

ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

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

**IMPLEMENTACIÓN DE *HARDENING* EN SISTEMAS
OPERATIVOS DE SERVIDOR LINUX DE BASE DEBIAN**

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

VLADIMIR GIOVANNY YANQUI VELA

vladimir.yanqui@epn.edu.ec

DIRECTOR: GABRIELA KATHERINE CEVALLOS SALAZAR

gabriela.cevalloss@epn.edu.ec

DMQ, agosto 2023

CERTIFICACIONES

Yo, VLADIMIR GIOVANNY YANQUI VELA 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.

VLADIMIR GIOVANNY YANQUI VELA

vladimir.yanqui@epn.edu.ec

vladigio@hotmail.com

Certifico que el presente trabajo de integración curricular fue desarrollado por VLADIMIR GIOVANNY YANQUI VELA, bajo mi supervisión.

GABRIELA KATHERINE CEVALLOS SALAZAR

DIRECTOR

gabriela.cevalloss@epn.edu.ec

DECLARACIÓN DE AUTORÍA

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

VLADIMIR GIOVANNY YANQUI VELA

DEDICATORIA

Quiero dedicar este logro a mis pilares fundamentales, como primera instancia a mi padre Manuel Yanqui, mi madre Susana Vela y a mis hermanos Darío y Jessica, que gracias a su constancia y apoyo de forma incondicional supieron apoyarme y guiarme en todo momento para continuar mis estudios y lograr el objetivo de graduarme; como segunda instancia dedico este logro a mi esposa Miriam Tzetzta que, gracias a su apoyo, su paciencia y entendimiento durante todo este trayecto me supo brindar para no rendirme y seguir adelante. Y como no darles gracias a mis dos pequeños hijos Mayte y Sebastián que ellos fueron el reflejo y mi inspiración diaria para culminar con éxito la etapa universitaria.

Vladi

AGRADECIMIENTO

El agradecimiento eterno y de corazón a mi Dios quien, con su bendición, su gracia y llevado de su mano me supo guiar, colocar los conocimientos, criterios, pensamientos y palabras correctas en las aulas de la Escuela Politécnica Nacional. También al complemento de este logro que son mis padres y el complemento final es el agradecimiento eterno a mi querida esposa y mis hijos, que gracias a su paciencia, comprensión y apoyo fueron pieza clave para obtener este logro y nunca rendirme para continuar con mis estudios, finalmente agradecer a todos los docentes de la ESFOT de la Escuela Politécnica Nacional que brindaron su conocimiento y arte de educar durante mi carrera y en especial a mi tutora Ingeniera Gabriela Cevallos siendo pieza clave para el desarrollo de este proyecto, el agradecimiento al ingeniero Fernando Becerra por su calidad de docencia, al ingeniero Leandro Pazmiño por sus conocimientos impartidos y demás profesores.

Vladi

ÍNDICE DE CONTENIDOS

1.	DESCRIPCIÓN DEL COMPONENTE DESARROLLADO.....	1
1.1	Objetivo general	1
1.2	Objetivos específicos	1
□	Identificar las vulnerabilidades en un sistema operativo de servidor sin políticas de seguridad.	1
1.3	Alcance.....	1
1.4	Marco Teórico.....	2
	<i>Hardening</i>	2
	Triángulo de la CIA.....	2
	Sistema Operativo de Servidor	3
2.	METODOLOGÍA.....	7
3.	RESULTADOS	8
3.1	Identificación de las vulnerabilidades del sistema operativo de servidor sin políticas de seguridad	8
3.2	Implementación de una política de seguridad en un sistema operativo de servidor.....	28
	Instalación de un nuevo sistema operativo de servidor	29
	Agregación de políticas de seguridad mediante el marco de referencia CIS	29
	Servicio de correo <i>Postfix</i> mediante <i>Squirrelmail</i>	31
	Proceso de escaneo para generar un nuevo reporte	33
3.3	Análisis de los reportes, resultado de aplicación de la herramienta de escaneo	35
	Análisis del reporte generado sin políticas de seguridad	35
	Análisis del reporte generado con políticas de seguridad	37
	Parámetros que no se corrigieron de forma automática solventados manualmente	39
	Corrección de primera regla de forma manual	39
	Corrección de segunda regla de forma manual	40

3.4	Verificación del <i>hardening</i> del servidor con base a los elementos de la triada CIA	42
	Verificación de reglas de la triada CIA severidad alta	42
	Verificación de reglas de la triada CIA severidad media	44
	Verificación de reglas de la triada CIA severidad baja	45
	Guía de buenas prácticas para un sistema operativo de servidor endurecido.....	46
	Guía de buenas prácticas en servidor de correo endurecido	47
4.	CONCLUSIONES.....	48
5.	RECOMENDACIONES.....	50
6.	REFERENCIAS BIBLIOGRÁFICAS	52

RESUMEN

El presente trabajo de integración curricular radica su funcionamiento en implementar un proceso de *hardening* en sistemas operativos de servidor Linux de base Debian, mediante Ubuntu Server 20.04, con el objetivo de aplicar una política de seguridad en base al marco de referencia *CIS* y de esta forma asegurar el servidor, reducir significativamente las superficies de ataques, disminuyendo los puntos donde un atacante pueda infiltrarse.

El primer apartado consiste en la implementación de un servidor de correo *Postfix* mediante *Squirrelmail*. Se instala las herramientas de OpenSCAP para ejecutar un análisis de vulnerabilidades del servidor con el fin de obtener un primer reporte.

El segundo apartado corresponde a la agregación de políticas de seguridad de forma automática en base al marco de referencia CIS dentro del sistema operativo de servidor Ubuntu Server 20.04, luego de ser aplicada la política de seguridad se levanta el servidor de correo *Postfix* mediante *Squirrelmail*, se instalan todas las herramientas de OpenSCAP para escanear y obtener el segundo reporte de vulnerabilidades del sistema operativo de servidor.

El tercer apartado consiste en el análisis de los reportes emitidos, donde se observa que implantada la política se reducen las vulnerabilidades en el servidor, además se solventaron dos parámetros críticos de forma manual, con el fin de mejorar el endurecimiento del servidor, se obtienen un tercer reporte.

El cuarto apartado consiste en el análisis del tercer reporte, verificando el impacto que tienen las recomendaciones implementadas sobre cada uno de los elementos de la triada CIA.

Finalmente se obtienen las conclusiones y recomendaciones en base al desarrollo y análisis del presente proyecto.

PALABRAS CLAVE: *Hardening*, *Postfix*, *Squirrelmail*, OpenSCAP, CIS

ABSTRACT

The present project of curricular integration work consists of in to implement the hardening process in the Debian-based Linux server operating systems in Ubuntu server 20.04, with the objective to implement a security police in system on the CIS frame of reference and in this form secure server operating system, significantly to reduce the attack surfaces, decreasing the points where an attacker can infiltrate.

The first section consists in the implementation of a mail server Postfix while Squirrelmail. It's installed the OpenSCAP tools for the run server vulnerability analysis with the objective obtained the first report.

The second section consists of in to aggregate the security policies automatically based on the CIS frame of reference in the server operating system Ubuntu Server 20.04, after that the security policy is applied, the Postfix mail server is lifted while Squirrelmail, its installed all OpenSCAP tools for scanning and obtained the second operating system vulnerability report.

The third section consists in the analysis of emitted reports, where it's observed that implanted the policy to reduce the vulnerabilities in the server, also to resolve two parameters manually, with in the order to improve the server hardening and obtaining a report three.

The fourth section consists in the analysis of third report, verified the impact have implemented a security policy on each element to the CIA triad.

Finally, it's obtained the conclusion and recommendations in base to the development and analysis this present project.

KEYWORDS: *Hardening, Postfix, Squirrelmail, OpenSCAP, CIS*

1. DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

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

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

1.1 Objetivo general

Implementar *hardening* en sistemas operativos de servidor.

1.2 Objetivos específicos

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

1.3 Alcance

En primera instancia se investigarán herramientas de escaneo, 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 implementará una política de seguridad en el sistema operativo de servidor con el fin de obtener una mejora en el reporte de vulnerabilidades obtenido de la herramienta de escaneo, se procede a levantar un servidor de correo en

el sistema operativo endurecido. Se compararán los reportes para observar cuáles parámetros críticos se han solventado según el manual de buenas prácticas de seguridad emitido por organizaciones de estandarización en esta área.

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

1.4 Marco Teórico

Hardening

Un administrador puede llevar a cabo un conjunto de actividades dentro de un sistema operativo en lo que concierne distintos niveles de seguridad de sus equipos para aumentar al máximo dichos niveles.

El objetivo del *hardening* es aumentar la seguridad del sistema al implementar medidas que reduzcan las vulnerabilidades y las posibilidades de que se produzca una intrusión o compromiso [1]. Se establece como un proceso de seguridad que va a consistir en tomar medidas para fortalecer la protección de un sistema operativo o dispositivo.

Varios puntos en donde el atacante podría acceder o dañar diferentes tipos de sistemas operativos son, por ejemplo: *software* instalado, usuarios finales, interfaces de red entre otros huecos que se tornan innecesarios dentro del sistema [2].

Para ello es importante realizar un análisis de vulnerabilidades para identificar brechas de seguridad como subsistemas inactivos o puertos que pueden quedar abiertos [2].

Triángulo de la CIA

Dentro de los niveles de seguridad existen parámetros importantes como son disponibilidad, integridad y confidencialidad que se manejan de la mano y brindan protección a todos los datos que se van a manejar, teniendo en cuenta que presentan un alto grado de sensibilidad [3].

- **Confidencialidad:** Tiene como finalidad proteger contra el acceso y la divulgación no autorizados. La confidencialidad toma medidas de seguridad mediante la implementación de dichas medidas, como el cifrado de datos y autenticación de usuarios que presente el sistema operativo. Entre los ataques que vulneran a este pilar se puede mencionar: robo de contraseñas mediante técnicas comunes

como el *phishing*, interceptaciones de datos entre dos puntos y que acceden a la información personal, ataques forzados al intentar múltiples veces conseguir combinaciones correctas.

- **Integridad:** Se refiere a la propiedad de la información de ser protegida contra la modificación no autorizada o la eliminación. La integridad se logra mediante la implementación de controles de acceso y la autenticación de usuarios, así como la utilización de técnicas de verificación de datos en un sistema, como los algoritmos de *hash*. Como ataques se menciona a la inyección de código en donde se inserta códigos maliciosos en bases de datos o aplicaciones alterando los comportamientos y de esta forma manipular datos, modificación de datos en donde se cambian los datos transmitidos o almacenados alterando los contenidos y la información se verá comprometida.
- **Disponibilidad:** Se refiere a la propiedad de la información de estar disponible y accesible cuando se necesita. La disponibilidad se logra mediante la agregación de medidas o políticas de seguridad e implementación también, redundancia de *hardware* y la planificación del negocio de la continuidad. Como ataques se puede mencionar al ataque de denegación de servicios distribuidos (*DDoS*) que tiene un comportamiento similar al ataque de denegación de servicios (*DoS*) en donde se va a inundar el sistema con solicitudes maliciosas o con tráfico para que de esta forma los servicios no estén disponibles para los legítimos usuarios [3].

Sistema Operativo de Servidor

Existen diferentes sistemas operativos que están diseñados por medio del *hardware* y *software* permitir gestionar recursos, así como a múltiples programas proporcionar servicios de forma segura. Estos sistemas están enfocados en entornos empresariales y están optimizados para arquitecturas cliente-servidor. Son orientados a la red y pueden gestionar múltiples escritorios y reducir el tiempo de inactividad [4].

Existen diferentes tipos de sistemas operativos de servidor, los cuales incluyen una amplia gama de opciones con ventajas y desventajas particulares, los más comunes son: Linux, *Windows*, Unix, Debian, *Red Hat*, etc [5].

Sistema Operativo de base Debian

Utiliza la distribución Debian como base y se construye sobre ella para agregar o modificar componentes y características específicas. Debian es la distribución de

software libre y de libre acceso, debido a ello cualquier sistema operativo que se base en ella también [6].

Se menciona que los sistemas operativos basados en Debian suelen ser muy estables, seguros y escalables, lo que los hace muy utilizados en entornos empresariales y conocidos en el mercado. Algunos ejemplos de sistemas operativos basados en Debian incluyen Ubuntu Server, Ubuntu Desktop, Proxmox VE y Kali Linux. Estos sistemas operativos se utilizan comúnmente para levantar servidores de correo, servidores web, base de datos, servidores de archivos, entre otros [7].

Requisitos de *hardware* para Debían

Dependerá mucho de las necesidades de cada usuario final para la instalación y ejecución de Debian, como requisitos mínimos se enlista las siguientes opciones:

- Procesador: procesador de 1 (GHz).
- Memoria RAM: mínimo 512 (MB) de RAM, como recomendación al menos 2 (GB) de RAM para el desarrollo óptimo.
- Espacio de almacenamiento: De los paquetes básicos del sistema operativo de espacio libre en disco se necesita 10 (GB) para empezar el proceso de instalación de los paquetes del sistema operativo que son considerados básicos en el sistema.
- Tarjeta gráfica: se recomienda una tarjeta gráfica con al menos 128 (MB) de RAM de video para una mejor experiencia visual.
- Conexión a Internet estable durante el proceso de instalación para descargar e instalar paquetes adicionales y actualizaciones de seguridad [6].

Si se desea ejecutar tareas más complejas se recomienda tener recursos del computador más altos.

Se nombra a continuación las diferentes ventajas que presenta el sistema operativo basado en Debian:

- Conocido por su estabilidad y fiabilidad, Debian hace que los sistemas operativos basados en él sean estables y confiables.
- Suelen contar con características y herramientas de seguridad avanzadas.
- Son libres por lo que tienen acceso los usuarios al código fuente y podrían realizar modificaciones dependiendo las necesidades [8].

Se nombra a continuación las diferentes desventajas que presenta el sistema operativo basado en Debian:

- Tiene una amplia gama de *software* disponible en sus repositorios, existen algunas aplicaciones o programas que no están disponibles o que requieren una instalación adicional.
- Están diseñados para entornos empresariales y de servidor, por lo que pueden no ser tan amigables para los usuarios finales a diferencia de otros sistemas operativos que existen en la actualidad.
- Los sistemas operativos basados en él pueden requerir más configuración y personalización para adaptarse a las necesidades específicas del usuario o empresa [8].

Herramientas de escaneo de configuración y vulnerabilidades

Este tipo de herramientas están diseñadas para identificar y analizar posibles debilidades en la seguridad de los sistemas informáticos. Estas herramientas pueden detectar vulnerabilidades conocidas en el *software*, problemas de configuración y otros riesgos de seguridad que puedan existir en el sistema [9].

Se aplican en auditorías de seguridad en sistemas informáticos, con el fin de identificar posibles debilidades y riesgos. Por ejemplo, se puede escanear un servidor web en busca de vulnerabilidades, como la falta de parches de seguridad, configuraciones inseguras, contraseñas débiles, entre otros [9].

Herramientas de escaneo basadas en SCAP

Las herramientas basadas en SCAP (*Security Content Automation Protocol*) son aquellas que utilizan este protocolo para automatizar los sistemas informáticos por medio de la evaluación de niveles de seguridad en el sistema que se trabaje.

SCAP es un estándar de seguridad que permite la comunicación de información sobre vulnerabilidades, configuraciones de seguridad y evaluaciones de cumplimiento entre herramientas de seguridad diferentes. Las herramientas de escaneo de configuración y vulnerabilidades basadas en SCAP aprovechan este estándar para realizar evaluaciones de seguridad en sistemas informáticos de forma automatizada [10].

Existen diferentes herramientas de escaneo de configuración de vulnerabilidades basadas en SCAP que son:

OpenSCAP: herramienta de seguridad de código abierto o libre que utiliza SCAP en los procesos de evaluación de seguridad de los sistemas informáticos. Permite la evaluación de aplicaciones, dispositivos de red y sistemas operativos de servidor.

SCAP Workbench: herramienta de seguridad gratuita que utiliza SCAP para evaluar la seguridad de los sistemas informáticos. Permite la evaluación de sistemas operativos, aplicaciones y dispositivos de red.

Red Hat Satellite: es una herramienta de gestión de sistemas que utiliza SCAP para evaluar la seguridad de los sistemas informáticos. Permite la evaluación de sistemas operativos, aplicaciones y dispositivos de red.

IBM BigFix Compliance: herramienta que permite la gestión de seguridad que utiliza SCAP para evaluar los sistemas informáticos a nivel de seguridad. Permite la evaluación de sistemas operativos, aplicaciones y dispositivos de red [10].

Marcos de referencia de seguridad

Son metodologías, modelos o estándares utilizados para establecer una estructura que permita a las organizaciones gestionar la seguridad de sus sistemas de manera eficiente y efectiva. Estos marcos proporcionan un conjunto de prácticas y controles que se pueden aplicar para proteger la información y los sistemas contra posibles riesgos de seguridad. Algunos de los marcos de referencia de seguridad más populares son [11]:

- *NIST Cybersecurity Framework*: desarrollado por el *National Institute of Standards and Technology* (NIST), establece una estructura para la gestión de la ciberseguridad en organizaciones de cualquier tamaño y sector. El marco tiene como principales las siguientes funciones: identificar, proteger, detectar, responder y recuperar los datos o información que tiene el sistema.
- *ISO 27001*: en la actualidad es considerado el estándar internacional que permitirá para un Sistema de Gestión de Seguridad de la Información (SGSI) establecer los requerimientos y que cumple con una norma muy utilizada y conocida. El estándar especifica controles de seguridad por medio de un conjunto que las organizaciones pueden implementar para resguardar la integridad, confidencialidad y disponibilidad de la información de las entidades que así lo requieran.
- *CIS Controls*: desarrollado por el *Center for Internet Security* (CIS), este marco proporciona controles de seguridad prioritarios que se aplicarían para aumentar el nivel de seguridad. Existen tres niveles que son: básico, intermedio y avanzado los cuales cumplen un papel importante al momento implementar *hardening*.
- *PCI DSS*: el *Payment Card Industry Data Security Standard* (PCI DSS) denominado como un paquete de requisitos de seguridad que se aplican a las

organizaciones que manejan información de tarjetas de crédito. El estándar establece un conjunto de controles que las organizaciones están en la obligación de poner en práctica niveles de seguridad y prevenir el fraude en las entidades.

La elección de un marco de referencia dependerá de distintos factores que se van a adaptar a las necesidades de una organización en específico, esto dependerá del sistema que se va a proteger teniendo en cuenta que este proceso no es estático y único si no que se debe actualizar y revisar periódicamente la presencia de nuevas amenazas, cambios y regulaciones en la organización o sistema.

2. METODOLOGÍA

El presente proyecto de titulación se rige en una investigación tipo exploratoria, documental, aplicativa de *hardening* en sistemas operativos de servidor Linux de base Debian, mediante Ubuntu Server 20.04.

El primer objetivo consta de la instalación del sistema operativo de servidor Linux de base Debian Ubuntu Server 20.04 con un servidor de correo *Postfix* en *Squirrelmail* sin tomar en cuenta ninguna política de seguridad. Mediante la herramienta de escaneo *OpenScap* se obtuvo un primer reporte de vulnerabilidades.

Se procedió a aplicar en el sistema operativo de servidor Linux de base Debian Ubuntu Server 20.04 una política de seguridad, con base a los lineamientos del marco de referencia CIS. Luego con el sistema operativo endurecido se levantó el servicio de correo *Postfix* en *Squirrelmail*. Se obtiene el reporte de vulnerabilidades con la herramienta de escaneo *OpenScap*.

Se analizan y comparan los reportes obtenidos, se observan cuáles parámetros críticos se han solventado según el marco de referencia CIS. De forma manual se solventaron dos recomendaciones que no fueron implementadas, con el fin de obtener una mejora en el *hardening* del servidor. Se obtiene un nuevo reporte, denominado reporte final.

Se analizó el reporte final, verificando el impacto que tienen las políticas implementadas sobre los elementos del triángulo de seguridad informática: confiabilidad, integridad y disponibilidad. Además, se realizó una guía que resume las mejores prácticas a tener en cuenta para implementar un servidor endurecido.

3. RESULTADOS

El desarrollo del presente proyecto requiere de diferentes pasos para la implementación de *hardening* en un servidor de correo con sistema operativo de servidor Linux base Debian, Ubuntu Server. Se aplicó políticas de seguridad en base al marco de referencia CIS que permitió robustecer el servidor, y mediante la aplicación de la herramienta de escaneo OpenSCAP se obtuvo el reporte de vulnerabilidades para el análisis respectivo.

3.1 Identificación de las vulnerabilidades del sistema operativo de servidor sin políticas de seguridad

Para la identificación de vulnerabilidades en el sistema operativo de servidor Ubuntu Server previamente se debe realizar la instalación de una máquina virtual en el *software* de virtualización *VMware Workstation Pro 16.1.2*. Ahí se creó la máquina virtual de servidor Ubuntu Server 20.04 el cual tiene el servidor de correo *Postfix* en *Squirrelmail*.

La instalación de la máquina virtual conlleva un proceso de diferentes pasos importantes los cuales se detallan a continuación:

Creación de la máquina virtual en el *software* de virtualización *VMware Workstation Pro 16.1.2*. dando *click* en *Create a New Virtual Machine*, observar la Figura 3.1.

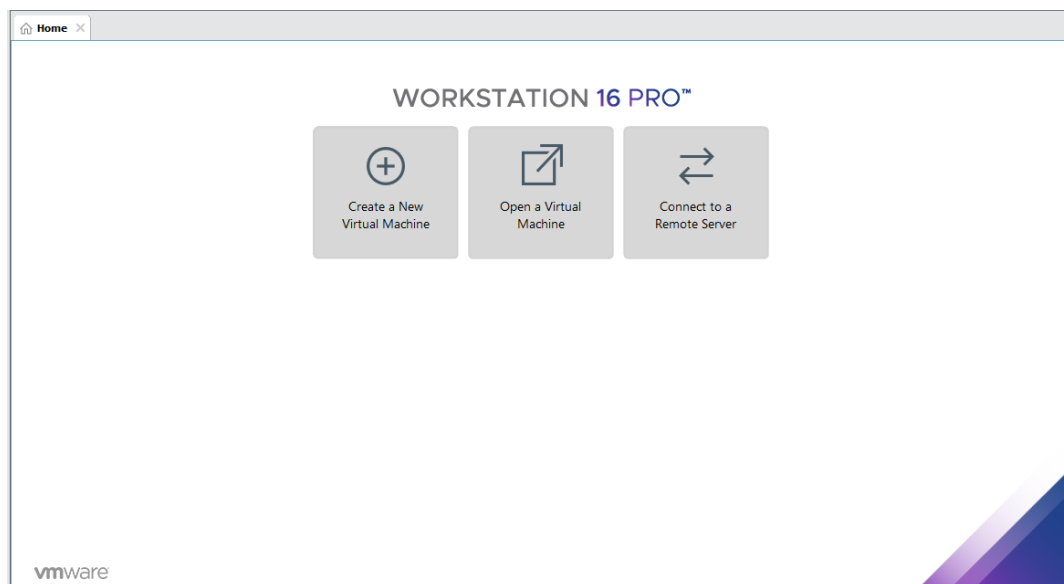


Figura 3.1 Creación de una nueva máquina virtual

Se selecciona el sistema operativo que se desea instalar y en este caso se elige el sistema operativo Linux de base Debian Ubuntu 64-bit, observar la Figura 3.2.

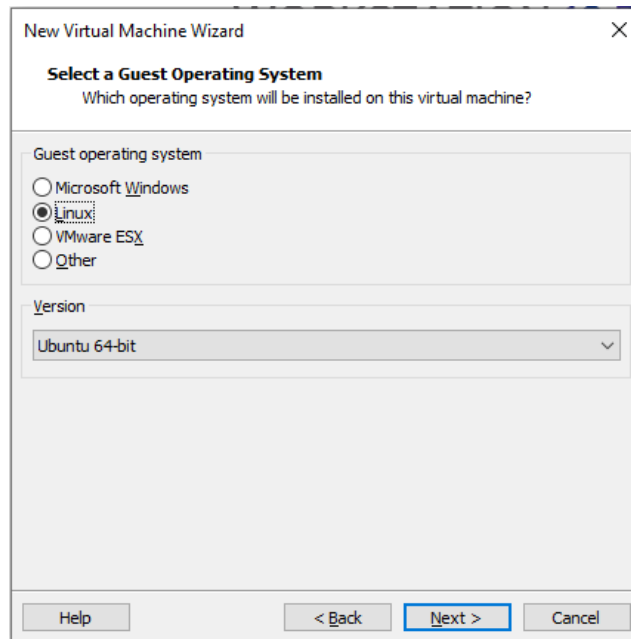


Figura 3.2 Selección del sistema operativo Linux Ubuntu 64-bit

Se elige la especificación del tamaño del disco duro de la máquina virtual el cual se escoge el valor de 20 (GB) que es un valor recomendado para el sistema operativo Ubuntu 64-bit, seleccionando almacenar el disco virtual como un único archivo, como se visualiza en la Figura 3.3.

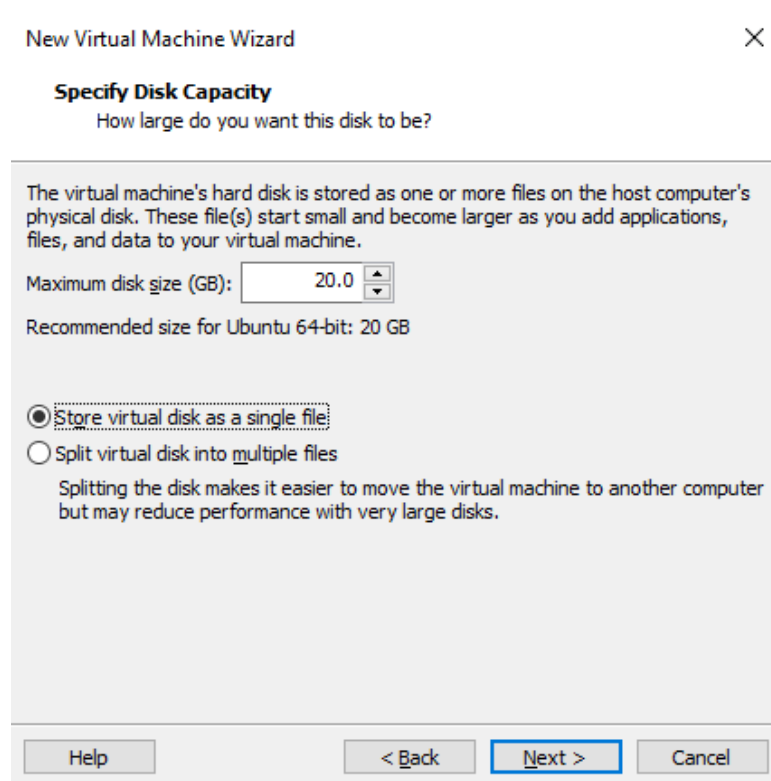


Figura 3.3 Se especifica el tamaño del disco de la máquina virtual

Se especifica en la máquina virtual la cantidad de memoria que se va a asignar, en este caso se asigna el valor de 2 (GB) de tamaño de memoria RAM siendo este valor el recomendado para poder implementar los requerimientos y se observa en la Figura 3.4 Tamaño memoria RAM de máquina virtual

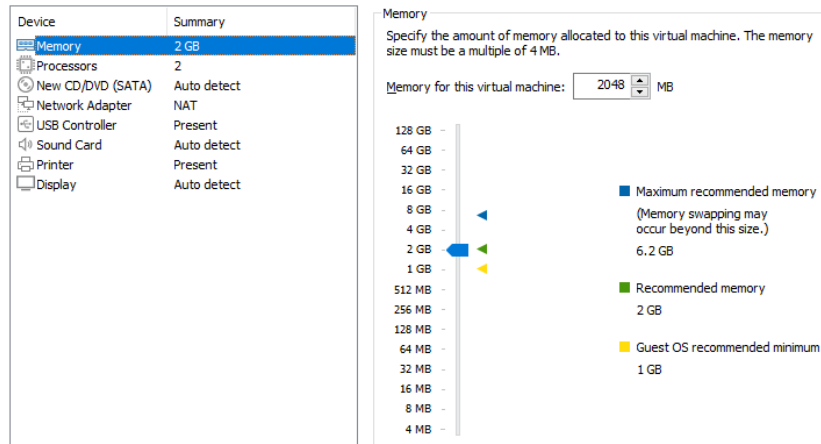


Figura 3.4 Tamaño memoria RAM de máquina virtual

Para la instalación correcta de la máquina virtual Ubuntu Server 20.04 es importante usar la imagen ISO adecuada del sistema operativo Ubuntu Server 20.04. Esta imagen ISO se obtuvo de la página oficial de Ubuntu <https://ubuntu.com/download/server> y se carga en la opción de *hardware* como se observa en la Figura 3.5. Se coloca *finish* y se cierra el cuadro de personalización del *hardware* para proceder con la instalación del sistema operativo de servidor.

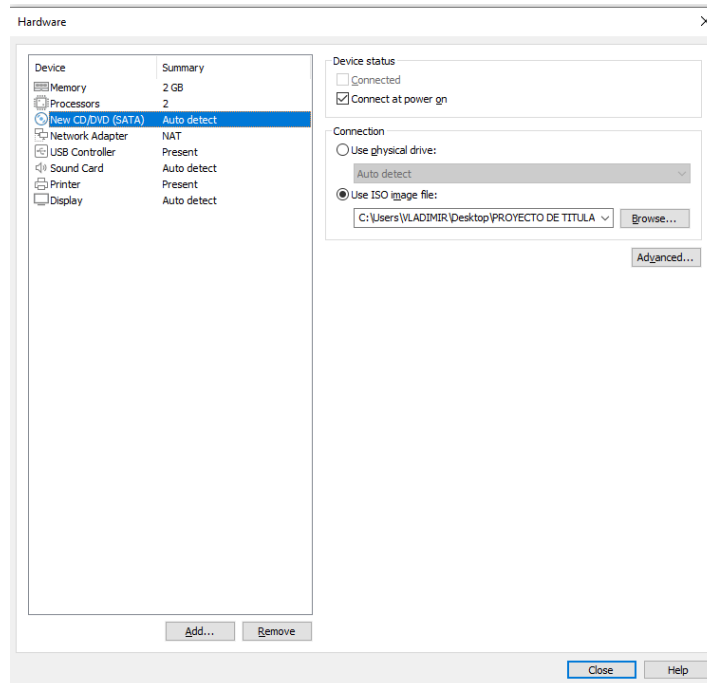


Figura 3.5 Asignación de la imagen ISO de Ubuntu Server 20.04

Al dar *click* en reanudar la máquina virtual se sigue diferentes pasos de instalación, se va a configurar un parámetro importante que será la asignación de nombre del servidor, de contraseña de usuario como se visualiza en la Figura 3.6. Estos datos son indispensables para el ingreso a la máquina virtual por medio del usuario y la contraseña, conforme se vaya desarrollando el proyecto se va a ir agregando los distintos comandos para los distintos requerimientos y será necesario ingresar la contraseña.

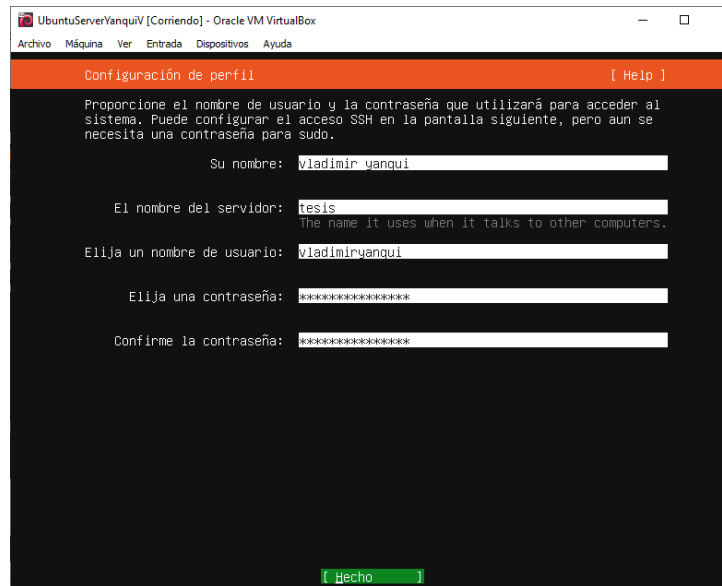


Figura 3.6 Asignación de nombre de servidor, contraseña y usuario

Finalizado el proceso de instalación del sistema operativo de servidor Linux de base Debian en Ubuntu Server 20.04 se presenta en la Figura 3.7. la interfaz de líneas de comando de Ubuntu.

```
Authorized uses only. All activity may be monitored and reported.
vladimiryanqui login: vladimiryanqui
Password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-155-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of lun 14 ago 2023 03:13:44 UTC

System load:  1.58      Processes:    257
Usage of /:   49.1% of 9.75GB   Users logged in:  0
Memory usage: 30%      IPv4 address for ens33: 192.168.142.145
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está activado.
Se pueden aplicar 0 actualizaciones de forma inmediata.

Last login: Thu Aug 10 15:29:30 UTC 2023 on tty1
vladimiryanqui@vladimiryanqui:~$ _
```

Figura 3.7 Interfaz de líneas de comandos de Ubuntu Server 20.04

En primera instancia antes de levantar el servicio de correo, se debe ingresar en la consola el comando **update** junto con la contraseña que se creó al momento de la instalación como se observa en la Figura 3.6. El cual va a permitir la actualización de la biblioteca que van a estar disponibles en los repositorios del sistema, ver Figura 3.8. posteriormente se ingresa el comando **upgrade** que va a permitir descargar e instalar las actualizaciones que se encuentran disponibles en el sistema, ver Figura 3.9.

```
vladimiryanqui@vladimiryanqui:~$ sudo apt update
[sudo] password for vladimiryanqui:
```

Figura 3.8 Comando *update*

```
vladimiryanqui@vladimiryanqui:~$ sudo apt upgrade
[sudo] password for vladimiryanqui:
```

Figura 3.9 Comando *upgrade*

Se levanta el servicio de correo *Postfix* mediante *Squirrelmail* ingresando el comando de la Figura 3.10. en donde se descarga e instalan todos los paquetes del servidor de correo electrónico *Postfix*.

```
vladimiryanqui@vladimiryanqui:~$ sudo apt-get install postfix
[sudo] password for vladimiryanqui:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Figura 3.10 Comando de instalación de *Postfix*

Se despliega una ventana que permite escoger el tipo de configuración del servidor de correo genérico que se va a utilizar y se selecciona la opción de configuración de paquetes por medio de sitio de internet, ver Figura 3.11.

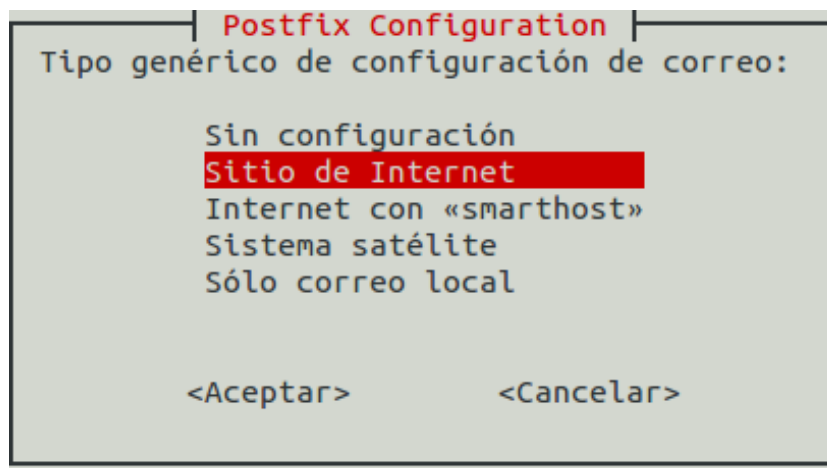


Figura 3.11 Selección de tipo de configuración de correo

La ventana que aparecerá va a permitir ingresar el nombre del dominio que se dio, este es **tesis.edu.ec**, el cual va a permitir el envío y recepción de correos entre un usuario y otro, como se puede ver en la Figura 3.12.

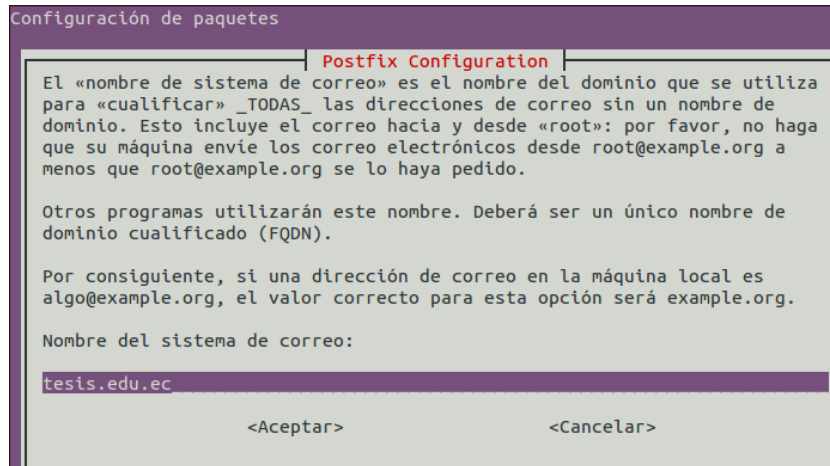


Figura 3.12 Asignación de nombre de dominio

Se verifica que las reglas del servidor de correo *Postfix* se encuentren bien escritas mediante el comando que se visualiza en la Figura 3.13. desplegándose que se encuentran actualizadas las reglas, como se evidencia en la Figura 3.13.

```
vladimiryanqui@vladimiryanqui:~$ sudo ufw allow 'Postfix'  
Skipping adding existing rule  
Skipping adding existing rule (v6)
```

Figura 3.13 Comando de verificación de reglas de *Postfix*

Se ingresa al archivo del directorio del servidor de correo *Postfix*, una vez dentro del archivo se va a realizar la respectiva copia de seguridad de este archivo como se observa en la Figura 3.14.

```
vladimiryanqui@vladimiryanqui:~$ cd /etc/postfix/  
vladimiryanqui@vladimiryanqui:/etc/postfix$ sudo cp main.cf main.cf.bkp_
```

Figura 3.14 Comando para realizar una copia de seguridad del archivo *Postfix*

Se ingresa al archivo de *Postfix* que en este caso se denomina *main.cf* mediante el comando **nano** para la configuración respectiva, como se observa en la Figura 3.15.

```
vladimiryanqui@vladimiryanqui:/etc/postfix$ sudo nano main.cf_
```

Figura 3.15. Comando para el ingreso al archivo *main.cf*

A continuación, se presenta el archivo en donde se encuentra las líneas de texto como se observa en la Figura 3.16. se dirige al final de las líneas de comando de este archivo

y se modifican los parámetros que se observan en la Figura 3.17. esto va a permitir la entrega de los mensajes de correos electrónicos en formato *Maildir*.

```
GNU nano 4.8 main.cf
# See /usr/share/postfix/main.cf.dist for a commented, more complete version

# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 2 on
# fresh installs.
compatibility_level = 2

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

[ Read 48 lines ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^G Cur Pos   M-U Undo
^X Exit      ^R Read File  ^N Replace    ^U Paste Text ^T To Spell  ^G Go To Line M-E Redo
```

Figura 3.16 Archivo de configuración de main.cf

```
home_mailbox = Maildir/
```

Figura 3.17 Agregación de parámetro para envío de mensajes de correo

Se procede a reiniciar el servidor de correo *Postfix* para que los parámetros de configuración anteriormente configurados se los guarde de forma correcta mediante el comando que se observa en la Figura 3.18.

```
vladimiryanqui@vladimiryanqui:/etc/postfix$ sudo systemctl restart postfix
```

Figura 3.18 Comando para reiniciar servidor de *Postfix*

Se procede a instalar el primer protocolo para la entrega y descarga de correos electrónicos en el *Courier* como indica la Figura 3.19.

```
vladimiryanqui@vladimiryanqui:/etc/postfix$ sudo apt-get install courier-pop_
```

Figura 3.19 Comando para la instalación del protocolo *courier-pop*

Se procede a instalar el segundo protocolo para acceder y administrar correos electrónicos que se van a almacenar en el servidor de correo *Postfix*, esto se realiza mediante el comando que se observa en la Figura 3.20.

```
vladimiryanqui@vladimiryanqui:/etc/postfix$ sudo apt-get install courier-imap
```

Figura 3.20 Comando para la instalación del protocolo *courier-imap*

Para poder inicializar el funcionamiento de los dos *courier*, *pop* e *imap* se necesita realizar la autenticación respectiva de usuarios y permitirá el correcto funcionamiento del servidor de correo por medio del comando que se observa en la Figura 3.21.

```
vladimiryanqui@vladimiryanqui:/etc/postfix$ sudo systemctl start courier-authdaemon
```

Figura 3.21 Comando para autenticación de *courier pop, imap*

Se instala el sistema de correo web *Squirrelmail* que permitirá el acceso a los correos electrónicos por medio de su navegador web descargándose por medio de la dirección que se ve en la Figura 3.22.

```
vladimiryanqui@vladimiryanqui:~$ sudo wget https://sourceforge.net/projects/squirrelmail/files/stable/1.4.22/squirrelmail-webmail-1.4.22.tar.gz_
```

Figura 3.22 Comando para la instalación de *Squirrelmail*

Para usar el sistema de correo web *Squirrelmail* se debe descomprimir el archivo descargado ya que las descargas se las realiza de forma comprimida, realizando este proceso ingresando el comando que la Figura 3.23. muestra.

```
vladimiryanqui@vladimiryanqui:~$ sudo tar -xvzf squirrelmail-webmail-1.4.22.tar.gz
```

Figura 3.23 Comando para descomprimir el archivo descargado de *Squirrelmail*

Los archivos que se encuentran dentro de la carpeta o directorio de *Squirrelmail* se van a mover dentro de un archivo *html* mediante el comando de la Figura 3.24.

```
vladimiryanqui@vladimiryanqui:~$ sudo mv squirrelmail-webmail-1.4.22 /var/www/html/
```

Figura 3.24 Comando para mover los archivos dentro de *html*

Se verifica las instalaciones realizadas ingresando al directorio de *html* mediante el comando que se observa en la Figura 3.25. y con el comando *ls* se visualiza lo instalado como se observa en la Figura 3.26.

```
vladimiryanqui@vladimiryanqui:~$ cd /var/www/html/  
vladimiryanqui@vladimiryanqui:/var/www/html$
```

Figura 3.25 Comando para ingresar al directorio HTML


```
vladimiryanqui@vladimiryanqui:/var/www/html$ ls  
index.html mail
```

Figura 3.26 Comando para verificar lo instalado

Una vez verificado lo instalado, se copia el archivo denominado *mail* para renombrarlo con este mismo nombre y de esa manera poder seguir utilizándolo mediante el comando que se observa en la Figura 3.27.

```
vladimiryanqui@vladimiryanqui:/var/www/html$ sudo mv squirrelmail-webmail-1.4.22 mail
```

Figura 3.27 Comando para copiar el archivo denominado *mail*

Mediante el comando que se observa en la Figura 3.28. se asignaron los permisos respectivos para la lectura, escritura, ejecución en los archivos y directorios.

```
vladimiryanqui@vladimiryanqui:/var/www/html$ sudo chown 755 -R /var/www/html/mail/
```

Figura 3.28 Comando para la agregación de permisos

Se ingresa al archivo denominado *mail* mediante el comando que se observa en la Figura 3.29. y una vez dentro de este se ingresa a la parte de configuración del archivo, ver la Figura 3.30. Posteriormente se modificó dicho archivo, renombrándolo con el nombre *config.php* mediante el comando como se observa en la Figura 3.31.

```
vladimiryanqui@vladimiryanqui:~$ cd /var/www/html/mail/
```

Figura 3.29 Comando para el ingreso al archivo *mail*

```
vladimiryanqui@vladimiryanqui:/var/www/html/mail$ cd config
```

Figura 3.30 Comando para configurar el archivo *mail*

```
vladimiryanqui@vladimiryanqui:/var/www/html/mail/config$ sudo cp config_default.php config.php
```

Figura 3.31 Comando para renombrar el archivo con el nombre php

Se ingresa al archivo *config.php* como se detalla en la Figura 3.32. y al haber ingresado a este archivo se realizaron diferentes modificaciones. La primera modificación es darle el nombre del dominio que se asignó al momento de la instalación y se lo denominó como *tesis.edu.ec* y que se observa en la Figura 3.12. mediante este nombre de dominio permitirá la recepción y envío de correos electrónicos en la bandeja de entrada y salida; en la Figura 3.33. se visualiza el procedimiento. La segunda modificación se ubica en la línea de archivo *data_dir* que en esta parte se va a modificar, como se observa en la

Figura 3.34. y que va a permitir crear una carpeta en donde se va a almacenar y manejar los correos electrónicos. La tercera modificación se la realiza en la línea de comando denominada *attachment_dir*, ver la Figura 3.35. y que permite gestionar y almacenar archivos adjuntos que se van a enviar o recibir en los correos electrónicos; se cierra el archivo y se guardarán los parámetros que se modificó.

```
vladimiryanqui@vladimiryanqui:/var/www/html/mail/config$ sudo nano config.php
```

Figura 3.32 Comando para ingresar al archivo de modificación config.php

```
* @global string $domain
*/
$domain = 'tesis.edu.ec';
```

Figura 3.33 Modificación y asignación de nombre de dominio

```
* @global string $data_dir
*/
$data_dir = '/var/www/html/mail/data/';
```

Figura 3.34 Modificación y asignación de dirección de datos

```
* @global string $attachment_dir
*/
$attachment_dir = '/var/www/html/mail/attach/';
```

Figura 3.35 Modificación y asignación de directorio de almacenamiento de archivos

Se crea un directorio o una carpeta nueva con el comando *mkdir* en la ubicación de la ruta que se observa en la Figura 3.36.

```
vladimiryanqui@vladimiryanqui:/var/www/html/mail/config$ sudo mkdir /var/www/html/mail/attach/_
```

Figura 3.36 Comando para la creación de una carpeta nueva

Mediante el proceso que detalla la Figura 3.37. se asignan permisos al archivo del directorio que se puede ver en la misma figura.

```
vladimiryanqui@vladimiryanqui:/var/www/html/mail/config$ sudo chown -R www-data:www-data /var/www/html/mail/_
```

Figura 3.37 Comando para la asignación de permisos a los archivos del directorio

Se reinicia el servidor web *Apache* para que los cambios realizados se guarden de forma correcta mediante la línea de código de la Figura 3.38.

```
vladimiryanqui@vladimiryanqui:/var/www/html/mail/config$ sudo systemctl restart apache2
```

Figura 3.38 Comando para reiniciar servidor *web Apache2*

Se instala las utilidades del sistema de correo electrónico que proporcionan las herramientas para la gestión y envío de correos electrónicos, como se observa en la Figura 3.39.

```
vladimiryanqui@vladimiryanqui:/var/www/html/mail/config$ sudo apt-get install mailutils
```

Figura 3.39 Comando para la instalación de *mailutils*

Se reinicia la máquina virtual para que todos los parámetros de instalación se lo realicen de forma correcta mediante el comando que se observa en la Figura 3.40.

```
vladimiryanqui@vladimiryanqui:/var/www/html/mail/config$ sudo reboot
```

Figura 3.40 Comando para reiniciar la máquina virtual

Una vez finalizado el proceso de instalación del servidor de correo *Postfix* mediante *Squirrelmail* se realiza el proceso de comprobación, para ello se ingresa el comando *ifconfig* para poder identificar la dirección IP como se observa en la Figura 3.41. y que tiene como valor de dirección **192.168.142.145**. Con ello se puede direccionar a una máquina cliente para poder verificar su funcionamiento en el servidor *web* que en este caso es *Squirrelmail*, usando el navegador predeterminado de la máquina cliente que en este caso se utilizó *Ubuntu Desktop 20.04*.

```
vladimiryanqui@vladimiryanqui:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.142.145 netmask 255.255.255.0 broadcast 192.168.142.255
    inet6 fe80::20c:29ff:feb8:86ac prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:b8:86:ac txqueuelen 1000 (Ethernet)
    RX packets 77534 bytes 112166414 (112.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12793 bytes 1034884 (1.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 926 bytes 79314 (79.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 926 bytes 79314 (79.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 3.41 Comando para identificación de la dirección IP

En la máquina cliente se abre el navegador predeterminado que es *Firefox* y en la barra de dirección se ingresa la dirección IP **192.168.142.145/mail** y se despliega la página web del servidor de correo *Postfix* mediante *Squirrelmail*, observándose en la Figura 3.42.



Figura 3.42 Ingreso a la página de *Squirrelmail*

Para el ingreso al servidor de correo se deben crear dos usuarios, en este caso se debe realizar este procedimiento dentro de la máquina servidor. En la Figura 3.43. se muestra el comando crear el usuario 1 como se lo va a nombrar, seguido de la creación de una contraseña nueva y que en este caso se va a crear una contraseña no robusta para evidenciar los parámetros críticos al momento de realizar el análisis de vulnerabilidades. Se reingresa la contraseña asignada y los demás parámetros se los deja por defecto y finalmente se corrobora la información si es correcta dando clic en sí.

```
vladimiryanqui@vladimiryanqui:~$ sudo adduser usuario1
Adding user `usuario1' ...
Adding new group `usuario1' (1001) ...
Adding new user `usuario1' (1001) with group `usuario1' ...
The home directory `/home/usuario1' already exists. Not copying from `/etc/skel'.
New password:
BAD PASSWORD: The password is shorter than 14 characters
Retype new password:
Password has been already used.
passwd: password updated successfully
Changing the user information for usuario1
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
vladimiryanqui@vladimiryanqui:~$ _
```

Figura 3.43 Comando para crear el usuario1 y parámetros de configuración

Se ingresa el usuario 1 en la página de *Squirrelmail* con la contraseña respectiva para acceder al servidor de correo, como se observa en la Figura 3.44.

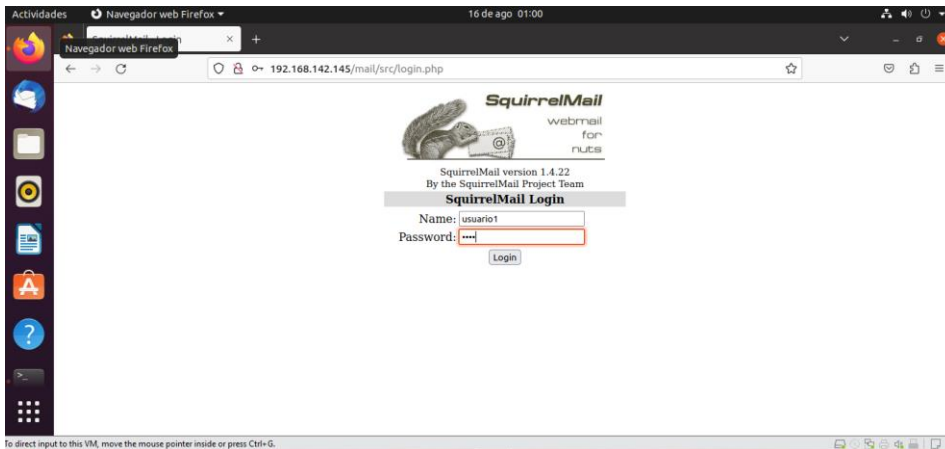


Figura 3.44 Ingreso de usuario1 con la contraseña

Al ingresar estos datos se va a reflejar un mensaje erróneo, evidenciándose por medio de la Figura 3.45. esto debido a que el usuario1 creado, mediante el servicio *IMAP*, no encuentra la carpeta del *maildir* y para corregir este problema se debe crear un usuario2 desde la máquina servidor y al enviar correos entre ellos se cree automáticamente.



Figura 3.45 Mensaje de error del servidor *IMAP*

Para la creación del usuario2 se lo realiza de la misma forma como se lo hizo con el usuario1, agregando los parámetros de contraseña y demás parámetros se los deja por defecto. La Figura 3.46. muestra lo expuesto.

```
vladimiryanqui@vladimiryanqui:~$ sudo adduser usuario2
Adding user `usuario2' ...
Adding new group `usuario2' (1002) ...
Adding new user `usuario2' (1002) with group `usuario2' ...
The home directory `/home/usuario2' already exists. Not copying from `/etc/skel'.
New password:
BAD PASSWORD: The password is shorter than 14 characters
Retype new password:
Password has been already used.
passwd: password updated successfully
Changing the user information for usuario2
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
```

Figura 3.46 Creación del usuario2

Para que la configuración se realice de forma automática se procede a enviar un correo desde el usuario1 al usuario2 por medio de una serie de pasos que se mencionan seguidamente:

- Ingreso al usuario1 por medio del comando de la Figura 3.47. al igual que la contraseña de usuario.
- Se coloca la palabra *mail* seguido del nombre del usuario2 al cual se le va a enviar el correo seguido del nombre de dominio *tesis.edu.ec*, esto se detalla en la Figura 3.48.
- Se ingresa un título del correo que se desea enviar en la parte de *subject*, luego se presiona la tecla *enter* y se direcciona a la escritura de cualquier mensaje que se desee redactar en el contenido del correo, cuando el mensaje a enviar se finalice se da un punto final en la parte inferior y para enviar el correo se presiona la tecla *control+d* y el correo se envía, todo este proceso se observa en la Figura 3.49.

```
vladimiryanqui@vladimiryanqui:~$ sudo su usuario1  
[sudo] password for vladimiryanqui:
```

Figura 3.47 Comando para ingreso de usuario1 seguido de la contraseña respectiva

```
usuario1@vladimiryanqui:/home/vladimiryanqui$ mail usuario2@tesis.edu.ec
```

Figura 3.48 Colocación de nombre de usuario2 y nombre de dominio

```
usuario1@vladimiryanqui:/home/vladimiryanqui$ mail usuario2@tesis.edu.ec  
Cc:  
Subject: Correo de prueba  
Hola estas dentro del servidor de correo.  
.  
-
```

Figura 3.49 Envío de correo electrónico desde el usuario1 al usuario2

Para la verificación de que la configuración se realizó de forma correcta y se corrigió el error que se desplegó en la Figura 3.45. lo que procede es ingresar nuevamente en el servidor de correo en *Squirrelmail* ingresando el nombre de usuario2 y la contraseña, como se lo realizó en la Figura 3.44. Se desplegó la bandeja de entrada con el correo que se recibió por parte del usuario1. La Figura 3.50. evidencia la bandeja de entrada con el correo recibido, el contenido del correo que se generó se observa de forma clara en la máquina cliente en *Squirrelmail*, ver la Figura 3.51.

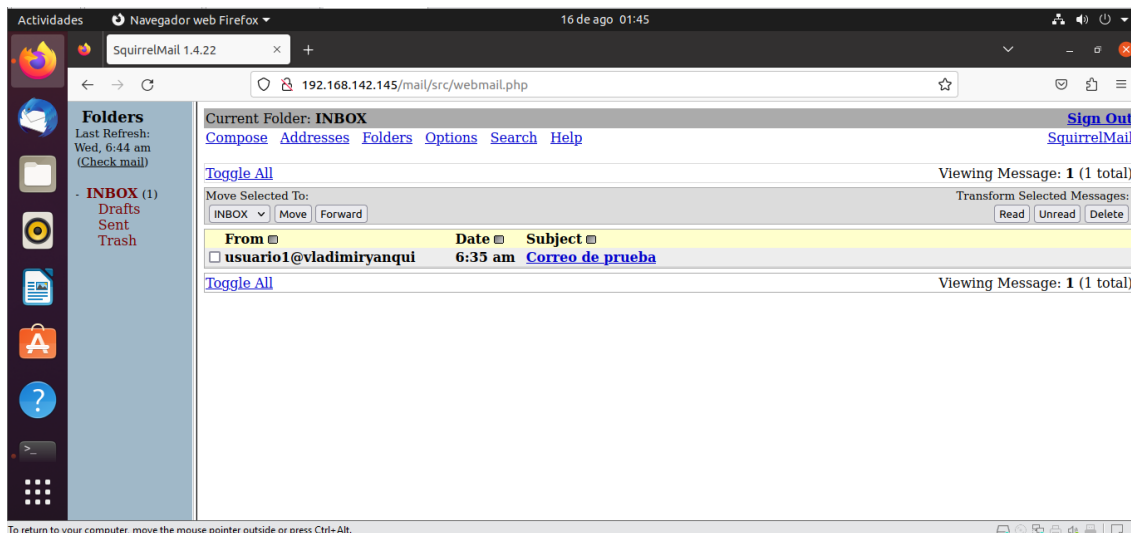


Figura 3.50 Bandeja de entrada del usuario 2 con el correo recibido

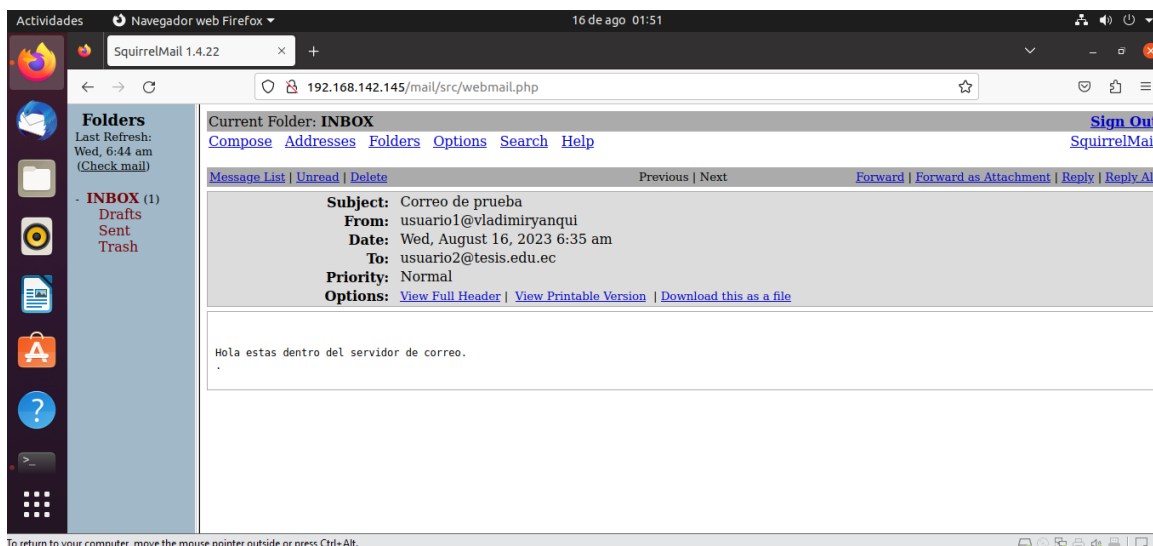


Figura 3.51 Contenido del correo enviado desde usuario1 al usuario2

Una parte importante para generar y visualizar el primer reporte de vulnerabilidades es crear un usuario y contraseña en el *software* de seguridad que ofrece *Ubuntu* desarrollado por *Canonical* y que por medio de esta suscripción se posibilita la agregación de políticas de seguridad en base al marco de referencia CIS.

Ubuntu Pro ofrece la herramienta de configuración y aplicación de las diferentes reglas de *hardening* mediante las herramientas de CIS *Benchmark*, de esa forma se obtuvieron los resultados de los análisis de vulnerabilidades sin políticas de seguridad o con políticas de seguridad.

Para esta sección se realizó el análisis sin políticas de seguridad, permitiendo identificar las vulnerabilidades en el sistema operativo de servidor mediante un reporte generado

el cual fue visualizado en la máquina cliente *Ubuntu Desktop 20.04* por medio del navegador *web mozilla*.

Como primera instancia se debe crear una cuenta y realizar la suscripción de *Ubuntu Pro* en la página oficial de Ubuntu <https://ubuntu.com/pro> como se observa en la Figura 3.52.



Figura 3.52 Suscripción a Ubuntu Pro

Se coloca dirección de correo electrónico del suscriptor, nombres, nombre de usuario y contraseñas como se observa en la Figura 3.53.

Ubuntu.com

Por favor escriba su correo electrónico:

No tengo una cuenta de Ubuntu One

Tengo una cuenta de Ubuntu One y *mi contraseña es:*

Díganos su nombre completo y elija un nombre de usuario y contraseña:

Nombre completo

Nombre de usuario

- Entre 3 y 32 caracteres de largo.
- Permitido: minúsculas, números y guiones.
- NO permitido: letras CAPITAL, caracteres especiales.
- NO permitido: solo números o guiones consecutivos.

Elegir contraseña

Figura 3.53 Suscripción en Ubuntu PRO

Luego se accede por medio del correo y contraseña creada para dirigirse a la página en donde se despliega un *token* que va a permitir por medio de la consola acceder al modo *Ubuntu Pro* y acceder a los servicios de *CIS Benchmark* para obtener los reportes de vulnerabilidades, ver la Figura 3.54.

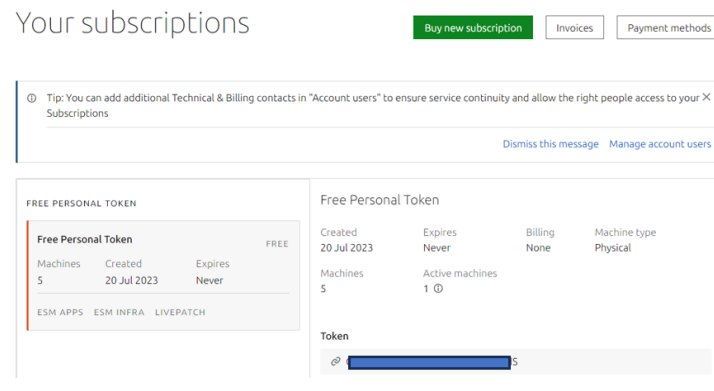


Figura 3.54 Asignación de *Token* para acceder a servicios de Ubuntu Pro

En la máquina servidor se ingresa el *token* para acceder a los servicios de *Ubuntu Pro* como se observa en la Figura 3.55. por medio de la consola, el proceso de instalación de los servicios inicia y al final de la instalación se observa que se realizó el proceso de forma correcta. Se visualizan los servicios a los que se puede acceder, estando en color verde los servicios que están habilitados por defecto y el servicio que está por habilitar y que va a permitir acceder a las herramientas de cumplimiento de normativas *CIS* es la herramienta *usg*.

```
vladimiryanqui@vladimiryanqui:~$ sudo pro attach C13jwTCgnvFdjh6PGRvRHBznAbkqds
Enabling default service esm-apps
Updating package lists
Ubuntu Pro: ESM Apps enabled
Enabling default service esm-infra
Updating package lists
Ubuntu Pro: ESM Infra enabled
Enabling default service livepatch
Canonical livepatch enabled.
This machine is now attached to 'Ubuntu Pro - free personal subscription'

SERVICE      ENTITLED  STATUS   DESCRIPTION
esm-apps      yes      enabled  Expanded Security Maintenance for Applications
esm-infra     yes      enabled  Expanded Security Maintenance for Infrastructure
fips          yes      disabled NIST-certified core packages
fips-updates  yes      disabled NIST-certified core packages with priority security updates
livepatch     yes      enabled  Canonical Livepatch service
usg           yes      disabled Security compliance and audit tools

NOTICES
Operation in progress: pro attach

For a list of all Ubuntu Pro services, run 'pro status --all'
Enable services with: pro enable <service>

Account: vladigio@hotmail.com
Subscription: Ubuntu Pro - free personal subscription
```

Figura 3.55 Ingreso de *token* de Ubuntu Pro por medio de consola

Se procede a habilitar y va a permitir acceder a las herramientas de cumplimiento de normativas CIS es la herramienta *usg* como se visualiza en la Figura 3.56. y luego de ello se instalan las herramientas *usg* por medio del comando que se observa en la Figura 3.57.

```
vladimiryanqui@vladimiryanqui:~$ sudo ua enable usg
One moment, checking your subscription first
```

Figura 3.56 Comando de habilitación de herramientas usg

```
vladimiryanqui@vladimiryanqui:~$ sudo apt install usg
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Figura 3.57 Comando para instalación de herramientas usg

Se instaló los paquetes que tienen dependencias para el servicio de *usg-cisbenchmark* por medio del comando que se observa en la Figura 3.58.

```
vladimiryanqui@vladimiryanqui:~$ sudo apt-get install usg-common _
```

Figura 3.58 Comando de instalación de paquetes dependientes

Se instalan los paquetes de *CIS benchmark* como se observa en la Figura 3.59.

```
vladimiryanqui@tesis:~$ sudo apt install usg-cisbenchmark
[sudo] password for vladimiryanqui: _
```

Figura 3.59 Comando para la instalación del paquete *CIS benchmark*

Se verifica en donde se encuentra la dirección de la ruta de los archivos de la auditoría que se va a realizar, para generar los reportes de vulnerabilidad y se va a mostrar la ruta mediante el comando que se observa en la Figura 3.60.

```
vladimiryanqui@vladimiryanqui:~$ which cis-audit
/usr/sbin/cis-audit
```

Figura 3.60 Comando para verificar la dirección de ruta de los archivos

Para verificar la versión que se tiene instalada, mediante una lista de los archivos que se encuentran en el directorio de *CIS Benchmark* se ingresa el contenido que muestra la Figura 3.61. para posteriormente desplegar una lista de los archivos generados y verificar la ruta en donde se van a generar los reportes de vulnerabilidades.

```
vladimiryanqui@vladimiryanqui:~$ ls /usr/share/ubuntu-scrap-security-guides/
Canonical_Ubuntu_20.04_CIS_Benchmark-oval.xml    CIS-3.5.3.2.2.sh
Canonical_Ubuntu_20.04_CIS_Benchmark-xccdf.xml  CIS-3.5.3.2.4.sh
CIS-1.7.1.3.sh                                  CIS-3.5.3.3.1.sh
CIS-1.7.1.4.sh                                  CIS-3.5.3.3.2.sh
cis-20.04-report.html                            CIS-4.1.10.sh
cis-20.04-results.xml                           CIS-4.1.11.sh
CIS-3.5.1.1.sh                                  CIS-4.1.12.sh
CIS-3.5.1.2.sh                                  CIS-4.1.13.sh
CIS-3.5.1.3.sh                                  CIS-4.1.14.sh
CIS-3.5.1.4.sh                                  CIS-4.1.15.sh
CIS-3.5.1.7.sh                                  CIS-4.1.16.sh
CIS-3.5.2.10.sh                                 CIS-4.1.3.sh
CIS-3.5.2.1.sh                                  CIS-4.1.4.sh
CIS-3.5.2.2.sh                                  CIS-4.1.5.sh
CIS-3.5.2.4.sh                                  CIS-4.1.6.sh
CIS-3.5.2.5.sh                                  CIS-4.1.7.sh
CIS-3.5.2.6.sh                                  CIS-4.1.8.sh
CIS-3.5.2.8.sh                                  CIS-4.1.9.sh
CIS-3.5.2.9.sh                                  CIS-5.4.1.5.sh
CIS-3.5.3.1.1.sh                                CIS-6.2.6.sh
CIS-3.5.3.1.2.sh                                cis-hardening
CIS-3.5.3.1.3.sh                                Ubuntu_20.04_Benchmark-cpe-dictionary.xml
CIS-3.5.3.2.1.sh                                Ubuntu_20.04_Benchmark-cpe-oval.xml
```

Figura 3.61 Comando para el listado de archivos generados

Ubicación dentro del directorio de los archivos que contienen las guías de seguridad de *Ubuntu Scap* para la obtención del primer reporte, como se observa en la Figura 3.62.

```
vladimiryanqui@vladimiryanqui:~$ cd /usr/share/ubuntu-scrap-security-guides/
vladimiryanqui@vladimiryanqui:/usr/share/ubuntu-scrap-security-guides$ cd cis-hardening/
vladimiryanqui@vladimiryanqui:/usr/share/ubuntu-scrap-security-guides/cis-hardening$
```

Figura 3.62 Comando para ubicación dentro de directorio de CIS *hardening*

El comando que permitirá realizar todo el proceso de escaneo de vulnerabilidades, en el sistema operativo con el servidor de correo, es el comando que se observa en la Figura 3.63. el cual emitió el primer registro de vulnerabilidades que se visualizó mediante la maquina cliente *Ubuntu Desktop 20.04*.

```
vladimiryanqui@vladimiryanqui:/usr/share/ubuntu-scrap-security-guides/cis-hardening$ sudo cis-audit
```

Figura 3.63 Comando para el proceso de escaneo

El proceso de escaneo se realiza en un tiempo determinado y al finalizar dicho análisis presenta el mensaje que se realizó de forma correcta, incluyendo la ruta en donde se puede visualizar el reporte generado como se observa en la Figura 3.64.

```

Title  Ensure users' .netrc Files are not group or world accessible
Rule   xccdf_com.ubuntu.focal.cis_rule_CIS-6.2.10
Result pass

Title  Ensure no users have .rhosts files
Rule   xccdf_com.ubuntu.focal.cis_rule_CIS-6.2.11
Result pass

Title  Ensure all groups in /etc/passwd exist in /etc/group
Rule   xccdf_com.ubuntu.focal.cis_rule_CIS-6.2.12
Result pass

Title  Ensure no duplicate UIDs exist
Rule   xccdf_com.ubuntu.focal.cis_rule_CIS-6.2.13
Result pass

Title  Ensure no duplicate GIDs exist
Rule   xccdf_com.ubuntu.focal.cis_rule_CIS-6.2.14
Result pass

Title  Ensure no duplicate user names exist
Rule   xccdf_com.ubuntu.focal.cis_rule_CIS-6.2.15
Result pass

Title  Ensure no duplicate group names exist
Rule   xccdf_com.ubuntu.focal.cis_rule_CIS-6.2.16
Result pass

Title  Ensure shadow group is empty
Rule   xccdf_com.ubuntu.focal.cis_rule_CIS-6.2.17
Result pass

CIS audit scan completed. The scan results are available in /usr/share/ubuntu-scrap-security-guides/cis-20.04-report.html report.

```

Figura 3.64 Escaneo finalizado, ubicación del reporte generado

Mediante el comando que se muestra en la Figura 3.65. se procede a copiar la ruta de los archivos generados en la carpeta de la máquina cliente, se dirige al sitio *web* de la máquina cliente para visualizarlo.

```

vladimiryanqui@vladimiryanqui:~$ sudo cp /usr/share/ubuntu-scrap-security-guides/cis-20.04-report.html /var/www/html/index.html

```

Figura 3.65 Comando para copiar la ruta de archivos generados de CIS *hardening*

Una vez realizado el proceso de la Figura 3.65. se abre el navegador web *mozilla* en la máquina cliente, ingresando en el navegador la dirección IP que se verificó en la Figura 3.41. con el valor de **192.168.142.145** desplegándose el reporte de vulnerabilidades como se observa en la Figura 3.66.

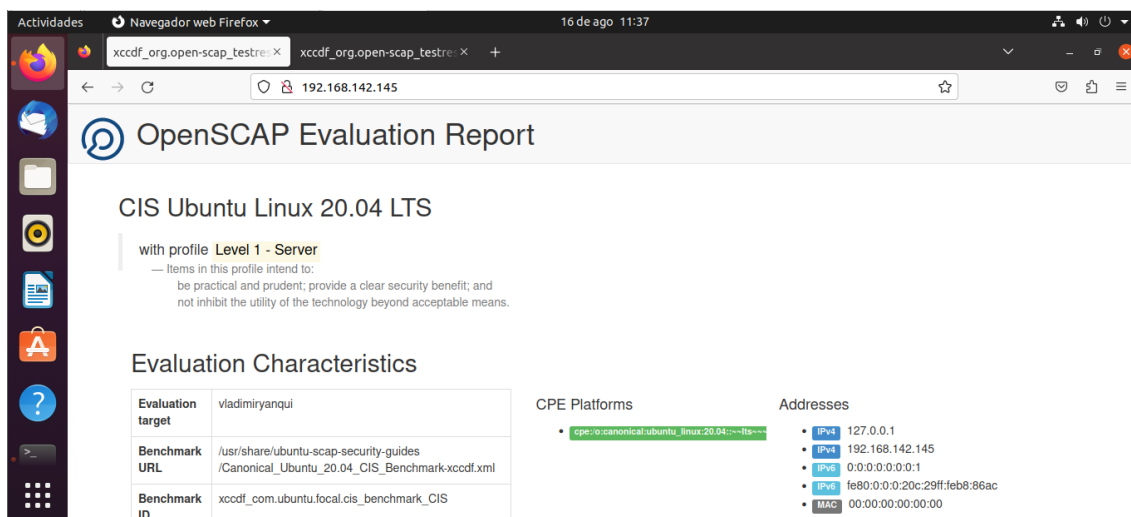


Figura 3.66 Reporte de vulnerabilidades generado

El reporte generado en la Figura 3.67. muestra que el servidor está protegido en un 52,35%, el restante 47,65% son reglas que no se han cumplido, vulnerabilidades de este servidor. Posteriormente se debe asignar un comando que permita agregar una política de seguridad en base al marco de referencia *C/S* con el fin de endurecer y reducir el porcentaje de severidad.

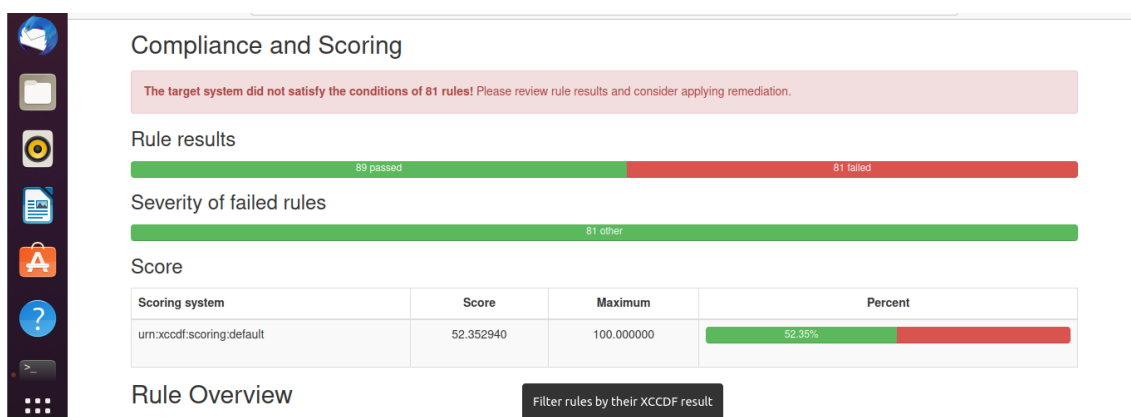


Figura 3.67. Porcentaje de protección del servidor sin políticas de seguridad

3.2 Implementación de una política de seguridad en un sistema operativo de servidor

En el sistema de servidor para la implementación de la política de seguridad se procede a instalar una nueva máquina, la cual debe seguir de forma ordenada una serie de pasos de instalación para obtener los resultados correctos y que se detallan a continuación.

Instalación de un nuevo sistema operativo de servidor

Para este proceso la nueva máquina virtual que contenga un sistema operativo de servidor *Ubuntu Server 20.04* se sigue el orden indicado en la sección 3.1 empezando desde la Figura 3.1. hasta la Figura 3.7. considerando que la instalación de la nueva máquina virtual conlleva el mismo procedimiento y orden.

Para verificar que la nueva máquina virtual no contenga ningún tipo de servicio instalado, como el servidor de correo *Postfix* mediante *Squirrelmail*, se evidencia por medio de la línea de código que se muestra en la Figura 3.68. se evidenció que no aparece ningún paquete instalado. Para verificar que no contenga ningún paquete de *CIS Benchmark* se implementa ingresando el comando que la Figura 3.69. se observa que no contiene ningún paquete instalado.

Se verifica también, mediante el ingreso de la línea de código de la Figura 3.70. que los paquetes del servidor web *Apache2* no estén instalados y no exista ningún paquete, evidenciando de esa forma que la máquina virtual nueva no contiene nada.

```
vladimiryanqui@vladimiryanqui:~$ sudo dpkg -l | grep postfix
vladimiryanqui@vladimiryanqui:~$ sudo dpkg -l | grep squirrelmail
```

Figura 3.68 Comando para verificación de los paquetes de *Postfix* y *Squirrelmail* no están instalados en la máquina virtual

```
vladimiryanqui@vladimiryanqui:~$ sudo dpkg -l | grep usg-cisbenchmark
vladimiryanqui@vladimiryanqui:~$
```

Figura 3.69 Comando para la verificación de paquetes de *CIS Benchmark* no están instalados en la máquina virtual

```
vladimiryanqui@vladimiryanqui:~$ sudo dpkg -l | apache2
Command 'apache2' not found, but can be installed with:
sudo apt install apache2-bin
```

Figura 3.70 Comando para verificación de paquetes de *Apache2* no se encuentran instalados en la máquina virtual

Agregación de políticas de seguridad mediante el marco de referencia CIS

Para la agregación de la política de seguridad mediante el marco de referencia *CIS* se realiza siguiendo el orden que muestra la Figura 3.55. hasta la Figura 3.62. que son las herramientas de *CIS Benchmark* para el proceso de escaneo y obtención del

reporte de vulnerabilidades, considerando que este proceso de instalación es el mismo en la nueva máquina virtual.

El parámetro importante en esta sección se basa en la agregación del comando que va a permitir agregar una política de seguridad en base al marco de referencia *CIS* y que permitirá evidenciar la reducción de severidades o vulnerabilidades en el sistema operativo.

El comando que permite realizar este proceso se despliega en la Figura 3.71. teniendo en cuenta que la herramienta *CIS Benchmark* posee diferentes niveles de seguridad dependiendo del uso que se vaya a realizar, para el caso de estudio del presente proyecto se ubica en nivel uno debido a que ayuda a mejorar la seguridad del sistema, reducción significativa de vulnerabilidades, cumplimiento de estándares de seguridad, bases sólidas de seguridad, no afectación de forma negativa en la funcionalidad del sistema implementado. Se aplica nivel uno porque es un punto de partida para la aplicación de recomendaciones de seguridad esenciales, cada empresa puede implementar niveles de seguridad más estrictas (nivel 2 y 3) dependiendo de la utilización, el proceso de asignación de este comando se observa en la Figura 3.72.

```
vladimiryanqui@vladimiryanqui:/usr/share/ubuntu-scrap-security-guides/cis-hardening$ sudo ./Canonical_1_Ubuntu_20.04_CIS-harden.sh lv11_server_
```

Figura 3.71 Comando para la agregación de política de seguridad

```
***Applying Level-1 scored server remediation for failures on a fresh Ubuntu 20.04 install***
Obj:1 http://ec.archive.ubuntu.com/ubuntu focal InRelease
Des:2 http://ec.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Des:3 http://ec.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Des:4 http://ec.archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Des:5 https://esm.ubuntu.com/cis/ubuntu focal InRelease [3.138 B]
Des:6 https://esm.ubuntu.com/apps/ubuntu focal-apps-security InRelease [7.568 B]
Des:7 https://esm.ubuntu.com/apps/ubuntu focal-apps-updates InRelease [7.459 B]
Des:8 https://esm.ubuntu.com/infra/ubuntu focal-infra-security InRelease [7.453 B]
Des:9 https://esm.ubuntu.com/infra/ubuntu focal-infra-updates InRelease [7.452 B]
```

Figura 3.72 Proceso de instalación de políticas de seguridad

Se verifica el archivo que se ha generado mediante el comando que se observa en la Figura 3.73. y se evidencia que el *log* que contiene los parámetros de la configuración de las reglas de *CIS hardening* se ha creado de forma automática.

```

vladimiryanqui@vladimiryanqui:/usr/share/ubuntu-scrap-security-guides/cis-hardening$ ls
audit_rules          CIS-ruleset-1.sh   CIS-ruleset-4.sh   ruleset-
Canonical_Ubuntu_20.04_CIS-harden.log  CIS-ruleset-2.sh  CIS-ruleset-5.sh   ruleset-params.conf
Canonical_Ubuntu_20.04_CIS-harden.sh  CIS-ruleset-3.sh  CIS-ruleset-6.sh   ruleset-tools.sh

```

Figura 3.73 Comando para visualizar el *log* que contiene los parámetros de la configuración de las reglas de *CIS hardening*

Servicio de correo *Postfix* mediante *Squirrelmail*

Se levanta el servidor de correo siguiendo el procedimiento ordenado que se muestra desde la Figura 3.9. hasta la Figura 3.40. siendo de esta forma el mismo proceso de instalación del servidor de correo para la máquina nueva de servidor.

Se verificó la dirección IP de este servidor, con un valor **192.168.142.145** como se observa en la Figura 3.74.

```

vladimiryanqui@vladimiryanqui:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.142.145  netmask 255.255.255.0  broadcast 192.168.142.255
    inet6 fe80::20c:29ff:feb8:86ac  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:b8:86:ac  txqueuelen 1000  (Ethernet)
    RX packets 92977  bytes 132472620 (132.4 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 20552  bytes 1748725 (1.7 MB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 2097  bytes 180877 (180.8 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 2097  bytes 180877 (180.8 KB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

```

Figura 3.74 Visualización de la dirección IP, nueva máquina virtual

Para la agregación de usuarios en este nuevo parámetro se procede a robustecer las contraseñas tanto al usuario1 como al usuario2 para de esta forma reducir el porcentaje de severidad al realizar el proceso de auditoría de vulnerabilidades, visualizando en la Figura 3.75. la agregación del usuario1 con una contraseña robusta y en la Figura 3.76. la agregación del usuario2 con una contraseña robusta también.


```

vladimiryanqui@vladimiryanqui:~$ sudo adduser usuario1
Adding user `usuario1' ...
Adding new group `usuario1' (1001) ...
Adding new user `usuario1' (1001) with group `usuario1' ...
The home directory `/home/usuario1' already exists. Not copying from `/etc/skel'.
New password:
BAD PASSWORD: The password is shorter than 14 characters
Retype new password:
Password has been already used.
passwd: password updated successfully
Changing the user information for usuario1
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
vladimiryanqui@vladimiryanqui:~$ _

```

Figura 3.75 Creación de Usuario1 con robustes de contraseña

```

vladimiryanqui@vladimiryanqui:~$ sudo adduser usuario2
Adding user `usuario2' ...
Adding new group `usuario2' (1002) ...
Adding new user `usuario2' (1002) with group `usuario2' ...
The home directory `/home/usuario2' already exists. Not copying from `/etc/skel'.
New password:
BAD PASSWORD: The password is shorter than 14 characters
Retype new password:
Password has been already used.
passwd: password updated successfully
Changing the user information for usuario2
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y

```

Figura 3.76 Creación de Usuario2 con robustes de contraseña

La comprobación del funcionamiento correcto del servidor se lo realizó inicializando el servidor de correo *Postfix* en *Squirrelmail* mediante el explorador del sistema que es *mozilla* en la máquina virtual cliente, se ingresa la dirección IP que se identificó en la Figura 3.74. con un valor **192.168.142.145**. En la barra de navegación como despliega la Figura 3.77. y se abre la página del servidor de correo para el ingreso de usuarios.

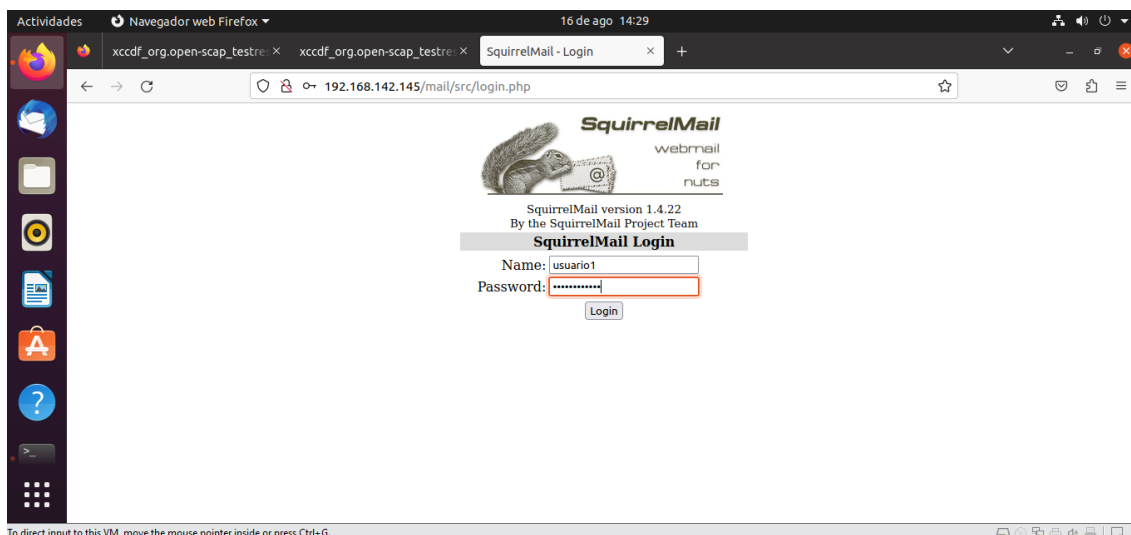


Figura 3.77 Ingreso al servidor de correo en la nueva máquina virtual

Se ingresa al usuario1 y la contraseña robusta para administrar, recibir o enviar correos electrónicos entre el usuario1 y usuario2 como se observa en la Figura 3.78. evidenciándose el correcto funcionamiento del servidor de correo por medio de envíos de correos electrónicos entre usuarios.

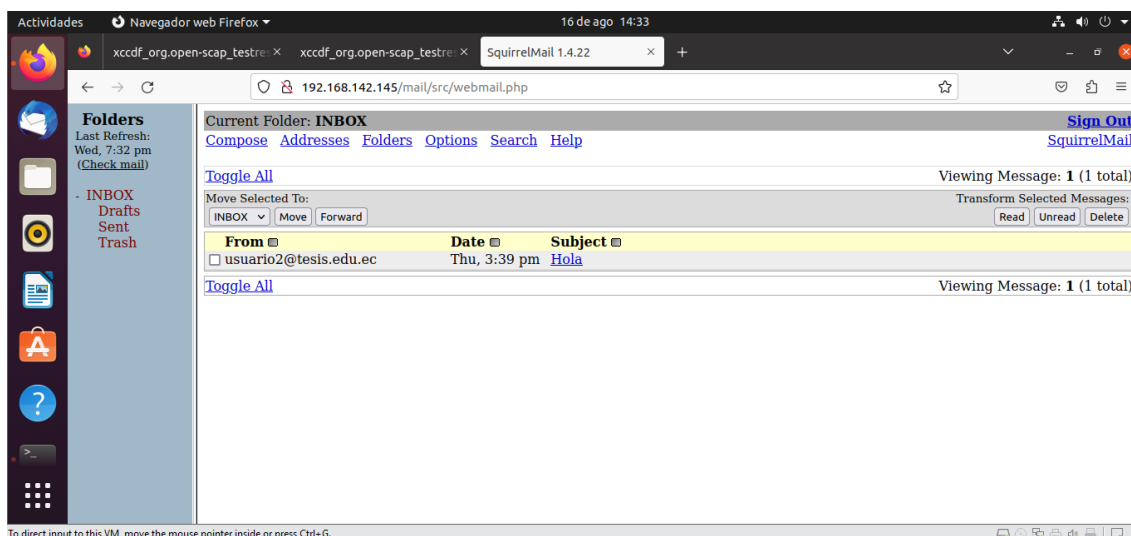


Figura 3.78 Comprobación del correcto funcionamiento del servidor de correo

Proceso de escaneo para generar un nuevo reporte

Una vez colocada la política y levantado el servidor de correo se procede a generar un reporte nuevo de vulnerabilidades. Se dirige a la máquina cliente *Ubuntu Desktop 20.04* por medio del navegador *web mozilla* ingresar la dirección IP,

192.168.142.145, evidenciándose que el reporte generado se realizó de forma correcta como se observa en la Figura 3.79.

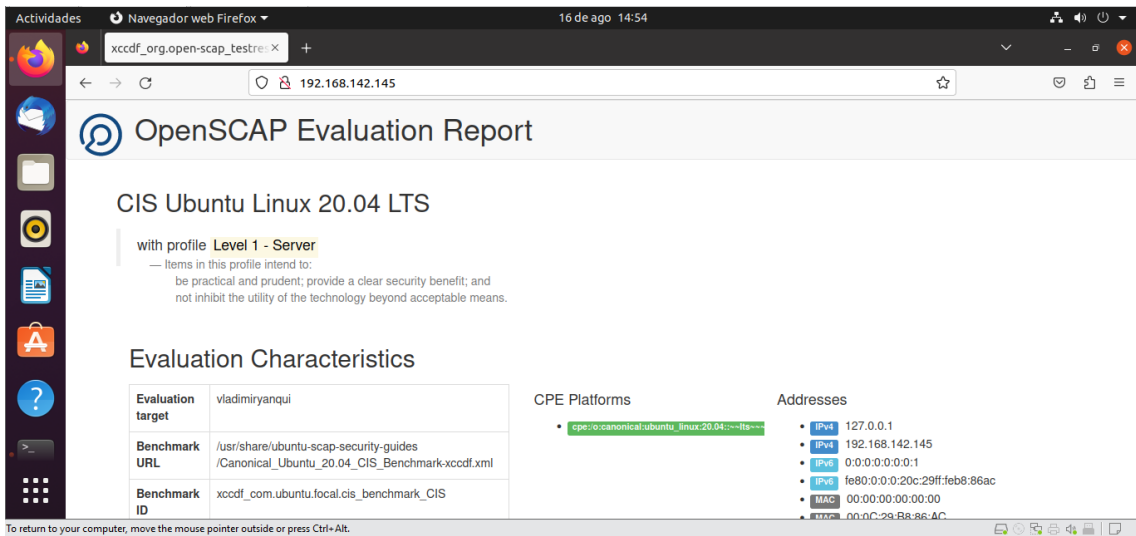


Figura 3.79 Reporte generado en el servidor con políticas de seguridad

Los valores obtenidos en el presente reporte se los visualiza en la Figura 3.80. se evidencia el gran porcentaje de reducción de severidades o vulnerabilidades. El servidor está protegido en 91.18% con la inclusión de las políticas de seguridad en base al marco de referencia CIS. El 8.82% representa las vulnerabilidades que el servidor contiene, en comparación con el reporte generado en la Figura 3.67. que tenía el 47,65 % de severidad en las reglas de vulnerabilidades que presentó dicho servidor. De esta forma se garantiza el proceso de *hardening* en el servidor que se realizó de forma correcta.

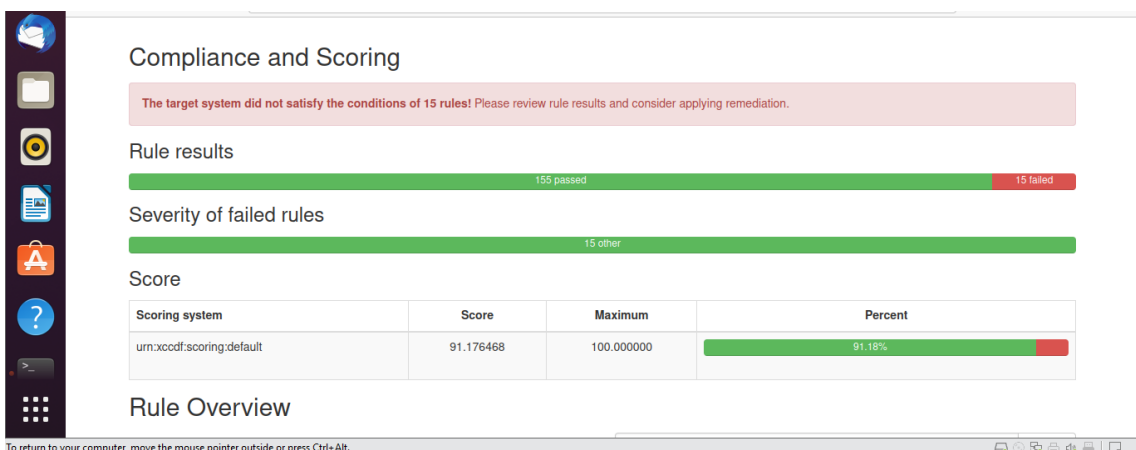


Figura 3.80 Visualización del porcentaje de reducción de vulnerabilidades

3.3 Análisis de los reportes, resultado de aplicación de la herramienta de escaneo

El análisis de los reportes generados va a determinar el nivel de seguridad que tiene cada uno de los sistemas operativos de servidor sin aplicar ninguna política de seguridad y al aplicar una política de seguridad. Para ello mediante los reportes generados se realiza el análisis respectivo empezando por el primer reporte el cual consistió en el diseño e implementación del sistema operativo servidor sin política de seguridad y el segundo análisis será en el sistema operativo de servidor aplicando una política de seguridad.

Análisis del reporte generado sin políticas de seguridad

El primer parámetro que se indaga es el número de reglas que el sistema no cumple con las condiciones que el marco de referencia *C/S* establece, por tal motivo luego se debe aplicar una política de seguridad para mejorar este parámetro, en la Figura 3.81. se observa que **81 reglas** no cumplen con las reglas o son fallidas y **89 reglas** sí cumplieron con las condiciones.

Compliance and Scoring

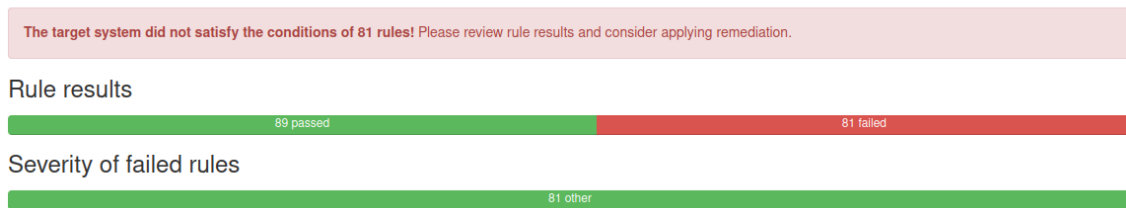


Figura 3.81 Número de reglas que el servidor, sin políticas, cumple y no cumple

El segundo parámetro que se analiza es el porcentaje de severidad de las reglas que cumplen o no con las reglas de severidad que el marco de referencia *C/S* establece y que el sistema operativo de servidor no las cumple. La Figura 3.82. muestra un **52.35 %** de reglas del sistema operativo de servidor si cumple y el **47,67 %** restante son las reglas de severidad que el sistema no cumple. Siendo un porcentaje bastante alto que el servidor no cumple por lo que se determina que el nivel de seguridad es altamente severo.

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	52.352940	100.000000	

Figura 3.82 Porcentaje de severidad de las reglas que cumplen y no sin políticas de seguridad

El tercer parámetro que se analiza son las reglas que presentan un resultado fallido dentro del sistema operativo de servidor, el reporte muestra 81 reglas que resultaron fallidas y que representaran un riesgo, la Figura 3.83. muestra los detalles de las siete primeras reglas fallidas que el sistema identificó después de realizar el escaneo.

Ensure mounting of cramfs filesystems is disabled	unknown	fail
Ensure mounting of freevxfs filesystems is disabled	unknown	fail
Ensure mounting of jffs2 filesystems is disabled	unknown	fail
Ensure mounting of hfs filesystems is disabled	unknown	fail
Ensure mounting of hfsplus filesystems is disabled	unknown	fail
Ensure mounting of udf filesystems is disabled	unknown	fail
Ensure /tmp is configured	unknown	fail

Figura 3.83 Reglas fallidas dentro del sistema operativo de servidor

Las reglas fallidas enmarcan un grupo de reglas que necesitan asegurarse, realizando el montaje de distintos parámetros que en el sistema de archivos se encuentran desactivados. A continuación, se evidencia el análisis de reglas fallidas mismas que posteriormente en el proceso de agregación de una política de seguridad se muestran que han sido solventadas.

En la Figura 3.84. se muestra una regla que su parámetro de configuración se basa en el conjunto de archivos que van a impedir que los usuarios puedan ejecutar programas desde el disco compartido. Es un gran problema tenerlo como una regla fallida dentro del sistema de servidor ya que al implementarla se logrará disminuir la introducción de *softwares* malicioso dentro del servidor.

Ensure noexec option set on /dev/shm partition	unknown	fail
--	---------	------

Figura 3.84 Regla de la opción noexec activa

En la Figura 3.85. se muestra una regla que si no se la tiene activa, puede conducir a que un *malware* basado en *USB* sea un mecanismo fácil para la infiltración dentro de la red. Esto se convierte en una amenaza que va a persistir si no se la corrige dentro de la red por medio del almacenamiento *USB* cuando se transfiere o almacena archivos.

Disable USB Storage	unknown	fail
---------------------	---------	------

Figura 3.85 Regla de almacenamiento *USB* desactivada

En la Figura 3.86. se muestra una regla que va a permitir asegurarse de que los comandos *sudo* utilicen *pty*, de esa forma se reducirá la ejecución de programas maliciosos utilizando *sudo* por medio de atacantes.



Figura 3.86 Regla para la utilización de comandos sudo que usen pty

Análisis del reporte generado con políticas de seguridad

En base al análisis anterior de los reportes generados, este apartado va a hacer hincapié en la importancia que implica reducir de gran manera el nivel de severidad, que los sistemas operativos de servidor presentan, al aplicar una política de seguridad en base al marco de referencia *CIS*. Para ello mediante la política agregada, los nuevos reportes generados presentan un porcentaje alto de reducción y endurecimiento del servidor.

El primer parámetro por estudiar es el número de reglas que el sistema operativo de servidor no cumple con las condiciones que el marco de referencia *CIS* establece, haciendo referencia al reporte generado en el apartado anterior y que se observa en la Figura 3.81. agregando una política de seguridad para mejorar este parámetro, se observa en la Figura 3.87. la cantidad de 15 reglas fallidas, siendo una reducción bastante considerable, son ahora 155 reglas que sí cumplieron con las condiciones. Cumpliendo con el objetivo de tener un mejoramiento, endurecimiento y aplicación de *hardening* al servidor.

Compliance and Scoring

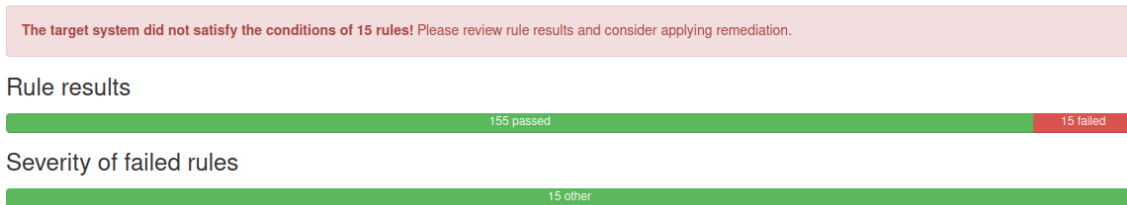


Figura 3.87 Número de reglas que el sistema operativo de servidor cumple y no cumple con las condiciones que el marco de referencia *CIS* establece

El segundo parámetro que se analiza es el porcentaje de severidad, el cual indica qué reglas cumplen o no en base a lo que el marco de referencia *CIS* establece y que el sistema operativo de servidor no las cumple. En referencia al apartado anterior y que se observa en la Figura 3.82. muestra un **52.35 %** de reglas del sistema operativo de servidor si cumple, al aplicar una política de seguridad en base al marco de referencia *CIS* se evidencia un aumento del porcentaje al **91.18 %** de reglas que sí cumplen y que se solventaron al aplicar la política de seguridad.

Evidenciándose por medio del porcentaje presentado que cumple con el objetivo de endurecimiento del sistema y un mejoramiento en el sistema operativo de servidor y que se muestra la Figura 3.88.

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	91.176468	100.000000	91.18%

Figura 3.88 Porcentaje de severidad de las reglas que cumplen y no en el sistema operativo de servidor

El tercer parámetro que se analiza son las reglas que ya no presentan como resultado fallido dentro del sistema operativo de servidor en referencia al apartado anterior y que se muestra en la Figura 3.83. Al momento de aplicar la política de seguridad y realizando un nuevo escaneo, de las siete reglas fallidas, mostradas en la Figura 3.83. se evidencia que seis reglas se solventaron de forma automática, cumpliendo con el objetivo del mejoramiento del sistema operativo de servidor, reduciendo las reglas que podrían ser consideradas vulnerables dentro del sistema y se observa en la Figura 3.89.

Ensure mounting of cramfs filesystems is disabled	unknown	pass
Ensure mounting of freevxfs filesystems is disabled	unknown	pass
Ensure mounting of jffs2 filesystems is disabled	unknown	pass
Ensure mounting of hfs filesystems is disabled	unknown	pass
Ensure mounting of hfsplus filesystems is disabled	unknown	pass
Ensure mounting of udf filesystems is disabled	unknown	pass

Figura 3.89 Reglas solventadas dentro del sistema operativo de servidor

La siguiente regla que fue solventada, ver la Figura 3.90. se la realizó bajo el criterio de configuración basada en el conjunto de archivos que van a impedir que los usuarios puedan ejecutar programas desde el disco compartido y así disminuir la introducción de *softwares* malicioso dentro del sistema. Se observa en la Figura 3.84. presentándose como una regla corregida de forma automática al aplicar la política de seguridad.

Ensure noexec option set on /tmp partition	unknown	pass
--	---------	------

Figura 3.90 Regla de la opción *noexec* solventada en la partición

En la Figura 3.85. mostrada en el apartado anterior, como una regla que si no se la tiene activa mediante su utilidad puede conducir a que un *malware* basado en *USB* sea un mecanismo fácil para la infiltración, una vez implementado la política de seguridad se observa que esta regla ha sido solventada. En la Figura 3.91. se evidencia que ha sido solventada de forma automática cumpliendo con el objetivo de mejoramiento en el sistema operativo.

Disable USB Storage	unknown	pass
---------------------	---------	------

Figura 3.91 Regla de almacenamiento *USB* desactivada

En la Figura 3.86. del apartado anterior se muestra una regla que permitiría asegurarse que los comandos sudo utilicen *pty*, al aplicar la política de seguridad se ha solventado de forma automática y se la observa en la Figura 3.92. siendo un parámetro de mejoramiento y endurecimiento en nuestro sistema de servidor.

Ensure sudo commands use pty	unknown	pass
------------------------------	---------	------

Figura 3.92 Regla solventada para la utilización de comandos sudo usen *pty*

Parámetros que no se corrigieron de forma automática solventados manualmente

En base al manual que proporciona el marco de referencia *CIS Benchmark*, se puede corregir diferentes parámetros o reglas que el sistema operativo de servidor después de aplicar la política de seguridad no logró solventar. Se los puede corregir de forma manual siguiendo la aplicación de comandos que la guía establece a cada una de las reglas de forma específica.

Corrección de primera regla de forma manual

Se observa en la Figura 3.93. la regla que se va a corregir de forma manual siguiendo los pasos y agregación de comandos en base a la guía que establece *CIS Benchmark*, observándose en la Figura 3.94. teniendo la descripción de la regla en la Tabla 3.1 el tipo de severidad, resultado y descripción.

Ensure AIDE is installed	unknown	fail
--------------------------	---------	------

Figura 3.93 Regla a ser corregida *Ensure AIDE is installed*

Tabla 3.1 Descripción de la regla *Ensure AIDE*

<i>Ensure AIDE is installed</i>	
ID Regla	<i>xccdf_com.ubuntu.focal.cis_rule_CIS-1.4.1</i>
Resultado	Fail
Severidad	Alta
Descripción	Realiza una captura o foto instantánea del estado del sistema de archivos, incluido el tiempo en horas de modificación, los permisos y los <i>hash</i> de los archivos, que puede utilizarse para compararlos con el estado actual del sistema de archivos y detectar modificaciones en el sistema AIDE

Luego de haber identificado y leído la descripción de la regla que no se solventó, se procede a buscar en la guía proporcionada por *CIS Benchmark* el detalle a seguir para poder solventar esta regla siguiendo el proceso que se observa en la Figura 3.94.

Install AIDE using the appropriate package manager or manual installation:

```
# yum install aide
# dnf install aide
# apt-get install aide
# zypper install aide
# emerge aide
```

Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options.

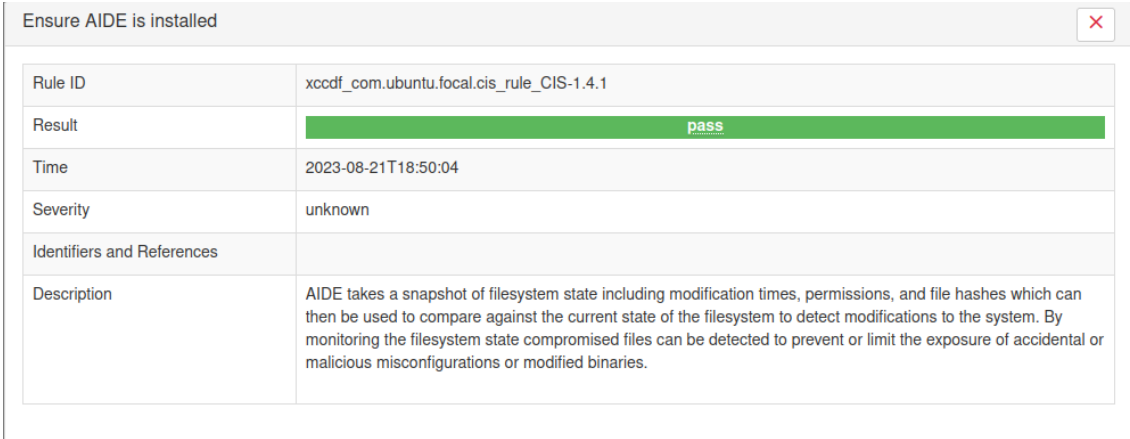
Initialize AIDE:

```
# aide --init
```

Figura 3.94 Guía que permite solventar regla de manera manual proporcionada por *CIS Benchmark*

Para la aplicación de esta regla se elige la adecuada en base al sistema operativo que se está utilizando, para la aplicación del sistema Ubuntu Server 20.04 el cual se está utilizando se aplicó el comando ***apt-get install aide***.

En la Figura 3.95. se muestra a la regla *Ensure AIDE* como solventada o corregida.



Rule ID	xccdf_com.ubuntu.focal.cis_rule_CIS-1.4.1
Result	pass
Time	2023-08-21T18:50:04
Severity	unknown
Identifiers and References	
Description	AIDE takes a snapshot of filesystem state including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system. By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

Figura 3.95 Regla corregida *Ensure AIDE is installed*

Corrección de segunda regla de forma manual

El análisis y corrección de la regla número dos es similar a la corrección de forma manual de la regla uno, siguiendo los pasos y agregación de comandos en base a la guía que

establece el marco de referencia *CIS Benchmark*. De igual forma en la Figura 3.6. se muestra la regla a corregir y se la observa como regla fallida.

Ensure filesystem integrity is regularly checked	unknown	fail
--	---------	------

Figura 3.96 Regla a corregir *Ensure filesystem integrity is regularly checked*

La Tabla 3.2 muestra la descripción de la regla fallida, en donde se procede a realizar la corrección respectiva mediante la guía de *CIS Benchmark*.

Tabla 3.2 Descripción de la regla *Ensure filesystem integrity is regularly checked*

<i>Ensure filesystem integrity is regularly checked</i>	
ID Regla	<i>xccdf_com.ubuntu.focal.cis_rule_CIS-1.4.2</i>
Resultado	<i>Fail</i>
Severidad	<i>Alta</i>
Descripción	Comprobación periódica de la integridad del sistema es necesario detectar los cambios dentro del sistema.

Luego de haber identificado y leído la descripción de la regla que no se solventó, se procede a buscar en la guía proporcionada por *CIS Benchmark* el detalle a seguir para solventarla, siguiendo el proceso que se observa en la Figura 3.957.

Run the following command:

```
# crontab -u root -e
```

Figura 3.957 Guía para solventar regla de forma manual proporcionada por CIS Benchmark

La Figura 3.968. muestra a la regla *Ensure filesystem integrity is regularly checked* como solventada o corregida. Cabe mencionar que se puede corregir todas las reglas que se presentan como fallidas dentro del sistema operativo de servidor, debido a que *CIS Benchmark* presenta un manual para las reglas que se ejecutan dentro del sistema. En base a las necesidades se puede ir resolviendo una a una las reglas que se vea conveniente.

Ensure filesystem integrity is regularly checked	
Rule ID	xccdf_com.ubuntu.focal.cis_rule_CIS-1.4.2
Result	pass
Time	2023-08-21T18:50:04
Severity	unknown
Identifiers and References	
Description	Periodic checking of the filesystem integrity is needed to detect changes to the filesystem.

Figura 3.968 Regla corregida *Ensure filesystem integrity is regularly checked*

Consecuentemente se realiza un nuevo proceso de escaneo y se muestra una reducción de vulnerabilidad del **94.71 %** en la Figura 3.9. en comparación al reporte generado en la Figura 3.88.

Compliance and Scoring

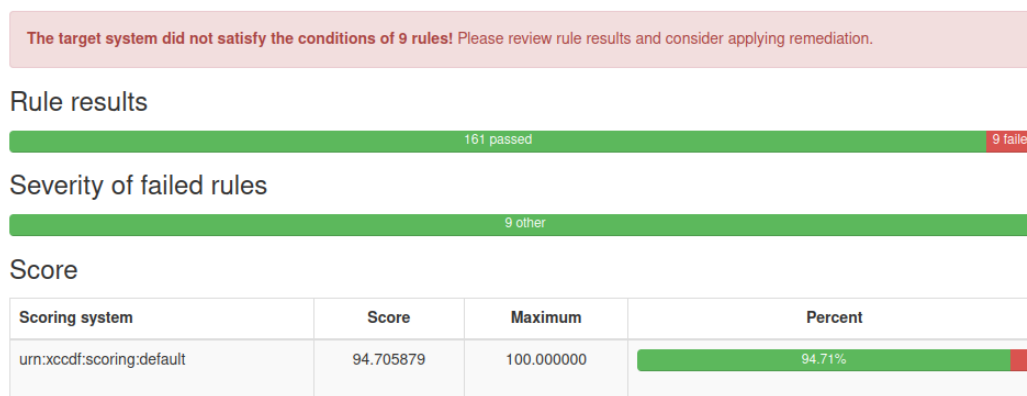


Figura 3.99 Nuevo reporte generado solventando reglas de forma manual

El nuevo reporte generado evidencia que la agregación de forma manual se realizó de forma correcta siguiendo los parámetros de modificación y corrección de reglas que no cumplieran con el nivel de seguridad, en base al marco de referencia CIS.

3.4 Verificación del *hardening* del servidor con base a los elementos de la triada CIA

Verificación de reglas de la triada CIA severidad alta

Los parámetros principales de la triada CIA enfocan su análisis en sus tres principios esenciales, para ello la verificación de *hardening* en el sistema operativo de servidor

implica verificar y evidenciar la ejecución de las medidas de seguridad que se implementaron en base al marco de referencia CIS.

En base a la Tabla 3.3, que se presenta a continuación se verifica y se establece un nivel de impacto en base a la triada CIA. Se muestran como reglas corregidas dentro del sistema operativo de servidor, implementando políticas de seguridad en base al marco de referencia CIS, ver Tabla 3.4 que corresponden a las reglas de vulnerabilidades corregidas por medio de la aplicación de políticas de seguridad en el sistema operativo de servidor.

Tabla 3.3 Parámetros de la triada CIA, severidad alta

No	Confidencialidad	Integridad	Disponibilidad
1	Alta	Alta	Baja
2	Alta	Alta	Media
3	Alta	Alta	Media
4	Media	Alta	Media

Tabla 3.4 Reglas que se corrigieron mediante el ingreso de las políticas de seguridad para aplicar *hardening*, severidad alta

ALTA			
No	Nombre	Descripción	Resultado
1	<i>Ensure mounting of cramfs filesystem is disabled</i>	Tipo de archivo Linux comprimido de lectura de tamaño reducido integrado en los sistemas.	PASS
2	<i>Ensure mounting of freevxfs filesystem is disabled</i>	Versión libre tipo Veritas. Es el tipo de sistema de archivo principal HP-UX de sistemas operativos servidor.	PASS
3	<i>Ensure mounting of jffs2 filesystems is disabled</i>	La estructura de registro utilizado en dispositivos de memoria <i>flash</i> en sistema de archivos que se vaya a trabajar.	PASS
4	<i>Ensure mounting of hfs filesystems is disabled</i>	Permite montar sistemas de archivos Mac OS en sistema de archivos jerárquico con funcionalidad activa.	PASS

En la Tabla 3.4 se muestran algunas de las reglas que se corrigieron mediante el ingreso de las políticas de seguridad para aplicar *hardening* y presentaron un nivel alto de

vulnerabilidad o severidad al generar el reporte de vulnerabilidades, cabe mencionar que estas reglas basan su análisis de la Triada CIA haciendo referencia a las reglas expuestas en la Tabla 3.3.

Verificación de reglas de la triada CIA severidad media

El análisis de las reglas que se solventaron con un nivel medio implica un análisis en base la triada CIA que va a enfocar su análisis en los tres principios esenciales que son la Confidencialidad, Integridad y Disponibilidad.

En base a la Tabla 3.5. que se presenta a continuación se verifica y se establece un nivel de impacto en base a la triada CIA.

Tabla 3.5 Parámetros de la triada CIA, severidad media

No	Confidencialidad	Integridad	Disponibilidad
1	Alta	Baja	Alta
2	Alta	Alta	Media
3	Alta	Media	Media
4	Media	Alta	Media

Tabla 3.6 Reglas que se corrigieron mediante el ingreso de las políticas de seguridad para aplicar *hardening*, severidad media

MEDIA			
No	Nombre	Descripción	Resultado
1	<i>Disabled USB Storage</i>	Permite proporcionar un medio para transferir y almacenar archivos asegurando su persistencia y disponibilidad independientemente del estado de la conexión a la red	PASS
2	<i>Ensure sudo commands use pty</i>	Sudo puede ser configurado para ejecutar solo desde un <i>psuedo-pty</i>	PASS
3	<i>Ensure sudo log file exist</i>	Puede utilizar un archivo de registro personalizado <i>sudo</i>	PASS
4	<i>Ensure filesystems integrity is regularly checked</i>	Comprobación periódica de integridad del sistema, ayuda a detectar cambios en el sistema.	PASS

En la Tabla 3.6. se muestran algunas de las reglas que se corrigieron mediante el ingreso de las políticas de seguridad para aplicar *hardening* y presentaron un nivel medio de vulnerabilidad o severidad al generar el reporte de vulnerabilidades. Cabe mencionar que estas reglas basan su análisis de la Triada CIA haciendo referencia a las reglas expuestas en la Tabla 3.5.

Verificación de reglas de la triada CIA severidad baja

El análisis de las reglas que se solventaron con un nivel bajo implica un análisis en base la triada CIA que va a enfocar su análisis en los tres principios esenciales que son la Confidencialidad, Integridad y Disponibilidad.

En base a la Tabla 3.7. que se presenta a continuación se verifica y se establece un nivel de impacto en base a la triada CIA

Tabla 3.7 Parámetros de la triada CIA, severidad baja

No	Confidencialidad	Integridad	Disponibilidad
1	Alta	Alta	Media
2	Alta	Media	Baja
3	Alta	Media	Baja
4	Alta	Alta	Media

Tabla 3.8 Reglas que se corrigieron, severidad baja

BAJA			
No	Nombre	Descripción	Resultado
1	<i>Ensure no duplicate GIDs exist</i>	Asignar a los grupos de usuarios GIDs únicos para garantizar la responsabilidad y protecciones apropiadas de acceso	PASS
2	<i>Ensure no duplicate usernames exist</i>	<i>Es posible que un administrador pueda editar y cambie el nombre de usuario de forma manual</i>	PASS
3	<i>Ensure no duplicate group names exist</i>	<i>Es posible que un administrador pueda editar y cambie el nombre del grupo de forma manual</i>	PASS
4	<i>Ensure shadow group is empty</i>	Atacantes pueden acceder a archivos de lectura para ejecutar programas de descifrados de contraseñas y descifrar las contraseñas que se encuentran cifradas.	PASS

Guía de buenas prácticas para un sistema operativo de servidor endurecido

El fortalecer el sistema operativo de servidor es una forma de aplicar normas y reglas que están sujetas a un marco de referencia, en este caso es el marco de referencia CIS. De esta forma se disminuyen las vulnerabilidades que puede presentar un sistema operativo de servidor, reduciendo también la exposición a diferentes ataques y minimizando las brechas que presentan los sistemas operativos en temas de seguridad.

Es por ello que se presenta una guía de buenas prácticas para un sistema operativo de servidor.

1. Establecer un análisis profundo de la importancia que va a permitir implementar *hardening* dentro de un sistema operativo de servidor para reducir y proteger al sistema de vulnerabilidades que puede estar expuesto.
2. Priorizar los distintos riesgos que puede estar expuesto el sistema operativo de servidor y realizar un proceso de escaneo de vulnerabilidades mediante el uso de herramientas que cumplan un marco de referencia de ciberseguridad.
3. Elegir de forma correcta el *software* de virtualización que tenga buenas prestaciones para la ejecución del sistema operativo de servidor siendo una ayuda para la implementación de *hardening*.
4. Al momento de realizar la instalación del sistema operativo de servidor con el que se desee trabajar agregar nombres de usuarios y contraseñas robustas para que de esta forma delimitar el acceso indebido a personas no autorizadas.
5. Iniciar el sistema operativo agregando comandos de actualización a paquetes de versiones recientes o actuales, instalación de características de seguridad y corrección de errores que pueda presentar el sistema.
6. Acceder en modo *root* o privilegiado para el ingreso de comandos por medio de consola.
7. Realizar periódicamente procesos de escaneo para monitorear el sistema por medio de las herramientas de verificación de vulnerabilidades, aplicando políticas de seguridad en base al marco de referencia *CIS Benchmark* de preferencia.
8. Corregir de forma automática o manual las reglas o vulnerabilidades que presente el sistema para reducir aún más el nivel de inseguridad que presente el sistema.
9. Configurar y deshabilitar servicios innecesarios o que no se utilicen dentro del sistema.

10. Acceder a los *logs* de *CIS Benchmark* para configurar parámetros como acceso a usuarios específicos, limitar el número de intentos fallidos al ingresar al sistema operativo de servidor, tiempo de duración corto para bloqueo automático al estar inactivo la máquina virtual.
11. Realizar de forma periódica campaña de socialización al personal de una entidad y concientizar a las personas del buen uso de prácticas de seguridad de un sistema operativo de servidor.

Guía de buenas prácticas en servidor de correo endurecido

Al igual que el fortalecimiento en el sistema operativo de servidor también en un servidor de correo es importante aplicar normas y reglas que están sujetas a un marco de referencia que en este caso es el marco de referencia CIS. De esta forma se reducen las vulnerabilidades que puede presentar un sistema operativo de servidor, a continuación, se presenta una guía de buenas prácticas que permitirá mantener de forma segura y reducir el aumento de vulnerabilidades dentro del servidor.

1. Analizar y determinar la importancia que del uso del servidor de correo y e proceso de endurecimiento del mismo.
2. Utilizar versiones actuales tanto en el sistema operativo de servidor como en el servidor de correo.
3. Realizar el proceso de actualización dentro del sistema por medio de los comandos *update* y *upgrade*.
4. Usar TLS/SSL en el servidor de correo para comunicarse de forma segura con diferentes servidores de correo.
5. Restringir los servicios que no se vayan a utilizar al igual que los protocolos que no se usen en el servidor de correo.
6. Agregar políticas de seguridad en base al marco de referencia *CIS Benchmark*.
7. Agregar usuarios con nombres que sea difícil de usar de forma indebida por persona no autorizadas.
8. Crear contraseñas robustas, incluyendo caracteres especiales y letras mayúsculas, generando contraseñas fuertes evitando el robo de información.
9. Establecer políticas claras sobre el uso aceptable del servidor de correo.
10. Educar a los usuarios sobre la seguridad de correo electrónico y las amenazas comunes.

4. CONCLUSIONES

- El uso de sistemas operativos Linux de base Debian, por ser un sistema de código abierto, va a estar expuesto a manipulación indebida por distintos niveles de expertos y desarrolladores de seguridad. Debido a esto es necesario que se audite, examinen y realicen correcciones en las reglas que no cumplan con el marco de referencia *CIS*. Por tal motivo es importante endurecer de manera estructurada el sistema operativo de servidor.
- Conforme avanzan las actualizaciones en los sistemas operativos Linux de base Debian, estos requieren nuevas bibliotecas y repositorios que permiten ejecutar tareas específicas como niveles de seguridad, compatibilidad dentro del *hardware* para un rendimiento eficaz con nuevos entornos. Es por ello que se utilizó el sistema operativo Linux de base Debian Ubuntu Server 20.04 que es una versión que permite emplear el acceso a los repositorios de Ubuntu Pro *CIS Benchmark* para la aplicación de *hardening* dentro del sistema operativo, versiones anteriores a esta no permiten aplicar estos repositorios. Además, es un entorno que requiere menos recursos físicos como espacio en disco duro y memoria *RAM* de la máquina física al no poseer una máquina de buenas prestaciones, no se utilizó versiones actuales como la versión 23.04 debido a que no permite levantar el servidor de correo de *Postfix* y requiere mayores recursos en la *PC*.
- El proceso de escaneo de vulnerabilidades realizado dentro de un sistema operativo de servidor recién instalado mostró un alto porcentaje de reglas que no cumplen con el marco de referencia *CIS*. Concluyendo que al momento de tener un servidor se debe agregar una política de seguridad para el endurecimiento del mismo y así evitar la manipulación del sistema por personas no autorizadas y ataques en el sistema.
- En el acceso a herramientas de Ubuntu Pro, que tiene privilegios de funcionalidad para aplicar parámetros de seguridad de nivel uno, es importante hacer uso de estos recursos para realizar e implementar *hardening* dentro de un sistema operativo de servidor.
- La aplicación del marco de referencia *CIS* permite establecer niveles de seguridad y cumplir con guías de buenas prácticas en los sistemas operativos de servidor, para que de esta forma se vea reducido de gran manera el servidor. Esto viene a ser una garantía que tiene el administrador del sistema frente a distintos ataques y amenazas que día a día evoluciona en el ciber espacio.

- Levantar un servidor de correo *Postfix* mediante *Squirrelmail* permite la comunicación rápida y eficaz entre usuarios para enviar y recibir correos electrónicos dentro de una entidad para una interacción fluida y efectiva entre usuarios.
- El servidor de correo *Postfix* mediante *Squirrelmail* permite una configuración sencilla y amigable con el usuario, facilita la agregación de políticas de seguridad que permitirán establecer parámetros sólidos protegiendo a los datos que se envían por medio de los correos electrónicos.
- La generación de archivos que contenga información importante como detalle de datos, porcentajes y tipos de vulnerabilidades se redireccionó a un sistema operativo con interfaz gráfica, *Ubuntu Desktop 20.04*, con esto se consiguió una visualización idónea de los datos generados y en base a un análisis correcto se determinaron los parámetros de seguridad a solventar siguiendo la guía del marco de referencia CIS.
- Utilizar herramientas de escaneo como *OpenSCAP* permite la generación de informes detallados con la identificación de vulnerabilidades dentro del sistema operativo de servidor, teniendo compatibilidad con el estándar de seguridad *CIS*. Se obtuvieron datos claros y precisos del tipo de reglas que no se solventaron de forma automática, facilitando al administrador la correcta aplicación de niveles de seguridad.
- El acceso a los beneficios de *Ubuntu Pro* permite la obtención de un *token* que dará acceso a las utilidades de niveles de seguridad de hasta cinco máquinas virtuales, que se desarrollen con fines de educativos.
- El análisis correcto de los reportes de vulnerabilidades antes de implementar políticas seguridad y después de aplicar las políticas de seguridad van a permitir determinar el nivel de porcentaje de vulnerabilidades que presenta el servidor. En base a los reportes generados se corrigieron los parámetros que el marco de referencia recomienda, siendo este proceso el idóneo para tomar medidas de seguridad adecuadas.
- Al implementar las políticas de seguridad de forma automática existen algunos parámetros que deben ser corregidos o solventados de forma manual. Debido al alto nivel de severidad que son consideradas algunas reglas, las actualizaciones del sistema no son suficientes para corregir dicho problema, es por ello que en base a la guía que *CIS* ofrece se pueden solventar los parámetros que presenta el sistema de forma manual.

- La implementación de *hardening* en el entorno Ubuntu Server 20.04 requiere de un conocimiento más amplio, ya que la agregación de políticas de seguridad se lo debe realizar por medio de líneas de comando, siendo un entorno difícil de descifrar para cualquier persona que quiera acceder al sistema sin autorización o de forma indebida. Esto es una ventaja en nivel de seguridad a diferencia de un entorno gráfico que se tornaría fácil de entender y descifrar las utilidades del sistema.
- El presente proyecto muestra una guía completa del proceso de implementación de *hardening* en el sistema operativo de servidor Ubuntu Server 20.04 desde la instalación del sistema operativo, levantamiento de servidor de correo *Postfix* mediante *Squirrelmail* hasta la corrección de forma manual de políticas de seguridad en base al marco de referencia *CIS Benchmark*. Esto servirá como una guía para el desarrollo e implementación de *hardening*. Siguiendo los estándares de buenas prácticas.
- Es importante garantizar la funcionalidad y seguridad de los datos dentro de un sistema operativo de servidor creando entornos confiables y resistentes a distintos ataques cibernéticos; es por ello que la aplicación de los parámetros de la triada CIA implica un factor importante al momento de endurecer el sistema operativo.

5. RECOMENDACIONES

- Evaluar y analizar de forma idónea el uso del *software* de virtualización que se va a usar en el desarrollo del proyecto, en base a los requerimientos y especificaciones que tendrá cada máquina virtual dependiendo de los recursos que posee la computadora física.
- Investigar si el sistema operativo de servidor a ser utilizado cumple con las actualizaciones para acceder a distintas herramientas. Si se utilizan versiones antiguas que no cumplan con actualizaciones va a ser imposible acceder a herramientas necesarias generando problemas para la obtención de los resultados adecuados.
- Es recomendable usar una computadora con un espacio de disco duro de al menos 20 (GB) disponibles para la implementación de las máquinas virtuales al igual que un tamaño mínimo de 8 (GB) de memoria RAM. Esto debido al alto consumo de recursos que genera el usar hasta 3 o 4 máquinas virtuales dentro del *software* de virtualización *VMware Workstation Pro 16.1.2*.

- Es recomendable antes de empezar la instalación de cualquier servicio o paquetes darle una actualización al sistema operativo de servidor para que los paquetes complementarios a dichas herramientas se instalen y sean compatibles para poder ejecutar los comandos necesarios, esto se lo puede realizar mediante los comandos *update* y *upgrade*.
- Se recomienda realizar el proceso de suscripción en Ubuntu Pro para acceder a las herramientas de configuración y aplicación en distintos niveles de seguridad. Mediante esto se logra obtener algunas reglas protegen al sistema de ataques cibernéticos e implementan *hardening* de forma correcta.
- Para obtener reportes de vulnerabilidades que genera Ubuntu Server 20.04 solo mediante líneas de código es recomendable transferir los archivos generados a una máquina virtual con interfaz gráfica, obteniendo una visibilidad adecuada y entendible al usuario para el análisis respectivo y toma de decisiones adecuadas para la implementación y corrección de vulnerabilidades.
- Después de aplicar las políticas de seguridad de *CIS Benchmark*, en el sistema operativo de servidor Ubuntu Server 20.04, al momento de instalar el servidor de correo en *Postfix* se recomienda agregar un nombre de dominio que haga referencia al proyecto de titulación, para que al momento de enviar correos sea fácil de recordar dicho nombre de dominio y se envíen de forma correcta los correos.
- Antes de agregar políticas de seguridad en el sistema operativo de servidor cuando se verifique el funcionamiento del servidor de correo de *Postfix* en *Squirrelmail* al agregar los usuarios de envíos y recepción de correos se recomienda usar contraseñas de nivel bajo, para luego tener una comparativa clara cuando se agregue la política de seguridad y agregar un usuario con contraseñas robustas.
- Para la modificación y corrección de las reglas fallidas de forma manual, se recomienda el uso correcto del manual que proporciona *CIS Benchmark* para la aplicación de reglas siguiendo el orden y estructura que expone en el documento.
- Al momento que ya no se vaya a utilizar una máquina virtual y después de cada implementación, se recomienda no apagar de forma completa las máquinas virtuales debido a que en ciertas instancias las modificaciones que se vayan realizando no se guardaran, generando de esta forma errores o datos incorrectos en la implementación, lo recomendable es dejarle a cada máquina virtual en modo suspensión y así reanudar con las modificaciones.

6. REFERENCIAS BIBLIOGRÁFICAS

- [1] smartekh, «smartekh.com,» [En línea]. Available: <https://blog.smartekh.com/que-es-hardening>. [Último acceso: 10 05 2023].
- [2] ciset.es, «www.ciset.es,» [En línea]. Available: <https://www.ciset.es/publicaciones/blog/746-hardening#:~:text=El%20Hardening%20consiste%20en%20el,de%20vulnerabilidades%20en%20el%20sistema..> [Último acceso: 10 05 2023].
- [3] openwebinars, «openwebinars.net,» [En línea]. Available: <https://openwebinars.net/blog/triangulo-de-seguridad-informatica-que-es-y-sus-objetivos/>. [Último acceso: 10 05 2023].
- [4] fp.uoc.fje.edu, «fp.uoc.fje.edu,» [En línea]. Available: <https://fp.uoc.fje.edu/blog/que-es-un-sistema-operativo-para-servidor/>. [Último acceso: 10 05 2023].
- [5] ucloudglobal, «ucloudglobal.com,» [En línea]. Available: <https://ucloudglobal.com/blog/sistema-operativo-de-servidores/>. [Último acceso: 10 05 2023].
- [6] debian.org, «www.debian.org,» [En línea]. Available: <https://www.debian.org/derivatives/index.es.html>. [Último acceso: 10 05 2023].
- [7] debian.org, «www.debian.org,» [En línea]. Available: <https://www.debian.org/releases/jessie/i386/ch03s04.html.es>. [Último acceso: 10 05 2023].
- [8] debian.org, «www.debian.org,» [En línea]. Available: https://www.debian.org/intro/why_debian.es.html. [Último acceso: 10 05 2023].
- [9] ciberseguridad, «ciberseguridad.blog,» [En línea]. Available: <https://ciberseguridad.blog/10-herramientas-para-escanear-vulnerabilidades-web/>. [Último acceso: 10 05 2023].

[10] mancomun.gal, «www.mancomun.gal,» [En línea]. Available:
<https://www.mancomun.gal/es/artigo-tic/scap-35-usando-openscap/>. [Último
acceso: 10 05 2023].

[11] es.slideshare.net, «es.slideshare.net,» [En línea]. Available:
<https://es.slideshare.net/LuisFerAguas/9unidad-3-marcos-de-referencia-para-seguridad-de-la-informacin-31-iso-27000>. [Último acceso: 05 10 2023].

