Universidad de Valladolid

E.U. DE INFORMÁTICA (SEGOVIA)

Grado en Ingeniería Informática de Servicios y Aplicaciones

Hardening Linux (Guia de Securización)

Autora: *Laura Montalbán Sánchez*
Tutor: *Juan Jose Álvarez*

Versiones del Documento e Historial de Cambios

Versión	Fecha	Razón de Cambio
1.0	10.11.2022	Primera versión del documento
1.1	21.12.2022	Mejoras en el formato del documento
1.2	23.01.2023	Versión formal
2.0	17.02.2023	Correcciones y añadidos
2.1	10.03.2023	Mejoras futuras
3.0	27.03.2023	Versión final

Convenciones Usadas

Esta guía utiliza varias convenciones para resaltar ciertas palabras y frases y llamar la atención sobre información específica.

- ## Convenciones de Nomenclatura

Esta guía utiliza varias convenciones para resaltar ciertas palabras y frases y llamar la atención sobre información específica.

Este documento utiliza las siguientes convenciones de nomenclatura para las rutas de archivo comunes.

Nombre	Valor	Descripción
AAA	AAA	Authentication, Authorisation and Accounting
IDM	IDM	Identity Manager. Centraliza la gestión de todas las identidades de todos los repositorios de todos los centros de control de NATS
PAM	PAM	Pluggable Authentication Modules. Se utiliza en sistemas Linux para autenticarse a través de LDAP
LDAP	LDAP	Lightweight Directory Access Protocol
AD	AD	Microsoft Active Directory
XML	XML	eXtensible Markup Language
NTP	NTP	Network Time Protocol
DNS	DNS	Domain Name System
OU	OU	Organizational Unit
GID	GID	Group IDentifier
UID	UID	User IDentifier
TLS	TLS	Transport Layer Security
DC	DC	Windows Domain Controller
RL	RL	Remote Loader
QoS	QoS	Quality of Service
SSL	SSL	Secure Sockets Layer

- ## Convenciones Tipográficas

Convención	Significado
Calibri	Se utiliza para bloques de código, comandos y ejemplos de secuencias de comandos. El texto debe interpretarse exactamente como se presenta.
<italic font in brackets>	Los textos en cursiva entre paréntesis angulares indican una variable que requiere sustitución por un valor real.
Italic font	Se utiliza para denotar el título de un libro, artículo u otra publicación.

Convención	Significado
Nota	Información adicional o advertencias. Las notas son consejos, atajos o enfoques alternativos para la tarea en cuestión. Ignorar una nota no debería tener consecuencias negativas, pero es posible que te pierdas un truco que te hace la vida más fácil.
Importante	Los cuadros importantes detallan cosas que se pasan por alto fácilmente: cambios de configuración que solo se aplican a la sesión actual o servicios que deben reiniciarse antes de que se aplique una actualización. Ignorar una casilla etiquetada como "Importante" no provocará la pérdida de datos, pero puede causar irritación y frustración.

Tabla de Contenidos

CAPÍTULO 1. INTRODUCCIÓN

Este proyecto ha sido desarrollado para el cliente NATS; empresa británica encargada del control de tráfico aéreo, por la empresa Indra, en concreto por un equipo de Ciber Defensa de Digital Labs.

Conviene recalcar que este documento no contiene datos confidenciales.

A continuación se presenta un resumen de contrato.

NATS ha contratado con su socio estratégico Indra el suministro de la última generación de iTEC (interoperability Through European Collaboration – interoperabilidad Mediante la Colaboración Europea), la tecnología necesaria para modernizar los sistemas de gestión del tráfico aéreo. Este contrato esencial forma parte integral del plan de inversiones de NATS a lo largo de los próximos 10 años y permitirá la transformación de las operaciones de control de tráfico aéreo de la empresa para apoyar el Cielo Único Europeo.

El contrato se ha diseñado para fomentar y permitir la estrecha colaboración entre NATS e Indra. También exigirá la colaboración con otros proveedores importantes de NATS para el desarrollo y la integración de la próxima versión del Procesador de Datos de Vuelo (FDP) y la Posición de Trabajo de Controlador Aéreo (CWP), establecida dentro de la colaboración con iTEC. Asimismo, contempla el apoyo de Indra para poner iTEC en pleno servicio operativo en los centros de control de Prestwick y Swanwick. Este nuevo paso se sustenta sobre la exitosa entrega y transición realizada previamente al sistema iTEC del Centro de Control del Espacio Aéreo Superior de Prestwick, por el que Indra recibió el año pasado el premio al Proveedor del Año de NATS.

Rob Watkins, director de servicios técnicos de NATS, afirmó: "iTEC ofrece la tecnología más avanzada para el control del tráfico aéreo y es esencial para nuestro programa de transformación que nos permitirá modernizar nuestras capacidades. Una vez instalados, los nuevos sistemas reducirán la carga de trabajo de los controladores, aumentarán la eficiencia de los vuelos y permitirán aumentar la capacidad general de tráfico en el espacio aéreo del Reino Unido. iTEC es la clave para el futuro éxito de algunos de los espacios aéreos más saturados del mundo y estamos encantados de trabajar con Indra para incorporar la última generación de iTEC a nuestras operaciones".

Tim Bullock, director de la Cadena de Suministro de NATS, dijo: "Estoy encantado de que hayamos concedido este importante contrato a Indra. Esto representa otro hito clave en nuestra relación estratégica y la continuación del largo historial de trabajo conjunto de NATS e Indra en el desarrollo y entrega de sistemas críticos para respaldar la prestación de servicios a nuestros clientes".

Este es el primer contrato que NATS concede a Indra dentro del Acuerdo Marco de 10 años que se estableció en mayo de 2017. Este acuerdo conforma y rige la relación comercial de NATS con Indra hasta 2027 y durante este periodo se llevará a cabo la entrega de algunos de los sistemas críticos de NATS.

Rafael Gallego, director general de Indra, Programas Europeos de ATM, afirmó: "Estamos extremadamente satisfechos de firmar este contrato y suministrar el sistema iTEC que respaldará a NATS y a la gestión del espacio aéreo británico en el futuro. Culminamos un viaje que iniciamos hace más de quince años en colaboración con los socios de la Alianza iTEC. Con este proyecto, reafirmamos nuestro compromiso con los objetivos estratégicos de NATS y del Cielo Único Europeo."

iTEC

iTEC (interoperability Through European Collaboration – interoperabilidad Mediante la Colaboración Europea) es la tecnología de sistemas de gestión del tráfico aéreo que reúne a los proveedores de servicios de navegación aérea de España, Alemania, Reino Unido, Países Bajos, Noruega, Polonia y Lituania con el proveedor de sistemas Indra. Esta tecnología reforzará la seguridad, aumentará la eficiencia y mejorará el impacto ambiental de los vuelos. Mejorará la interoperabilidad entre los centros de control en Europa y también hará posible que las aeronaves optimicen sus rutas.

Acerca de NATS

NATS es una importante empresa de gestión del tráfico aéreo y soluciones, creada en el Reino Unido en 1962 y que ahora opera en países de todo el mundo.

NATS gestionó 2,4 millones de vuelos en 2016, abarcando el Reino Unido y el Atlántico Norte oriental desde sus centros de Swanwick, Hampshire y Prestwick, Ayrshire. NATS también presta servicios de tráfico aéreo a 14 aeropuertos británicos; en el aeropuerto de Gibraltar y, en una empresa conjunta con Ferrovial, a diversas torres de control de aeropuertos de España.

Sobre la base de su reputación en cuanto a excelencia operativa e innovación, NATS también ofrece soluciones de aeródromos, datos, ingeniería, capacidad, eficiencia y rendimiento medioambiental a clientes de todo el mundo, incluyendo aeropuertos, aerolíneas, proveedores de servicios de tráfico aéreo y Gobiernos.

Acerca de Indra

Indra es una de las principales empresas globales de consultoría y tecnología y el socio tecnológico para las operaciones clave de los negocios de sus clientes en todo el mundo. Dispone de una oferta integral de soluciones propias y servicios avanzados y de alto valor añadido en tecnología, que combina con una cultura única de fiabilidad, flexibilidad y adaptación a las necesidades de sus clientes. Indra es líder mundial en el desarrollo de soluciones tecnológicas integrales en campos como Defensa y Seguridad; Transporte y Tráfico; Energía e Industria; Telecomunicaciones y Media; Servicios financieros; y Administraciones públicas y Sanidad. A través de su unidad Minsait, Indra da respuesta a los retos que plantea la transformación digital. En el ejercicio 2016 tuvo ingresos de 2.709 millones de euros, 34.000 empleados, presencia local en 46 países y operaciones comerciales en más de 140 países.

1.1. Estructura del Documento

El contenido de este documento es el siguiente:

CAPÍTULO 1, Introducción y estructura del documento.

CAPÍTULO 2, Motivación

CAPÍTULO 3, Objetivos

CAPÍTULO 4, Metodología y Planificación

CAPÍTULO 5, Estudio Presupuestario

CAPÍTULO 6, Tecnologías y Herramientas Implicadas

CAPÍTULO 7, Configuración de Seguridad de RHEL8

CAPÍTULO 8, Scap y Ansible

CAPÍTULO 9, Pruebas de ejecución

CAPÍTULO 10, Conclusiones

CAPÍTULO 11, Bibliografía

CAPÍTULO 2. MOTIVACIÓN

El propósito de este documento es proporcionar una guía para el fortalecimiento del SO Red Hat Enterprise Linux (RHEL), más específicamente, en su versión 8.6 con una arquitectura x64. Además, aprovechando las versiones anteriores de este mismo documento, basado en la guía de la NSA, el objetivo es actualizar las guías anteriores para el fortalecimiento del sistema operativo para toda la entidad.

Para esta actualización, se tienen en cuenta las guías públicas de securización de RHEL del propio proveedor y otro material, como definiciones de *OpenSCAP*.

Su objetivo es proporcionar detalles sobre los diferentes pasos que se deben completar para asegurar la organización de manera integral, pero al mismo tiempo independiente de una instalación en particular.

La guía está dirigida a los administradores de sistemas. Todas las instrucciones deben seguirse completamente y con comprensión de sus efectos para evitar efectos adversos graves en el sistema y su seguridad.

CAPÍTULO 3. OBJETIVOS

El objetivo de este proyecto es proporcionar una auditoria de cumplimiento de configuración automatizada.

Una auditoría de cumplimiento es un proceso para determinar si un objeto dado sigue todas las reglas especificadas en una política de cumplimiento. La política de cumplimiento la definen los profesionales de la seguridad que especifican las configuraciones necesarias, a menudo en forma de lista de comprobación, que debe utilizar un entorno informático.

Las políticas de cumplimiento pueden variar sustancialmente entre organizaciones e incluso entre diferentes sistemas dentro de la misma organización. Las diferencias entre estas políticas se basan en el propósito de cada sistema y su importancia para la organización. Las configuraciones de software personalizadas y las características de despliegue también plantean la necesidad de contar con listas de comprobación de políticas personalizadas.

El proceso de automatización se realizará mediante la herramienta *OpenSCAP*, desarrollando *playbooks* con *Ansible* que cumplan con las políticas de configuración establecidas por la organización. Gracias a estos scripts, los administradores del sistema con sólo ejecutar un fichero en *bash* actualizarán la configuración de seguridad del sistema.

CAPÍTULO 4. METODOLOGÍA Y PLANIFICACIÓN

En este capítulo se detallará la metodología empleada en el desarrollo de las actividades del proyecto, así como la planificación para la consecución de los objetivos del mismo.

4.1. Metodología

Para llevar a cabo el hardening del sistema y su automatización se ha elegido la **Metodología agile de Scrum**. La característica principal de esta metodología es la rapidez y la flexibilidad.

El trabajo se ha divido en pequeños bloques con iteraciones cada semana, obteniendo feedback del avance por parte del cliente, aumentando así la probabilidad de éxito y reduciendo la necesidad de grandes cambios en el proyecto.

Scrum se basa en: la transparencia (el progreso del trabajo es visible para todos los implicados), la inspección (se compara el progreso con los objetivos) y la adaptación (se debe adaptar las desviaciones lo antes posible).

Scrum está formado por tres artefactos y cinco eventos.

EQUIPO SCRUM

El *scrum team* normalmente está formado por entre 5 y 11 personas.

- **Desarrolladores**: se ocupan del desarrollo del producto. Desarrollan un plan de trabajo para cumplir con los objetivos de cada *sprint*.
- **Product Owner**: el propietario del producto. Es el responsable de maximizar el valor del producto. También se ocupa de que el trabajo sea transparente, visible y comprendido, y de organizar y gestionar el *Product Backlog*.
- **Scrum Master**: es el líder del equipo de trabajo. Se encarga de eliminar los problemas que puedan surgir durante el desarrollo, de asegurarse de que se lleven a cabo todos los eventos de *scrum*, de capacitar al resto de los miembros de autogestión y multifuncionalidad, etc.

EVENTOS SCRUM

El desarrollo del proyecto se divide en eventos temporales denominados *sprints*. Un *sprint* es un marco temporal de longitud fija y de duración máxima un mes, cuya finalidad es entregar un incremento de producto funcional tras su finalización. Todos los *sprints* deben tener la misma duración, un objetivo a alcanzar, y las herramientas necesarias para lograrlo.

En cada *sprint* se realizan los siguientes eventos:

- **Sprint Planning**: es una reunión que tiene lugar al comienzo del *sprint* y cuyo objetivo es planificar el desarrollo del *sprint*. Participa todo el *scrum team*. Tiene de duración máxima 8 horas.

- **Daily Scrum**: es reunión que se realiza diariamente y que tiene como objetivo planificar el trabajo de las siguientes 24 horas y hacer una retrospectiva del día anterior. Participa todo el *scrum team*. Tiene de duración máxima 15 minutos.
- **Sprint Review**: es una reunión que se celebra tras finalizar el *sprint*. En esta reunión el *scrum team* revisa con los *stakeholders* el resultado del *sprint* y se analiza el progreso hacia el objetivo del producto. Tiene de duración máxima 4 horas.
- **Sprint Retrospective**: tiene de duración máxima 8 horas realizada después del *sprint review*. En ella el *scrum team* analiza cómo se desarrolló el último *sprint* y cómo se podría aumentar la calidad y la eficacia del trabajo realizado.

ARTEFACTOS SCRUM

Nos permiten organizar y gestionar el trabajo realizado en cada sprint, y las tareas necesarias para alcanzar el producto final.

- **Product Backlog**: es una lista priorizada que contiene las funcionalidades, los requisitos y las mejoras que se deben realizar en el producto. Es creada por el *product owner* y mantenida de acuerdo a la visión de negocio y las necesidades del cliente.
- **Sprint Backlog**: es una lista de elementos seleccionados del *product backlog* para un *sprint.* Es gestionada por el equipo de desarrolladores. Constituye la imagen visible del avance y su consecución implica que se han cumplido los objetivos fijados en dicho *sprint*.
- **Incremento**: suma de todas las tareas pertenecientes al *product backlog* que han sido completadas (durante un *sprint* y todos los anteriores).

4.2. Planificación

El desarrollo del proyecto ha durado **6 meses**, lo que equivale a **6 *sprints*.**

Suponemos que un mes se corresponde con **26 días laborales**.

Seis meses de desarrollo hace un total de **156 días**, esta es la cantidad de días laborales que ha tardado en desarrollarse este proyecto.

Suponemos que este proyecto ha sido desarrollado por un equipo de **5 personas** con diferentes roles. La suma de las horas trabajadas en el proyecto por el equipo completo es **3276 horas totales.**

NOTA: en el punto 5.2 Recursos Humanos se detalla la cantidad de horas trabajadas por cada miembro del equipo en el proyecto.

Cada ***sprint*** ha supuesto un total de **546 horas.**

Tabla 4.2-1: Planificación

Total Sprints/ Meses	Total días de desarrollo	Total nº de miembros en el equipo	Total horas de desarrollo	Total horas por sprint
6	156	5	3276	546

Para las tareas generales se realizará una estimación de la dificultad de realización de cada una de ellas. Se evaluarán asignando una puntuación comprendida entre el 1 y el 10, siendo 1 la mínima y 10 la máxima. Con ello obtenemos el coste del esfuerzo de cada *sprint*.

Tabla 4.2-2: Estimación del Esfuerzo

Nº de Sprint	Tareas	Coste del Esfuerzo de cada Tarea	Total del Esfuerzo de cada Sprint
1	1.1. Cálculo del presupuesto necesario.	5	21
	1.2. Estudio de la metodología a seguir.	7	
	1.3. Planificación de las diferentes tareas a realizar.	6	
	1.4. Reparto de las tareas entre los diferentes roles del equipo.	3	
2	2.1. Lectura de todos los documentos de hardening del sistema.	4	17
	2.2. Unificación de todos los documentos en uno general.	4	

	2.3. Lectura de guías oficiales de RHEL8.	6	
	2.4. Selección de guía a seguir.	3	
3	3.1. Actualización del documento de hardening a la versión de RHEL8.	4	14
	3.2. Adición de mejoras.	5	
	3.3. Corrección de errores.	5	
4	4.1. Lectura guías de OpenScap.	6	15
	4.2. Creación de instancia de rocky en OpenStack e instalación de OpenScap.	3	
	4.2. Pruebas e investigación de OpenScap.	6	
5	5.1. Lectura e investigación de ansible.	6	14
	5.2. Investigación para creación de playbooks personalizados con OpenScap.	8	
6	6.1. Creación de checks.	7	29

	6.2. Creación de fixes.	8	
	6.3. Integración de todos los scripts.	7	
	6.4. Pruebas.	7	

CAPÍTULO 5. ESTUDIO PRESUPUESTARIO

A continuación, se presenta una estimación del coste total de realización de este proyecto.

Esta estimación tiene en cuenta los recursos hardware, software, humanos y otro tipo de costes como la electricidad e internet.

Para la estimación del coste de los recursos hardware y software se tendrá en cuenta el Coste de Amortización por año según la siguiente fórmula.

$$CA = \frac{\text{Coste total del producto (€)}}{\text{Duración del producto (años)}}$$

El resultado será dividido entre dos para conocer la amortización del producto que se corresponde a medio año. El Coste de Amortización del producto en el proyecto lo determina la siguiente fórmula.

$$CA \text{ en proyecto} = \frac{\text{CA}}{2}$$

5.1. Recursos Hardware

Tabla 5.1-1: Estimación Coste Recursos Hardware

HP EliteBook 640 G9 Notebook PC	
Componente	**Especificación**
Procesador	12th Gen Intel(R) Core(TM) i7-1265U 1.80 GHz
Memoria RAM	16 GB de RAM DDR4
Tarjeta gráfica	Intel Iris Xe Graphics
Disco Duro	512 GB SSD M.2 NVMe PCIe
Dimensiones	322 x 214 x 19.9 mm
Precio	**1284.74 €**

Además del precio de los componentes, debemos tener en cuenta el tiempo de vida del ordenador que se va a usar en el desarrollo del software.

Suponiendo un tiempo de vida de 5 años para este ordenador, de los cuales medio año será empleado en el desarrollo de este software, es decir un 10% del coste total del producto

hardware será destinado al desarrollo de este software. El Coste de Amortización en el proyecto es **128.474 €**.

5.2. Recursos Software

Para la estimación del coste del software se tendrán en cuenta las herramientas y los sistemas operativos utilizados.

Tabla 5.2-1: Estimación Coste Recursos Software

Componente	Especificación	Tiempo de Vida/ Coste Total	Coste de Amortización en el Proyecto
Sistema Operativo	Windows 11 Pro (22H2)	4 años/ 26 €	3.25 €
Software Office	Microsoft Office ProPlus	10 años/ 579 €	28.95 €
Infraestructura Cloud	OpenStack	10 años/ 1000 €	50 €
VPN	FortiClient	10 años/ 500 €	25 €
Máquina Virtual	VMware	3 años/ 50 €	8.333 €
Imágen de SO	Rocky	0 €	0 €
Coste de Amortización Total			**115.533 €**

5.3. Recursos Humanos

Por último, debemos tener en cuenta el coste del personal. Para ello, tendremos en cuenta diferentes roles.

NOTA 1: recordamos que este proyecto ha sido desarrollado por un equipo de **5 personas** con diferentes roles.

Analistas (2) y Consultor (1) → 8 h/ día → 26 días laborales al mes → 208 h/ mes → 156 días en 6 meses → 1248 horas en 6 meses.

Jefe de proyecto (1) → 4h/ día → 26 días laborales al mes → 104h/mes → 156 días en 6 meses → 624 horas en 6 meses.

Project Manager (1) → 1h/ día → 26 días laborales al mes → 26h/ mes → 156 días en 6 meses → 156 horas en 6 meses.

La suma de las horas trabajadas en el proyecto por el equipo completo es **3276 horas totales.**

Tabla 5.3-1: Estimación Coste Recursos Humanos

Rol	Coste Mensual	Horas totales en el proyecto	Coste Final
Jefe de Proyecto	2500 €/ mes → 12.019 €/ hora	624 horas	(1 rol) 7499.856 €
Analista de seguridad	1500 €/ mes → 7.211 €/ hora	1248 horas	(2 roles) 18000 €
Consultor de seguridad	1800 €/ mes → 8.653 €/ hora	1248 horas	(1 rol) 10800 €
Project Manager	3300 €/ mes → 15.86 €/ hora	156 horas	(1 rol) 2472.60 €
Coste Total			**56772.456 €**

NOTA: la tabla 5.3-1 muestra los sueldos brutos que reciben los trabajadores. El empleador paga una serie de impuestos por cada sueldo correspondiente al 30% del sueldo bruto aproximadamente.

5.4. Otros Recursos

En el cálculo de costes, debemos tener en cuenta otro tipo de recursos como; el coste de conexión a Internet y el uso de la electricidad.

El gasto de electricidad del ordenador para la realización del software ha sido de 20 euros mensuales.

En cuanto al gasto de Internet, se tiene contratada una tarifa de 60 euros mensuales asociada a varios servicios.

Tabla 5.4-1: Estimación Costes de Otros Recursos

Recurso	Coste Mensual	Tiempo	Coste
Electricidad	20 €/ mes	6 meses	120 €
Internet	15 €/ mes	6 meses	90 €
Coste Total			**210 €**

5.5. Suma de Costes

Tabla 5.5-1: Suma de Costes

Tipo de Recurso	Coste
Hardware	128.474 €
Software	115.533 €
Humanos	63600 €
Adicionales	210 €
Coste Total	64054.007 €

CAPÍTULO 6. TECNOLOGÍAS Y HERRAMIENTAS IMPLICADAS

En este capítulo se muestran las herramientas y las tecnologías utilizadas en el desarrollo de este producto.

6.1. Herramientas

- **Visual Studio Code**: editor de código fuente desarrollado por Microsoft, siendo uno de los más extendidos del mercado.

- **Microsoft Word**: procesador de textos perteneciente al paquete Office. Utilizado en la realización de la memoria del trabajo.

- **Microsoft Teams**: espacio de trabajo cloud para desarrollar un proyecto en equipo que permite colaborar a los miembros de este mediante diferentes canales de comunicación. Además, permite la edición de archivos de forma colaborativa y la integración con otras aplicaciones.

- **Rocky Linux 8:** es una distribución de Linux, desarrollada por Rocky Enterprise Software Foundation. Está destinada para ser una distribución "downstream", lanzada completamente para ser compatible con código binario usando el código fuente del sistema operativo de Red Hat Enterprise Linux.

```
[rocky@vm-rocky-3 ~]$ cat /etc/os-release
NAME="Rocky Linux"
VERSION="8.7 (Green Obsidian)"
ID="rocky"
ID_LIKE="rhel centos fedora"
VERSION_ID="8.7"
PLATFORM_ID="platform:el8"
PRETTY_NAME="Rocky Linux 8.7 (Green Obsidian)"
ANSI_COLOR="0;32"
LOGO="fedora-logo-icon"
CPE_NAME="cpe:/o:rocky:rocky:8:GA"
HOME_URL="https://rockylinux.org/"
BUG_REPORT_URL="https://bugs.rockylinux.org/"
ROCKY_SUPPORT_PRODUCT="Rocky-Linux-8"
ROCKY_SUPPORT_PRODUCT_VERSION="8.7"
REDHAT_SUPPORT_PRODUCT="Rocky Linux"
REDHAT_SUPPORT_PRODUCT_VERSION="8.7"
```

Figura 6-1: Rocky Linux 8

- **Trello**: software en línea para la gestión y organización de proyectos cuya estructura está basada en un tablero Kanban (herramienta empleada para mapear y visualizar los flujos de trabajo en la metodología ágil Kanban). Permite organizar ideas y tareas en diferentes columnas para lograr una rápida visión del avance de un proyecto.

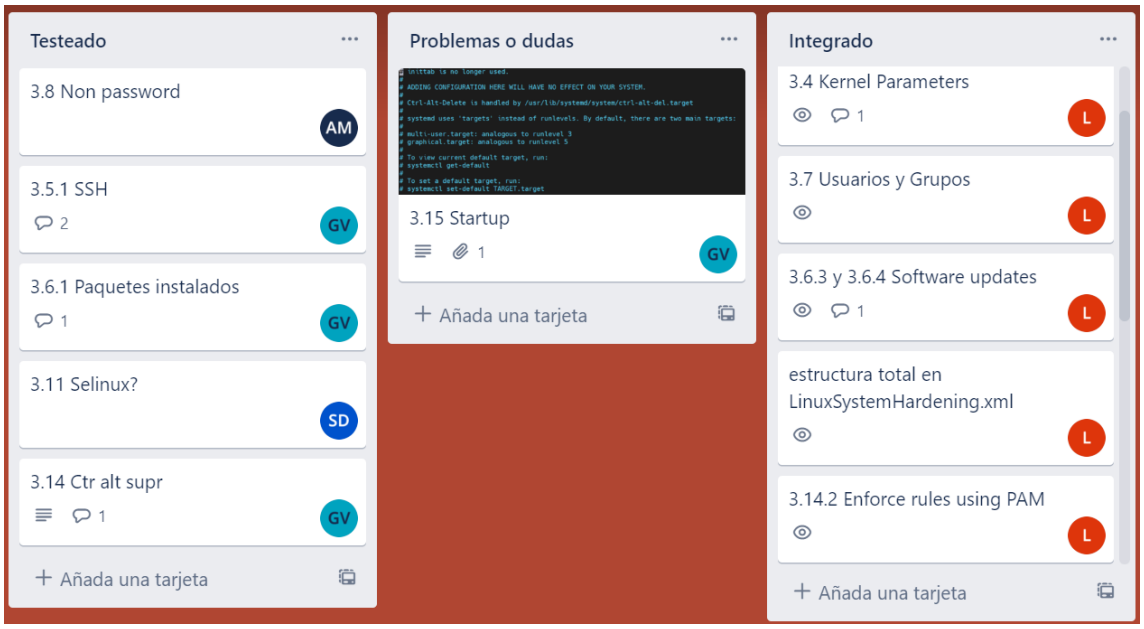


Figura 6-2: Trello

6.2. Tecnologías

- **XML:** el lenguaje de marcado extensible (XML) permite definir y almacenar datos de forma compartible. XML admite el intercambio de información entre sistemas de computación, como sitios web, bases de datos y aplicaciones de terceros.

- **OpenScap**: es un conjunto de herramientas open source para implementación y cumplimiento con el estándar *Security Content Automation Protocol (SCAP)* certificado por NIST (Instituto Nacional de Estándares y Tecnología).

  La biblioteca *OpenSCAP*, con la utilidad de línea de comandos que la acompaña *oscap*, está diseñada para realizar escaneos de configuración y vulnerabilidad en un sistema local, para validar el contenido de cumplimiento de la configuración y para generar informes y guías basadas en estos escaneos.

- **Ansible**: es una plataforma de software libre para configurar y administrar ordenadores. Combina instalación multi-nodo, ejecuciones de tareas ad hoc y administración de configuraciones. Adicionalmente, Ansible es categorizado como una herramienta de orquestación.

  Ansible Automation Platform ofrece un marco empresarial para diseñar y ejecutar la automatización de la TI según sea necesario. Además, permite que los usuarios de toda la empresa creen, compartan y gestionen la automatización, desde los del equipo de desarrollo y de operaciones hasta los del equipo de seguridad y de redes.

NOTA: en el capítulo 8 de este documento se detalla el funcionamiento y la aplicación de estas tecnologías en el presente proyecto.

CAPÍTULO 7. CONFIGURACIÓN DE SEGURIDAD DE RHEL8

Este capítulo contiene información detallada sobre las prácticas aplicadas para securizar un sistema RHEL8.

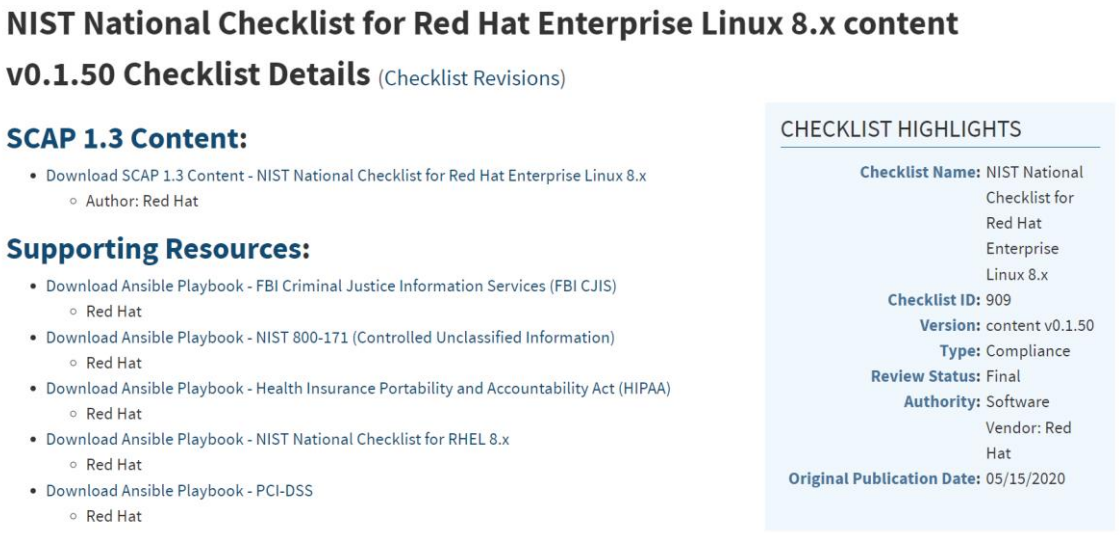
7.1. Principios Generales

El conjunto de tareas realizadas se ha basado en diferentes guías de hardening y buenas prácticas como las mostradas en la siguiente tabla.

Tabla 7.1-1: Referencias

NOMBRE	URL
NSA	https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.html
NIST	https://ncp.nist.gov/checklist/909
Red hat	https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/security_hardening/red_hat_enterprise_linux-8-security_hardening-en-us.pdf

Tenga en cuenta que algunas tareas que se incluyen comúnmente en diferentes guías se configuran de forma predeterminada durante la instalación o implementación de sistemas Linux; esas tareas también se han verificado.



NIST National Checklist for Red Hat Enterprise Linux 8.x content v0.1.50 Checklist Details (Checklist Revisions)

SCAP 1.3 Content:

- Download SCAP 1.3 Content - NIST National Checklist for Red Hat Enterprise Linux 8.x
  - Author: Red Hat

Supporting Resources:

- Download Ansible Playbook - FBI Criminal Justice Information Services (FBI CJIS)
  - Red Hat
- Download Ansible Playbook - NIST 800-171 (Controlled Unclassified Information)
  - Red Hat
- Download Ansible Playbook - Health Insurance Portability and Accountability Act (HIPAA)
  - Red Hat
- Download Ansible Playbook - NIST National Checklist for RHEL 8.x
  - Red Hat
- Download Ansible Playbook - PCI-DSS
  - Red Hat

CHECKLIST HIGHLIGHTS

Checklist Name: NIST National Checklist for Red Hat Enterprise Linux 8.x
Checklist ID: 909
Version: content v0.1.50
Type: Compliance
Review Status: Final
Authority: Software Vendor: Red Hat
Original Publication Date: 05/15/2020

Figura 7-1: NIST National Checklist for Red Hat Enterprise Linux 8.x content

Figura 7-2: RHEL8 Security Hardening

7.2. Parámetros del Kernel

Hay varias modificaciones de configuración de red que permiten aumentar la seguridad del servidor/estación de trabajo.

- Desactivar el reenvío de IP (IP forwarding).
- No permitir el enrutamiento de origen.
- Asegurarse de que el enrutado no está instalado.

NOTA: Al establecer manualmente los siguientes controles, el proceso a seguir es verificar manualmente las configuraciones afectadas descritas en las siguientes secciones, y realizar los cambios solo en caso de que la bandera no venga como se recomienda por defecto.

En las siguientes comprobaciones, se puede usar el comando *sysctl -n key_id* sustituyendo el key_id por el indicador correspondiente. Cada sección describe cómo parchear solo si es necesario.

7.2.1. IPv4

La siguiente table muestra los archivos de configuración y las líneas en estos que serán modificadas en esta sección.

Tabla 7.2-1: Configuraciones IPv4

FILE	LINE	
/etc/sysctl.conf	Habilitar protección de cookies TCP Syn	*net.ipv4.tcp_syncookies = 1*
	Deshabilitar enrutamiento de origen IP	*net.ipv4.conf.all.accept_source_route = 0* *net.ipv4.conf.default.accept_source_route = 0*
	Deshabilitar aceptación de redireccionamiento IP	*net.ipv4.conf.all.accept_redirects = 0* *net.ipv4.conf.all.send_redirects = 0* *net.ipv4.conf.default.accept_redirects = 0* *net.ipv4.conf.default.send_redirects = 0*
	Habilitar la protección contra la falsificación de IP	*net.ipv4.conf.all.rp_filter = 1* *net.ipv4.conf.default.rp_filter = 1*
	Deshabilitar el reenvío de IP	*net.ipv4.ip_forward = 0*
	Habilitar la protección contra mensajes de error erróneos	*net.ipv4.icmp_ignore_bogus_error_responses = 1*
	Protección contra ataques de desbordamiento de buffer	*kernel.kptr_restrict = 1* *kernel.randomize_va_space = 1*
	Registro de actividades sospechosas	*net.ipv4.conf.all.log_martians = 1* *net.ipv4.conf.default.log_martians = 1*
	Paquetes de redirecciones seguras	*net.ipv4.conf.all.secure_redirects = 0* *net.ipv4.conf.default.secure_redirects = 0*
	Ignorar peticiones ‘echo’ de difusión ICMP	*net.ipv4.icmp_echo_ignore_broadcasts = 1*

- **Habilitar la protección de cookies TCP Syn**

Un "ataque SYN" es un ataque de denegación de servicio que consume y degrada la QoS de red de todos los recursos de una máquina. Cualquier servidor conectado a una red está potencialmente sujeto a este ataque.

Este ataque consiste en llenar la tabla de conexiones TCP de un sistema con conexiones en el estado SYN_RCVD. Las cookies de sincronización se pueden usar para rastrear una conexión cuando se recibe un ACK posterior, verificando que el iniciador esté intentando una conexión válida y no sea una fuente de inundación. Esta característica se activa cuando se detecta una condición de inundación y permite que el sistema continúe atendiendo solicitudes de conexión válidas.

Debe asegurarse de que el indicador tcp_syncookies esté configurado a uno, lo que se puede verificar desde un shell con el comando:

```
cat /proc/sys/net/ipv4/tcp_syncookies
or
sysctl -n net.ipv4.tcp_syncookies
```

Que debe devolver un "1". De lo contrario, la siguiente línea debe modificarse en el archivo ***/etc/sysctl.conf*** o ***/etc/sysctl.d*** para evitar este tipo de ataque (permanente). En caso de que este indicador no aparezca en el archivo de configuración, se puede agregar manualmente.

- **Deshabilitar enrutamiento de origen IP**

El enrutamiento de origen se utiliza para especificar una ruta a través de la red desde el origen hasta el destino.

Los paquetes enrutados en el origen permiten que el origen del paquete sugiera que los enrutadores reenvíen el paquete a lo largo de una ruta diferente a la configurada en el enrutador, lo que se puede usar para eludir las medidas de seguridad de la red.

La aceptación de paquetes enrutados en origen en el protocolo IPv4 tiene pocos usos legítimos. Debe deshabilitarse a menos que sea absolutamente necesario, como cuando el reenvío de IPv4 está habilitado y el sistema funciona legítimamente como un enrutador.

Se ha modificado la siguiente línea en el archivo ***/etc/sysctl.conf*** para evitar este tipo de ataques (permanente).

```
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
```

- **Deshabilitar la aceptación de redirección ICMP**

Los enrutadores utilizan los mensajes de redirección ICMP para informar a los hosts que existe una ruta más directa para un destino en particular.

Estos mensajes modifican la tabla de rutas del host y no están autenticados. Un mensaje de redirección ICMP ilícito podría resultar en un ataque de "man in the middle".

Además, estos mensajes contienen información de la tabla de rutas del sistema que posiblemente revela partes de la topología de la red.

La capacidad de enviar redireccionamientos ICMP solo es adecuada para sistemas que actúan como enrutadores.

Actualizar la tabla de enrutamiento del sistema es una forma de permitir un dispositivo de enrutamiento externo. Con esta configuración, el sistema no aceptará ningún mensaje de redirección ICMP y, por lo tanto, no permitirá que personas ajenas actualicen las tablas de enrutamiento del sistema.

Las siguientes líneas se han modificado en el archivo ***/etc/sysctl.conf*** para evitar este tipo de ataque.

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
```

- **Habilitar la protección contra la falsificación de IP**

Habilitar el filtrado de ruta inversa descarta paquetes con direcciones de origen que no deberían haberse recibido en la interfaz en la que se recibieron.

No debe usarse en sistemas que son enrutadores para redes complicadas, pero es útil para hosts finales y enrutadores que prestan servicios a redes pequeñas.

La suplantación de IP es una técnica mediante la cual un intruso envía paquetes que afirman haber sido enviados desde otro host mediante la manipulación de la dirección de origen.

Las siguientes líneas se han modificado en el archivo ***/etc/sysctl.conf*** para evitar este tipo de ataques.

```
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
```

- **Deshabilitar el reenvío de IP**

Los demonios de protocolo de enrutamiento generalmente se usan en enrutadores para intercambiar información de topología de red con otros enrutadores. Si esta capacidad se

usa cuando no se requiere, la información de la red del sistema puede transmitirse innecesariamente a través de la red.

El reenvío de paquetes está deshabilitado en máquinas que no están dedicadas a este propósito.

La siguiente línea se ha modificado en el archivo ***/etc/sysctl.conf***.

```
net.ipv4.ip_forward = 0
```

NOTA: Ciertas tecnologías, como máquinas virtuales, contenedores, etc., se basan en el reenvío de IPv4 para habilitar y usar redes. Deshabilitar el reenvío de IPv4 haría que esas tecnologías dejaran de funcionar. Por lo tanto, esta regla no debe usarse en perfiles o puntos de referencia que tengan como objetivo el uso del reenvío de IPv4.

- **Habilitar la protección contra mensajes de error erróneos**

Esta opción alerta al administrador del sistema de la existencia de mensajes de error en la red, lo que podría indicar una posible intrusión.

Ignorar las respuestas de error ICMP falsas reduce el tamaño del registro, aunque algunas actividades no se registran.

La siguiente línea se ha modificado en el archivo ***/etc/sysctl.conf***.

```
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

- **Exec-shield**

La función Kernel Exec Shield debe estar configurada. Exec Shield brinda protección contra ciertos tipos de ataques de desbordamiento de búfer.

Estas características incluyen la ubicación aleatoria de la pila y otras regiones de la memoria, la prevención de la ejecución en la memoria que solo debe contener datos y el manejo especial de los búferes de texto.

La exposición de los punteros del kernel (a través de procfs o seq_printf()) expone las estructuras del kernel que se pueden escribir y que pueden contener punteros de funciones. Si ocurre una vulnerabilidad de escritura en el kernel que permite el acceso de escritura a cualquiera de esta estructura, el kernel puede verse comprometido. Esta opción impide que cualquier programa sin la capacidad CAP_SYSLOG obtenga las direcciones de los punteros del kernel, reemplazándolos con 0.

Las siguientes líneas se han modificado en el archivo ***/etc/sysctl.conf.***

```
kernel.kptr_restrict = 1
kernel.randomize_va_space = 1
```

- **Registro de actividades sospechosas**

Esta función registra paquetes con direcciones de origen no enrutables en el núcleo. Habilitar esta función y registrar estos paquetes permite que un administrador investigue el caso de un atacante que envía paquetes falsificados a un servidor.

La presencia de paquetes "marcianos" (que tienen direcciones imposibles), así como paquetes falsificados, paquetes enrutados en origen y redireccionamientos, podría ser un signo de actividad de red nefasta. El registro de estos paquetes permite detectar esta actividad.

Las siguientes líneas se han modificado en el archivo ***/etc/sysctl.conf***.

```
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
```

El archivo de registro se encuentra en la siguiente ruta: ***/proc/sys/net/ipv4/conf/all/log_martians***.

- **Paquetes de redirecciones seguras**

A través de las redirecciones ICMP, un host puede averiguar a qué redes se puede acceder desde la red local y cuáles son los enrutadores utilizados para cada una de esas redes. El problema de seguridad proviene del hecho de que los paquetes ICMP, incluida la redirección ICMP, son extremadamente fáciles de falsificar y, básicamente, sería bastante fácil para un atacante falsificar paquetes de redirección ICMP.

Aceptar redirecciones ICMP "seguras" (desde las puertas de enlace enumeradas como puertas de enlace predeterminadas) tiene pocos usos legítimos. Debe desactivarse a menos que sea absolutamente necesario.

Las siguientes líneas se han modificado en el archivo ***/etc/sysctl.conf***.

```
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
```

- **Ignorar peticiones echo de difusión ICMP**

La respuesta a los *echos* de difusión (ICMP) facilita el mapeo de la red y proporciona un vector para los ataques de amplificación.

Ignorar las solicitudes de echo ICMP (pings) enviados a direcciones de difusión o multidifusión hace que el sistema sea un poco más difícil de enumerar en la red.

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

7.2.2. IPv6

La siguiente table muestra las configuraciones que se tratarán en esta sección.

Tabla 7.2-2: Configuraciones IPv6

FILE	LINE	
/etc/sysctl.conf	Deshabilitar enrutamiento de origen IP	*net.ipv6.conf.all.accept_source_route = 0* *net.ipv6.conf.default.accept_source_route = 0*
	Deshabilitar aceptación de redireccionamiento IP	*net.ipv6.conf.all.accept_redirects = 0* *net.ipv6.conf.default.accept_redirects = 0*
	Deshabilitar el reenvío de IP	*net.ipv6.conf.all.forwarding = 0*
	Deshabilitar la aceptación de anuncios de enrutador	*net.ipv6.conf.default.accept_ra = 0* *net.ipv6.conf.default.autoconf = 0* *net.ipv6.conf.all.accept_ra = 0*

- **Deshabilitar enrutamiento de origen de IP**

  Se ha modificado la siguiente línea en el archivo ***/etc/sysctl.conf*** para evitar este tipo de ataques (permanente).

```
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0
```

- **Deshabilitar la aceptación de redirección**

  Se agregaron las siguientes líneas en el archivo ***/etc/sysctl.conf*** para evitar este tipo de ataque.

```
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0
```

- **Deshabilitar el reenvío de IP**

  La siguiente línea se ha modificado en el archivo ***/etc/sysctl.conf***.

```
net.ipv6.conf.all.forwarding = 0
```

- **Deshabilitar la aceptación de anuncios de enrutador**

  Los anuncios de enrutadores se utilizan para configurar automáticamente las interfaces en los hosts. En caso de que un intruso sea capaz de enviar anuncios de enrutador a través de

la red, podría cambiar la configuración de las interfaces (por ejemplo, la dirección de la puerta de enlace predeterminada o asignar una dirección de unidifusión global).

Un mensaje de anuncio de enrutador ilícito podría resultar en un ataque de "man in the middle".

Se agregaron las siguientes líneas en el archivo ***/etc/sysctl.conf.***

```
net.ipv6.conf.default.accept_ra = 0
net.ipv6.conf.default.autoconf = 0
net.ipv6.conf.all.accept_ra = 0
```

7.3. Servicio SSH

La siguiente tabla muestra la adaptación de las configuraciones que se realizarán en esta sección.

Tabla 7.3-1: Configuraciones SSH

FILE	LINE	
/etc/ssh/ssh_config	Versión segura del protocolo	*Protocol 2*
	Autenticación GSSAPI	*GSSAPIAuthentication no*
/etc/ssh/sshd_config	Versión segura del protocolo	*Protocol 2*
	Autenticación GSSAPI	*GSSAPIAuthentication no* *GSSAPICleanupCredentials yes*
	Ejecución remota de aplicaciones gráficas	*X11Forwarding yes*
	Tiempo de acceso al sistema	*LoginGraceTime 120*
	Contraseña requerida	*PermitEmptyPasswords no*
	Restringir uso del servicio ssh	*AllowUsers nor root installer*
	Tiempo de inactividad	*ClientAliveInterval 300*
	Tiempo de espera de inactividad	*ClientAliveCountMax 0*
	Autenticación basada en host	*HostbasedAuthentication no*
	Ignorar archivos .rhosts	*IgnoreRhosts yes*
	Último inicio de sesión	*PrintLastLog yes*
	Opciones de entorno	*PermitUserEnvironment no*
	Verificar permisos de archivo y propiedad	*StrictModes yes*
	Habilitar banners	*Banner /etc/issue.net*
/etc/issue.net	Texto del banner al inicio de sesión	*'NATS'*

Se recomienda el servicio SSH para el inicio de sesión remoto, la realización de copias de seguridad, la transferencia remota de archivos a través de SCP o SFTP, y mucho más. SSH es adecuado para mantener la confidencialidad e integridad de los datos intercambiados entre dos redes y sistemas, ya que se basa en una comunicación cifrada. Sin embargo, el principal beneficio obtenido es la autenticación del servidor, mediante el uso de criptografía de clave pública.

- Para evitar versiones inseguras del uso del protocolo SSH, se realizó la siguiente modificación, en el archivo ***/etc/ssh/ssh_config*** y en el archivo ***/etc/ssh/sshd_config***, que hará cumplir el uso de la versión segura.

```
Protocol 2
```

- La autenticación GSSAPI se utiliza para proporcionar mecanismos de autenticación adicionales a las aplicaciones. Permitir la autenticación GSSAPI a través de SSH expone el GSSAPI del sistema a hosts remotos, lo que aumenta la superficie de ataque del sistema.
  Para evitar demoras lentas en el inicio de sesión de SSH, se modificó la siguiente línea en el archivo ***/etc/ssh/ssh_config.***

```
GSSAPIAuthentication no
```

  Y en el archivo ***/etc/ssh/sshd_config*** se modificaron las siguientes líneas.

```
GSSAPIAuthentication no
GSSAPICleanupCredentials yes
```

- Para permitir la ejecución remota de aplicaciones gráficas a través de un túnel encriptado, se ha modificado la siguiente línea en el archivo ***/etc/ssh/sshd_config***.

```
X11Forwarding yes
```

- Para limitar el tiempo máximo de acceso al sistema, se ha agregado la siguiente línea en el archivo ***/etc/ssh/sshd_config***. Si el usuario no introduce un usuario y contraseña correctos en este tiempo máximo, la conexión SSH se cerrará. El valor se establecerá en 120 segundos:

```
LoginGraceTime 120
```

- Para solicitar una contraseña para acceder a la máquina de destino, se agregó la siguiente línea en el archivo ***/etc/ssh/sshd_config***.

```
PermitEmptyPasswords no
```

  La configuración de esta configuración para el demonio SSH proporciona una garantía adicional de que el inicio de sesión remoto a través de SSH requerirá una contraseña, incluso en el caso de una configuración incorrecta en otro lugar.

- Para restringir el uso del servicio SSH, se agregó la siguiente línea en el archivo ***/etc/ssh/sshd_config***.

```
AllowUsers nor root installer
```

- Cualquier usuario puede iniciar sesión en el servidor a través de SSH, por lo que se ha establecido un intervalo de tiempo de inactividad para evitar una sesión SSH desatendida. Se agregó la siguiente línea en el archivo ***/etc/ssh/sshd_config***.

```
ClientAliveInterval 300
```

Terminar una sesión ssh inactiva dentro de un período de tiempo corto reduce la ventana de oportunidad para que el personal no autorizado tome el control de una sesión de administración habilitada en la consola o el puerto de la consola que se ha dejado desatendido.

- Para garantizar que el tiempo de espera de inactividad de SSH ocurra precisamente cuando se establece ClientAliveInterval, se agregó la siguiente línea en el archivo ***/etc/ssh/sshd_config***.

```
ClientAliveCountMax 0
```

Esto garantiza que el inicio de sesión de un usuario finalizará tan pronto como se alcance el ClientAliveInterval.

- Para deshabilitar la autenticación basada en host, se agregó la siguiente línea en el archivo ***/etc/ssh/sshd_config***.

```
HostbasedAuthentication no
```

La autenticación basada en host criptográfico de SSH es más segura que la autenticación .rhosts. Sin embargo, no se recomienda que los hosts confíen mutuamente de manera unilateral, incluso dentro de una organización.

Las relaciones de confianza de SSH significan que un compromiso en un host puede permitir que un atacante se mueva trivialmente a otros hosts.

- El demonio SSH debe ignorar los archivos .rhosts.

```
IgnoreRhosts yes
```

- Fecha y hora SSH del último inicio de sesión.

El sistema operativo, al iniciar sesión con éxito, debe mostrar al usuario la fecha y hora del último inicio de sesión o acceso a través de SSH.

```
PrintLastLog yes
```

- El demonio SSH no debe permitir la configuración del entorno del usuario.

Para asegurarse de que los usuarios no puedan presentar opciones de entorno al demonio SSH, agregue o corrija la siguiente línea en ***/etc/ssh/sshd_config***.

```
PermitUserEnvironment no
```

- Comprobación del modo estricto de SSH.

La opción StrictModes de SSH verifica los permisos de archivo y propiedad en la carpeta .ssh del directorio de inicio del usuario antes de aceptar el inicio de sesión.

Si otros usuarios tienen acceso para modificar los archivos de configuración de SSH específicos del usuario, es posible que puedan iniciar sesión en el sistema como otro usuario.

Para habilitar StrictModes en SSH, agregue o corrija la siguiente línea en ***/etc/ssh/sshd_config***.

```
StrictModes yes
```

- Configuración del banner de inicio de sesión SSH.

Se ha configurado un banner de inicio de sesión para que cualquier intento de conexión a la máquina se muestre con un mensaje de advertencia. Se utiliza el archivo ***/etc/issue.net*** para mostrar un mensaje a los usuarios de SSH antes de iniciar sesión.

Se reemplazó el texto en los archivos ***/etc/issue.net***, ***/etc/issue***, ***/etc/motd*** con el texto apropiado.

Se ha editado el parámetro "Banner" en el archivo de configuración ***/etc/ssh/sshd_config*** habilitando banners. Luego, se ha agregado un banner que se mostrará antes de la autenticación. Se ha añadido la siguiente línea.

```
Banner /etc/issue.net
```

Por lo tanto, antes de iniciar una sesión, se mostrará un mensaje de banner. Se proporciona información detallada en el capítulo 7.11 Establecer Banner de este documento.

7.4. Mantenimiento del Software

La siguiente table muestra las configuraciones que se tratarán en esta sección.

Tabla 7.4-1: Configuraciones Mantenimiento del Sistema

FILE	LINE	
/etc/sysconfig/packagekit-background	Deshabilitar actualizaciones de software automáticas	*ENABLED = no*
/etc/yum.conf	Habilitar verificación de la firma de paquetes RPM	*gpgcheck = 1*
	Habilitar verificación de firmas de paquetes locales	*localpkg_gpgcheck = 1*
/etc/yum.repos.d	Verificación de la firma habilitada en todos los repositorios	*gpgcheck = 0*
/etc/dnf/automatic.conf	Habilitar actualizaciones de seguridad	*upgrade_type = security* *apply_updates = yes*

Los cambios en cualquier componente de software pueden tener efectos significativos en la seguridad general del sistema operativo. Se debe garantizar que el software no haya sido manipulado y que haya sido proporcionado por un proveedor de confianza.

En consecuencia, los parches, los service packs, los controladores de dispositivos o los componentes del sistema operativo deben estar firmados con un certificado reconocido y aprobado por la organización (***gpgcheck***, ***localpkg_gpgcheck***).

Aunque las actualizaciones automáticas de software deben estar deshabilitadas, no es el mismo caso que las actualizaciones emitidas como parte de un aviso de seguridad (paquete ***dnf-automatic***).

La instalación de actualizaciones de software es una mitigación fundamental contra la explotación de vulnerabilidades conocidas públicamente. Si no se instalan los parches y actualizaciones de seguridad más recientes, los usuarios no autorizados pueden aprovechar las debilidades del software sin parches. La falta de atención inmediata a la aplicación de parches podría resultar en un compromiso del sistema. La instalación automática de actualizaciones garantiza que los parches de seguridad recientes se apliquen de manera oportuna.

7.4.1. Deshabilitar Actualizaciones Automáticas

Los siguientes paquetes deben estar instalados:

```
#rpm -ivh rhnsd PackageKit-cron PackageKit-yum
```

Para deshabilitar las actualizaciones automáticas, el archivo ***/etc/sysconfig/packagekit-background*** se modificó cambiando el siguiente valor (de sí a no) como se muestra a continuación.

```
ENABLED=no
```

7.4.2. Actualizaciones del Software

- La opción gpgcheck controla si la firma de los paquetes RPM siempre se verifica antes de la instalación. Para garantizar que la opción gpgcheck esté habilitada en la configuración principal de yum, la siguiente línea debe aparecer en ***/etc/yum.conf*** en la sección ***[main]***.

  ```
  gpgcheck=1
  ```

  La verificación de la autenticidad del software antes de la instalación valida la integridad del parche o la actualización recibida de un proveedor. Esto garantiza que el software no haya sido manipulado y que haya sido proporcionado por un proveedor de confianza. Este requisito no permite los certificados autofirmados. Los certificados utilizados para verificar el software deben ser de una autoridad de certificación (CA) aprobada.

- Para asegurarse de que esta verificación de firma no esté deshabilitada para ningún otro repositorio, elimine cualquier línea de los archivos en ***/etc/yum.repos.d*** del formulario.

```
gpgcheck=0
```

- Para configurar ***yum*** para verificar firmas de paquetes locales, establezca ***localpkg_gpgcheck*** en ***1*** en ***/etc/yum.conf***.

```
localpkg_gpgcheck=1
```

- El sistema puede verificar criptográficamente que los paquetes de software base provienen de Red Hat, la clave GPG de Red Hat debe estar instalada correctamente. Esta clave se puede cargar previamente durante la instalación de RHEL y se puede instalar ejecutando el siguiente comando.

```
sudo rpm –import /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

- Alternativamente, si la clave no está precargada en el sistema, debe instalarla. Puede instalarla ejecutando el siguiente comando.

```
sudo subscription-manager register
```

- Aunque las actualizaciones automáticas de software se han deshabilitado, el paquete ***dnf-automatic*** nos permitirá instalar las actualizaciones disponibles solo para aquellas emitidas como parte de un aviso de seguridad y no para todas las actualizaciones disponibles. Para hacerlo, es necesario instalar el paquete ***dnf-automatic*** y habilitar el temporizador ***dnf-automatic*** usando los siguientes comandos.

```
sudo yum install dnf-automatic
sudo systemctl enable dnf-automatic.timer
```

- Para garantizar que solo se instalen actualizaciones de seguridad, es necesario configurar ***upgrade_type*** en ***security*** en la sección ***[commands]*** en ***/etc/dnf/automatic.conf***.

  De forma predeterminada, ***dnf-automatic*** instala todas las actualizaciones disponibles. Reducir la cantidad de paquetes actualizados solo a las actualizaciones que se emitieron como parte de un aviso de seguridad aumenta la estabilidad del sistema.

- Para asegurarse de que ***dnf-automatic*** instalará automáticamente los paquetes que comprenden las actualizaciones disponibles, establezca ***apply_updates*** en ***yes*** en la sección ***[commands]*** en ***/etc/dnf/automatic.conf.***

7.5. Users y Groups

La siguiente table muestra los archivos de configuración que se tendrán en cuenta en esta sección.

Tabla 7.5-1: Configuraciones de Users y Groups

FILE	LINE	
/etc/passwd	Información relevante de todos los usuarios del sistema	*user:pass:UID:GID:descripcion:home:shell*
/etc/group	Información relevante de todos los grupos de usuarios del sistema	*group:pass:UID:miembros*

7.5.1. Users

La siguiente tabla representa los usuarios genéricos, así como las consolas a las que deben acceder.

Tabla 7.5-1: OS Users

User	Shell
root	/bin/bash.
bin	/sbin/nologin
daemon	/sbin/nologin
adm	/sbin/nologin
lp	/sbin/nologin
sync	/bin/sync
shutdown	/sbin/shutdown
halt	/sbin/halt
mail	/sbin/nologin
uucp	/sbin/nologin
operator	/sbin/nologin
games	/sbin/nologin
gopher	/sbin/nologin
ftp	/sbin/nologin
nobody	/sbin/nologin
dbus	/sbin/nologin
vcsa	/sbin/nologin
nscd	/sbin/nologin
abrt	/sbin/nologin
haldaemon	/sbin/nologin
ntp	/sbin/nologin
saslauth	/sbin/nologin
postfix	/sbin/nologin
sshd	/sbin/nologin
nslcd	/sbin/nologin

User	Shell
tcpdump	/sbin/nologin
ossec	/sbin/nologin
ossecr	/sbin/nologin
nor	/bin/ksh
installer	/bin/ksh

7.5.2. Groups

La siguiente tabla representa la lista de grupos existentes en cada subsistema y la relación entre grupos y usuarios.

NOTA: Los espacios vacíos no significan que falte información.

Tabla 7.5-2: OS Groups

Group	Users
root	
bin	bin,daemon
daemon	bin,daemon
sys	bin,adm
adm	adm,daemon
tty	
disk	
lp	daemon
mem	
kmem	
wheel	
mail	mail,postfix
uucp	
man	
games	
gopher	
video	
dip	
ftp	
lock	
audio	
nobody	
users	
dbus	

Group	Users
utmp	
utempter	
floppy	
vcsa	
nscd	
abrt	
cdrom	
tape	
dialout	
haldaemon	haldaemon
ntp	
saslauth	
postdrop	
postfix	
stapusr	
stapsys	
stapdev	
sshd	
ldap	
tcpdump	
slocate	
ossec	ossec, ossecr
nor	

7.6. Deshabilitación de Cuenta sin Contraseña

Todas las cuentas de usuario en el sistema que tengan un shell interactivo, deben tener definida una contraseña y es necesaria para acceder al sistema. Esta contraseña debe cumplir con las políticas predefinidas.

7.7. Bloqueo de Usuarios no Root con UID 0

Un usuario no Root no debe tener el UID ***0*** en el archivo ***/etc/passwd***, ya que esto haría que esta cuenta tuviera todos los privilegios en el sistema (root).

7.8. Revisar los Permisos y la Propiedad de los Archivos

7.8.1. Archivos de Cuenta y Grupos

Se ha prestado especial atención a los siguientes archivos, ya que la autenticación local del sistema se basa en ellos.

Se han asegurado los archivos ***/etc/group***, ***/etc/passwd***, ***/etc/shadow***, ***/etc/gshadow*** y ***/etc/sysctl.conf*** para evitar borrarlos o sobrescribirlos accidentalmente.

Tabla 7.8-1: Atributos para archivos de cuenta y grupos

File	Commands	Permissions
/etc/group	chattr +i /etc/group	-rw-r--r--
/etc/passwd	chattr +i /etc/passwd	-rw-r--r--
/etc/shadow	chattr +i /etc/shadow	-------
/etc/gshadow	chattr +i /etc/gshadow	-------
/etc/sysctl.conf	chattr +i /etc/sysctl.conf	-rw-r--r--

El uso de esta bandera en estos archivos los mantiene a salvo de un ***rm -f*** accidental evitando también la posibilidad de agregar nuevas cuentas en caso de un exploit. El único propietario de estos archivos es root, y el grupo propietario de los archivos también es root.

7.8.2. Deshabilitar Binarios SUID y SGID

Se han deshabilitado los bits SUID y SGID en los siguientes archivos.

Tabla 7.8-2: Deshabilitar SUID y SGID

File	Commands	Permissions
/bin/ping6	chmod g-s /bin/ping6 chmod u-s /bin/ping6	-rwxr-xr-x
/usr/bin/chage	chmod g-s /usr/bin/chage chmod u-s /usr/bin/chage	-rwxr-xr-x
/usr/bin/chfn	chmod g-s /usr/bin/chfn chmod u-s /usr/bin/chfn	-rwx—x—x
/usr/bin/chsh	chmod g-s /usr/bin/chsh chmod u-s /usr/bin/chsh	-rws—x—x
/usr/bin/wall	chmod g-s /usr/bin/wall chmod u-s /usr/bin/wall	-r-xr-xr-x
/usr/bin/write	chmod g-s /usr/bin/write chmod u-s /usr/bin/write	-rwxr-xr-x
/usr/libexec/openssh/ssh-keysign	chmod g-s /usr/libexec/openssh/ssh-keysign chmod u-s /usr/libexec/openssh/ssh-keysign	-rwxr-xr-x
/usr/sbin/usernetctl	chmod g-s /usr/sbin/usernetctl chmod u-s /usr/sbin/usernetctl	-rwxr-xr-x

7.9. Bloquear uso de Ctrl + Alt + Sup o Ctrl + Alt + Del

Un usuario conectado localmente que presiona Ctrl + Alt + Del, cuando está en la consola, puede reiniciar el sistema. Si se presiona accidentalmente, como podría suceder en el caso de un

entorno de SO mixto, esto puede crear el riesgo de pérdida de disponibilidad a corto plazo de los sistemas debido a un reinicio involuntario.

Para evitar reinicios no deseados del sistema, esta combinación de teclas se deshabilita verificando los siguientes archivos y asegurando lo siguiente.

La siguiente línea se ha modificado en el archivo ***/etc/init/control-alt-delete.conf.***

```
#start on control-alt-delete
#exec /sbin/shutdown –r now “control-alt-delete pressed”
```

7.10. Establecer Requisitos de Contraseña en el proceso de Cambio de Contraseña

La siguiente table muestra las configuraciones que se tratarán en esta sección.

Tabla 7.10-1: Configuraciones Políticas de Contraseñas

FILE	LINE	
/usr/bin/passwd_reqs	Informar de las políticas de contraseñas	
/etc/profile	Habilitar alias para el comando *passwd*	*alias passwd=". /usr/bin/passwd_reqs"*
/etc/security/pwquality.conf	Verificación de la firma habilitada en todos los repositorios	*ucredit = -1* *lcredit = -1* *dcredit = -2* *ocredit = -1* *minlen = 8*

7.10.1. Informar al Usuario sobre las Políticas de Contraseñas

Como el IDM es el encargado de las tareas de gestión de usuarios, toda la política de contraseñas y aplicación de bloqueos, entre otros relacionados, se definen desde él hasta los subsistemas, incluida la propia AAA. Si por alguna razón el servicio AAA no está disponible, hay dos usuarios locales definidos en cada servidor (nor y root). Ambos podrán iniciar sesión en todo momento.

El uso de una contraseña compleja ayuda a aumentar el tiempo y los recursos necesarios para comprometer la contraseña. Cuanto más compleja sea la contraseña, mayor será el número de combinaciones posibles (ataques de fuerza bruta) que deben probarse antes de que la contraseña se vea comprometida.

Para ayudar al usuario a cumplir con los requisitos de contraseña durante el proceso de cambio de contraseña, se ha configurado un mensaje personalizado.

Se ha insertado el siguiente comando para crear un archivo de requisitos de contraseña.

```
# vi /usr/bin/passwd_reqs
```

El siguiente contenido se ha insertado en el archivo:

```
#echo " *****password requirements******* "
echo " Number of days before password expires    90"
echo " Number of days before password can be changed     1"
echo " Limit the number of grace logins allowed  5"
echo " Excluded password En route"
echo " Excluded password NERL"
echo " Excluded password Services"
echo " Excluded password Traffic"
echo " Excluded password Air"
echo " Excluded password National"
echo " Excluded password [redacted]
echo " Minimum number of characters in password  8"
echo " Maximum number of times a specific character can be used  11"
echo " Minimum number of numerals in password    2"
echo " Minimum number of lower case characters required in password
1"
echo " Minimum number of upper case characters required in password
1"
echo " Minimum number of non-alphabetic characters      1"
echo " Minimum number of non-alphanumeric characters     2"

/usr/bin/passwd "$1"
```

NOTA: el contenido de este archivo puede variar si cambia la política de contraseñas aplicada.

El archivo ***/etc/profile*** se ha editado para agregar la siguiente línea en negrita en la parte inferior. El objetivo es crear un alias para el comando passwd.

```
# /etc/profile
# System wide environment and startup programs, for login setup
# Functions and aliases go in /etc/bashrc

REDACTED

   fi
done
alias passwd=". /usr/bin/passwd_reqs"
unset i
unset pathmunge
```

Una vez que se haya ejecutado el comando *passwd*, se mostrará el texto en el archivo ***/usr/bin/passwd_reqs*** para mostrar los requisitos de la política de contraseñas. Cuando todos los pasos se realizan correctamente, la contraseña se cambia como se muestra a continuación.

```
login as: [redacted]
[redacted]@X.X.X.X's password:
Last login: Tue Dec  2 16:06:37 2014 from 10.70.45.144
[[redacted]@localhost ~]$ passwd
```

```
*****password requirements*******
Number of days before password expires    90
Number of days before password can be changed     1
Limit the number of grace logins allowed  5
Excluded password Keyword1
REDACTED
Minimum number of characters in password  8
Maximum number of times a specific character can be used  11
Minimum number of numerals in password    2
Minimum number of lower case characters required in password      1
Minimum number of upper case characters required in password      1
Minimum number of non-alphabetic characters       1
Minimum number of non-alphanumeric characters     2
Changing password for user [redacted]
Enter login(LDAP) password:
New password:
Retype new password:
LDAP password information changed for [redacted]
passwd: all authentication tokens updated successfully.
#
```

Nota: donde X.X.X.X es la dirección IP del servidor al que se está conectando.

7.10.2. Hacer cumplir las reglas mediante PAM

Además de notificar a los usuarios, PAM se ha configurado para asegurarse de que las nuevas contraseñas sigan las reglas descritas anteriormente. El módulo ***pwquality*** de PAM se encarga de esta tarea y ha sido configurado en consecuencia modificando el archivo ***/etc/security/pwquality.conf***.

```
ucredit = -1
lcredit = -1
dcredit = -2
ocredit = -1
minlen = 8
```

El parámetro en negativo quiere decir que al menos un carácter de ese tipo debe tener la contraseña.

El parámetro en positivo quiere decir que debe contener ese número de caracteres.

ucredit. Cantidad de letras en mayúscula.

lcredit. Cantidad de letras en minúscula.

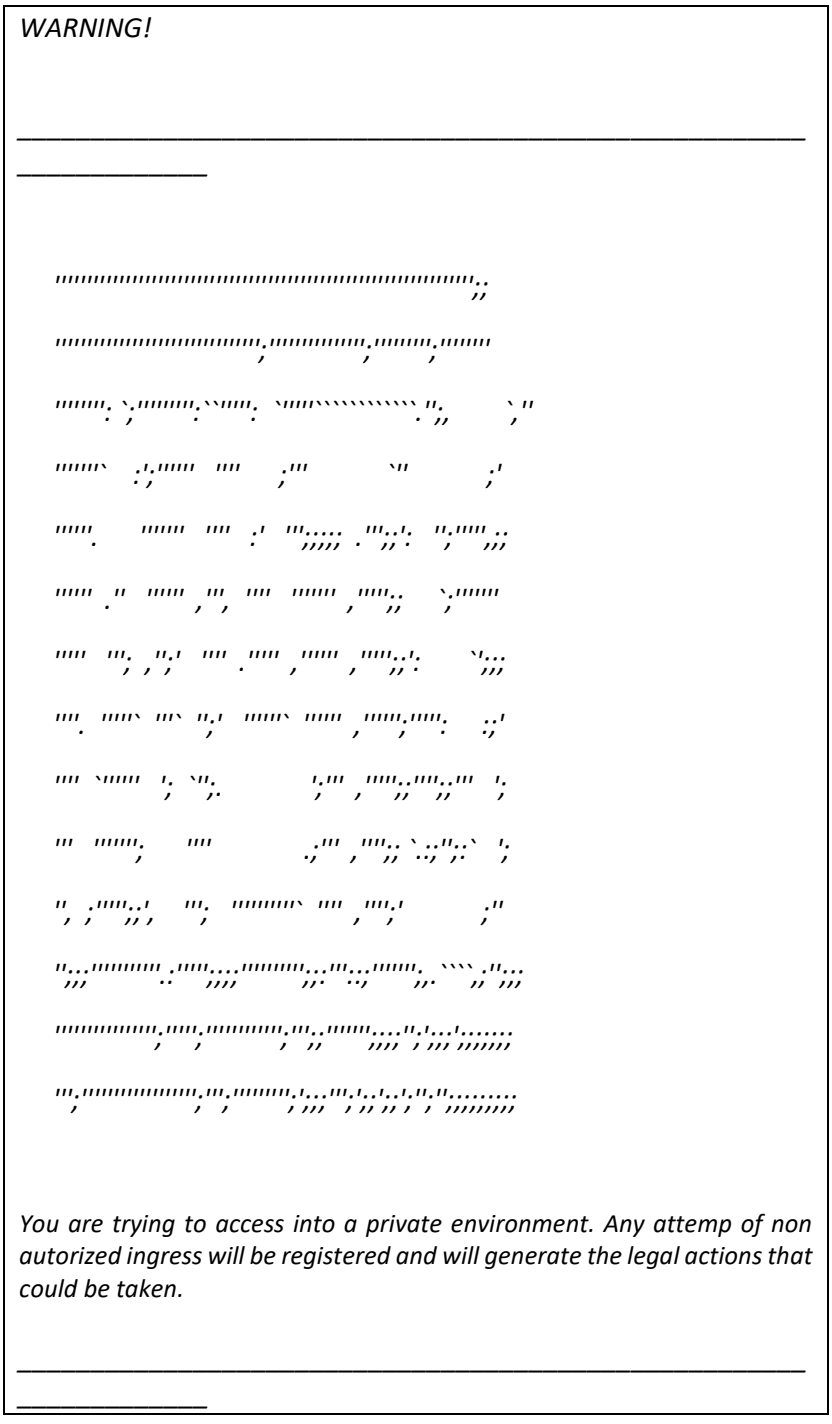
dcredit. Cantidad de dígitos.

ocredit. Cantidad de caracteres especiales.

minlen. Longitud mínima que debe tener la contraseña.

7.11. Establecer el banner

Se ha configurado un banner para que se muestre en cada intento de inicio de sesión de la siguiente manera.



7.12. Configuración de las políticas criptográficas del Sistema

Tabla 7.12-1: Configuración Políticas Criptográficas

FILE	LINE	
/etc/pki/tls/openssl.cnf	Configuración de la biblioyeca OpenSSL	*.include /etc/crypto-policies/back-ends/openssl.config*

Linux tiene la capacidad de configurar políticas criptográficas de forma centralizada. El comando ***update-crypto-policies*** se utiliza para establecer la política aplicable a los diversos backends criptográficos, como las bibliotecas SSL/TLS. Las políticas criptográficas configuradas serán la política predeterminada utilizada por estos backends a menos que el usuario de la aplicación las configure de otra manera. Cuando el sistema se ha configurado para usar las políticas criptográficas centralizadas, se garantiza que cualquier aplicación que utilice los backends admitidos seguirá una política que se adhiere al perfil configurado.

- El comando ***update -crypto-policies*** está incluido en el paquete ***crypto-policies*** y se puede instalar a través del comando de ***yum***.

```
sudo yum install crypto-policies
```

- Posteriormente, la política se puede configurar con el siguiente comando.

```
update-crypto-policies –set DEFAULT
```

- Una vez que se haya establecido la política, configuraremos la biblioteca OpenSSL para usar dicha política. Para lograr esto, se debe incluir la siguiente línea en la sección ***[crypto_policy]*** del archivo de configuración ***/etc/pki/tls/openssl.cnf.***

```
.include /etc/crypto-policies/back-ends/openssl.config
```

7.13. Configuración del Sistema de Registro mediante Audit

La siguiente tabla muestra los archivos de configuración que se tratarán en esta sección.

Tabla 7.13-1: Configuración del Sistema de Registro

FILE	LINE	
/etc/audit/rules.d/rhel-hardening.rules	Almacenar reglas audit	
/etc/audir/auditd.conf	Configuración de reglas audit	*log_format = ENRICHED* *flush = incremental_async* *name_format = hostname* *local_events = yes* *write_logs = yes* *freq = 50*
/etc/logrotate.d/audit	Almacenar configuración de registro de audit	*/var/log/audit/*.log {* *daily* *missingok* *rotate 14* *compress* *notifempty* *create 0640 root root* *}*

El programa auditd puede realizar un seguimiento exhaustivo de la actividad del sistema. El siguiente conjunto de reglas de audit se guardó en el archivo ***/etc/audit/rules.d/rhel-hardening.rules.***

```
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

## Successful ownership change
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-owner-change
-a always,exit -F arch=b64 -S lchown,fchown,chown,fchownat -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-owner-change

## Unsuccessful file delete
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-delete
-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-delete
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat -F exit=-
```

EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-delete
-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-delete

Successful file delete
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-delete
-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-delete

Unsuccessful file creation (open with O_CREAT)
-a always,exit -F arch=b32 -S openat,open_by_handle_at -F a2&0100 -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-create
-a always,exit -F arch=b64 -S openat,open_by_handle_at -F a2&0100 -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-create
-a always,exit -F arch=b32 -S open -F a1&0100 -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-create
-a always,exit -F arch=b64 -S open -F a1&0100 -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-create
-a always,exit -F arch=b32 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-create
-a always,exit -F arch=b64 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-create
-a always,exit -F arch=b32 -S openat,open_by_handle_at -F a2&0100 -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-create
-a always,exit -F arch=b64 -S openat,open_by_handle_at -F a2&0100 -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-create
-a always,exit -F arch=b32 -S open -F a1&0100 -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-create
-a always,exit -F arch=b64 -S open -F a1&0100 -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-create
-a always,exit -F arch=b32 -S creat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-create
-a always,exit -F arch=b64 -S creat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-create

Successful file access (any other opens) This has to go last.
These next two are likely to result in a whole lot of events
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-access
-a always,exit -F arch=b64 -S open,openat,open_by_handle_at -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-access

Unsuccessful file modifications (open for write or truncate)
-a always,exit -F arch=b32 -S openat,open_by_handle_at -F a2&01003 -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-modification
-a always,exit -F arch=b64 -S openat,open_by_handle_at -F a2&01003 -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-modification
-a always,exit -F arch=b32 -S open -F a1&01003 -F exit=-EACCES -F

```
auid>=1000 -F auid!=unset -F key=unsuccessful-modification
-a always,exit -F arch=b64 -S open -F a1&01003 -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-modification
-a always,exit -F arch=b32 -S truncate,ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-modification
-a always,exit -F arch=b64 -S truncate,ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-modification
-a always,exit -F arch=b32 -S openat,open_by_handle_at -F a2&01003 -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-modification
-a always,exit -F arch=b64 -S openat,open_by_handle_at -F a2&01003 -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-modification
-a always,exit -F arch=b32 -S open -F a1&01003 -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-modification
-a always,exit -F arch=b64 -S open -F a1&01003 -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-modification
-a always,exit -F arch=b32 -S truncate,ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-modification
-a always,exit -F arch=b64 -S truncate,ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-modification

## Unsuccessful permission change
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-perm-change
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-perm-change
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-perm-change
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-perm-change

## Successful file modifications (open for write or truncate)
-a always,exit -F arch=b32 -S openat,open_by_handle_at -F a2&01003 -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-modification
-a always,exit -F arch=b64 -S openat,open_by_handle_at -F a2&01003 -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-modification
-a always,exit -F arch=b32 -S open -F a1&01003 -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-modification
-a always,exit -F arch=b64 -S open -F a1&01003 -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-modification
-a always,exit -F arch=b32 -S truncate,ftruncate -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-modification
```

```
-a always,exit -F arch=b64 -S truncate,ftruncate -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-modification

## Successful permission change
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-perm-change
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-perm-change

## Successful file creation (open with O_CREAT)
-a always,exit -F arch=b32 -S openat,open_by_handle_at -F a2&0100 -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-create
-a always,exit -F arch=b64 -S openat,open_by_handle_at -F a2&0100 -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-create
-a always,exit -F arch=b32 -S open -F a1&0100 -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-create
-a always,exit -F arch=b64 -S open -F a1&0100 -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-create
-a always,exit -F arch=b32 -S creat -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-create
-a always,exit -F arch=b64 -S creat -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-create

## Unsuccessful file access (any other opens) This has to go last.
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-access
-a always,exit -F arch=b64 -S open,openat,open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-access
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-access
-a always,exit -F arch=b64 -S open,openat,open_by_handle_at -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-access

## Unsuccessful ownership change
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-owner-change
-a always,exit -F arch=b64 -S lchown,fchown,chown,fchownat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=unsuccessful-owner-change
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-owner-change
-a always,exit -F arch=b64 -S lchown,fchown,chown,fchownat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=unsuccessful-owner-change

## These rules watch for kernel module insertion. By monitoring
## the syscall, we do not need any watches on programs.
-a always,exit -F arch=b32 -S init_module,finit_module -F key=module-load
```

```
-a always,exit -F arch=b64 -S init_module,finit_module -F key=module-load
-a always,exit -F arch=b32 -S delete_module -F key=module-unload
-a always,exit -F arch=b64 -S delete_module -F key=module-unload

## Date and time modifications
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change

## Users and groups information
-w /etc/shadow -p wa -k usergroup_modification
-w /etc/security/opasswd -p wa -k usergroup_modification
-w /etc/gshadow -p wa -k usergroup_modification
-w /etc/passwd -p wa -k usergroup_modification
-w /etc/group -p wa -k usergroup_modification


## Discretionary Access Control permission modification
-a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=unset -F
```

```
key=perm_mod
-a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=unset -F
key=perm_mod
-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=unset -F
key=perm_mod
-a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=unset -F
key=perm_mod
-a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=unset -
F key=perm_mod
-a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=unset -
F key=perm_mod
-a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=unset -F
key=perm_mod
-a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=unset -F
key=perm_mod
-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=unset -F
key=perm_mod
-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=unset -F
key=perm_mod
-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=unset -
F key=perm_mod
-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=unset -
F key=perm_mod


## Changes on MAC
-w /etc/selinux/ -p wa -k MAC-policy


## Privileged commands usage
-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F
auid!=unset -F key=privileged_command
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F
auid!=unset -F key=privileged_command
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F
auid!=unset -F key=privileged_command
-a always,exit -F path=/usr/bin/pkexec -F perm=x -F auid>=1000 -F
auid!=unset -F key=privileged_command
-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F
auid!=unset -F key=privileged_command
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F
auid!=unset -F key=privileged_command
-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F
auid!=unset -F key=privileged_command
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F
auid!=unset -F key=privileged_command
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F
auid!=unset -F key=privileged_command
-a always,exit -F path=/usr/bin/chfn-F perm=x -F auid>=1000 -F
auid!=unset -F key=privileged_command
```

```
## Changes in system administration
-w /etc/sudoers -p wa -k admin_changes
-w /etc/sudoers.d/ -p wa -k admin_changes

## Network changes
-w /etc/hosts -p wa -k network_modification
-w /etc/etc/resolv.conf -p wa -k network_modification
-w /etc/nsswitch.conf -p wa -k network_modification
-w /etc/sysconfig/network -p wa -k network_modification
-w /etc/systemd/network -p wa -k network_modification

## Mount
-a always,exit -F arch=b32 -S mount -k mount
-a always,exit -F arch=b64 -S mount -k mount


## Set immutable
-e 2
```

Además, el archivo de configuración de audit, ***/etc/audit/auditd.conf*** también se ha modificado con el siguiente contenido:

```
log_format = ENRICHED
flush = incremental_async
name_format = hostname
local_events = yes
write_logs = yes
freq = 50
```

7.13.1. Configurar Logrotate

Es necesario asegurarse de que los archivos de registro se rotan para que no ocupen demasiado espacio. Se ha creado un nuevo archivo ***/etc/logrotate.d/audit*** que contiene la configuración de registro para audit.

```
/var/log/audit/*.log {
        daily
        missingok
        rotate 14
        compress
        notifempty
        create 0640 root root
}
```

7.14. Integración con el Método de Autenticación LDAP (PAM)

La siguiente tabla muestra los archivos de configuración modificados en esta sección.

Tabla 7.14-1: Configuración PAM de LDAP

FILE	LINE	
/etc/pam.d/system-auth	No permitir cuentas con contraseñas vacias	~~*nullok*~~
/etc/ldap.conf	Modificar el archivo	
/etc/pam_ldap.conf	Crear el fichero	
/etc/openldap/ldap.conf	Modificar el archivo	
/etc/nslcd.conf	Modificar el archivo y cambiar sus permisos	
/etc/nsswitch.conf	Realizar copia de seguridad del archivo y modificación del original.	
/etc/ssl/certs	Almacenar el certificado raíz	

7.14.1. Configurar el Cliente LDAP través de la línea de comandos

Se ha realizado una configuración automática como *root* con la siguiente línea de comandos para configurar el cliente LDAP.

```
#authconfig --enableldap --enableldapauth --
ldapserver=ldap://X.X.X.X,ldap:// X.X.X.X --ldapbasedn="o=[redacted]" --
enablemkhomedir --update
```

NOTA: La configuración de ambas direcciones IP (donde X.X.X.X son las direcciones IP del servidor LDAP) permite a los usuarios conectarse al servidor LDAP principal. En caso de no responder el primer servidor intentará conectarse al segundo, por lo que no es necesario configurar un balanceador de carga. Finalmente, en caso de ocurrir una emergencia, si ninguno de los servidores LDAP está disponible, los usuarios locales autorizados siempre podrán iniciar sesión.

7.14.2. Modificación del Archivo PAM

El archivo ***/etc/pam.d/system-auth*** se ha modificado con los valores marcados en negrita de la siguiente manera:

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        sufficient    pam_ldap.so use_first_pass
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
```

```
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     required      pam_permit.so

password  required  pam_pwquality.so  try_first_pass  local_users_only
retry=3 authtok_type=
password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass
use_authtok
password    sufficient    pam_ldap.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     optional      pam_mkhomedir.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond
quiet use_uid
session     required      pam_unix.so
session     optional      pam_ldap.so
```

Si una cuenta tiene una contraseña vacía, cualquiera puede iniciar sesión y ejecutar comandos con los privilegios de esa cuenta. Las cuentas con contraseñas vacías nunca deben usarse en entornos operativos.

Hay que eliminar cualquier instancia de la opción ***nullok*** para evitar inicios de sesión con contraseñas vacías.

7.14.3. Modificación de ficheros LDAP

- **Modificar el fichero */etc/ldap.conf***

  Se ha modificado el archivo ***/etc/ldap.conf*** con los valores marcados en negrita de la siguiente manera.

```
#
# The distinguished name of the search base.
base o=[redacted]

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
#uri ldapi[redacted]
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
#ldap_version 3
```

 # The distinguished name to bind to the server with.
 # Optional: default is to bind anonymously.
#binddn cn=proxyuser,dc=example,dc=com

 # The credentials to bind with.
 # Optional: default is no credential.
#bindpw secret

 # The distinguished name to bind to the server with
 # if the effective user ID is root. Password is
 # stored in / [redacted] *(mode 600)*
[redacted]

 # The port.
 # Optional: [redacted]
[redacted]

 # The search scope.
[redacted]
#scope one
#scope base

 # Search timelimit
#timelimit 30

 # Bind/connect timelimit
#bind_timelimit 30

 # Reconnect policy:
 # hard_open: reconnect to DSA with exponential backoff if
 # opening connection failed
 # hard_init: reconnect to DSA with exponential backoff if
 # initializing connection failed
 # hard: alias for hard_open
 # soft: return immediately on server failure
bind_policy [redacted]

 # Connection policy:
 # persist: DSA connections are kept open (default)
 # oneshot: DSA connections destroyed after request
#nss_connect_policy persist

 # Idle timelimit; client will close connections
 # (nss_ldap only) if the server has not been contacted
 # for the number of seconds specified below.
#idle_timelimit 3600

 # Use paged rseults
#nss_paged_results yes

```
# Pagesize: when paged results enable, used to set the
# pagesize to a custom value
#pagesize 1000

# Filter to AND with uid=%s
#pam_filter objectclass=account

# The user ID attribute (defaults to uid)
#pam_login_attribute uid

# Search the root DSE for the password policy (works
# with Netscape Directory Server). Make use of
# Password Policy LDAP Control (as in OpenLDAP)
pam_lookup_policy [redacted]

# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
pam_check_host_attr [redacted]


# Check the 'authorizedService' attribute for access
# control
# Default is no; if set to yes, and the user has no
# value for the authorizedService attribute, and
# pam_ldap is configured for account management
# (authorization) then the user will not be allowed
# to login.
#pam_check_service_attr yes

# Group to enforce membership of
#pam_groupdn cn=PAM,ou=Groups,dc=example,dc=com

# Group member attribute
#pam_member_attribute uniquemember

# Specify a minium or maximum UID number allowed
#pam_min_uid 0
#pam_max_uid 0

# Template login attribute, default template user
# (can be overriden by value of former attribute
# in user's entry)
#pam_login_attribute userPrincipalName
#pam_template_login_attribute uid
#pam_template_login nobody

# HEADS UP: the pam_crypt, pam_nds_passwd,
# and pam_ad_passwd options are no
```

```
# longer supported.
#
# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
#pam_password clear

# Hash password locally; required for University of
# Michigan LDAP server, and works with Netscape
# Directory Server if you're using the UNIX-Crypt
# hash mechanism and not using the NT Synchronization
# service.
#pam_password crypt

# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
#pam_password nds

# RACF is an alias for the above. For use with
# IBM RACF
#pam_password racf

# Update Active Directory password, by
# creating Unicode password and updating
# unicodePwd attribute.
#pam_password ad

# Use the OpenLDAP password change
# extended operation to update the password.
pam_password [redacted]

# Redirect users to a URL or somesuch on password
# changes.
#pam_password_prohibit_message Please visit http://internal to change
            your password.

# Use backlinks for answering initgroups()
#nss_initgroups backlink

# returns NOTFOUND if nss_ldap's initgroups() is called
# for users specified in nss_initgroups_ignoreusers
# (comma separated)
[redacted]

# Enable support for [redacted] (distinguished names in group
# members)

# [redacted] naming contexts
# Syntax:
# nss_base_XXX        base?scope?filter
```

```
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
# You can omit the suffix eg:
# nss_base_passwd       ou=People,
# to append the default base DN but this
# may incur a small performance impact.

nss_base_passwd o=[redacted]
nss_base_shadow o=[redacted]
nss_base_group  o=[redacted]

#nss_base_hosts        ou=Hosts,dc=example,dc=com?one
#nss_base_services     ou=Services,dc=example,dc=com?one
#nss_base_networks     ou=Networks,dc=example,dc=com?one
#nss_base_protocols    ou=Protocols,dc=example,dc=com?one
#nss_base_rpc          ou=Rpc,dc=example,dc=com?one
#nss_base_ethers       ou=Ethers,dc=example,dc=com?one
#nss_base_netmasks     ou=Networks,dc=example,dc=com?ne
#nss_base_bootparams   ou=Ethers,dc=example,dc=com?one
#nss_base_aliases      ou=Aliases,dc=example,dc=com?one
#nss_base_netgroup     ou=Netgroup,dc=example,dc=com?one

# attribute/objectclass mapping
# Syntax:
#nss_map_attribute      [redacted]      mapped_attribute
#nss_map_objectclass    [redacted]      mapped_objectclass

# Enable support for [redacted]distinguished names in group
# members)

# configure --enable-nds is no longer supported.
# NDS mappings
nss_map_attribute      uniqueMember member

# Services for UNIX 3.5 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount User
#nss_map_attribute uid [redacted]Name
#nss_map_attribute uniqueMember m[redacted]PosixMember
#nss_map_attribute userPassword m[redacted]Password
#nss_map_attribute homeDirectory ms[redacted]HomeDirectory
#nss_map_attribute homeDirectory [redacted]HomeDirectory
#nss_map_objectclass posixGroup Group
#pam_login_attribute m[redacted]Name
#pam_filter objectclass=User
#pam_password ad

# configure --enable-mssfu-schema is no longer supported.
# Services for UNIX 2.0 mappings
#nss_map_objectclass posixAccount User
```

```
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid msSFUName
#nss_map_attribute uniqueMember posixMember
#nss_map_attribute userPassword msSFUPassword
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup Group
#nss_map_attribute cn msSFUName
#pam_login_attribute msSFUName
#pam_filter objectclass=User
#pam_password ad

# RFC 2307 (AD) mappings
#nss_map_objectclass posixAccount user
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid sAMAccountName
#nss_map_attribute homeDirectory unixHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup group
#nss_map_attribute uniqueMember member
#pam_login_attribute sAMAccountName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# AuthPassword mappings
#nss_map_attribute userPassword authPassword

# AIX SecureWay mappings
#nss_map_objectclass posixAccount aixAccount
#nss_base_passwd ou=aixaccount,?one
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_base_group ou=aixgroup,?one
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
#pam_password clear

# For pre-RFC2307bis automount schema
#nss_map_objectclass automountMap nisMap
#nss_map_attribute automountMapName nisMapName
#nss_map_objectclass automount nisObject
#nss_map_attribute automountKey cn
#nss_map_attribute automountInformation nisMapEntry

# Netscape SDK LDAPS
```

```
#ssl on

# Netscape SDK SSL options
#sslpath /[redacted]

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically [redacted]
ssl start_tls
uri ldap://X.X.X.X ldap://X.X.X.X
ldap_version [redacted]
pam_filter      objectClass=posixAccount

# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is to use libldap's default behavior, which can be configured in
# /etc/openldap/ldap.conf using the TLS_REQCERT setting.  The default for
# OpenLDAP 2.0 and earlier is "no", for 2.1 and later is "yes".
#tls_checkpeer yes
[redacted]

# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
[redacted]

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
#tls_ciphers [redacted]

# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key

# Disable SASL security layers. This is needed for AD.
#[redacted]

# Override the default Kerberos ticket cache location.
#[redacted]
```

NOTA: las direcciones IP para los servidores LDAP serán reemplazadas de X.X.X.X a las correspondientes.

- **Crear el fichero *<u>/etc/pam_ldap.conf</u>***

Para cada sistema de la organización se debe crear el archivo ***/etc/pam_ldap.conf*** y completarlo con el contenido del cuadro a continuación.

```
# #
# The distinguished name of the search base.
base o=[redacted]

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
#uri ldapi:/[redacted]
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
#ldap_version [redacted]

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
#[redacted]

# The credentials to bind with.
# Optional: default is no credential.
#[redacted]

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /[redacted] mode 600)
[redacted]

# The port.
# Optional: default is [redacted]
port [redacted]

# The search scope.
scope sub
#scope one
#scope base

# Search timelimit
#timelimit 30

# Bind/connect timelimit
```

```
#bind_timelimit 30

# Reconnect policy:
#  hard_open: reconnect to DSA with exponential backoff if
#           opening connection failed
#  hard_init: reconnect to DSA with exponential backoff if
#           initializing connection failed
#  hard:      alias for hard_open
#  soft:      return immediately on server failure
bind_policy [redacted]

# Connection policy:
#  persist:   DSA connections are kept open (default)
#  oneshot:   DSA connections destroyed after request
#nss_connect_policy persist

# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
#idle_timelimit 3600

# Use paged rseults
#nss_paged_results yes

# Pagesize: when paged results enable, used to set the
# pagesize to a custom value
#pagesize 1000

# Filter to AND with uid=%s
#pam_filter objectclass=account

# The user ID attribute (defaults to uid)
#pam_login_attribute uid

# Search the root DSE for the password policy (works
# with Netscape Directory Server). Make use of
# Password Policy LDAP Control (as in OpenLDAP)
pam_lookup_policy [redacted]

# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
pam_check_host_attr [redacted]

# Check the 'authorizedService' attribute for access
# control
# Default is no; if set to yes, and the user has no
# value for the authorizedService attribute, and
# pam_ldap is configured for account management
```

```
# (authorization) then the user will not be allowed
# to login.
#pam_check_service_attr yes

# Group to enforce membership of
#pam_groupdn cn=PAM,ou=Groups,dc=example,dc=com

# Group member attribute
#pam_member_attribute uniquemember

# Specify a minium or maximum UID number allowed
#pam_min_uid 0
#pam_max_uid 0

# Template login attribute, default template user
# (can be overriden by value of former attribute
# in user's entry)
#pam_login_attribute userPrincipalName
#pam_template_login_attribute uid
#pam_template_login nobody

# HEADS UP: the pam_crypt, pam_nds_passwd,
# and pam_ad_passwd options are no
# longer supported.
#
# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
#pam_password clear

# Hash password locally; required for University of
# Michigan LDAP server, and works with Netscape
# Directory Server if you're using the UNIX-Crypt
# hash mechanism and not using the NT Synchronization
# service.
#pam_password crypt

# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
#pam_password nds

# RACF is an alias for the above. For use with
# IBM RACF
#pam_password racf

# Update Active Directory password, by
# creating Unicode password and updating
# unicodePwd attribute.
#pam_password ad
```

```
# Use the OpenLDAP password change
# extended operation to update the password.
pam_password [redacted]

# Redirect users to a URL or somesuch on password
# changes.
#pam_password_prohibit_message Please visit http://internal to change
        your password.

# Use backlinks for answering initgroups()
#nss_initgroups backlink

# returns NOTFOUND if nss_ldap's initgroups() is called
# for users specified in nss_initgroups_ignoreusers
# (comma separated)
nss_initgroups_ignoreusers [redacted]

# Enable support for [redacted]distinguished names in group
# members)
nss_schema [redacted]

# [redacted] naming contexts
# Syntax:
# nss_base_XXX        base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
# You can omit the suffix eg:
# nss_base_passwd     ou=People,
# to append the default base DN but this
# may incur a small performance impact.

nss_base_passwd o=[redacted]
nss_base_shadow o=[redacted]
nss_base_group o=[redacted]

#nss_base_hosts       ou=Hosts,dc=example,dc=com?one
#nss_base_services    ou=Services,dc=example,dc=com?one
#nss_base_networks    ou=Networks,dc=example,dc=com?one
#nss_base_protocols   ou=Protocols,dc=example,dc=com?one
#nss_base_rpc         ou=Rpc,dc=example,dc=com?one
#nss_base_ethers      ou=Ethers,dc=example,dc=com?one
#nss_base_netmasks    ou=Networks,dc=example,dc=com?ne
#nss_base_bootparams  ou=Ethers,dc=example,dc=com?one
#nss_base_aliases     ou=Aliases,dc=example,dc=com?one
#nss_base_netgroup    ou=Netgroup,dc=example,dc=com?one

# attribute/objectclass mapping
# Syntax:
#nss_map_attribute [redacted]
#nss_map_objectclass [redacted]
```

```
# configure --enable-nds is no longer supported.
# NDS mappings
[redacted]

# Services for UNIX 3.5 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount User
#nss_map_attribute uid msSFU30Name
#nss_map_attribute uniqueMember msSFU30PosixMember
#nss_map_attribute userPassword msSFU30Password
#nss_map_attribute homeDirectory msSFU30HomeDirectory
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_objectclass posixGroup Group
#pam_login_attribute msSFU30Name
#pam_filter objectclass=User
#pam_password ad

# configure --enable-mssfu-schema is no longer supported.
# Services for UNIX 2.0 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid msSFUName
#nss_map_attribute uniqueMember posixMember
#nss_map_attribute userPassword msSFUPassword
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup Group
#nss_map_attribute cn msSFUName
#pam_login_attribute msSFUName
#pam_filter objectclass=User
#pam_password ad

# RFC 2307 (AD) mappings
#nss_map_objectclass posixAccount user
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid sAMAccountName
#nss_map_attribute homeDirectory unixHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup group
#nss_map_attribute uniqueMember member
#pam_login_attribute sAMAccountName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# AuthPassword mappings
#nss_map_attribute userPassword authPassword

# AIX SecureWay mappings
#nss_map_objectclass posixAccount aixAccount
```

```
#nss_base_passwd ou=aixaccount,?one
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_base_group ou=aixgroup,?one
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
#pam_password clear

# For pre-[redacted] schema
#nss_map_objectclass automountMap nisMap
#nss_map_attribute automountMapName nisMapName
#nss_map_objectclass automount nisObject
#nss_map_attribute automountKey cn
#nss_map_attribute automountInformation nisMapEntry

# Netscape SDK LDAPS
#ssl on

# Netscape SDK SSL options
#sslpath /[redacted]

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically [redacted]

ssl start_tls
uri ldap://X.X.X.X ldap:// X.X.X.X
ldap_version [redacted]
pam_filter     objectClass=[redacted]

# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is to use libldap's default behavior, which can be configured in
# /etc/openldap/ldap.conf using the TLS_REQCERT setting.  The default for
# OpenLDAP 2.0 and earlier is "no", for 2.1 and later is "yes".
#tls_checkpeer yes

# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
tls_cacertfile [redacted]
tls_cacertdir [redacted]

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile [redacted]

# SSL cipher suite
# See man ciphers for syntax
```

```
#tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key

# Disable SASL security layers. This is needed for AD.
#sasl_secprops maxssf=0

# Override the default Kerberos ticket cache location.
#[redacted]
```

NOTA: las direcciones IP de los servidores LDAP serán reemplazadas de X.X.X.X a las correspondientes.

- **Modificar el fichero *<u>/etc/openldap/ldap.conf</u>***

Para cada sistema de la organización se debe modificar el fichero ***/etc/openldap/ldap.conf*** de la siguiente forma.

```
# #
# The distinguished name of the search base.
base o=NATS

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
#uri ldapi://[redacted]
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
#ldap_version [redacted]

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
#binddn cn=proxyuser,dc=example,dc=com

# The credentials to bind with.
# Optional: default is no credential.
#bindpw secret

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /[redacted]mode 600)
[redacted]
```

```
# The port.
# Optional: default is [redacted]
port [redacted]

# The search scope.
scope sub
#scope one
#scope base

# Search timelimit
#timelimit 30

# Bind/connect timelimit
#bind_timelimit 30

# Reconnect policy:
#  hard_open: reconnect to DSA with exponential backoff if
#           opening connection failed
#  hard_init: reconnect to DSA with exponential backoff if
#           initializing connection failed
#  hard:      alias for hard_open
#  soft:      return immediately on server failure
bind_policy [redacted]

# Connection policy:
#  persist:   DSA connections are kept open (default)
#  oneshot:   DSA connections destroyed after request
#nss_connect_policy persist

# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
#idle_timelimit 3600

# Use paged rseults
#nss_paged_results yes

# Pagesize: when paged results enable, used to set the
# pagesize to a custom value
#pagesize 1000

# Filter to AND with uid=%s
#pam_filter objectclass=account

# The user ID attribute (defaults to uid)
#pam_login_attribute uid

# Search the root DSE for the password policy (works
# with Netscape Directory Server). Make use of
# Password Policy LDAP Control (as in OpenLDAP)
pam_lookup_policy [redacted]
```

```
# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
[redacted]


# Check the 'authorizedService' attribute for access
# control
# Default is no; if set to yes, and the user has no
# value for the authorizedService attribute, and
# pam_ldap is configured for account management
# (authorization) then the user will not be allowed
# to login.
#pam_check_service_attr yes

# Group to enforce membership of
#pam_groupdn cn=PAM,ou=Groups,dc=example,dc=com

# Group member attribute
#pam_member_attribute uniquemember

# Specify a minium or maximum UID number allowed
#pam_min_uid 0
#pam_max_uid 0

# Template login attribute, default template user
# (can be overriden by value of former attribute
# in user's entry)
#pam_login_attribute userPrincipalName
#pam_template_login_attribute uid
#pam_template_login nobody

# HEADS UP: the pam_crypt, pam_nds_passwd,
# and pam_ad_passwd options are no
# longer supported.
#
# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
#pam_password clear

# Hash password locally; required for University of
# Michigan LDAP server, and works with Netscape
# Directory Server if you're using the UNIX-Crypt
# hash mechanism and not using the NT Synchronization
# service.
#pam_password crypt
```

```
# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
pam_password [redacted]

# RACF is an alias for the above. For use with
# IBM RACF
#pam_password [redacted]

# Update Active Directory password, by
# creating Unicode password and updating
# unicodePwd attribute.
#pam_password [redacted]

# Use the OpenLDAP password change
# extended operation to update the password.
#pam_password [redacted]

# Redirect users to a URL or somesuch on password
# changes.
#pam_password_prohibit_message Please visit http://internal to change
            your password.

# Use backlinks for answering initgroups()
#nss_initgroups [redacted]

# returns NOTFOUND if nss_ldap's initgroups() is called
# for users specified in nss_initgroups_ignoreusers
# (comma separated)
[redacted]

# Enable support for RFC2307bis (distinguished names in group
# members)

# [redacted] contexts
# Syntax:
# nss_base_XXX        base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
# You can omit the suffix eg:
# nss_base_passwd      ou=People,
# to append the default base DN but this
# may incur a small performance impact.

nss_base_passwd o=[redacted]
nss_base_shadow o=[redacted]
nss_base_group  o=[redacted]

#nss_base_hosts       ou=Hosts,dc=example,dc=com?one
#nss_base_services     ou=Services,dc=example,dc=com?one
```

```
#nss_base_networks      ou=Networks,dc=example,dc=com?one
#nss_base_protocols     ou=Protocols,dc=example,dc=com?one
#nss_base_rpc           ou=Rpc,dc=example,dc=com?one
#nss_base_ethers        ou=Ethers,dc=example,dc=com?one
#nss_base_netmasks      ou=Networks,dc=example,dc=com?ne
#nss_base_bootparams    ou=Ethers,dc=example,dc=com?one
#nss_base_aliases       ou=Aliases,dc=example,dc=com?one
#nss_base_netgroup      ou=Netgroup,dc=example,dc=com?one

# attribute/objectclass mapping
# Syntax:
#nss_map_attribute      [redacted]      mapped_attribute
#nss_map_objectclass    [redacted]      mapped_objectclass

# Enable support for [redacted]distinguished names in group
# members)
[redacted]

# configure --enable-nds is no longer supported.
# NDS mappings
nss_map_attribute       uniqueMember member

# Services for UNIX 3.5 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount User
#nss_map_attribute uid msSFU30Name
#nss_map_attribute uniqueMember msSFU30PosixMember
#nss_map_attribute userPassword msSFU30Password
#nss_map_attribute homeDirectory msSFU30HomeDirectory
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_objectclass posixGroup Group
#pam_login_attribute msSFU30Name
#pam_filter objectclass=User
#pam_password ad

# configure --enable-mssfu-schema is no longer supported.
# Services for UNIX 2.0 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid msSFUName
#nss_map_attribute uniqueMember posixMember
#nss_map_attribute userPassword msSFUPassword
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup Group
#nss_map_attribute cn msSFUName
#pam_login_attribute msSFUName
#pam_filter objectclass=User
#pam_password ad

# RFC 2307 (AD) mappings
```

```
#nss_map_objectclass posixAccount user
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid sAMAccountName
#nss_map_attribute homeDirectory unixHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup group
#nss_map_attribute uniqueMember member
#pam_login_attribute sAMAccountName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# AuthPassword mappings
#nss_map_attribute userPassword authPassword

# AIX SecureWay mappings
#nss_map_objectclass posixAccount aixAccount
#nss_base_passwd ou=aixaccount,?one
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_base_group ou=aixgroup,?one
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
#pam_password clear

# For pre-RFC2307bis automount schema
#nss_map_objectclass automountMap nisMap
#nss_map_attribute automountMapName nisMapName
#nss_map_objectclass automount nisObject
#nss_map_attribute automountKey cn
#nss_map_attribute automountInformation nisMapEntry

# Netscape SDK LDAPS
#ssl on

# Netscape SDK SSL options
#sslpath /[redacted]

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically [redacted]
ssl start_tls
uri ldaps://X.X.X.X ldaps:// X.X.X.X
ldap_version [redacted]
pam_filter     objectClass=posixAccount
ssl on
```

```
# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is to use libldap's default behavior, which can be configured in
# /etc/openldap/ldap.conf using the TLS_REQCERT setting.  The default for
# OpenLDAP 2.0 and earlier is "no", for 2.1 and later is "yes".
#tls_checkpeer yes
TLS_REQCERT allow

# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
tls_cacertfile [redacted]
tls_cacertdir /[redacted]

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
#tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key

# Disable SASL security layers. This is needed for AD.
#sasl_secprops maxssf=0

# Override the default Kerberos ticket cache location.
#krb5_ccname FILE:/etc/.ldapcache
#URI ldaps://[redacted]
BASE  o=[redacted]
```

NOTA: las direcciones IP de los servidores LDAP serán reemplazadas de X.X.X.X a las correspondientes.

- **Modificar el fichero /etc/nslcd.conf**

El archivo /etc/nslcd.conf ha sido modificado con los valores marcados en negrita de la siguiente manera.

```
#
# This is the configuration file for the LDAP nameservice
# switch library's nslcd daemon. It configures the mapping
# between NSS names (see /[redacted] and LDAP
# information in the directory.
# See the manual page nslcd.conf(5) for more information.

# The uri pointing to the LDAP server to use for name lookups.
```

```
# Multiple entries may be specified. The address that is used
# here should be resolvable without using LDAP (obviously).
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
#uri ldapi[redacted]
# Note: %2f encodes the '/' used as directory separator
# uri ldap://127.0.0.1/

# The LDAP version to use (defaults to 3
# if supported by client library)
#ldap_version [redacted]

# The distinguished name of the search base.
# base dc=example,dc=com
# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
#binddn cn=proxyuser,dc=example,dc=com

# The credentials to bind with.
# Optional: default is no credentials.
# Note that if you set a bindpw you should check the permissions of this
        file.
#bindpw secret

# The distinguished name to perform password modifications by root by.
#rootpwmoddn cn=admin,dc=example,dc=com

# The default search scope.
#scope sub
#scope one
#scope base

# Customize certain database lookups.
#base   group  ou=Groups,dc=example,dc=com
#base   passwd ou=People,dc=example,dc=com
#base   shadow ou=People,dc=example,dc=com
#scope  group  onelevel
#scope  hosts  sub

# Bind/connect timelimit.
#bind_timelimit 30

# Search timelimit.
#timelimit 30

# Idle timelimit. nslcd will close connections if the
# server has not been contacted for the number of seconds.
#idle_timelimit 3600

# Use StartTLS without verifying the server certificate.
ssl start_tls
```

tls_reqcert [redacted]

 # CA certificates for server certificate verification
#tls_cacertdir / [redacted]
#tls_cacertfile / [redacted]

 # Seed the PRNG if /dev/urandom is not provided
#tls_randfile [redacted]

 # SSL cipher suite
 # See man ciphers for syntax
#tls_ciphers TLSv1

 # Client certificate and key
 # Use these, if your server requires client authentication.
#tls_cert
#tls_key

 # NDS mappings
#map group uniqueMember member

 # Mappings for Services for UNIX 3.5
#filter passwd (objectClass=User)
#map passwd uid msSFU30Name
#map passwd userPassword msSFU30Password
#map passwd homeDirectory msSFU30HomeDirectory
#map passwd homeDirectory msSFUHomeDirectory
#filter shadow (objectClass=User)
#map shadow uid msSFU30Name
#map shadow userPassword msSFU30Password
#filter group (objectClass=Group)
#map group uniqueMember msSFU30PosixMember

 # Mappings for Services for UNIX 2.0
#filter passwd (objectClass=User)
#map passwd uid msSFUName
#map passwd userPassword msSFUPassword
#map passwd homeDirectory msSFUHomeDirectory
#map passwd gecos msSFUName
#filter shadow (objectClass=User)
#map shadow uid msSFUName
#map shadow userPassword msSFUPassword
#map shadow shadowLastChange pwdLastSet
#filter group (objectClass=Group)
#map group uniqueMember posixMember

 # Mappings for Active Directory
#pagesize 1000
#referrals off
#filter passwd
[redacted]

```
[redacted]
#map    passwd uid              sAMAccountName
#map    passwd homeDirectory    unixHomeDirectory
#map    passwd gecos            displayName
#filter                                                    shadow
[redacted]
#map    shadow uid              sAMAccountName
#map    shadow shadowLastChange pwdLastSet
#filter group  (objectClass=group)
#map    group  uniqueMember     member

# Mappings for AIX SecureWay
#filter passwd (objectClass=aixAccount)
#map    passwd uid              userName
#map    passwd userPassword     passwordChar
#map    passwd uidNumber        uid
#map    passwd gidNumber        gid
#filter group  (objectClass=aixAccessGroup)
#map    group  cn               groupName
#map    group  uniqueMember     member
#map    group  gidNumber        gid
uid [redacted]
gid [redacted]
# This comment prevents repeated auto-migration of settings.
uri ldap://X.X.X.X ldap://X.X.X.X
base o=[redacted]
scope sub
ssl start_tls
tls_cacertfile /[redacted]
tls_cacertdir /[redacted]
```

NOTA: las direcciones IP de los servidores LDAP serán reemplazadas de X.X.X.X a las correspondientes.

El siguiente comando debe ejecutarse para cambiar los permisos de este fichero.

```
#chmod 600 /etc/nslcd.conf
```

- **Modificar el fichero *<u>/etc/nsswitch.conf</u>***

Se ha realizado una copia de seguridad del archivo ***/etc/nsswitch.conf***, luego se ha modificado el archivo original con los valores marcados en negrita de la siguiente manera.

```
#
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
```

```
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Legal entries are:
#
#       compat              Use compatibility setup
#       nisplus             Use NIS+ (NIS version 3)
#       nis                 Use NIS (NIS version 2), also called YP
#       dns                 Use DNS (Domain Name Service)
#       files               Use the local files
#       [NOTFOUND=return]       Stop searching if not found so far
#
# For more information, please read the nsswitch.conf.5 manual page.
#

passwd: files
shadow: files
group: files

#passwd:       compat
#group: files ldap

hosts:  files dns
networks:       files dns

services:       files
protocols:      files
rpc:    files
ethers: files
netmasks:       files
netgroup:       files
publickey:      files

bootparams:     files
automount:      files nis
aliases:        files
#passwd_compat:  ldap
```

NOTA: el orden de los parámetros introducidos (primero ldap y luego archivos) indica que el primer repositorio de usuarios/grupos que se revisará es el LDAP (IDM eDirectory) y luego el archivo local ***/etc/passwd*** o ***/etc/group***. Si las condiciones cambian y el primer repositorio a revisar es el local ***(/etc/passwd***) en lugar del remoto (LDAP), se debe cambiar el orden de

estos parámetros en el archivo, estableciendo como primer parámetro, archivos, y como segundo parámetro ldap.

7.14.4. Importar el Root Certificate de confianza

El certificado raíz de confianza debe exportarse desde cualquiera de los servidores IDM (donde se generó primero) e importarse en el directorio ***/etc/ssl/certs*** del sistema Red Hat. El siguiente comando se ejecutó desde el servidor IDM donde se creó inicialmente el certificado.

```
vidm1:# scp -r /etc/ssl/certs/cert.pem root@Z.Z.Z.Z:/etc/ssl/certs/
This server has restricted Access.
root@Z.Z.Z.Z's password:
[redacted]                                                    100% 1858
1.8KB/s   00:00
vidm1:#
```

NOTA: el Z.Z.Z.Z representa la dirección IP remota donde se debe copiar el certificado.

NOTA 2: una vez que el certificado se haya copiado correctamente, se debe reiniciar el sistema.

7.14.5. Testing de grupos y usuarios de LDAP

- **Test User**

El comando ***getent*** se ha utilizado para obtener usuarios y grupos locales y LDAP de la siguiente manera. Si se muestran todos los usuarios o grupos de LDAP, significa que hay conectividad entre los servidores del sistema y LDAP, por lo que la configuración es correcta.

Para buscar usuarios locales, se ha ejecutado el siguiente comando.

```
#cat /etc/passwd
```

Muestra lo siguiente (solo usuarios locales).

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
dbus:x:81:81:System message bus:/:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
nor:x:131:500::/home/users/nor:/bin/ksh
ntp:x:38:38::/etc/ntp:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
```

```
nslcd:x:65:55:LDAP Client User:/:/sbin/nologin
```

Por otro lado, para verificar que todos los usuarios (locales y LDAP) puedan iniciar sesión en el servidor, se ha ejecutado el siguiente comando.

```
#getent passwd
```

Muestra lo siguiente (usuarios locales y LDAP). Los usuarios de LDAP están marcados en negrita.

```
test2:*:70003:50000:test2:/home/test2:/bin/ksh
test1:*:70000:50000:test1:/home/test1:/bin/bash
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
dbus:x:81:81:System message bus:/:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
nslcd:x:65:55:LDAP Client User:/:/sbin/nologin
nor:x:131:500::/home/users/nor:/bin/ksh
ntp:x:38:38::/etc/ntp:/sbin/nologin
```

NOTA: home y Shell pueden variar según el entorno.

NOTA 2: los usuarios locales y LDAP que se muestran en el cuadro anterior son ejemplos y pueden variar según la cantidad final de usuarios locales/LDAP en ambos repositorios.

- **Test Group**

El mismo caso ocurre para los grupos. Para ver solo los grupos locales, se ha ejecutado el siguiente comando.

```
#cat /etc/group
```

La salida del comando anterior muestra lo siguiente:

```
root:x:0:
bin:x:1:bin,daemon
daemon:x:2:bin,daemon
sys:x:3:bin,adm
adm:x:4:adm,daemon
tty:x:5:
disk:x:6:
mem:x:8:
```

```
kmem:x:9:
wheel:x:10:
man:x:15:
video:x:39:
lock:x:54:
users:x:100:
dbus:x:81:
utmp:x:22:
cdrom:x:11:
tape:x:33:
dialout:x:18:
haldaemon:x:68:haldaemon
saslauth:x:76:
ntp:x:38:
sshd:x:74:
nor:x:500:
ossec:x:499:ossec,ossecr
nscd:x:28:
ldap:x:55:
```

Para ver los grupos locales y LDAP, se ha ejecutado el siguiente comando:

```
#getent group
```

El resultado de este comando muestra lo siguiente (las líneas en negrita muestran los grupos LDAP).

```
eDirectoryUsersSecured:*:50005:nor
eDirectoryUsers:*:50000:
root:x:0:
bin:x:1:bin,daemon
daemon:x:2:bin,daemon
sys:x:3:bin,adm
adm:x:4:adm,daemon
tty:x:5:
disk:x:6:
mem:x:8:
kmem:x:9:
wheel:x:10:
man:x:15:
video:x:39:
lock:x:54:
users:x:100:
dbus:x:81:
utmp:x:22:
cdrom:x:11:
tape:x:33:
dialout:x:18:
haldaemon:x:68:haldaemon
saslauth:x:76:
ntp:x:38:
```

```
sshd:x:74:
nor:x:500:
ossec:x:499:ossec,ossecr
nscd:x:28:
ldap:x:55
```

NOTA: los grupos locales y LDAP que se muestran en el cuadro sobre esta línea son ejemplos y pueden variar según la cantidad final de local/LDAP en ambos repositorios.

CAPÍTULO 8. SCAP Y ANSIBLE

Las siguientes tecnologías serán usadas para el cumplimiento de la configuración en RHEL.

8.1. ¿Qué es y Cómo funciona SCAP?

Red Hat Enterprise Linux proporciona herramientas que nos permiten realizar una auditoría de cumplimiento totalmente automatizada. Estas herramientas se basan en el estándar *Security Content Automation Protocol (SCAP)* y están diseñadas para la adaptación automatizada de las políticas de cumplimiento.

- **SCAP Workbench** - La utilidad gráfica *scap-workbench* está diseñada para realizar escaneos de configuración y vulnerabilidad en un solo sistema local o remoto. También se puede utilizar para generar informes de seguridad basados en estos escaneos y evaluaciones.

- **OpenSCAP** - La biblioteca OpenSCAP, con la utilidad de línea de comandos que la acompaña *oscap*, está diseñada para realizar escaneos de configuración y vulnerabilidad en un sistema local, para validar el contenido de cumplimiento de la configuración y para generar informes y guías basados en estos escaneos y evaluaciones. Esta utilidad sirve como *front-end* de la biblioteca OpenSCAP y agrupa sus funcionalidades en módulos (subcomandos) basados en el tipo de contenido SCAP que procesa.

- **SCAP Security Guide (SSG)** - El paquete *scap-security-guide* proporciona la última colección de políticas de seguridad para sistemas Linux. La guía consiste en un catálogo de consejos prácticos de *hardening*, vinculados a los requisitos del gobierno cuando sea aplicable. El proyecto tiende un puente entre los requisitos políticos generalizados y las directrices de aplicación específicas.

- **Script Check Engine (SCE)** - SCE es una extensión del protocolo SCAP que permite a los administradores escribir su contenido de seguridad utilizando un lenguaje de scripting, como Bash, Python y Ruby. La extensión SCE se proporciona en el paquete *openscap-engine-sce*. El SCE en sí no forma parte del estándar SCAP.

Se puede utilizar el escaneo de cumplimiento de configuración para ajustarse a una línea de base definida por una organización específica. Por ejemplo, si se trabaja con el gobierno de EEUU, tendremos que cumplir con el Perfil de Protección del Sistema Operativo (OSPP), y si es un procesador de pagos, tendrá que cumplir con el estándar de Seguridad de Datos de la Industria de las Tarjetas de Pago (PCI - DSS). También se puede realizar un análisis de cumplimiento de la configuración para reforzar la seguridad del sistema.

Red Hat recomienda seguir el contenido del Protocolo de Automatización de Contenidos de Seguridad (SCAP) proporcionado en el paquete de la Guía de Seguridad SCAP porque está en línea con las mejores prácticas de Red Hat para los componentes afectados.

NOTA 1: en este proyecto queremos asegurar el cumplimiento de la configuración de la línea de base definida por el cliente (capítulo 7), es decir, se ha creado una SSG personalizada según los requisitos del cliente y mejoras consideradas por el equipo de desarrollo.

El conjunto de guías de seguridad SCAP proporciona perfiles para varias plataformas en forma de documentos de flujo de datos. Un flujo de datos es un archivo (XML) que contiene definiciones, puntos de referencia, perfiles y reglas individuales. Cada regla especifica la aplicabilidad y los requisitos de cumplimiento. RHEL 8 proporciona varios perfiles para el cumplimiento de las políticas de seguridad. Además del estándar de la industria, los flujos de datos de Red Hat también contienen información para remediar las reglas fallidas.

NOTA 2: el flujo de datos desarrollado para este proyecto cuenta con un único perfil (*--profile*) llamado *standard*.

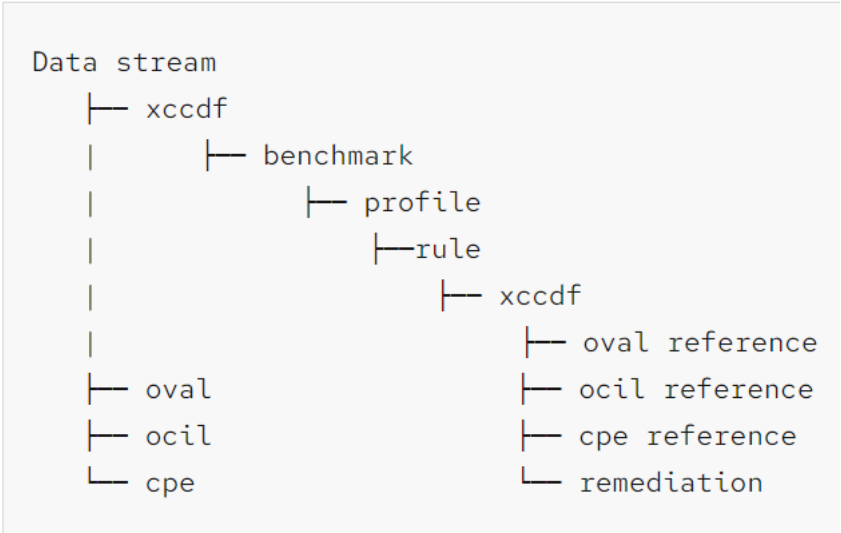


Figura 8-1: Estructura de los recursos de exploración de la conformidad

Un perfil es un conjunto de reglas basadas en una política de seguridad, como el Perfil de Protección del Sistema Operativo (OSPP) o el Estándar de Seguridad de Datos de la Industria de las Tarjetas de Pago (PCI-DSS). Esto permite auditar el sistema de forma automatizada para comprobar el cumplimiento de las normas de seguridad.

Oscap procesa principalmente el XCCDF (*Extensible Configuration Checklist Description Format*) que es una forma estándar de expresar el contenido de una lista de verificación y define las listas de verificación de seguridad. También se combina con otras especificaciones como CPE (*Common Platform Enumeration*), CCE (*Common Configuration Enumeration*) and OVAL (*Open Vulnerability and Assessment Language*) para crear una lista de verificación expresada por SCAP que pueda ser procesada por productos validados por SCAP.

Los resultados posibles de las reglas definidas en este proyecto tras realizar una exploración OpenSCAP son los siguientes:

- **Pass**: la exploración no encontró ningún conflicto en esta norma.
- **Fail:** se encontró conflicto en esa regla.
- **Error:** el escaneo encontró un error.
- **Unknown:** el escaneo encontró una situación inesperada.

8.2. ¿Qué es y Cómo funciona Ansible?

Es una herramienta de orquestación usada internamente para administrar sistemas. Usaremos los módulos de Ansible para la remediación.

8.3. Uso en el Proyecto

El proceso se divide en los siguientes pasos.

[1] INSTALACIÓN

Debemos instalar oscap en el objetivo y, los paquetes y dependencias necesarios para su uso y para crear reglas personalizadas.

```
$ sudo yum update
$ sudo yum install ansible
$ sudo yum install epel-release
$ yum install openscap-scanner
$ sudo yum install scap-security-guide
$ sudo yum install openscap-engine-sce
```

[2] ESCANEO

Para evaluar la conformidad del sistema con el perfil seleccionado usaremos el siguiente comando.

```
$ oscap xccdf eval –profile standard –results results.xml prueba.xml
```

El flujo de datos es el fichero *prueba.xml*. los resultados del escaneo sobre *prueba.xml* se guardan en *results.xml.*

A continuación se aplicará la remediación a los resultados *fail* del escaneo para alinear el sistema con la línea de base definida.

[3] REMEDIACIÓN

Generamos un playbook de Ansible basado en el archivo generado en el paso anterior.

```
$ oscap xccdf generate fix –fix-type ansible –profile standard –result-id
xccdf_org.open-scap_testresult_standard –output remediat.yml
results.xml
```

El comando *--result-id xccdf_org.open-scap_testresult_standard* nos garantiza que sólo se aplicará el *fix* a los resultados *fail* tras realizar el *check*.

El resultado se guardará en un fichero de tipo ansible llamado *remediat.yml*. Este archivo contiene las correcciones de Ansible para las reglas que fallaron durante el análisis realizado en el escaneo.

IMPORTANTE: la remediación debe llevarse a cabo con cuidado, ya que puede hacer que el sistema no funcione. Red Hat no proporciona ningún método automatizado para revertir

los cambios realizados por las correcciones de seguridad. Las correcciones son compatibles con los sistemas RHEL en la configuración por defecto. Si el sistema ha sido alterado después de la instalación, la ejecución de la remediación podría hacer que no cumpla con el perfil de seguridad requerido.

Por último, tras revisar el archivo generado, aplicamos las correcciones con el siguiente comando.

```
$ ansible-playbook remediat.yml
```

Las mejoras incluidas por el grupo de desarrollo en la línea de base establecida para la securización del sistema se basan en las siguientes guías, en concreto en *ssg-rhel8-guide-cui.*

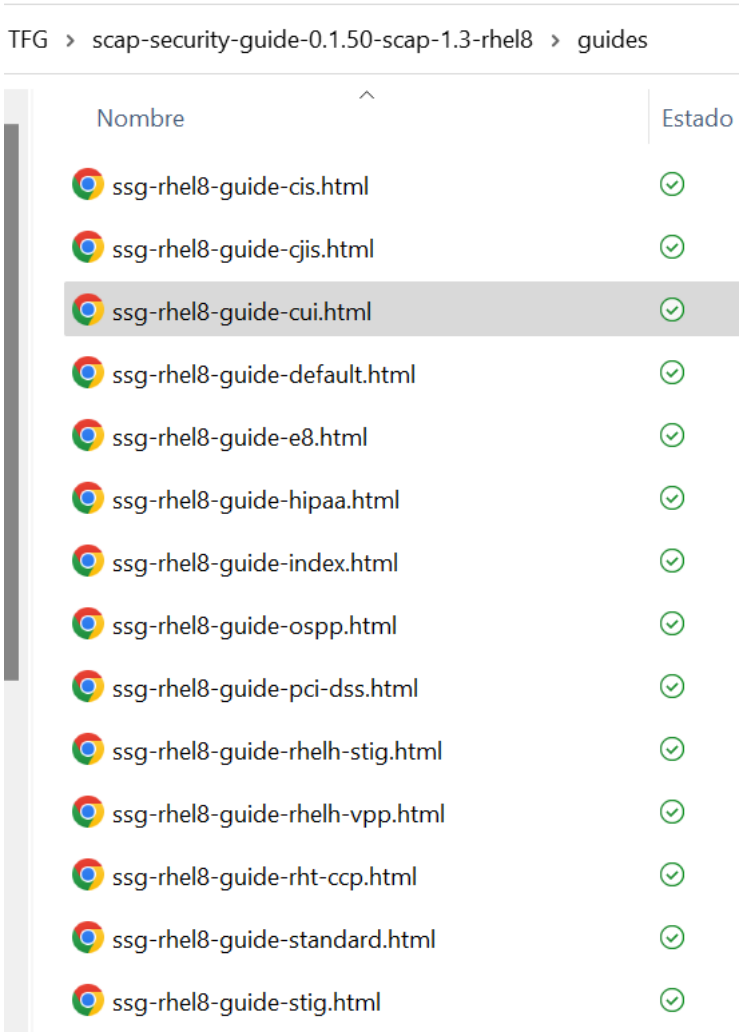


Figura 8-2: Guías seguidas

-cis – Prueba de referencia de CIS Red Hat Enterprise Linux 8.

-cui – Información no clasificada en sistemas de información y organizaciones no federales (NIST 800-171).

-e8 – Centro Australiano de Ciberseguridad (ACSC). Ocho esenciales.

-hipaa – Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA).

-ospp – Perfil de Protección para Sistemas Operativos de uso general.

8.4. Scripts personalizados

Los scripts para la verificación del cumplimiento de reglas; los *checks* se han desarrollado en bash y las remediaciones; los *fix* en anisble.

A continuación, un pequeño ejemplo de los scripts para explicar su funcionamiento.

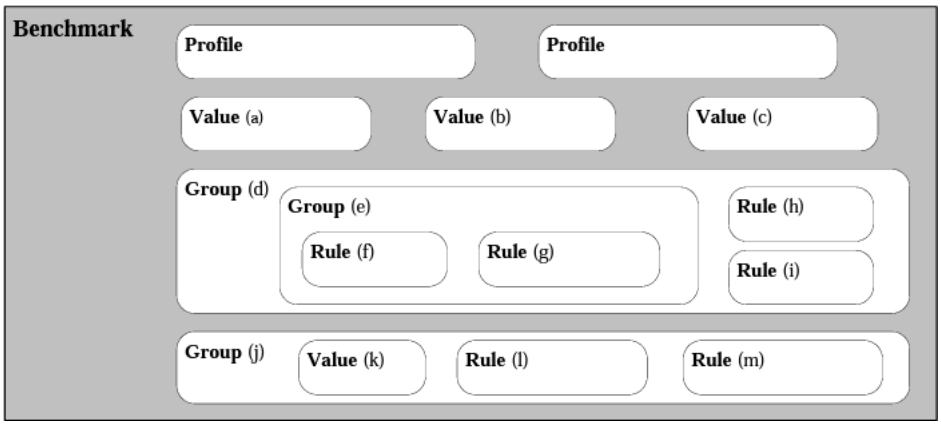


Figura 8-3: Estructura de un Benchmark

```
<?xml version="1.0" encoding="UTF-8"?>
<Benchmark
  xmlns="http://checklists.nist.gov/xccdf/1.1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  id="test">
  <status date="2023-02-15">draft</status>
  <title>Users and Groups</title>
  <version>1</version>

  <Profile id="standard">
    <title>Standard System Security Profile</title>
  </Profile>

  <Group id="Users_Groups">

  <Value id="root_line" operator="equals" type="string">
    <value>root</value>
  </Value>
```

Figura 8-4: Fragmento de código 1

```
    <Group id="Users">
      <title>Users</title>

      <Value id="passwd_file" operator="equals" type="string">
        <value>/etc/passwd</value>
      </Value>
```

Figura 8-5: Fragmento de código 2

```
      <Value id="bash_shell" operator="equals" type="string">
        <value>/bin/bash</value>
      </Value>
```

Figura 8-6: Fragmento de código 3

```
      <Rule id="Root_Shell" selected="true" severity="medium">
        <title>Check Root Shell</title>
        <fix system="urn:xccdf:fix:script:ansible">
- name: Get line to change
  command: grep '^root:x:' /etc/passwd
  register: line

- debug: msg="{{ line.stdout }}"

- name: Split old line
  set_fact:
    user: "{{ line.stdout.split(':') }}"
  when: line.stdout_lines|length > 0

- name: replace bash
  replace:
    path: /etc/passwd
    regexp: '{{ line.stdout }}'
    replace: '{{ line.stdout | replace(user[6], "/bin/bash")}}'

- name: Get changed line
  command: grep '^root:x:' /etc/passwd
  register: line

- debug: msg="{{ line.stdout }}"
        </fix>
```

Figura 8-7: Fragmento de código 4

```
        <check system="http://open-scap.org/page/SCE">
            <check-export export-name="file" value-id="passwd_file"/>
            <check-export export-name="line" value-id="root_line"/>
            <check-export export-name="shell" value-id="bash_shell"/>
            <check-content-ref href="shell_check.sh"/>
        </check>
      </Rule>
```

Figura 8-8: Fragmento de código 5

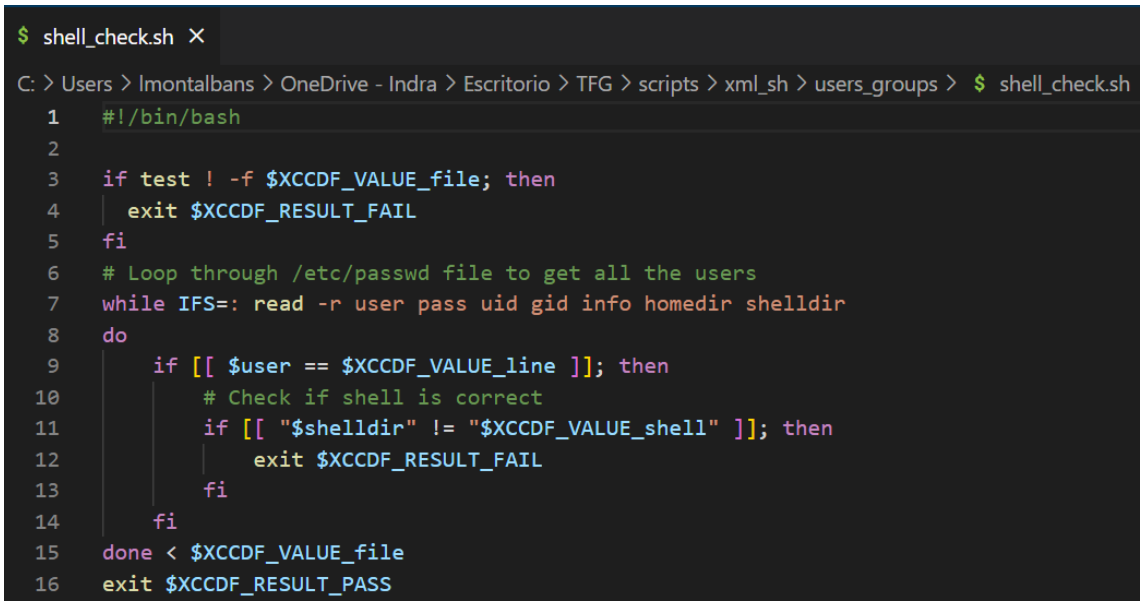


Figura 8-9: Script de check

En la figura 8-8 hacemos referencia al script de verificación personalizado en XCCDF usamos *<check-content-ref href = ruta del script check>*

En la figura 8-9 tenemos:

XCCDF_VALUE_nombredelavariable

XCCDF_RESULT_codigodesalida

Las variables y los operadores XCCDF se comunican con el ejecutable de verificación mediante variables de entorno.

<check-export export-name="line" value-id="root-line" />

CAPÍTULO 9. PRUEBAS DE EJECUCIÓN

A continuación, se mostrarán las pruebas de ejecución realizadas de los módulos de forma individual.

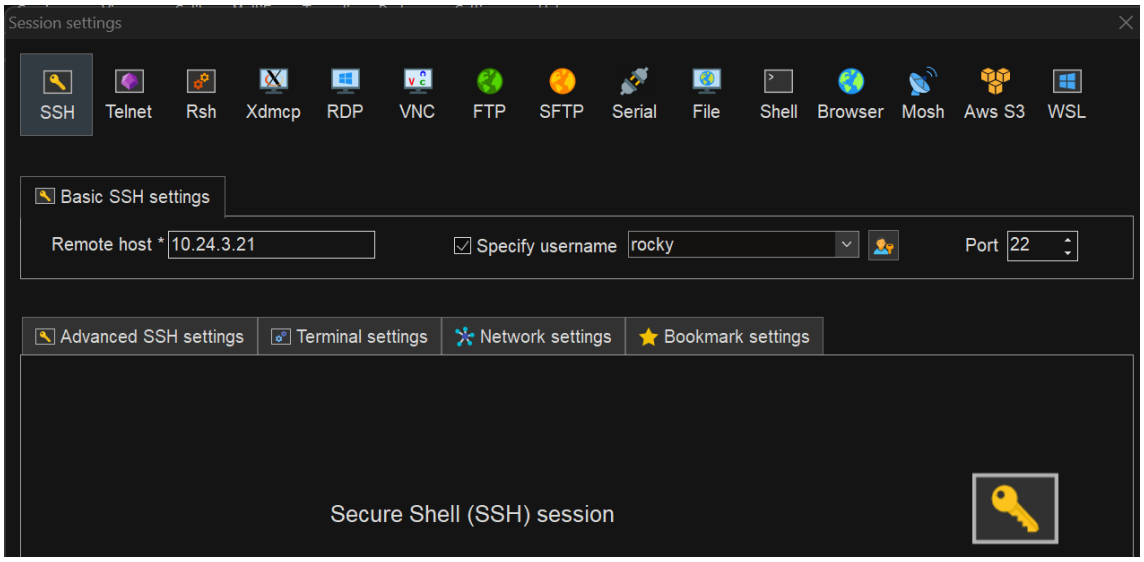
En el directorio *xml_sh* tenemos cada configuración organizada en directorios de forma individual.

En el directorio *linux_system_hardening* tenemos un único fichero que incluye toda la configuración. Estos ficheros son los que debe ejecutar el administrador del sistema para implementar todas las configuraciones deseadas en el sistema.

Las pruebas se han realizado sobre una máquina *rocky Linux 8*, la cual está basada en RHEL8. La máquina *rocky* está desplegada en *OpenStack*, donde me conecto con una vpn.

NOTA 1: durante el desarrollo del producto, algunas pruebas se han realizado sobre copias del fichero de configuración para evitar colapsar la máquina.

NOTA 2: las capturas de pantalla que se muestran a continuación del contenido de los ficheros tratados sólo muestran una parte del contenido de estos debido a su extensión, de la misma forma ocurre con los *check* y los *fix.*



Los comandos de *oscap* y *ansible* referenciados en el capítulo 8 se han añadido al fichero ejecutable *oscap_ansible.sh* para ejecutar un único fichero.

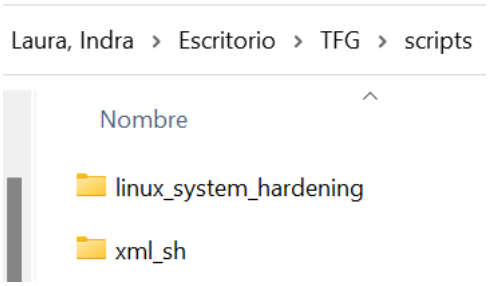


Figura 9-1: Organización Directorios

9.1. Xml_sh

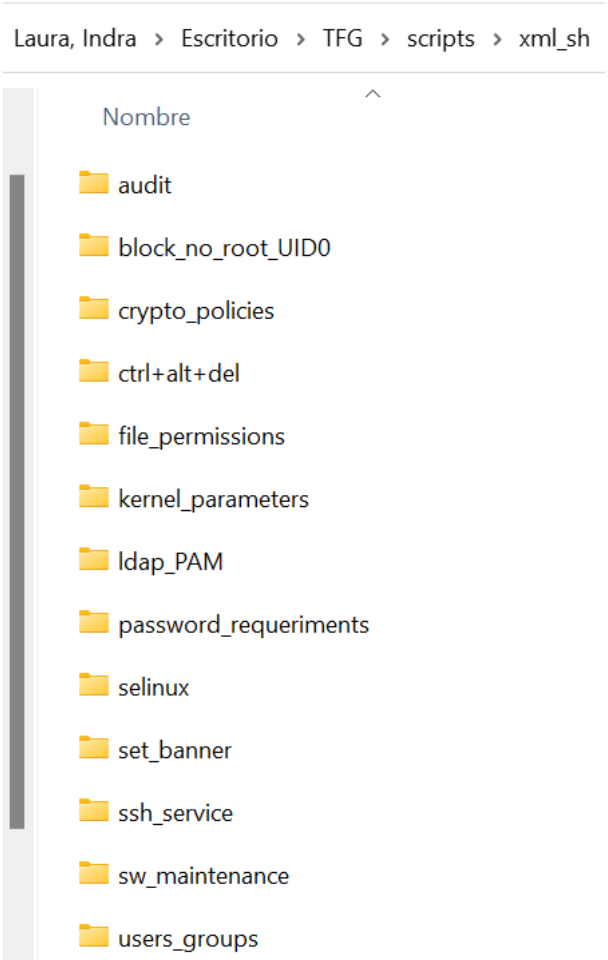


Figura 9-2: Organización del directorio xml_sh

- **Kernel Parameters**

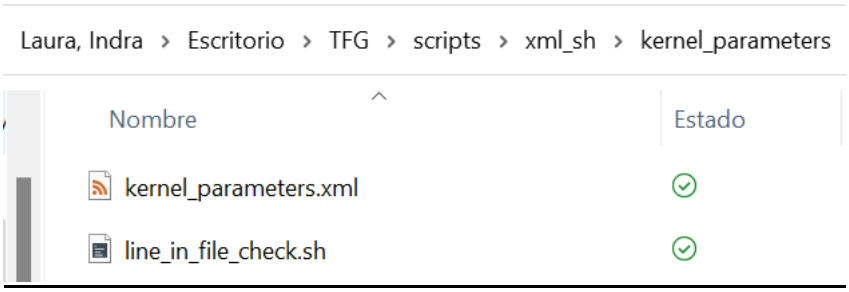


Figura 9-3: Directorio kernel_parameters

```
  GNU nano 2.9.8                    /etc/sysctl.conf

# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
```

Figura 9-4: Fichero /etc/sysctl.conf antes

```
[rocky@vm-rocky-3 laura]$ sudo sh oscap_ansible.sh
--- Starting Evaluation ---

Title   Test if TCP SYN Cookie Protection is enabled
Rule    TCP_Syn_Cookie_Protection
Result  fail

Title   Test if IPv4 Source Routing is disabled (all)
Rule    IPv4_Source_Routing_all
Result  fail
```

Figura 9-5: Check kernel_parameters

```
PLAY [all] *********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [localhost]

TASK [Ensure sysctl net.ipv4.tcp_syncookies is set] ****************************
changed: [localhost]

TASK [Ensure sysctl net.ipv4.conf.all.accept_source_route is set] ********
changed: [localhost]
```

Figura 9-6: Fix kernel_parameters

```
[rocky@vm-rocky-3 laura]$ cat /etc/sysctl.conf
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.tcp_syncookies=1
net.ipv4.conf.all.accept_source_route=0
net.ipv4.conf.default.accept_source_route=0
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.default.accept_redirects=0
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
net.ipv4.ip_forward=0
net.ipv4.icmp_ignore_bogus_error_responses=1
kernel.kptr_restrict=1
kernel.randomize_va_space=1
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
net.ipv4.conf.all.secure_redirects=0
net.ipv4.conf.default.secure_redirects=0
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv6.conf.all.accept_source_route=0
net.ipv6.conf.default.accept_source_route=0
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
net.ipv6.conf.all.forwarding=0
```

Figura 9-7: Fichero /etc/sysctl.conf después

- **Ssh Service**

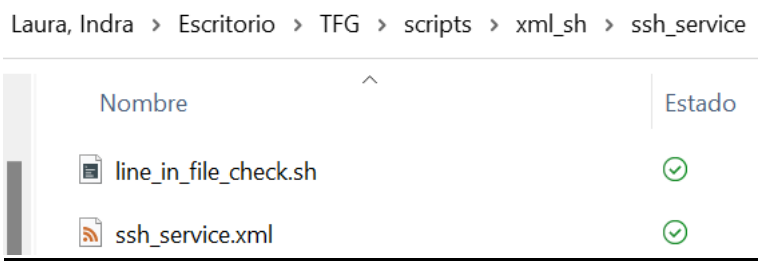


Figura 9-8: Directorio ssh_service

```
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication no
```

Figura 9-9: Fichero /etc/ssh/sshd_config antes

```
# Host *
#   ForwardAgent no
#   ForwardX11 no
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
#
# This system is following system-wide crypto policy.
# To modify the system-wide ssh configuration, create a  *.conf  file under
#  /etc/ssh/ssh_config.d/  which will be automatically included below
Include /etc/ssh/ssh_config.d/*.conf
```

Figura 9-10: Fichero /etc/ssh/ssh_config antes

```
[rocky@vm-rocky-3 laura]$ sh oscap_ansible.sh
W: oscap: Selector ID(no_direct_root_logins) does not exist in Benchmark and it will be ignored.
--- Starting Evaluation ---

Title   Tests if Protocol 2 is selected as SSH protocol
Rule    SSHd_protocol_usage
Result  fail

Title   Tests if Protocol 2 is selected as SSH protocol
Rule    SSH_protocol_usage
Result  fail

Title   Allow running graphical applications remotely via encrypted tunnel
Rule    X11Forwarding
Result  fail

Title   Limit the maximum time for accessing the system
Rule    LoginGraceTime
Result  fail
```

Figura 9-11: Check ssh_services

```
PLAY [all] *********************************************************

TASK [Gathering Facts] *********************************************
ok: [localhost]

TASK [Deduplicate values from /home/rocky/laura/sshd_config] ***********
ok: [localhost]

TASK [Insert correct line to /home/rocky/laura/sshd_config] ************
changed: [localhost]

TASK [Deduplicate values from /home/rocky/laura/ssh_config] ************
ok: [localhost]

TASK [Insert correct line to /home/rocky/laura/ssh_config] *************
changed: [localhost]

TASK [Deduplicate values from /home/rocky/laura/sshd_config] ***********
changed: [localhost]

TASK [Insert correct line to /home/rocky/laura/sshd_config] ************
changed: [localhost]

TASK [SSH LoginGraceTime] ******************************************
ok: [localhost]

TASK [Check for duplicate values] **********************************
ok: [localhost]

TASK [Deduplicate values from /home/rocky/laura/sshd_config] ***********
skipping: [localhost]
```

Figura 9-12: Fix ssh_services

```
Protocol 2
X11Forwarding yes
LoginGraceTime 120
PermitEmptyPasswords no
AllowUsers nor root installer
ClientAliveInterval 300
ClientAliveCountMax 0
HostbasedAuthentication no
IgnoreRhosts yes
PrintLastLog yes
PermitUserEnvironment no
StrictModes yes
Banner /etc/issue
GSSAPIAuthentication no
GSSAPICleanupCredentials yes
[rocky@vm-rocky-3 laura]$
```

Figura 9-13: Fichero /etc/ssh/sshd_config después

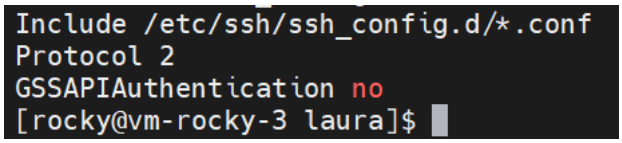


Figura 9-14: Fichero /etc/ssh/ssh_config después

- **Software Maintenance**

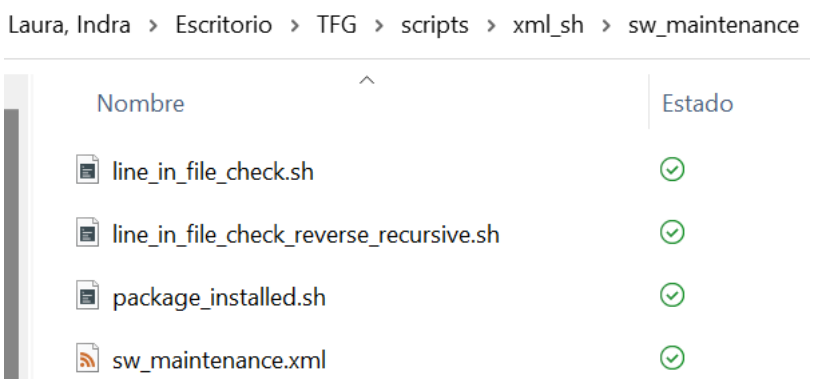


Figura 9-15: Directorio sw_maintenance

```
[rocky@vm-rocky-3 laura]$ sudo cat /etc/sysconfig/packagekit-background
cat: /etc/sysconfig/packagekit-background: No such file or directory
```

Figura 9-16: Fichero /etc/sysconfig/packagekit-background antes

```
[rocky@vm-rocky-3 laura]$ sudo cat /etc/yum.conf
[main]
gpgcheck=1
installonly_limit=3
clean_requirements_on_remove=True
best=True
skip_if_unavailable=False
proxy=http://proxy.indra.es:8080
[rocky@vm-rocky-3 laura]$
```

Figura 9-17: Fichero /etc/yum.conf antes

```
[rocky@vm-rocky-3 laura]$ cd /etc/yum.repos.d
[rocky@vm-rocky-3 yum.repos.d]$ ls
epel-modular.repo          Rocky-HighAvailability.repo
epel.repo                  Rocky-Media.repo
epel-testing-modular.repo  Rocky-NFV.repo
epel-testing.repo          Rocky-Plus.repo
Rocky-AppStream.repo       Rocky-PowerTools.repo
Rocky-BaseOS.repo          Rocky-ResilientStorage.repo
Rocky-Debuginfo.repo       Rocky-RT.repo
Rocky-Devel.repo           Rocky-Sources.repo
Rocky-Extras.repo
```

Figura 9-18: Directorio /etc/yum.repos.d

```
[rocky@vm-rocky-3 yum.repos.d]$ cd /etc/pki/rpm-gpg
[rocky@vm-rocky-3 rpm-gpg]$ ls
RPM-GPG-KEY-EPEL-8  RPM-GPG-KEY-rockyofficial  RPM-GPG-KEY-rockytesting
```

Figura 9-19: Directorio /etc/pki/rpm-gpg antes

```
[rocky@vm-rocky-3 etc]$ cd dnf
[rocky@vm-rocky-3 dnf]$ ls
aliases.d  dnf.conf  modules.d  modules.defaults.d  plugins  protected.d  vars
```

Figura 9-20: Directorio /etc/dnf antes

```
[rocky@vm-rocky-3 laura]$ sudo sh oscap_ansible.sh
--- Starting Evaluation ---

Title   Test if PakageKit packages are installed
Rule    PakageKit_Installed
Result  fail

Title   Test if Automatic sw updates are disabled
Rule    Automatic_sw_updates
Result  fail

Title   Test if the gpgcheck option is enabled in main yum configuration
Rule    Gpgcheck_in_main_yum_configuration
Result  fail

Title   Test to ensure signature checking is not disabled for any repos
Rule    Gpgcheck_Enabled_for_All_yum_Package_Repositories
Result  fail

Title   Test to ensure gpgcheck is enabled for local packages
Rule    Localpkg_Enabled_for_Local_Packages
Result  fail

Title   Test to ensure redhat gpgkey is installed
Rule    Red_Hat_GpgKey_Installed
Result  fail

Title   Test if dnf-automatic package is installed
Rule    Dnf-automatic_package_Installed
Result  fail
```

Figura 9-21: Check sw_maintenance

```
PLAY [all] *********************************************************************************

TASK [Gathering Facts] *********************************************************************
ok: [localhost]

TASK [Install a list of packages with a list variable] *************************************
changed: [localhost] => (item=PackageKit-cron)
ok: [localhost] => (item=PackageKit-yum)

TASK [Ensure ENABLED is set accordingly] ***************************************************
changed: [localhost]

TASK [Check existence of yum on Fedora] ****************************************************
skipping: [localhost]

TASK [Ensure GPG check is globally activated (yum)] ****************************************
ok: [localhost]

TASK [Ensure GPG check is globally activated (dnf)] ****************************************
skipping: [localhost]

TASK [Grep for yum repo section names] *****************************************************
ok: [localhost]

TASK [Set gpgcheck=1 for each yum repo] ****************************************************
ok: [localhost] => (item=['/etc/yum.repos.d/Rocky-AppStream.repo', 'appstream'])
ok: [localhost] => (item=['/etc/yum.repos.d/Rocky-BaseOS.repo', 'baseos'])
ok: [localhost] => (item=['/etc/yum.repos.d/Rocky-Debuginfo.repo', 'baseos-debug'])
ok: [localhost] => (item=['/etc/yum.repos.d/Rocky-Debuginfo.repo', 'appstream-debug'])
ok: [localhost] => (item=['/etc/yum.repos.d/Rocky-Debuginfo.repo', 'ha-debug'])
ok: [localhost] => (item=['/etc/yum.repos.d/Rocky-Debuginfo.repo', 'powertools-debug'])
ok: [localhost] => (item=['/etc/yum.repos.d/Rocky-Debuginfo.repo', 'resilient-storage-debug'])
ok: [localhost] => (item=['/etc/yum.repos.d/Rocky-Devel.repo', 'devel'])
```

Figura 9-22: Fix sw_maintenance

```
[rocky@vm-rocky-3 laura]$ cat /etc/sysconfig/packagekit-background
## Path:        System/Cron/PackageKit
## Description: Cron job to update the system daily with PackageKit

## Type:        yesno
## Default:     no
#
# Run the cron job.
#
ENABLED = no

## Type:        yesno
## Default:     no
#
# Check if updates are available, instead of installing.
#
CHECK_ONLY=no
```

Figura 9-23: Fichero /etc/sysconfig/packagekit-background después

```
[rocky@vm-rocky-3 laura]$ sudo cat /etc/yum.conf
[main]
gpgcheck=1
installonly_limit=3
clean_requirements_on_remove=True
best=True
skip_if_unavailable=False
proxy=http://proxy.indra.es:8080
localpkg_gpgcheck = 1
[rocky@vm-rocky-3 laura]$ sudo cat /etc/dnf/dnf.conf
[main]
gpgcheck=1
installonly_limit=3
clean_requirements_on_remove=True
best=True
skip_if_unavailable=False
proxy=http://proxy.indra.es:8080
localpkg_gpgcheck = 1
[rocky@vm-rocky-3 laura]$
```

Figura 9-24: Ficheros /etc/yum.conf y /etc/dnf/dnf.conf después

```
[rocky@vm-rocky-3 etc]$ cd dnf
[rocky@vm-rocky-3 dnf]$ ls
aliases.d  automatic.conf  dnf.conf  modules.d  modules.defaults.d  plugins  protected.d  vars
```

Figura 9-25: Directorio /etc/dnf después

```
[rocky@vm-rocky-3 laura]$ cat /etc/dnf/automatic.conf

[commands]
upgrade_type = security
apply_updates = yes
```

Figura 9-26: Fichero /etc/dnf/automatic.conf después

- **Users and Groups**

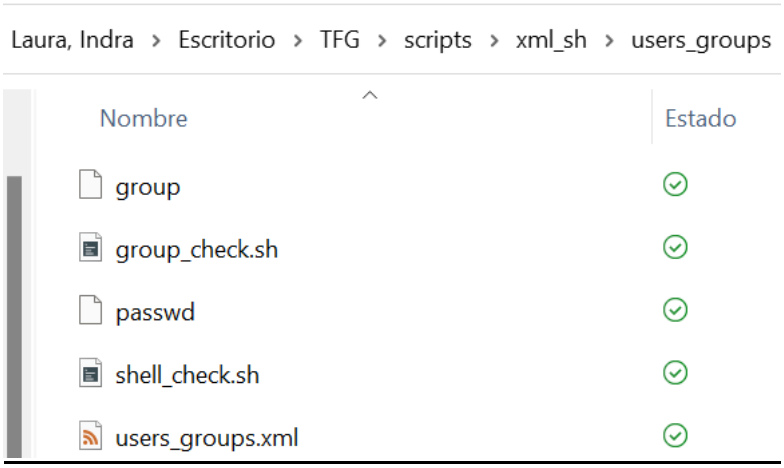


Figura 9-27: Directorio users_groups

```
root:x:0:0:root:/root:/bin/sh
bin:x:1:1:bin:/bin:/sbin/sh
daemon:x:2:2:daemon:/sbin:/sbin/sh
adm:x:3:4:adm:/var/adm:/sbin/sh
lp:x:4:7:lp:/var/spool/lpd:/sbin/sh
sync:x:5:0:sync:/sbin:/bin/sh
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/sh
mail:x:8:12:mail:/var/spool/mail:/sbin/sh
operator:x:11:0:operator:/root:/sbin/sh
games:x:12:100:games:/usr/games:/sbin/sh
ftp:x:14:50:FTP User:/var/ftp:/sbin/sh
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/sh
dbus:x:81:81:System message bus:/:/sbin/sh
```

Figura 9-28: Fichero /etc/passwd antes

```
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:rocky
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:
cdrom:x:11:
mail:x:12:
man:x:15:
```

Figura 9-29: Fichero /etc/group antes

```
[rocky@vm-rocky-3 laura]$ sudo sh oscap_ansible.sh
--- Starting Evaluation ---

Title   Check Root Shell
Rule    Root_Shell
Result  fail

Title   Check Bin Shell
Rule    Bin_Shell
Result  fail

Title   Check Daemon Shell
Rule    Daemon_Shell
Result  fail

Title   Check Adm Shell
Rule    Adm_Shell
Result  fail

Title   Check Lp Shell
Rule    Lp_Shell
Result  fail

Title   Check Sync Shell
Rule    Sync_Shell
Result  fail

Title   Check Shutdown Shell
Rule    Shutdown_Shell
Result  pass
```

Figura 9-30: Check users_groups

```
PLAY [all] *********************************************

TASK [Gathering Facts] *********************************
ok: [localhost]

TASK [Get line to change] ******************************
changed: [localhost]

TASK [debug] *******************************************
ok: [localhost] => {
    "msg": "root:x:0:0:root:/root:/bin/sh"
}

TASK [Split old line] **********************************
ok: [localhost]

TASK [replace bash] ************************************
changed: [localhost]

TASK [Get changed line] ********************************
changed: [localhost]

TASK [debug] *******************************************
ok: [localhost] => {
    "msg": "root:x:0:0:root:/root:/bin/bash"
}

TASK [Get line to change] ******************************
changed: [localhost]

TASK [debug] *******************************************
ok: [localhost] => {
```

Figura 9-31: Fix users_groups

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
```

Figura 9-32: Fichero /etc/passwd después

```
[rocky@vm-rocky-3 laura]$ cat /etc/group
root:x:0:
bin:x:1:bin,daemon
daemon:x:2:bin,daemon
sys:x:3:bin,adm
adm:x:4:adm,daemon
tty:x:5:
disk:x:6:
lp:x:7:daemon
mem:x:8:
kmem:x:9:
wheel:x:10:
cdrom:x:11:
mail:x:12:mail,postfix
uucp:x:15:
```

Figura 9-33: Fichero /etc/group después

- **Block No Root UID0**

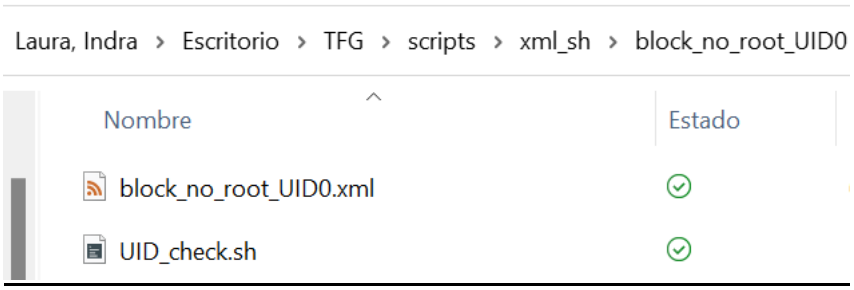


Figura 9-34: Directorio block_no_root_UID0

```
root:x:0:0:root:/root:/bin/bash
bin:x:0:1:bin:/bin:/sbin/nologin
daemon:x:0:2:daemon:/sbin:/sbin/nologin
adm:x:0:4:adm:/var/adm:/sbin/nologin
lp:x:0:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:0:0:sync:/sbin:/bin/sync
shutdown:x:0:0:shutdown:/sbin:/sbin/shutdown
halt:x:0:0:halt:/sbin:/sbin/halt
mail:x:0:12:mail:/var/spool/mail:/sbin/nologin
operator:x:0:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```

Figura 9-35: Fichero /etc/passwd antes

```
[rocky@vm-rocky-3 laura]$ sudo sh oscap_ansible.sh
--- Starting Evaluation ---

Title   Check /home/rocky/laura/passwd_check_fail UIDs
Rule    check_users_UID
Result  fail
```

Figura 9-36: Check block_no_root_UID0

```
PLAY [all] ***************************************

TASK [Gathering Facts] ***************************
ok: [localhost]

TASK [Get user with UID] *************************
changed: [localhost]

TASK [Set username] ******************************
ok: [localhost]

TASK [Set default UID] ***************************
ok: [localhost]

TASK [Check if UID is already in use] ************
changed: [localhost]

TASK [Find a UID that is not being used] *********
changed: [localhost] => (item=1000)
changed: [localhost] => (item=1001)
skipping: [localhost] => (item=1002)
skipping: [localhost] => (item=1003)
skipping: [localhost] => (item=1004)
skipping: [localhost] => (item=1005)
skipping: [localhost] => (item=1006)
```

Figura 9-37: Fix block_no_root_UID0

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
```

Figura 9-38: Fichero /etc/passwd después

- **File Permissions**

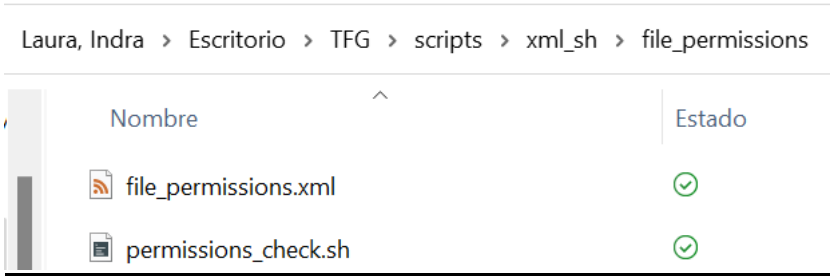


Figura 9-39: Directorio file_permissions

```
[rocky@vm-rocky-3 laura]$ ls -l /etc/group && ls -l /etc/passwd && ls -l /etc/s
hadow && ls -l /etc/gshadow && ls -l /etc/sysctl.conf
-rwxrwxrwx. 1 root root 679 Feb 21 10:31 /etc/group
-rwxrwxrwx. 1 root root 1632 Feb 20 20:13 /etc/passwd
-rwxrwxrwx. 1 root root 826 Feb 20 20:13 /etc/shadow
-rwxrwxrwx. 1 root root 677 Feb 21 10:31 /etc/gshadow
-rwxrwxrwx. 1 root root 1331 Mar  1 17:43 /etc/sysctl.conf
```

Figura 9-40: Permisos ficheros antes

```
[rocky@vm-rocky-3 laura]$ sudo sh oscap_ansible.sh
--- Starting Evaluation ---

Title   Check /etc/group permissions
Rule    group_permissions
Result  fail

Title   Check /etc/passwd permissions
Rule    passwd_permissions
Result  fail

Title   Check /etc/shadow permissions
Rule    shadow_permissions
Result  fail

Title   Check /etc/gshadow permissions
Rule    gshadow_permissions
Result  fail

Title   Check /etc/sysctl.conf permissions
Rule    sysctl.conf_permissions
Result  fail

Title   Check /bin/ping6 permissions
Rule    ping_permissions
Result  fail

Title   Check /usr/bin/chage permissions
Rule    chage_permissions
Result  pass
```

Figura 9-41: Check file_permissions

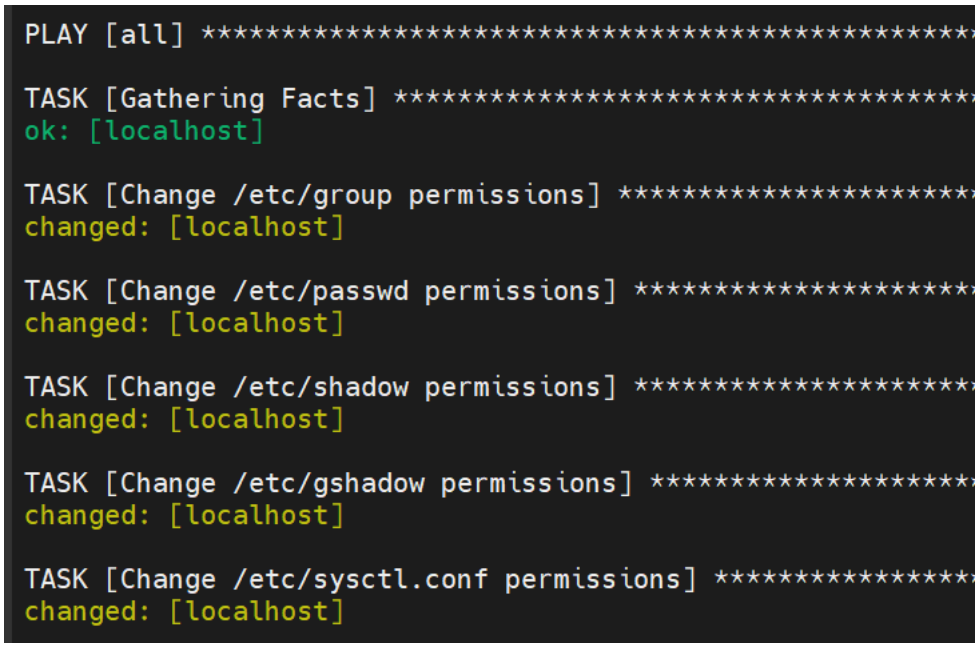


Figura 9-42: Fix file_permissions

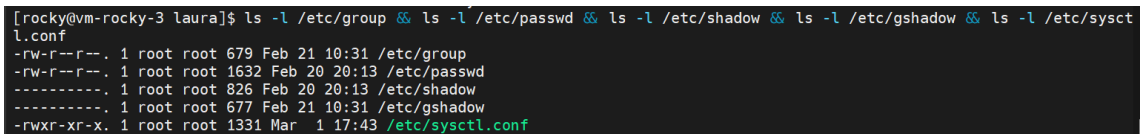


Figura 9-43: Permisos ficheros depués

- **Lock Ctrl + Alt + Sup/Del Usage**

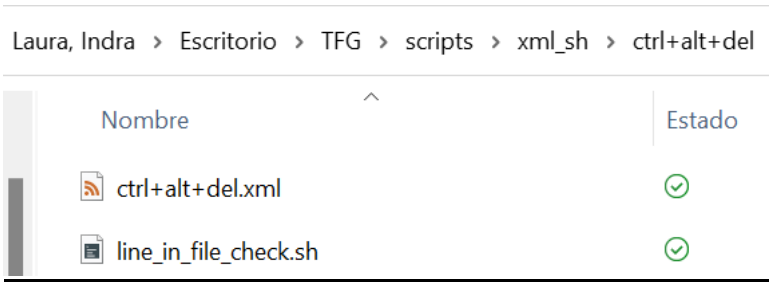


Figura 9-44: Directorio ctrl+alt+del

```
[rocky@vm-rocky-3 laura]$ cat /etc/systemd/system.conf
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See systemd-system.conf(5) for details.

[Manager]
#LogLevel=info
#LogTarget=journal-or-kmsg
#LogColor=yes
#LogLocation=no
#DumpCore=yes
#ShowStatus=yes
#CrashChangeVT=no
#CrashShell=no
#CrashReboot=no
#CtrlAltDelBurstAction=reboot-force
#CPUAffinity=1 2
#JoinControllers=cpu,cpuacct net_cls,net_prio
```

Figura 9-45: Fichero /etc/systemd/system.conf antes

```
--- Starting Evaluation ---

Title   Disable Ctrl-Alt-Del Burst Action
Rule    CtrlAltDelBurstAction
Result  fail
```

Figura 9-46: Check ctrl+alt+del

```
PLAY [all] ***************************************************

TASK [Gathering Facts] ***************************************
ok: [localhost]

TASK [Disable Ctrl-Alt-Del Burst Action] *********************
changed: [localhost]

TASK [Disable Ctrl-Alt-Del Reboot Activation] ****************
changed: [localhost]
```

Figura 9-47: Fix ctrl+alt+del

```
#DefaultLimitNPROC=
#DefaultLimitMEMLOCK=
#DefaultLimitLOCKS=
#DefaultLimitSIGPENDING=
#DefaultLimitMSGQUEUE=
#DefaultLimitNICE=
#DefaultLimitRTPRIO=
#DefaultLimitRTTIME=
#IPAddressAllow=
#IPAddressDeny=
CtrlAltDelBurstAction=none
[rocky@vm-rocky-3 laura]$
```

Figura 9-48: Fichero /etc/systemd/system.conf después

- **Password Requeriments**

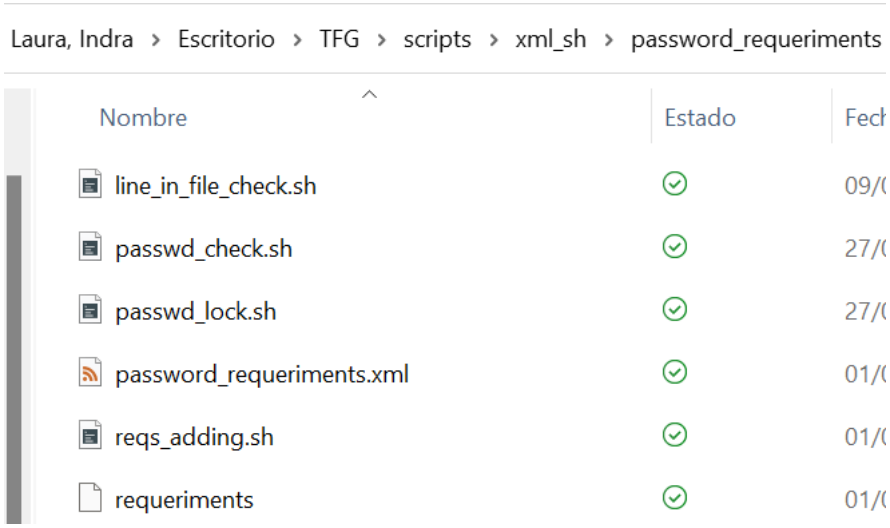


Figura 9-49: Directorio password_requeriments

```
[rocky@vm-rocky-3 laura]$ cat /usr/bin/passwd_reqs
cat: /usr/bin/passwd_reqs: No such file or directory
[rocky@vm-rocky-3 laura]$
```

Figura 9-50: Fichero /usr/bin/passwd_reqs antes

```
[rocky@vm-rocky-3 laura]$ cat /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
# minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 0
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 0
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = 0
```

Figura 9-51: Fichero /etc/security/pwquality.conf antes

```
[rocky@vm-rocky-3 laura]$ sudo sh oscap_ansible.sh
--- Starting Evaluation ---

Title   Test if there is some non set passwd
Rule    passwd_check
Result  pass

Title   Checks if passwd requirements are shown
Rule    passwd_requirements
Result  pass

Title   minimun uppercase characters (ucredit)
Rule    Minumun_Uppercase_Characters
Result  fail

Title   minimun lowercase characters (lcredit)
Rule    Minumun_Lowercase_Characters
Result  fail

Title   minimun digit characters (dcredit)
Rule    Minumun_Digit_Characters
Result  fail

Title   minimun special characters (ocredit)
Rule    Minumun_Special_Characters
Result  fail

Title   minimun length (minlen)
Rule    Minumun_Length
Result  fail
```

Figura 9-52: Check password_requeriments

```
PLAY [all] *********************************************

TASK [Gathering Facts] *********************************
ok: [localhost]

TASK [Ensure PAM variable ucredit is set accordingly] ******
changed: [localhost]

TASK [Ensure PAM variable lcredit is set accordingly] ******
changed: [localhost]

TASK [Ensure PAM variable dcredit is set accordingly] ******
changed: [localhost]

TASK [Ensure PAM variable ocredit is set accordingly] ******
changed: [localhost]

TASK [Ensure PAM variable minlen is set accordingly] *******
changed: [localhost]
```

Figura 9-53: Fix password_requeriments

```
[rocky@vm-rocky-3 laura]$ cat /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
dcredit = -2
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
ucredit = -1
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
lcredit = -1
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
ocredit = -1
#
```

Figura 9-54: Fichero /etc/security/pwquality.conf después

```
[rocky@vm-rocky-3 laura]$ cat /usr/bin/passwd_reqs
echo ' *****password requirements******* '
echo ' Number of days before password expires    90'
echo ' Number of days before password can be changed     1'
echo ' Limit the number of grace logins allowed  5'
echo ' Excluded password En route'
echo ' Excluded password NERL'
echo ' Excluded password Services'
echo ' Excluded password Traffic'
echo ' Excluded password Air'
echo ' Excluded password National'
echo ' Excluded password NATS'
echo ' Minimum number of characters in password  8'
echo ' Maximum number of times a specific character can be used  11'
echo ' Minimum number of numerals in password    2'
echo ' Minimum number of lower case characters required in password      1'
echo ' Minimum number of upper case characters required in password      1'
echo ' Minimum number of non-alphabetic characters       1'
echo ' Minimum number of non-alphanumeric characters     2'
/usr/bin/passwd '$1'
```

Figura 9-55: Fichero /usr/bin/passwd_reqs después

- **Set Banner**

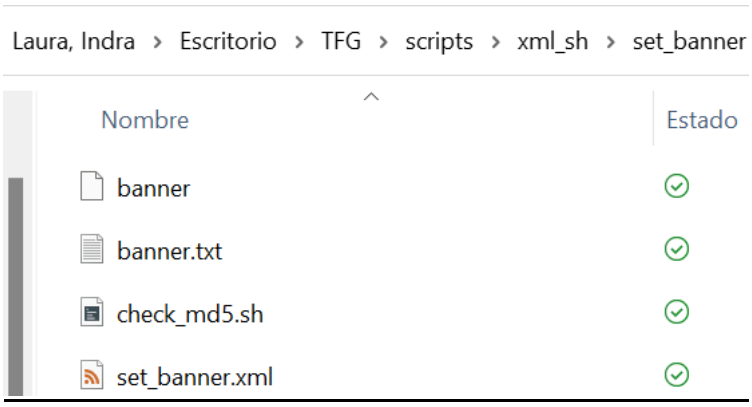


Figura 9-56: Directorio set_banner

Figura 9-57: Imagen banner

➢ Crypto Policies

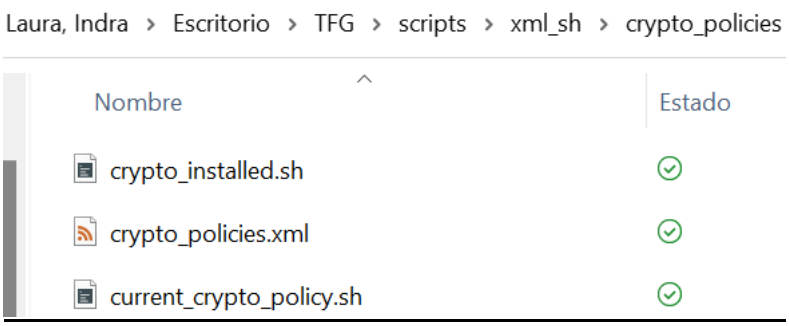


Figura 9-58: Directorio crypto_policies

```
[rocky@vm-rocky-3 crypto-policies]$ cat config
[rocky@vm-rocky-3 crypto-policies]$
```

Figura 9-59: Fichero /etc/crypto-policies/config antes

```
# Load default TLS policy configuration
openssl_conf = default_modules
[ default_modules ]
ssl_conf = ssl_module
[ ssl_module ]
system_default = crypto_policy
[ crypto_policy ]
.include /etc/crypto-policies/back-ends/opensslcnf.config
[ new_oids ]
```

Figura 9-60: Fichero /etc/pki/tls/openssl.cnf antes

```
[rocky@vm-rocky-3 laura]$ sudo sh oscap_ansible.sh
--- Starting Evaluation ---

Title   Test if crypto_policies package is installed
Rule    crypto_install
Result  pass

Title   Set policy to DEFAULT
Rule    crypto_policies_policy
Result  fail

Title   Enable default crypto policy for openssl
Rule    openssl_crypto
Result  fail
```

Figura 9-61: Check crypto-policies

```
PLAY [all] *********************************************************

TASK [Gathering Facts] *********************************************
ok: [localhost]

TASK [Configure System Cryptography Policy] ************************
changed: [localhost]

TASK [Test for crypto_policy group] ********************************
ok: [localhost]

TASK [Add .include for openssl.config to crypto_policy section] ****
changed: [localhost]

TASK [Add crypto_policy group and set include openssl.config] ******
skipping: [localhost]
```

Figura 9-62: Fix crypto-policies

```
[rocky@vm-rocky-3 crypto-policies]$ ls
back-ends  config  local.d  policies  state
[rocky@vm-rocky-3 crypto-policies]$ cat config

DEFAULT
[rocky@vm-rocky-3 crypto-policies]$
```

Figura 9-63: Fichero /etc/crypto-policies/config después

```
# Load default TLS policy configuration

openssl_conf = default_modules

[ default_modules ]

ssl_conf = ssl_module

[ ssl_module ]

system_default = crypto_policy

[ crypto_policy ]
.include /etc/crypto-policies/back-ends/openssl.config

.include /etc/crypto-policies/back-ends/opensslcnf.config

[ new_oids ]
```

Figura 9-64: Fichero /etc/pki/tls/openssl.cnf después

- **Audit**

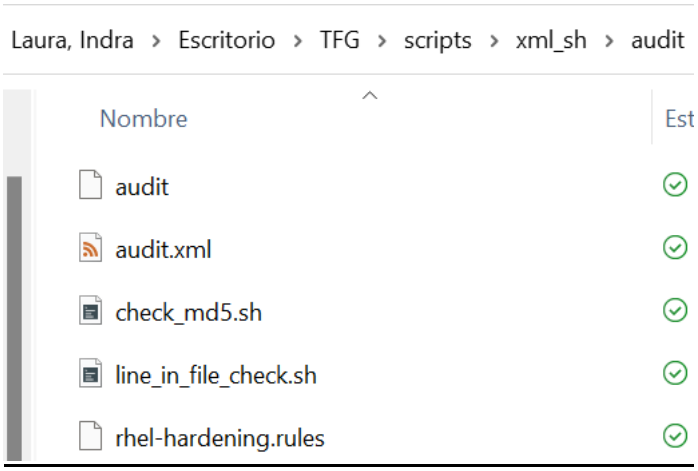


Figura 9-65: Directorio audit

NOTA: los ficheros *audit* y *rhel-hardening.rules* deben estar presentes en la misma carpeta en la cual ejecutaremos el *script*.

```
[root@vm-rocky-3 rules.d]# pwd
/etc/audit/rules.d
[root@vm-rocky-3 rules.d]# ls
audit.rules
[root@vm-rocky-3 rules.d]#
```

Figura 9-66: Fichero /etc/audit/rules.d/rhel-hardening.rules antes

```
[root@vm-rocky-3 audit]# cat auditd.conf
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
max_log_file = 8
num_logs = 5
priority_boost = 4
##name = mydomain
```

Figura 9-67: Fichero /etc/audit/auditd.conf antes

```
[root@vm-rocky-3 logrotate.d]# ls
btmp  chrony  dnf  kvm_stat  sssd  syslog  wtmp
[root@vm-rocky-3 logrotate.d]# pwd
/etc/logrotate.d
[root@vm-rocky-3 logrotate.d]#
```

Figura 9-68: Fichero /etc/logrotate.d/audit antes

```
[root@vm-rocky-3 laura]# sh oscap_ansible.sh
--- Starting Evaluation ---

Title   Write audit rules into new file
Rule    audit_rules
Result  fail

Title   Resolve information before writing to audit logs
Rule    audit_log_format
Result  fail

Title   Configure auditd flush priority
Rule    audit_flush
Result  fail

Title   Set hostname as computer node name in audit logs
Rule    audit_name_format
Result  pass

Title    Include Local Events in Audit Logs
Rule    audit_local_events
Result  pass

Title   Write Audit Logs to the Disk
Rule    audit_write_logs
Result  pass

Title   Set number of records to cause an explicit flush to audit logs
Rule    audit_freq
Result  fail
```

Figura 9-69: Check audit

```
PLAY [all] ********************************************************************

TASK [Gathering Facts] ********************************************************
ok: [localhost]

TASK [Copy contents of audit file] ********************************************
changed: [localhost]

TASK [Deduplicate values from /etc/audit/auditd.conf] *************************
ok: [localhost]

TASK [Insert correct line to /etc/audit/auditd.conf] **************************
changed: [localhost]

TASK [Configure auditd Flush Priority] ****************************************
changed: [localhost]

TASK [Deduplicate values from /etc/audit/auditd.conf] *************************
ok: [localhost]

TASK [Insert correct line to /etc/audit/auditd.conf] **************************
changed: [localhost]

TASK [Copy contents of audit file] ********************************************
changed: [localhost]
```

Figura 9-70: Fix audit

```
[root@vm-rocky-3 rules.d]# ls
audit.rules  rhel-hardening.rules
[root@vm-rocky-3 rules.d]# cat rhel-hardening.rules
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

## Successful ownership change
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-owner-c
hange
-a always,exit -F arch=b64 -S lchown,fchown,chown,fchownat -F success=1 -F auid>=1000 -F auid!=unset -F key=successful-owner-c
hange
```

Figura 9-71: Fichero /etc/audit/rules.d/rhel-hardening.rules después

```
[root@vm-rocky-3 audit]# cat auditd.conf
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
log_format = ENRICHED
flush = incremental_async
freq = 50
max_log_file = 8
```

Figura 9-72: Fichero /etc/audit/auditd.conf después

```
[root@vm-rocky-3 etc]# cd logrotate.d
[root@vm-rocky-3 logrotate.d]# ls
audit  btmp  chrony  dnf  kvm_stat  sssd  syslog  wtmp
[root@vm-rocky-3 logrotate.d]# cat audit
/var/log/audit/*.log {
        daily
        missingok
        rotate 14
        compress
        notifempty
        create 0640 root root
}
```

Figura 9-73: Fichero /etc/logrotate.d/audit después

- **Ldap PAM**

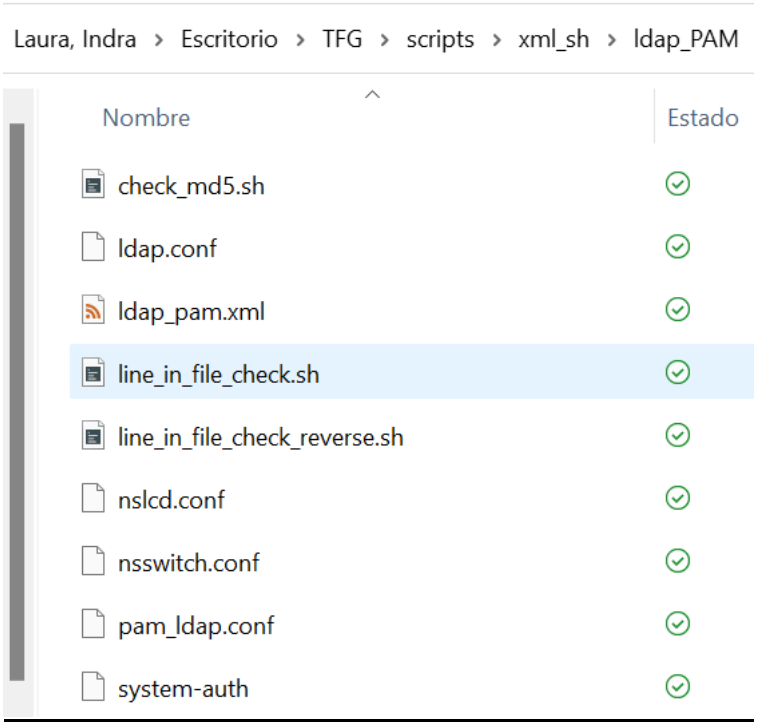


Figura 9-74: Directorio ldap_PAM

```
# Generated by authselect on Mon Feb 13 16:23:16 2023
# Do not modify this file manually.

auth        required                                     pam_env.so
auth        required                                     pam_faildelay.so delay=2000000
auth        [default=1 ignore=ignore success=ok]         pam_usertype.so isregular
auth        [default=1 ignore=ignore success=ok]         pam_localuser.so
auth        sufficient                                   pam_unix.so nullok try_first_pass
auth        [default=1 ignore=ignore success=ok]         pam_usertype.so isregular
auth        sufficient                                   pam_sss.so forward_pass
auth        required                                     pam_deny.so

account     required                                     pam_unix.so
account     sufficient                                   pam_localuser.so
account     sufficient                                   pam_usertype.so issystem
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required                                     pam_permit.so

password    requisite                                    pam_pwquality.so local_users_only
password    sufficient                                   pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    sufficient                                   pam_sss.so use_authtok
password    required                                     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type
=
password    required                                     pam_deny.so

session     optional                                     pam_keyinit.so revoke
session     required                                     pam_limits.so
-session    optional                                     pam_systemd.so
session     [success=1 default=ignore]                   pam_succeed_if.so service in crond quiet use_uid
session     required                                     pam_unix.so
session     optional                                     pam_sss.so
[rocky@vm-rocky-3 laura]$
```

Figura 9-75: Fichero /etc/pam.d/system-auth antes

```
# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is to use libldap's default behavior, which can be configured in
# /etc/openldap/ldap.conf using the TLS_REQCERT setting.  The default for
# OpenLDAP 2.0 and earlier is "no", for 2.1 and later is "yes".
#tls_checkpeer yes
TLS_REQCERT allow

# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
tls_cacertfile /etc/ssl/certs/cert.pem
tls_cacertdir /etc/ssl/certs

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
#tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key

# Disable SASL security layers. This is needed for AD.
#sasl_secprops maxssf=0

# Override the default Kerberos ticket cache location.
#krb5_ccname FILE:/etc/.ldapcache
```

Figura 9-76: Fichero /etc/ldap.conf antes

```
# Require and verify server certificate (yes/no)
# Default is to use libldap's default behavior, which can be configured in
# /etc/openldap/ldap.conf using the TLS_REQCERT setting.  The default for
# OpenLDAP 2.0 and earlier is "no", for 2.1 and later is "yes".
#tls_checkpeer yes
TLS_REQCERT allow

# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
tls_cacertfile /etc/ssl/certs/cert.pem
tls_cacertdir /etc/ssl/certs/

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
#tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key

# Disable SASL security layers. This is needed for AD.
#sasl_secprops maxssf=0

# Override the default Kerberos ticket cache location.
#krb5_ccname FILE:/etc/.ldapcache
#URI ldaps://10.70.45.10
BASE   o=NATS
```

Figura 9-77: Fichero /etc/openldap/ldap.conf antes

```
#pagesize 1000
#referrals off
#filter passwd (&(objectClass=user)(!(objectClass=computer))(uidNumber=*)(unixHomeDirectory=*))
#map    passwd uid              sAMAccountName
#map    passwd homeDirectory    unixHomeDirectory
#map    passwd gecos            displayName
#filter shadow (&(objectClass=user)(!(objectClass=computer))(uidNumber=*)(unixHomeDirectory=*))
#map    shadow uid              sAMAccountName
#map    shadow shadowLastChange pwdLastSet
#filter group  (objectClass=group)
#map    group  uniqueMember     member

# Mappings for AIX SecureWay
#filter passwd (objectClass=aixAccount)
#map    passwd uid              userName
#map    passwd userPassword     passwordChar
#map    passwd uidNumber        uid
#map    passwd gidNumber        gid
#filter group  (objectClass=aixAccessGroup)
#map    group  cn               groupName
#map    group  uniqueMember     member
#map    group  gidNumber        gid
uid nslcd
gid ldap
# This comment prevents repeated auto-migration of settings.
# uri ldap://X.X.X.X ldap://X.X.X.X
base o=NATS
scope sub
ssl start_tls
tls_cacertfile /etc/ssl/certs/cert.pem
tls_cacertdir /etc/ssl/certs
```

Figura 9-78: Fichero /etc/nslcd.conf antes

```
# For more information, please read the nsswitch.conf.5 manual page.
#

passwd:  files systemd
shadow: files
group:  files systemd

#passwd:        compat
#group: files ldap

hosts:  files dns myhostname
networks:       files dns

services:       files
protocols:      files
rpc:    files
ethers: files
netmasks:       files
netgroup:       files
publickey:      files

bootparams:     files
automount:      files nis
aliases:        files
#passwd_compat:  ldap
```

Figura 9-79: Fichero /etc/nsswitch.conf antes

```
[rocky@vm-rocky-3 laura]$ sudo sh oscap_ansible.sh
--- Starting Evaluation ---

Title   Check if nullok in pam_unix.so line
Rule    check_nullok_pam_unix.so
Result  notchecked

Title   Check if pam_pwquality.so line exists
Rule    checkif_pam_pwquality.so_line_exists
Result  pass

Title   Check if nullok in pam_unix.so line
Rule    check_nullok_pam_unix.so2
Result  notchecked

Title   Check if pam_succeed_if.so line exists
Rule    check_if_pam_suceed.so_line_exists
Result  pass

Title   Look for the name of the search base
Rule    base_o_ldap
Result  pass

Title   Name to bind to the server with
Rule    rootbindn_ldap
Result  pass

Title   Specify port for ldap
Rule    ldap_port_ldap
Result  pass
```

Figura 9-80: Check ldap_pam

```
PLAY [all] *********************************

TASK [Gathering Facts] *********************
ok: [localhost]
```

Figura 9-81: Fix ldap_pam

9.2. Linux_system_hardening

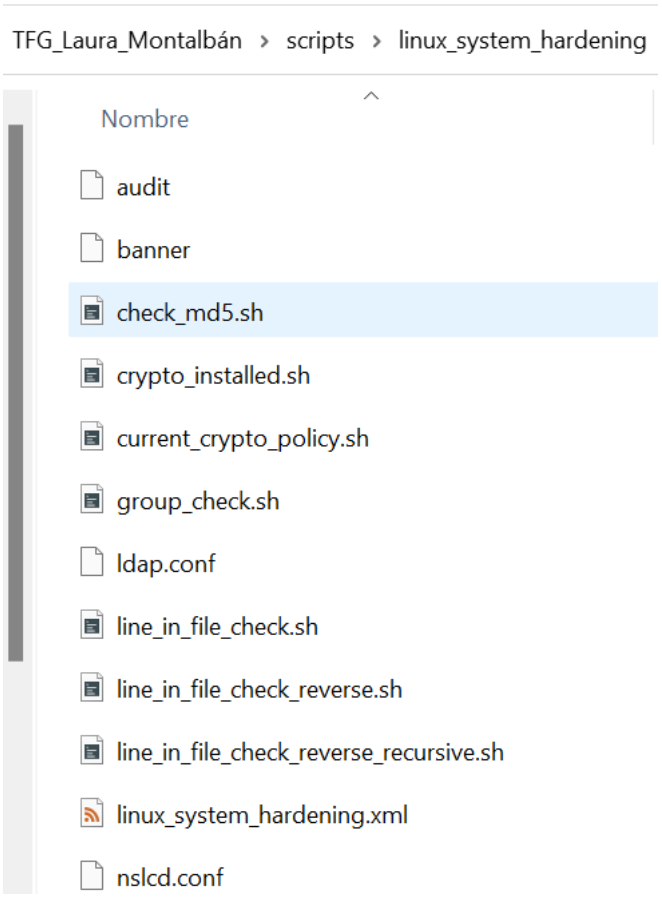


Figura 9-82: Directorio linux_system_hardening

CAPÍTULO 10. CONCLUSIONES

Como mejora futura se contempla la realización de la auditoria de cumplimiento de forma remota.

El proceso para seguir es el siguiente:

[1] Trabajar con privilegios de root.

sudo su

[2] Exportar la variable del entorno para especificar la clave privada de acceso a la máquina remota.

El path en la máquina rocky sería: */home/rocky/CyberRange-key.pem*.

export SSH_ADDITIONAL_OPTIONS="-i <path/to/key/.pem>"

[3] Ejecutar el escaneo.

oscap-ssh --sudo <user>@<ip> 22 xccdf eval --profile <profile> --results results.xml --report report.html --local-files <path/to/directory> script.xml

Local files es la ruta de la carpeta donde se encuentran los scripts *.sh* de comprobación.

CAPÍTULO 11. BIBLIOGRAFÍA

[1] *Contrato NATS con Indra*. Indracompany.com. <https://www.indracompany.com/es/noticia/nats-adjudica-importante-contrato-indra-afrontar-proximo-hito-itec>

[2] *NIST National Checklist for Red Hat Enterprise Linux 8.x*. NIST. <https://ncp.nist.gov/checklist/909/download/6089>

[3] *Security Hardening*. RHEL8. <https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/8/html/security_hardening/index>

[4] *Perfilado de Seguridad Red Hat Enterprise Linux 9*.0. CCN-CERT.cni.es. <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6768-ccn-stic-610a22-perfilado-de-seguridad-red-hat-enterprise-linux-9-0/file.html>

[5] *Herramientas para la audición de la seguridad*. Linux Adictos. <https://www.linuxadictos.com/openscap-herramientas-seguridad-linux.html>

[6] *Oscap – man pages section 8: System Administration Commands*. Oracle. <https://docs.oracle.com/cd/E88353_01/html/E72487/oscap-8.html>

[7] *Red Hat Ansible Automation Platform*. Red Hat. <https://www.redhat.com/es/technologies/management/ansible>

[8] *How Ansible Works?.* Ansible. <https://www.ansible.com/overview/how-ansible-works>

[9] *Script Check Engine*. OpenSCAP. <https://www.open-scap.org/features/other-standards/sce/>

[10] *Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2*. NIST. <https://csrc.nist.gov/CSRC/media/Publications/nistir/7275/rev-4/final/documents/nistir-7275r4_updated-march-2012_clean.pdf>

[11] *How can I verify that a PKG key is imported into RPM*. Stack Exchange Unix. <https://unix.stackexchange.com/questions/21226/how-can-i-verify-that-a-pgp-key-is-imported-into-rpm>

[12] *Ansible documentation*. Documentación de Ansible. <https://docs.ansible.com/ansible/latest/collections/ansible/builtin/>

[13] *Using Special Characters in XML*. Oracle. <https://docs.oracle.com/cd/A97335_02/apps.102/bc4j/developing_bc_projects/obcCustomXml.htm>

[14] *Red Hat Enterprise Linux 8. Uso de SELinux*. Red Hat. <https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/8/pdf/using_selinux/red_hat_enterprise_linux-8-using_selinux-es-es.pdf>

[15] *Aprende SELinux coloreando*. Red Hat. <https://people.redhat.com/duffy/selinux/selinux-coloring-book_A4-Stapled.pdf>

[16] *Trabajos Fin de Grado Uva*. Inf5g. <http://www.inf5g.uva.es/node/150>

[17] *Características HP EliteBook 640 G9.* PC Components. <https://www.pccomponentes.com/hp-elitebook-640-g9-intel-core-i7-1255u-16gb-256gb-ssd-14?gclid=EAIaIQobChMIm82S7KDF_QIV7hcGAB1t_AXxEAAYASAAEgICcPD_BwE>

CAPÍTULO 12. TABLA DE FIGURAS