ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE HARDENING EN SISTEMAS OPERATIVOS DE SERVIDOR

IMPLEMENTACIÓN DE *HARDENING* EN UN SISTEMA OPERATIVO DE SERVIDOR *LINUX* DE BASE RED HAT

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO SUPERIOR EN REDES Y TELECOMUNICACIONES

JESSICA CRISTINA TOAPANTA ROCHA

jessica.toapanta@epn.edu.ec

DIRECTOR: GABRIELA KATHERINE CEVALLOS SALAZAR

gabriela.cevalloss@epn.edu.ec

DMQ, agosto 2023

CERTIFICACIONES

Yo, JESSICA CRISTINA TAOAPANTA ROCHA declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

JESSICA CRISTINA TAOAPANTA ROCHA

jessica.toapanta@epn.edu.ec

jessicatoapanta15@hotmail.com

Certifico que el presente trabajo de integración curricular fue desarrollado por JESSICA CRISTINA TAOAPANTA ROCHA, bajo mi supervisión.

GABRIELA KATHERINE CEVALLOS SALAZAR

DIRECTOR

gabriela.cevalloss@epn.edu.ec

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

JESSICA CRISTINA TAOAPANTA ROCHA

DEDICATORIA

Este trabajo está dirigido a toda mi familia que fue parte fundamental en el proceso de convertirme en una profesional. A mis padres por siempre estar a mi lado y apoyarme económica y afectivamente para alcanzar este objetivo.

JESSICA CRISTINA TAOAPANTA ROCHA

AGRADECIMIENTO

Agradezco a la Escuela de Formación de Tecnólogos por ayudarme en mi formación académica y personal para lograr mis objetivos en el área profesional.

A todas las personas que influyeron en mi desarrollo y me ayudaron a culminar esta etapa de mi vida.

JESSICA CRISTINA TAOAPANTA ROCHA

ÍNDICE DE CONTENIDOS

RESUMEN

A medida que la tecnología avanza, surgen dificultades asociadas con la privacidad de la información y ciberseguridad. El incremento de ataques y amenazas a los sistemas informáticos y a la privacidad de los datos son aspectos importantes que son estudiados en la actualidad. Para lo cual se plantea el presente proyecto, el cual consta de las siguientes secciones:

La primera sección se define el enfoque del problema, los propósitos del proyecto, el alcance y la investigación de temas como la seguridad de la información, el *hardening*, herramientas de escaneo en base al protocolo SCAP y marcos de ciberseguridad.

La segunda sección corresponde a la exposición de la metodología de la investigación, además, se explica de manera concisa lo que se conseguirá con cada uno de los objetivos planteados.

La sección tres corresponde a la identificación de vulnerabilidades en Alma *Linux* sin políticas de seguridad. Luego, se implementa la política de seguridad NIST en Alma *Linux*. Esto con el fin de analizar los reportes de escaneo de la ejecución de la herramienta de escaneo SCAP *Workbench.* Por consiguiente*,* verificar el *hardening* del sistema operativo en base a los elementos de la triada CIA (*Confidentiality, Integrity, Availability)*.

La cuarta sección corresponde a las conclusiones que se obtuvo en base al cumplimento de los objetivos planteados.

La quinta sección corresponde a recomendaciones con respecto al desarrollo del proyecto.

Finalmente se tiene la sección de bibliografía que sustenta la información presentada en el desarrollo del proyecto.

PALABRAS CLAVE: *Hardening*, Seguridad de la información, NIST, SCAP *Workbench*, Triada CIA.

ABSTRACT

As technology advances, there are difficulties associates with information privacy and cybersecurity. The increase of attacks and threats to computer systems and data privacy are important aspects that are currently being studied. For which, the present project is proposed, this is project consists of the following sections:

The first section defines the approach to the problem, the purposes of the project, the scope and the investigation of topic such as information security, hardening, scanning tools based on SCAP protocol and cybersecurity frameworks.

The second section describes the methodology of research, also the way in which each objective is achieved.

The third section corresponds to the identification of vulnerabilities in Alma Linux without security policies. Then, implement the NIST (National Institute of Standards and Technology) security policy on Alma Linux. Then, analyze scan reports of the scanning tool SCAP Workbench. Subsequently, verify the hardening of the operating system based on the elements of the CIA triad (*Confidentiality, Integrity, Availability).*

The fourth section corresponds to the conclusions based on the achievement of the objectives.

The fifth section corresponds to the recommendations based on the development of the project.

Finally, this is the bibliography that supports the information of this project.

KEYWORDS: *Hardening, Information Security, NIST, SCAP Workbench, Triada CIA.*

1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

El presente proyecto radica en implementar un proceso de *hardening* en sistemas operativos de servidor, aplicando una política de seguridad basado en un marco de referencia. Con esto se asegura al sistema operativo de servidor, reduciendo significativamente la superficie de ataques, disminuyendo los puntos donde un atacante pueda infiltrarse.

Se tiene un sistema operativo de servidor con un servidor de correo electrónico, se escaneará el mismo mediante una herramienta de escaneo de configuración y vulnerabilidades basada en el protocolo SCAP, donde se obtendrá un reporte inicial el cual será comparado con un reporte luego de aplicar una política de seguridad. Este análisis determinará si las reglas especificadas por la política se han cumplido y se ha mejorado la seguridad del sistema operativo.

1.1 OBJETIVO GENERAL

Implementar *hardening* en sistemas operativos de servidor.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar las vulnerabilidades en un sistema operativo de servidor sin seguridad.
- Implementar una política de seguridad en un sistema operativo de servidor.
- Analizar los reportes, resultado de la aplicación de la herramienta de escaneo.
- Verificar el *hardening* del sistema operativo con base en los elementos de la triada CIA.

1.3 ALCANCE

En primera instancia se investigarán herramientas de escaneo, configuración y vulnerabilidades, basados en el protocolo SCAP. Partiendo de esto, se instalará un sistema operativo de servidor con un servidor de correo, sin ninguna política de

seguridad; con la herramienta de escaneo se procede a obtener un primer informe de vulnerabilidades. Luego se implementará una política de seguridad en el sistema operativo de servidor con el fin de obtener una mejora en el reporte de vulnerabilidades obtenido de la herramienta de escaneo, se procede a levantar un servidor de correo en el sistema operativo endurecido. Se compararán los reportes para observar cuáles parámetros críticos se han solventado según el manual de buenas prácticas de seguridad emitido por organizaciones de estandarización en esta área.

Se realizará una guía que resuma las mejoras prácticas, con esto se implementa *hardening* en un sistema operativo de servidor, reduciendo la superficie de ataques y por ende mitigando las debilidades que puedan ser aprovechadas por intrusos locales o remotos.

1.4 MARCO TEÓRICO

SEGURIDAD DE LA INFORMACIÓN

Se describe como un mecanismo para la protección y el buen funcionamiento de la transmisión de la información a través de métodos automatizados que prevé fugas, fallas, violación o alteración de esta.

Según la (*International Organization for Standardization*) ISO 27001.2005, define a la seguridad de la información como la garantía de salvaguardar la información transmitida por diferentes medios, preservando cada uno de los principios fundamentales de información, los cuales son la confidencialidad, integridad y disponibilidad. Según (*Information Technology Infrastructure Library*) ITIL v3 la seguridad de la información viene a ser un proceso de aseguramiento de los elementos de la triada CIA [1].

Existen 3 pilares fundamentales con respecto a la seguridad de la información, se conoce como el triángulo de la CIA que son: Confidencialidad, Integridad y Disponibilidad. A continuación, se detalla cada uno de estos pilares.

Disponibilidad: hace referencia a la disposición permanente o accesibilidad de la información para los usuarios autorizados. Varios tipos de ataques pueden afectar

la disponibilidad de la información, debido a que estos pueden interrumpir, limitar o denegar el acceso a la misma [2]. Algunos de estos ataques son:

- Ataque de denegación de servicio DoS (Denial of Service): estos ataques tienen como fin colapsar o inundar la red o un sistema mediante una gran cantidad de peticiones a una propiedad web haciendo que sea inaccesible para los usuarios [3].
- Ataque de denegación de servicio distribuido DDoS (Distributed Denial of Service): este ataque es similar al ataque DoS, sin embargo, en DDoS se involucra una red de computadoras que se encuentran distribuidas en diferentes ubicaciones haciendo que la interrupción del servicio sea aún más significante [4].

Para la prevención de estos ataques de debe aplicar ciertas medidas de seguridad como:

- Implementar un sistema de filtrado en el enrutador para la gestión de direcciones IP.
- Realizar configuraciones de red de tal manera que solo permita el acceso de tráfico autorizado.
- Desactivar servicios de red que no sean necesarios.
- Actualizar el antivirus de forma regular.
- Establecer políticas de contraseña de nivel alto y seguro.
- Utilizar herramientas de filtrado de acceso a la red para el control de conexiones remotas.

Confidencialidad: hace referencia a asegurar la información que se transmite para que solo puedan acceder, a la misma, personas autorizadas. En este tema se pueden presentar ataques que comprometan la confidencialidad de la información [2]. Estos ataques son los siguientes:

- Ataque *Man In The Middle*: ocurre cuando un atacante se inserta en una comunicación entre dos sistemas y altera o modifica la información que se transmite entre ellos [5].
- Ataque de *Phishing*: la temática de este ataque es por medio de envíos de correos eléctricos o mensajes falsos que aparentan ser confiables, este tipo de ataque intenta obtener información sensible, como contraseñas, nombres de usuario, numeros de cuenta bancaria y tarjetas de débito y crédito [5].
- Ataque de ingeniería social: los atacantes manipulan y engañan a los usuarios para obtener acceso a datos privados en especial información bancaria. Los atacantes lo utilizan ya que generalmente es más fácil engañar y *hackear* [5].
- Ataque de *ransomware*: los atacantes cifran los datos confidenciales de una organización o empresa y exigen un rescate para desbloquearlos. Si no se paga por el rescate de la información esta puede llegar a divulgarse o ser eliminada [5].

Para prevenir este tipo de ataques es importante implementar medidas de seguridad como:

- Cifrado de datos.
- Doble autenticación.
- Capacitación en la concienciación de la ciberseguridad.
- Auditorías regulares para proteger la confidencialidad de la información.

Integridad: Consiste en no realizar ninguna modificación a la información por personas que no están autorizadas, asegurando la integridad [2]. Existen varios tipos de ataques que puede comprometer la integridad de la información, estos son: Ataque de *ransomware*, Ataque *Man In The Middle*, estos ataques ya fueron expuestos anteriormente. Otro ataque involucrado es el Ataque de inyección SQL el cual consiste en insertar código malicioso en una aplicación o sistema con el objetivo de alterar su comportamiento y modificar la base de datos del sistema o aplicación [5].

Es importante implementar medidas de prevención para la integridad de la información y estas medidas son las siguientes:

- Validación de datos de entrada.
- Implementar un Sistema de Detección de Intrusiones IDS (Intrusion Detection System).
- Realizar copias de seguridad del sistema.

HARDENING

El *hardening* consiste en una serie de técnicas o herramientas que mejoran la seguridad reduciendo las vulnerabilidades que se han detectado. El fin principal es minorar los riesgos de vulnerabilidad que se presentan [6].

Hardening en sistemas operativos

Es un método o proceso de endurecimiento de un sistema el cual consiste en aplicar configuraciones y políticas de seguridad al sistema operativo para asegurarlo y protegerlo de ataques informáticos, disminuyendo vulnerabilidades del sistema. Algunas medidas que se deben seguir para la mantener un sistema operativo más seguro son las siguientes [7]:

- Deshabilitar servicios innecesarios.
- Establecer políticas de contraseñas seguras.
- Configuración de *firewall*.
- Aplicar parches de seguridad.
- Cerrar puertos que se encuentren en desuso.
- Utilizar *backups* como respaldo de datos importantes.
- Desinstalar *softwares* innecesarios.

Hardening en aplicaciones

Es un proceso de seguridad que implica tomar medidas de seguridad específicas para mejorar la capacidad de una aplicación y resistir ante los ataques informáticos

que se presenten [8]. Algunas de las medidas utilizadas en el *hardening* de aplicaciones son:

- Autenticación y autorización.
- Validación de datos de entrada.
- Aplicar controles de acceso.
- Establecer permisos adecuados para archivos.

Hardening de dispositivos de red

Consiste en fortalecer la seguridad de los dispositivos como *routers, switches*, *firewall* y servidores, el cual se aplican configuraciones adecuadas a cada dispositivo [9]. Esto puede incluir medidas de seguridad como:

- Cambiar contraseñas predeterminadas.
- Deshabilitar puertos y servicios no utilizados.
- Utilizar doble autenticación o una autenticación fuerte para el acceso remoto.

Hardening de base de datos

Este tipo de *hardening* implementa configuraciones y parámetros de seguridad en la base de dato, esto con lleva a la ejecución de parches y actualizaciones, autenticación robusta para el acceso remoto, encriptación de datos sensible, configuración de permisos y auditorias periódicas [10].

SISTEMAS OPERATIVOS DE SERVIDOR

Sistema operativo de servidor está diseñado para desempeñar específicamente funciones de servidor. Este sistema operativo de servidor dispone de atributos y funcionalidades necesarias para trabajar dentro de una arquitectura cliente-servidor [7].

Las distribuciones de servidor basados en *Red Hat* están optimizados para entornos de red que ofrecen características y funcionalidades mejoradas para el despliegue y administración de servidores en infraestructuras empresariales. Algunos de los sistemas operativos de servidor de base en *Red Hat* son los siguientes:

Alma *Linux*

Es un sistema *Open Source,* se maneja de forma gratuita [6]. Alma Linux fue creado en referencia al código de *Red Hat Enterprise Linux* y es cien por ciento compatible con los paquetes de *Red Hat Enterprise Linux* (RHEL). La finalidad de Alma Linux es proporcionar un sistema operativo seguro, de calidad y estable.

Alma Linux fue creado posteriormente a que Centos se descontinuara, por lo que la empresa *CloudLinux* anunció el nuevo sistema operativo Alma Linux en reemplazo de Centos.

Alma Linux dispone de la alternativa de instalación de servidor con interfaz gráfica (GUI), esta alternativa hace que sea más eficaz y eficiente el manejo del sistema operativo, además brinda una mejor experiencia al usuario.

Para la instalación de Alma *Linux* versión 9 se necesita de los siguientes requerimientos mínimos [11]:

Unidad flash USB: 12 (GB)

Memoria RAM: 1.5 (GB)

Procesador: Doble núcleo de 1 (GHz)

Espacio libre en disco duro: 20 (GB)

Red Hat Enterprise Linux (RHEL)

Plataforma *Linux* dedicada para el ámbito empresarial. RHEL se conecta con el entorno de la nube, además incluye servicio de soporte permanente, pero bajo una suscripción de paga. La última versión de *Red Hat* es RHEL9, esta última versión es compatible con las anteriores versiones en un rango de 10 años.

La arquitectura de *Red Hat Enterprise Linux* es compatible con otras arquitecturas de *hardware* como las siguientes: IBM Z, X86, ARM. Además, ofrece una plataforma segura en entornos de implementaciones físicas, virtuales y de nube. Las características mínimas para la configuración e instalación de RHEL9 son [12]:

Unidad flash USB: *Red Hat* no admite la instalación en unidades USB o tarjetas de memoria SD.

Memoria RAM: 1.5 (GB)

Procesador: de 64 bits con al menos 1.5 (GHz)

Espacio libre en disco duro: 10 (GB)

Centos

Distribución de código abierto basado en RHEL. En el ámbito empresarial de TI es uno de los sistemas operativos de servidor más utilizados. Ofrece características y funcionalidades similares a RHEL, pero sin los costos asociados con la suscripción de soporte. La versión Centos7 es compatible con las anteriores versiones, la versión Centos8 es descontinuada por lo que no es compatible con otras versiones. Es compatible con las siguientes arquitecturas i386. X86_64, ia64, Alpha, entre otras.

Los requisitos mínimos recomendables para la instalación de Centos 8 son [13]:

Memoria RAM: 2 (GB)

Procesador: de 64 bits con al menos 2 (GHz)

Espacio libre en disco duro: 20 (GB)

Rocky *Linux*

Sistema operativo gratuito, 100% compatible con RHEL, proporciona una sólida estabilidad con actualizaciones periódicas con un soporte de 10 años sin ningún costo. La última versión es Rocky *Linux* es 9.1 es compatible para las arquitecturas x86.64, ARM64 e IBMZ. Para la instalación de Rocky 9 se requiere mínimo [14]:

Unidad USB: 16 (GB)

Memoria RAM: 2 (GB)

Procesador: 1.1 (GHz)

Espacio libre en disco duro: 15 (GB)

HERRAMIENTAS DE ESCANEO

El objetivo principal de una herramienta de escaneo de vulnerabilidades y configuraciones para sistemas operativos de servidor Linux es detectar vulnerabilidades y configuraciones inseguras en el sistema. Las herramientas de escaneo de vulnerabilidades examinan a fondo el sistema de forma remota o local,

en busca de errores de configuración o de posibles puntos de entrada para atacantes [15].

Los principales objetivos de estas herramientas son:

- Identificación de vulnerabilidades: Se escanea el sistema en busca de *software* instalado, en la cual se identifican problemas como brechas de inseguridad, puertos abiertos no deseados y configuraciones inseguras.
- Evaluación de configuraciones: Verifica las configuraciones del sistema operativo y explora los fallos o errores que puedan exponer la seguridad del sistema, como los permisos insuficientes y contraseñas débiles.
- Análisis de cumplimiento: Determina si el sistema cumple las normas de seguridad, como las recomendaciones establecidas por los marcos de ciberseguridad como NIST, CIS u otros marcos. Estos contribuyen a garantizar que el sistema este configurado de acuerdo con las mejores prácticas de seguridad.
- Elaboración de informes: Generan informes que detallan las vulnerabilidades identificadas, el nivel de gravedad, sugerencias y referencias a recursos adicionales para la solución de las vulnerabilidades detectadas [16].

Protocolo SCAP

El Protocolo de Configuración Automatizada de Seguridad (SCAP) es un estándar ampliamente utilizado para evaluar y medir la seguridad de los sistemas de TI. Existen varias herramientas de escaneo de vulnerabilidades basadas en el protocolo SCAP. Estas herramientas son las siguientes:

SCAP *Workbench*

Es una herramienta que dispone de una interfaz gráfica para el escaneo de vulnerabilidades basado en el protocolo SCAP. Permite elegir diferentes perfiles de seguridad y generar informes con resultados detallados en varios formatos. SCAP *Workbench* permite realizar escaneos de manera remota o local, emplea el archivo XCCDF para la reparación del sistema ante las vulnerabilidades detectadas [11].

OpenSCAP

Es una herramienta que se basa en lineamientos o normas del estándar SCAP. Permite escanear y evaluar la configuración de seguridad de los sistemas operativos de servidor y generar informes basados en los resultados obtenidos.

Red Hat Security Data API

Es una API proporcionada por *Red Hat* que accede a la información y los datos SCAP de los sistemas operativos de servidor basados en *Red Hat*. Puede utilizarse para automatizar el escaneo de vulnerabilidades y realizar evaluaciones de seguridad [17]. Proporciona ayuda a profesionales de la tecnología para mantener sus sistemas actualizados y protegidos.

Nessus SCAP *Plugin*

Nessus es una herramienta de escaneo de vulnerabilidades la cual ofrece un *plugin* que permite realizar escaneos basados en SCAP. Esta herramienta ofrece una forma estandarizada y automatizada de evaluar la seguridad de los sistemas operativos. Detecta configuraciones inseguras, compara con los perfiles de seguridad definidos y genera informes que facilitan la identificación y corrección de vulnerabilidades [18].

MARCOS DE CIBERSEGURIDAD

Es un conjunto de procesos documentados que establecen políticas de seguridad en la ejecución y administración de la seguridad de la información. Estos marcos referente a la ciberseguridad constituyen una normativa para administrar el riesgo y la exposición a vulnerabilidades, amenazas [19]. A continuación, se expone detalles importantes de cada uno de los marcos de ciberseguridad empleados en la actualidad.

NIST (*National Institute of Standards and Technology*)

Agencia perteneciente al Departamento de Comercio de los Estados Unidos, promueve y desarrolla normativas y directrices en la seguridad de la información. NIST ha desarrollado el "Marco de Ciberseguridad NIST" que proporciona una estructura basada en mejores prácticas para gestionar y mitigar los riesgos de ciberseguridad.

El marco de NIST se enfoca en la identificación, protección y recuperación de las plataformas de información de una institución. Proporciona una estructura flexible y adaptable que puede ser aplicada a organizaciones de diferentes sectores económicos [20].

CIS *(Center for Internet Security)*

CIS desarrolla y mantiene una serie de controles de seguridad conocidos como las "CIS *Controls*". Estos controles son un conjunto de prácticas recomendadas y medidas de seguridad que se enfocan en proteger los sistemas y datos de las organizaciones. Los CIS *Controls* comprende una amplia gama de áreas, como la configuración segura de sistemas, la gestión de parches, el control de acceso. Además, proporciona una guía detallada para implementar medidas de seguridad efectivas [21].

PDS (*Privacy by Design Security Framework*)

El Marco de Seguridad de Privacidad por Diseño (*Privacy by Design Security Framework*) tiene como objetivo integrar la privacidad y la seguridad en la creación y elaboración de sistemas, aplicaciones y procesos desde el principio. Proporciona una guía para garantizar que las consideraciones de privacidad y seguridad sean incorporadas de manera activa en el desarrollo de un proyecto [22].

NIST y CIS son dos marcos de referencia ampliamente utilizados en el campo de la seguridad de la información. La implementación entre los marcos de referencia de CIS y NIST dependerá de los requisitos regulatorios, las normativas de la empresa, las directrices gubernamentales, para la ejecución de buenas prácticas de seguridad de la organización.

2 METODOLOGÍA

El presente proyecto empleó la investigación aplicada, que se caracteriza en ejercer los conocimientos que fueron adquiridos para la solución de problemas. Además, se trabajó de la mano con investigación documental, la cual se construye a partir de varias fuentes escritas o grabadas para la implementación de soluciones en el planteamiento del *hardening*.

Se instaló el sistema operativo de servidor Alma *Linux* con un servidor de correo sin tomar en cuenta ninguna política de seguridad. Mediante la herramienta de escaneo SCAP *Workbench* se obtuvo un primer reporte de vulnerabilidades.

Se aplicó en el sistema operativo de servidor Alma *Linux* una política de seguridad, con base a los lineamientos del marco de referencia NIST (*National Institute of Standards and Technology*). Luego con el sistema operativo endurecido se levantó el servicio de correo. Se obtuvo un reporte de vulnerabilidades con la herramienta de escaneo SCAP *Workbench*.

Se analizó y compararon los reportes obtenidos, se observó cuáles parámetros críticos se han solventado según el marco de referencia NIST. De forma manual se solventaron seis vulnerabiliades de nivel alto, con el fin de obtener una mejora en el *hardening*.

Se analizó el reporte final, verificando el impacto que tienen las políticas implementadas en relación con el triángulo de la CIA; confiabilidad, integridad y disponibilidad. Además, se realizó una guía que resume las mejores prácticas a tener en cuenta para implementar un servidor endurecido.

3 RESULTADOS

Para la implementación de *hardening* en el sistema operativo Alma *Linux,* primero se instaló el sistema operativo sin políticas de seguridad, en el cual se levantó el servidor de correo y se instaló la herramienta de escaneo SCAP *Workbench*, con el fin de generar el primer informe de escaneo de vulnerabilidades.

Después, se instaló Alma *Linux* con el perfil de seguridad en base a NIST, la ejecución del perfil de seguridad se realizó en las configuraciones de inicio de instalación del sistema operativo en la opción de *security profile*. Luego se levantó el servidor de correo y se realizó la instalación de SCAP *Workbench* para generar el segundo informe de escaneo de vulnerabilidades. Posteriormente se solventaron seis reglas de seguridad fallidas de forma manual y se generó un tercer informe.

Una vez obtenidos los informes, se analizaron los resultados y se lleva a cabo una comparación para identificar las mejoras prácticas a ser realizadas en el servidor. Finalmente, se verifica el *hardening* en el servidor en base a los elementos de la triada CIA.

3.1 IDENTIFICACIÓN DE VULNERABILIDADES EN ALMA LINUX SIN POLÍTICAS DE SEGURIDAD

INSTALACIÓN DEL SISTEMA OPERATIVO DE SERVIDOR

Se descargó la imagen del sistema operativo Alma Linux en el siguiente enlace: Alma *Linux*. Una vez descargado la ISO de Alma *Linux*, se abrió VirtualBox para crear una nueva máquina virtual, ver la Figura 3.1.

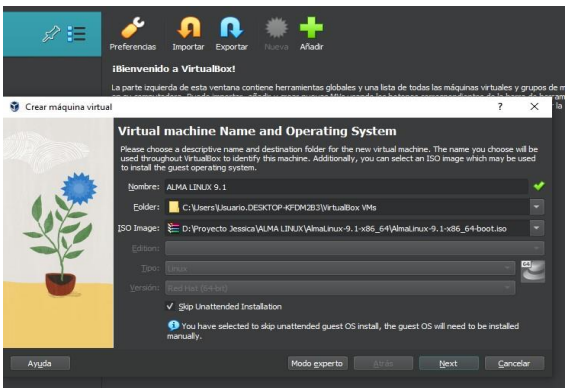


Figura 3.1 Creación de máquina virtual en virtualbox

Se realizó las configuraciones de *hardware* que requiere la máquina virtual como: memoria, espacio en disco, cantidad de núcleos del procesador. En la Figura 3.2 se observan las características de *hardware* mencionadas, las cuales fueron especificaciones mayores a los requerimientos mínimos mencionados en el marco teórico.

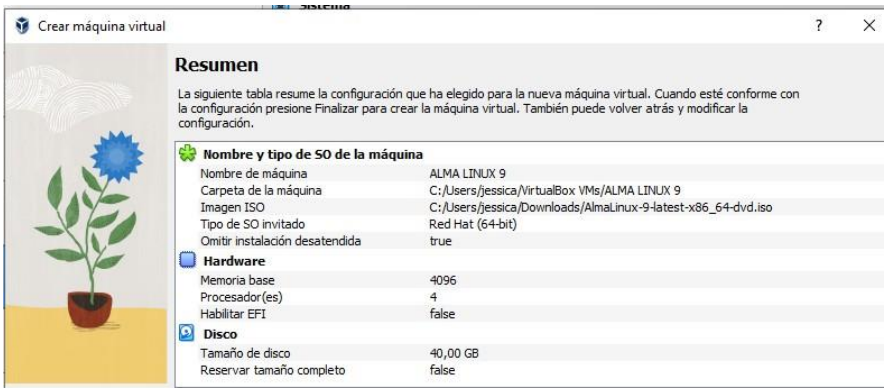


Figura 3.2 Configuraciones de *hardware* de la máquina virtual

Se arrancó la máquina virtual de Alma *Linux* y se seleccionó "*Install* Alma *Linux* 9.1", en la Figura 3.3 se observa cómo los procesos esenciales del sistema operativo se cargan.

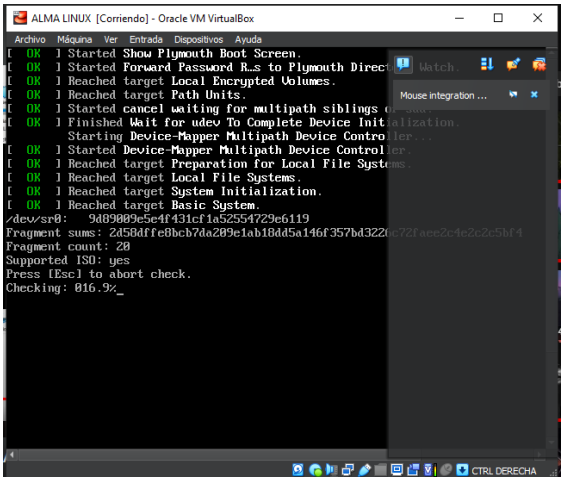


Figura 3.3 Carga de procesos esenciales del sistema operativo

Después de concluir con el arranque, se realizó las siguientes configuraciones de instalación del sistema operativo Alma *Linux* 9.1 que se puede observar en la Figura 3.4. Se configuró el destino de la instalación que hace referencia a la elección del disco estándar local, ver la Figura 3.5 y la contraseña de *ROOT* que se puede ver en Figura 3.6.

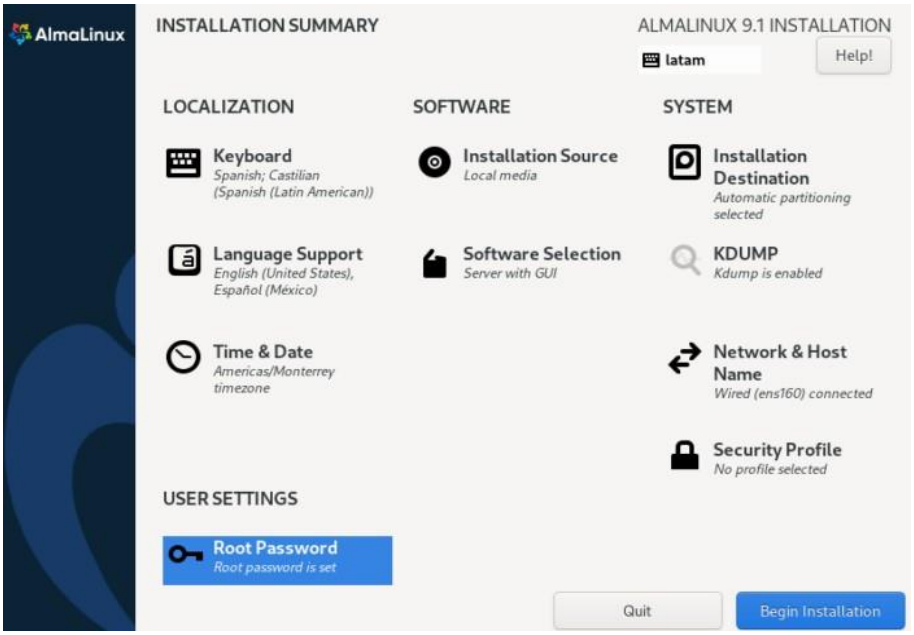


Figura 3.4 Configuraciones de instalación

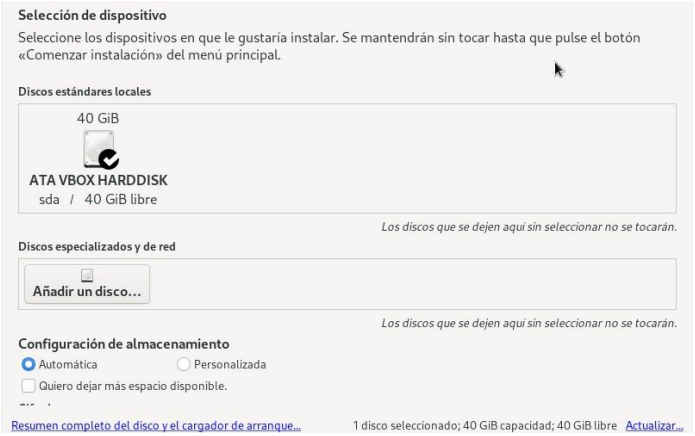


Figura 3.5 Destino de instalación

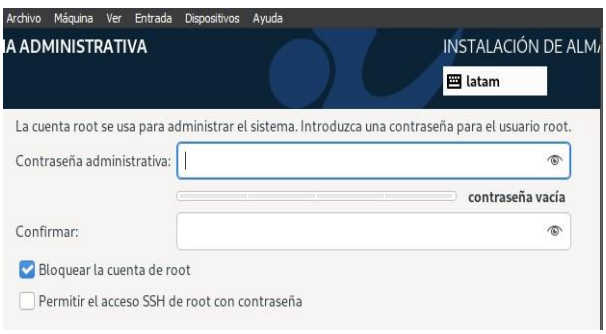


Figura 3.6 Contraseña de *Root*

Luego de haber realizado las configuraciones necesarias, se inició la instalación del sistema operativo. Al finalizar la descarga de los paquetes necesarios para la instalación se reinició el sistema operativo, ver Figura 3.7. Finalmente se puede empezar con el uso del sistema operativo de servidor GUI de Alma *Linux, se* indica en la Figura 3.8.

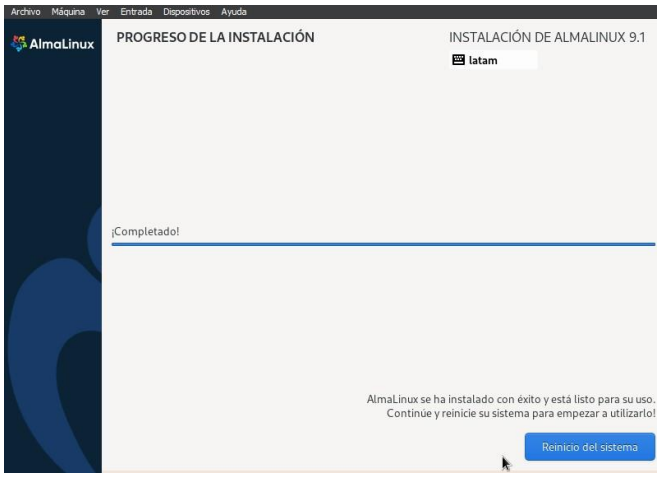


Figura 3.7 Reinicio del sistema operativo

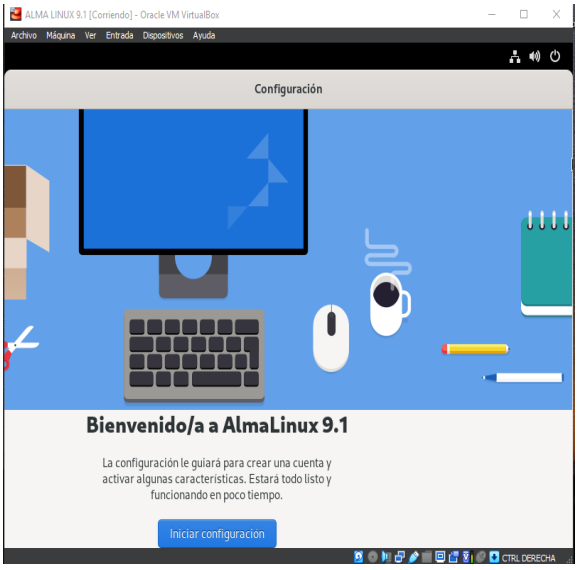


Figura 3.8 Interfaz gráfica del usuario Alma *Linux*

De esta manera concluye la instalación de *Server* GUI Alma *Linux* 9.1.

LEVANTAMIENTO DE SERVIDOR DE CORREO

Con la instalación correcta del sistema operativo se ingresó al sistema y se abrió la terminal, ahí se ingresó el comando “sudo su” para trabajar en modo administrador, debido a los privilegios que posee este perfil de usuario. Se ingresó a la terminal

para descargar los paquetes de Postfix, ver Figura 3.9, Dovecot, ver Figura 3.10 y Telnet, ver Figura 3.11, que son necesarios para la configuración del servidor de correo.

El paquete de Postfix se encarga de recibir, enviar y reenviar mensajes de correo electrónico entre servidores. Actúa como intermediario para entregar el correo electrónico desde el remitente hasta el destinatario.

Dovecot proporciona el acceso al correo electrónico a través de los protocolos IMAP y POP3. Dovecot permite a los clientes de correo electrónico acceder a sus buzones y mensajes almacenados en el servidor mediante los protocolos IMAP y POP3.

Telnet permite a los usuarios establecer sesiones remotas en otros sistemas mediante la red, puede ser por medio de internet o una red local. Utiliza el puerto TCP 23 para establecer la conexión de forma predeterminada.

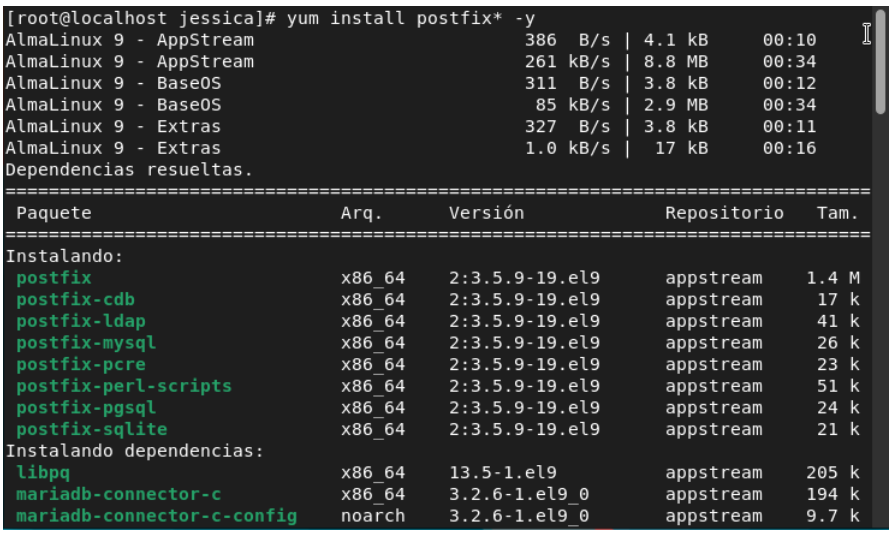


Figura 3.9 Descarga de paquetes de Postfix

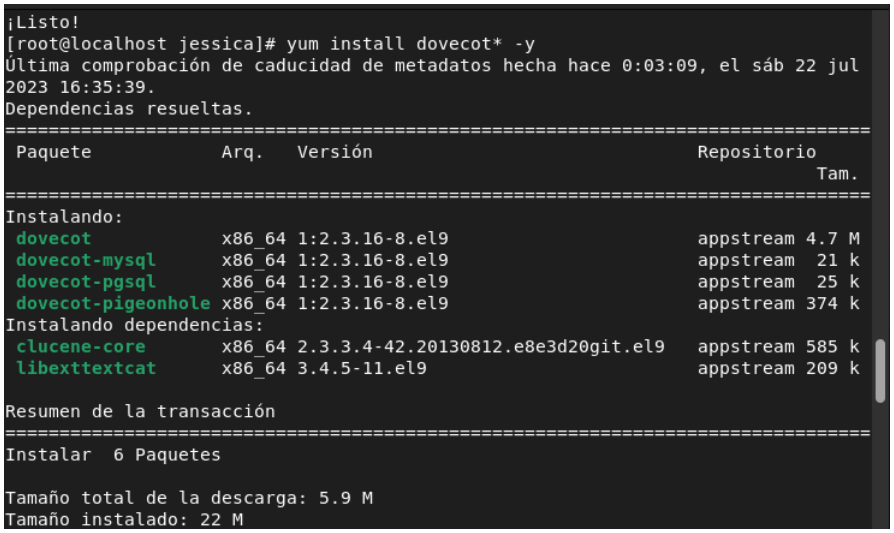


Figura 3.10 Descarga de paquetes de Dovecot

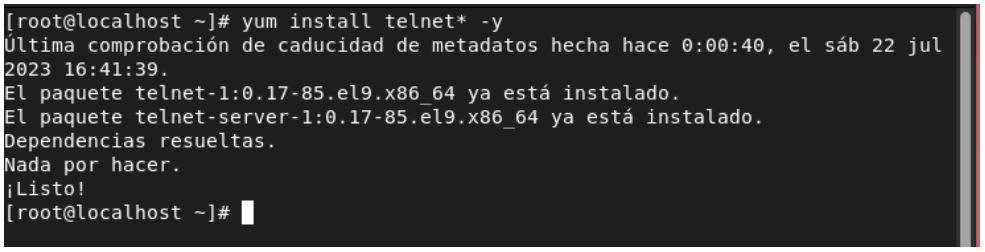


Figura 3.11 Descarga de paquetes de Telnet

En la configuración del servidor de Postfix se ingresó a la siguiente ruta “cd /etc/postfix/”. Luego se escribió el comando “ls” para observar el contenido del directorio de Postfix, ver la Figura 3.12.

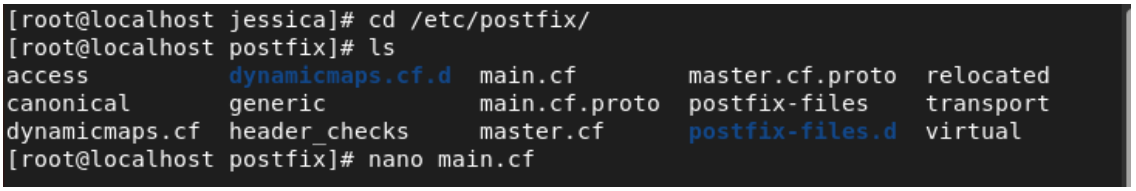


Figura 3.12 Directorio Postfix

Al ejecutar el comando “nano main.cf” se ingresó al archivo main.cf mediante el editor de texto nano y se realizó las siguientes configuraciones:

myhostname = Jess.epn.edu.ec, que es el nombre del dominio del servidor de correo

mydomain = epn.edu.ec, es el dominio principal del servidor de correo. Estas dos líneas de configuración se observan en la Figura 3.13.

```
myhostname = Jess.epn.edu.ec
#myhostname = virtual.domain.tld

# The mydomain parameter specifies the local internet domain name.
# The default is to use $myhostname minus the first component.
# $mydomain is used as a default value for many other configuration
# parameters.
#
mydomain = epn.edu.ec
```

Figura 3.13 Dominio del servidor

myorigin = $ mydomain, especifica el dominio que emplea como origen en e direccionamiento del correo electrónico, ver Figura 3.14.

```
#myorigin = $myhostname
myorigin = $mydomain

# RECEIVING MAIL
```

Figura 3.14 Dominio de origen

mydestination = $myhostname, localhost. $mydomain, localhost, $mydomain, considera una lista de nombres de dominio de manera local del servidor, ver la Figura 3.15.

```
#
#mydestination = $myhostname, localhost.$mydomain, localhost
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
#mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain,
#       mail.$mydomain, www.$mydomain, ftp.$mydomain
```

Figura 3.15 Registro de nombre de dominios

mynetworks = 10.0.2.15/24, 127.0.0.1/8, redes permitidas para el envío de correos mediante el servidor, se indica en la Figura 3.16.

```
#
mynetworks = 10.0.2.15/24, 127.0.0.1/8
#mynetworks = $config_directory/mynetworks
#mynetworks = hash:/etc/postfix/network_table
```

Figura 3.16 IP del servidor de correo

home_mailbox = Maildir/, es un directorio donde se almacenan los mensajes que contiene el correo electrónico, ver la Figura 3.17.

```
#
#home_mailbox = Mailbox
home_mailbox = Maildir/

# The mail_spool_directory parameter specifies the directory where
# UNIX-style mailboxes are kept. The default setting depends on the
# system type.
```

Figura 3.17 Directorio Maildir/

La Figura 3.18 muestra los siguientes comandos," systemctl *start* postfix*"* esta inicia el servidor de postfix. En el comando "systemctl *status* postfix*"* se observa el estado del servidor.

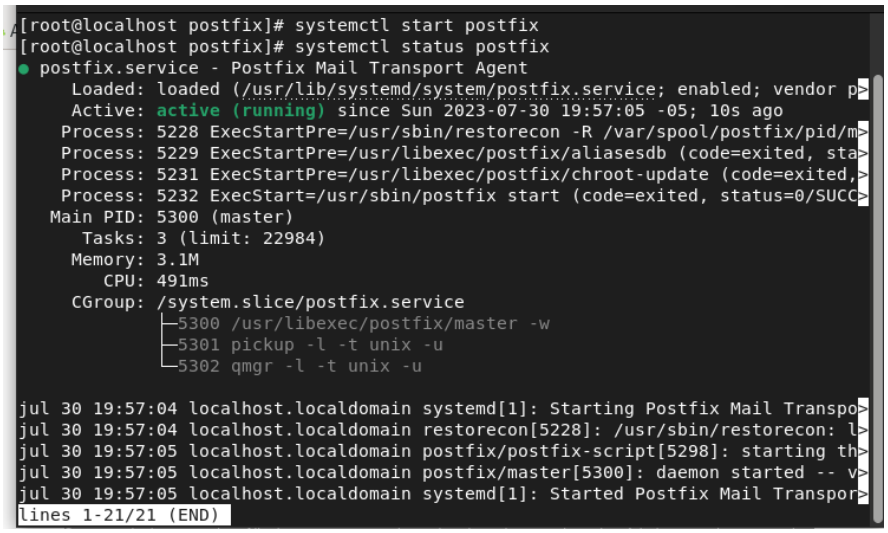


Figura 3.18 Servidor Postfix

Para la configuración de Dovecot, se ingresó a la siguiente ruta "cd /etc/dovecot/". Una vez dentro del directorio de Dovecot, se ingresó el comando "ls" para ver los archivos que contiene el directorio, ver la Figura 3.19.

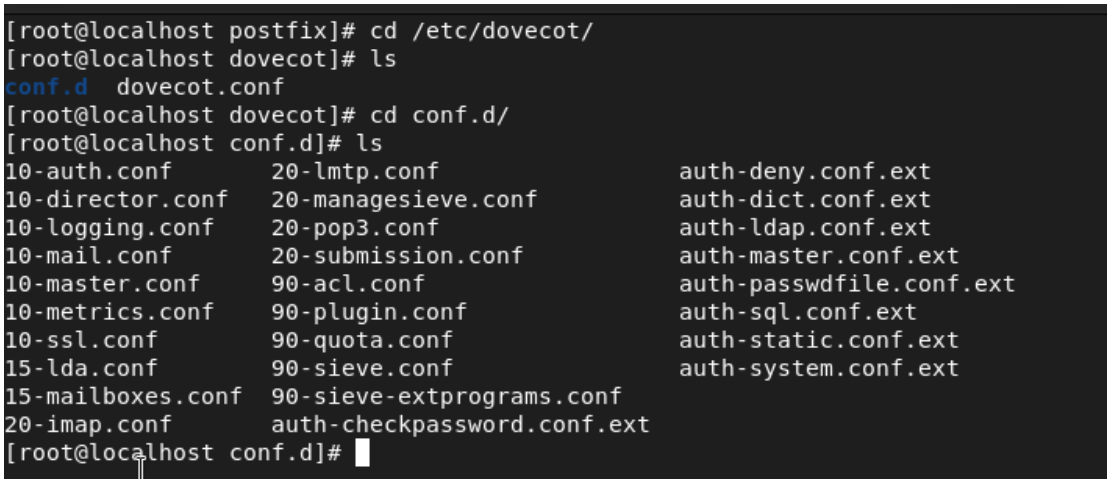


Figura 3.19 Archivos del directorio de Dovecot

Se modificó el archivo 10-*master*.conf con el editor de texto nano, este archivo contiene información sobre la configuración del servicio de Dovecot. Se añadió dos líneas de texto; user = postfix y group = postfix, ver la Figura 3.20.

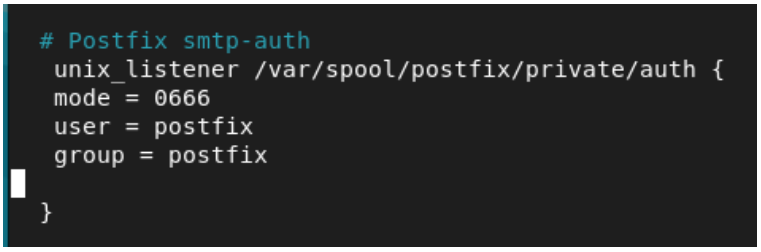


Figura 3.20 Archivo 10-*master.*conf

En la Figura 3.21, se observa el archivo 10-auth.conf. Se quitó el comentario de la línea auth_mechanisms = plain y se añadió la palabra login.

Figura 3.21 Archivo 10-auth.conf

En el siguiente archivo con el editor de texto nano se modificó el archivo 10-mail.conf. Se quitó el comentario de las líneas mail_location = maildir:-/Maildir y mail_uid y mail_gid, en las dos líneas se añadió la palabra vmail, ver la Figura 3.22.

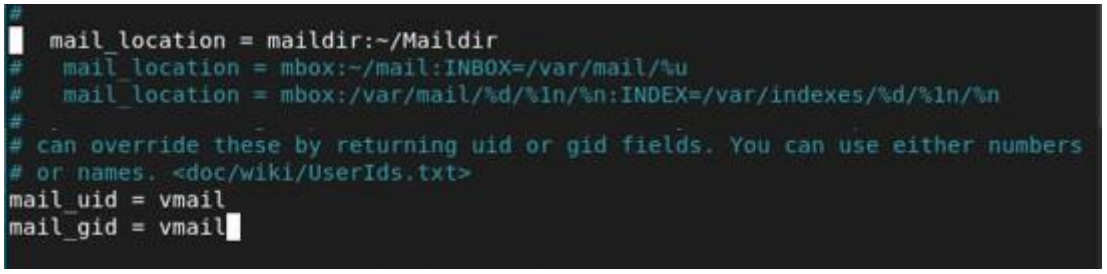


Figura 3.22 Archivo 10-mail.conf

Con el comando “systemctl *start* dovecot*”* inicia el servidor de Dovecot, con “systemctl *status* dovecot” muestra el estado del servidor, observar la Figura 3.23.

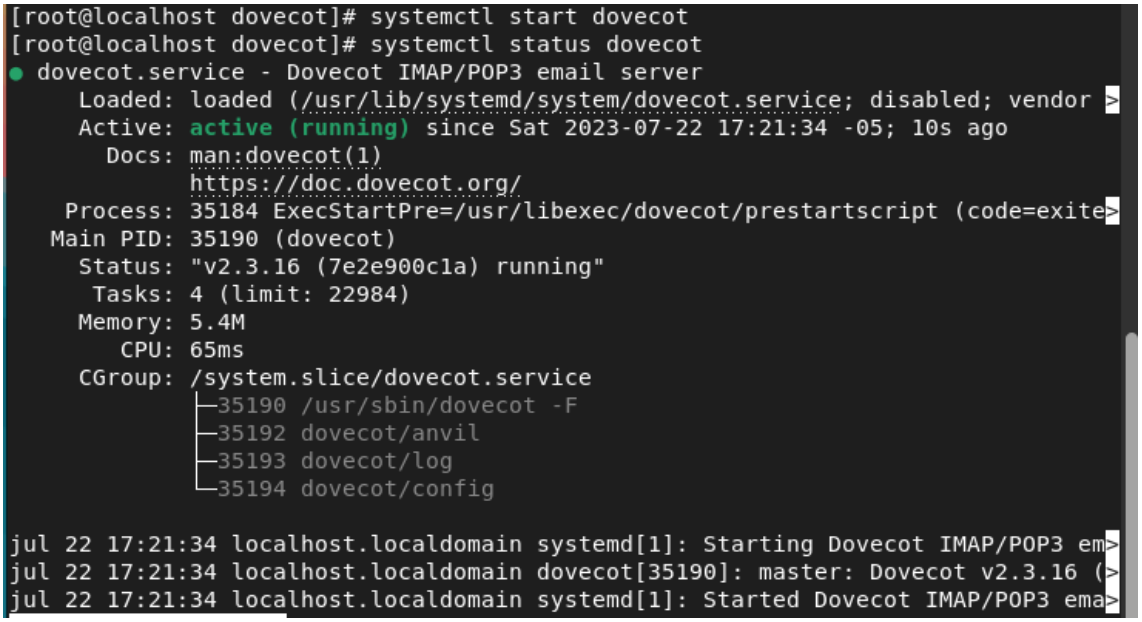


Figura 3.23 Servidor Dovecot

Después de realizar la configuración del servidor de correo se procedió a crear los usuarios. Con el comando “useradd” se creó los perfiles de los usuarios y con el comando “passwd” se ingresó una contraseña correspondiente a cada usuario como se puede ver en la Figura 3. **24**. Estos usuarios se emplearon para la comprobación de envío y recepción de correo electrónicos.

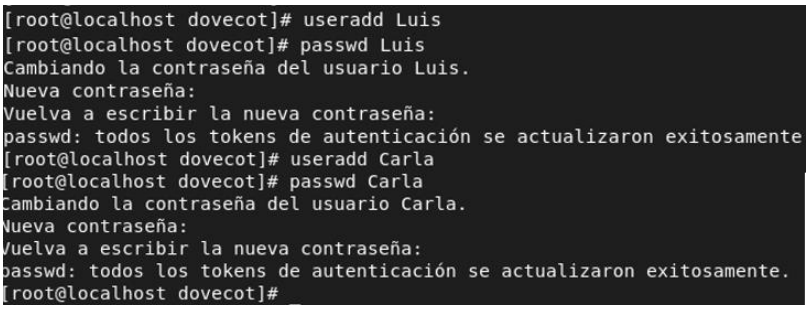


Figura 3. 24 Creación de usuarios

Con el propósito de verificar la funcionalidad correcta del servidor de correo, se llevó a cabo una prueba de envío y recepción de correo electrónico entre los usuarios creados anteriormente. Los comandos que se utilizaron para conectar con el servidor de correo y generar un correo, de la cuenta del usuario Luis a la cuenta de usuario Carla, ver la Figura 3.25. La recepción del correo en el buzón del usuario Carla se puede observar en la Figura 3.26.

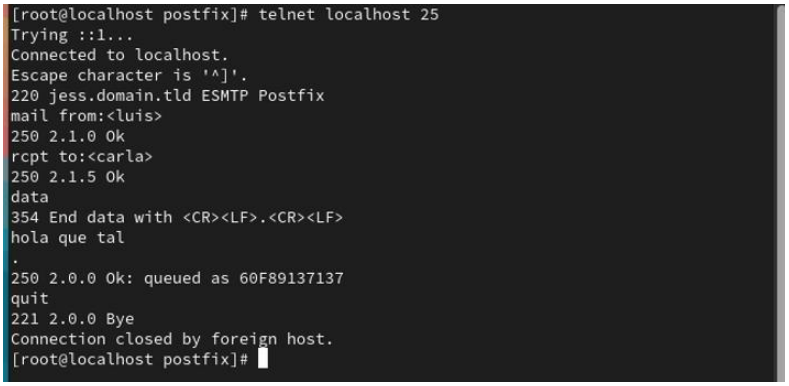


Figura 3.25 Envió de correo

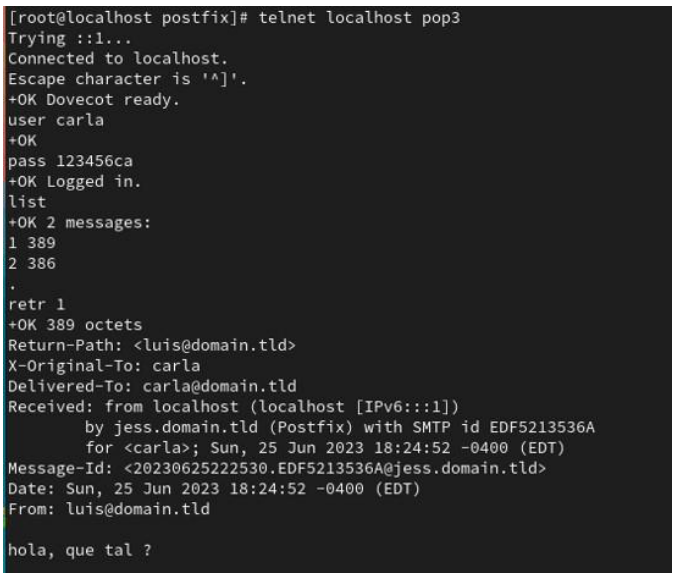


Figura 3.26 Verificación de recepción de correo

En relación con la prueba de correo electrónico que se realizó, se puede decir que, el servidor funciona correctamente. Sin embargo, es importante recalcar que el uso de Telnet para el envío de correos electrónicos no es apropiado, debido que la información transmitida por este medio no se encuentra cifrada.

Durante la investigación de las herramientas de escaneo, realizamos pruebas con *OpenSCAP*, la cual presentó inconvenientes al ejecutarse a través de la línea de comandos (CLI). Estos problemas incluyeron la dificultad para visualizar el archivo HTML generado después del escaneo del sistema operativo y un error relacionado con el archivo de perfiles de *OpenSCAP* al aplicar la política de seguridad durante la instalación. Debido a estas complicaciones, optamos por utilizar un sistema operativo de servidor con interfaz gráfica para lograr los objetivos, que incluían el

análisis de los informes generados por la herramienta de escaneo y la verificación de las políticas de seguridad.

De esta manera, se trabajó con SCAP *Workbench* que es una herramienta que ofrece una interfaz gráfica para el escaneo de vulnerabilidades basado en el protocolo SCAP. Además, las configuraciones del servidor funcionaron correctamente, por lo que la decisión de emplear un servidor con interfaz gráfica resultó adecuada.

INSTALACIÓN DE LA HERRAMIENTA DE ESCANEO SCAP *WORKBENCH*

Esta herramienta permite analizar las vulnerabilidades de un sistema operativo de forma local o remoto el cual genera informes en base a las evaluaciones de escaneo del sistema. Sé abrió la terminal del sistema y se ejecutó el siguiente comando "sudo dnf *install* scap-*workbench"* para proceder con su instalación, después de instalar la herramienta se puede visualizar el símbolo de la aplicación en el menú de programas del entorno de alma Linux, como se onberva en la Figura 3.27. Luego se abrió la aplicación y en "*select content to load*" se eligió "Almalinux9" que es la guía de seguridad del protocolo SCAP, ver Figura 3.28.

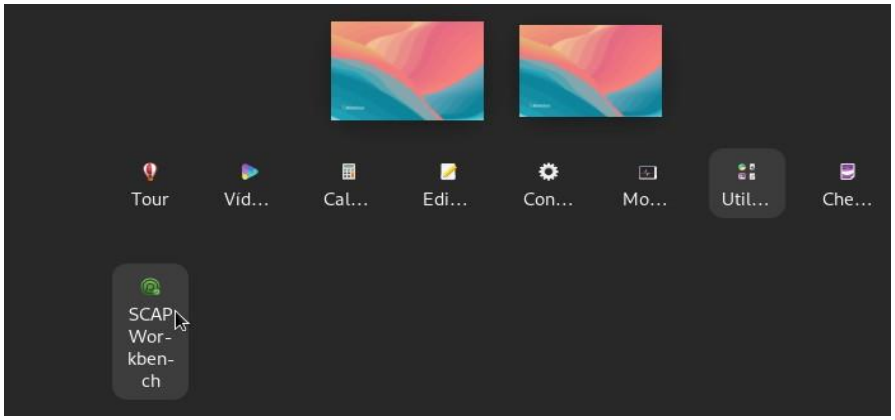


Figura 3.27 SCAP *Workbench*

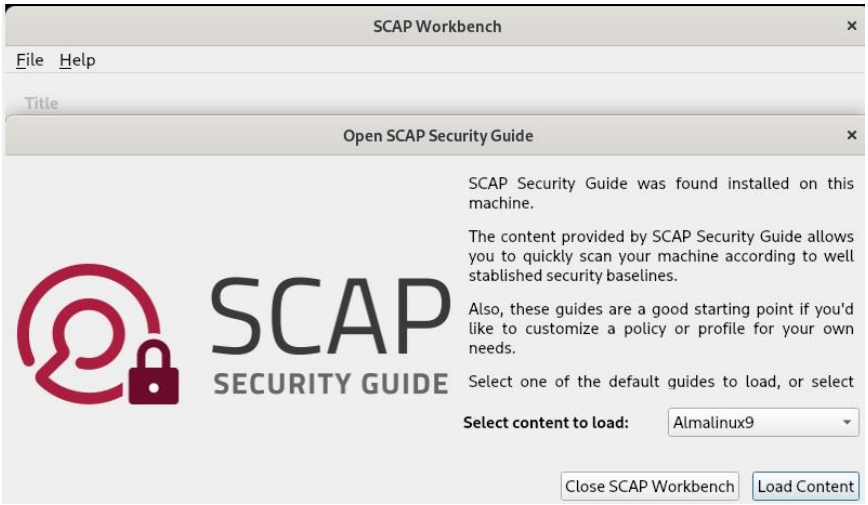


Figura 3.28 Guía de seguridad SCAP

Una vez seccionada la guía de seguridad, se despliega una ventana principal de SCAP *Workbench*, en la cual presenta algunas opciones para la configuración del escaneo, estas son:

Customization: Esta opción permite la personalización de un perfil de seguridad.

Profile: Esta opción permite la elección de un perfil de seguridad, la herramienta SCAP *Workbench* dispone de 16 perfiles, como se indica en la **Figura 3.29**.

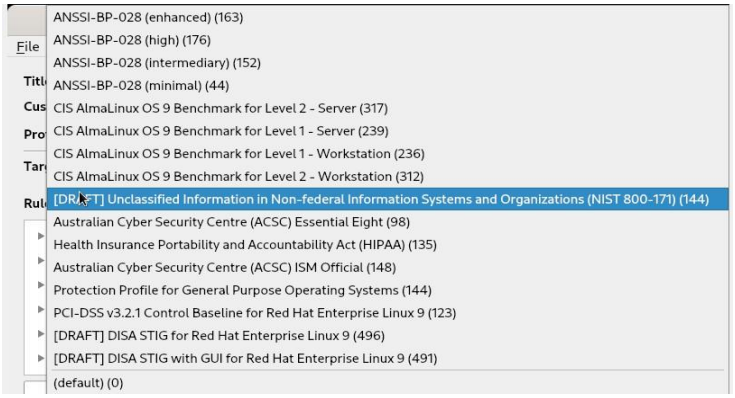


Figura 3.29 Perfiles de SCAP *Workbench*

Target: Se puede seleccionar si se desea evaluar el sistema de forma remota o local.

Rules: Muestra una lista de reglas de seguridad que se aplican en la política de seguridad seleccionada.

Fetch remote resources: Esta opción se marca en caso de que se desee que el escaneo descargue contenido OVAL (archivo de escaneo) definido en un archivo XML.

Remediate: Esta opción permite que SCAP *Workbench* corrija la configuración del sistema que no coincida con el estado de la política de seguridad seleccionada.

Al presionar el botón *SCAN*, empieza el proceso de escaneo del sistema que se puede ver en la Figura 3.30, con el botón *Save Results*, se guardan los resultados en un archivo en formato XCCDF, ARF o informe HTML. Si se presiona el botón *Show Report*, el informe se muestra en el navegador.

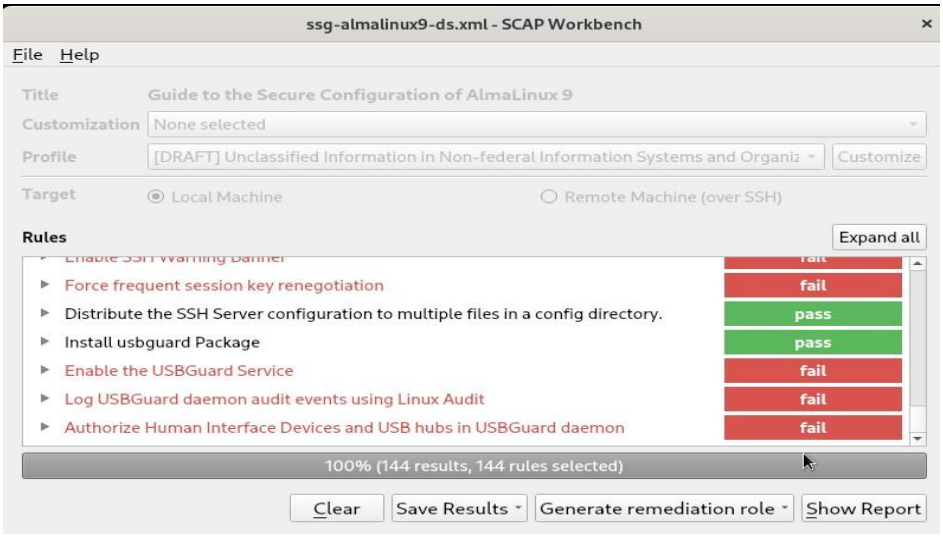


Figura 3.30 Escaneo del sistema con SCAP *Workbench*

PRIMER REPORTE DE VULNERABILIDADES

“NIST” fue el marco de referencia empleado para el escaneo de vulnerabilidades del sistema operativo de servidor Alma *Linux* 9.1.

En el primer informe de escaneo de vulnerabilidades se obtuvo 32.56% de seguridad en el servidor, ver la Figura 3.31. En este informe se realizó el escaneo de 144 reglas que están establecidas por el marco de referencia de NIST. De estas reglas, 76 se encuentran en estado fallido (*failed)*, lo que indica que el sistema es vulnerable. Para solucionar estas vulnerabilidades es necesario aplicar parches de seguridad a través de la modificación de archivos o la ejecución de comandos correspondientes a cada regla.

Se identificaron 30 reglas con un estado de aprobación (*passed*), las cuales cumplen con parches de seguridad del sistema. Las 38 reglas restantes no son de alcance para el marco de referencia NIST, debido a que la regla podría haber sido especificada a una versión diferente del sistema operativo de destino.

Además, se muestra el nivel de severidad de las reglas fallidas (*severity of failed rules*) que el sistema no cumple, esto quiere decir que son reglas fallidas clasificadas en nivel alto, medio y bajo que provocan que el servidor sea vulnerable. De las 76 reglas que resultaron fallidas, 7 son de nivel bajo, 61 en el nivel medio y 8 en el nivel alto.

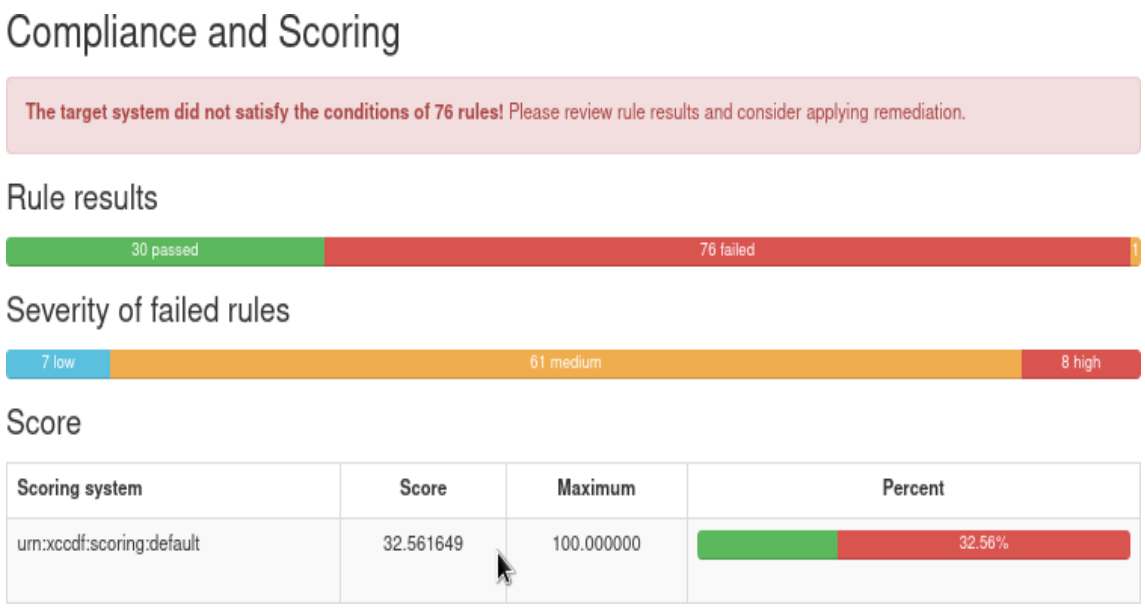
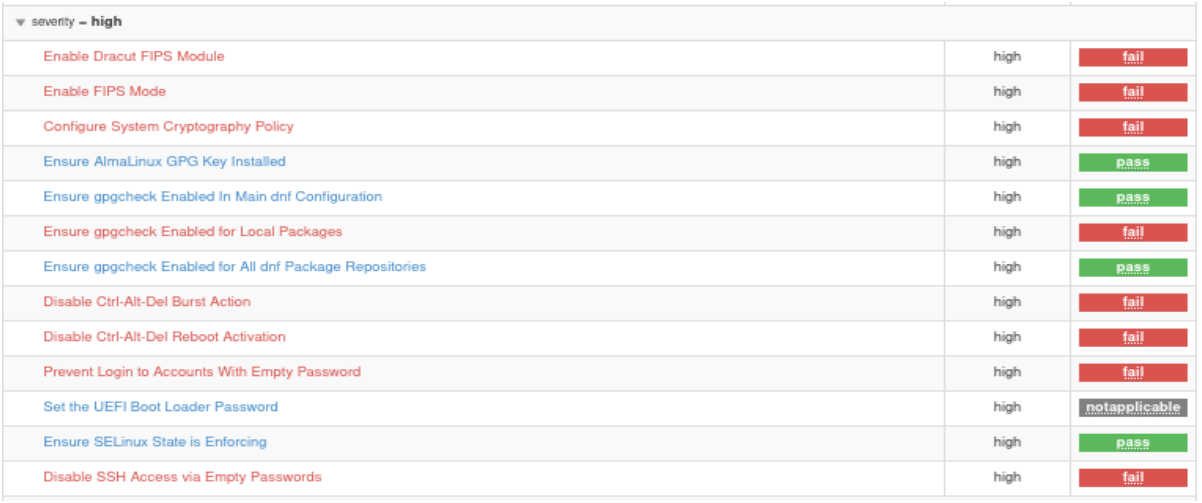


Figura 3.31 Informe del escaneo del sistema sin aplicar políticas de seguridad

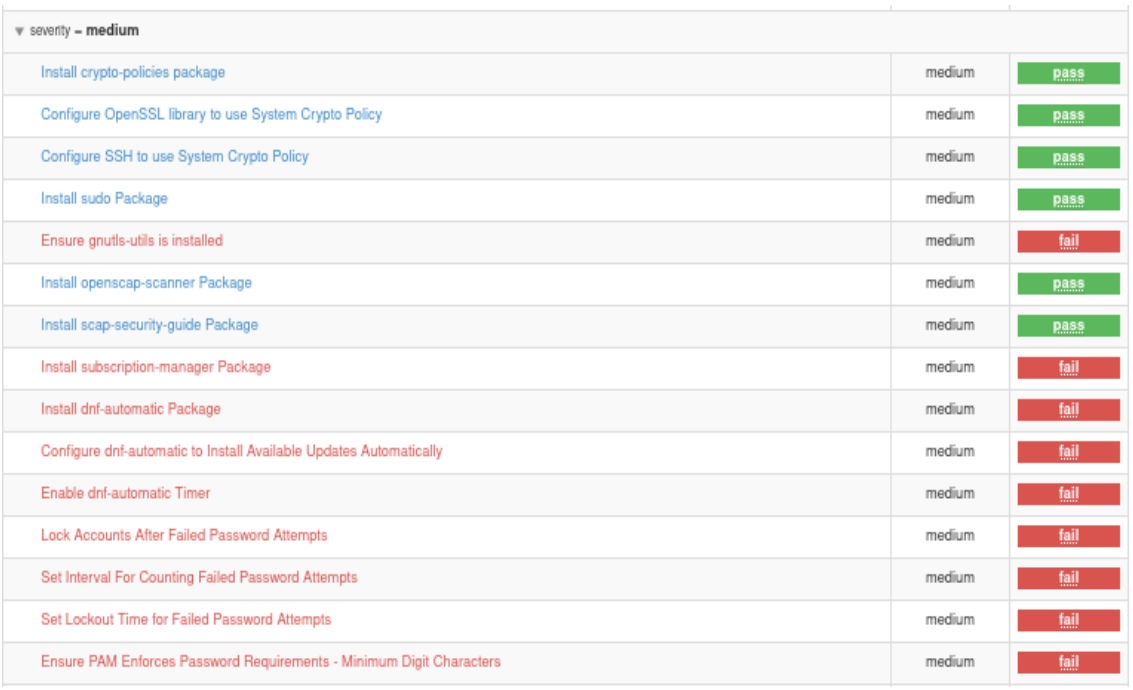
En la Figura 3.32, se enlista las reglas severas fallidas que se encuentran en el nivel alto, las cuales exponen al servidor a vulnerabilidades más peligrosas. Por lo que, es importante tomar una acción inmediata en la solución de estas vulnerabilidades. Para más información del primer reporte se puede ver en el Anexo III. I.



severity – high		
Enable Dracut FIPS Module	high	fail
Enable FIPS Mode	high	fail
Configure System Cryptography Policy	high	fail
Ensure AlmaLinux GPG Key Installed	high	pass
Ensure gpgcheck Enabled In Main dnf Configuration	high	pass
Ensure gpgcheck Enabled for Local Packages	high	fail
Ensure gpgcheck Enabled for All dnf Package Repositories	high	pass
Disable Ctrl-Alt-Del Burst Action	high	fail
Disable Ctrl-Alt-Del Reboot Activation	high	fail
Prevent Login to Accounts With Empty Password	high	fail
Set the UEFI Boot Loader Password	high	notapplicable
Ensure SELinux State is Enforcing	high	pass
Disable SSH Access via Empty Passwords	high	fail

Figura 3.32 Vulnerabilidades de nivel alto

Las vulnerabilidades de nivel medio como se muestra en la **Figura 3.33**, representan un riesgo moderado. Si son expuestas, podrían permitir al atacante acceder a cierta información del sistema, se requiere de parches para evitar daños en el servidor.

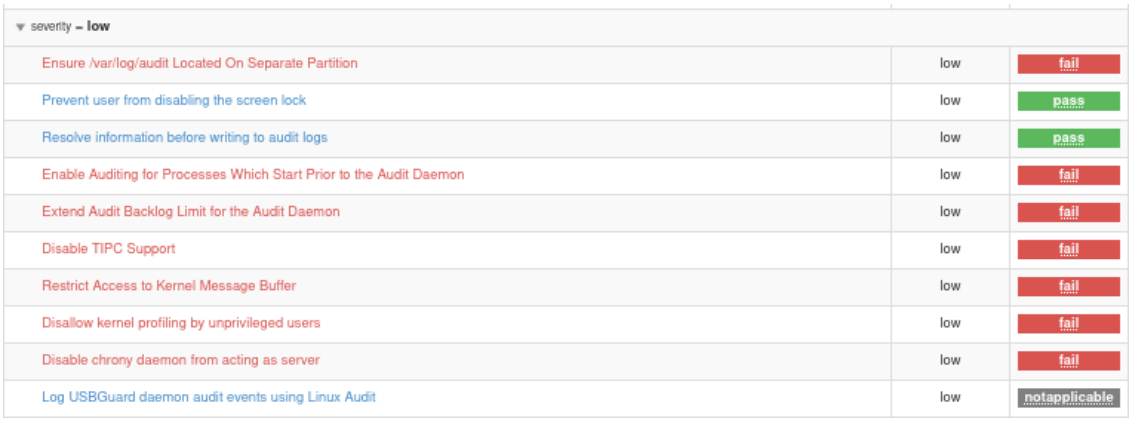


severity – medium		
Install crypto-policies package	medium	pass
Configure OpenSSL library to use System Crypto Policy	medium	pass
Configure SSH to use System Crypto Policy	medium	pass
Install sudo Package	medium	pass
Ensure gnutls-utils is installed	medium	fail
Install openscap-scanner Package	medium	pass
Install scap-security-guide Package	medium	pass
Install subscription-manager Package	medium	fail
Install dnf-automatic Package	medium	fail
Configure dnf-automatic to Install Available Updates Automatically	medium	fail
Enable dnf-automatic Timer	medium	fail
Lock Accounts After Failed Password Attempts	medium	fail
Set Interval For Counting Failed Password Attempts	medium	fail
Set Lockout Time for Failed Password Attempts	medium	fail
Ensure PAM Enforces Password Requirements - Minimum Digit Characters	medium	fail

Figura 3.33 Vulnerabilidades de nivel medio

La **Figura 3.34** muestra las vulnerabilidades de bajo nivel que son las de menor riesgo para el sistema. Pero se puede presentar situaciones menores que exponen la seguridad del sistema, a pesar de que son de menor grado no hay que dejarlas

de lado, puesto que es necesario aplicar parches para garantizar la seguridad del servidor.



severity – low		
Ensure /var/log/audit Located On Separate Partition	low	fail
Prevent user from disabling the screen lock	low	pass
Resolve information before writing to audit logs	low	pass
Enable Auditing for Processes Which Start Prior to the Audit Daemon	low	fail
Extend Audit Backlog Limit for the Audit Daemon	low	fail
Disable TIPC Support	low	fail
Restrict Access to Kernel Message Buffer	low	fail
Disallow kernel profiling by unprivileged users	low	fail
Disable chrony daemon from acting as server	low	fail
Log USBGuard daemon audit events using Linux Audit	low	notapplicable

Figura 3.34 Vulnerabilidades de nivel bajo

3.2 IMPLEMENTACIÓN DE UNA POLÍTICA DE SEGURIDAD

EJECUCIÓN DE LA POLÍTICA NIST EN ALMA *LINUX* 9.1

Se implementó la política de seguridad basada en el marco de referencia NIST. Este marco de referencia cumple con los tres pilares fundamentales de la información. Proporciona una guía de seguridad e integridad en referencia a la información de una organización para gestionar y mitigar los riesgos de ciberseguridad [23].

Para aplicar una política de seguridad en Alma Linux, después del arranque de la ISO del sistema operativo se despliega la ventana de inicio de instalación, ver Figura 3.4, ahí es necesario acceder a la configuración de security *profile,* como se observa en la Figura 3.35. Particularmente, el perfil NIST requiere la asignación de una partición en el disco para el directorio “/var/log/audit”, ver la Figura 3.36, lo cual es un requerimiento importante para en el proceso de la ejecución de la política de

seguridad en el sistema. Una vez realizada las configuraciones se empieza con la instalación y el sistema operativo aplica la política de seguridad NIST.

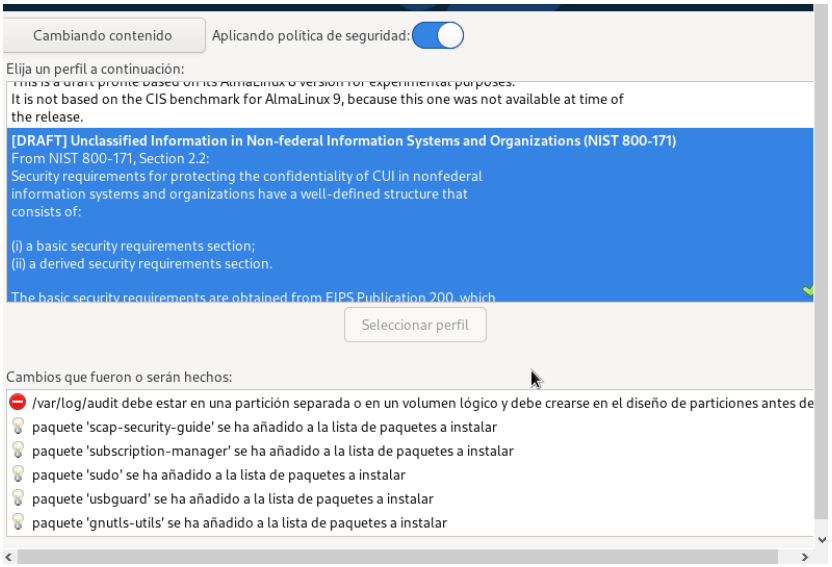


Figura 3.35 Selección de perfil NIST

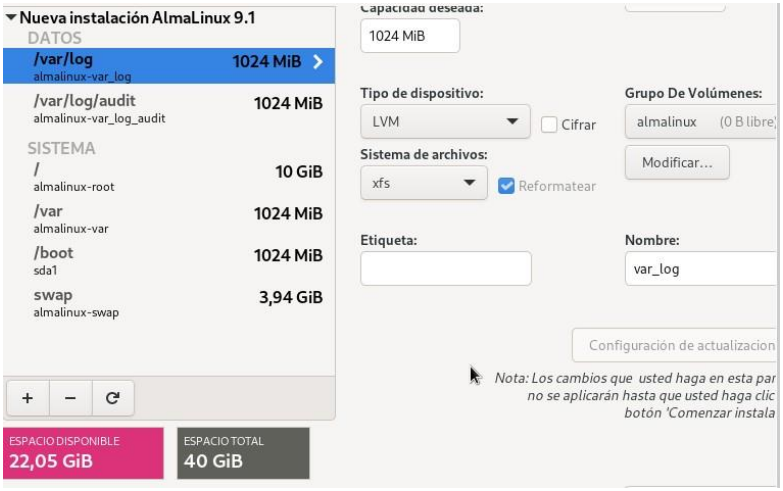


Figura 3.36 Partición de disco

LEVANTAMIENTO DE SERVIDOR DE CORREO EN UN SISTEMA OPERATIVO CON POLÍTICAS DE SEGURIDAD NIST

Después de aplicar *hardening* en el sistema operativo, se procedió a realizar las configuraciones previas del servidor de correo que se encuentran detalladas en la sección de “LEVANTAMIENTO DE SERVIDOR DE CORREO**”**. Sin embargo, se

realizó un cambio en las contraseñas de los usuarios, con el fin de implementar contraseñas seguras, para proteger la seguridad del servidor de correo.

Creación de contraseñas seguras de los usuarios

Las contraseñas débiles son vulnerables a ataques y amenazas de ciberseguridad. En consecuencia, es necesario generar contraseñas seguras para los usuarios del sistema creados previamente. Para cumplir con esto, se aplicó las siguientes recomendaciones: utilizar contraseñas con un mínimo de 8 caracteres que contienen, caracteres especiales, letras mayúsculas y minúsculas, números. En la Figura 3.37 se puede observar la nueva contraseña que se generó para el usuario Luis.

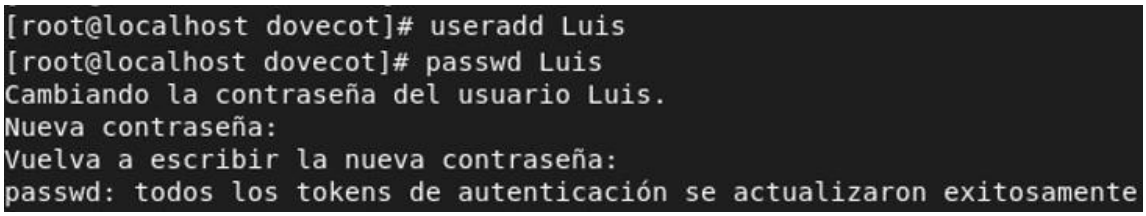


Figura 3.37 Contraseña segura

SEGUNDO REPORTE DE VULNERABILIDADES

Una vez aplicada la política de seguridad y realizadas las configuraciones del servidor de correo, se instala la herramienta de escaneo SCAP *Workbench.* Se llevó a cabo el segundo escaneo de vulnerabilidades, en la Figura 3.38 se observa un resultado del 45.96% de seguridad del sistema. Se identificaron 69 reglas fallidas y 39 reglas aprobadas, además se observa la clasificación de nivel de severidad de las reglas fallidas. En el nivel de severidad bajo se encuentran 8 reglas fallidas, en el nivel medio están 53 reglas fallidas y en el nivel alto 8 reglas fallidas. El informe completo se puede observar en el Anexo III. II.

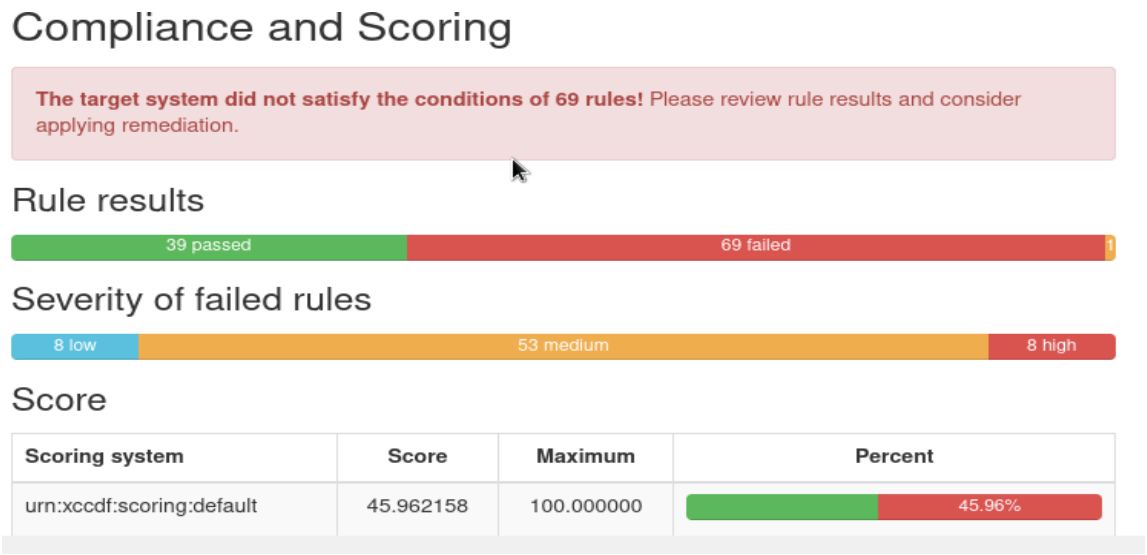


Figura 3.38 Escaneo del servidor con política de seguridad NIST

En la Figura 3.39 se observa que no se solventó ninguna vulnerabilidad de alto nivel, a pesar de haber aplicado previamente la política de seguridad en el sistema operativo, es decir, no fueron solventadas de forma automática.

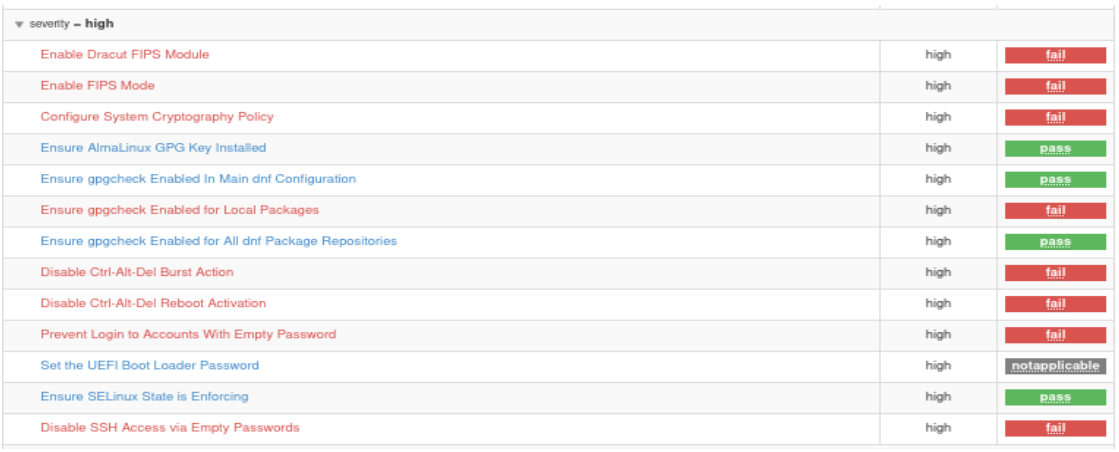
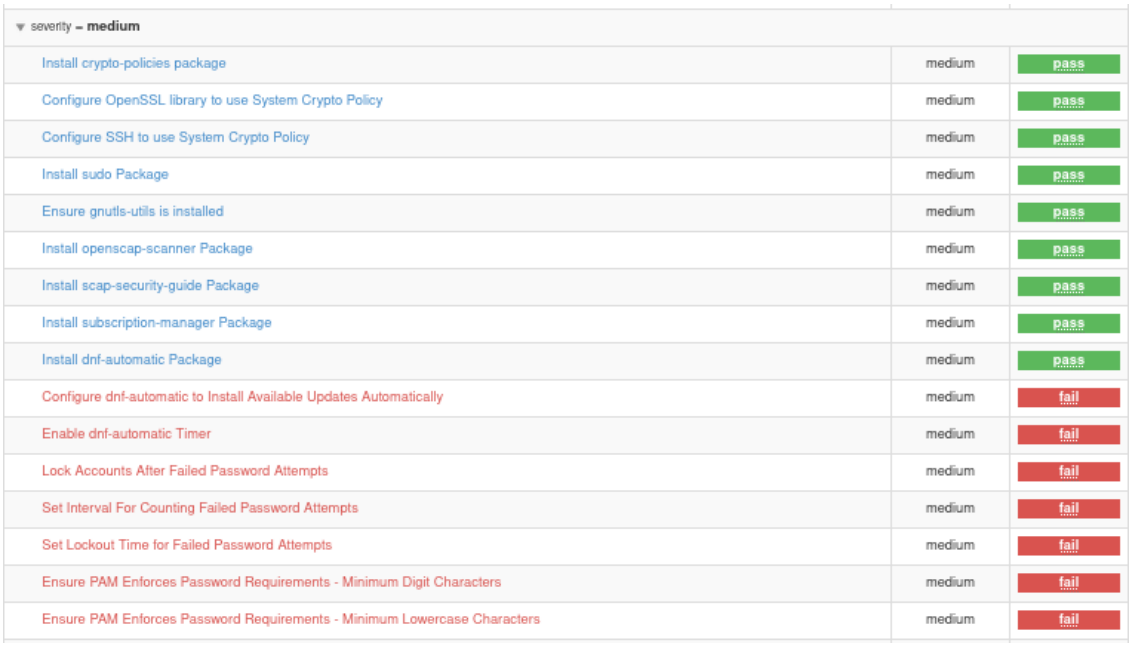


Figura 3.39 Vulnerabilidades de nivel alto después de aplicar políticas de seguridad

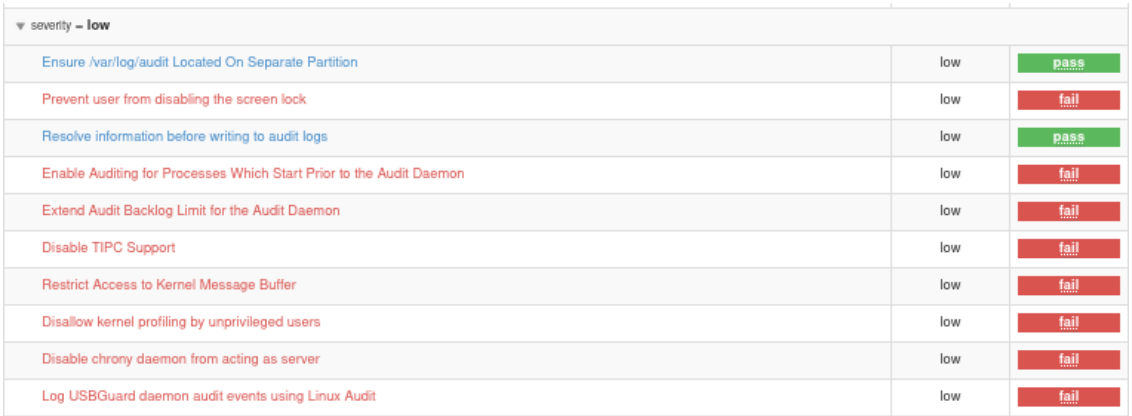
En las vulnerabilidades de nivel medio hubo una mejora en la seguridad del sistema, la Figura 3.40 muestra que no fueron solventadas en su totalidad; sin embargo, aquellas políticas que fueron solucionadas de manera automática ayudaron a incrementar la seguridad del sistema.



severity – medium		
Install crypto-policies package	medium	pass
Configure OpenSSL library to use System Crypto Policy	medium	pass
Configure SSH to use System Crypto Policy	medium	pass
Install sudo Package	medium	pass
Ensure gnutls-utils is installed	medium	pass
Install openscap-scanner Package	medium	pass
Install scap-security-guide Package	medium	pass
Install subscription-manager Package	medium	pass
Install dnf-automatic Package	medium	pass
Configure dnf-automatic to Install Available Updates Automatically	medium	fail
Enable dnf-automatic Timer	medium	fail
Lock Accounts After Failed Password Attempts	medium	fail
Set Interval For Counting Failed Password Attempts	medium	fail
Set Lockout Time for Failed Password Attempts	medium	fail
Ensure PAM Enforces Password Requirements - Minimum Digit Characters	medium	fail
Ensure PAM Enforces Password Requirements - Minimum Lowercase Characters	medium	fail

Figura 3.40 Vulnerabilidades de nivel medio después de aplicar políticas de seguridad

Las vulnerabilidades de nivel bajo fueron solventadas 2 de las 10 vulnerabilidades identificadas. Una de estas soluciones se aplicó de forma manual, que es la partición de disco realizada el momento de la aplicación de la política, mientras que la otra se realizó de forma automática que es "*Resolve information before writing to Audit logs*", se muestra en la Figura 3.41.



severity – low		
Ensure /var/log/audit Located On Separate Partition	low	pass
Prevent user from disabling the screen lock	low	fail
Resolve information before writing to audit logs	low	pass
Enable Auditing for Processes Which Start Prior to the Audit Daemon	low	fail
Extend Audit Backlog Limit for the Audit Daemon	low	fail
Disable TIPC Support	low	fail
Restrict Access to Kernel Message Buffer	low	fail
Disallow kernel profiling by unprivileged users	low	fail
Disable chrony daemon from acting as server	low	fail
Log USBGuard daemon audit events using Linux Audit	low	fail

Figura 3.41 Vulnerabilidades de nivel bajo después de aplicar políticas de seguridad

3.3 ANÁLISIS DE LOS REPORTES, RESULTADO DE LA APLICACIÓN DE LA HERRAMIENTA DE ESCANEO

En el primer reporte de vulnerabilidades, donde el sistema operativo no disponía de una política en referente a un marco de ciberseguridad se obtuvo un 32.56% de seguridad en el mismo, al momento de aplicar la política de seguridad el servidor se obtuvo un 45.96% de seguridad en el mismo. Al realizar esta comparación se puede reflejar una mejora en el servidor con un incremento del 13% en seguridad del sistema operativo con el servidor de correo.

Las vulnerabilidades severas de alto nivel no fueron solventadas de manera automática al aplicar la política de seguridad, por lo que su solución fue de forma manual.

VULNERABILIDADES DE NIVEL MEDIO QUE FUERON SOLUCIONADAS AL APLICAR LA POLÍTICA DE SEGURIDAD NIST

Las vulnerabilidades severas de nivel medio que fueron solventadas de forma automática según el marco de referencia NIST se los describe a continuación.

GnuTLS-utils protocolos de comunicación

GnuTLS es una biblioteca de comunicaciones seguras que implementa los protocolos SSL, TLS y DTLS. Estos protocolos protegen la comunicación en línea y garantizan la privacidad mediante la encriptación de datos [24].

En la Figura 3.42 se observa que la vulnerabilidad fue solucionada exitosamente, el sistema descargó el paquete que contiene herramientas de manipulación de certificado y cliente TLS de línea de comando.

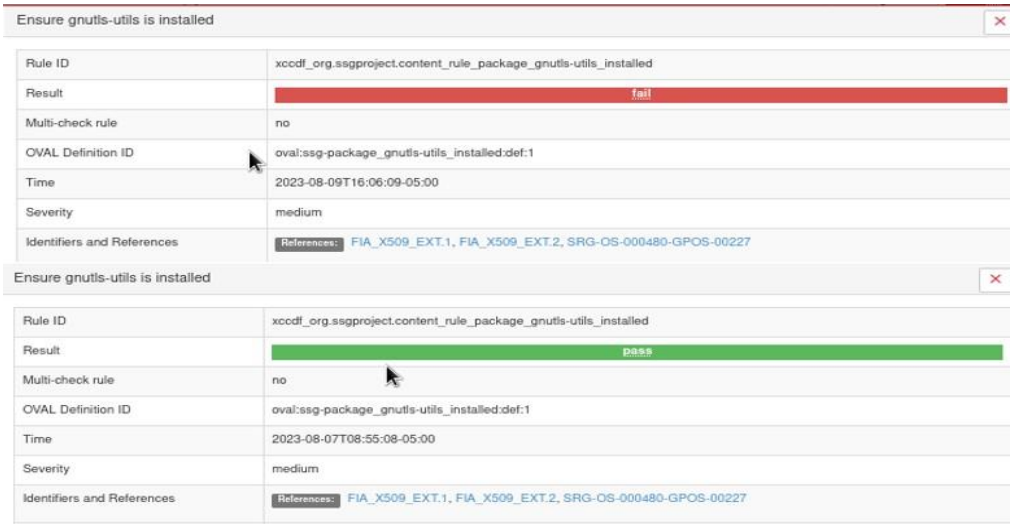


Figura 3.42 GnuTLS protocolos de comunicación

Paquete administrador de suscripción (*subcription-manager package*)

El paquete *suscription manager* de *Red Hat* es un servicio local, el cual administra los productos instalados, suscripciones y licencias de *software* en sistemas operativos de *Red Hat*. La instalación y configuración de *suscription manager* permite la descarga de actualizaciones y parches de seguridad, acceso al soporte técnico que proporciona *Red Hat,* gestión de suscripciones y licencia de *software* en el sistema. [25]

El paquete fue instalado de forma automática al aplicar la política de seguridad al sistema, la vulnerabilidad fue solucionada, ver la Figura 3.43.

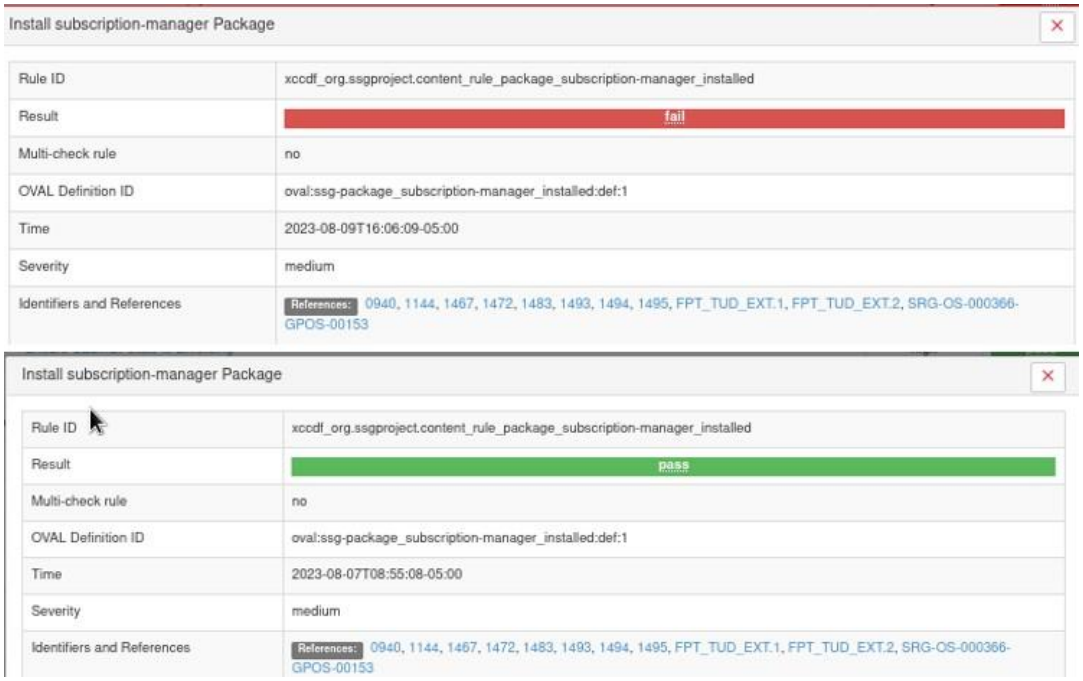


Figura 3.43 *Suscription manager* de *Red Hat*

Paquete dnf-*automatic*

En la figura Figura 3.44 se muestra que el paquete dnf-*automatic* fue solucionado al aplicar la política de seguridad. Dnf-*automatic* permite la gestión de actualizaciones de paquetes mediante el sistema dnf. Este paquete es muy necesario debido a que, mantiene el sistema actualizado de forma regular, disminuyendo el riesgo de vulnerabilidades en el sistema [26].

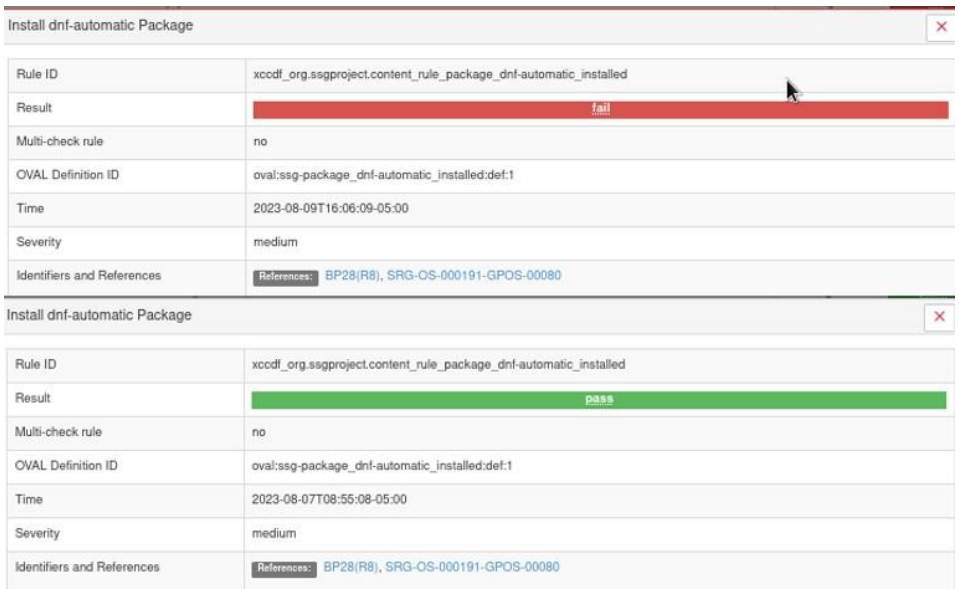


Figura 3.44 Paquete dnf-*automatic*

Paquete tmux

El paquete tmux permite implementar y configurar un mecanismo de bloqueo de sesión. Un bloque de sesión es la suspensión temporal de la sesión de un usuario, esta se ejecuta cuando el usuario deja de trabajar en el sistema operativo. En ocasiones, el usuario no realiza el bloqueo de sesión de forma manual, por lo que lleva al sistema operativo a identificar la inactividad y automáticamente bloquea la sesión de usuario [27]. En la Figura 3.45 se observa que el paquete fue instalado en el sistema operativo al aplicar la política de seguridad de forma automática.

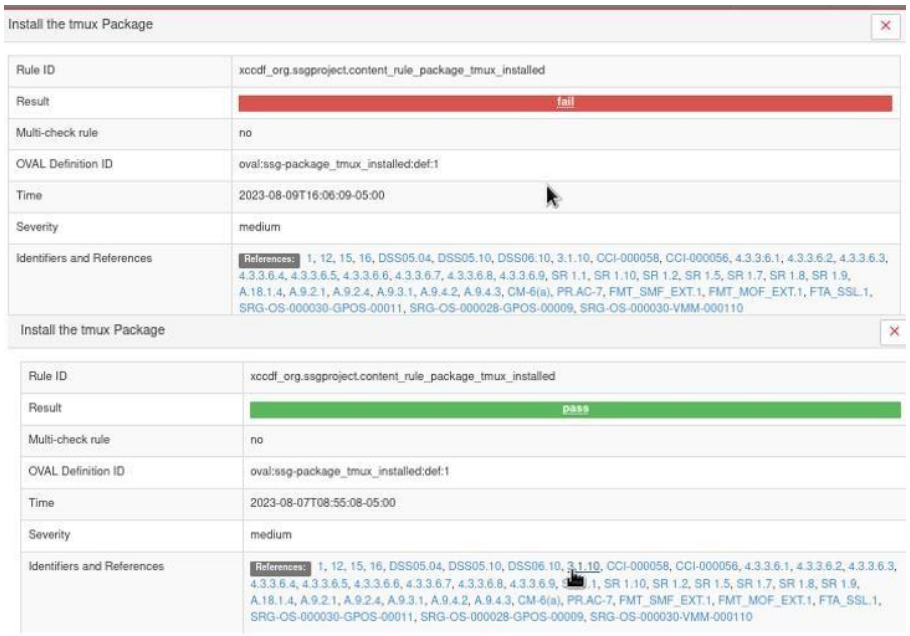


Figura 3.45 Paquete tmux

Paquete usbguard

El paquete usbguard protege al sistema de amenazas que pueden ser ocasionadas por dispositivos USB que son conectados al sistema. Su principal función es proteger al sistema de USB no autorizados. Esto se realiza mediante la implementación de funcionalidades básicas de inclusión en listas blancas y negras basadas en características específicas del dispositivo USB [28].

En la Figura 3.46 se muestra que la vulnerabilidad fue solventada de forma automática, el paquete *usbguard* se encuentra presente en el sistema operativo para la seguridad de este.

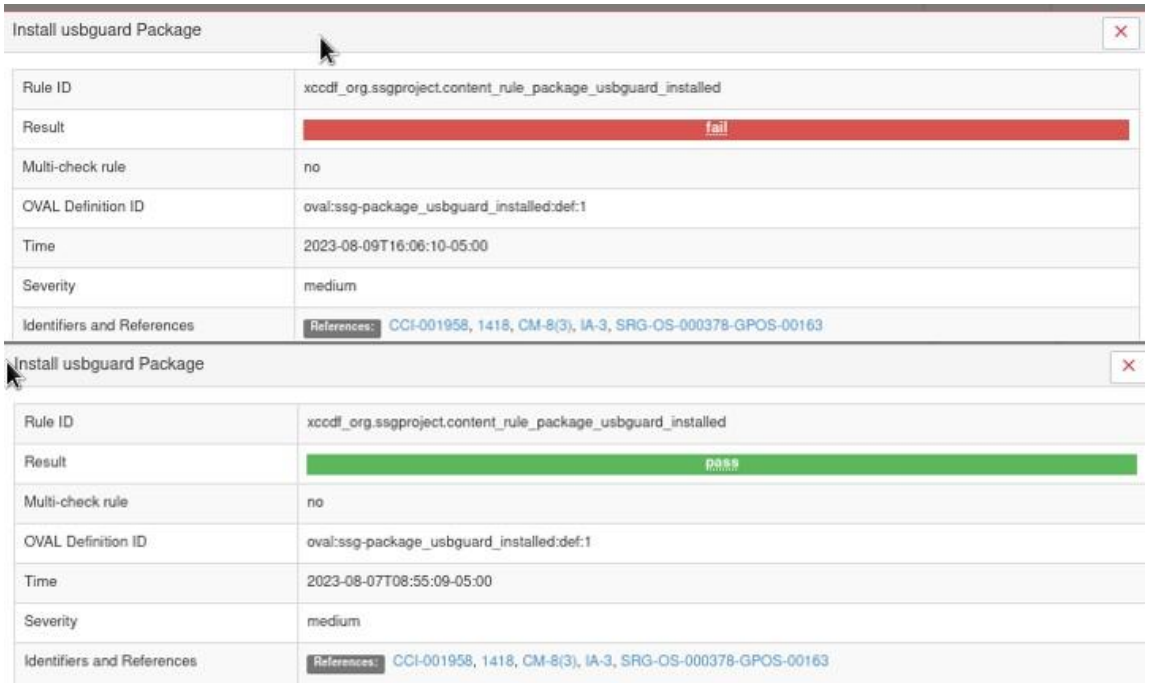


Figura 3.46 Paquete usbguard

SOLUCIÓN DE FORMA MANUAL DE LAS VULNERABILIDADES CON SEVERIDAD ALTA

Las políticas de alto nivel no fueron solventadas de manera automática, lo que conllevó a solucionarlas de manera manual; dado que son vulnerabilidades de alto riesgo, resulta importante corregirlas para salvaguardad la información y datos del sistema.

Habilitación del módulo FIPS

El módulo FIPS, definido por el marco de referencia NIST, asegura la integridad de un sistema mediante la implementación de módulos criptográficos que cifra la información. La Figura 3.47 muestra que el módulo de FIPS no se encuentra habilitado. Se ingresó el comando “” *fips-mode-setup –enable*” como se puede ver en la Figura 3.48.Despues de que el comando se haya ejecutado, se reinició el sistema para aplicar los cambios de la política en el sistema.

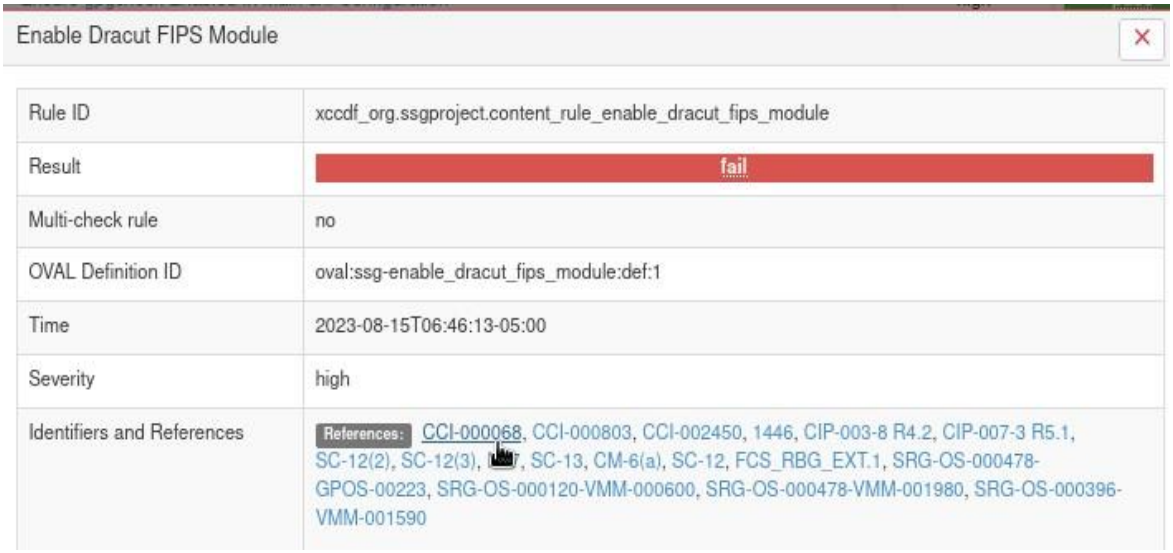


Figura 3.47 Módulo FIPS

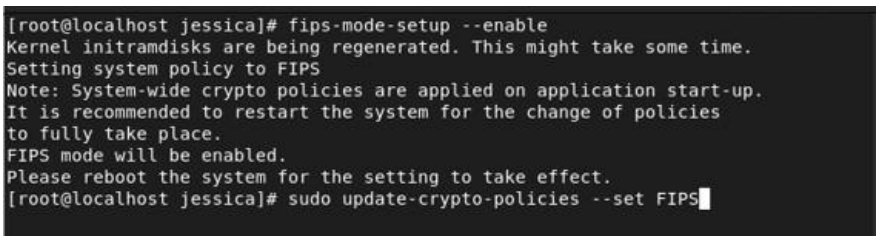


Figura 3.48 Habilitación del módulo de FIPS

Configuración de política criptográfica del sistema

Las políticas criptográficas se enfocan en la aplicación de cifrados seguros en el sistema operativo y de los programas que son implementados en el mismo, en este caso el servidor de correo. El uso de algoritmos seguros certifica la integridad y confidencialidad de la información. En la Figura 3.49 se puede ver que el sistema no cuenta con la configuración de esta política.

Para la configuración de la política de criptografía del sistema se ejecutó el comando “sudo update-crypto-policies –set FIPS” que emplea el cifrado de la política FIPS que se configuró anteriormente. Esta configuración se indica en la Figura 3.50.

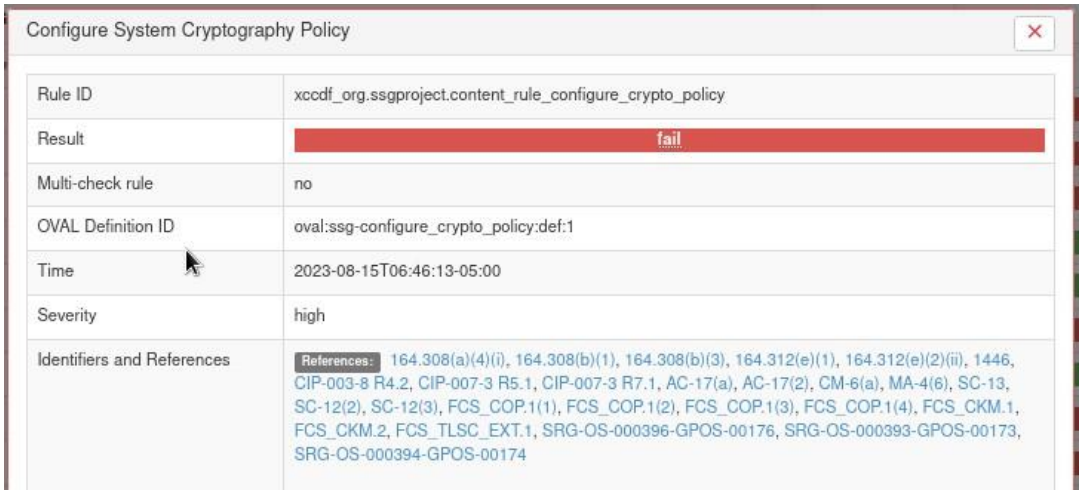


Figura 3.49 Política criptográfica

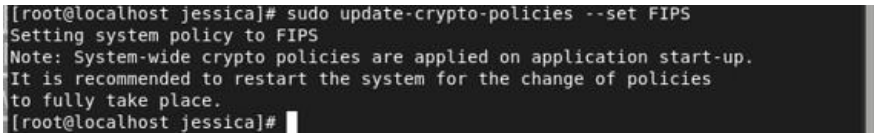


Figura 3.50 Ejecución de la política criptográfica

Habilitación del paquete gpg*check* para la verificación de paquetes locales

La implementación de esta política permite la verificación de las firmas de los paquetes locales antes de la instalación, lo que proporciona seguridad al sistema. En la Figura 3.51 se observa que la política no fue solventada de manera automática, por lo cual se realizó de forma manual.

La configuración de este paquete se llevó a cabo en el documento dnf.conf, el cual se encuentra en la ruta “cd /etc/dnf”, ver Figura 3.52. Para realizar la configuración, se ingresó con el comando “nano dnf.conf” al archivo y se insertó la siguiente línea: “*localpkg_gpgcheck*=1”. Posteriormente, se guardó los cambios realizados en el archivo a fin de aplicar las modificaciones.

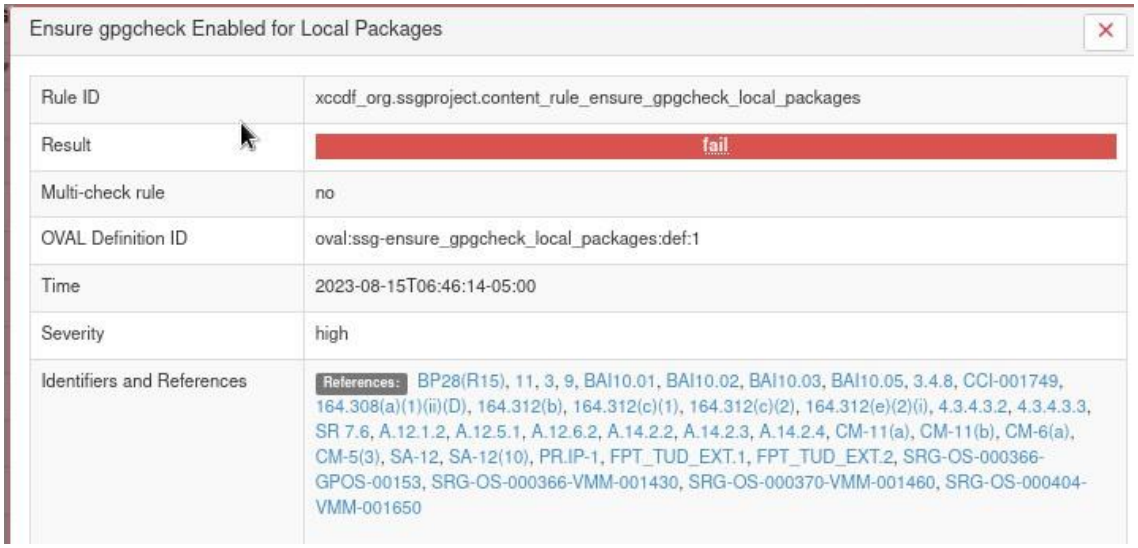


Figura 3.51 Local packages

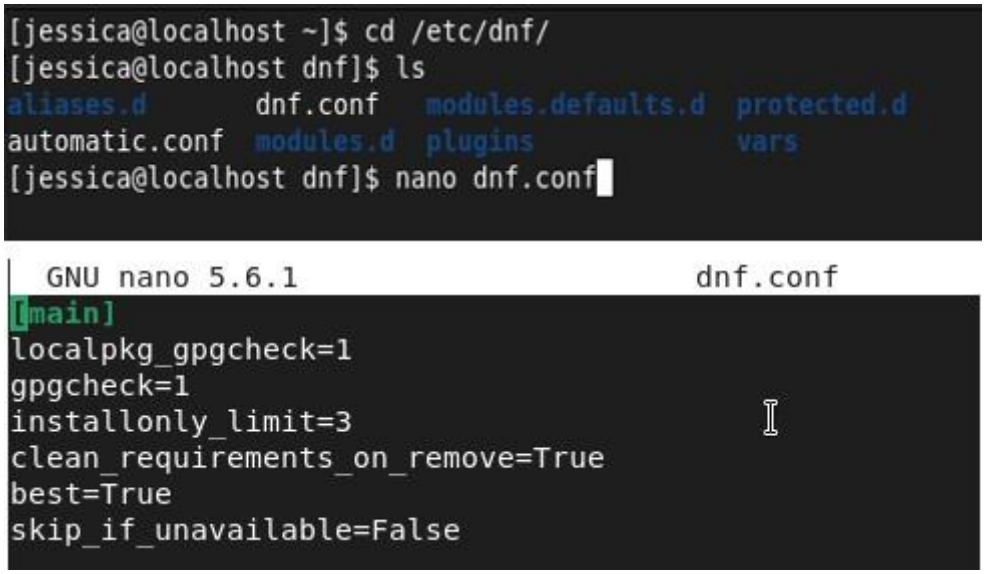


Figura 3.52 Archivo dnf.conf

Deshabilitar la acción de ráfaga Ctrl-Alt-Del

Es necesario deshabilitar esta política, ya que su activación puede ocasionar riesgos que afecten de disponibilidad a corto plazo del sistema. Por ejemplo, si un usuario está conectado por consola, existe la posibilidad presionar las teclas Ctrl-Alt-Del de manera involuntaria y provoqué el reinicio del sistema. En la Figura 3.53 se indica la ruta del archivo *system.conf* y la línea que se des comento para deshabilitar la ejecución las teclas Ctrl-Alt-Del.

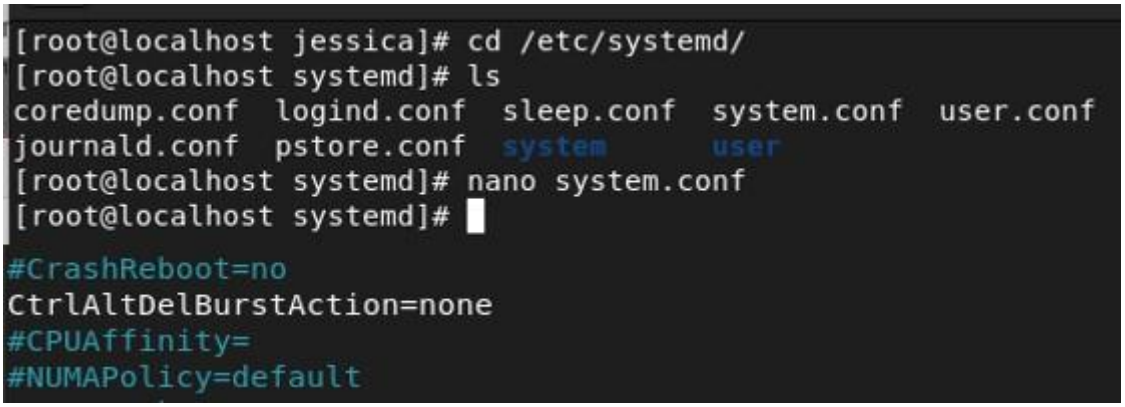


Figura 3.53 Archivo system.conf

Deshabilitar el acceso SSH a través de contraseñas vacías

Es importante educar al usuario colocar una contraseña para acceder al servidor por medio de SSH. Dado que acceder al servidor sin una contraseña implica riegos importantes para la seguridad del sistema. En la Figura 3.54 se puede ver la ruta donde se encuentra el archivo sshd_ config. en la Figura 3.55 se quitó el comentario de la siguiente línea "*PermitEmptyPasswords* no" para prohibir el inicio de sesión de SSH de cuentas con contraseñas vacías.

Figura 3.54 Archivo sshd_config

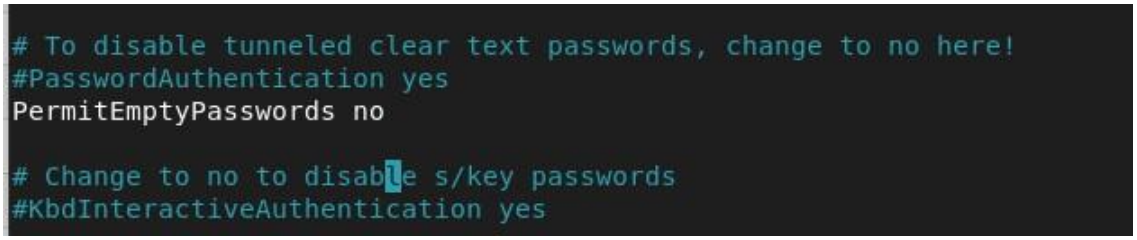


Figura 3.55 Deshabilitar el acceso SSH de contraseñas vacías

Modificar el puerto estándar de SSH

El puerto predeterminado de SSH es el puerto número 22. Por lo que es necesario cambiar el puerto de acceso a SSH debido a que existen numerosos *bots*

intentando acceder al sistema, además que expone al sistema operativo a ataques y amenazas. El cambio se realizó en el archivo ssh_cnfig donde se cambió el número de puerto y se quitó el comentario a la línea del puerto modificado, ver la Figura 3.56.

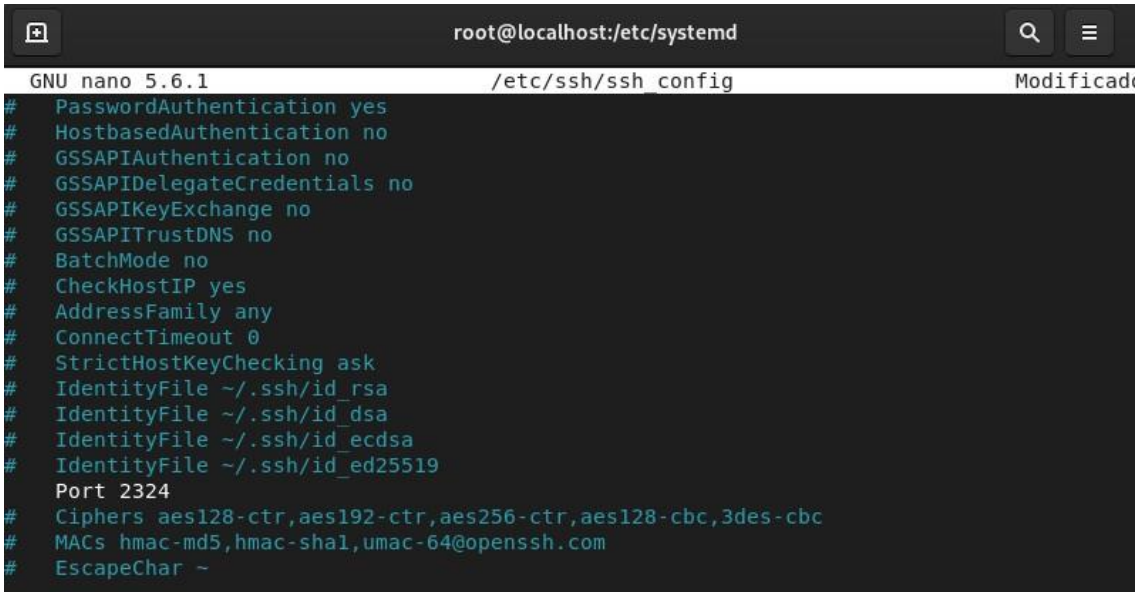


Figura 3.56 Cambio de puerto de SSH

TERCER REPORTE DE VULNERABILIDAD

Luego de haber solucionado las vulnerabilidades de forma manual. Se realizó un tercer escaneo, para obtener el informe de vulnerabilidades como se observa en la Figura 3.57. Se obtuvo un 47.73% de seguridad en el servidor después de solventar las vulnerabilidades de forma manual. Se solucionaron 6 de las 8 vulnerabilidades de nivel alto, ver la Figura 3.58.

En el Anexo III. III se puede observar el informe a detalle donde se constata el cambio realizado en el servidor.

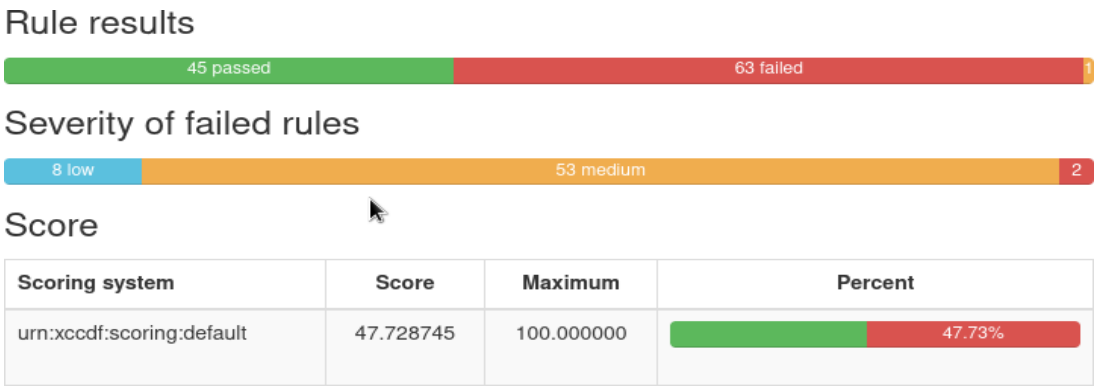


Figura 3.57 Escaneo del sistema después de solventar las vulnerabilidades con severidad alta

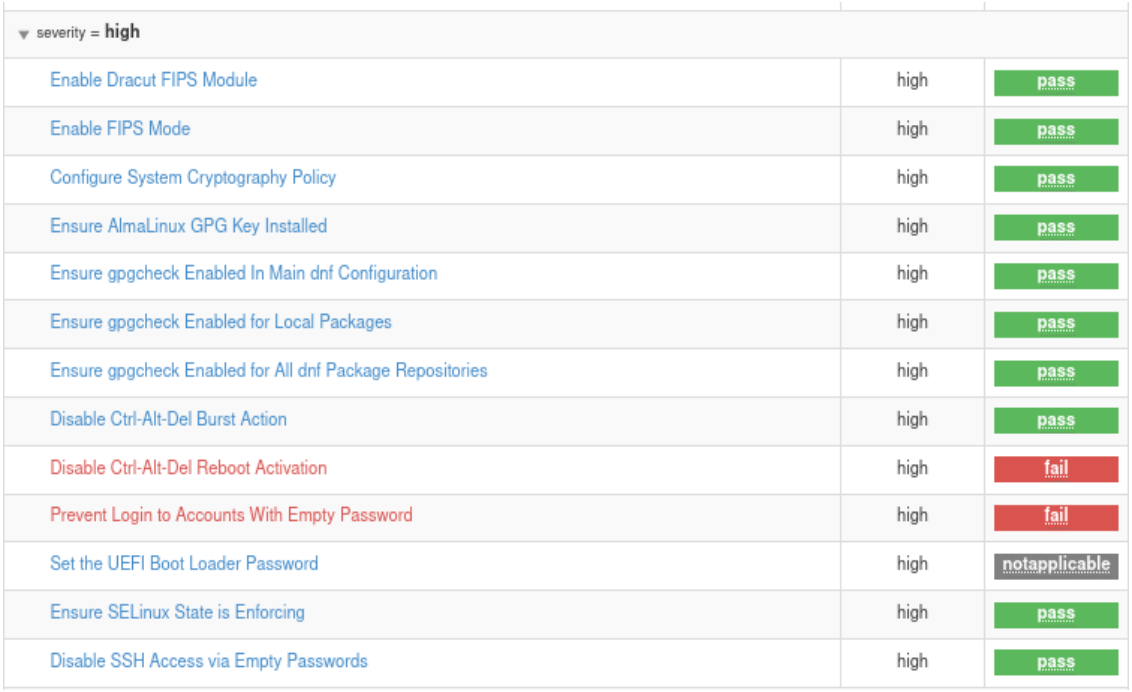


Figura 3.58 Vulnerabilidades de nivel alto después de solventar de forma manual

3.4 VERIFICACIÓN DEL *HARDENING* DEL SISTEMA OPERATIVO CON BASE EN LOS ELEMENTOS DE LA TRIADA CIA

Con el escaneo del tercer reporte de vulnerabilidades obtenido se valida que el sistema operativo de servidor cumpla con los principios fundamentales de la triada CIA. Para llevar a cabo, se organizó una tabla con los siguientes parámetros.

Severidad: es una clasificación de las vulnerabilidades en nivel alto, medio y bajo.

Políticas: nombre referente a la regla a implementar para solventar una vulnerabilidad.

Confidencialidad: parámetro de evaluación de confiabilidad que se cumple o no en el sistema.

Integridad: evaluación de integridad que se cumple o no en el sistema.

Disponibilidad: evaluación de disponibilidad que se cumple o no en el sistema.

En la Tabla 3.1,

Tabla **3.2** y Tabla 3.3 se muestran las reglas de severidad que fueron solventadas. Cada una de estas reglas corresponde un valor: alto, medio o bajo, en los elementos de triada CIA.

Tabla 3.1. Reglas de severidad de alto nivel

Severidad	Políticas	Confidencialidad	Integridad	Disponibilidad
Alta	Habilitación del módulo FIPS	Alta	Alta	Baja
	Habilitación del módulo Dracut FIPS	Alta	Alta	Baja
	Configuración de política criptográfica del sistema	Alta	Alta	Baja
	Habilitación del paquete gpgcheck para la verificación de paquetes locales	Media	Alta	Media
	Deshabilitar la acción de ráfaga Ctrl-Alt-Del	Baja	Baja	Alta

	Deshabilitar el acceso SSH a través de contraseñas vacías	Alta	Alta	Medio
	Modificar el puerto estándar de SSH	Alta	Media	Baja
	Asegurar que la clave GPG de Alma *Linux* está instalada	Alta	Alta	Baja
	Asegurar que gpgcheck esté habilitado en la configuración principal de dnf	Alta	Media	Baja
	Asegurar que gpgcheck esté habilitado para todos los repositorios de paquetes dnf	Alta	Media	Baja

Tabla 3.2 Reglas de severidad de medio nivel

Severidad	Vulnerabilidad	Confidencialidad	Integridad	Disponibilidad
Media	GnuTLS-utils protocolos de comunicación	Alta	Alta	Baja
	Instalar el paquete Crypto-policies	Alta	Media	Baja

	Configuración la biblioteca OpenSSL para utilizar la política de cifrado del sistema	Media	Alta	Baja
	Paquete scap-security-guide	Alta	Alta	Baja
	Paquete administrador de suscripción (*subcription-manager package*)	Alta	Baja	Baja
	Paquete dnf-automatic	Baja	Baja	Alta
	Paquete tmux	Alta	Alta	Baja
	Paquete usbguard	Alta	Alta	Baja
	Desactivación del servicio debug-shell systemD	Alta	Media	Baja
	Requerimiento de autenticación para el modo de usuario único	Baja	Media	Baja
	Habilitacion de *authselect*	Baja	Alta	Baja
	Configuración auditd flush priority	Baja	Alta	Baja

Tabla 3.3 Reglas de severidad de bajo nivel

Severidad	Vulnerabilidad	Confidencialidad	Integridad	Disponibilidad
Baja	Partición de disco /var/log/Audit	Media	Alta	Media
	Resolve information before writing to audit logs	Media	Alta	Media

GUÍA DE MEJORES PRÁCTICAS PARA EL ENDURECIMIENTO DEL SERVIDOR

Con el propósito de finalizar el cumplimento de los objetivos plateados para el desarrollo del proyecto, se estableció una guía de mejores prácticas de seguridad.

Para el sistema operativo.

- Controlar el acceso y permisos de los componentes de *hardware* a la red.
- Emplear herramientas de escaneo para la detención de vulnerabilidades en el sistema operativo.
- Implementar logaritmos de cifrado o módulos de criptografía para la codificación de los datos, tanto durante se encuentren almacenados o en tránsito.
- Realizar *backups* de la información de manera continua. Este proceso garantizará la recuperación de la información, si se llega a presentar alguna situación de ataque la información del sistema operativo.
- Actualizaciones continuas para mantener el sistema actualizado y protegido de vulnerabilidades que se presentan a diario. Actualizaciones del sistema y parches de seguridad configurados de forma automática ayuda a solventar al sistema inmediatamente se presente algún riesgo en la seguridad de este.
- Implementación de políticas que identifiquen la eliminación correcta y segura de archivos electrónicos.

- Implementar contraseñas fuertes para los usuarios y la cuenta del administrador.
- Capacitación sobre la ciberseguridad a todas las personas que tienen acceso a un computador o dispositivos informáticos. En caso de una organización, capacitar a los empleados para minimizar el riesgo de exposición de la información tanto personal como institucional.
- Monitoreo continuo del sistema para la detección de vulnerabilidades, detección de dispositivos no autorizados como USB y software adicionales.
- Examinar la red a la cual se encuentra conectado los equipos para la detección de usuarios o conexiones no autorizadas.
- Desactiva o desinstalar aplicaciones que no son necesarias en el sistema operativo.

Para el servidor de correo

- Instalación mínima, esto permitirá configurar el sistema operativo de servidor con servicios y aplicaciones esenciales para el correcto funcionamiento del servidor.
- Implementar contraseñas fuertes y seguras reduce el riesgo de exposición del sistema a amenazas y ataques al sistema.
- Deshabilitar servicios de acceso remoto al servidor. Emplear protocolos seguros para la conexión es una buena práctica para no exponer el sistema a una variedad de vulnerabilidades y ataques.
- Aplicar módulos de encriptación para mantener el sistema con algoritmos de cifrado, con el fin de resguardar los elementos correspondientes la triada CIA.
- Autenticación de multifactor para asegurar el acceso a las cuentas de correo.
- Implementación de cifrado SSL/TSSL para la comunicación y transmisión de los correos electrónicos.
- Configuración de firewall y segmentación de red para restringir el acceso de personal no autorizadas al servicio de correo desde el exterior.
- Realizar copias de seguridad diarias para la información y datos del servidor de correo.

- Restringir permisos y privilegios a las cuentas de usuarios, esto con el fin de evitar modificaciones o accesos no autorizados al servicio de correo.
- Realizar auditorías regulares del servidor para la identificación de vulnerabilidades que afecten la seguridad de este, esto permitirá que se solvente las posibles amenazas que exponen al servidor.
- Educar a los usuarios en ataques de *phishing* y otros riesgos relacionados con la afectación de la información.

En base a las buenas prácticas definidas previamente, las cual son esenciales para asegurar la integridad de la información del servidor, se puede concluir que no basta con simplemente aplicar una política de seguridad al sistema o realizar configuraciones esporádicas del mismo. Es muy importante realizar auditorías continuas que permitan la identificación de vulnerabilidades, permitiendo así solventar de forma adecuada las vulnerabilidades.

OPCIÓN DE SCAP *WORKBENCH* PARA ASEGURAMIENTO GLOBAL DEL SISTEMA OPERATIVO

Es importante abordar todas las vulnerabilidades, independientemente de su nivel de severidad, para garantizar la seguridad del sistema operativo. Dentro de la investigación realizada para el desarrollo del correspondiente trabajo de integración curricular, se ha identificado que la herramienta de escaneo de SCAP *Workbench* dispone de la funcionalidad de reglas de remediación, esta opción incluye configuraciones de sistema, parches de seguridad, la habilitación, des habilitación e instalación de servicios y paquetes que son necesarios para el sistema. En la Figura 3.59 se muestra el reporte final del escaneo después de aplicar la opción de "*remediation rule*".

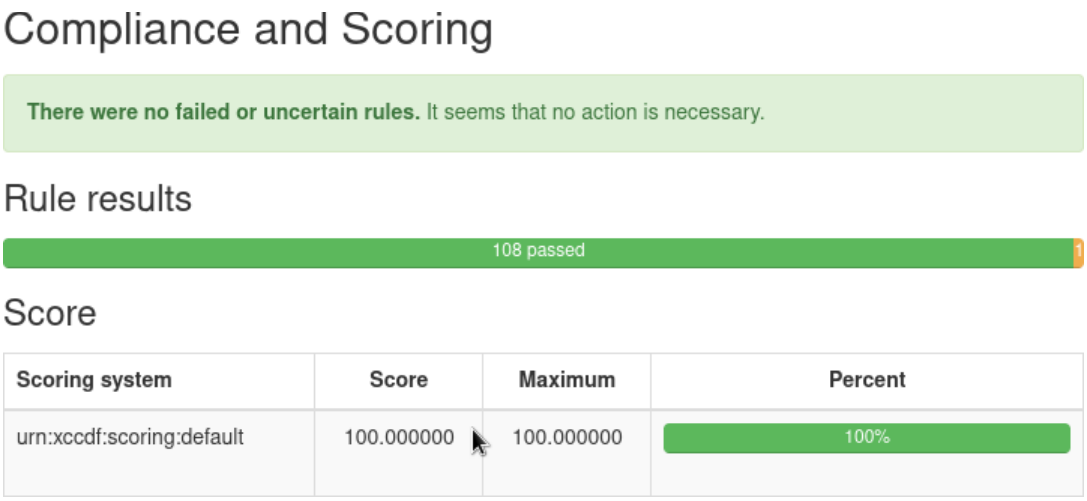


Figura 3.59 Aseguramiento global del sistema operativo

Después de realizar el escaneo del sistema operativo, se identificaron y resolvieron con éxito un total de 108 vulnerabilidades, lo que resultó en un sistema operativo completamente hardenizado.

Finalmente, se llevó a cabo una prueba de envió de correos electrónicos para verificar la efectivad de la implementación de las políticas de seguridad que se aplicaron por completo en el sistema operativo. En la Figura 3.60 y Figura 3.61 se pueden observar los comandos utilizados para la ejecución de envió de correos.

```
[root@localhost jessica]# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 Jess.epn.edu.ec ESMTP Postfix
mail from:<luis>
250 2.1.0 Ok
rcpt to:<carla>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
hla Carla, como te encuentras ?
.
250 2.0.0 Ok: queued as 75EC610768C
quit
221 2.0.0 Bye
Connection closed by foreign host.
[root@localhost jessica]# clear
```

Figura 3.60 Verificación de envió de correo

```
[root@localhost jessica]# telnet localhost 110
Trying ::1...
Connected to localhost.
Escape character is '^]'.
+OK Dovecot ready.
user carla
+OK
pass a1r2l3c4
+OK Logged in.
list
+OK 5 messages:
1 401
2 422
3 423
4 428
5 408
.
retr 5
+OK 408 octets
Return-Path: <luis@eppn.edu.ec>
X-Original-To: carla
Delivered-To: carla@eppn.edu.ec
Received: from localhost (localhost [IPv6:::1])
        by Jess.epn.edu.ec (Postfix) with SMTP id 75EC610768C
        for <carla>; Wed,  6 Sep 2023 10:04:44 -0500 (-05)
Message-Id: <20230906150457.75EC610768C@Jess.epn.edu.ec>
Date: Wed,  6 Sep 2023 10:04:44 -0500 (-05)
From: luis@eppn.edu.ec

hla Carla, como te encuentras ?
.
```

Figura 3.61 Verificación de recepción de correo

4 CONCLUSIONES

- Un sistema operativo de servidor sin políticas de seguridad es expuesto a una gran variedad de riesgos y amenazas que ponen en riesgo los principios fundamentales de la información. La falta de políticas de seguridad en el sistema lo hacen susceptible a los ataques de más comunes en la ciberdelincuencia. Por ende, es importante la implementación de políticas y perfiles de seguridad para disminuir las vulnerabilidades en el sistema.
- La ausencia de políticas y buenas prácticas de seguridad en el sistema tiene como consecuencias negativas como la alteración de la información, manipulación y robo de esta, infracción de la privacidad de los datos y alteración de la disponibilidad del sistema. Esto conlleva a pérdidas de tiempo y dinero a la organización a corto y largo plazo si no se solventan a tiempo las vulnerabilidades identificadas en el sistema
- Las herramientas de escaneo de vulnerabilidades ayudan con la detección de vulnerabilidades en el sistema operativo, esta acción permite al sistema solventar vulnerabilidades antes que sean explotadas por un atacante o ciberataques. La herramienta SCAP *Workbench* analiza el sistema y emite un informe de las vulnerabilidades y a su vez de la solución de esta. Esta herramienta permite obtener una guía completa de seguridad para el sistema operativo de servidor Alma *Linux*.
- El *hardening* en sistemas operativos de servidor y en servidores se enfoca en la detección de vulnerabilidades, por lo cual es importante que sea un proceso continuo que se realice, debido a que las amenazas y ataques van evolucionado constantemente. Realizar este proceso ayudará al sistema solventar a tiempo las vulnerabilidades que se presenten, salvaguardando la integridad, confiabilidad y disponibilidad del sistema.
- En el análisis del desarrollo del proyecto se eligió emplear el marco de referencia NIST, debido a que ofrece una estructura y guía para solventar los desafíos de seguridad y privacidad en las organizaciones. Además, ayuda en la ejecución de medidas de seguridad y gestión de amenazas efectivas en las organizaciones de modo que proporciona y garantiza la seguridad de la información.

- Es se suma importancia solucionar todas las vulnerabilidades del sistema, incluso si son de nivel de severidad baja, debido a que puede ocasionar problemas menores que involucren la seguridad del todo el sistema. A pesar de que sean vulnerabilidades de nivel bajo, no se debe pasar por alto este tipo de alertas que son identificadas, ya que el sistema se igual manera se encuentra expuesto. Actualmente, se dispone de varias herramientas de seguridad que permite el análisis minucioso de la seguridad del sistema, llevando a cabo el aseguramiento y fortalecimiento de la seguridad del sistema.
- Cómo consecuencia de llevar a cabo las políticas de seguridad se pudo observar que se cumplió con el modelo de la triada CIA para el referente de la seguridad de la información. La verificación de estos principios fundamentales fue de suma importancia en el desarrollo del *hardening.*

5 RECOMENDACIONES

- Se recomienda realizar evaluaciones regulares de seguridad en el sistema que se trabaja y mantener actualizaciones del sistema, empleando prácticas de *hardening* para garantizar la seguridad de sistema.
- Durante la instalación es recomendable optar por una configuración personalizada, debido a que se puede seleccionar los paquetes y servicios que estén disponibles en el sistema. Mientras más detalladas sean las configuraciones en el sistema menos riesgos de ataques puede ocurrir en el sistema. Las configuraciones por *default* en los sistemas pueden exponen los principios fundamentales de la información.
- Con respecto a la comprobación de envió de recepción de correo por telnet, no es recomendable emplear este tipo de conexión remota, ya que la información se transmite en texto plano, esto conlleva a que terceras personas pueden interceptar este tipo de conexión y causar una alteración en la información. En el proceso de análisis del proyecto se empleó este tipo de conexión debido a que, después de aplicar la política de seguridad permitió la comprobación de correo por medio de telnet ya que no se permitió el uso de SSH por temas de certificados de autenticación que dispone una organización avalada por NIST.
- Es recomendable educar a los usuarios a emplear contraseñas seguras y fuertes, desactivar cuentas de usuarios que no se encuentren activas, el uso de factores de autenticación de ingreso de sesión a una cuenta. El implementar estas acciones minimizara los riesgos de ataques en el sistema.
- Emplear módulos de encriptación de la información y datos en el sistema es muy importante. Esta práctica permite la implementación de cifrado, lo que establece cierto nivel de seguridad al sistema. A demás, garantiza la privacidad de los datos e información transmitidos, es una práctica muy importante para la protección del sistema y la confidencialidad e integridad del sistema.

6 REFERENCIAS BIBLIOGRÁFICAS

[1] «Seguridad de la información como una ventaja competitiva».

[2] «Triángulo de Seguridad Informática: Qué es y sus objetivos», *OpenWebinars.net*, 25 de agosto de 2021. https://openwebinars.net/blog/triangulo-de-seguridad-informatica-que-es-y-sus-objetivos/ (accedido 31 de julio de 2023).

[3] «¿Qué es un ataque de denegación de servicio (DoS)?», *Cloudflare*. https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/ (accedido 31 de julio de 2023).

[4] «¿Qué es un ataque DDoS? | Akamai». https://www.akamai.com/es/glossary/what-is-ddos (accedido 31 de julio de 2023).

[5] https://www.facebook.com/ciberseguridadblog, «25 Tipos de ataques informáticos y cómo prevenirlos», *CIBERSEGURIDAD .blog*, 20 de enero de 2018. https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/ (accedido 31 de julio de 2023).

[6] «Hardening informático ¿Qué es?» https://www.ciset.es/publicaciones/blog/746-hardening (accedido 31 de julio de 2023).

[7] «¿Qué es un sistema operativo de servidor (SO de servidor)? - definición de techopedia - Audio 2023», *Icy Science*, 2023. https://es.theastrologypage.com/server-operating-system (accedido 31 de julio de 2023).

[8] «Hardening de APP´s ¿Qué es y cómo funciona?» https://es.linkedin.com/pulse/hardening-de-apps-qu%C3%A9-es-y-c%C3%B3mo-funciona-topdigital-consulting (accedido 31 de julio de 2023).

[9] J. L. M. Cruz, «Endurecimiento (hardening) en dispositivos de red: Routers y switchs».

[10][10] https://rraae.cedia.edu.ec/Record/ESPOL_6032935157d38618be8d31e89e9ff56e (Accedido 31 de julio de 2023).

[11] «AlmaLinux Installation Guide | AlmaLinux Wiki». https://wiki.almalinux.org/documentation/installation-guide.html#requirements (accedido 31 de julio de 2023).

[12] «Apéndice A. Referencia de requisitos del sistema Red Hat Enterprise Linux 9 | Portal del cliente de Red Hat». https://goo.su/RzRjY (accedido 9 de septiembre de 2023).

[13] H. Maurya, «How to download and install CentOS 8 minimal server version», *Linux Shout*, 11 de mayo de 2020. https://linux.how2shout.com/download-install-centos-8-minimal-server-iso/ (accedido 9 de septiembre de 2023).

[14] «Cómo instalar Rocky Linux 9.0 paso a paso». https://es.linux-console.net/?p=2715#gsc.tab=0 (accedido 9 de septiembre de 2023).

[15] «Escáner de vulnerabilidades: 10 herramientas para conocer - Sky.One». https://skyone.solutions/es/centro/escaner-de-vulnerabilidad/ (accedido 31 de julio de 2023).

[16] «Escáner de vulnerabilidades de Linux | Herramienta de análisis de vulnerabilidades de Linux - ManageEngine Vulnerability Manager Plus». https://goo.su/lG6nC (accedido 31 de julio de 2023).

[17] «Red Hat Security Data API - Red Hat Customer Portal». https://access.redhat.com/labsinfo/securitydataapi (accedido 31 de julio de 2023).

[18] «Nessusv7SCAPAssessments.pdf». Accedido: 15 de agosto de 2023. [En línea]. Disponible en: https://docs.tenable.com/other/nessus/Nessusv7SCAPAssessments.pdf

[19] Alex, «Explicación de los 7 principales estándares y marcos de seguridad de TI», *Krypton Solid*, 4 de diciembre de 2021. https://kryptonsolid.com/explicacion-de-los-7-principales-estandares-y-marcos-de-seguridad-de-ti/ (accedido 31 de julio de 2023).

[20] «National Institute of Standards and Technology», *NIST*, 26 de julio de 2023. https://www.nist.gov/ (accedido 31 de julio de 2023).

[21] «CIS Controls», *CIS*. https://www.cisecurity.org/controls/ (accedido 15 de agosto de 2023).

[22] «The Seven Principles of Privacy By Design | Carbide», 25 de enero de 2023. https://carbidesecure.com/resources/the-seven-principles-of-privacy-by-design/ (accedido 15 de agosto de 2023).

[23] Joint Task Force Interagency Working Group, «Security and Privacy Controls for Information Systems and Organizations», National Institute of Standards and Technology, sep. 2020. doi: 10.6028/NIST.SP.800-53r5.

[24] por D. Wahlstrom, «Tu Guía Completa Sobre SSL/TLS y HTTPS», *Guías para Sitios Web, Tips & Conocimiento*, 25 de abril de 2022. https://www.dreamhost.com/blog/es/guia-completa-ssl-tls/ (accedido 18 de agosto de 2023).

[25] «1.8. Registro del sistema y gestión de las suscripciones Red Hat Enterprise Linux 8 | Red Hat Customer Portal». https://goo.su/sPNb (accedido 18 de agosto de 2023).

[26] «DNF Automático — documentación de dnf - latest». https://dnf.readthedocs.io/en/latest/automatic.html (accedido 19 de agosto de 2023).

[27] rgerardi, «A beginner's guide to tmux», *Enable Sysadmin*, 13 de septiembre de 2022. https://www.redhat.com/sysadmin/introduction-tmux-linux (accedido 20 de agosto de 2023).

[28] «Capítulo 15. Protección de sistemas contra dispositivos USB intrusivos Red Hat Enterprise Linux 8 | Portal de clientes de Red Hat». https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/protecting-systems-against-intrusive-usb-devices_security-hardening (accedido 20 de agosto de 2023).