ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE *HARDENING* EN SISTEMAS OPERATIVOS DE SERVIDOR

IMPLEMENTACIÓN DE *HARDENING* EN ROCKY LINUX CON CIS

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

ERIK FERNANDO ORTEGA HERNANDEZ

erik.ortega@epn.edu.ec

DIRECTOR: ING. GABRIELA KATHERINE CEVALLOS SALAZAR

gabriela.cevalloss@epn.edu.ec

DMQ, julio 2024

CERTIFICACIONES

Yo, Erik Fernando Ortega Hernández 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.

Erik Fernando Ortega Hernández

erik.ortega@epn.edu.ec

erik.ortega.f@gmail.com

Certifico que el presente trabajo de integración curricular fue desarrollado por Erik Fernando Ortega Hernández, bajo mi supervisión.

GABRIELA KATHERINE CEVALLOS SALAZAR

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.

Erik Fernando Ortega Hernández

C.I.:1754039046

DEDICATORIA

El presente proyecto es una forma de agasajo a mi madre, por darme su amor incondicional y apoyo en cada situación de mi vida, su presencia en todo momento fue fundamental en el desarrollo de este logro académico. Desde el primer instante en iniciar mi carrera ha sido mi guía, orientándome con su sabiduría y paciencia. Sus palabras de aliento me motivaron a continuar en cada momento de mi vida. Le dedico esta tesis por su confianza en mis habilidades, incluso cuando dudaba de mí mismo. Su creencia en mí ha sido lo que me da fuerza, haciéndome superar cada obstáculo y alcanzar mis metas.

Erik Ortega

AGRADECIMIENTO

Para empezar, quiero dar gracias a Dios quien es mi motor en todas mis acciones. De igual forma a mi madre, le agradezco por brindarme su mano no solo en mi carrera, sino en todos los aspectos de mi vida, agradezco todos sus esfuerzos para hacerme una persona de bien. A mis hermanos John y Diego, por darme un notorio apoyo en mis estudios y ayudarme en las situaciones más importantes de mi vida. Gracias a Michelle Vargas y Danna Ortega, por brindarme su apoyo incondicional y lealtad, que han motivado mi vida, además de darme palabras de aliento. Gracias a Raúl por sus enseñanzas y ayudarme a desarrollar mis habilidades.

Agradezco a todos los profesores que he tenido durante mi estancia en la Escuela Politécnica Nacional, sus conocimientos y experiencias me ayudaron en mi formación académica y personal. Finalmente, deseo hacer un agradecimiento especial a la ingeniera Gabriela Cevallos por su tutela de principio a fin en mi tesis, además de ayudarme en toda mi carrera universitaria con palabras de aliento y consejos que me fueron de mucha utilidad.

Erik Ortega

ÍNDICE DE CONTENIDOS

RESUMEN

La siguiente tesis se enfoca en el endurecimiento del sistema operativo Rocky Linux 8.9, este proceso es mejor conocido como *hardening* y busca mejorar la seguridad de los sistemas informáticos. Así pues, se tienen los propósitos de examinar vulnerabilidades, hallar huecos de seguridad y corregir dichas fallas para generar un sistema menos susceptible a diferentes ataques externos. Para trabajar este proyecto se tienen en cuenta las recomendaciones de seguridad CIS que son de importancia a la hora de la ciberseguridad.

Para empezar, la primera parte del trabajo presenta las características a lograr, el problema existente y los conceptos necesarios para entender el desafío a resolver como también su resolución. Se exponen los objetivos: general y específicos, el marco teórico que es fundamental para definir las herramientas a usar y el alcance de la tesis. En este apartado, se definen los estándares de seguridad, sistema operativo e instrumentos de trabajo para ejecutar el proceso de *hardening.*

A continuación, la parte dos define el proceso necesario para lograr los objetivos específicos y el objetivo general, es la explicación de la metodología a ocupar en todo el proceso.

En la parte tres se define la demostración de los resultados que se generaron en el transcurso del trabajo, además se otorga un análisis del producto resultante en las acciones ejecutadas. Los aspectos que involucran este ítem son la instalación del sistema operativo Rocky Linux 8.9, el levantamiento del servicio de correo, la instalación de OpenSCAP como herramienta de escaneo de huecos de seguridad y los diferentes resultados que otorga. Además, se presenta una serie de acciones recomendadas en la ciberseguridad.

Para finalizar, la última parte entrega conclusiones basadas en los objetivos establecidos, recomendaciones del proyecto y la bibliografía que se utilizó para el tema de tesis.

PALABRAS CLAVE: Rocky Linux, OpenSCAP, vulnerabilidades, *hardening*, CIS.

ABSTRACT

The thesis project presented is about the hardening of the Rocky Linux 8.9 operating system, this process seeks to improve the security of computer systems. Thus, the objective is to find vulnerabilities, find security holes and correct these flaws to generate a system less susceptible to different external attacks. In order to work on this thesis, the CIS security recommendations that are important for cybersecurity are taken into account.

In the first section of the work, the characteristics to be achieved, the existing problem and the concepts necessary to understand the challenge to be solved as well as its resolution are shown. The general and specific objectives, the theoretical framework that is essential to define the tools to be used and the scope of the thesis are presented. In this section, the security standards, operating system and working instruments to execute the hardening process are defined.

The next section defines the process necessary to achieve the general objective and the specific objectives, it is the explanation of the methodology to be used in the whole process.

Part three is intended for the demonstration of the results generated in the course of the work, and an analysis of the product resulting from the executed actions is also provided. The aspects involved in this item are the installation of the Rocky Linux 8.9 operating system, the installation of the mail service, the installation of OPENSCAP as a security hole scanning tool and the different results it provides. In addition, a series of recommended actions in cybersecurity is presented.

Finally, the last part delivers conclusions based on the established objectives, recommendations of the project and the bibliography used in the thesis topic.

KEYWORDS: Rocky Linux, OpenSCAP, *vulnerabilities, hardening,* CIS.

1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

El presente proyecto consiste en implementar un proceso de *hardening* en sistemas operativos de servidor 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 puede infiltrase.

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 mejorar la seguridad en el servidor. Este análisis determinará si se ha mejorado la seguridad del servidor.

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 políticas de seguridad.
- Implementar 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 en base a los elementos de la triada CIA.

1.3 Alcance

En primera instancia se investigarán herramientas de escaneo, de 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 endurecerá al servidor con el fin de obtener una mejora en el reporte de vulnerabilidades obtenido de la herramienta de escaneo. Se compararán los reportes para observar cuáles parámetros 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 mejores prácticas, con esto se implementa *hardening* en un 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

Hardening en sistemas operativos

El endurecimiento de un sistema es el proceso en le que se aplica configuraciones y medidas de prevención de vulnerabilidades para minimizar el área de peligro y proteger contra las amenazas. Se debe entender que aplicar seguridad a un entorno se inicia con la selección de un sistema operativo y las configuraciones respectivas durante su proceso de alogamiento. Esto incluye la exclusión de funciones irrelevantes, la instalación de actualizaciones, la asignación de reglas de acceso y la ejecución de controles de seguridad avanzados [1]. Este proceso asegura que el sistema sea seguro y confiable. Muchos sistemas operativos están hechos para ser fáciles de usar, pero no necesariamente seguros cuando se instalan por primera vez. Se pueden activar medidas de seguridad extra para que los sistemas sean parte de entornos muy seguros y confiables.

El endurecimiento, también conocido como *hardening*, es un método para mejorar la seguridad del sistema operativo usando varias estrategias y herramientas. En este proyecto se explica cómo se realizó el *hardening* en Rocky Linux 8.9, que se usa como servidor de correo. Por eso, es importante entender las ciber amenazas y la seguridad en los sistemas operativos de servidor.

Sistemas Operativos de Servidores Basados en Linux

Los sistemas operativos de servidor basados en Linux son muy populares en las empresas porque son estables, seguros y flexibles. La cantidad de vulnerabilidades que se encuentran cambian en función de los sistemas que se elijan [2]. Algunos riesgos pueden venir de software desactualizado, usuarios que no están activos, inicios de sesión innecesarios y servicios deshabilitados que no se han inventariado, todos los cuales pueden ser aprovechados por un atacante. A continuación, se muestran algunas variantes de Linux:

Red Hat Enterprise Linux (RHEL)

Este sistema operativo, conocido por su estabilidad y soporte a largo plazo, es la opción favorita en las empresas. Ofrece funciones de seguridad avanzadas y herramientas que hacen más fácil la administración de muchos servidores. RHEL es completamente

compatible para usar en producción, tanto en instalaciones locales como en la nube. Además, los usuarios de CentOS Linux pueden cambiarse directamente a RHEL [3].

Alma Linux

Alma Linux surgió como una alternativa a CentOS después de que Red Hat cambiara el enfoque hacia CentOS Stream. Es una distribución gratuita y estable, compatible en binario con RHEL, lo que asegura un entorno seguro y confiable. Además, Alma Linux tiene la característica de ser de código abierto que es impulsado por la comunidad [4].

Debian

Debian se diferencia por ser una de las versiones más antiguas de Linux y es conocida por su estabilidad y seguridad. Se utiliza tanto en servidores como en escritorios, ofrece un amplio repositorio de software y es completamente gratuito. Debian se enfoca en la libertad y la protección del software. [5].

CentOS

CentOS Linux ha sido una distribución popular para servidores debido a su compatibilidad con RHEL y su estabilidad. Sin embargo, la comunidad ha comenzado a buscar otras alternativas como Rocky Linux y Alma Linux. [6].

Rocky Linux

Rocky Linux se creó como una alternativa a CentOS, manteniendo la estabilidad y compatibilidad con RHEL [7].

Distribución Rocky Linux 8.9

Rocky Linux 8.9 proporciona una plataforma robusta y segura para servidores, enfocada en la estabilidad a largo plazo y con una comunidad activa. Fue desarrollado en respuesta a la discontinuación de CentOS por Red Hat, bajo el liderazgo de Gregory Kurtzer, el fundador original de CentOS [7].

Este sistema operativo de servidor se conoce por ser una versión sustentada en RHEL, se elaboró para ofrecer una plataforma segura y estable para empresas que utilizan servidores. Esta versión mantiene la compatibilidad binaria con Red Hat, ofreciendo una alternativa confiable tras los cambios en CentOS. Desde su lanzamiento en diciembre de 2020, Rocky Linux ha evolucionado rápidamente, con su primera versión estable lanzada en junio de 2021.

Herramientas de escaneo de vulnerabilidades

Las herramientas de escaneo son cruciales para encontrar y reducir vulnerabilidades en los sistemas operativos. Hay muchas herramientas diferentes diseñadas para distintos propósitos, como escanear aplicaciones web o dispositivos móviles [8]. Ejemplos de estas herramientas son Nessus Vulnerability Scanner y WhatWeb, que se especializan en escanear sitios web. Otras herramientas importantes incluyen:

SCAP Workbench

Esta herramienta se define como una interfaz gráfica que ayuda a los administradores evaluar la seguridad de sus sistemas según los estándares SCAP. Facilita la implementación de guías de seguridad y la evaluación del cumplimiento del sistema [9].

OpenSCAP

OpenSCAP es una agrupación de características que pueden implementar y verificar el cumplimiento de las políticas de seguridad basadas en SCAP. Permite realizar escaneos de seguridad, aplicar configuraciones de fortalecimiento y generar informes detallados sobre el estado de seguridad del sistema [10].

Scap-security-guide

Scap-security-guide da perfiles de seguridad y contenido SCAP para evaluar el cumplimiento con estándares de seguridad reconocidos, como los del NIST y CIS. Esta herramienta es clave para automatizar el fortalecimiento de los sistemas operativos [11].

Nessus Vulnerability Scanner

Se considera un mecanismo sofisticado para el análisis de amenazas que identifica vulnerabilidades tanto en redes como en sistemas. Se utiliza para auditorías de seguridad y pruebas de penetración [12].

OpenVAS

OpenVAS es una herramienta gratuita para administrar y escanear vulnerabilidades. Permite a los administradores identificar y corregir problemas de seguridad de manera proactiva [13].

Seguridad Informática

Este concepto hace alusión a las reglas y procedimientos que protegen los sistemas de información contra ataques y accesos no autorizados. Su objetivo es mantener la confidencialidad, integridad y disponibilidad de los datos y de los sistema operativos que los alojan [14]. Existen varias organizaciones y normas importantes en este campo:

NIST

El Instituto Nacional de Estándares y Tecnología (NIST) ofrece reglas y directrices para mejorar la seguridad de los datos que se tienen en los sistemas, un claro ejemplo es: *NIST Cybersecurity Framework* [15].

ISO 27001

Se conoce por ser un estándar a nivel mundial para los sistemas de gestión de la seguridad de la información, define los parámetros para desarrollar, aplicar, resguardar y renovar dichos sistemas. Asiste a las instituciones para escudar los recursos de los sistemas de manera sistemática como también eficaz [16].

CIS

El Centro de Seguridad de Internet ofrece directrices para la defensa ante vulnerabilidades y propone puntos de referencia para proteger sistemas y datos. Los controles CIS son un conjunto de acciones recomendadas para mitigar riesgos y mejorar la ciberseguridad de una organización [17].

Tríada CIA

La tríada CIA es un modelo que se compone de tres pilares: confidencialidad, integridad y disponibilidad [18]. Este esquema ayuda a identificar fallas de seguridad y formular soluciones adecuadas para la protección de datos:

Confidencialidad

La confidencialidad asegura que la información solo esté disponible para personas autorizadas. Esto se logra mediante controles de acceso estrictos para evitar que datos sensibles sean accesibles a individuos no autorizados.

Integridad

La integridad garantiza que los datos sean precisos y no hayan sido alterados sin autorización. Es crucial para que los datos se consideren fiables y auténticos, y se puede mantener utilizando métodos como hashes, cifrado y certificados digitales.

Disponibilidad

La disponibilidad se asegura de que los sistemas y datos estén accesibles para las personas autorizadas cuando los necesiten. Esto se logra mediante sistemas redundantes, actualizaciones constantes de software y copias de seguridad periódicas [18].

2 METODOLOGÍA

El actual trabajo de titulación tiene como finalidad identificar y evaluar las vulnerabilidades presentes en el sistema operativo Rocky Linux 8.9, haciendo uso del servicio de correo con ayuda de Postfix sin políticas de seguridad implementadas.

En primer lugar, se realizó el montaje del sistema Rocky Linux 8.9 en VirtualBox y se configuró Postfix para el levantamiento del servidor de correo con sus respectivas vulnerabilidades sin solucionar. Así mismo, se generó un reporte inicial con las reglas fallidas haciendo uso del ecosistema OpenSCAP.

Como siguiente punto se trabajó con Postfix porque es de código abierto, lo cual permite una amplia variedad de configuraciones y gestiones, facilitando su uso según las necesidades específicas. Posteriormente, se implementaron recomendaciones de seguridad referenciadas en las directrices del esquema CIS acerca del servidor de correo instalado.

Los reportes generados por OpenSCAP fueron analizados para identificar los parámetros corregidos conforme al marco de referencia CIS. Finalmente, se verificó el fortalecimiento del sistema operativo Rocky Linux 8.9 siguiendo las recomendaciones del marco de referencia CIS. Se revisó el último informe para medir el efecto de las reglas solventadas en base a los tres componentes de la seguridad informática: disponibilidad, integridad y confidencialidad. Además, se hizo un compendio de los puntos más importantes para configurar un servidor seguro.

3 RESULTADOS

El punto de partida para aplicar *hardening* a Rocky Linux 8.9 fue la instalación y configuración del sistema operativo sin políticas de seguridad preestablecidas, junto con la instalación de un servidor de correo.

Una vez que Rocky Linux 8.9 y el servidor de correo se encontraban en funcionamiento, se llevó a cabo la instalación de OpenSCAP. Esta herramienta de escaneo, basada en el marco de regulación CIS, permitió identificar las vulnerabilidades o amenazas existentes en el sistema.

Tras la generación del informe por parte de OpenSCAP, se realizó un análisis detallado de las vulnerabilidades detectadas, priorizando aquellas que representaban un mayor

riesgo para la seguridad del sistema. Posteriormente, se implementaron las medidas necesarias para solventar dichas vulnerabilidades y fortalecer al servidor.

3.1 Identificación de vulnerabilidades en Rocky Linux sin políticas de seguridad

Instalación de Rocky Linux 8.9 tipo servidor

Para realizar la evaluación, se descargó la imagen ISO de Rocky Linux 8.9, se instaló y configuró en un hipervisor. Se eligió usar VirtualBox, un software de virtualización conocido por ser estable y fácil de usar. Este programa ayuda a trabajar con múltiples sistemas operativos a la vez en el mismo equipo físico. La Figura 3.1 expone la construcción de la máquina virtual.

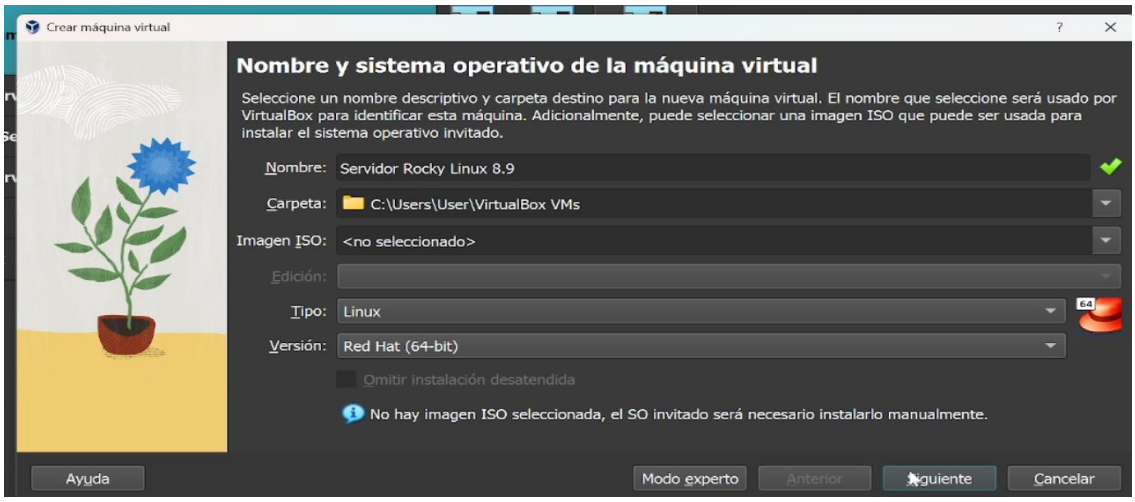


Figura 3.1 Instauración de la máquina virtual para el servidor

También se hicieron las configuraciones de hardware necesarias para preparar el entorno virtual, la Figura 3.2 expone un resumen de dichas ediciones. Se siguieron los requisitos recomendados en el sitio oficial de Rocky Linux para evitar problemas durante la instalación.

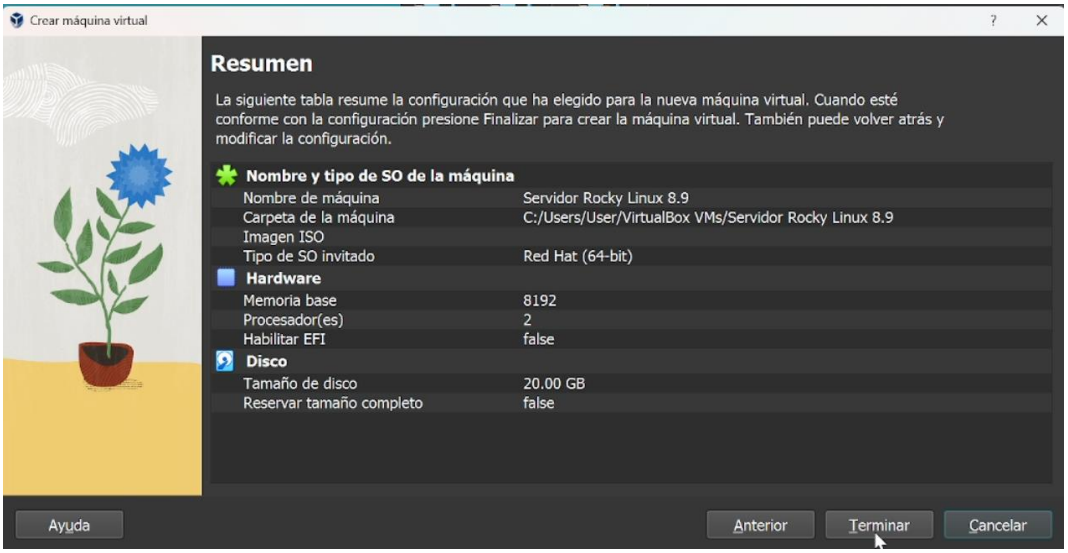


Figura 3.2 Configuración de la máquina virtual

Una vez que se cargó la imagen ISO del sistema operativo, Rocky Linux 8.9 se inició y mostró las opciones para instalar el sistema. En este caso, se eligió la primera opción, observar la Figura 3.3.

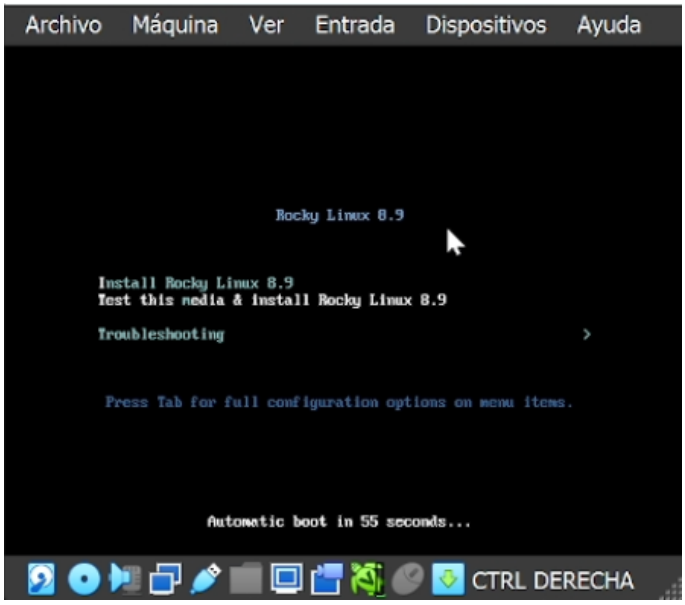


Figura 3.3 Menú de instalación

Tras finalizar el arranque, se procedió a configurar la instalación del sistema operativo Rocky Linux 8.9 sin interfaz gráfica, como está expuesto en la Figura 3.4. Se determinó la ubicación de la instalación, que corresponde a la unidad de almacenamiento local, observable en la Figura 3.5, y se estableció la clave administrativa, mostrada en la Figura 3.6.

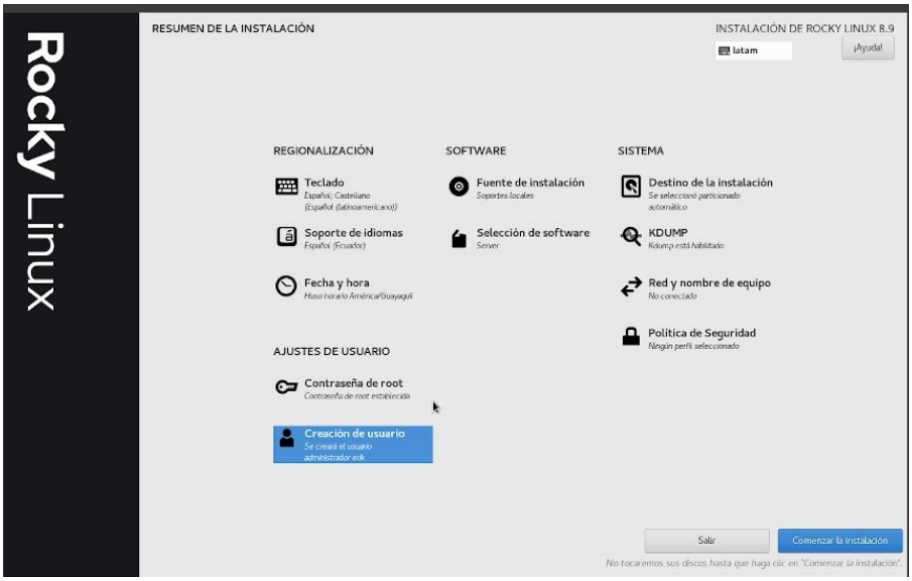


Figura 3.4 Configuración de parámetros de instalación

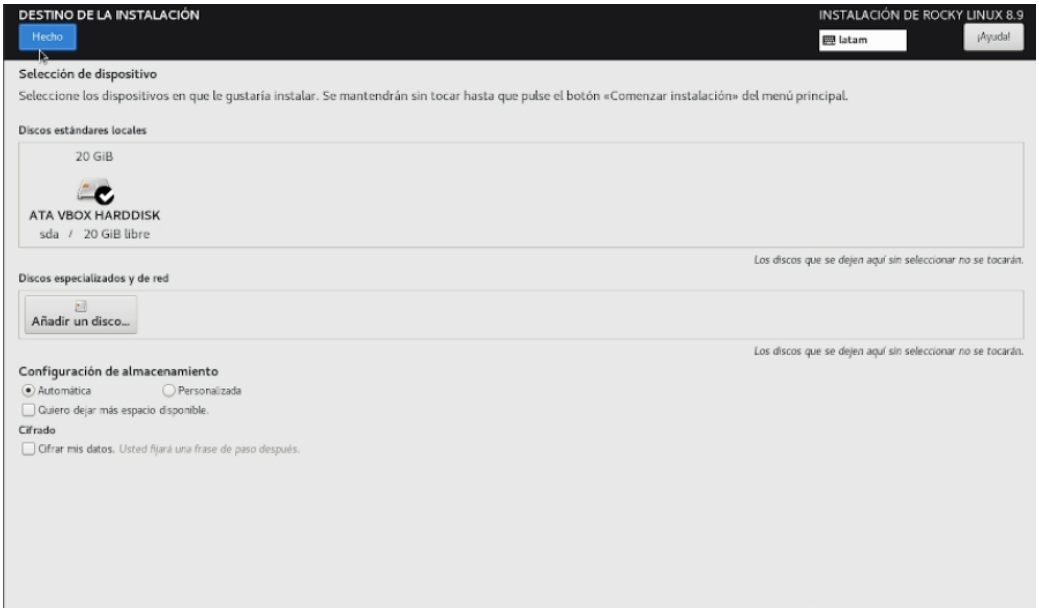


Figura 3.5 Ubicación de la unidad de almacenamiento

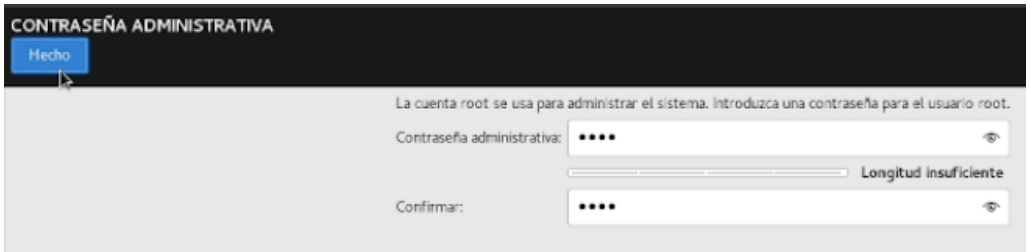


Figura 3.6 Clave administrativa

Una vez instalado el sistema operativo correspondiente se reinició y comenzó a funcionar correctamente, observar la Figura 3.7.

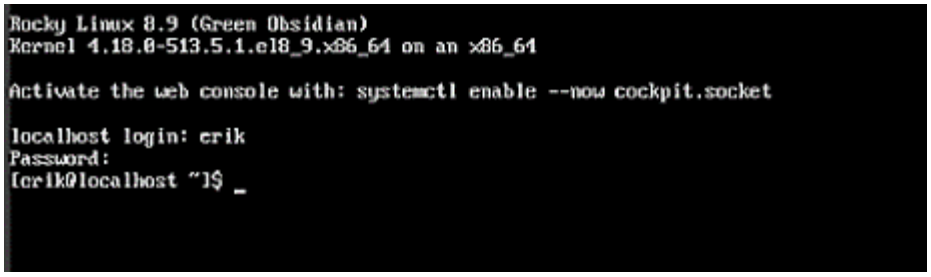


Figura 3.7 Funcionamiento de Rocky Linux 8.9

Implementación del servidor de correo

Es necesario configurar ciertas características de red antes de proceder con la configuración del servidor de correo. En este caso de trabajo con una red *NAT* llamada RED INTERNA, se ilustra los ajustes del adaptador uno en la Figura 3.8.

Figura 3.8 Adaptador de red 1

La Figura 3.9 enseña la aplicación del comando “ip address” para ver la red en la que trabaja el servidor y el direccionamiento que se la ha otorgado.

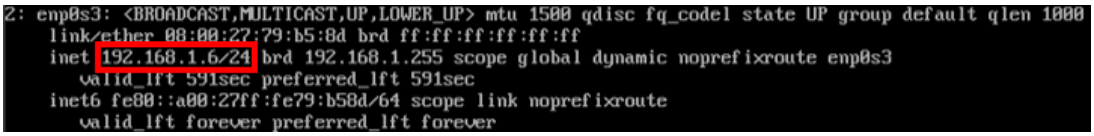


Figura 3.9 Dirección IP del servidor

A continuación, se realizaron todas las descargas necesarias para obtener los paquetes esenciales en la configuración del servicio de correo electrónico, la Figura 3.10 muestra la descarga de paquetes para Postfix y Dovecot,

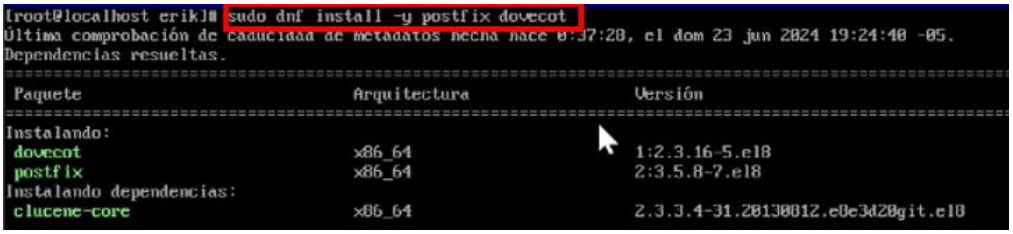


Figura 3.10 Paquetes de Postfix y Dovecot en descarga

Se realiza la descarga de Postfix porque cumple con las funciones de receptar, emitir y reenviar correos electrónicos, actuando como mediador en la entrega de correos desde el emisor hasta el receptor. Por otro lado, Dovecot facilita e ingreso al correo electrónico a través de los métodos IMAP y POP3, permitiendo a los clientes entrar a sus mensajes como a sus buzones guardados en el servidor con ayuda de los protocolos mencionados.

La Figura 3.11 se exhibe la descarga de los recursos para Telnet, esta herramienta posibilita a los usuarios conectarse de forma remota a otros sistemas mediante una red, ya sea por medio de una red externa o una red LAN.

Figura 3.11 Paquetes en descarga de Telnet

Una vez obtenidas todas las instancias que el servidor de correo necesita, se procedió a configurar los archivos respectivos. Primero, se configuró Postfix, para esto se accedió a colocar el comando “sudo nano etc/postfix/main.cf” para luego editar el fichero main.cf. Se habilitó la sección expuesta en la Figura 3.12 y se añadió la identificación del dominio del servidor de correo.

Figura 3.12 Configuración del nombre del dominio

Tal como muestra la Figura 3.13 se habilitó la línea “mydomain” que sirve para establecer el dominio del servidor de correo, este se usa para la comunicación entre los usuarios de correo, que en este caso fue rocky.com.

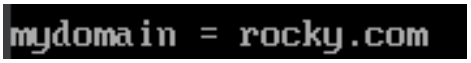


Figura 3.13 Configuración del dominio

También se habilitó el comentario de la línea “myorigin”, que define el dominio utilizado como origen en el direccionamiento del correo electrónico, esta acción se ilustra en la Figura 3.14.

Figura 3.14 Configuración del dominio de origen

Después, se colocaron las redes autorizadas para enviar correo a través del servidor, en este caso fue añadida la red 192.1681.0/24 y 127.0.0.0/8. La línea editada está expuesta en la Figura 3.15.

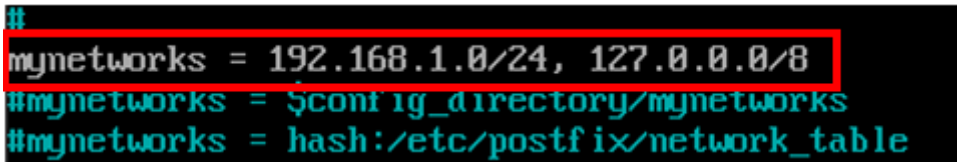


Figura 3.15 Redes permitidas

El paso final para la configuración de Postfix es habilitar la línea “home_mailbox = *Maildir/*” mostrada en la Figura 3.16. Esta carpeta trabaja como archivo de almacenamiento de los mensajes de correo.

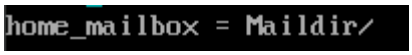


Figura 3.16 Habilitación de la carpeta *Maildir*

La Figura 3.17 muestra la orden “systemctl start postfix” que da la indicación de iniciar el servidor Postfix y la Figura 3.18 exhibe la orden “systemctl enable postfix” para habilitarlo automáticamente al iniciar el sistema.

Figura 3.17 Inicio del servidor Postfix

Figura 3.18 Habilitación automática del servidor Postfix

De igual forma la Figura 3.19 enseña la orden “systemctl start dovecot” para iniciar Dovecot y en la Figura 3.20 se tiene el comando “systemctl enable dovecot” para habilitarlo automáticamente al iniciar el sistema.

Figura 3.19 Inicio del servidor Dovecot

Figura 3.20 Habilitación automática del servidor Dovecot

Después de configurar el servidor de correo, se crearon dos usuarios, Fernando y Juan, utilizando el comando “useradd”. Posteriormente, se asignaron contraseñas a cada usuario mediante el comando “passwd”, se puede verificar en la Figura 3.21 para Fernando y en la Figura 3.22 para Juan. Los clientes mencionados fueron necesarios en la comprobación de creación y recepción de correos.

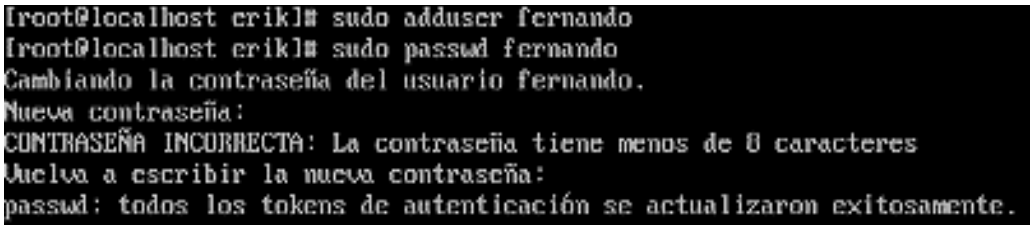


Figura 3.21 Creación del usuario Fernando para correo

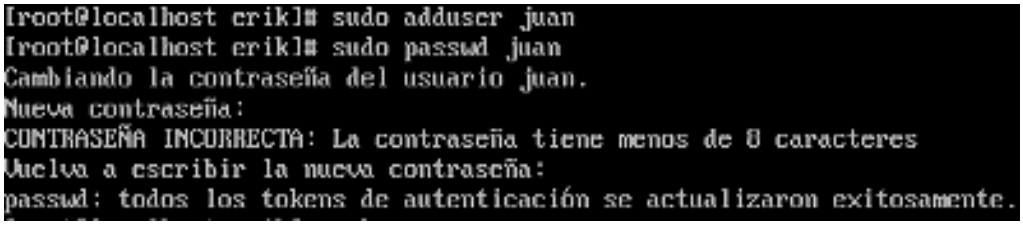


Figura 3.22 Creación del usuario Juan para correo

Se utilizó el comando “nmtui” para configurar el nombre del anfitrión del sistema, permitiendo así identificar de manera única al servidor en la red, como se expone en la Figura 3.23.

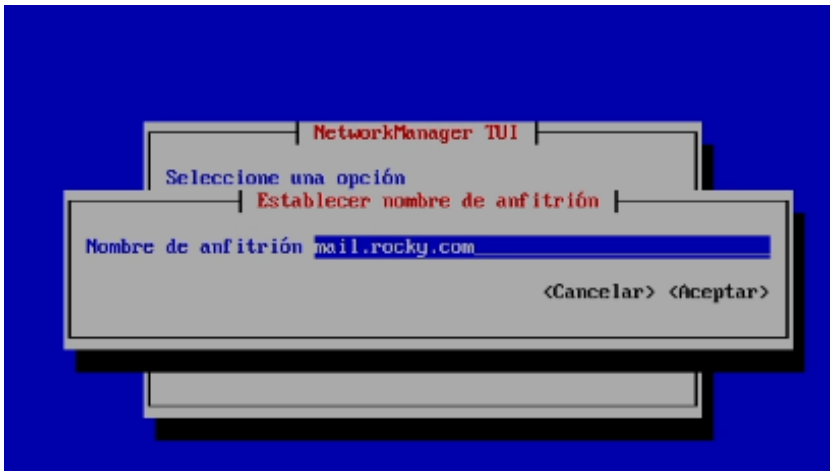


Figura 3.23 Nombre anfitrión del servidor

Con el fin de confirmar el funcionamiento adecuado del servicio correo electrónico, se realizó una evaluación enviando y recibiendo correos electrónicos entre los usuarios previamente creados. Se envió un mensaje de un usuario a otro para asegurar que el servidor operara correctamente y sin errores. Para llevar a cabo esta prueba, se aplicó la orden observable en la Figura 3.24.

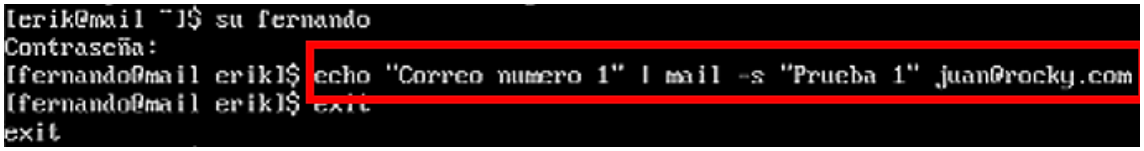


Figura 3.24 Correo enviado desde Fernando a Juan

Después de enviar el correo, se verificó que el mensaje llegue al usuario Juan. Como se ilustra en la Figura 3.25, al acceder a la ruta del usuario Juan, se puede ver la carpeta Maildir y, dentro de ella, el archivo "new", donde se almacenan los correos del usuario.

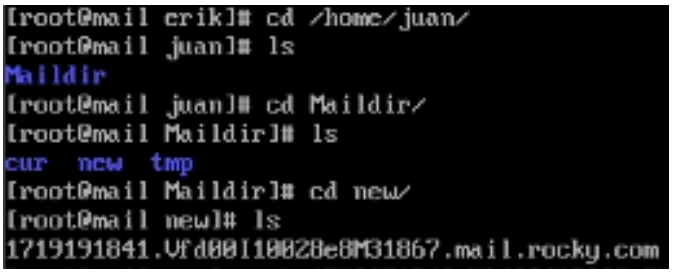


Figura 3.25 Correo recibido en el usuario Juan

A continuación, se verificó el envío y la recepción del mensaje utilizando la herramienta Telnet. La Figura 3.26 muestra remitente, destinatario, el tema del mensaje y el cuerpo del mensaje.

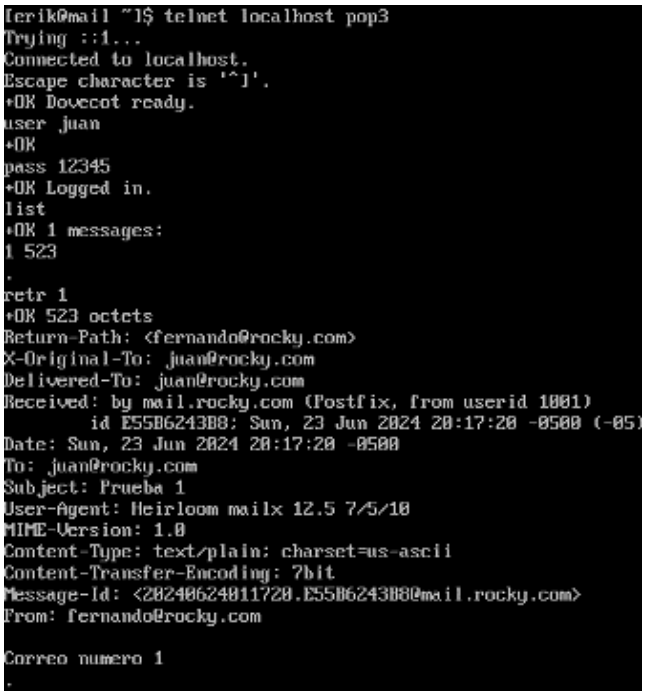


Figura 3.26 Verificación del correo enviado de Fernando a Juan

Es importante destacar que, en la Figura 3.26, se está utilizando la herramienta Telnet con el fin de evaluar el correcto desempeño del servicio de correo electrónico. Sin embargo, según las recomendaciones del estándar CIS, no se aconseja usar esta herramienta debido a que transmite datos entre máquinas sin cifrado, lo que la convierte en un protocolo muy inseguro con importantes vulnerabilidades de seguridad.

Instalación de la herramienta de escaneo OpenSCAP

Después de evaluar el cumplimento adecuado del servidor de correo, se continuó con a instalación la herramienta de escaneo OpenSCAP, utilizando la orden que aparece en la Figura 3.27.

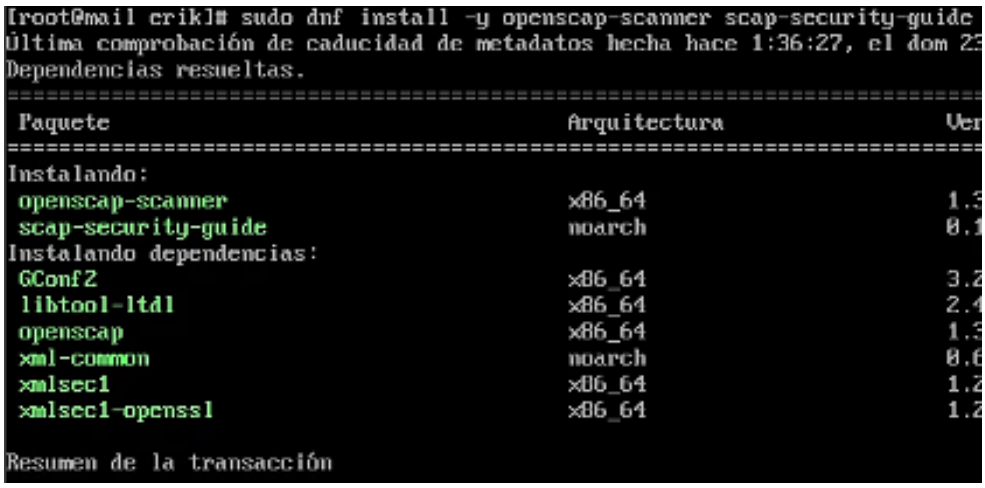


Figura 3.27 Instalación de OpenSCAP

Una vez instalada la herramienta, se pudo obtener una lista de los perfiles de seguridad disponibles utilizando el comando “oscap info /usr/share/xml/scap/ssg/content/ssg-rl8-ds.xml”, la Figura 3.28 enseña los resultados que expone la orden.

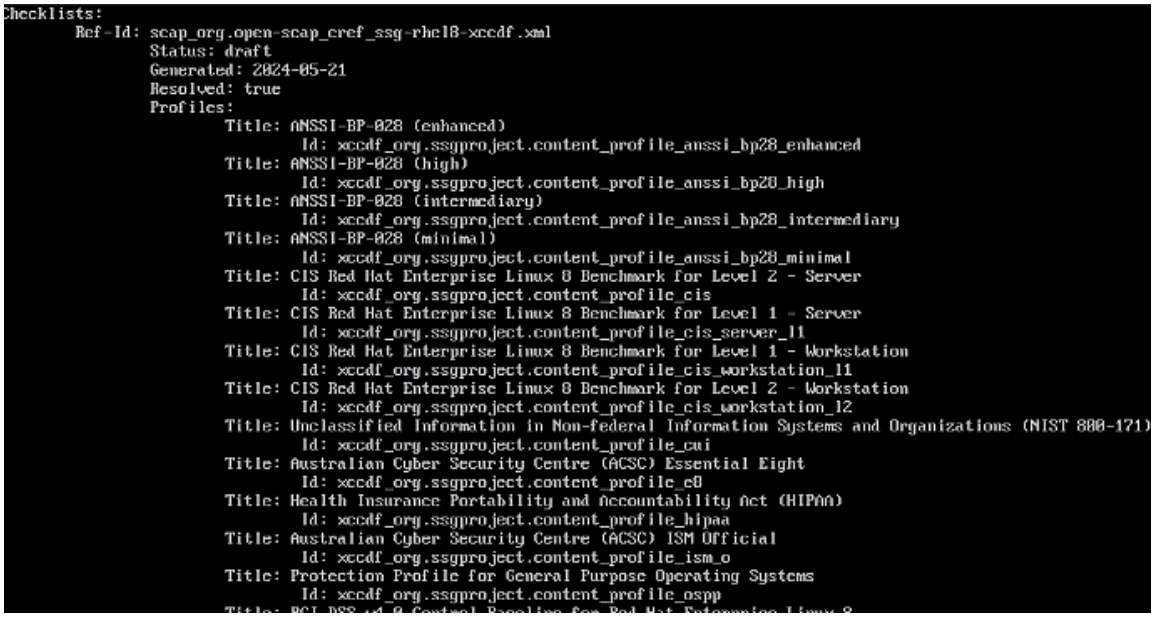


Figura 3.28 Lista de carpetas existentes a escanear

A continuación, se realizó el escaneo utilizando el comando “*sudo oscap xccdf eval --report reporte1-inicial.html --profile stig /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml*”, como se muestra en la Figura 3.29. Al finalizar la evaluación, los resultados se guardaron en un archivo HTML denominado “reporte1-inicial.html”.

Figura 3.29 Escaneo del sistema operativo Rocky Linux

En la ruta “/home/erik” se guardó el informe producido por OpenSCAP. La Figura 3.30 exhibe el archivo creado.

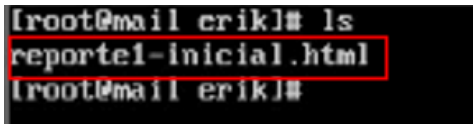


Figura 3.30 Reporte guardado con nombre “reporte1-inicial.html”

Para revisar el archivo reporte1-inicial.html, se empleó una interfaz gráfica para visualizar con mayor detalle los posibles fallos en las reglas de seguridad. Se utilizó una máquina cliente Rocky Linux 8.9 con GUI, que ya había sido configurada previamente. La dirección IP de la máquina cliente (192.168.1.7/24) está en la misma red que el servidor, permitiendo así la comunicación entre ambos. Se puede verificar en la Figura 3.31 que existe una conexión establecida de tipo cliente-servidor.

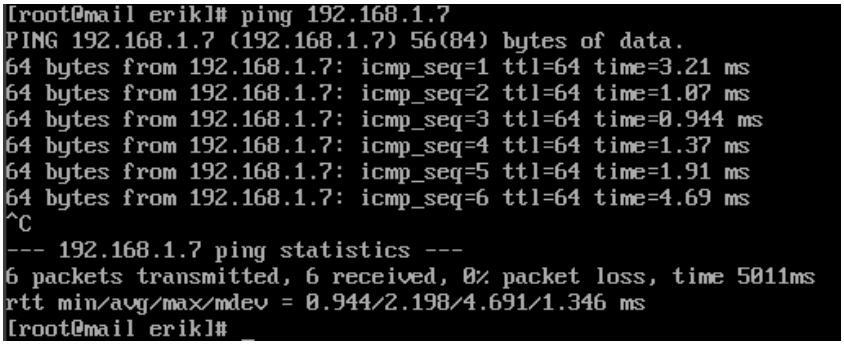


Figura 3.31 Verificación de conectividad cliente-servidor

De esta manera, utilizando la orden “scp” expuesta en la Figura 3.32, se logró transferir el archivo “reporte1-inicial.html” que contiene el informe del primer escaneo del servidor Rocky Linux 8.9 realizado con la herramienta OpenSCAP, desde el servidor hacia la máquina cliente Rocky Linux con interfaz gráfica. Se especificaron la ruta del informe en la máquina servidor y la ruta deseada para guardar el informe en la máquina cliente.

Figura 3.32 Transferencia /home del archivo html

Con la ruta del informe se pudo ingresar al navegador web Mozilla Firefox para visualizar de mejor manera el reporte, la Figura 3.33 enseña el resultado.

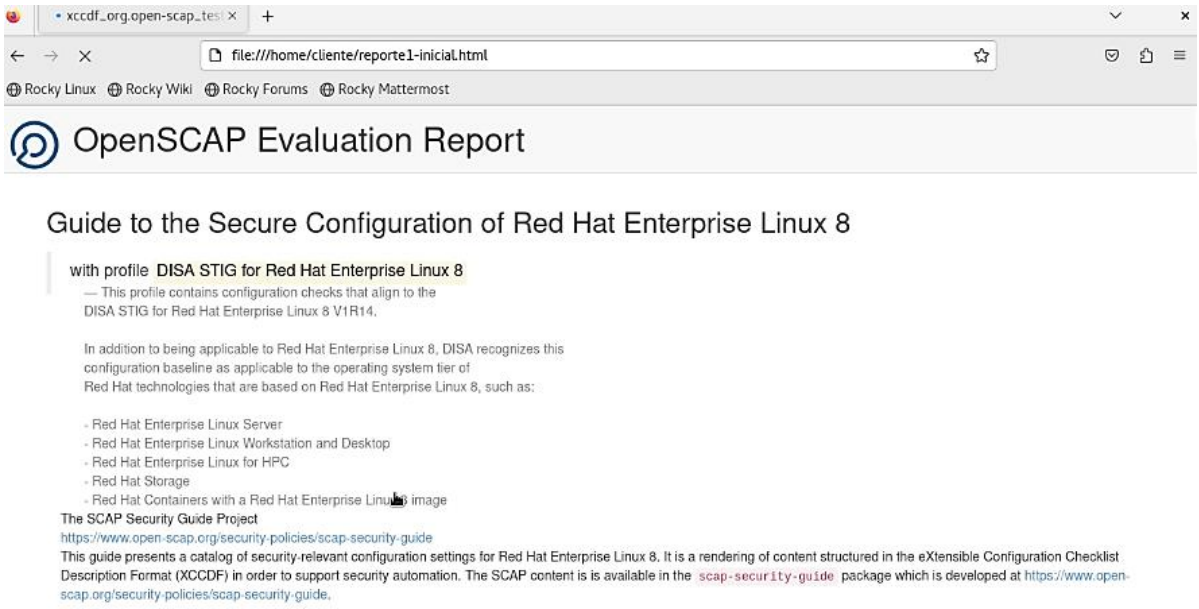
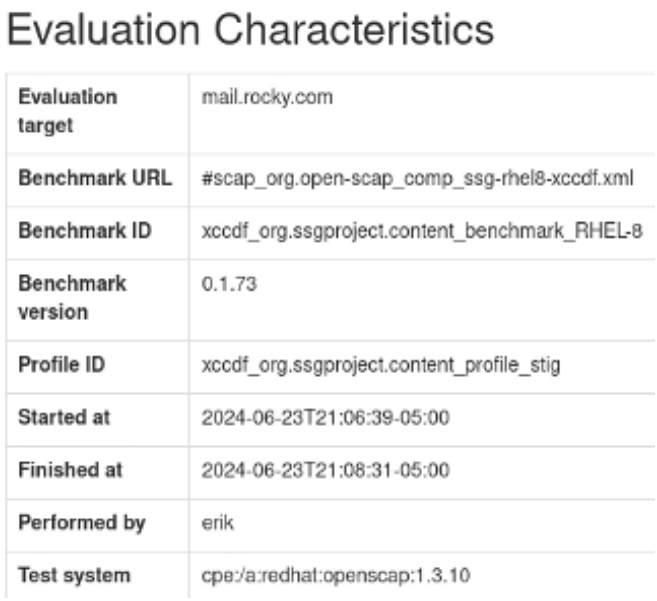


Figura 3.33 Informe de OpenSCAP en navegador web

Además, la Figura 3.34 expone los datos del sistema operativo de servidor Rocky Linux 8.9, escaneado.

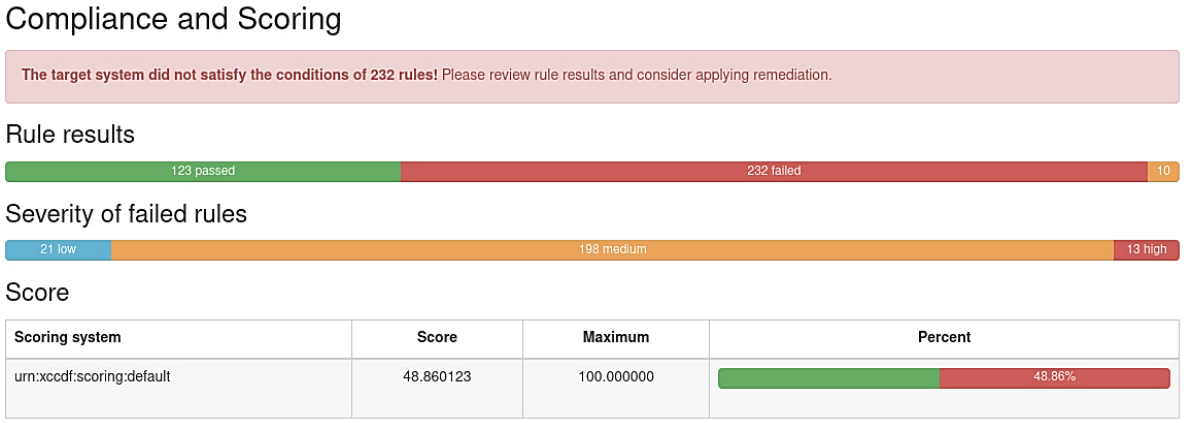


Evaluation Characteristics

Evaluation target	mail.rocky.com
Benchmark URL	#scap_org.open-scap_comp_ssg-rhel8-xccdf.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEL-8
Benchmark version	0.1.73
Profile ID	xccdf_org.ssgproject.content_profile_stig
Started at	2024-06-23T21:06:39-05:00
Finished at	2024-06-23T21:08:31-05:00
Performed by	erik
Test system	cpe:/a:redhat:openscap:1.3.10

Figura 3.34 Características de evaluación

En la Figura 3.35 se muestran y analizan los errores detectados por OpenSCAP en el entorno de Rocky Linux con el servidor de correo. El porcentaje de adherencia a las normativas de seguridad, de acuerdo al marco de seguridad CIS, es del 48,85%. El informe identificó un total de 123 reglas que cumplen con dicho marco, las cuales aparecen con estado *"passed"*. En contraste, 232 reglas están en estado fallido, indicando que no cumplen con las políticas de seguridad. Estas reglas fallidas se clasifican según su nivel de riesgo: alto, medio y bajo; con 13 errores de nivel alto, 198 de nivel medio y 21 de nivel bajo.



Compliance and Scoring

The target system did not satisfy the conditions of 232 rules! Please review rule results and consider applying remediation.

Rule results

123 passed | 232 failed | 10

Severity of failed rules

21 low | 198 medium | 13 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	48.860123	100.000000	48.86%

Figura 3.35 Resultado del primer reporte según OpenSCAP

Las reglas fallidas con nivel alto se priorizaron para su resolución debido a que representan un riesgo de vulnerabilidad muy significativo en el sistema operativo del servidor Rocky Linux 8.9, ver Figura 3.36.

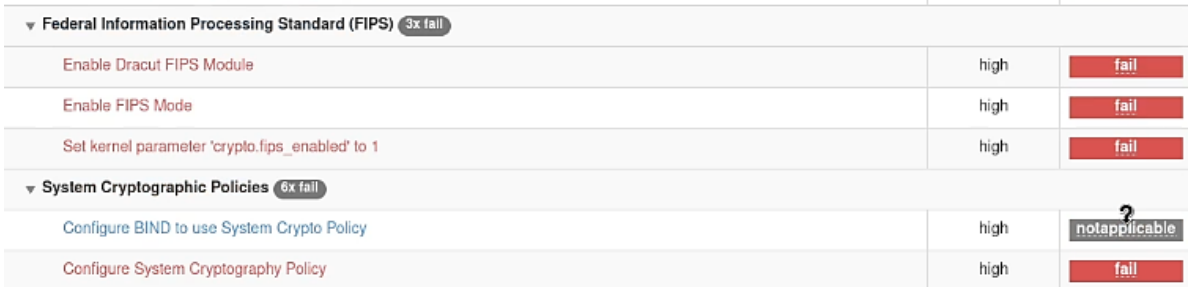


Figura 3.36 Reglas fallidas de nivel alto

En la Figura 3.37 se presenta algunos de los errores de nivel medio que también deben ser solucionados. Aunque no tienen la misma prioridad que las reglas de nivel alto, es fundamental abordarlos, ya que también representan un riesgo para el sistema operativo.

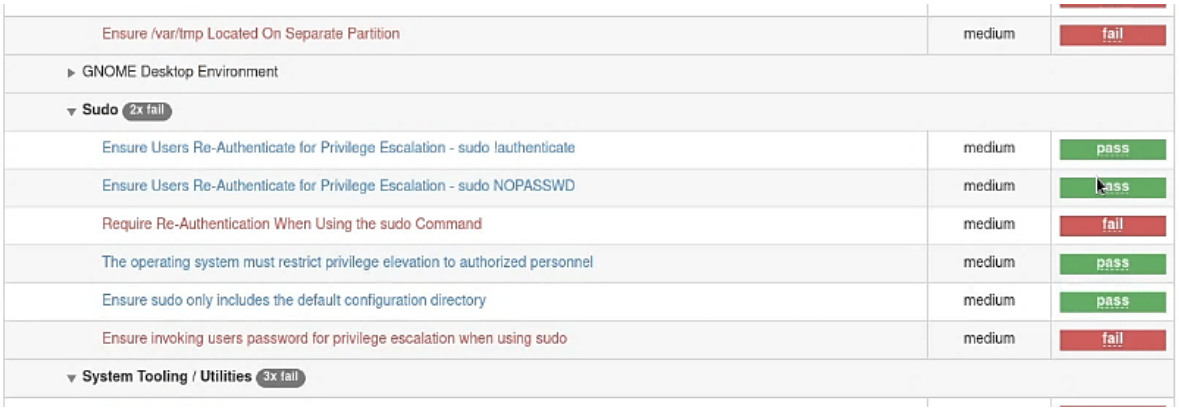


Figura 3.37 Reglas fallidas de nivel medio

De igual manera, como expone la Figura 3.38, están las vulnerabilidades de nivel bajo. Es recomendable resolver la mayor cantidad posible de estas reglas fallidas para mejorar el entorno conforme a las recomendaciones de CIS.

Figura 3.38 Reglas fallidas de nivel bajo

Para realizar un análisis posterior, el primer reporte generado se guarda tanto en el servidor de Rocky Linux, en la ruta “/home/erik”, como en la máquina cliente, en la ruta

“/home/cliente”. Esto permite comparar este archivo con el que contiene las reglas fallidas que han sido corregidas.

3.2 Implementación de políticas de seguridad en el sistema operativo

Resolución de reglas fallidas de nivel alto

Para resolver las reglas fallidas identificadas por la herramienta OpenSCAP, se utilizaron las recomendaciones del estándar CIS. Esta guía ofrece pasos específicos para gestionar y corregir las fallas de seguridad en un sistema informático, dependiendo de la naturaleza de cada falla.

Después del escaneo, se reinició el sistema escaneado para aplicar las políticas de seguridad y verificar que el servidor de correo funcione correctamente tras el escaneo. En la máquina cliente, se revisaron las reglas fallidas de nivel alto. El escaneo reveló y permitió analizar 13 reglas altas fallidas.

La primera regla de nivel alto que se corrigió fue: *Enable Dracut FIPS Module*.

El modelo FIPS (Estándares Federales de Procesamiento de la Información) se refiere a el conjunto de estándares de seguridad informática establecidos por el gobierno de Estados Unidos, que especifica requisitos para la seguridad criptográfica. La presencia de esta vulnerabilidad indica que el sistema carece de algoritmos y módulos criptográficos validados para proteger datos sensibles [19]. En este punto están contempladas 3 vulnerabilidades: *Enable Dracut FIPS Module, Enable FIPS Mode* y *Set kernel parameter “crypto.fips_enabled” to 1.*

La orden expuesta en la Figura 3.39 se utiliza para habilitar el modo FIPS. Este comando modifica la configuración del sistema para asegurar que solo se utilicen algoritmos y módulos criptográficos aprobados por FIPS.

Figura 3.39 Comando para que el sistema operativo este en modo FIPS

Después de aplicar la configuración, se reinició el sistema utilizando el comando “reboot” que se visualiza en la Figura 3.40, para garantizar que los cambios se implementaran correctamente.

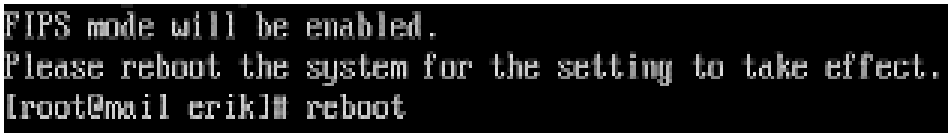


Figura 3.40 Reinicio el sistema

Como se muestra en la Figura 3.41, se realizó un nuevo escaneo luego de configurar los cambios en el servidor Rocky Linux, y el resultado se almaceno en un archivo llamado “reporte2.html”. Este archivo contiene todas las actualizaciones realizadas en el servidor Rocky Linux 8.9, incluyendo las vulnerabilidades que se han corregido.

Figura 3.41 Segundo escaneo del sistema

Luego de realizar el escaneo con la vulnerabilidad corregida, se transfirió el reporte “reporte2.html” a la máquina cliente para facilitar la comprobación de la amenaza resulta que su vez engloba 3 parámetros (*Enable Dracut FIPS Module, Enable FIPS Mode* y *Set kernel parameter “crypto.fips_enabled” to 1.*). La Figura 3.42 ilustra la primera vulnerabilidad que se ha solucionado.

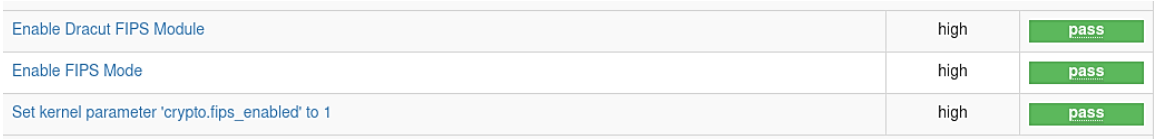


Figura 3.42 Vulnerabilidad de FIPS resuelta

La segunda vulnerabilidad de nivel alto fue: *Configure System Cryptography Policy*.

Esta vulnerabilidad en el sistema señala que la falta de una política de criptografía adecuadamente configurada deja al sistema sin directrices claras para proteger la información y los sistemas mediante técnicas criptográficas, lo que lo hace susceptible a ataques. Además, es esencial actualizar regularmente esta política para garantizar la protección del sistema frente a las vulnerabilidades más recientes [20]. Este parámetro contempla 3 vulnerabilidades: *Configure System Cryptography Policy, Configure Kerberos to use System Crypto Policy, Configure Libreswan to use System Crypto Policy.*

Para solucionar este problema de seguridad, se ejecutó el comando que aparece en la Figura 3.43. Esto actualiza las políticas criptográficas del sistema y configura el sistema para cumplir con los estándares FIPS, asegurando que solo se utilicen algoritmos y módulos criptográficos validados según estos estándares.

```
[root@mail erik]# sudo update-crypto-policies --set FIPS
```

Figura 3.43 Comando para configuración adecuada de políticas criptográficas

Se realizó un nuevo escaneo para verificar los cambios en OpenSCAP, utilizando el mismo comando mostrado en la Figura 3.41. El reporte se guardó con el nombre “reporte3.html”. Una vez copiado el nuevo reporte a la máquina cliente, se revisó el escaneo realizado por la herramienta OpenSCAP y se confirmó que la regla fallida había sido corregida con las configuraciones aplicadas al sistema operativo, ver Figura 3.44 y Figura 3.45.

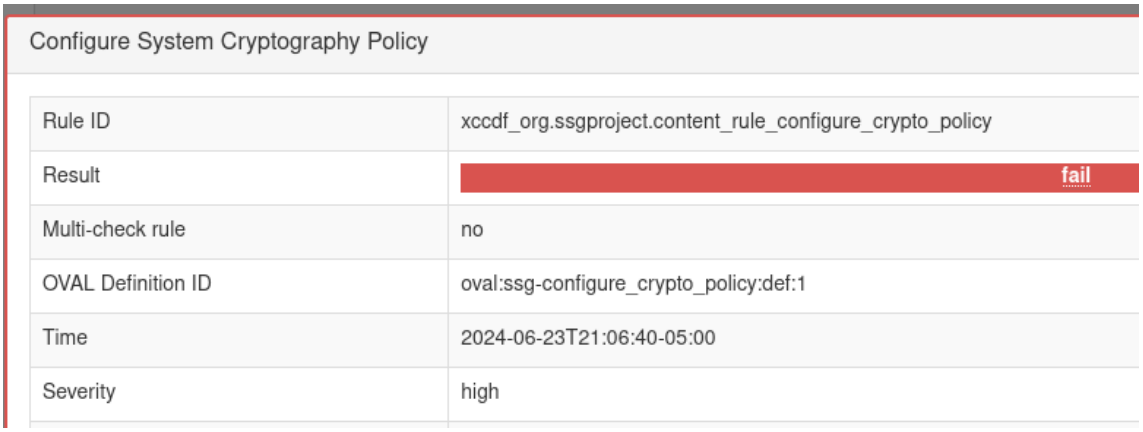


Figura 3.44 Vulnerabilidad de políticas criptográficas existente

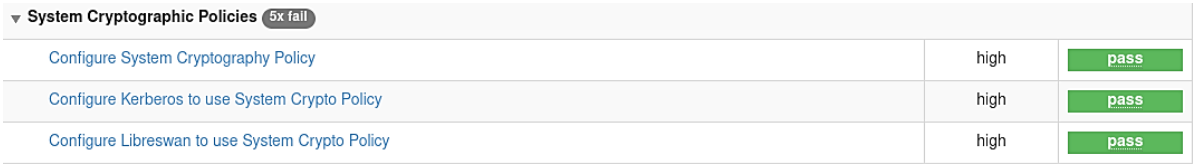


Figura 3.45 Vulnerabilidad de políticas criptográficas resuelta

Tras implementar los cambios en el sistema operativo Rocky Linux 8.9, se verificó que el servidor de correo continuara funcionando correctamente y que no hubiera errores al momento de enviar y recibir correos para los dos clientes previamente añadidos. Como se muestra en la Figura 3.46, el correo sigue funcionando sin ningún problema.

```
Return-Path: <fernando@rocky.com>
X-Original-To: juan@rocky.com
Delivered-To: juan@rocky.com
Received: by mail.rocky.com (Postfix, from userid 1001)
        id 581F8243B1; Sun, 23 Jun 2024 22:11:30 -0500 (-05)
Date: Sun, 23 Jun 2024 22:11:30 -0500
To: juan@rocky.com
Subject: Prueba 2
User-Agent: Heirloom mailx 12.5 7/5/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20240624031130.581F8243B1@mail.rocky.com>
From: fernando@rocky.com

Correo numero 2
```

Figura 3.46 Verificación de correo en funcionamiento

A continuación, se revisó la siguiente regla fallida alta que se visualiza en la Figura 3.47. Esta regla, titulada*: Ensure gpgcheck Enabled for Local Packages*, se refiere a la necesidad de comprobar la autenticidad e integridad de los paquetes locales instalados en el sistema. Permite comprobar las firmas GPG (*GNU Privacy Guard*) de los paquetes antes de su instalación o actualización. Esta verificación garantiza que los paquetes no hayan sido alterados y provengan de una fuente confiable. Al habilitar "*gpgcheck*", el sistema asegura que los paquetes no hayan sido modificados desde su firma por el proveedor, lo que ayuda a evitar la instalación de paquetes comprometidos que podrían contener malware o software dañino. La verificación de firmas GPG es esencial para confirmar que los paquetes provienen de una fuente confiable y no han sido interceptados o alterados por terceros, lo que es crucial para mantener la seguridad del sistema [21]. Esta regla se compone de 4 parámetros: *Ensure gpgcheck Enabled In Main yum Configuration, Ensure gpg Enabled for Local Packages, Ensure gpgcheck Enabled for All yum Package Repositories, Ensure Red Hat GPG Key Installed.*

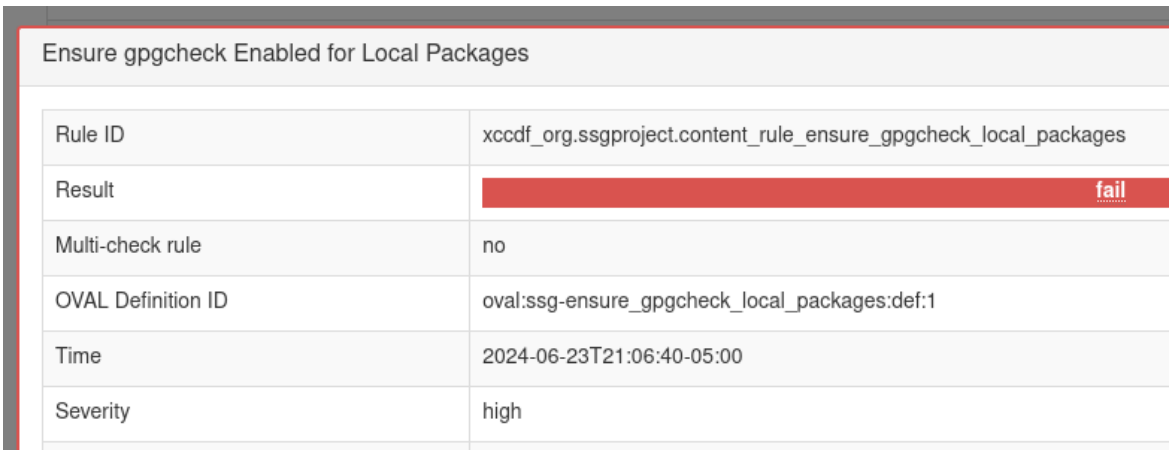


Figura 3.47 Vulnerabilidad de integridad y autenticidad de los paquetes instalados

Para corregir esta regla fallida en el sistema operativo, se accedió al archivo mostrado en la Figura 3.48 y se procedió a editarlo. Se configuró la línea “localpkg_gpgcheck=1” para habilitar “gpgcheck” en los paquetes locales, ayudando así a prevenir posibles vulnerabilidades relacionadas con la instalación de software comprometido, ver Figura 3.49.

Figura 3.48 Ingreso a la ruta para abrir el archivo yum.conf

Figura 3.49 Configuración de línea “localpkg_gpgcheck=1”

Utilizando la orden exhibida en la Figura 3.41, fue posible capturar un nuevo escaneo del sistema operativo, y el reporte se guardó con el nombre “reporte4.html”. Luego, se transfirió este reporte a la máquina cliente y, como se muestra en la Figura 3.50, se verificó que la vulnerabilidad había sido resuelta.

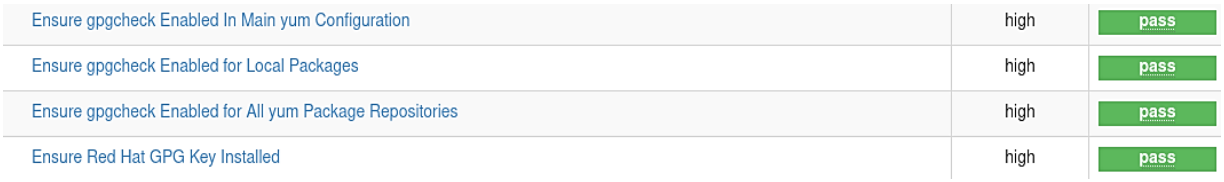
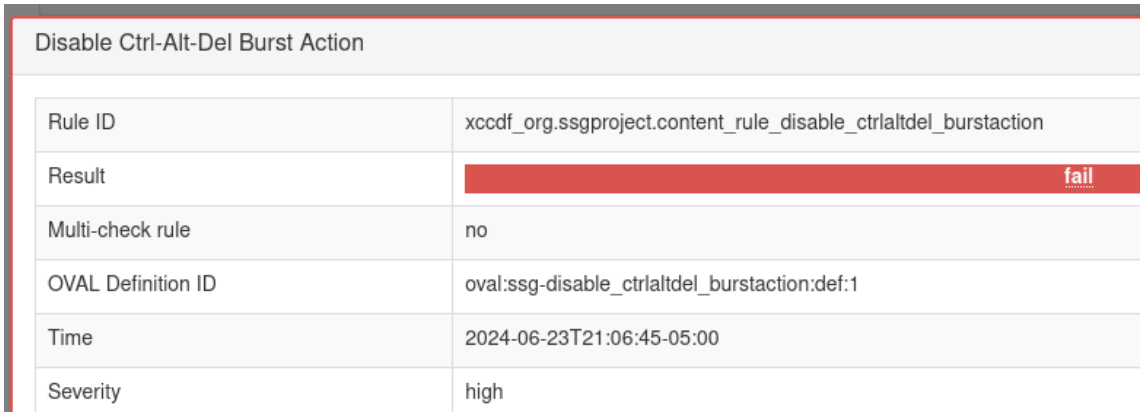


Figura 3.50 Verificación de vulnerabilidades solventadas

La cuarta regla fallida encontrada es: *Disable Ctrl-Alt-Del Burst Action,* ver Figura 3.51. Esta regla se refiere a la configuración del sistema para manejar la combinación de teclas Ctrl-Alt-Del, que tradicionalmente se utiliza para reiniciar el sistema. Si esta combinación reinicia el sistema sin una confirmación adecuada, puede causar interrupciones no deseadas, pérdida de datos y caída de servicios críticos. En entornos donde es posible el acceso físico al servidor o computadora, un atacante podría usar esta combinación de teclas para interrumpir los servicios. Por lo tanto, quitar la opción de presionar las teclas ctr-alt-del al mismo tiempo en Rocky Linux es una medida de seguridad crucial para prevenir reinicios no autorizados y mantener la estabilidad y disponibilidad del sistema [22].



Disable Ctrl-Alt-Del Burst Action

Rule ID	xccdf_org.ssgproject.content_rule_disable_ctrlaltdel_burstaction
Result	fail
Multi-check rule	no
OVAL Definition ID	oval:ssg-disable_ctrlaltdel_burstaction:def:1
Time	2024-06-23T21:06:45-05:00
Severity	high

Figura 3.51 Cuarta vulnerabilidad encontrada

Para resolver esta regla fallida en el sistema operativo, se accedió al archivo expuesto en la Figura 3.52 y se editó. Una vez adentro del sitio, se configuró el parámetro "*CtrlAltDelBurstAction=none*", lo que especifica qué acción debe tomarse cuando se detecta una pulsación repetida al mismo tiempo de las teclas ctl-alt-del en un corto período de tiempo. Al establecer la opción "*none*", se desactiva cualquier acción predeterminada que el sistema podría tomar en respuesta a estas pulsaciones, se puede confirmar la acción ejecutada en la Figura 3.53.

```
[root@mail erik]# sudo nano /etc/systemd/system.conf
```

Figura 3.52 Comando para ingresar a system.conf

```
 GNU nano 2.9.8                                          /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=none
```

Figura 3.53 Configuración de línea "CtrlAltDelBurstAction=none"

Luego, se reinició el servicio “systemd” (herramienta de control del sistema) para recargar sus configuraciones y aplicar los cambios realizados. Esto se logró con la orden planteada en la Figura 3.54.

```
[root@mail erik]# sudo systemctl daemon-reload
```

Figura 3.54 Reinicio de “*systemd*”

Posteriormente se usó la orden de la Figura 3.41, como resultado se obtuvo un nuevo escaneo del sistema operativo, y el reporte se guardó con el nombre “reporte5.html”. Luego, se transfirió este reporte a la máquina cliente y, como se muestra en la Figura 3.55, se verificó que la vulnerabilidad había sido resuelta.

Disable Ctrl-Alt-Del Burst Action

Rule ID	xccdf_org.ssgproject.content_rule_disable_ctrlaltdel_burstaction
Result	pass
Multi-check rule	no
OVAL Definition ID	oval:ssg-disable_ctrlaltdel_burstaction:def:1
Time	2024-06-24T02:11:04-05:00
Severity	high

Figura 3.55 Verificación de cuarta vulnerabilidad resuelta

Resolución de reglas fallidas de nivel medio

La primera vulnerabilidad de nivel medio resuelta fue: *Install AIDE*, como se muestra en la Figura 3.56. AIDE (Entorno Avanzado de Detección de Intrusiones) proporciona un sistema que descubre intrusiones, es utilizada para monitorear y verificar la integridad de los datos en un sistema. Esta herramienta realiza la función de construir una base de datos con información detallada sobre los archivos, incluyendo permisos, hashes, tamaños, entre otros, y luego la compara con el estado actual del sistema para detectar cualquier cambio no autorizado.

La implementación de AIDE es fundamental para detectar modificaciones no autorizadas en los archivos del sistema, lo cual es crucial para identificar actividades maliciosas y posibles intrusiones. Al asegurar que los archivos críticos del sistema no hayan sido alterados, AIDE contribuye significativamente a la seguridad y confiabilidad del sistema. Además, muchas normativas de seguridad exigen el uso de herramientas de monitoreo de integridad como la expuesta [23].

Install AIDE

Rule ID	xccdf_org.ssgproject.content_rule_package_aide_installed
Result	fail
Multi-check rule	no
OVAL Definition ID	oval:ssg-package_aide_installed:def:1
Time	2024-06-23T21:06:39-05:00
Severity	medium

Figura 3.56 Primera vulnerabilidad de nivel medio

Para corregir esta vulnerabilidad, se utilizó la orden visualizada en la Figura 3.57 para montar el paquete de AIDE, la herramienta avanzada de detección de intrusiones.

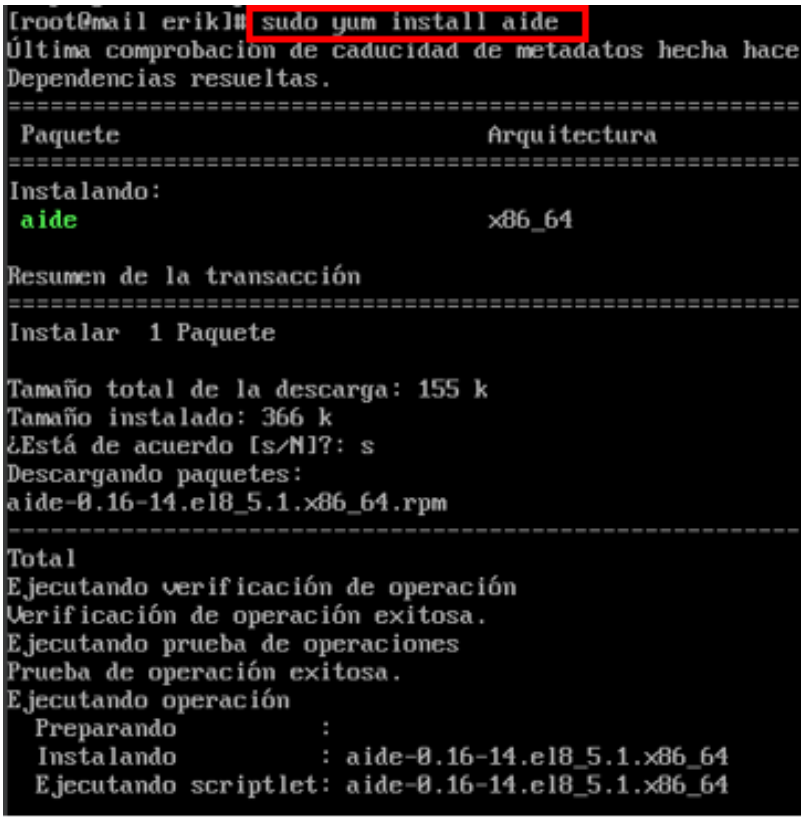


Figura 3.57 Instalación de *AIDE*

Después de configurar, se llevó a cabo un nuevo escaneo haciendo uso del comando de la Figura 3.41, guardándolo bajo el nombre "reporte6.html". Al revisar el reporte generado, se puede observar la Figura 3.58 para comprobar que la regla fallida ha sido solucionada.

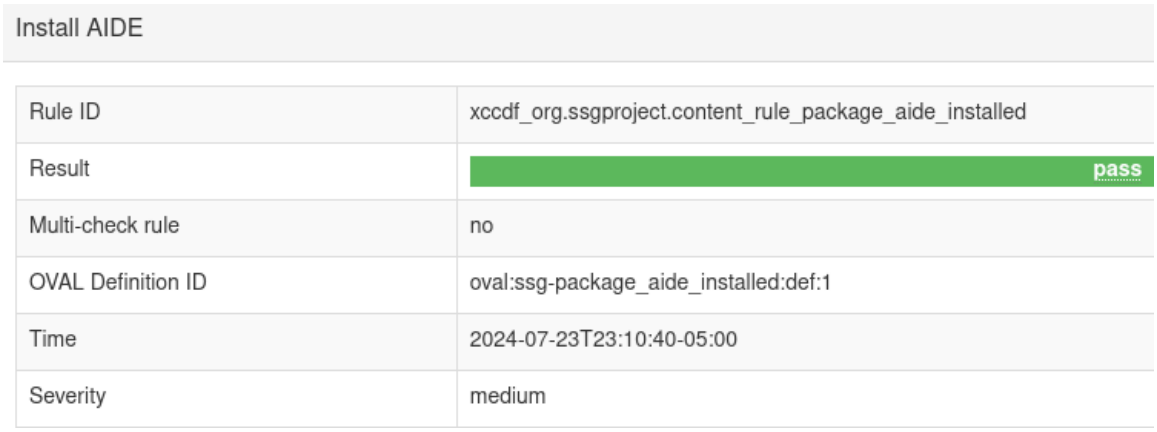


Figura 3.58 Vulnerabilidad AIDE de nivel medio resuelta

La siguiente vulnerabilidad de nivel medio está relacionada con la regla anterior que se resolvió. Esta regla se denomina: *Build and Test AIDE Database*, y se refiere a la necesidad de crear y verificar regularmente la base de datos de AIDE para garantizar la integridad del sistema [24]. La Figura 3.59 expone que la regla falló.

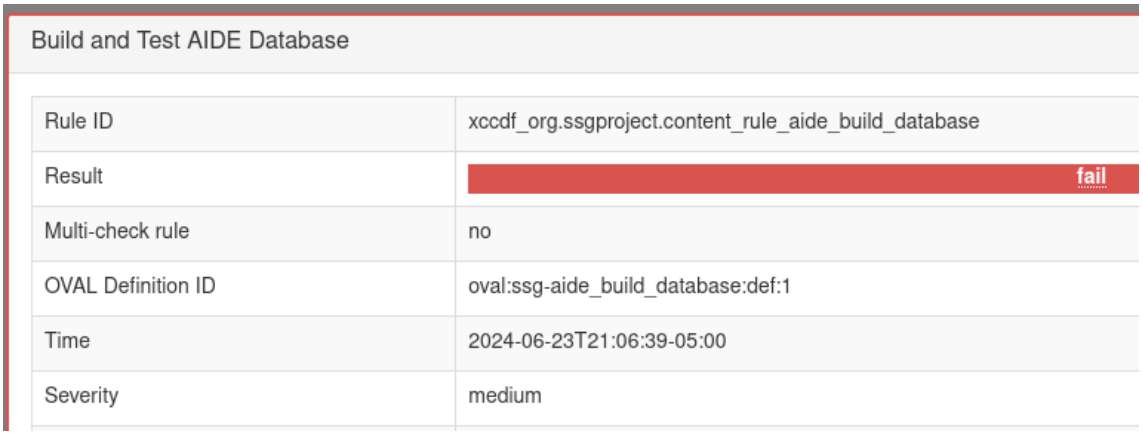


Figura 3.59 Segunda vulnerabilidad encontrada

En la Figura 3.60, se ejecutó la respectiva orden para generar una nueva base de datos inicial. Esto permite que, cuando la herramienta escanee el sistema, pueda compararlo y verificar su integridad.

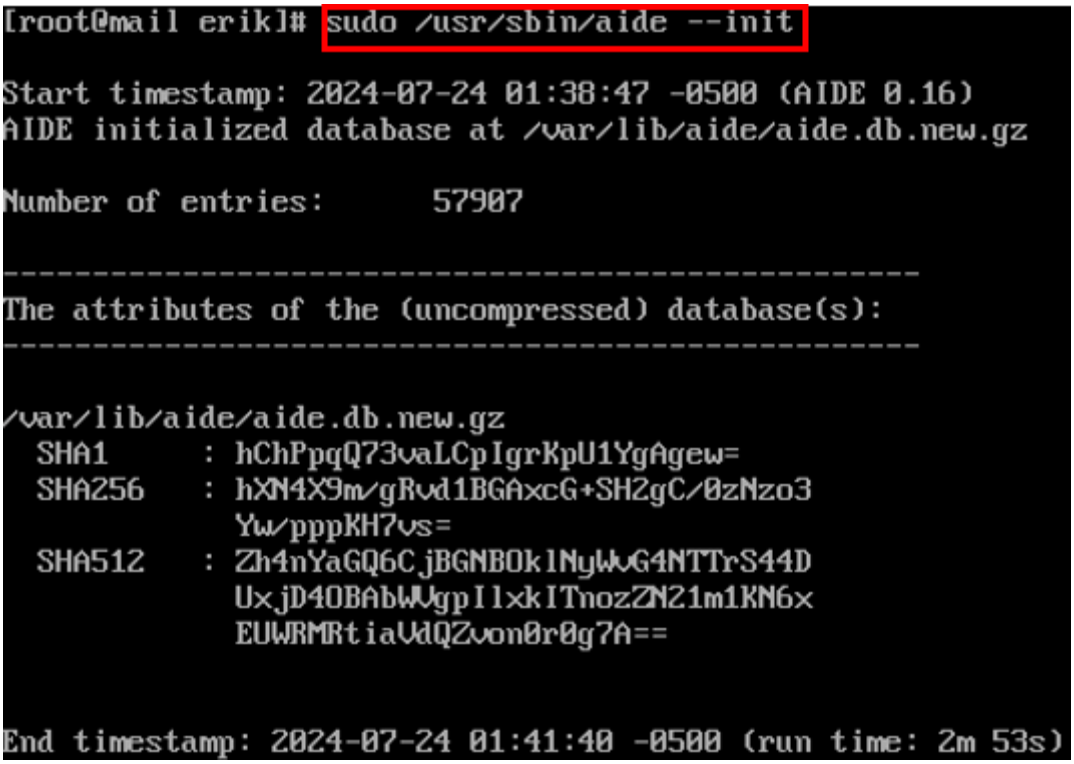


Figura 3.60 Nueva base de datos inicial

Para proseguir, se aplicó la orden de la Figura 3.61. La base de datos generada en el paso previo se almaceno correctamente. Esta línea de comando copia el archivo "aide.db.new.gz" a "aide.db.gz" en el directorio "/var/lib/aide/". Este paso es crucial para renombrar y ubicar la nueva base de datos generada (aide.db.new.gz) en el lugar correcto donde AIDE espera encontrar su base de datos (aide.db.gz).

```
[root@mail erik]# sudo cp /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Figura 3.61 Comando para guardar la base de datos creada

La orden perteneciente a la Figura 3.62 inicia una verificación manual utilizando AIDE para comparar las bases de datos, es decir la actual con el sistema de información. La verificación realizada por AIDE no detectó cambios no autorizados en el sistema de archivos, lo que confirma que la integridad del sistema se mantiene intacta.

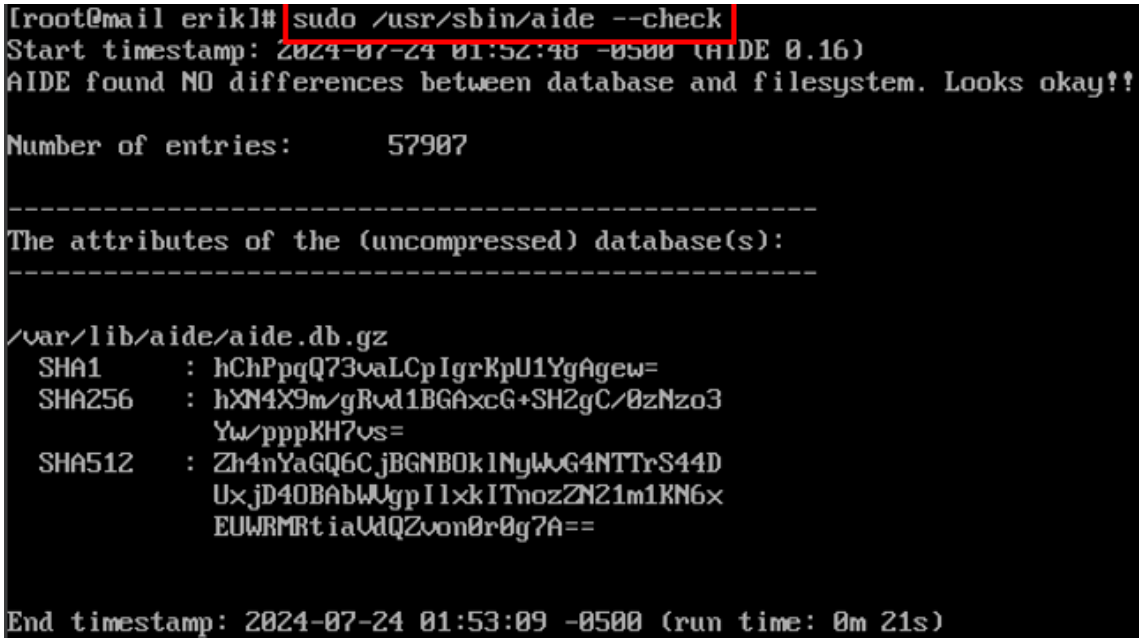


Figura 3.62 Comando para guardar la base de datos creada

Tal como exhibe la Figura 3.63, después del escaneo realizado con OpenSCAP, se resolvió la regla que había fallado.

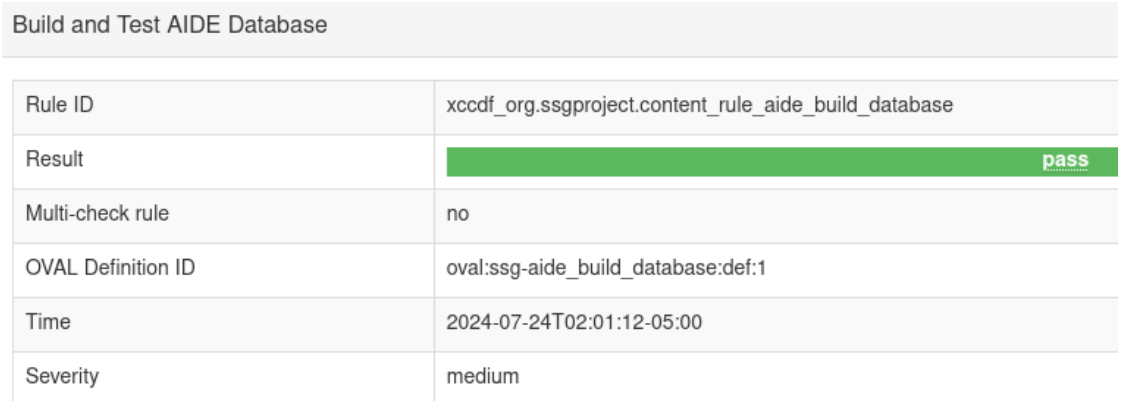


Figura 3.63 Segunda vulnerabilidad de nivel medio solucionada

La tercera vulnerabilidad de nivel medio se denomina: *Uninstall iprutils Package*. Esta vulnerabilidad se debe a la presencia innecesaria del paquete "iprutils" en el sistema, el cual contiene herramientas para la administración de controladores y dispositivos SCSI [25]. Tener paquetes innecesarios instalados en el sistema incrementa la superficie de ataque, es decir, el número de posibles puntos de entrada para un atacante. Un sistema más limpio y con menos paquetes innecesarios es más fácil de mantener y auditar, mejorando así el resguardo general de un sistema. Así pues, la Figura 3.64 enseña la regla que falló.

Uninstall iprutils Package

Rule ID	xccdf_org.ssgproject.content_rule_package_iprutils_removed
Result	fail
Multi-check rule	no
OVAL Definition ID	oval:ssg-package_iprutils_removed:def:1
Time	2024-06-23T21:06:40-05:00
Severity	medium

Figura 3.64 Tercera vulnerabilidad de nivel medio

Para solucionar esta regla fallida, se ingresó el comando mostrado en la Figura 3.65 que cumple la función de desinstalar el paquete "iprutils" del sistema Rocky Linux 8.9. Se muestra que la operación se completó con éxito.

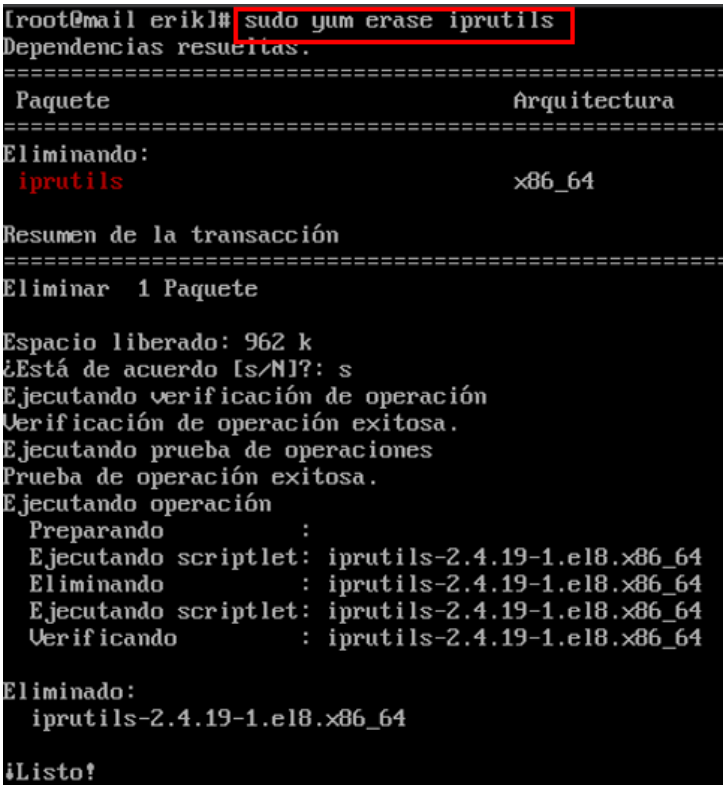


Figura 3.65 Desinstalación del paquete “iprutils”

Después de la configuración, se ejecutó un nuevo escaneo utilizando la respectiva orden de la Figura 3.41. Con el escaneo realizado, se verificó nuevamente el reporte, ahora llamado "reporte8.html". En la Figura 3.66 se puede observar que la vulnerabilidad fue resuelta sin problemas.

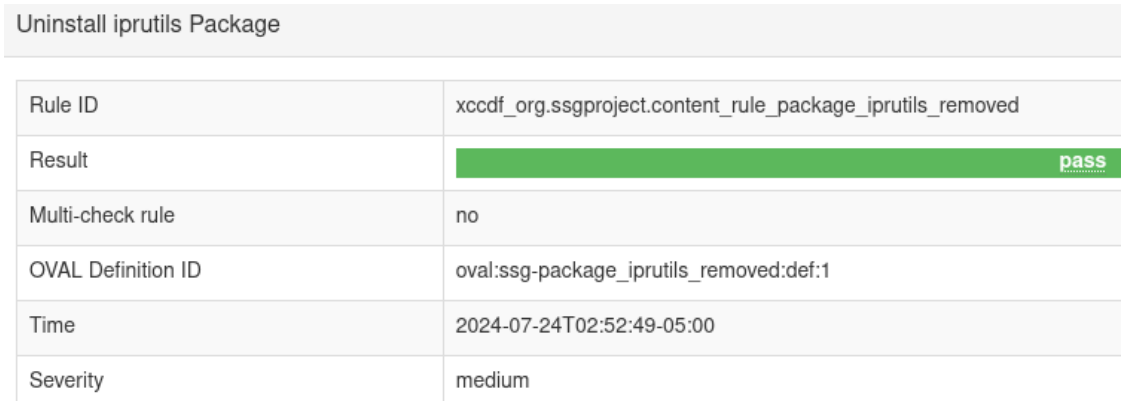


Figura 3.66 Tercera regla fallida resuelta

La siguiente vulnerabilidad de nivel medio que se encontró es: *Set Password Maximum Age*. Esta vulnerabilidad señala que, independientemente de la complejidad de una contraseña, es posible que eventualmente sea descifrada. Por esta razón, es crucial cambiar las contraseñas con regularidad. Si el sistema operativo no impone un límite en la duración de las contraseñas y no obliga a los usuarios a actualizarlas, existe el riesgo de que las contraseñas se vean comprometidas. Implementar una duración máxima para las contraseñas asegura que los usuarios tengan que modificarlas periódicamente. Aunque exigir contraseñas con una vida útil más corta puede reducir el riesgo de compromisos digitales, también puede llevar a que los usuarios escriban las contraseñas en lugares convenientes, lo que aumenta el riesgo de exposición física [26]. Ver Figura 3.67.

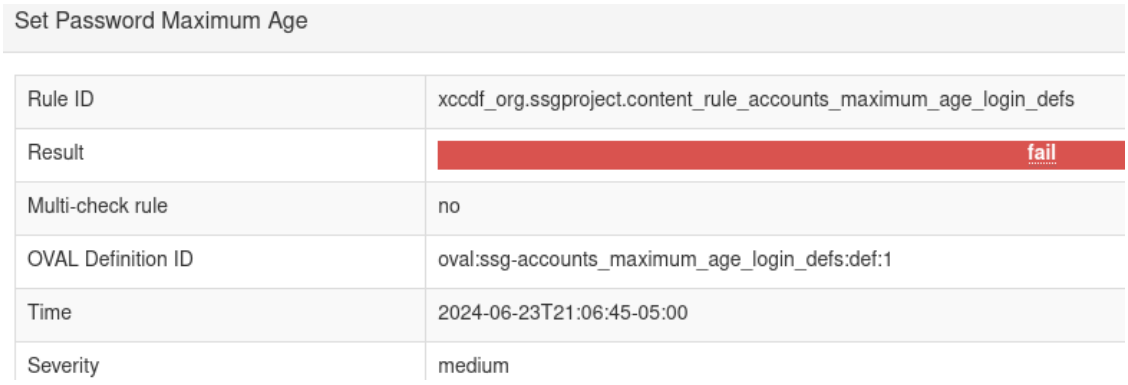


Figura 3.67 Cuarta regla de nivel medio fallida

Para solventar esta regla vulnerable, se accedió al archivo donde se configura la duración de las contraseñas utilizando el comando mostrado en la Figura 3.68.

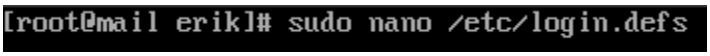


Figura 3.68 Ingreso al archivo login.defs

Una vez dentro del archivo, se localizó la línea PASS_MAX_DAYS y se estableció el valor recomendado por el protocolo, que es 60 días, ver Figura 3.69.

Figura 3.69 Cambio de duración de contraseñas máxima

Después de la configuración, se ejecutó el respectivo escaneo utilizando el comando de la Figura 3.41. Tras el escaneo, se revisó los resultados del reporte con el nombre "reporte9.html" y se verificó que la vulnerabilidad había sido solucionada en el servidor, ver Figura 3.70.

Set Password Maximum Age

Rule ID	xccdf_org.ssgproject.content_rule_accounts_maximum_age_login_defs
Result	pass
Multi-check rule	no
OVAL Definition ID	oval:ssg-accounts_maximum_age_login_defs:def:1
Time	2024-07-24T03:32:01-05:00
Severity	medium

Figura 3.70 Cuarta vulnerabilidad de nivel medio solventada

La quinta vulnerabilidad de nivel medio del sistema operativo fue: *Set Password Minimum Age*. Esta vulnerabilidad contrasta a la regla anterior que se solvento, pues busca imponer una duración mínima para las contraseñas con el fin de prevenir cambios excesivos y rápidos que podrían violar las políticas de reutilización de contraseñas. Si los usuarios pueden cambiar sus contraseñas de inmediato y de forma continua, podrían hacerlo repetidamente en un corto período para eludir las políticas de la organización sobre la reutilización de contraseñas. Es aconsejable establecer un período mínimo para que la contraseña permanezca sin cambios, evitando que los usuarios vuelvan a una contraseña previamente usada después de cumplir con los requisitos de reutilización [27]. Como muestra la Figura 3.71, la ausencia de configuración de esta política genera riesgos en la seguridad.

Set Password Minimum Age

Rule ID	xccdf_org.ssgproject.content_rule_accounts_minimum_age_login_defs
Result	fail
Multi-check rule	no
OVAL Definition ID	oval:ssg-accounts_minimum_age_login_defs:def:1
Time	2024-06-23T21:06:45-05:00
Severity	medium

Figura 3.71 Quinta regla de nivel medio fallida

Para corregir esta regla en el servidor, se accedió al archivo que gestiona la duración de las contraseñas utilizando el comando indicado en la Figura 3.68. En el archivo, se identificó la línea PASS_MIN_DAYS y se ajustó al valor mínimo recomendado por CIS, visualizar Figura 3.72.

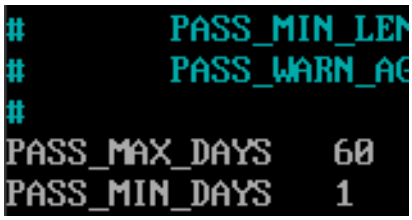


Figura 3.72 Cambio en la duración mínima de contraseñas

Al ejecutar esta modificación, se volvió a realizar el escaneo, generando el reporte “reporte10.html” con ayuda del comando de la Figura 3.41. Para la máquina cliente, se compartió el ultimo escaneo y, como se muestra en la Figura 3.73, se puede ver que la regla fallida ha sido solucionada.

Set Password Minimum Age

Rule ID	xccdf_org.ssgproject.content_rule_accounts_minimum_age_login_defs
Result	pass
Multi-check rule	no
OVAL Definition ID	oval:ssg-accounts_minimum_age_login_defs:def:1
Time	2024-07-24T08:02:03-05:00
Severity	medium

Figura 3.73 Quinta vulnerabilidad de nivel medio solventada

La siguiente vulnerabilidad de nivel medio que se presentó en el escaneo inicial es: *Uninstall Tuned Package*. Este paquete es una herramienta para la gestión de perfiles de rendimiento del sistema, diseñada para ajustar la configuración del sistema según distintos tipos de cargas de trabajo. Es recomendable desinstalar paquetes innecesarios o que no se usan, ya que esto reduce la cantidad de software que podría tener vulnerabilidades y disminuye la superficie de ataque del sistema [28]. En la Figura 3.74, se observa presente la vulnerabilidad en la máquina del servidor.

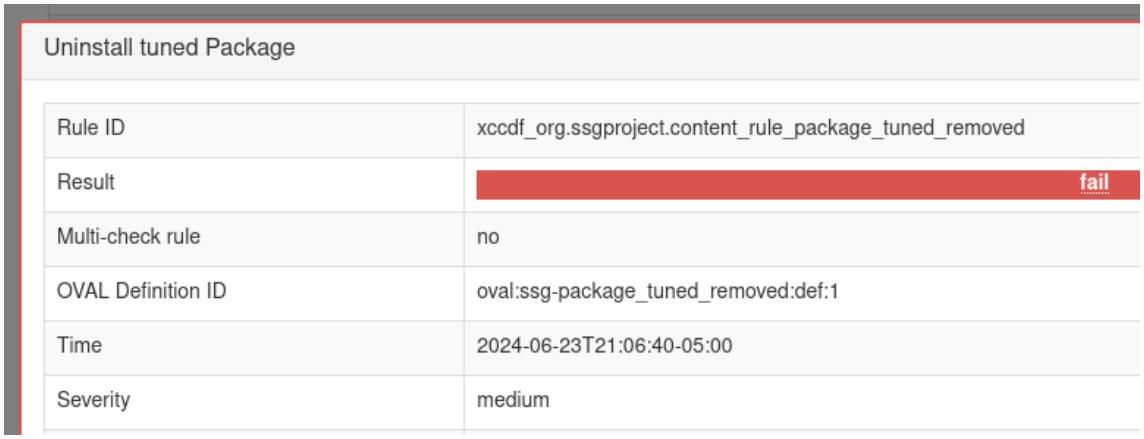


Figura 3.74 Vulnerabilidad del paquete “tuned” instalado

Para resolver esta regla vulnerable, se usó el comando expuesto en la Figura 3.75, el cual sirve para desinstalar el paquete "tuned" del sistema Rocky Linux 8.9. La operación se completó con éxito.

```
[root@mail erik]# sudo yum erase tuned
```

Figura 3.75 Desinstalación del paquete “Tuned”

Luego de la configuración, se volvió a ejecutar el escaneo. Al revisar el archivo “reporte11.html”, se constató que la vulnerabilidad había sido solucionada sin problemas adicionales, ver Figura 3.76.

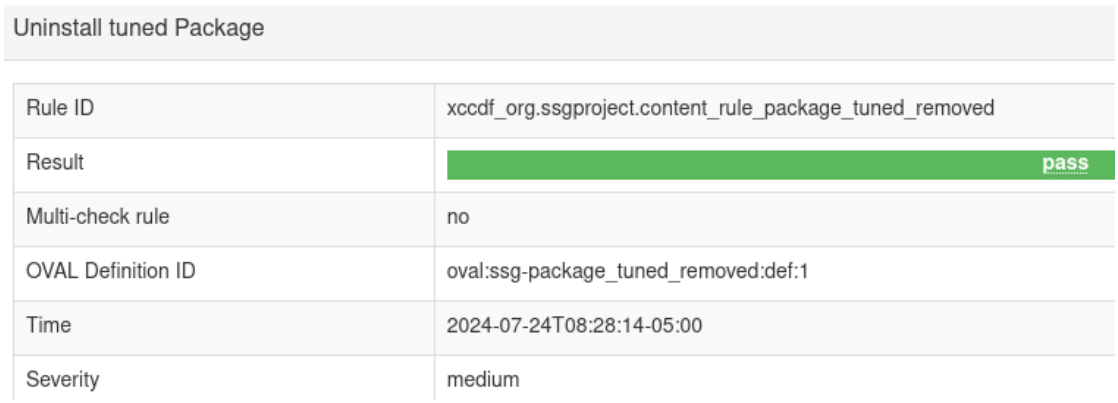


Figura 3.76 Sexta vulnerabilidad de nivel medio solventada

La última vulnerabilidad de nivel medio que se analizo fue: *Install the opensc Package Form Multifactor Authentication.* Esta regla hace referencia a la necesidad de instalación del paquete “opensc” para habilitar la autenticación multifactor. Dicho paquete es una biblioteca y un conjunto de herramientas diseñadas para el uso de tarjetas inteligentes y tokens de seguridad. Estas herramientas son necesarias para implementar sistemas de autenticación multifactor, que añaden una capa adicional de seguridad además de la contraseña. Incluso si una contraseña es comprometida, un atacante no podrá acceder al sistema sin el segundo factor de autenticación [29]. Como se muestra en la Figura 3.77, la vulnerabilidad aún no se ha solucionado.

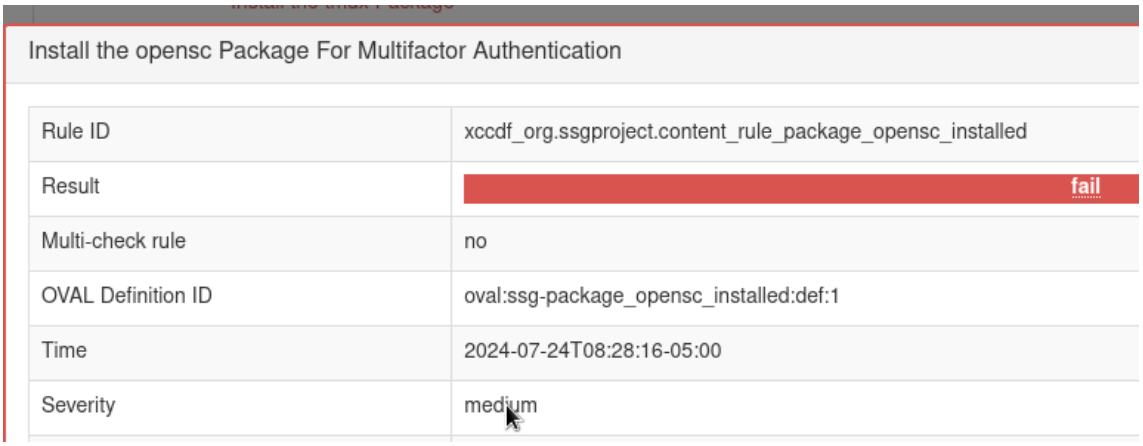


Figura 3.77 Última vulnerabilidad de nivel medio fallida

Para solucionar este parámetro, se utilizó la línea de comando dada en la Figura 3.78 para montar el paquete "opensc" en el sistema Rocky Linux 8.9. La instalación se completó sin problemas.

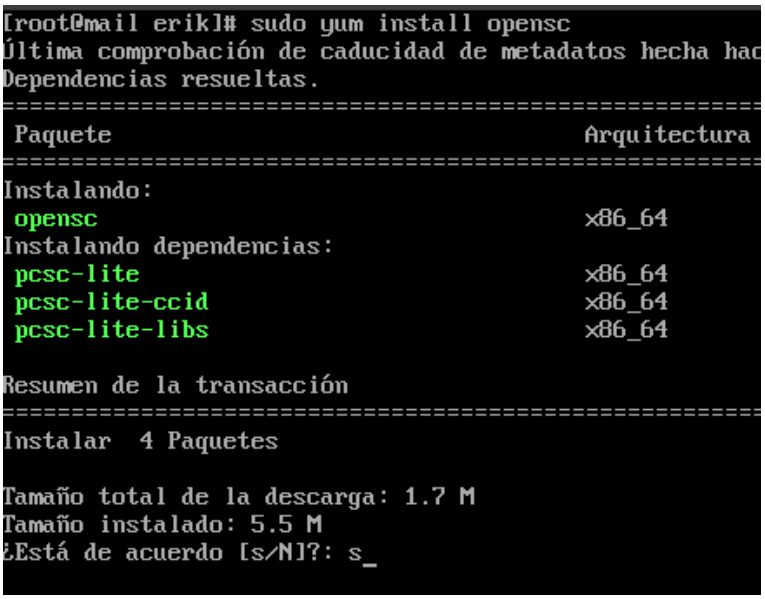
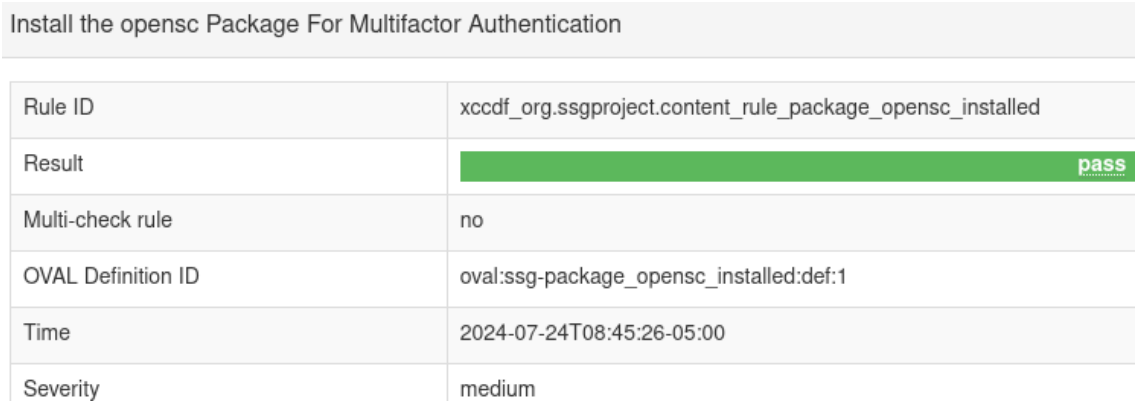


Figura 3.78 Instalación del paquete “opensc”

Al finalizar la configuración de la última vulnerabilidad, se ejecutó de nuevo el escaneo correspondiente. Al revisar el archivo “ultimo_reporte.html”, se comprobó en la Figura 3.79 que la vulnerabilidad había sido resuelta sin problemas adicionales.



Install the opensc Package For Multifactor Authentication

Rule ID	xccdf_org.ssgproject.content_rule_package_opensc_installed
Result	pass
Multi-check rule	no
OVAL Definition ID	oval:ssg-package_opensc_installed:def:1
Time	2024-07-24T08:45:26-05:00
Severity	medium

Figura 3.79 Última vulnerabilidad de nivel medio solventada

3.3 Análisis y resultados del proceso de escaneo

Tras finalizar el procedimiento de solución de vulnerabilidades en el sistema operativo Rocky Linux 8.9, los resultados finales se encuentran en el reporte "ultimo_reporte.html". La Figura 3.80 muestra las vulnerabilidades del informe inicial, es decir, antes de aplicar el *hardening* en el servidor. En contraste, la Figura 3.81 confirma que 11 vulnerabilidades de nivel alto y 6 reglas de nivel medio han sido corregidas según el estándar CIS, no se contabilizó la regla endurecida “*Install the opensc Package Form Multifactor Authentication”* ya que indica que se deben solventar otras reglas para registrarla. Así pues, el sistema operativo se ha vuelto menos vulnerable de acuerdo con la normativa CIS.

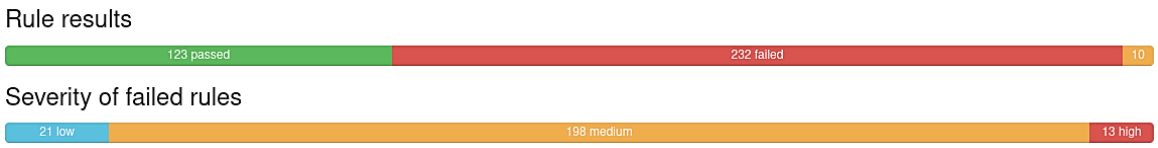


Figura 3.80 reporte1-inicial.html

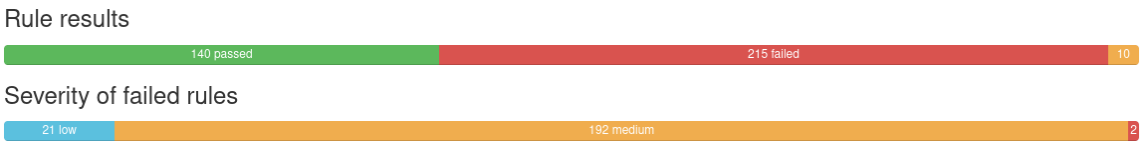


Figura 3.81 ultimo_reporte.html

En la Tabla 3.1 se exponen las reglas que se resolvieron en el servidor Rocky Linux 8.9, tanto de nivel alto como de nivel medio. Por lo tanto, se confirma el endurecimiento del sistema operativo.

Tabla 3.1 Vulnerabilidades solventadas

	Regla de nivel alto	Regla de nivel medio
Enable Dracut FIPS Module (soluciona tres vulnerabilidades altas)	✓	
Configure System Cryptography Policy (soluciona tres vulnerabilidades altas)	✓	
Ensure gpgcheck Enabled for Local Packages (soluciona cuatro vulnerabilidades altas)	✓	
Disable Ctrl-Alt-Del Burst Action	✓	
Install AIDE		✓
Build and Test AIDE Database		✓
Uninstall iprutils Package		✓
Set Password Maximum Age		✓
Set Password Minimum Age		✓
Uninstall Tuned Package		✓
*Install the opensc Package Form Multifactor Authentication (*no la contabiliza ya que indica que se deben solventar otras reglas para registrarla)		✓

Después de solucionar las vulnerabilidades listadas en la Tabla 3.1 y comparar el impacto de estos cambios entre el informe inicial y el final, se verificó el funcionamiento del servidor de correo instalado previamente. Cabe destacar que la herramienta telnet no es segura y no se recomienda su uso; sin embargo, en este caso, se utilizó únicamente en la comprobación del correcto trabajo local del servidor de correo. Con esta aclaración, fue posible realizar las pruebas locales. Se inició sesión con el usuario Fernando y se envió un mensaje de correo al usuario Juan, ver Figura 3.82

```
[root@mail erik]# su fernando
[fernando@mail erik]$ echo "Correo final de prueba" | mail -s "Prueba final" juan@rocky.com
```

Figura 3.82 Envío de correo de Fernando a Juan

A continuación, se accedió a la ruta “home/juan/Maildir/new” para confirmar que el usuario Juan recibió el correo, ver la Figura 3.83.

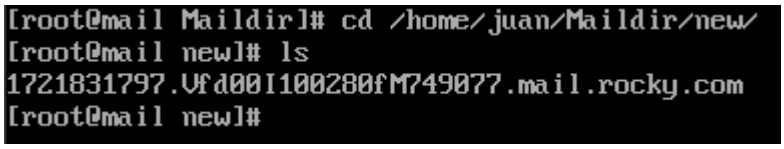


Figura 3.83 Confirmación del correo recibido por Juan

Después de la prueba de funcionamiento del correo, se usó el servicio de telnet para verificar el destinatario y el contenido del mensaje, ver Figura 3.84.

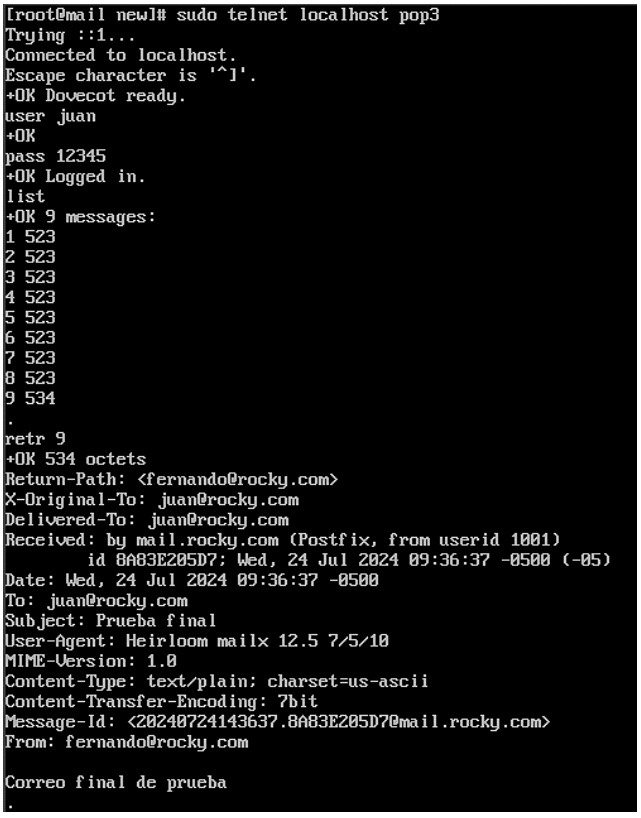


Figura 3.84 Revisión del correo enviado

Para resumir, se confirmó la correcta implementación de *hardening* en Rocky Linux 8.9 con ayuda de la herramienta OpenSCAP, además de observar el funcionamiento adecuado del servidor de correo tras los cambios y configuraciones aplicados

3.4 Verificación del *hardening* en base a la triada CIA

En este punto, se presenta un análisis detallado del último informe generado por la herramienta OpenSCAP, utilizando el protocolo CIS para evaluar la seguridad del sistema. Para ello, se ha elaborado la Tabla 3.2 que resume las vulnerabilidades

resueltas durante el proceso de *hardening*, destacando las variables clave relacionadas con los tres pilares fundamentales de la triada CIA.

Tabla 3.2 Análisis de vulnerabilidades

Vulnerabilidad	Perfil de nivel	Severidad	Confidencialidad	Integridad	Disponibilidad
Enable Dracut FIPS Module	Nivel 2	Alta	✓	✓	✓
Configure System Cryptography Policy	Nivel 2	Alta	✓	✓	✓
Ensure gpgcheck Enabled for Local Packages	Nivel 1	Alta	✓	✓	
Disable Ctrl-Alt-Del Burst Action	Nivel 1	Alta		✓	✓
Install AIDE	Nivel 1	Media	✓	✓	✓
Build and Test AIDE Database	Nivel 1	Media	✓	✓	✓
Uninstall iprutils Package	Nivel 1	Media			✓
Set Password Maximum Age	Nivel 1	Media	✓	✓	✓
Set Password Minimum Age	Nivel 1	Media	✓	✓	✓
Uninstall Tuned Package	Nivel 1	Media			✓
Install the opensc Package Form Multifactor Authentication	Nivel 2	Media	✓	✓	✓

La Tabla 3.3 explica de mejor manera los pilares de seguridad que incluye los Tabla 3.2.

Tabla 3.3 Parámetros analizados en las vulnerabilidades

Parámetro	Explicación
Vulnerabilidad	Nombre de la regla vulnerable.
Perfil de nivel	El protocolo CIS utiliza perfiles para clasificar la criticidad de las vulnerabilidades y orientar su análisis. El perfil de nivel 1 se refiere a recomendaciones básicas que no requieren configuraciones complejas. Por otro lado, el perfil de nivel 2 incluye recomendaciones urgentes debido a la alta criticidad de las vulnerabilidades, y puede implicar configuraciones más complejas de implementar y validar.
Severidad	Es el grado de gravedad asociado a la vulnerabilidad.

Parámetro	Explicación
Confidencialidad	Se centra en la protección de los datos transmitidos por una red, garantizando que únicamente los usuarios con autorización puedan acceder a la información.
Integridad	Asegura que los datos generados y transmitidos no sean modificados durante su tránsito, manteniendo la información original y sin alteraciones.
Disponibilidad	Garantiza que los datos enviados por la red lleguen al usuario, mediante el uso de sistemas redundantes, planificación de capacidad y balanceo de carga, entre otras estrategias.

Los resultados indican que, al corregir las reglas fallidas conforme a las directrices del protocolo CIS, se ha logrado una alineación efectiva con los principios de la triada CIA. Esto ha permitido reforzar la seguridad del sistema operativo Rocky Linux 8.9 y, al mismo tiempo, garantizar el funcionamiento adecuado del servicio de correo en el servidor.

Guía de buenas prácticas para dar mayor seguridad a un sistema operativo

A medida que las amenazas tecnológicas evolucionan, es esencial adoptar medidas para reforzar la seguridad de un sistema operativo. A continuación, se detallan las mejores prácticas recomendadas para proteger eficazmente los sistemas frente a vulnerabilidades, siguiendo directrices y principios de seguridad establecidos:

- Es fundamental crear un almacenamiento de copias de seguridad robusto. Así pues, se puede garantizar que, ante posibles fallos, la información pueda ser recuperados de manera rápida y eficiente, minimizando así el impacto de posibles pérdidas.
- La instalación y configuración de *firewalls* es una estrategia clave para complementar las contraseñas y fortalecer la defensa del sistema. Además, el uso de contraseñas seguras para proteger archivos y directorios sensibles es crucial para evitar accesos no autorizados.
- Mantener el sistema operativo al día con las últimas actualizaciones y parches es esencial para corregir vulnerabilidades y prevenir explotaciones por parte de atacantes. Las actualizaciones periódicas ayudan a cerrar posibles brechas de seguridad.

- La integridad de los datos durante su transmisión también es vital. La utilización de algoritmos de verificación garantiza que la información no sea alterada durante el tránsito, asegurando que los datos recibidos coincidan con los enviados.
- Para asegurar la disponibilidad constante de la información, es necesario establecer sistemas de respaldo y redundancia. Aunque esto puede ser complejo, es fundamental para garantizar que los datos estén siempre accesibles incluso en caso de fallos del sistema.
- Es recomendable ejecutar una evaluación exhaustiva de absolutamente todos los elementos de un sistema informático, siguiendo estándares internacionales. Este análisis ayuda a identificar y reducir brechas de seguridad, mejorando así la protección general del sistema.
- Las auditorías periódicas son cruciales para comprobar la veracidad de la información como también para rastrear accesos. Estas revisiones permiten detectar y corregir fallos de seguridad, manteniendo el sistema bajo vigilancia continua.
- La aplicación de algoritmos de cifrado es totalmente esencial para asegurar la privacidad de la información, protegiéndolos contra accesos no autorizados y garantizando su privacidad.
- Un análisis regular del sistema es una práctica recomendada para identificar y abordar vulnerabilidades a medida que surgen, asegurando una respuesta proactiva a posibles brechas de seguridad.

Guía de buenas prácticas para dar mayor seguridad en un servidor de correo

Al igual que en la gestión de sistemas operativos, es crucial aplicar directrices específicas para asegurar la protección de un servidor de correo electrónico contra diversas amenazas y vulnerabilidades. A continuación, se presentan una serie de recomendaciones diseñadas para dar un funcionamiento seguro y eficiente del servidor, así como para proteger la información que maneja:

- Es fundamental establecer políticas de seguridad que se basen en estándares y marcos de referencia reconocidos en ciberseguridad, con el fin de garantizar una protección integral del servidor.
- Para mantener la integridad de los correos electrónicos, se recomienda el uso de firmas digitales. Estas firmas permiten verificar que la información contenida en los mensajes no haya sido alterada durante su transmisión.

- La configuración y gestión de *firewalls* es esencial para filtrar la información, restringir accesos y permitir solo las conexiones necesarias para el funcionamiento del servicio de correo electrónico.
- La existencia de filtros en los mensajes de spam es otra medida clave para reducir la llegada de mensajes no deseados, lo cual contribuye a disminuir posibles amenazas y mantener el servidor libre de contenido indeseado.
- Es importante realizar un monitoreo constante del servidor de correo para identificar y analizar patrones sospechosos. Este seguimiento continuo ayuda a detectar comportamientos anómalos y posibles intentos de intrusión.
- La segmentación de red es una técnica efectiva que consiste en dividir la red en segmentos para dar ingreso al servidor de correo únicamente al personal y sistemas designados, mejorando así la seguridad general.
- Se debe llevar a cabo una instalación mínima del servidor, limitando los servicios a los estrictamente necesarios. Esta práctica reduce las superficies de ataque potenciales y fortalece la seguridad del sistema.
- Establecer contraseñas fuertes para todas las cuentas del servidor es indispensable. Las claves obligatoriamente deben contener un mínimo de 8 caracteres y estar compuestas por una combinación de caracteres especiales, números, así como letras mayúsculas y minúsculas, para garantizar un nivel adecuado de seguridad.

4 CONCLUSIONES

La aplicación de *hardening* en Rocky Linux 8.9 y el servidor de correo ha puesto de manifiesto una serie de riesgos significativos que, en ausencia de una política de seguridad adecuada, podrían poner en serio peligro la integridad del sistema. Al emplear el marco de seguridad CIS como guía y herramientas de escaneo como OpenSCAP, se lograron identificar y evaluar detalladamente estas vulnerabilidades. A continuación, se exponen las conclusiones del trabajo realizado:

- El análisis de vulnerabilidades del sistema operativo ha sido fundamental para abordar y solucionar las reglas de alto peligro que representaban serias amenazas tanto para el sistema operativo Rocky Linux 8.9 como para el servidor de correo, según el marco de seguridad CIS.
- Se evidenciaron las vulnerabilidades y riesgos inherentes a Rocky Linux 8.9 en ausencia de una política de seguridad adecuada basada en estándares específicos. Estas vulnerabilidades, si no se abordan, pueden tener graves

repercusiones en el funcionamiento del sistema. Por tanto, el uso de herramientas de escaneo como OpenSCAP resulta crucial en el ámbito de la ciberseguridad. Estas herramientas permiten la identificación, evaluación y gestión detallada de las vulnerabilidades, facilitando la formalización de los estándares recomendados en el marco de referencia de seguridad CIS.

- Varias reglas fallidas de nivel medio fueron abordadas. Aunque no presentan un riesgo tan elevado, podrían afectar la integridad del sistema. Es importante no subestimar la importancia de resolver estas vulnerabilidades, ya que cualquier brecha puede comprometer el sistema en su conjunto.
- El trabajo expuesto muestra la relevancia de aplicar políticas de seguridad rigurosas durante la instalación y configuración de Rocky Linux 8.9 y en la configuración del servidor de correo asociado. Es crucial considerar los marcos de referencia de seguridad y seguir sus recomendaciones para asegurar que los pilares de seguridad estén correctamente implementados en el servidor y el sistema operativo.
- Los resultados y el análisis de los escaneos y correcciones realizadas destacan la importancia de la concienciación sobre los riesgos actuales en la ciberseguridad y la seguridad informática. Es fundamental conocer las herramientas y estrategias para mitigar las brechas de protección tanto en el montaje de sistemas operativos como en servidores.
- Aunque OpenSCAP puede solucionar vulnerabilidades de sus informes de forma automática, se decidió realizar el proceso manualmente, abordando cada vulnerabilidad de manera individual para garantizar una resolución más segura.
- Las mejoras en la seguridad y robustez tanto de Rocky Linux 8.9 como del servidor de correo fueron evidentes tras la ejecución de las configuraciones respectivas. La cantidad de porcentaje en los resultados del informe aumentó del 48.86% al 50.65% tras la aplicación de las políticas de seguridad.

5 RECOMENDACIONES

- Un problema que se ubica dentro de los más comunes en la seguridad informática es el propio usuario. Por esta razón, es esencial educar a todas las personas involucradas en un sistema informático sobre la importancia de aplicar políticas de seguridad adecuadas. La formación en ciberseguridad es crucial para reducir los riesgos.

- Es fundamental seguir rigurosamente las recomendaciones de los marcos de referencia de seguridad, como el estándar CIS en este caso. Evitar las indicaciones de fuentes no oficiales ayuda a prevenir configuraciones incorrectas y posibles daños en el servidor.
- Dentro de los parámetros del servidor de correo se recomienda el uso de una dirección IP estática. Esto permite un mejor control sobre el acceso al servidor y facilita la gestión del *firewall*, lo que contribuye a una mayor seguridad.
- Se sugiere utilizar un sistema operativo sin interfaz gráfica en servidores, ya que esto facilita la gestión a través de la línea de comandos. Además, para mejorar la toma de decisiones sobre vulnerabilidades y sus soluciones, es útil emplear una máquina cliente con una interfaz gráfica que sea compatible para transferir y visualizar los reportes generados en un navegador.
- Todos los estándares de seguridad tienen el propósito de fortalecer un sistema informático. Se aconseja seleccionar y aplicar los estándares de seguridad más apropiados según las necesidades y el alcance específico del sistema.
- Es importante realizar copias de seguridad del sistema operativo para asegurar la recuperación en caso de fallos derivados de configuraciones incorrectas. Esto permite corregir errores sin perder los cambios realizados anteriormente.
- Aunque es más laborioso realizar el *hardening* de manera manual, abordando cada vulnerabilidad por separado, ofrece un mejor control sobre los ajustes. Es recomendable verificar el funcionamiento del servidor después de resolver cada vulnerabilidad para asegurar su eficacia y estabilidad.

6 REFERENCIAS BIBLIOGRÁFICAS

[1] O. Cruz, «Repositorio Libertadores,» 2017. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repository.libertadores.edu.co/server/api/core/bitstreams/cd43cbd8-04b2-4dc9-9ef5-ea8733dbeeca/content. [Último acceso: 15 mayo 2024].

[2] I. Andrea, «Repositorio Unipiloto,» [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2826/00001572.pdf?sequence=1&isAllowed=y. [Último acceso: 15 mayo 2024].

[3] «Red Hat,» 2024. [En línea]. Available: https://www.redhat.com/es/technologies/linux-platforms/enterprise-

linux#:~:text=Red%20Hat%C2%AE%20Enterprise%20Linux%C2%AE%20es%20un%20sistema%20operativo,como%20proceso%20de%20migraci%C3%B3n%20directo. [Último acceso: 15 mayo 2024].

[4] «Almalinux,» 2024. [En línea]. Available: https://almalinux.org/es/. [Último acceso: 15 mayo 2024].

[5] «Debian,» 11 febrero 2022. [En línea]. Available: https://www.debian.org/intro/why_debian. [Último acceso: 15 mayo 2024].

[6] «CentOS,» 2024. [En línea]. Available: https://www.centos.org/about/. [Último acceso: 15 mayo 2024].

[7] «Rocky Linux,» [En línea]. Available: https://rockylinux.org/about. [Último acceso: 15 mayo 2024].

[8] A. Hernandez, «Redalyc,» febrero 2015. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.redalyc.org/pdf/5122/512251501005.pdf. [Último acceso: 15 mayo 2024].

[9] «OpenSCAP,» [En línea]. Available: https://www.open-scap.org/tools/scap-workbench/. [Último acceso: 15 mayo 2024].

[10] «OpenSCAP,» 2024. [En línea]. Available: https://www.open-scap.org/tools/openscap-base/. [Último acceso: 15 mayo 2024].

[11] «OpenSCAP,» 2024. [En línea]. Available: https://www.open-scap.org/security-policies/scap-security-guide/. [Último acceso: 15 mayo 2024].

[12] D. Wendlandt, «Nessus,» [En línea]. Available: https://www.cs.cmu.edu/~dwendlan/personal/nessus.html#:~:text=Nessus%20is%20a%20remote%20security,have%20connected%20to%20a%20network.. [Último acceso: 15 mayo 2024].

[13] «OpenVAS,» [En línea]. Available: https://www.openvas.org/. [Último acceso: 15 mayo 2024].

[14] R. Lopez, «Repositorio USAM,» [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.usam.ac.cr/xmlui/bitstream/handle/11506/2036/LEC%20ING%20SIST%200004%202017.pdf?sequence=1&isAllowed=y. [Último acceso: 15 mayo 2024].

[15] «NIST,» 11 enero 2022. [En línea]. Available: https://www.nist.gov/about-nist. [Último acceso: 15 mayo 2024].

[16] M. Ladino, «Universidad Tecnológica de Pereira,» abril 2011. [En línea]. Available: https://ojs2.utp.edu.co/index.php/revistaciencia/article/view/1177/669. [Último acceso: 2024 mayo 2024].

[17] «CIS security,» 2024. [En línea]. Available: https://www.cisecurity.org/about-us. [Último acceso: 15 mayo 2024].

[18] «FORTINET,» [En línea]. Available: https://www.fortinet.com/lat/resources/cyberglossary/cia-triad. [Último acceso: 25 mayo 2024].

[19] «Ret Hat Documentation,» [En línea]. Available: https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-federal_standards_and_regulations-federal_information_processing_standard#sect-Security_Guide-Federal_Standards_And_Regulations-Federal_Information. [Último acceso: 25 mayo 2024].

[20] «Red Hat Documentation,» [En línea]. Available: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/security_hardening/using-the-system-wide-cryptographic-policies_security-hardening. [Último acceso: 25 mayo 2024].

[21] S. Varghese, «Quora,» 2017. [En línea]. Available: https://www.quora.com/What-is-gpgcheck-in-a-yum-configuration-file-in-Rhel. [Último acceso: 25 mayo 2024].

[22] «STIG Viewer,» [En línea]. Available: https://www.stigviewer.com/stig/red_hat_enterprise_linux_8/2023-12-01/finding/V-230531. [Último acceso: 25 mayo 2024].

[23] «RAPID7,» 10 agosto 2023. [En línea]. Available: https://www.rapid7.com/blog/post/2017/06/30/how-to-install-and-configure-aide-on-ubuntu-linux/. [Último acceso: 2024 mayo 2024].

[24] «Red Hat Documentation,» [En línea]. Available: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/security_guide/sec-using-aide#sec-Using-AIDE. [Último acceso: 25 mayo 2024].

[25] «STIG Viewer,» [En línea]. Available: https://www.stigviewer.com/stig/red_hat_enterprise_linux_8/2022-12-06/finding/V-230560. [Último acceso: 25 mayo 2024].

[26] «DATADOG,» [En línea]. Available: https://docs.datadoghq.com/security/default_rules/xccdf-org-ssgproject-content-rule-accounts-maximum-age-login-defs/. [Último acceso: 25 mayo 2024].

[27] «stack Exchange,» [En línea]. Available: https://security.stackexchange.com/questions/78758/what-is-the-purpose-of-the-password-minimum-age-setting. [Último acceso: 25 mayo 2024].

[28] «STIG Viewer,» [En línea]. Available: https://www.stigviewer.com/stig/red_hat_enterprise_linux_8/2021-06-14/finding/V-230561. [Último acceso: 25 mayo 2024].

[29] «ATO Pathways,» [En línea]. Available: https://ato-pathways.com/catalogs/xccdf/items/8284. [Último acceso: 25 mayo 2024].

7 ANEXOS

ANEXO I: Certificado de Originalidad

CERTIFICADO DE ORIGINALIDAD

Quito, D.M. 31 de Julio de 2024

De mi consideración:

Yo, GABRIELA KATHERINE CEVALLOS SALAZAR, en calidad de Directora del Trabajo de Integración Curricular titulado IMPLEMENTACIÓN DE *HARDENING* EN UN SISTEMA OPERATIVO DE SERVIDOR LINUX DE BASE RED HAT asociado al proyecto IMPLEMENTACIÓN DE *HARDENING* EN SISTEMAS OPERATIVOS DE SERVIDOR elaborado por el estudiante ERIK FERNANDO ORTEGA HERNANDEZ de la carrera en Tecnología Superior en Redes y Telecomunicaciones, certifico que he empleado la herramienta Turnitin para la revisión de originalidad del documento escrito completo, producto del Trabajo de Integración Curricular indicado.

El documento escrito tiene un índice de similitud del 11%.

Es todo cuanto puedo certificar en honor a la verdad, pudiendo el interesado hacer uso del presente documento para los trámites de titulación.

NOTA: Se adjunta el link del informe generado por la herramienta Turnitin.

https://epnecuador-my.sharepoint.com/personal/gabriela_cevalloss_epn_edu_ec/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fgabriela%5Fcevalloss%5Fepn%5Fedu%5Fec%2FDocuments%2FProyecto%20de%20Titulaci%C3%B3n%20Sr%20Erik%20Ortega%2FTIC%20Sr%20Erik%20Ortega%20TSRT%2FTurnitin%20Sr%20Erik%20Ortega%2Epdf&parent=%2Fpersonal%2Fgabriela%5Fcevalloss%5Fepn%5Fedu%5Fec%2FDocuments%2FProyecto%20de%20Titulaci%C3%B3n%20Sr%20Erik%20Ortega%2FTIC%20Sr%20Erik%20Ortega%20TSRT&ga=1

Atentamente,

Gabriela Katherine Cevallos Salazar

Docente

Escuela de Formación de Tecnólogos

ANEXO II: Reporte Inicial del Escaneo

ANEXO III: Reporte Final del Escaneo

ANEXO IV: Enlace del Video