el Hardening. Si desea actualizar el sistema antes del Hardening, por favor seleccione "Si", de lo contrario, seleccione "No"

Actualizar	Si
Siguiete >>	

ACIS X | Jornada de Seguridad Informática

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

Permisos de logs

El objetivo de mantener uno o varios logs del sistema es poder identificar responsables de configuraciones ejecutadas y descubrir el origen de ataques. Esta política de seguridad presenta los permisos sugeridos para varios archivos de log del sistema (e.g. log de boot, log de cron, log de httpd, log de kernel, log de mail, entre otros). A continuación, puede seleccionar las políticas que desea aplicar:

¿Configurar?	Archivo	Usuario			Permiso		
		Usuario	Grupo	Otro	Lectura	Ejecución	Escritura
<input type="checkbox"/>	Boot.log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	box*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	cron*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	dmesg1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Dmesg1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	gdm*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	httpd*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	httpd/*1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Httpd/*1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	kernel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	ksyms*1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ksyms*1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	maillog*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

ACIS X | Jornada de Seguridad Informática

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

¿Qué es TLUHS?

Licencia

¿Quiénes somos?

¿Por Qué TLUHS?

Asegurar Servidor Ubuntu

Distribucion:	Ubuntu 10.04.1
Kernel:	2.6.32-26-generic

Seleccione si quiere reiniciar el Sistema

Reiniciar:	<input type="button" value="Si"/>
------------	-----------------------------------

Seleccione la Ruta adecuada para almacenar su backup

Realizar Backup*:	<input type="button" value="Si"/>	Ubicacion*:	<input type="text" value="/tmp"/>
-------------------	-----------------------------------	-------------	-----------------------------------

Los Siguientes datos NO serán almacenados en nuestra base de datos

Usuario Administrador*:	<input type="text"/>
Password*:	<input type="text"/>

ACIS XI Jornada de Seguridad Informática

El usuario puede consultar los reportes de un servidor

¿Qué es TLUHS?

Licencia

¿Quiénes somos?

¿Por Qué TLUHS?

Reportes

Fecha	Opciones
2010-12-05 21:54:56	Ver Reporte (PDF)

1 Reportes

ACIS X | Jornada de Seguridad Informática

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

[¿Qué es TLUHS?](#)

[Licencia](#)

[¿Quiénes somos?](#)

[¿Por Qué TLUHS?](#)

Logs

Usuario	Fecha	Descripcion	Script
admin	2010-12-05 18:33:14	Script para detectar el Sistema Operativo, su distribución	Descargar
admin	2010-12-05 18:33:17	Script para detectar la versión de Kernel	Descargar
admin	2010-12-05 18:34:37	Script para detectar el Sistema Operativo, su distribución	Descargar
admin	2010-12-05 18:34:38	Script para detectar la versión de Kernel	Descargar
admin	2010-12-05 21:49:03	Script para detectar las aplicaciones a instalar pre-hardening	Descargar
admin	2010-12-05 21:49:05	Script para detectar warnings, errores del sistema	Descargar
admin	2010-12-05 21:54:50	Script para instalar una aplicación necesaria para ejecutar el Hardening	Descargar
admin	2010-12-05 21:54:51	Script para instalar una aplicación necesaria para ejecutar el Hardening	Descargar
admin	2010-12-05 21:54:51	Script para instalar una aplicación necesaria para ejecutar el Hardening	Descargar
admin	2010-12-05 21:54:52	Script para instalar una aplicación necesaria para ejecutar el Hardening	Descargar

◀ ◁ 1 2 ▶ ▷

14 Logs - página 1/2

ACIS X | Jornada de Seguridad Informática

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]