

# **ESCUELA POLITÉCNICA NACIONAL**

## **ESCUELA DE FORMACIÓN DE TECNÓLOGOS**

### **IMPLEMENTACIÓN DE *HARDENING* EN SISTEMAS OPERATIVOS DE SERVIDOR**

### **IMPLEMENTACIÓN DE *HARDENING* EN CENTOS CON CIS**

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

**ABRAHAN DARIO JARAMILLO CALVACHE**

abraham.jaramillo@epn.edu.ec

**DIRECTOR: ING. GABRIELA KATHERINE CEVALLOS SALAZAR**

gabriela.cevalloss@epn.edu.ec

**DMQ, febrero 2024**

## **CERTIFICACIONES**

Yo, Abraham Darío Jaramillo Calvache 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.

---

Abraham Dario Jaramillo Calvache

**abraham.jaramillo@epn.edu.ec**

**isaac77jaramillo@gmail.com**

Certifico que el presente trabajo de integración curricular fue desarrollado por ABRAHAN DARIO JARAMILLO CALVACHE, 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.

Abraham Darío Jaramillo Calvache

CI: 1725200917

## **DEDICATORIA**

Dedico el presente trabajo a mi madre, mi pilar fundamental toda la vida. Gracias a su excepcional esfuerzo, las desveladas, los trabajos de más de 12 horas, incluso fines de semana, en las madrugadas, etc., sus cuidados de forma incondicional que me ayudaron y me guiaron a lo largo de mi vida. Dedico también este trabajo y logro a mi querida hermana, gracias a ella por su apoyo constante para alcanzar mis metas. Gracias a ellas, a su apoyo y paciencia que se reflejan en mi día a día. Finalmente, pero no menos importante, este trabajo y logro también lo dedico a Angie Mora Rodríguez, a quien tuve el privilegio de conocer gracias a la Escuela Politécnica Nacional. Ella ha sido mi apoyo fundamental e incondicional estos últimos años y es mi inspiración y motivación para ser una mejor persona en todos los ámbitos de la vida; mi novia y compañera de vida.

Abrahan Jaramillo

## **AGRADECIMIENTO**

Le doy gracias a Dios por su cuidado y bendiciones a lo largo de mi vida, porque a pesar de todo, él siempre ha estado guiándome a través de este camino. Le agradezco también a mi familia, mi madre, mi hermana que sin ellas este logro no podría haber sido posible. Su paciencia, sus cuidados han sido fundamentales para avanzar en este camino.

Quisiera agradecer también a mi padre, porque a pesar de todas las dificultades también estuvo allí apoyándome de la manera en que le fue posible.

Les agradezco a las personas que conocí en este camino en la Escuela Politécnica Nacional, a los que ahora considero mis amigos.

Abrahan Jaramillo

# ÍNDICE DE CONTENIDOS

CERTIFICACIONES .....	I
DECLARACIÓN DE AUTORÍA .....	II
DEDICATORIA .....	III
AGRADECIMIENTO .....	IV
ÍNDICE DE CONTENIDOS .....	V
RESUMEN .....	VII
ABSTRACT.....	VIII
1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO .....	1
1.1 Objetivo general.....	1
1.2 Objetivos específicos.....	1
1.3 Alcance .....	1
1.4 Marco Teórico .....	2
Sistemas operativos Linux basados en distribución <i>Linux Red Hat Enterprise</i> .....	2
Sistema Operativo CentOS.....	2
<i>Hardening</i> .....	3
Marcos de regulación de seguridad.....	4
2 METODOLOGÍA.....	7
3 RESULTADOS .....	8
3.1 Identificación de vulnerabilidades en un sistema operativo de servidor .....	8
Instalación y configuración del servidor de correo .....	10
Instalación de la herramienta de escaneo OpenSCAP.....	14
3.2 Implementación de políticas de seguridad en el sistema operativo .....	21
Resolución de reglas fallidas de nivel alto.....	21
Resolución de reglas fallidas de nivel medio.....	28
3.3 Análisis y resultados del proceso de escaneo .....	36
3.4 Verificación del <i>hardening</i> en base a la triada CIA .....	39

	Guía de buenas prácticas para reforzar la seguridad de un sistema operativo ....	41
	Guía de buenas prácticas para reforzar la seguridad de servidor de correo .....	43
4	CONCLUSIONES.....	44
5	RECOMENDACIONES .....	45
6	Referencias .....	47
7	ANEXOS.....	50
	ANEXO I: Certificado de Originalidad .....	50

# RESUMEN

El presente proyecto de titulación tiene como propósito la implementación de *hardening* en un sistema operativo CentOS 8 con el objetivo de buscar, encontrar, analizar y erradicar, en la medida de lo posible y bajo las recomendaciones de CIS, vulnerabilidades o posibles amenazas que afecten a los pilares de la ciberseguridad. Para dicho fin, se plantean las siguientes secciones:

En la primera sección se presenta cada una de las variables que componen el enfoque del problema. El objetivo principal, los objetivos específicos, el alcance de la investigación y el marco teórico. Estos puntos engloban los pilares fundamentales del problema, entre los que destacan: el sistema operativo, *hardening*, marcos de regulación de seguridad, estándar CIS y las herramientas de escaneo que se basan en el estándar CIS.

En la segunda sección se expone la metodología usada para la ejecución del presente proyecto, detallando de manera precisa y concisa el proceso para que los objetivos señalados sean cumplidos a cabalidad.

En la tercera sección se exponen y analizan cada uno de los resultados que la implementación del *hardening* arroja. En este sentido, se detalla la implementación de un servidor de correo en CentOS 8 sin ninguna política de seguridad, la instalación de la herramienta de escaneo de vulnerabilidades OpenSCAP, así como el reporte que esta herramienta presenta. Se implementaron varias políticas de seguridad contemplando las recomendaciones de CIS y se presenta una guía de buenas prácticas de seguridad para sistemas informáticos.

La cuarta sección presenta las conclusiones basadas en cada uno de los objetivos propuestos y de igual forma las recomendaciones que se deben tener presente al momento de endurecer un servidor.

La última sección corresponde a la bibliografía en la cual la investigación del presente proyecto se basó.

**PALABRAS CLAVE:** OpenSCAP, *hardening*, estándar CIS, CentOS 8.



## **ABSTRACT**

*The purpose of this graduation project is the implementation of hardening on a CentOS 8 operating system with the goal of searching, identifying, analyzing, and eradicating vulnerabilities or potential threats that may affect the pillars of cybersecurity, to the extent possible and in accordance with CIS recommendations. To achieve this aim, the following sections are outlined:*

*In the first section, each variable that constitutes the problem's approach is presented. The main objective, specific goals, research scope, and theoretical framework are discussed. These points encompass the fundamental pillars of the problem, including the operating system, hardening, security regulation frameworks, CIS standard, and scanning tools based on the CIS standard.*

*The second section details the methodology used for the execution of this project, providing a precise and concise overview of the process to ensure the stated objectives are fully met.*

*The third section exposes and analyzes the results yielded by the implementation of hardening. It outlines the deployment of a mail server on CentOS 8 without any security policies, the installation of the vulnerability scanning tool OpenSCAP, and the report generated by this tool. Multiple security policies were implemented in line with CIS recommendations, and a guide to best security practices for computer systems is presented.*

*The fourth section presents conclusions based on each of the proposed objectives, along with recommendations to keep in mind when hardening a server.*

*The last section corresponds to the bibliography on which the research of this project is based.*

**KEYWORDS:** *Operating system, hardening, CIS standard, CentOS 8.*

# 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 infiltrarse.

Se tiene un sistema operativo de servidor con un servidor de correo electrónico, se escaneará el mismo mediante una herramienta de escaneo de configuración y vulnerabilidades basada en el protocolo SCAP, donde se obtendrá un reporte inicial el cual será comparado con un reporte luego de endurecer al 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

### **Sistemas operativos Linux basados en distribución *Linux Red Hat Enterprise***

Los sistemas operativos Linux son sistemas con código abierto lo que permite la configuración y edición de su código fuente con varios fines. Fue desarrollado en la época de los años 90 por *Linus Trovards*.

Las distribuciones de estos sistemas están basadas en *Red Hat Enterprise* y poseen un código fuente RHEL (*Red Hat Enterprise Linux*), lo cual les brinda varios beneficios entre los que destacan:

- Interfaz de usuario amigable con el usuario.
- Soporte en el ciclo de vida.
- Selección de paquetes de *software*.

Estos beneficios les permiten ser estables tanto en compatibilidad como en seguridad, con lo cual están orientados a entornos empresariales y entornos de servicios [1].

Entre las distribuciones más destacadas se encuentra el sistema operativo CentOS, cuyo soporte finalizo el 31 de diciembre del 2021, no obstante, los usuarios aún tienen soporte en seguridad por 4 años más.

### **Sistema Operativo CentOS**

El sistema operativo CentOS es de las distribuciones más usadas de Linux siendo una de las razones más importantes el hecho de que cuenta con una base RHEL.

RHEL es la distribución más comercializada en sistemas Linux. Principalmente está destinado para entornos empresariales. RHEL también es considerada como una actualización de la distribución del sistema operativo Fedora, con un entorno mucho más optimizado, con certificado y soporte técnico [2].

Entre las características más importantes de RHEL destacan:

- Código Abierto: En esta distribución se puede acceder completamente al código fuente para hacer modificantes del sistema según se requiera.
- Compatibilidad con estándares industriales: Generalmente todas las distribuciones basadas en *Red Hat Enterprise* y en el código RHEL cuentan y cumplen con estándares específicos y precisos de requisitos de seguridad. Esto

permite que, en este caso el sistema operativo CentOS sea un entorno que permita el cumplimiento de normativas de seguridad.

- **Compatibilidad con herramientas de *hardening*:** Al ser una distribución que tiene compatibilidad con estándares industriales, CentOS tiene un entorno con múltiples herramientas de auditoría de seguridad, lo que facilita el endurecimiento del sistema operativo y sus elementos.

La instalación del entorno virtualizado del sistema operativo CentOS 8 para efectos del presente proyecto, tuvo que cumplir con varios requisitos en la máquina local para su correcto funcionamiento:

- 4GB de RAM recomendado
- Procesador de virtualización en la máquina local VT-x o AMD-V
- Instalación de un sistema de virtualización (VMware o VirtualBox)
- Imagen ISO del sistema CentOS 8

### ***Hardening***

El endurecimiento de un sistema informático o también llamado "*Hardening*" es un proceso que permite reforzar o robustecer dicho sistema mediante una configuración avanzada y cuidadosa del *software* con el objetivo de reducir significativamente las vulnerabilidades, debilidades o amenazas que pueden presentar tanto el sistema como todos los elementos que lo componen [3].

El uso y aplicación del *hardening* surge a raíz de las diversas y nuevas amenazas que se han manifestado proporcionalmente al avance de la tecnología. Este proceso asegura y refuerza los métodos convencionales de seguridad garantizando la seguridad de la información y de los elementos que componen un sistema informático [4].

La seguridad informática contempla tres aspectos fundamentales al momento de fortalecer un sistema informático: la confidencialidad, la integridad y la disponibilidad. Hay que destacar también que existen dos aspectos más llamados no repudio y autenticidad los que completan los aspectos de la seguridad informática.

- **Confidencialidad:** Los datos que se transmiten por medio de la red tienen que estar accesibles solo a los sistemas o entes que se encuentran autorizados a recibirlos. La confidencialidad permite este fin mediante la autorización y control [5].
- **Integridad:** La integridad trabaja de la mano con la confidencialidad. Y es que a más de que los datos lleguen solo a las personas autorizadas, en seguridad informática es imperiosa la necesidad de que estos datos lleguen tal y cual como se crearon, es decir, que estos datos en el transcurso de su envío mediante la

red e incluso desde la misma creación, no hayan sido alterados [6]. Entre los riesgos que pueden existir en este contexto están: errores humanos, errores de programación, errores de transferencia.

- **Disponibilidad:** El acceso a los datos o también llamado disponibilidad es uno de los tres pilares fundamentales de la seguridad informática. En resumen, este principio asegura el acceso a los datos a las personas que, mediante el principio de la confidencialidad están autorizadas a hacerlo [7].
- **Autenticidad:** Es un componente fundamental dentro del contexto de ciber seguridad. Permite proteger y asegurar los datos contra accesos que no estén autorizados. Básicamente la autenticidad se encarga de verificar la identidad de un usuario asegurando que la información se entregue a quien tiene que entregarse.
- **No repudio:** Este componente igual de importante que los anteriores tiene el objetivo de evitar que una entidad niegue acciones que previamente haya realizado dentro del sistema operativo. Este elemento de ciber seguridad se puede asegurar mediante el uso de protocolos como HTTPS, configuración de firewalls o segmentación de red.

### **Marcos de regulación de seguridad**

Los marcos de regulación están definidos como un conjunto de normas o estándares cuya función principal es la de contribuir a gestionar y fortalecer el ámbito de la seguridad informática a organizaciones o empresas. Las organizaciones tienen la oportunidad de apegarse a los diversos marcos de seguridad que existen y al cumplir los requisitos que cada uno de estos marcos posee puedan identificar, proteger y responder de manera adecuada a los múltiples ataques informáticos y cibernéticos que existen en la actualidad. Existen varios estándares de seguridad entre los cuales destacan:

- *NIST Cybersecurity Framework*  
Este es un estándar que adecua una guía con normas y reglas detalladas para fortalecer un sistema informático mediante la gestión de riesgos. Fue desarrollado por el Instituto Nacional de Estándares y Tecnologías.
- *ISO 270001*  
Se trata de un marco de regulación internacional cuyo objetivo radica en establecer, implementar, mantener y mejorar la gestión de seguridad SGSI. Este estándar está basado en el ciclo de planificar, hacer, verificar y actuar (PDCA) asegurando de esta manera la mejora continua en la gestión de seguridad.
- *CIS Center for Internet Security*

Se trata de un conjunto de normas o reglas que provee a las organizaciones la ayuda necesaria para la protección informática en contra de amenazas latentes [8].

### **Estándar CIS (*Center for Internet Security*)**

Los controles críticos de seguridad CIS son un conjunto de métodos o procedimientos que promueven las buenas prácticas de seguridad mediante recomendaciones. Están destinados a la protección de sistemas informáticos para evitar ataques a todos los elementos que los conforman y por ende a la información que estos contengan. Fueron propuestos y creados en el año 2008 por organizaciones de seguridad en conjunto con el gobierno de los Estados Unidos.

Los controles CIS están regidos bajo la aplicación de ciertas actividades que permiten que, aparte de ser una lista de recomendaciones de seguridad para la prevención de ataques informáticos, sean acciones que prioricen los requerimientos de seguridad de sistemas informáticos.

Los controles CIS disponen de 20 principales recomendaciones en el marco de la seguridad para organizaciones. Desde esta perspectiva, las 20 recomendaciones están divididas en 3 grupos cuyas características se diferencia según el perfil de riesgo de la empresa.

- Grupo 1 (IG1): Las recomendaciones giran en torno a las vulnerabilidades más comunes que existen. Son las más básicas y las que cualquier organización debería poseer en su entorno informático. También se aplica a empresas u organizaciones pequeñas que no manejen información sensible.
- Grupo 2 (IG2): Estas recomendaciones se aplican a organizaciones que tengan un manejo de información mucho más sensible. Se complementan con las recomendaciones del IG1 para el fortalecimiento de la seguridad de los sistemas informáticos.
- Grupo 3 (IG3): Este grupo va dirigido a importantes y grandes empresas, cuya información sea muy sensible. Las recomendaciones del grupo 1 y del grupo 2 hacen un complemento con este grupo y mitigan de manera significativamente los posibles ataques y las posibles vulnerabilidades que están dirigidas a los sistemas informáticos de estas empresas [9].

Algunas de las actividades desarrolladas por CIS son:

- Identificación de los problemas más comunes.
- Seguimiento y focalización de todas las amenazas existentes dentro de la comunidad.

- La información obtenida, completa y visual de las amenazas escaneadas tanto como del ataque en sí. También las herramientas para solucionarlas, las cuales pueden y deben ser compartida [10].

Para la correcta realización de al menos este último punto se suele hacer uso de sistemas operativos de base Linux, debido a su gran estabilidad operativa y alto nivel de configuración en su código base.

### **Herramientas de escaneo de sistemas informáticos basados en CIS**

Como se mencionó anteriormente, CIS es una guía de seguridad informática específica que es muy utilizada sobre todo en entornos empresariales y servidores. Esta guía permite el uso de herramientas y protocolos que a su vez miden los niveles de seguridad en un sistema informático. Por lo general estas herramientas basadas en estos protocolos emiten un informe detallado de cada una de las reglas fallidas en un sistema operativo, así como también de las reglas de seguridad que sí se cumplen [10]. Esta es una manera relativamente sencilla de saber lo vulnerable que puede llegar a ser un sistema operativo, así como también las soluciones que pueden existir para tener un entorno mucho más fortalecido y seguro.

Para el escaneo de un sistema informático que se basa en la guía CIS, existen varias herramientas entre las que destacan:

- **CIS Configuration Assessment Tool (CIS-CAT):** Esta es una herramienta elaborada por CIS, permite la elaboración de informes de seguridad basados en la guía CIS; además tiene potencial de resolución de posibles vulnerabilidades que en el escaneo encuentre [11].
- **SCAP Workbench:** Esta herramienta al ser de código abierto permite realizar el escaneo de un sistema informático basado en bibliotecas SCAP. En base a esto, también suele ser configurado para que el escaneo que realice este basado en la guía CIS [12].
- **OpenSCAP:** Son un conjunto de herramientas o aplicaciones basadas tanto en SCAP como en CIS *Benchmarks*, realizan una comprobación y auditoría de sistemas informáticos para medir el nivel de seguridad [13].

OpenSCAP por su flexibilidad en librerías además de compatibilidad con muchos sistemas informáticos es elegida entre varias herramientas. OpenSCAP, gracias a su línea de comandos (*oscap*), permite el escaneo automático en la misma línea de comandos del sistema. Este escaneo también se guarda en un informe base, que posterior puede ser usado para visualizar a mayor detalle cada una

de las reglas de CIS que, en el sistema operativo fueron aprobadas o fallaron y representan una vulnerabilidad en el sistema.

OpenSCAP tiene la capacidad de implementar perfiles de seguridad específicos que estén basados en marcos de referencia independientes. Es gracias a esta flexibilidad que esta herramienta es una de las más usadas dentro del contexto de escaneo de sistemas informáticos [14].

## 2 METODOLOGÍA

El presente trabajo de integración curricular tiene el objetivo de verificar e identificar las vulnerabilidades en un sistema operativo CentOS 8 con un servidor de correo electrónico *Postfix* sin políticas de seguridad.

El primer objetivo consta de la instalación del sistema operativo CentOS 8 en donde se levantó un servidor de correo *Postfix* sin tomar en cuenta ninguna política de seguridad. Mediante la herramienta de escaneo OpenSCAP se obtuvo un primer reporte de vulnerabilidades.

En el presente trabajo se tenía dos opciones como servidor, *Postfix* y *Zimbra*, pero al final se eligió el servidor *Postfix* debido a que ofrece un servicio bastante seguro además de que es un servidor de código abierto lo que permite una gran variedad de configuraciones y gestiones que facilitan el uso, según se convenga.

Sobre el servidor de correo *Postfix* instalado se procedió a implementar recomendaciones de seguridad en base a los lineamientos del marco de referencia CIS. Se obtuvo un segundo reporte de vulnerabilidades con la herramienta de escaneo.

A continuación, se analizaron los reportes generados, resultado de la aplicación de la herramienta de escaneo OpenSCAP, se observaron cuales parámetros se han solventado según el marco de referencia CIS.

Por último, se verifico el *hardening* del sistema operativo CentOS 8 en base a las recomendaciones del marco de referencia CIS. Se analizó el reporte final, verificando el impacto que tienen las políticas implementadas sobre cada uno de los tres elementos del triángulo de seguridad informática: confiabilidad, integridad y disponibilidad. Además, se realizó una guía que resume las mejores prácticas para tener en cuenta en la implementación de un servidor endurecido.



### 3 RESULTADOS

El proceso de la implementación de *hardening* en el sistema operativo CentOS 8 inició con la instalación y configuración de dicho sistema operativo sin ningún tipo de políticas de seguridad; además de la instalación de un servidor de correo dentro de CentOS. Con el sistema operativo y el servidor funcionando de manera correcta, se instaló la herramienta de escaneo OpenSCAP, con el fin de identificar las vulnerabilidades o amenazas existentes, basado en el marco de regulación CIS.

Una vez generado el reporte con la herramienta, se procedió a identificar las vulnerabilidades, teniendo en cuenta las vulnerabilidades de mayor riesgo y colocándolas como prioridad; esto con el fin de solventarlas y así fortalecer el sistema operativo.

#### 3.1 Identificación de vulnerabilidades en un sistema operativo de servidor

El proceso de identificación de vulnerabilidades inició con la instalación y configuración del sistema operativo de servidor CentOS 8, cuyo *software* se instaló en un hipervisor tipo 2 llamado *VirtualBox*, cuyo sistema permite la virtualización de varios sistemas operativos. *VirtualBox* es uno de los entornos más utilizados y con mayor estabilidad en todo su sistema.

En la Figura 3.1 se puede observar el proceso de creación de la máquina virtual, en la opción *New* de la página principal de *VirtualBox*. En la imagen se puede observar el nombre de la máquina virtual, así como el tipo y la versión, en este caso *Linux* y *Red Hat* (64-bit), respectivamente.

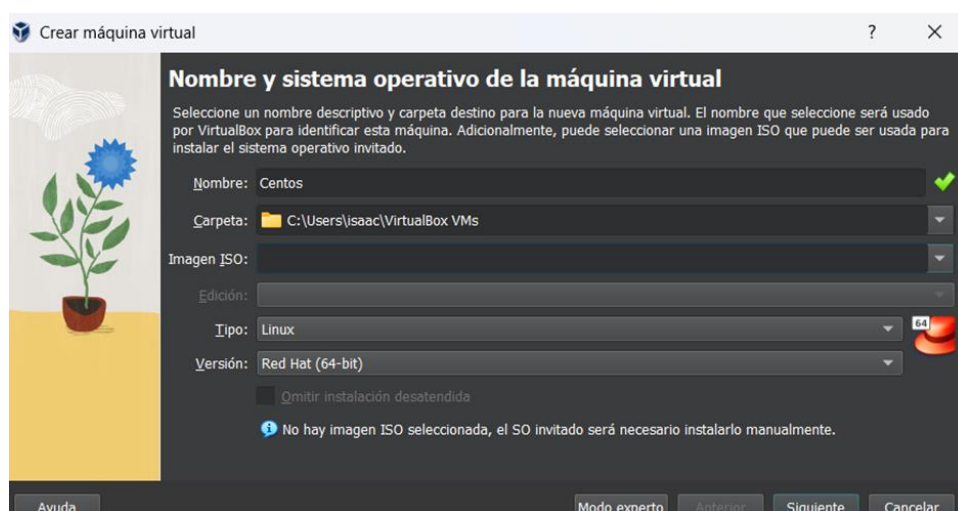
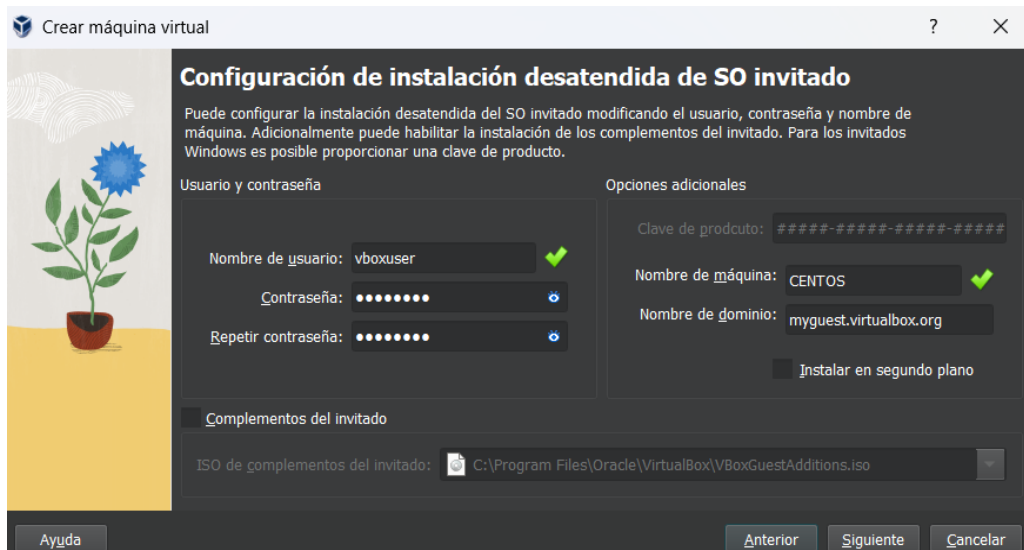


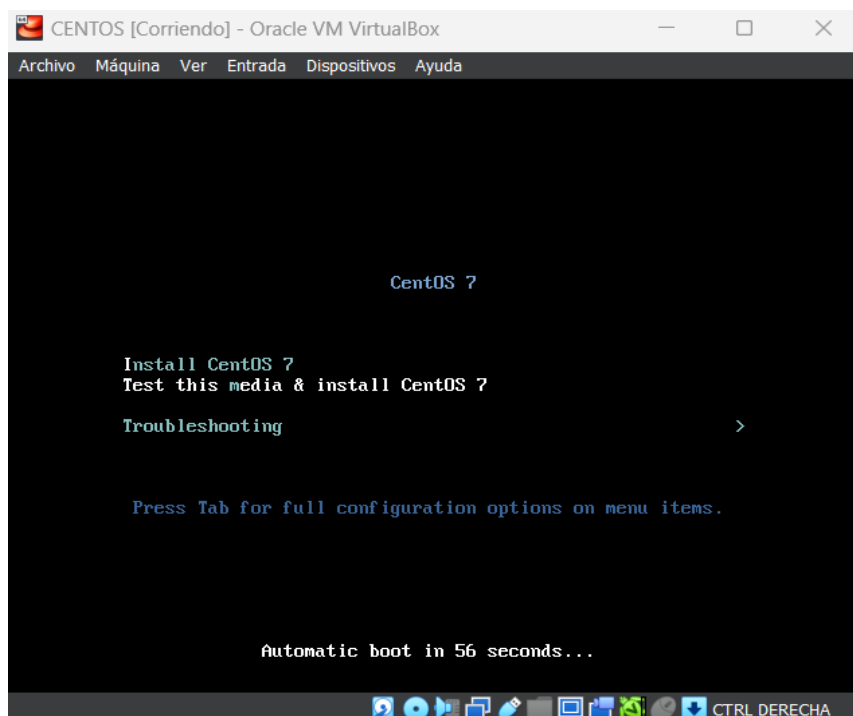
Figura 3.1 Creación de la máquina virtual CentOS 8

Se eligió el nombre de usuario, así como la contraseña del sistema operativo, en este caso, estos datos se los dejó por defecto, tal como se puede apreciar en la Figura 3.2.



**Figura 3.2** Configuración inicial del SO

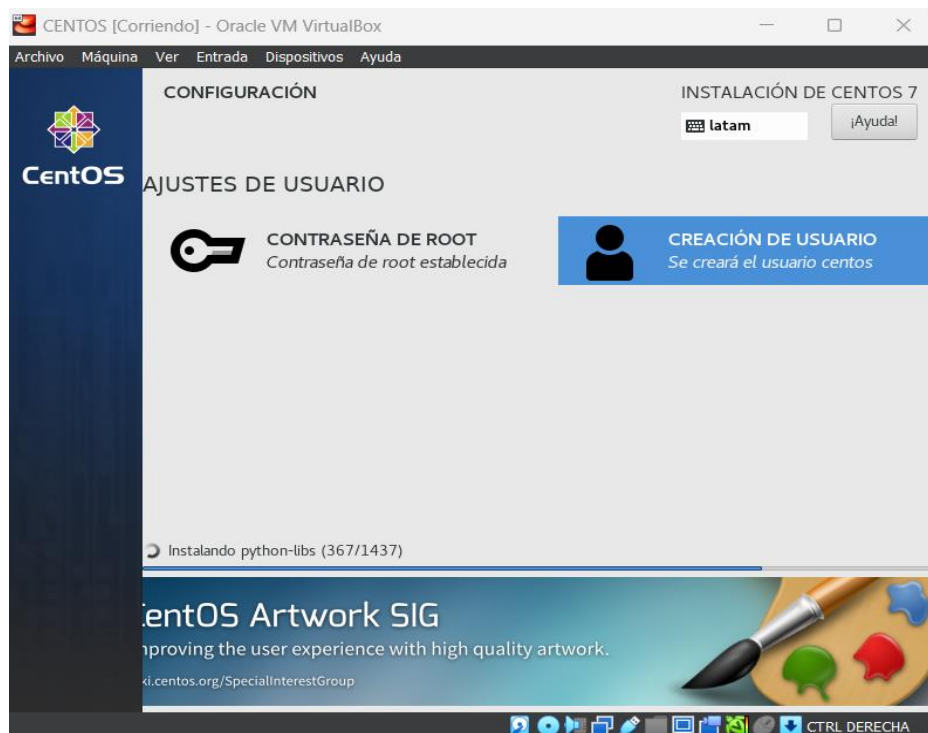
A continuación, después de haber ingresado la imagen ISO del sistema operativo, y como se puede observar en la Figura 3.3, CentOS 8 se abrió y mostró las opciones de instalación del sistema. En este caso se eligió la primera opción.



**Figura 3.3** Página inicial de instalación

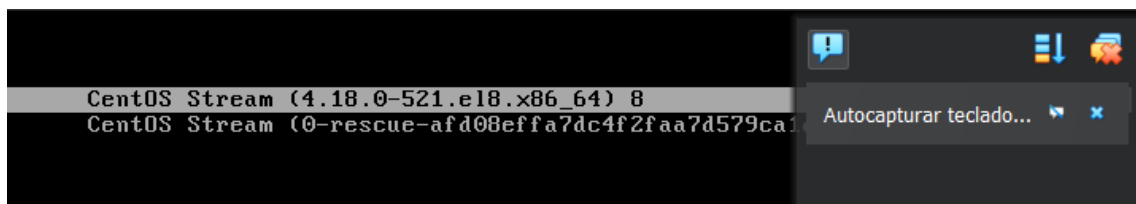
Después de unos minutos, el sistema operativo se abre en la página principal de instalación en donde se encuentran varias opciones. Se configuró tanto el usuario como la contraseña *ROOT* del sistema operativo tal y como se muestra en la Figura 3.4. Al

trabajar con un sistema operativo sin interfaz gráfica, la opción elegida fue: sistema operativo sin GUI.



**Figura 3.4** Instalación del SO

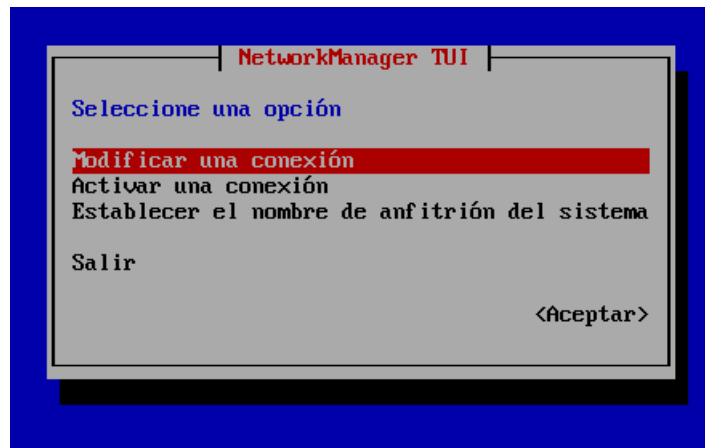
La instalación de un sistema operativo con interfaz gráfica conlleva muchos recursos y por ende mucho más tiempo de instalación. Al elegir el sistema operativo sin GUI, el proceso de instalación no conlleva más de 10 minutos. Una vez concluido este tiempo, el sistema operativo se reinició y empezó a funcionar, tal y como muestra la Figura 3.5.



**Figura 3.5** Reinicio del sistema

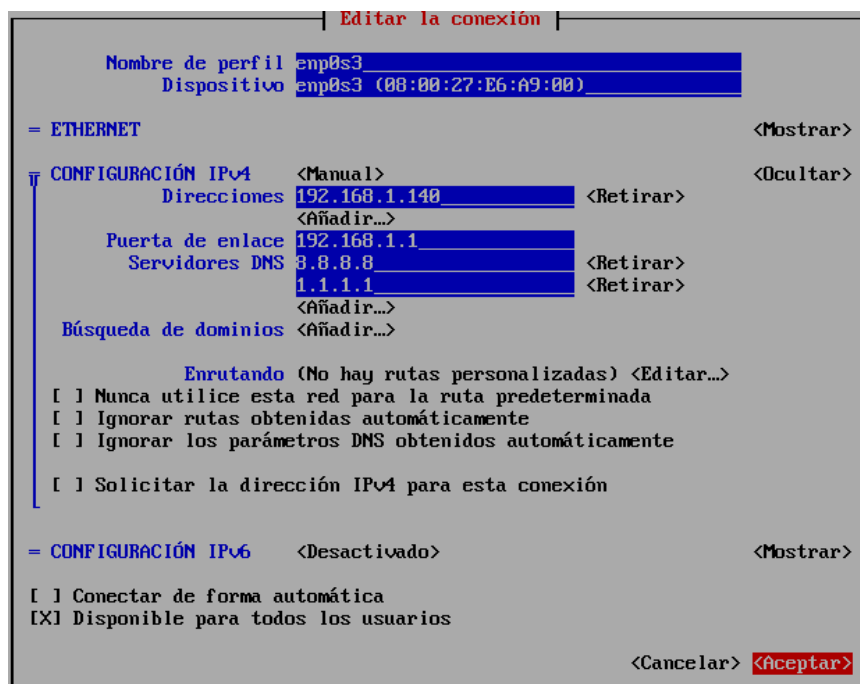
### **Instalación y configuración del servidor de correo**

Antes de realizar la configuración del servidor de correo, se ejecutaron ciertas configuraciones en opciones de red. Es así como, mediante el comando **nmtui** se accede a las configuraciones de red, tal y como se muestra en la Figura 3.6.



**Figura 3.6** Interfaz de configuración de red

Una vez dentro de la interfaz de red, se coloca una dirección estática, así como la puerta de enlace y los servidores DNS que permitieron la conexión a Internet, todo esto indicado en la Figura 3.7. El objetivo es realizar las descargas necesarias de todas las instancias del servidor de correo.



**Figura 3.7** Interfaz de configuración de red

Después de realizar la configuración estática de red, se ejecutaron todas las descargas necesarias, empezando por la instalación de *Postfix*, mediante el comando que se muestra en la Figura 3.8.

```
[root@localhost conf]# dnf install postfix
Última comprobación de caducidad de metadatos hecha hace 0:00:04, el sáb 11 nov 2023 12:17:32 EST.
Dependencias resueltas.
```

**Figura 3.8** Instalación de *Postfix*

Con el mismo comando se realizó la instalación de Telnet, como se muestra en la Figura 3.9, que es aceptado en la versión 8 de CentOS y que además sirvió para el envío y recepción de mensajes.

```
[root@localhost conf]# dnf install telnet
Última comprobación de caducidad de metadatos hecha hace 0:00:56, el sáb 11 nov 2023 12:17:32 EST.
Dependencias resueltas.
```

**Figura 3.9** Instalación de Telnet

Ya con todas las instancias requeridas para el servidor de correo, se ejecutó la configuración dentro de los ficheros; en primera instancia de *Postfix* con el comando **cd /etc/postfix** se establecen las configuraciones, en el fichero **nano main.cf**. Se habilitó la línea que muestra la Figura 3.10 y se añadió el dominio que se usó para la comunicación entre los usuarios del correo. En este caso el dominio usado fue **tesis.com**. Como se puede observar en la Figura 3.11 también se eliminó el signo que comentaba la línea que se puede observar, esto con el objetivo de que el dominio configurado este habilitado. Otra de las líneas configuradas dentro del fichero fue la línea de las interfaces, como se muestra en la Figura 3.12. En la Figura 3.13 se puede observar la configuración de la línea *Maildir*. Esta carpeta contendrá los correos que recibe el usuario.

```
#
mydomain = tesis.com
```

**Figura 3.10** Configuración del dominio

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

**Figura 3.11** Configuración de la línea de myorigin

```
#inet_interfaces = $myhostname, localhost
inet_interfaces = all
```

**Figura 3.12** Configuración de las interfaces

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

**Figura 3.13** Configuración de la línea *Maildir*

Realizada la configuración tanto en los ficheros de *Postifx* como de *Dovecot*, se realizaron algunas pruebas. Para esto se crearon dos usuarios: user1: abraham y user2: morocho, tal y como se muestra en la Figura 3.14.

```

[root@localhost postfix]# adduser abraham
[root@localhost postfix]# passwd abraham
Cambiando la contraseña del usuario abraham.
Nueva contraseña:
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 8 caracteres
Vuelva a escribir la nueva contraseña:
Las contraseñas no coinciden.
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: todos los tokens de autenticación se actualizaron exitosamente.
[root@localhost postfix]#

```

**Figura 3.14** Usuarios de correo creados

Con los usuarios creados se envió un mensaje de un usuario a otro para verificar que el servidor está en pleno funcionamiento y no exista error alguno. Se utilizó el comando **echo** para este fin, ver la Figura 3.15.

```

[root@mail ~]# su abraham
[abraham@mail root]$ echo "Prueba de servidor de correo al usuario morocho" | mail -s "IMPORTANTE" morocho@tesis.com
[abraham@mail root]$ exit
exit

```

**Figura 3.15** Envío de correo del usuario abraham al usuario morocho

Una vez realizado el envío del correo se comprobó que este haya llegado al usuario morocho. Como se muestra en la Figura 3.16, con el ingreso a la ruta del usuario morocho se puede observar la carpeta *Maildir* y dentro de este el archivo *new* donde se guardan los correos del usuario.

```

[root@mail ~]# cd /home/morocho
[root@mail morocho]# ls
Maildir
[root@mail morocho]# cd Maildir
[root@mail Maildir]# ls
cur          dovecot.list.index.log  dovecot-uidlist.lock  dovecot-uidvalidity  maildirfolder  tmp
dovecot.index.log  dovecot-uidlist        dovecot-uidlist.tmp  dovecot-uidvalidity.655ece05  new
[root@mail Maildir]# cd new
[root@mail new]# ls
1700924600.Ufd00130bd1ccM315152.mail
[root@mail new]#

```

**Figura 3.16** Correo guardado en el archivo *Maildir* del usuario morocho

Enseguida se comprobó mediante la herramienta Telnet, en la línea de comandos, el envío y recepción del mensaje. En la Figura 3.17 se observa el remitente y el destinatario, el título del mensaje y el cuerpo del mensaje.

```

[root@mail new]# telnet localhost pop3
Trying ::1...
Connected to localhost.
Escape character is '^I'.
+OK Dovecot ready.
user morocho
+OK
pass Nos3qponer*
+OK Logged in.
list
+OK 2 messages:
1 550
2 564
.
retr 2
+OK 564 octets
Return-Path: <abrahan@tesis.com>
X-Original-To: morocho@tesis.com
Delivered-To: morocho@tesis.com
Received: by mail.tesis.com (Postfix, from userid 1001)
        id 426B3DFAC7; Sat, 25 Nov 2023 10:04:40 -0500 (EST)
Date: Sat, 25 Nov 2023 10:04:40 -0500
To: morocho@tesis.com
Subject: IMPORTANTE
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: <20231125150440.426B3DFAC7@mail.tesis.com>
From: abrahan@tesis.com

Prueba de servidor de correo al usuario morocho
.

```

**Figura 3.17** Recepción de los mensajes en línea de comandos

Es importante recalcar que en la Figura 3.17 se está utilizando la herramienta Telnet para verificar que el servidor de correo funcione. No obstante, y bajo las recomendaciones del estándar CIS, no es recomendable usar esta herramienta por el hecho de que envía los datos entre máquinas sin cifrado alguno lo que lo convierte en un protocolo muy inseguro con brechas de seguridad importantes.

### **Instalación de la herramienta de escaneo OpenSCAP**

Una vez comprobado el funcionamiento del servidor de correo, se llevó a cabo la instalación de la herramienta de escaneo OpenSCAP, con el comando que se muestra en la Figura 3.18.

```

¡Listo!
[root@tesis ~]# sudo yum install openscap-scanner scap-security-guide

```

**Figura 3.18** Instalación de OpenSCAP

Después de la instalación, se configuraron versiones de respaldo en la ruta de OpenSCAP además de la descarga de las versiones más recientes, respectivamente, dentro de la ruta de OpenSCAP, como lo muestra la Figura 3.19. Esto con el objetivo de que la herramienta tenga todos los archivos actualizados y pueda realizar el escaneo de todo el sistema operativo.

```

root@tesis ~# sudo cp /usr/share/openscap/cpe/openscap-cpe-oval.xml /usr/share/openscap/cpe/openscap-cpe-oval.xml.dist
root@tesis ~# sudo cp /usr/share/openscap/cpe/openscap-cpe-dict.xml /usr/share/openscap/cpe/openscap-cpe-dict.xml.dist
root@tesis ~# sudo curl -L https://raw.githubusercontent.com/OpenSCAP/openscap/main/1.3/cpe/openscap-cpe-dict.xml -o /usr/share/openscap/cpe/openscap-cpe-dict.xml
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total      Spent    Left     Speed
100 3969  100 3969    0     0  9230      0 --:--:-- --:--:-- --:--:--   9230
root@tesis ~# sudo curl -L https://raw.githubusercontent.com/OpenSCAP/openscap/main/1.3/cpe/openscap-cpe-oval.xml -o /usr/share/openscap/cpe/openscap-cpe-oval.xml
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total      Spent    Left     Speed
100 101k  100 101k    0     0  115k      0 --:--:-- --:--:-- --:--:--  115k
root@tesis ~# _

```

**Figura 3.19** Configuración de archivos de respaldo de OpenSCAP

Con la herramienta configurada, se pudo enlistar todas las carpetas y ficheros existentes en el sistema operativo, como muestra la Figura 3.20.

```

Title: ANSSI-BP-028 (enhanced)
  Id: xccdf_org.ssgproject.content_profile_anssi_bp28_enhanced
Title: ANSSI-BP-028 (high)
  Id: xccdf_org.ssgproject.content_profile_anssi_bp28_high
Title: ANSSI-BP-028 (intermediary)
  Id: xccdf_org.ssgproject.content_profile_anssi_bp28_intermediary
Title: ANSSI-BP-028 (minimal)
  Id: xccdf_org.ssgproject.content_profile_anssi_bp28_minimal
Title: CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 - Server
  Id: xccdf_org.ssgproject.content_profile_cis
Title: CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 - Server
  Id: xccdf_org.ssgproject.content_profile_cis_server_11
Title: CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 - Workstation
  Id: xccdf_org.ssgproject.content_profile_cis_workstation_11
Title: CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 - Workstation
  Id: xccdf_org.ssgproject.content_profile_cis_workstation_12
Title: Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)
  Id: xccdf_org.ssgproject.content_profile_cui
Title: Australian Cyber Security Centre (ACSC) Essential Eight
  Id: xccdf_org.ssgproject.content_profile_e8
Title: Health Insurance Portability and Accountability Act (HIPAA)
  Id: xccdf_org.ssgproject.content_profile_hipaa
Title: Australian Cyber Security Centre (ACSC) ISM Official
  Id: xccdf_org.ssgproject.content_profile_ism_o
Title: Protection Profile for General Purpose Operating Systems
  Id: xccdf_org.ssgproject.content_profile_ospp
Title: PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 8
  Id: xccdf_org.ssgproject.content_profile_pci-dss
Title: DISA STIG for Red Hat Enterprise Linux 8
  Id: xccdf_org.ssgproject.content_profile_stig
Title: DISA STIG with GUI for Red Hat Enterprise Linux 8
  Id: xccdf_org.ssgproject.content_profile_stig_gui

```

**Figura 3.20** Lista de carpetas existentes para el escaneo

Con las listas creadas, se pudo realizar el escaneo con el ID: *xccdf\_org.ssgproject.content\_profile\_cis* el cual contiene las reglas según el marco de referencia CIS, esto se realizó mediante el comando **oscap infor /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml**. Los resultados se muestran en la Figura 3.21.



```

Rule      xccdf_org.ssgproject.content_rule_sshd_do_not_permit_user_env
Ident    CCE-80903-8
Result   fail

Title    Enable PAM
Rule     xccdf_org.ssgproject.content_rule_sshd_enable_pam
Ident    CCE-86721-8
Result   pass

Title    Enable SSH Warning Banner
Rule     xccdf_org.ssgproject.content_rule_sshd_enable_warning_banner_net
Ident    CCE-87978-3
Result   fail

Title    Limit Users' SSH Access
Rule     xccdf_org.ssgproject.content_rule_sshd_limit_user_access
Ident    CCE-82422-7
Result   fail

Title    Ensure SSH LoginGraceTime is configured
Rule     xccdf_org.ssgproject.content_rule_sshd_set_login_grace_time
Ident    CCE-86551-9
Result   fail

Title    Set SSH Daemon LogLevel to VERBOSE
Rule     xccdf_org.ssgproject.content_rule_sshd_set_loglevel_verbos
Ident    CCE-82420-1
Result   fail

Title    Set SSH authentication attempt limit
Rule     xccdf_org.ssgproject.content_rule_sshd_set_max_auth_tries
Ident    CCE-83500-9
Result   fail

Title    Set SSH MaxSessions limit
Rule     xccdf_org.ssgproject.content_rule_sshd_set_max_sessions
Ident    CCE-83357-4
Result   fail

Title    Ensure SSH MaxStartups is configured
Rule     xccdf_org.ssgproject.content_rule_sshd_set_maxstartups
Ident    CCE-90710-8
Result   fail

Title    Remove the X Windows Package Group
Rule     xccdf_org.ssgproject.content_rule_package_xorg-x11-server-common_removed
Ident    CCE-82757-6
Result   pass

[root@tesis ~]#

```

**Figura 3.21** Escaneo del sistema operativo de servidor

Una vez realizado el escaneo, el informe se guardó en el archivo report.html. En esta parte se pudo observar el archivo, el cual guarda todo el escaneo realizado, ver la Figura 3.22.

```

[root@mail new]# ls -al /tmp
total 73188
drwxrwxrwt. 10 root root 4096 nov 25 10:04 .
dr-xr-xr-x. 17 root root 224 nov 22 22:14 ..
-rw-r--r--. 1 root root 33977010 nov 24 21:05 arf.xml
-rw-r--r--. 1 root root 33977010 nov 24 21:06 arf.xml
drwxrwxrwt. 2 root root 6 nov 22 22:22 .font-unix
drwxrwxrwt. 2 root root 6 nov 22 22:22 .ICE-unix
-rwx-----. 1 root root 291 nov 22 22:19 ks-script-2zlnx9yz
-rwx-----. 1 root root 701 nov 22 22:19 ks-script-8Vblykr_
-rw-r--r--. 1 root root 6969947 nov 24 21:06 report.html
drwx-----. 3 root root 17 nov 25 10:03 systemd-private-8ae82f6ed485494e848e933409717678-chronyd.service-6U3KhP
drwx-----. 3 root root 17 nov 25 10:03 systemd-private-8ae82f6ed485494e848e933409717678-dovecot.service-psursC
drwx-----. 3 root root 17 nov 25 10:03 systemd-private-8ae82f6ed485494e848e933409717678-postfix.service-u0Klqi
drwxrwxrwt. 2 root root 6 nov 22 22:22 .test-unix
drwxrwxrwt. 2 root root 6 nov 22 22:22 .X11-unix
drwxrwxrwt. 2 root root 6 nov 22 22:22 .XIM-unix
[root@mail new]#

```

**Figura 3.22** Reporte guardado en los archivos de OpenSCAP en la ruta /tmp

Para observar el archivo report.html se utilizó una interfaz gráfica con el fin de visualizar, más detalladamente los posibles fallos en las reglas de seguridad. Se hizo uso de una máquina cliente CentOS 7 con GUI previamente configurada. El servidor responde a las solicitudes de red en la máquina cliente, como se observa en la Figura 3.23.

```
[root@localhost jaramillo]# ping 192.168.100.147
PING 192.168.100.147 (192.168.100.147) 56(84) bytes of data.
64 bytes from 192.168.100.147: icmp_seq=1 ttl=64 time=2.86 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=64 time=1.06 ms
64 bytes from 192.168.100.147: icmp_seq=3 ttl=64 time=0.955 ms
64 bytes from 192.168.100.147: icmp_seq=4 ttl=64 time=1.12 ms
64 bytes from 192.168.100.147: icmp_seq=5 ttl=64 time=2.51 ms
^C
--- 192.168.100.147 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.955/1.702/2.861/0.812 ms
[root@localhost jaramillo]#
```

**Figura 3.23** Ping exitoso de la máquina servidor a la máquina cliente

Es así que, mediante el comando mostrado en la Figura 3.24, se pudo transferir el archivo report.html, que contiene el informe de la herramienta OpenSCAP del escaneo de servidor CentOS 8, desde CentOS 8 hacia la máquina cliente CentOS 7 GUI. Se consideró la ruta donde estaba el informe en la máquina servidor y la ruta donde se deseaba guardar el informe en la máquina cliente.

```
[root@localhost jaramillo]# scp root@192.168.100.140:/var/www/html/report.html /var/www/html/
root@192.168.100.140's password:
report.html 100% 6822KB 15.6MB/s 00:00
```

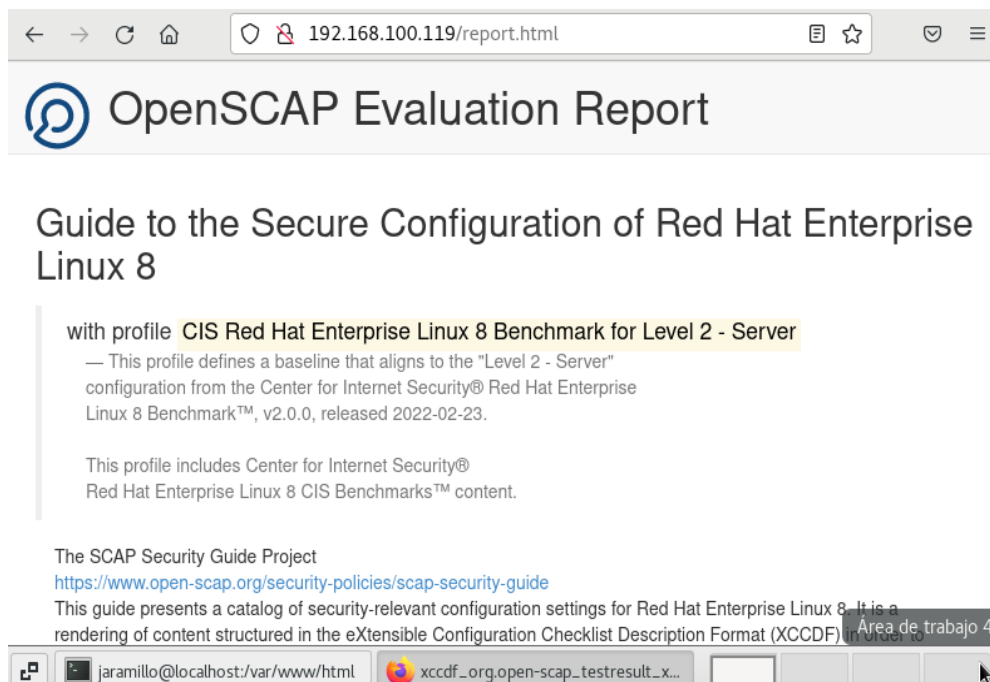
**Figura 3.24** Transferencia del archivo html

En la ruta del informe en donde se guardó el informe se habilita la página web, en este caso Python 2 con el puerto 8000, tal y como se muestra en la Figura 3.25.

```
[root@localhost jaramillo]# cd /var/www/html/
[root@localhost html]# ls
report.html
[root@localhost html]# python --version
Python 2.7.5
[root@localhost html]# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

**Figura 3.25** Habilitación de la página web

Con la dirección IP de la máquina cliente y la ruta del informe, como se muestra en la Figura 3.26, se pudo ingresar a la página web del reporte. En la Figura 3.27 se observan los datos del sistema operativo de servidor CentOS 8, escaneado.



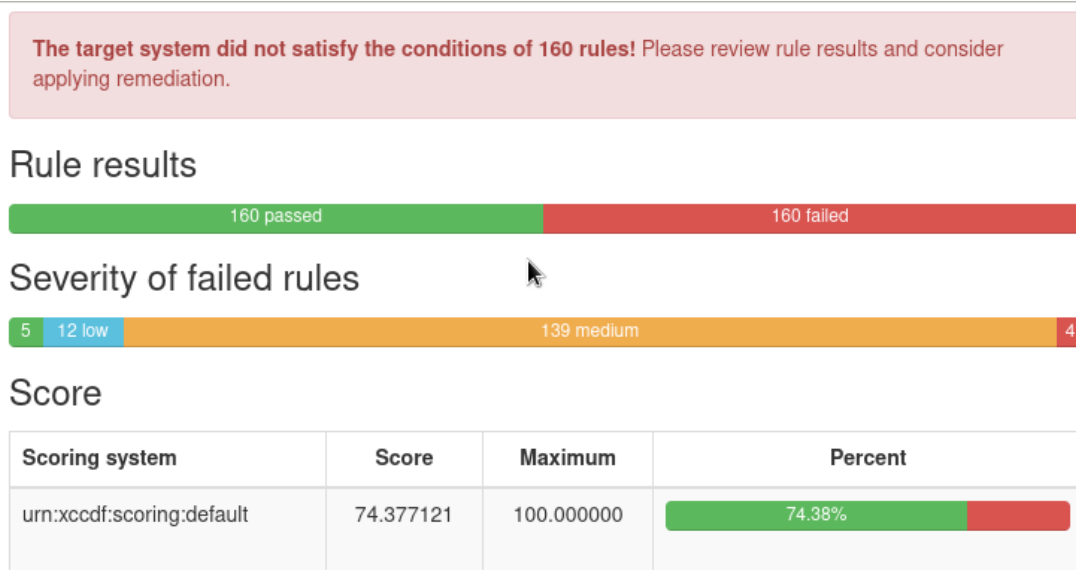
**Figura 3.26** Página Web del informe de OpenSCAP

Evaluation Characteristics	
Evaluation target	tesis
Benchmark URL	#scap_org.open-scap_comp_ssg-rhel8-xccdf.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEL-8
Benchmark version	0.1.69
Profile ID	xccdf_org.ssgproject.content_profile_cis
Started at	2023-11-11T16:44:11-05:00
Finished at	2023-11-11T16:44:47-05:00
Performed by	root
Test system	cpe:/a:redhat:openscap:1.3.8

**Figura 3.27** Datos del sistema operativo y ficheros escaneados

En la Figura 3.28 se pudo observar y analizar los errores que OpenSCAP encontró en el entorno de CentOS 8 con el servidor de correo. El porcentaje de cumplimiento de las políticas de seguridad, según el marco de seguridad CIS, es del 74,38%. El reporte encontró un total de 160 reglas que cumplen con este marco de seguridad. Se las puede visualizar con estado (*passed*), mientras que 160 se encuentran en un estado fallido, es decir que no cumplen con las políticas de seguridad. Estas reglas fallidas se encuentran clasificadas de acuerdo con un orden de riesgo: alto, medio y bajo; se tiene 4 errores de alta gravedad que tuvieron que resolverse a la brevedad y 156 errores de gravedad media y baja.

Cabe destacar que, 139 reglas de nivel medio representan el 86,87% de las reglas fallidas, además existen 12 reglas con nivel bajo y 5 reglas que pueden pasar desapercibidas.



**Figura 3.28** Resultado del primer reporte según OpenSCAP

En la Figura 3.29 se pueden observar las 4 reglas fallidas con nivel alto. Estas reglas se tomaron como prioridad de resolución ya que representan un riesgo de vulnerabilidad muy alto en el sistema operativo de servidor CentOS 8.

Group	Severity	Result
▼ severity = high		
Disable XDMCP in GDM	high	notapplicable
Make sure that the dconf databases are up-to-date with regards to respective keyfiles	high	notapplicable
Prevent Login to Accounts With Empty Password	high	fail
Set Boot Loader Password in grub2	high	fail
Set the UEFI Boot Loader Password	high	notapplicable
Uninstall telnet-server Package	high	fail
Disable SSH Access via Empty Passwords	high	fail

**Figura 3.29** Reglas fallidas de nivel alto

La Figura 3.30 muestra algunos de los errores de nivel medio que también tienen que resolverse, no con la prioridad de las anteriores reglas, pero sin duda deben ser puestas a resolución porque también representan un riesgo para el sistema operativo.

▼ severity = medium		
Install AIDE	medium	fail
Build and Test AIDE Database	medium	fail
Configure Periodic Execution of AIDE	medium	fail
Ensure /var/tmp Located On Separate Partition	medium	fail
Ensure Only Users Logged In To Real tty Can Execute Sudo - sudo use_pty	medium	fail
Require Re-Authentication When Using the sudo Command	medium	fail
Modify the System Login Banner	medium	fail
Modify the System Login Banner for Remote Connections	medium	fail
Limit Password Reuse: password-auth	medium	fail
Limit Password Reuse: system-auth	medium	fail
Lock Accounts After Failed Password Attempts	medium	fail

**Figura 3.30** Reglas fallidas de nivel medio

Así mismo, y como se observa en la Figura 3.31, las reglas de nivel bajo. Es recomendable solucionar la mayor cantidad de reglas fallidas para tener un entorno mejorado según las recomendaciones de CIS.

▶ severity = medium		
▼ severity = low		
Ensure /home Located On Separate Partition	low	fail
Ensure /tmp Located On Separate Partition	low	fail
Ensure /var Located On Separate Partition	low	fail
Ensure /var/log Located On Separate Partition	low	fail
Ensure /var/log/audit Located On Separate Partition	low	fail
Ensure Sudo Logfile Exists - sudo logfile	low	fail
Enable Auditing for Processes Which Start Prior to the Audit Daemon	low	fail
Extend Audit Backlog Limit for the Audit Daemon	low	fail
Disable Mounting of cramfs	low	fail
Disable Mounting of squashfs	low	fail

**Figura 3.31** Reglas fallidas de nivel bajo

Para realizar posteriormente un análisis, se realizó una copia de este primer reporte generado, esto con el objetivo de poder compararlo con el archivo que contiene las reglas fallidas solventadas. Como se muestra la Figura 3.32, en la máquina cliente se cambió el nombre del primer reporte report.html por el nombre old\_report.html.

```
[root@localhost jaramillo]# sudo mv /var/www/html/report.html /var/www/html/old_report.html
```

**Figura 3.32** Cambio de nombre de reporte en la máquina cliente

En la máquina servidor, con el comando mostrado en la Figura 3.33 se creó un nuevo archivo tipo xml en donde estará alojado el nuevo reporte con las reglas solventadas.

```
[root@mail ~]# sudo oscap xccdf eval --oval-results --profile cis --results-arf /tmp/arf.xml --report /tmp/report.html /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

**Figura 3.33** Comando para la creación del nuevo archivo xml

En la Figura 3.34 se puede observar la creación del nuevo archivo xml el cual tendrá alojado el nuevo reporte con las fallas solventadas. El nuevo archivo tiene el nombre arf.xml.

```
[root@mail ~]# ls -al /tmp
total 40016
drwxrwxrwt. 10 root root    4096 nov 24 18:45 .
dr-xr-xr-x. 17 root root     224 nov 22 22:14 ..
-rw-r--r--.  1 root root 33972378 nov 24 18:45 arf.xml
```

**Figura 3.34** Creación del archivo arf.xml

## 3.2 Implementación de políticas de seguridad en el sistema operativo

### Resolución de reglas fallidas de nivel alto

Para la resolución de las reglas fallidas encontradas por la herramienta OpenSCAP se hizo uso de las recomendaciones del estándar CIS. Esta guía proporciona pasos puntuales para gestionar y resolver las fallas de seguridad que pueden existir en un sistema informático dependiendo de la falla que se haya encontrado.

Después del escaneo, para poder aplicar políticas de seguridad y solucionar estas reglas fallidas, se inició nuevamente el sistema escaneado y se verificó antes que el servidor de correo funcione después del escaneo realizado. En la máquina cliente se verificaron las reglas fallidas de nivel alto. Con el escaneo se pudieron observar y analizar 4 reglas fallidas con nivel alto, ver Figura 3.29.

La primera regla de nivel alto solventado fue: *Disable SSH Access via Empty Passwords*.

Esta vulnerabilidad informática permite acceder a la configuración de *Secure Shell* (SSH) mediante contraseñas vacías o incluso sin contraseña. Esta vulnerabilidad según el marco de seguridad CIS es una de las reglas fallidas con mayor riesgo en sistemas informáticos. La resolución de esta amenaza se la realiza mediante su archivo de configuración, el objetivo es reducir significativamente la probabilidad de acceso no autorizado [15].

Para la resolución de esta regla fallida, en el servidor y mediante el comando mostrado en la Figura 3.35 se ingresó al archivo de configuración del programa SSH.

```
[root@mail ~]# nano /etc/ssh/sshd_config_
```

**Figura 3.35** Comando para ingresar al fichero de SSH

Una vez dentro del archivo de configuración se habilitó la línea denominada: *PermitEmptyPasswords* y se impide mediante la palabra “no” la autenticación con contraseñas vacías. Haciendo esto se obliga al protocolo SSH a no permitir el uso de contraseñas vacías o en blanco. Se reinició el servidor SSH para verificar los cambios, ver Figura 3.36.

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

**Figura 3.36** Configuración en el archivo del servidor SSH

Como muestra la Figura 3.37 se efectuó nuevamente el escaneo con los cambios hechos en el sistema operativo y se guarda en el archivo arf.xml previamente configurado. En este archivo se guardarán todas las actualizaciones que se hagan conforme se vayan solventando las vulnerabilidades.

```
[root@mail ~]# sudo oscap xccdf eval --oval-results --profile cis --results-arf /tmp/arf.xml --report /tmp/report.html /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

**Figura 3.37** Escaneo realizado con la primera vulnerabilidad resuelta

Después del escaneo realizado con la vulnerabilidad resuelta, se copió el reporte arf.xml hacia la máquina cliente. Es así como la Figura 3.38 muestra la primera vulnerabilidad solventada.

Disable SSH Access via Empty Passwords	
Rule ID	xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords
Result	pass
Multi-check rule	no
OVAL	oval:ssg-sshd_disable_empty_passwords:def:1

**Figura 3.38** Vulnerabilidad SSH solventada

La segunda vulnerabilidad de nivel alto fue: *Prevent Login to Accounts With Empty Password*. Esta vulnerabilidad encontrada en el sistema indica que existen una o varias cuentas de usuario que tienen contraseñas vacías. Esto implica un riesgo en la confidencialidad y autenticidad de los datos porque cualquier persona podría acceder a las cuentas sin la necesidad de una contraseña [16].

Para solventar este problema de seguridad se ingresó, mediante el comando mostrado en la Figura 3.39, al archivo de configuración de *Pluggable Authentication Modules* (PAM), el cual es una herramienta generalizada de autenticación en sistemas operativos basados en Unix.

```
[root@mail ~]# nano /etc/pam.d/system-auth_
```

**Figura 3.39** Comando para ingresar al archivo PAM

Una vez dentro del archivo de configuración se revisaron las líneas de cada una de las cuentas que existen en el sistema operativo y efectivamente se verificó que existían varias líneas que permiten el acceso con contraseñas vacías. Esto se pudo verificar debido a que en estas líneas estaba la palabra “*nullok*” la cual permitía esta falla de seguridad, ver Figura 3.40.

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authselect is run.
auth      required      pam_env.so
auth      sufficient    pam_unix.so try_first_pass nullok
auth      required      pam_deny.so

account   required      pam_unix.so

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

**Figura 3.40** Archivo PAM con las líneas con *nullok*

Es así que, se eliminó de las dos líneas la palabra “*nullok*” permitiendo así que estas cuentas de usuario ya no puedan tener las contraseñas vacías, como se observa en la Figura 3.41, solventando de esta manera el problema de seguridad.

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authselect is run.
auth      required      pam_env.so
auth      sufficient    pam_unix.so try_first_pass
auth      required      pam_deny.so

account   required      pam_unix.so

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

**Figura 3.41** Archivo PAM configurado

Se realizó nuevamente el escaneo para verificar los cambios en OpenSCAP. Se utilizó el mismo comando mostrado en la Figura 3.37.

Con el escaneo realizado y el reporte nuevamente copiado en la máquina cliente, se verificó el nuevo escaneo realizado por la herramienta OpenSCAP y se pudo validar que la regla fallida fue solventada con las configuraciones realizadas en el sistema operativo, ver la Figura 3.42.



Prevent Login to Accounts With Empty Password	
Rule ID	xccdf_org.ssgproject.content_rule_no_empty_passwords
Result	pass
Multi-check rule	no
OVAL Definition ID	oval:ssg-no_empty_passwords:def:1

**Figura 3.42** Vulnerabilidad de contraseñas PAM solventada

Después de realizar los dos primeros cambios en el sistema operativo CentOS 8, se validó que el servidor de correo todavía siga funcionando y que no exista ningún error en el envío y recepción de correo entre los dos usuarios creados con anterioridad. Como se observa en la Figura 3.43, el correo sigue funcionando sin alteración alguna.

```
Return-Path: <morocho@tesis.com>
X-Original-To: abraham@tesis.com
Delivered-To: abraham@tesis.com
Received: by mail.tesis.com (Postfix, from userid 1000)
        id 0D4E6DFACE; Tue, 28 Nov 2023 15:40:06 -0500 (EST)
Date: Tue, 28 Nov 2023 15:40:05 -0500
To: abraham@tesis.com
Subject: IMPORTANTE
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: <20231128204006.0D4E6DFACE@mail.tesis.com>
From: morocho@tesis.com

Prueba despues de la segunda vulnerabilidad critic
```

**Figura 3.43** Correo en funcionamiento después de la resolución de dos vulnerabilidades

A continuación, se verificó la siguiente regla fallida de nivel alto, ver Figura 3.44. Esta regla tiene el nombre: *Set Boot Loader Password in grub2. Grand Unified Bootloader 2*, es el sistema que permite el arranque del dispositivo en sistemas Linux como CentOS, iniciándolo en la memoria RAM. Este sistema puede tener ciertas vulnerabilidades entre las que destaca el hecho de que no tenga una contraseña fijada. Esta vulnerabilidad provoca que cualquier persona que ingrese de manera física al sistema operativo pueda realizar configuraciones que de una u otra forma comprometan la seguridad del mismo y de todos sus componentes lógicos [17].

Set Boot Loader Password in grub2	
Rule ID	xccdf_org.ssgproject.content_rule_grub2_password
Result	<b>fail</b>
Multi-check rule	no
OVAL Definition ID	oval:ssg-grub2_password:def:1
Time	2023-11-28T15:34:58-05:00
Severity	high

**Figura 3.44** Tercera regla de nivel alto fallida

Para solucionar esta regla fallida dentro del sistema operativo se colocó el comando mostrado en la Figura 3.45, en donde se dispuso una contraseña para impedir que cualquier persona ingrese en el menú grub2.

```
[root@mail ~]# sudo grub2-setpassword
Enter password:
Confirm password:
[root@mail ~]# _
```

**Figura 3.45** Comando para fijar contraseña en el menú grub2

Inmediatamente se reinició el sistema por completo, para que las configuraciones realizadas queden guardadas en el sistema. Esto se logró mediante el comando mostrado en la Figura 3.46.

```
[root@mail ~]# sudo reboot
```

**Figura 3.46** Comando para reiniciar el sistema

Con el comando mostrado en la Figura 3.37 se realizó nuevamente el escaneo del sistema operativo.

A continuación, se copió el reporte arf.xml del último escaneo hecho hacia la máquina cliente y como muestra la Figura 3.47 se comprobó que la vulnerabilidad se haya resuelto.

Set Boot Loader Password in grub2	
Rule ID	xccdf_org.ssgproject.content_rule_grub2_password
Result	<b>pass</b>
Multi-check rule	no
OVAL Definition ID	oval:ssg-grub2_password:def:1
Time	2023-11-28T16:03:44-05:00
Severity	high

**Figura 3.47** Tercera vulnerabilidad de alto nivel resuelta

En un principio, para resolver esta regla fallida se ingresó al archivo de configuración del sistema *grub2* en donde, y como muestra la Figura 3.48, se añadió lo siguiente: *grub\_pbkdf2.hash <hash>* a la línea de *kernel*. Esto basado en recomendaciones ubicadas en ciertos foros en donde resolvían este inconveniente de manera satisfactoria [18].

```
GRUB_CMDLINE_LINUX="crashkernel=auto resume=/dev/mapper/cs-swap rd.lvm.lv=cs/root rd.lvm.lv=cs/swap rhgb quiet grub_pbkdf2.hash=<hash>"
```

**Figura 3.48** Línea configurada dentro del archivo del sistema grub2

Una vez realizado este proceso y con el comando mostrado en la Figura 3.49 se añadió una contraseña.

```
[root@tesis ~]# sudo grub2-mkconfig -o /boot/grub2/grub.cfg
Generating grub configuration file ...
done
[root@tesis ~]# sudo grub2-setpassword
Enter password:
Confirm password:
[root@tesis ~]# _
```

**Figura 3.49** Ingreso de contraseña para grub2

Con este proceso ejecutado, se reinició el sistema, pero al momento de tratar de ingresar se generó el error mostrado en la Figura 3.50.

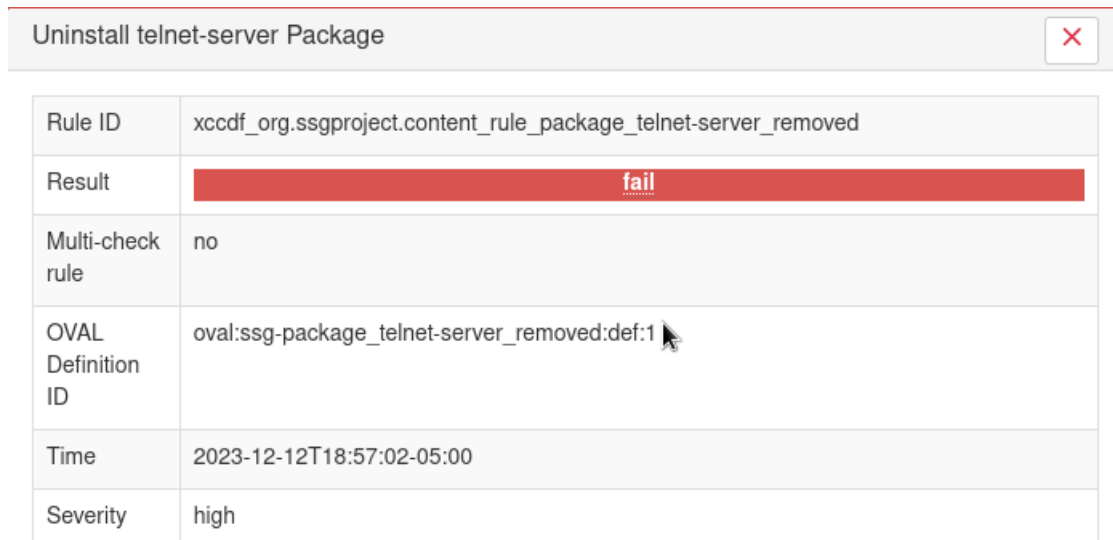
```
error: ../../grub-core/script/lexer.c:352:syntax error.
error: ../../grub-core/script/lexer.c:352:Incorrect command.
error: ../../grub-core/script/lexer.c:352:syntax error.
```

**Figura 3.50** Error por mala inclusión de contraseña en grub2

Se ingreso al menú de configuración *grub2* desde el arranque del sistema y se encontró la línea mencionada en la Figura 3.48. Aquí se borró lo que se configuró con anterioridad, de esta forma se pudo iniciar el sistema operativo ya sin el problema antes mencionado. Este error se debió al hecho de que se modificó el archivo de configuración

y no se siguieron los pasos mostrados en la herramienta de escaneo, en donde solo se tenía que ir al *set-password* y colocar una sola contraseña para cuando se quiera ingresar al menú de edición del *grub2*. Esto se visualiza en la Figura 3.49.

Como se mencionó con anterioridad, la última regla fallida mostrada en la Figura 3.51, correspondiente a Telnet, no se resolvió debido a que se necesita este protocolo para poder verificar el funcionamiento, de manera local, del servidor de correo.

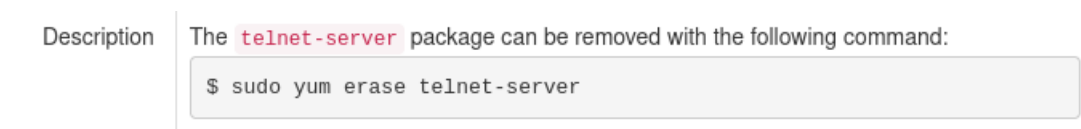


Uninstall telnet-server Package	
Rule ID	xccdf_org.ssgproject.content_rule_package_telnet-server_removed
Result	fail
Multi-check rule	no
OVAL Definition ID	oval:ssg-package_telnet-server_removed:def:1
Time	2023-12-12T18:57:02-05:00
Severity	high

**Figura 3.51** Cuarta regla fallida de nivel alto

La regla fallida es *Uninstall telnet-server Package*. El protocolo telnet es usado aún en conexiones remotas. Está basado en TCP/IP y fue creado en 1960. Es compatible con la mayoría de los sistemas operativos. El modo de funcionamiento de este protocolo es por medio de línea de comandos; se tiene una máquina cliente y una máquina destino. En la máquina destino se necesita tener habilitada una sesión con usuario y contraseña para, desde la máquina cliente, acceder remotamente. El problema principal de este protocolo radica en el hecho de que se envía el usuario y contraseña, para establecer la comunicación, en texto plano lo que facilita a los atacantes la intrusión a la conexión y por ende a todos los datos sensibles de la conexión.

La recomendación es desinstalar por completo el servidor de telnet para evitar ataques, ya que, aunque no se la use, el protocolo presente en el sistema informático representa una brecha de seguridad importante. Esto se observa en la Figura 3.52.



Description

```
The telnet-server package can be removed with the following command:  
$ sudo yum erase telnet-server
```

**Figura 3.52** Comando para desinstalar el servidor de telnet

## Resolución de reglas fallidas de nivel medio

La primera vulnerabilidad de nivel medio resuelto fue: *Set Password Maximum Age*. Esta vulnerabilidad tiene que ver con la configuración del tiempo de antigüedad de las contraseñas del sistema operativo. Por lo general este parámetro no viene configurado, y se convierte en una ventana en donde los datos de todo el sistema están comprometidos y expuestos. Si no se configura este parámetro, existe el riesgo de un ataque de fuerza bruta [15].

Como se ve en la Figura 3.53, el parámetro de *PASS\_MAX\_DAYS* no tiene un valor configurado lo que lo convierte en un riesgo de seguridad.



Set Password Maximum Age	
Rule ID	xccdf_org.ssgproject.content_rule_accounts_maximum_age_login_defs
Result	fail
Multi-check rule	no
OVAL Definition	oval:ssg-accounts_maximum_age_login_defs:def:1

**Figura 3.53** Primera regla de nivel medio detectada en el escaneo

Para la resolución de esta regla fallida, se ingresó mediante el comando mostrado en la Figura 3.54 al archivo de configuración de contraseñas.

```
[root@mail ~]# nano /etc/login.defs_
```

**Figura 3.54** Comando para ingresar al archivo de configuración de contraseñas

Una vez en el archivo, se ubica la línea *PASS\_MAX\_DAYS* y se colocó el número recomendado por el protocolo CIS: 365, ver Figura 3.55.

```
PASS_MAX_DAYS 365
PASS_MIN_DAYS 7_
```

**Figura 3.55** Configuración dentro del archivo login.defs

Después de la configuración se realizó nuevamente el escaneo, mediante el comando mostrado en la Figura 3.37. Con el escaneo realizado se vuelve a verificar el reporte y se observa en la Figura 3.56 que la vulnerabilidad fue resuelta sin ninguna novedad en la máquina servidor.

Set Password Maximum Age <span style="float: right;">✕</span>	
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	2023-11-28T16:03:37-05:00
Severity	medium

**Figura 3.56** Primera vulnerabilidad de nivel medio solventada

La siguiente vulnerabilidad de nivel medio va de la mano de la anterior regla fallida. El nombre de esta regla es: *Set Password Minimum Age*. Por lo general este parámetro también suele venir deshabilitado representando un riesgo medio de seguridad en el sistema. CIS recomienda colocar un valor mínimo de 7 a este parámetro, con el fin de evitar que cualquier persona cambie las contraseñas después de que el administrador lo haya hecho [15]. En la Figura 3.57 se puede observar la regla fallida.

Set Password Minimum Age <span style="float: right;">✕</span>	
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

**Figura 3.57** Segunda regla fallida

Para la resolución de esta regla se ingresó al archivo de configuración de contraseñas, como muestra la Figura 3.54. En el archivo de configuración se verificó la línea *PASS\_MIN\_DAYS* y se le colocó el número mínimo recomendado por CIS, ver Figura 3.55.

Con este proceso, se efectuó nuevamente el escaneo mediante el comando mostrado en la Figura 3.37. En la máquina cliente se actualizó el escaneo y como indica la Figura 3.58 se puede observar la regla fallida solventada.

Set Password Minimum Age	
Rule ID	xccdf_org.ssgproject.content_rule_accounts_minimum_age_login_defs
Result	<b>pass</b>
Multi-check rule	no
OVAL Definition ID	oval:ssg-accounts_minimum_age_login_defs:def:1
Time	2023-11-28T16:03:37-05:00
Severity	medium

**Figura 3.58** Segunda vulnerabilidad de nivel medio resuelta

Otra de las vulnerabilidades encontrada en el escaneo fue la ausencia de la herramienta AIDE en el sistema operativo. *Advanced Intrusion Detection Environment* es una herramienta propia de sistemas operativos Unix. La función principal de AIDE es el monitoreo y la detección de cualquier cambio no autorizado en todo el sistema (archivos, directorios, configuraciones, ficheros, etc.) lo que podría determinarse como una intrusión o un ataque de fuerza bruta lo que deriva en un fallo en la seguridad del sistema [19].

Para la resolución de esta regla fue suficiente realizar la instalación de todos los paquetes del programa AIDE con el comando **dnf install aide**, tal y como muestra la Figura 3.59.

```

Última comprobación de caducidad de metadatos hecha hace 3:14:50, el vie 24 nov 2023 17:39:13 EST.
Dependencias resueltas.
=====
Paquete                Arquitectura          Versión              Repositorio
=====
Instalando:
aide                   x86_64                0.16-14.e18_5.1    appstream

```

**Figura 3.59** Instalación de AIDE

Realizando y verificando nuevamente el escaneo se pudo validar que la regla fue corregida, como indica la Figura 3.60.

Install AIDE	
Rule ID	xccdf_org.ssgproject.content_rule_package_aide_installed
Result	<b>pass</b>
Multi-check rule	no
OVAL Definition ID	oval:ssg-package_aide_installed:def:1
Time	2023-11-28T16:03:36-05:00
Severity	medium

**Figura 3.60** Tercera regla solucionada

La herramienta de escaneo también encontró la vulnerabilidad, *Build and Test AIDE Database*. Esta regla fallida se trata de la configuración que se tiene que realizar a la herramienta AIDE para que pueda detectar archivos potencialmente comprometidos. Esta regla fallida se evidencia en la Figura 3.61.

Build and Test AIDE Database	
Rule ID	xccdf_org.ssgproject.content_rule_aide_build_database
Result	<b>fail</b>
Multi-check rule	no
OVAL Definition ID	oval:ssg-aide_build_database:def:1

**Figura 3.61** Cuarta regla de nivel medio fallida

AIDE utiliza una base de datos principal para que cuando haga un escaneo pueda compararlo con la primera base de datos y así detectar si existe algún cambio en algún componente lógico del sistema operativo que pueda representar un riesgo de seguridad. Como se muestra en la Figura 3.62, se realizó la base de datos inicial para que cuando la herramienta haga el escaneo al sistema pueda compararlo y verificar. Con el comando de la Figura 3.63 se almacenó la base de datos creada en el anterior paso.



```

[root@mail ~]# sudo aide --init
Start timestamp: 2023-11-24 20:54:54 -0500 (AIDE 0.16)
AIDE initialized database at /var/lib/aide/aide.db.new.gz

Number of entries:      39472

-----
The attributes of the (uncompressed) database(s):
-----

/var/lib/aide/aide.db.new.gz
MD5      : g+Zx0y+B/icXkbhRUGrbxg==
SHA1     : jLO+NPzYUE7yYD6J6QvpE1SbEMU=
RMD160  : wHBm2UX5pYnutTfw6lWgysg1iZI=
TIGER   : dFADZFWR1WB/3biiMhFA7wOtNHp2dRR7
SHA256  : uyyqM/NZj+UjbFaH8p?LXm6MpZ6jqSYJp
        jzCgr+luQEk=
SHA512  : kBjiPKC0SPq6eojlt9EYPQOM7hxas+sd
        Ustdy0r1VlceImz60I4UirdrAdicmws
        IwH1fUct2E7DoTf5SEphYA==

End timestamp: 2023-11-24 20:55:35 -0500 (run time: 0m 41s)

```

**Figura 3.62** Creación de la base de datos de AIDE

```

[root@mail ~]# sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

```

**Figura 3.63** Comando para guardar la base de datos creada

Como se observa en la Figura 3.64, después del escaneo realizado con OpenSCAP, la regla fallida se solucionó.

Build and Test AIDE Database <span style="float: right;">✖</span>	
Rule ID	xccdf_org.ssgproject.content_rule_aide_build_database
Result	<b>pass</b>
Multi-check rule	no
OVAL Definition ID	oval:ssg-aide_build_database:def:1
Time	2023-11-28T16:03:36-05:00
Severity	medium

**Figura 3.64** Cuarta regla solucionada.

Otras vulnerabilidades encontradas en el escaneo de OpenSCAP, ver Figura 3.65, es sobre la aceptación de anuncios en las interfaces IPv6. Por lo general, con el protocolo IPv6 los anuncios se envían desde los enrutadores con información, por ejemplo, sobre la configuración de red. En este sentido, OpenSCAP bajo las recomendaciones de CIS indica que se evite configurar el sistema para que no acepte anuncios. Esto puede representar una ventana de vulnerabilidad, ya que al exponer las interfaces de red se

expone todo el sistema a un ataque de fuerza bruta derivando, por ejemplo, en un envenenamiento de la tabla de rutas de red del sistema operativo en cuestión [15].

Configure Accepting Router Advertisements on All IPv6 Interfaces	
Rule ID	xccdf_org.ssgproject.content_rule_sysctl_net_ipv6_conf_all_accept_ra
Result	<b>fail</b>
Multi-check rule	no
OVAL Definition ID	oval:ssg-sysctl_net_ipv6_conf_all_accept_ra:def:1
Time	2023-11-28T16:03:47-05:00
Severity	medium

**Figura 3.65** Quinta regla fallida de nivel medio

Para abordar y solucionar esta regla fallida se procedió a deshabilitar los anuncios de IPv6 (*IPv6 Router Advertisement*), con el comando mostrado en la Figura 3.66.

```
[root@mail ~]# systemctl -w net.ipv6.conf.all.accept_ra=0
```

**Figura 3.66** Comando para deshabilitar los anuncios de IPv6

Con el anterior paso se deshabilitó solo temporalmente los anuncios de IPv6, no obstante, para deshabilitar de manera permanente los anuncios se ingresó con el comando mostrado en la Figura 3.67 al archivo de configuración de IPv6, en donde se agregó la línea mostrada en la Figura 3.68.

```
[root@mail ~]# nano /etc/sysctl.d
```

**Figura 3.67** Comando para ingresar al archivo de configuración de IPv6

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

**Figura 3.68** Línea ingresada en el archivo de configuración de IPv6

Con los cambios realizados y guardados se procedió a reiniciar el sistema *Kernel*, ver Figura 3.69.

```
[root@mail ~]# sudo systemctl -p
```

**Figura 3.69** Reinicio del comando de *kernel*

Mediante el comando de la Figura 3.37 se realizó nuevamente el escaneo del sistema operativo. De esta forma, en la máquina cliente se pudo verificar mediante el reporte realizado, que la vulnerabilidad después de estos cambios en la máquina servidor, se solucionó de manera satisfactoria, como la Figura 3.70 indica.

Configure Accepting Router Advertisements on All IPv6 Interfaces	
Rule ID	xccdf_org.ssgproject.content_rule_sysctl_net_ipv6_conf_all_accept_ra
Result	<b>pass</b>
Multi-check rule	no
OVAL Definition ID	oval:ssg-sysctl_net_ipv6_conf_all_accept_ra:def:1
Time	2023-12-05T18:24:57-05:00
Severity	medium

**Figura 3.70** Quinta regla fallida solucionada

La siguiente regla fallida de vulnerabilidad media, como se muestra en la Figura 3.71 es: “*Verify Permissions on cron.d*”. Los servicios “cron.d” se encuentran relacionados con tareas en específico dentro del sistema, tareas que pueden ser actualizaciones de archivos o programas del sistema operativo, copias de seguridad, entre otras [20]. La recomendación del marco de seguridad, indica que se debe asegurar que los permisos de los archivos de configuración sean restrictivos. Esto significa que solo el propietario del sistema operativo pueda acceder o pueda tener todos los permisos de los archivos del servicio “cron.d”. De esta manera se asegura en esta configuración y en esta regla fallida uno de los puntos esenciales de la seguridad de los sistemas informáticos, la integridad de los datos.

Verify Permissions on cron.d	
Rule ID	xccdf_org.ssgproject.content_rule_file_permissions_cron_d
Result	<b>fail</b>
Multi-check rule	no
OVAL Definition ID	oval:ssg-file_permissions_cron_d:def:1
Time	2023-11-28T16:03:56-05:00
Severity	medium

**Figura 3.71** Sexta regla fallida de nivel medio

Para la resolución de esta regla, se siguió la misma sugerencia de CIS, se habilitaron los permisos de este servicio mediante el comando mostrado en la Figura 3.72. El número 0700 brinda los permisos completos del servicio “cron.d” solo para el propietario del sistema operativo, asegurando de esta forma que nadie, a parte del propietario

pueda ingresar a los archivos del servicio y pueda modificarlos, brindando completa seguridad sobre este servicio.

```
[root@mail ~]# sudo chmod 0700 /etc/cron.d
```

**Figura 3.72** Comando para habilitar los permisos del servicio cron.d

Con la configuración realizada y la confirmación de que se habilitaron los permisos de este servicio, se realizó nuevamente el escaneo y se verificó en la máquina cliente que la vulnerabilidad haya sido solventada, ver Figura 3.73.

Verify Permissions on cron.d	
Rule ID	xccdf_org.ssgproject.content_rule_file_permissions_cron_d
Result	pass
Multi-check rule	no
OVAL Definition ID	oval:ssg-file_permissions_cron_d:def:1
Time	2023-12-05T18:25:08-05:00
Severity	medium

**Figura 3.73** Sexta vulnerabilidad solventada

La última vulnerabilidad solventada tiene que ver también con los servicios “cron.d”. Esta regla fallida es: *Ensure that /etc/cron.deny does not exist*, tal como se muestra en la Figura 3.74.

Como indica el manual *CIS CentOS Linux 8 Benchmark*; el archivo */etc/cron.deny* es parte de los archivos del servicio “cron.d”, sin embargo, este archivo permite a los usuarios que hagan uso del sistema operativo al ingresar a “cron.d” y por ende a la programación de tareas, lo que representa un riesgo completo de seguridad.

Ensure that /etc/cron.deny does not exist	
Rule ID	xccdf_org.ssgproject.content_rule_file_cron_deny_not_exist
Result	fail
Multi-check rule	no
OVAL Definition ID	oval:ssg-file_cron_deny_not_exist:def:1
Time	2023-11-28T16:03:56-05:00
Severity	medium

**Figura 3.74** Séptima regla fallida encontrada por OpenSCAP

Para solventar esta vulnerabilidad, en primer lugar, se cotejó que el archivo efectivamente se encuentre dentro de los archivos del servicio “cron.d”, ver Figura 3.75.

```
[root@mail ~]# ls /etc/cron.deny
/etc/cron.deny
[root@mail ~]#
```

**Figura 3.75** Verificación de archivo existente en el sistema operativo

Una vez que se haya constatado que el archivo sí hace parte de “cron.d” se procedió a eliminarlo con el comando mostrado en la Figura 3.76.

```
[root@mail ~]# sudo rm /etc/cron.deny
```

**Figura 3.76** Comando para eliminar el archivo en cuestión

Con este procedimiento ejecutado se realizó nuevamente el escaneo se demostró que en la máquina cliente ya no se refleje la regla fallida, esto se evidencia en la Figura 3.77.

Ensure that /etc/cron.deny does not exist	
Rule ID	xccdf_org.ssgproject.content_rule_file_cron_deny_not_exist
Result	<b>pass</b>
Multi-check rule	no
OVAL Definition ID	oval:ssg-file_cron_deny_not_exist:def:1
Time	2023-12-05T18:25:08-05:00
Severity	medium

**Figura 3.77** Séptima regla fallida de nivel medio solventada

### 3.3 Análisis y resultados del proceso de escaneo

Con todo el proceso realizado se pueden observar y analizar los resultados finales. En la Figura 3.78 se observan los resultados del primer reporte de la herramienta de escaneo. En la Figura 3.79 se confirma la resolución de 10 reglas con estándar CIS fallidas entre las que se encuentran 3 reglas fallidas de nivel alto y 7 reglas fallidas de nivel medio. Esto confirma el endurecimiento del sistema operativo bajo la normativa CIS.

#### Rule results



#### Severity of failed rules



**Figura 3.78** Primer reporte (old\_report)

## Rule results



## Severity of failed rules



**Figura 3.79** Reporte final (report)

Con el proceso de *hardening* realizado se puede verificar y confirmar todas las reglas fallidas que fueron solventadas. Estas reglas se resumen en la Tabla 3.1 que se presenta a continuación:

**Tabla 3.1** Reglas consideradas para el escaneo

	Regla fallida solventada	Regla fallida no solventada
<i>Disable SSH Access via Empty Passwords</i>	x	
<i>Prevent Login to Accounts With Empty Password</i>	x	
<i>Set Boot Loader Password in grub2</i>	x	
<i>Uninstall telnet-server Package</i>		x
<i>Set Password Maximum Age</i>	x	
<i>Set Password Minimum Age</i>	x	
<i>Advanced Intrusion Detection Environment</i>	x	
<i>Build and Test AIDE Database</i>	x	
<i>Configure Accepting Router Advertisements on All Ipv6 Interfaces</i>	x	
<i>Verify Permissions on cron.d</i>	x	
<i>Ensure that /etc/cron.deny does not exist</i>	x	

Con la resolución de las reglas fallidas encontradas por la herramienta OpenSCAP en el sistema operativo CentOS 8, y comprobado el cambio que hubo en el reporte final con respecto al reporte inicial, se verificó el funcionamiento del servidor *mail* instalado al principio. Una de las principales reglas fallidas encontradas por la herramienta fue el

servidor telnet, sin embargo, este servidor no pudo ser desinstalado porque con telnet se prueba que el servidor de correo funcione de manera local. Establecido este punto, se procedió a realizar la prueba localmente. Como muestra la Figura 3.80, se ingresó a uno de los usuarios creados y desde allí se envió el mensaje al otro usuario.

```
[root@mail ~]# su abraham
[abraham@mail root]# echo "Correo funcionando con las 10 vulnerabilidades resueltas" | mail -s "PRUEBA FINAL DE CORREO FUNCIONANDO" morocho@tesis.com
```

**Figura 3.80** Comando para el envío de correo de un usuario a otro

Una vez enviado el mensaje, se verificó en el usuario morocho la recepción del correo. Esto se realizó verificando en el archivo *Maildir*, configurado previamente en el servidor de correo, ver Figura 3.81.

```
[root@mail ~]# cd /home/morocho
[root@mail morocho]# ls
Maildir
[root@mail morocho]# cd Maildir
[root@mail Maildir]# ls
cur dovecot.index.log dovecot.list.index.log dovecot-uidlist dovecot-uidvalidity dovecot-uidvalidity.655ece05 maildirfolder new tmp
[root@mail Maildir]# cd new
[root@mail new]# ls
1701819301.Ufd00130bb38cM256545.mail
```

**Figura 3.81** Confirmación de correo recibido por el usuario morocho

Con la verificación lista y como se muestra en la Figura 3.82, se comprobó mediante el servicio de telnet, el destinatario del correo, así como el título, el cuerpo del correo, la fecha y la hora de envío.

```
[root@mail new]# telnet localhost pop3
Trying ::1...
Connected to localhost.
Escape character is '^]'.
+OK Dovecot ready.
user morocho
+OK
pass Nos3qponer*
+OK Logged in.
list
+OK 10 messages:
1 550
2 564
3 520
4 525
5 117341
6 256951
7 7297956
8 562
9 517
10 597
.
retr 10
+OK 597 octets
Return-Path: <abraham@tesis.com>
X-Original-To: morocho@tesis.com
Delivered-To: morocho@tesis.com
Received: by mail.tesis.com (Postfix, from userid 1001)
        id 31E61CC025: Tue, 5 Dec 2023 18:36:21 -0500 (EST)
Date: Tue, 05 Dec 2023 18:36:21 -0500
To: morocho@tesis.com
Subject: PRUEBA FINAL DE CORREO FUNCIONANDO
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: <20231205233621.31E61CC025@mail.tesis.com>
From: abraham@tesis.com

Correo funcionando con las 10 vulnerabilidades resueltas
.
```

**Figura 3.82** Uso de la herramienta telnet para la confirmación de los detalles del correo enviado

De esta manera, se comprobó que tanto el sistema operativo como el servidor de correo están funcionando de manera correcta después de los cambios y configuraciones realizadas en el sistema. Con ello se logró solventar las reglas fallidas encontradas en el escaneo de la herramienta OpenSCAP y así endurecer al sistema operativo de servidor.

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

Con las vulnerabilidades del sistema operativo encontradas, analizadas y resueltas mediante CIS y la herramienta OpenSCAP y validado que el servidor de correo siga funcionando de manera óptima, se ejecutó un análisis entre los dos reportes generados para verificar que la máquina servidor cumpla con las recomendaciones que emite el protocolo CIS en cuanto a la seguridad de sistemas informáticos.

En este sentido, se elaboraron dos tablas con las vulnerabilidades, que fueron resueltas en el proceso de *hardening*, y con las variables esenciales como son los tres pilares fundamentales de la seguridad (triada CIA) y dos parámetros que complementan el aspecto de seguridad de la información, esto se describe a continuación:

- Vulnerabilidad encontrada: Nombre de cada vulnerabilidad encontrada por la herramienta de escaneo.
- Perfil de nivel: CIS hace uso de puntos de perfil para ayudar a los usuarios en los análisis realizados al sistema informático referenciado el nivel de criticidad de las vulnerabilidades. Los perfiles de nivel son:  
Nivel 1: Son recomendaciones básicas y no implican un nivel elevado de configuraciones al sistema informático.  
Nivel 2: Son recomendaciones que se deben aplicar a la brevedad posible ya que las vulnerabilidades pueden afectar mucho al sistema informático. Las configuraciones realizadas pueden ser un poco complejas de aplicarlas y de validarlas.
- Severidad de la vulnerabilidad: El nivel de criticidad de cada una de las vulnerabilidades.
- Confidencialidad del sistema: Es uno de los pilares más importantes dentro de la ciberseguridad debido a la criticidad dentro del contexto. Se refiere a la protección de los datos y de la información que se transmite en la red. Básicamente se asegura que solo las personas que tienen la autorización puedan tener el acceso a la información generada. La recomendación de CIS en base a la confidencialidad hace uso del perfil de nivel 2, el cual recomienda la configuración para que los datos sean altamente confiables.



- **Integridad del sistema:** La integridad tiene el objetivo de que los datos o la información que se genera y se envía no sea alterada en el transcurso de su transmisión y llegue tal cual salió. Esto implica que la información no se altera en la transmisión del mensaje.
- **Disponibilidad del sistema:** Los datos que se envían mediante la red deben tener un respaldo para asegurarse que los datos puedan llegar al usuario. La disponibilidad de los datos se la puede asegurar mediante la implementación de sistemas duplicados en caso de fallos, la planificación de capacidades, balanceo de carga entre otros.
- **Autenticidad del sistema:** Se debe asegurar que el usuario que reciba los datos transmitidos sea el mismo al cual estaba destinado desde un principio. La autenticidad según el perfil de CIS se lo cataloga dentro del perfil de nivel 2.
- **No repudio:** Este pilar de la ciberseguridad es el último, pero no el menos importante. Trata de evitar que una entidad niegue acciones que previamente haya realizado en un sistema operativo. Este pilar se asegura con el uso de protocolos seguros, implementación de *firewalls*, segmentaciones de red, registro de eventos, etc.

En la Tabla 3.2 se puede visualizar las vulnerabilidades de nivel alto y su relación con cada uno de los pilares de la seguridad.

**Tabla 3.2** Análisis de vulnerabilidades de nivel alto

Vulnerabilidad	Perfil de nivel	Severidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	No repudio
<i>Disable SSH Access via Empty Passwords.</i>	2	Alta	x	x		x	
<i>Prevent Login to Accounts With Empty Password.</i>	2	Alta	x	x		x	
<i>Set Boot Loader Password in grub2.</i>	2	Alta	x	x	x	x	

En la Tabla 3.3 se visualizan todas las vulnerabilidades de nivel medio solventadas y su vínculo con los 5 pilares de la seguridad.

**Tabla 3.3** Análisis de vulnerabilidades de nivel medio

Vulnerabilidad	Perfil de nivel	Severidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	No repudio
<i>Set Password Maximum Age.</i>	1	Media	x	x		x	
<i>Set Password Minimun Age.</i>	1	Media	x	x		x	
<i>Install AIDE</i>	1	Media	x	x	x	x	
<i>Build and Test AIDE Database.</i>	2	Media		x			
<i>Configure Accepting Ruter Advertisements on All IPv6 Interfaces.</i>	2	Media		x			
<i>Verify Permissions on cron.d</i>	1	Media	x	x		x	x
<i>Ensure that /etc/cron.deny does not exist.</i>	1	Media	x	x			

Con los resultados presentados se concluye que las reglas fallidas solventadas bajo la normativa CIS cumplen con los parámetros de la triada CIA y en consecuencia se genera un sistema operativo y un servidor seguro.

### **Guía de buenas prácticas para reforzar la seguridad de un sistema operativo**

En el marco actual de la tecnología es importante reconocer el avance de la seguridad informática como de las amenazas que se adaptan a dichos avances tecnológicos. En este sentido es importante seguir y aplicar reglas y normas sujetas a un marco de referencia que permitan reducir al mínimo las amenazas y vulnerabilidades que un sistema informático puede presentar.

Es así que, a continuación, se presenta una guía de buenas prácticas que tienen el objetivo de garantizar la seguridad en un sistema:

- Considerar un análisis exhaustivo y detallado de cada uno de los elementos que conforman un sistema informático. Este análisis debe estar regido bajo normas

y estándares internacionales que permitan reducir las brechas de seguridad del sistema operativo.

- La planificación para realizar un análisis de un sistema informático es una buena práctica de seguridad ya que permite realizar el escaneo y análisis del sistema cada cierto tiempo impidiendo que las vulnerabilidades puedan replicarse a través del tiempo.
- Garantizar el acceso a la información solo a los entes que estén autorizados a hacerlo. Se tiene que realizar este proceso para prevenir accesos no autorizados protegiendo de esta manera la confidencialidad (pilar de la ciber seguridad) y minimizar al máximo los riesgos de seguridad.
- Es importante implementar en el sistema operativo las actualizaciones que estén vigentes con el fin de solventar riesgos propios del sistema y que representen una oportunidad para que los ciber atacantes pueden vulnerar la información que contenga el sistema.
- Es necesario garantizar la integridad de los datos mediante la verificación de información que viaja a través de la red. Mediante *checksums* se puede comprobar que la información que se recibe sea la misma información que fue enviada y no hubo alteración alguna mientras esta información viajaba por la red.
- Se debe asegurar la disponibilidad de toda la información. Para este fin es necesario la implementación de sistemas duplicados en caso de fallo. Es un proceso complejo de aplicar, pero necesario para garantizar la disponibilidad.
- El diseño de sistemas que funcionen en caso de fallos es importante para asegurar la disponibilidad del sistema informático.
- Es imperiosa la necesidad de auditorías internas del sistema operativo, con el fin de garantizar la integridad de los datos además del rastreo de acceso.
- El uso de contraseñas fuertes para carpetas o ficheros sensibles se hace necesario para impedir que personas tengan acceso a estos datos y puedan vulnerar el sistema operativo.
- Es necesario añadir capas extras de seguridad que sean complemento de las contraseñas del sistema y puedan ser otro factor de seguridad que permita afianzar las anteriores medidas de seguridad. En este contexto los *firewalls* se presentan como una opción para cumplir este objetivo.
- El uso y aplicación de algoritmos tipográficos garantizan la confidencialidad de los datos del sistema.
- Implementación de tácticas o enfoques de respaldo para una recuperación de datos rápida en caso de fallo de algún elemento del sistema operativo.

## Guía de buenas prácticas para reforzar la seguridad de servidor de correo

La instalación y configuración de un servidor regido a buenas prácticas de seguridad, es fundamental para reforzar y asegurar la seguridad de los datos. Para lo cual es importante seguir los siguientes lineamientos:

- Agregar e implementar políticas de seguridad que estén basados en marcos de referencia de ciber seguridad.
- Monitorear constante del funcionamiento del servidor de correo, con el fin de buscar y analizar patrones que puedan representar algún comportamiento sospechoso dentro del servidor.
- Es necesario realizar segmentación de red para impedir el acceso al servidor de correo a entes que no estén autorizados.
- Se tiene que implementar el principio de menor privilegio para impedir el acceso a información sensible del servidor.
- Establecer e implementar contraseñas que fortalezcan la seguridad de los elementos del servidor de correo. Estas contraseñas, según los marcos de referencia deben tener al menos 8 caracteres entre los que deben estar números, caracteres especiales y letras mayúsculas y minúsculas.
- Es primordial implementar buenas contraseñas para cada uno de los usuarios del servidor de correo.
- Limitar servicios que no se usen. Para este fin es recomendable realizar una instalación mínima del servidor para configurarlo de manera personalizada, de esta forma estarán accesibles solo los servicios necesarios.
- Restringir el acceso a puertos que no estén ligados a los servicios que brinda el servidor de correo.
- Implementar y configurar los servicios de *firewall* para filtrar información, restringir acceso y permitir solo las conexiones netamente necesarias para el funcionamiento del servidor.
- Configurar el filtro de *spam*, que permita la reducción de mensajes no deseados con el fin de prevenir y reducir amenazas.
- Mediante el uso de firmas digitales asegurar la integridad de la información de los correos.

## 4 CONCLUSIONES

- El presente proyecto demostró la importancia de implementar políticas de seguridad tanto en la instalación y configuración de un sistema operativo, así como en la configuración de un servidor de correo.
- Se demostró las afectaciones y vulnerabilidades que presenta el sistema operativo si no se aplica una correcta política de seguridad basada en un marco de referencia; así también las consecuencias de cada una de estas vulnerabilidades si no se solucionan.
- Tal como se evidenció, el uso de herramientas de escaneo es fundamental dentro del contexto de ciber seguridad ya que permite buscar, encontrar, evaluar, analizar y gestionar una por una las vulnerabilidades que se puedan presentar. De esta manera, se logró cumplir con las recomendaciones del marco de referencia de seguridad CIS.
- En el proceso de *hardening* se utilizó la herramienta de escaneo OpenSCAP, la cual permite implementar varios marcos de referencia entre ellos CIS, utilizado en el presente proyecto. Al ser de código abierto, ofrece al usuario la capacidad de generar reportes estandarizados, estos mejoran de gran manera el análisis y posterior configuración de cada una de las vulnerabilidades que pueda tener el sistema operativo.
- Con el análisis realizado se pudieron solventar las reglas fallidas de nivel alto que representaban una amenaza tanto al sistema operativo como al servidor de correo. Estas amenazas según el marco de referencia CIS están catalogadas como perfil 2 debido al peligro que representan para el sistema operativo y también debido a la dificultad que presenta la vulnerabilidad para solventarla.
- Así también, con el escaneo se resolvieron varias reglas fallidas de nivel medio que, a pesar de no tener un nivel alto de amenaza al sistema, sin duda tienen la capacidad de afectar elementos o variables del sistema o del servidor. No se debe dejar pasar por alto estas reglas fallidas ya que de una u otra forma todo el sistema está expuesto.
- Se constataron las mejoras de seguridad y el robustecimiento que tuvieron tanto el sistema operativo como el servidor de correo, después de realizar las configuraciones de las reglas fallidas. En primera instancia, el reporte se encontraba cerca el 74.38% y al implementar las políticas de seguridad este porcentaje se incrementó a 76.18%.

- El proceso de *hardening* se lo llevó a cabo de manera manual, es decir, se fueron solventando las vulnerabilidades una por una. Esto tiene sus ventajas y desventajas. La desventaja más sobresaliente es el hecho de que si se tienen muchas vulnerabilidades va a tomar mucho tiempo resolverlas, no obstante, al ir resolviendo una por una las vulnerabilidades se puede tener constancia de que se solventaron. En este sentido, se resolvieron todas las vulnerabilidades de nivel alto, excepto la vulnerabilidad del servicio Telnet por cuestiones del servidor de correo, y las que se consideraron las más importantes dentro de las reglas de nivel medio.
- A raíz de los resultados presentados y de los análisis realizados al principio, durante y después del escaneo y resolución de vulnerabilidades, se concluye que es de suma importancia la concientización acerca de los peligros reales que existen en la actualidad, más aún con el avance de la tecnología que lo hace a pasos agigantados. Es importante conocer todas las herramientas que se usan para mitigar y reducir las brechas de peligro que son usuales en la instalación y configuración de sistemas operativos y servidores.
- Es importante también tener en cuenta los marcos de referencia de seguridad, así como las recomendaciones generadas por dichos marcos de seguridad para de esta forma asegurar que se cumplan los pilares de la seguridad en el sistema operativo de servidor.

## 5 RECOMENDACIONES

- En un sistema operativo sin GUI se puede aplicar un escaneo de herramientas de seguridad, sin embargo, al ser una línea de comandos el análisis se puede tornar complejo. Es recomendable el uso de otra máquina que contenga GUI y que sea compatible con el sistema operativo en el cual se está realizando el escaneo. De esta forma se puede transferir el reporte generado a la máquina con GUI para visualizarlo en un navegador y así tener un mayor campo de visualización del reporte mejorando la toma de decisiones con respecto a las vulnerabilidades y su respectiva solución.
- El realizar *hardening* manual representa un mayor tiempo de dedicación en este proceso; sin embargo, se puede y es recomendable realizar pruebas del correcto funcionamiento del servidor con cada regla fallida que se vaya solventando.
- Se recomienda realizar copias de seguridad del sistema operativo para que, en caso de fallas del sistema por las configuraciones que se realicen, se garantice

la resolución de las reglas fallidas y se pueda recuperar el sistema operativo, evitando que se pierdan los cambios previos realizados.

- Al momento de instalar un sistema operativo, se recomienda verificar si el sistema aún cuenta con soporte que permita actualizaciones constantes en el tema de seguridad tanto para el sistema en sí como para las aplicaciones. El sistema operativo usado en el presente proyecto es CentOS 8, en el cual todavía se aplican actualizaciones de seguridad a usuarios que tenían este sistema operativo antes del 31 de diciembre del 2021, esta rige por 4 años a partir de esta fecha.
- Es importante realizar un monitoreo constante de todo el sistema para verificar si existe algún comportamiento anormal que pueda representar riesgo de seguridad de sistema. Para este fin es recomendable aplicar auditorias de sistema para el registro de eventos.
- Se recomienda seguir al pie de la letra las recomendaciones que indican los marcos de referencia. No es recomendable seguir indicaciones de otros entes ya que se corre el riesgo de dañar o configurar de mala manera los elementos del servidor.
- Para el servidor de correo se sugiere el uso de una dirección IP estática ya que, entre otras cosas permite un mayor control sobre el acceso al servidor. También se puede gestionar el *firewall* de mejor manera con el fin de mejorar y robustecer la seguridad.
- Es importante establecer políticas claras sobre el manejo de la seguridad y privacidad de información dentro del envío y recepción de correos en el servidor.
- Todos los estándares de seguridad persiguen el mismo objetivo; robustecer un sistema informático. En este sentido, se recomienda el uso de los estándares de seguridad según el alcance y su aplicación.
- Uno de los puntos más sensibles, pero que representa una brecha de seguridad importante, es la capacitación sobre la importancia de la aplicación de políticas de seguridad en un sistema informático. Es recomendable educar a todos los actores que son partícipes de un sistema informático, sobre la influencia que puede tener una correcta aplicación de políticas de seguridad.

## 6 REFERENCIAS

- [1] F. S. S., «Redalyc,» 2009. [En línea]. Available: <https://www.redalyc.org/pdf/729/72917905006.pdf>. [Último acceso: 2023].
- [2] J. D. & P. J., «Repositorio Institucion Universitaria,» 2018. [En línea]. Available: <https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/434/JimenezBoteroDanielFelipe2018.pdf?sequence=1&isAllowed=y>. [Último acceso: 2023].
- [3] E. Varela, «REPOSITORIO RUA,» 12 11 2023. [En línea]. Available: <https://rua.ua.es/dspace/bitstream/10045/107860/1/146131169.pdf>. [Último acceso: 2023].
- [4] E. A. Chinchay Toribio, «Repositorio Universidad César Vallejo,» 2022. [En línea]. Available: [https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/108673/Chinchay\\_TEASD.pdf?sequence=1&isAllowed=y](https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/108673/Chinchay_TEASD.pdf?sequence=1&isAllowed=y). [Último acceso: 2024].
- [5] G. ESGGINVOVA, «GRUPO ESGGINVOVA,» 2018. [En línea]. Available: <https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/>. [Último acceso: 2023].
- [6] B. C. Center, «Basque Cybersecurity Center,» [En línea]. Available: <https://www.ciberseguridad.eus/ciberglosario/integridad>. [Último acceso: 2023].
- [7] UNIR, «UNIR,» 2021. [En línea]. Available: <https://www.unir.net/ingenieria/revista/disponibilidad-seguridad-informatica/>. [Último acceso: 2023].
- [8] J. J. J. S., «Implementacion de hardening en sistemas operativos de servidor: implementacion de hardening en un sistema operativo de servidor microsoft,» 2023. [En línea]. Available: <https://bibdigital.epn.edu.ec/handle/15000/24975>. [Último acceso: 2023].
- [9] ManageEngine, «¿Qué son los controles de CIS@?,» [En línea]. Available: <https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html>. [Último acceso: 2024].



- [10] L. Honores, «REPOSITORIO ESPOCH,» 2021. [En línea]. Available: <http://dspace.esepoch.edu.ec/bitstream/123456789/14702/1/20T01447.pdf>. [Último acceso: 2023].
- [11] R. S., «International Journal of Computer Trends and Technology,» 2022. [En línea]. Available: [https://www.researchgate.net/profile/Rajeshkumar-Sasidharan-2/publication/362219539\\_A\\_Case\\_Study\\_to\\_Implement\\_Windows\\_System\\_Hardening\\_using\\_CIS\\_Controls/links/62dc8d8382bb4729929ddee9/A-Case-Study-to-Implement-Windows-System-Hardening-using-CIS-Controls..](https://www.researchgate.net/profile/Rajeshkumar-Sasidharan-2/publication/362219539_A_Case_Study_to_Implement_Windows_System_Hardening_using_CIS_Controls/links/62dc8d8382bb4729929ddee9/A-Case-Study-to-Implement-Windows-System-Hardening-using-CIS-Controls..) [Último acceso: 2023].
- [12] M. S., «Information Innovative Technologies,» 2019. [En línea]. Available: <https://elibrary.ru/item.asp?id=38534577>. [Último acceso: 2023].
- [13] F. J., «Universidad Oberta de Catalunya,» 2019. [En línea]. Available: <https://openaccess.uoc.edu/bitstream/10609/107667/7/jfandinocTFM1219memoria.pdf>. [Último acceso: 2023].
- [14] O. S. Guide, « Guide to the Secure Configuration of Red Hat Enterprise Linux 8,» 23 02 2022. [En línea]. Available: <https://static.open-scap.org/ssg-guides/ssg-rhel8-guide-cis.html>.
- [15] C. L. 8. Benchmark, «CentOS Linux 8 Benchmark,» 2019. [En línea]. Available: <https://www.cisecurity.org/terms-and-conditions-table-of-contents>. [Último acceso: 2023].
- [16] Complimony, «Complimony,» 2023. [En línea]. Available: <https://complimony.com/catalogs/xccdf/items/24948>. [Último acceso: 2023].
- [17] M. O. & P. M. Hagl Jakob, «Scitepress,» 2021. [En línea]. Available: <https://www.scitepress.org/PublishedPapers/2021/103139/103139.pdf>. [Último acceso: 2023].
- [18] F. Project, «Fedora Project,» [En línea]. Available: <https://docs.fedoraproject.org/en-US/fedora-coreos/grub-password/>. [Último acceso: 2023].
- [19] R. Hat, «Red Hat,» Red Hat, 2023. [En línea]. Available: [https://access.redhat.com/documentation/es-es/red\\_hat\\_enterprise\\_linux/8/html/security\\_hardening/checking-integrity-with-aide\\_security-](https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/8/html/security_hardening/checking-integrity-with-aide_security-)

hardening#:~:text=Advanced%20Intrusion%20Detection%20Environment%20(%  
20AIDE,detectar%20intrusiones%20en%20el%20sistema.. [Último acceso:  
2023].

- [20] J. B. Dueñas, «alcanle libre,» 20 07 2016. [En línea]. Available:  
<https://blog.alcancelibre.org/staticpages/index.php/configuracion-uso-cron>.  
[Último acceso: 2023].

## 7 ANEXOS

### ANEXO I: Certificado de Originalidad

#### CERTIFICADO DE ORIGINALIDAD

Quito, D.M. 14 de febrero de 2024

De mi consideración:

Yo, GABRIELA KATHERINE CEVALLOS SALAZAR, en calidad de Directora del Trabajo de Integración Curricular titulado IMPLEMENTACIÓN DE HARDENING EN CENTOS CON CIS asociado al proyecto IMPLEMENTACIÓN DE HARDENING EN SISTEMAS OPERATIVOS DE SERVIDOR elaborado por el estudiante ABRAHAN DARIO JARAMILLO CALVACHE 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 12%.

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/:b/g/personal/gabriela\\_cevalloss\\_epn\\_edu\\_ec/ESL0uORe8HRPmUO7fKxe1o8Bfyo4AmP1OaiaQwhISKApvQ7e-zPkK2F](https://epnecuador-my.sharepoint.com/:b/g/personal/gabriela_cevalloss_epn_edu_ec/ESL0uORe8HRPmUO7fKxe1o8Bfyo4AmP1OaiaQwhISKApvQ7e-zPkK2F)

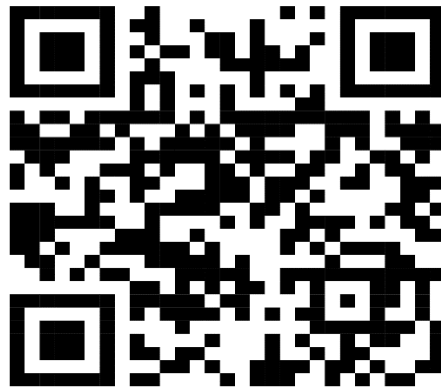
Atentamente,

GABRIELA KATHERINE CEVALLOS SALAZAR

Docente

Escuela de Formación de Tecnólogos

**ANEXO II: Reporte Inicial del Escaneo**



**ANEXIO III: Reporte Final del Escaneo**



**ANEXO IV: Enlace del Video**

