AUDITORIA EN SEGURIDAD INFORMÁTICA DE SERVIDOR UBUNTU 14.04 PARA CONTROLAR VULNERABILIDADES EN CONFIGURACIÓN POR DEFECTO

JEISON SNEIDER CABEZA SEGURA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD CÚCUTA
2018

AUDITORIA EN SEGURIDAD INFORMÁTICA DE SERVIDOR UBUNTU 14.04 PARA CONTROLAR VULNERABILIDADES EN CONFIGURACIÓN POR DEFECTO

JEISON SNEIDER CABEZA SEGURA

Monografía para optar al título de Especialista en Seguridad Informática

Director: Ing. JULIO ALBERTO VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD CÚCUTA
2018

Nota de Aceptación

_____
Firma del Decano de la Facultad

_____
Firma del primer jurado

_____
Firma del segundo jurado

Bogotá, D.C., febrero de 2018

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

Ing. Julio Alberto Vargas, director del proyecto por las orientaciones dadas, las cuales aportaron al desarrollo del documento de grado.

A todas aquellas personas que de una u otra forma han colaborado en la elaboración de este proyecto.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

Este trabajo proporciona una serie de controles a aplicar para mitigar el riesgo presente en la configuración por defecto de la distribución Linux Ubuntu 14.04, teniendo en cuenta que las configuraciones por defecto de esta distribución son vulnerables debido a ciertos parámetros inherentes en sus configuraciones iniciales.

Utilizando la herramienta Lynis se realizó un análisis de las vulnerabilidades encontradas en las configuraciones por defecto de la distribución Ubuntu 14.04, habiendo identificado estos riesgos se procedió a realizar un análisis de los mismos utilizando como referencia la metodología magerit para establecer el nivel del riesgo en el cual se encuentra la distribución Linux analizada.

Teniendo claros los riesgos presentes en la distribución Linux Ubuntu 14.04 y habiendo cuantificado los riesgos para conocer el nivel de exposición en el que se encuentra el sistema, se determinan y establecen controles necesarios para mitigar el nivel de riesgo. Con los controles aplicados se realiza nuevamente el análisis de vulnerabilidades con la herramienta Lynis para corroborar que el nivel de exposición de las configuraciones del servidor se haya reducido, con lo cual se puede realizar un análisis general de la eficiencia de los controles aplicados y determinar una serie de recomendaciones para las personas que utilizan esta distribución.

Palabras claves: Ubuntu 14.04, Vulnerabilidades, Nivel de riesgo, Control.

INTRODUCCIÓN

A través de los últimos años se ha hecho más frecuente y común el tema de seguridad informática, los virus conocidos en los años actuales han provocado en la sociedad y en la industria que interactúa con diversas tecnologías la necesidad de sentirse protegidos de posibles ataques informáticos.

Los sistemas operativos y los servicios que se ejecutan en ellos en ocasiones presentan diversos parámetros que pueden exponer el sistema a un posible ataque debido a que las personas que realizan dichas irrupciones aprovechan las vulnerabilidades que pueda presentar dichos sistemas como una puerta de entrada para afectar directamente una organización y/o realizar actos ilícitos.

Teniendo en cuenta el aumento de ataques informáticos, es necesario que los diferentes sistemas sean lo más confiables posible en cuanto a seguridad se refiere, además es de gran importancia contar con acceso a documentos que aborden temas de seguridad en las distintas tecnologías y distribuciones de sistemas operativos existentes.

Con el presente trabajo se busca exponer las vulnerabilidades presentes en la distribución Linux Ubuntu 14.04 en cuanto a sus configuraciones por defecto y establecer controles pertinentes para reducir el nivel de exposición inherente a esas configuraciones.

1. PLANTEAMIENTO DEL PROBLEMA

Las configuraciones por defecto de un sistema operativo contienen vulnerabilidades conocidas por los delincuentes informáticos, estas proporcionan un punto de partida para establecer posibles víctimas de sus ataques. Teniendo en cuenta lo anterior, es de gran importancia tener claridad de las vulnerabilidades de estos sistemas y los controles que se deben tomar para mitigar el riesgo presente en las configuraciones por defecto del servidor que se maneja.

Si bien se sabe que el sistema operativo Linux proporciona un grado mayor de seguridad, esto no es suficiente para estar a salvo de algún ataque malintencionado, concretamente la distribución Ubuntu ha tenido un crecimiento en su aceptación y uso como servidor, por tal razón se necesita otorgar un nivel de confianza alto que no se puede brindar con las configuraciones por defecto, ya que sus vulnerabilidades son reveladas y/o descubiertas paulatinamente, por lo anterior surge el interrogante ¿Qué configuraciones por defecto del servidor Ubuntu 14.04 representan los mayores riesgos en cuanto a seguridad se refiere?

2. JUSTIFICACIÓN

Teniendo en cuenta la proyección de los servidores Linux distribución Ubuntu en cuanto a su uso es necesario conocer sus vulnerabilidades en lo referente a su configuración por defecto, para así determinar controles a implementar y esto permitirá tener un sistema robusto y con riesgos controlados en cuanto a sus configuraciones iniciales.

Comúnmente no se conocen los riesgos a los que se está expuesto al trabajar con la distribución Linux Ubuntu ya que Linux se asocia siempre con seguridad en comparación con el sistema operativo Windows. Por lo anterior se requiere una síntesis teórica sobre las características adicionales a tener en cuenta al momento de trabajar con estos servidores para lograr establecer controles adecuados que proporcionen un sistema con el menor índice de riesgo posible frente a ataques de los que pueden ser víctimas, en el caso de este proyecto se pretende referenciar la distribución Linux Ubuntu 14.04.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Establecer los controles necesarios aplicables a la distribución Linux Ubuntu 14.04 para una disminución del riesgo de exposición frente a vulnerabilidades identificadas en su configuración por defecto

3.2 OBJETIVOS ESPECÍFICOS

- Determinar las vulnerabilidades en configuraciones por defecto presentes en la distribución Ubuntu versión 14.04 para la posterior aplicación de controles pertinentes.

- Documentar pruebas realizadas sobre ataques al servidor Ubuntu 14.04 en su configuración por defecto.

- Determinar controles pertinentes para mitigar los riesgos encontrados en las configuraciones por defecto del servidor Ubuntu 14.04 con base en el análisis de los riesgos y las pruebas documentadas.

- Describir paso a paso el proceso de aplicación de los controles determinados para controlar vulnerabilidades en configuraciones por defecto del servidor Ubuntu 14.04.

4. MARCO REFERENCIAL

4.1 ESTADO DEL ARTE

Para desarrollar este proyecto de investigación se realiza una indagación sobre proyectos similares que hayan sido desarrollados sobre el tema, buscando contextualizar este trabajo en el ámbito propuesto.

Como resultado de la exploración se han encontrado investigaciones que se asemejan en cuanto al análisis de riesgo que realizan a sistemas informáticos completos, en los cuales la seguridad en servidores Linux (Ubuntu) solo hace parte de una mención de aspectos a tener en cuenta, este es el caso de una evaluación de riesgos y vulnerabilidades presentes en la infraestructura de red de la editorial Don Bosco de Ecuador, realizado por Cristina Jaramillo y Juan Riofrío.[1]

Otro de los resultados que se puede asemejar en ciertos aspectos es un análisis del crecimiento y los cambios del sistema operativo Ubuntu[2], que, aunque si bien no proporciona mayor información en cuanto a las vulnerabilidades de estos servidores permite familiarizarse con las mejoras que ha tenido el servidor Ubuntu versión 14.04 con respecto a las anteriores versiones.

A nivel nacional no se han elaborado investigaciones enfocadas en las vulnerabilidades presentes en la distribución Linunx Ubuntu 14.04 en sus configuraciones por defecto.

[1] JARAMILLO CASTILLO C.M && RIOFRIO HERRERA J.C. Metodología para realizar la evaluación, detección de riesgos, vulnerabilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la editorial Don Bosco, mediante un test de intrusión de caja blanca. Universidad Politécnica Salesiana Ecuador: Sede Cuenca,. 2015. [En línea], [consultado el 23 de enero de 2018]. Disponible en: http://dspace.ups.edu.ec/handle/123456789/7910

[2] TABASSUM, M. Análisis de la evolución del software de Linux OS (Ubuntu). Ciencias de la Computación y Tecnología (ICCST). Editorial: IEEE. 28 Agosto del 2014. Kota Kinabalu–Malasia. [En línea], [consultado el 23 de enero de 2018].Disponible en: http://ieeexplore.ieee.org/xpl/article Details .jsp? arnumber=7045194

4.2 MARCO TEÓRICO

Un servidor se puede definir a nivel de software o hardware, cómo un software ofrece un servicio que otros programas pueden usar en red o a nivel local, en hardware se puede definir como un dispositivo en el cual funcionan otros programas además del sistema operativo.

4.2.1. Servidor Ubuntu. Los sistemas operativos GNU/Linux tienen como principal característica que son basados en software libre, es decir, que el usuario tiene libertad de manipular el código del software y esto lleva inherente grandes ventajas como mejora y personalización del mismo.
Al contar con tantos usuarios trabajando en un mismo objetivo (código) se obtiene un sistema con características de funcionalidad como:

- Escalabilidad
- Disponibilidad
- Rendimiento
- Seguridad
- Administrabilidad dedicadas a configuraciones centralizadas y automatizadas.
- Facilidad de Uso
- Adaptabilidad
- Asequible

Ubuntu server hace parte de una de las distribuciones de Linux basada en Debían. Es un sistema operativo de código abierto, su demanda ha ido aumentando exponencialmente gracias a que cada vez es más amigable e intuitivo para usuarios medios. Gradualmente ha sido utilizada en mayor número en servidores llegando en la actualidad a estar entre los más usados en el mundo con una proyección de estar en los primeros lugares[3].

Aspectos relevantes por los cuales conviene elegir un servidor Ubuntu[4]:

- El padre de distribución Linux de Ubuntu es Debían. Debían, también conocida como Debían GNU / Linux, tiene un público fiel gracias a su estabilidad, su sistema de apt-get de envases y su compromiso con el software libre según la definición de la Free Software Foundation.

[3]METALBYTE. Debian sigue siendo la número uno en servidores. MuyLinux. 2013. [En línea], [consultado el 23 de enero de 2018].Disponible en: http://www.muylinux.com/2013/10/25/debian-sigue-numero-uno-en-servidores

[4]HESS KENETH. Ubuntu Server: The Linux Server Operating Systems Dark Horse. [En línea], [consultado el 23 de enero de 2018]. Disponible en: http://www.serverwatch.com/trends/article.php/3870141/Ubuntu-Server-The-Linux-Server-Operating-Systems-Dark-Horse.htm

- Ubuntu tiene una dedicación fuerte de desarrollo detrás de él y una comunidad mundial de colaboradores que trabajan juntos para actualizar y mantener sus actualizaciones de código y de seguridad. Esto aporta confianza ante bugs, fallos de seguridad y mejoras vendrán rápidamente y con regularidad para proteger sus sistemas y los datos que recogen y almacenan.

- Ubuntu cuenta con soporte 24x7 en caso de fallos o errores que requieren su ayuda gracias a la empresa Canonical ltd quien se encarga de estos procesos. Se puede confiar en la experiencia y respuesta rápida para aquellas cargas de trabajo de impacto crítica cuando más lo necesita.

- Ubuntu es fácil de instalar, mantener y actualizar. Puede completar la instalación en 25 minutos o menos en el hardware de clase servidor. Linux es estable y requiere poco mantenimiento o mantenimiento diario. Reiniciar el sistema rara vez es necesario, por lo que es la plataforma perfecta para aquellas aplicaciones y servicios de tiempo de inactividad cero. Ubuntu actualiza fácilmente desde la línea de comandos a través de un comando de actualización de la distribución.

4.2.2 Auditoria en seguridad informática. Una auditoría de seguridad es una evaluación sistemática de la seguridad del sistema de información determinando mediante la medición de lo bien que se ajusta a una serie de criterios establecidos. Una auditoría exhaustiva normalmente evalúa la seguridad de la configuración del sistema físico y el medio ambiente, el software, los procesos de manejo de la información, y las prácticas de los usuarios.

Las auditorías de seguridad no tienen lugar en el vacío; son parte del proceso de definir y mantener políticas de seguridad eficaces, establece procedimientos para todos los que usan los recursos informáticos en la organización de tal manera que su uso no representa un aumento en el riesgo. Cabe resaltar que en las auditorias de seguridad informática se analizan solamente los procesos concernientes a la seguridad física y lógica con énfasis en proteger la información, la anterior aclaración es la principal diferencia entre auditoria de seguridad informática y auditoria de sistemas, ya que la última está más enfocada a parámetros más administrativos[5].

[5] MARTÍNEZ J.E, GIRALDO C.A. Auditoria de seguridad informática. Password S.A. [En línea], [consultado el 23 de enero de 2018]. Disponible en: http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/ponencia_PASSWORD_siti2004.pdf

Uno de los aspectos más importante de la auditoria en seguridad informática y en general en cualquier auditoria es la organización, para esto es fundamental adoptar una metodología que proporcione un consecutivo de procesos a realizar para llevar a buen término la auditoría y garantizar que todos los aspectos requeridos se tuvieron en cuenta a cabalidad.

La metodología PHVA proporciona una consecución de procesos claros a implementar para desarrollar de una manera correcta, ordenada y eficiente un trabajo (auditoría), se compone de cuatro fases[6] (figura 1).

Figura 1. Metodología PHVA

Fuente: http://sinergiasong.org/cajasdeherramientas/prenatal/mejoramiento.html

[6] BOWEN RONDA. (2013). ¿Qué es el plan PHVA?. 13 de Julio del 2013. [En línea], [consultado el 23 de enero de 2018].Disponible en: http://www.brighthubpm.com/methods-strategies/73268-what-is-plan-do-check-act/

- **Planear**: Es en realidad un proceso de dos pasos. La primera etapa consiste en identificar y definir un problema existente dentro de un proceso. El segundo paso implica el análisis de este problema. Durante estos dos procesos, muchas herramientas y pasos tendrán que llevarse a cabo, incluyendo:

  - La determinación de la causa raíz del problema.
  - La determinación de las intervenciones necesarias para corregir el problema.
  - Determinar cuáles son los resultados esperados
  - La programación de los pasos de la corrección.
  - La planificación de los recursos.
  - Justificar la necesidad de la mejora.
  - La determinación de las métricas para la mejora.

- **Hacer:** Una vez que el plan ha sido creado, el enunciado del alcance del proyecto firmado en, y el calendario de hecho, es el momento de ejecutar el plan.

Durante esta fase, una solución será:

  - Implementar a modo de prueba.
  - Comprobarlo continuamente.
  - Implementado de forma permanente (si la prueba tiene éxito).
  - Medido por el rendimiento.

- **Verificar**: Una vez que se ha iniciado la implementación de la solución, utilizando la metodología de mejora PHVA, tendrá que hacer un seguimiento del rendimiento de esta solución con el tiempo. Tómese el tiempo para comparar la calidad del producto o servicio antes y después de la implementación. Responde las siguientes preguntas:

  - ¿La implementación de un cambio alcanza los resultados deseados?
  - ¿Qué pasa con la aplicación o el cambio funcionó bien?
  - ¿Que no funcionó?

En el caso de no obtener los resultados deseados se requiere regresar a la primera fase y revisar el análisis de la causa raíz.

- **Actuar:** Luego de verificar los resultados (y después de algunos intentos de ajustar su proceso), entonces es el momento de normalizar la mejora de procesos y colocarlo en práctica en el sistema. Durante esta fase final del ciclo PDCA, tendrá que:

  - Identificar las necesidades de capacitación para la plena aplicación de la mejora.

- Adoptar completamente la solución para la mejora de procesos.

- Continuar monitoreando su solución.

- Observar si no se puede mejorar la solución a través de nuevas implementaciones

- Encuentra oportunidades de mejora.

La metodología de mejora PHVA, como gestión de calidad total, es un método continuo. Eso significa que no se deja de trabajar a través del ciclo PHVA.

- Magerit. Tiene su origen en el Consejo Superior de la Administración Electrónica, como un resultado de la dependencia de las tecnologías de información actual, se trata de una metodología de análisis y gestión de riesgo diseñada para ser mejor aplicable a las TI7.

Magerit es una metodología de interés para personas que trabajan con sistemas de información. La información como activo tiene un valor muy alto, esta metodología permite conocer el nivel de exposición en el que se encuentra y ayudará a protegerlo. Conocer el riesgo en el que se encuentra un sistema es fundamental para su correcta gestión, Magerit impulsa un enfoque metódico completo sin dejar lugar para improvisar.

Esta metodología se fundamenta en el impacto que pueda tener la violación de la seguridad en una entidad, con esto busca detectar posibles amenazas que pudiesen afectar la organización, para así establecer medidas de corrección y prevención pertinentes y efectivas.

Una característica importante de esta metodología es su muy completa guía que expone paso a paso la manera de implementar el análisis de riesgo. Magerit se compone de tres libros

- El primero contiene todo lo concerniente al método, expone la estructura del modelo de gestión de riesgos (se ajusta al modelo propuesto por ISO en cuanto a gestión de riesgos).

[7] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. riesgo y control informático. Estándar Magerit para Análisis de Riesgos Informático. [en línea]. [consultado el 2 de diciembre de 2017]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_8_estndar_ magerit_ para_anlisis_de_riesgos_informticos.html

- El segundo libro básicamente es un catálogo de elementos en el cual se incluye una estructuración y categorización de activos a considerar, que aspectos tener en cuenta para valorarlos y adicionalmente ofrece una lista de amenazas y controles.

- El tercer libro se exponen las diversas técnicas que usualmente son usadas en el análisis de riesgo.

Algunos conceptos importantes que aplica esta metodología son[8]:

- Activo: Un activo se refiere a todo lo que represente un valor para la entidad. Magerit categoriza los activos en:

  - El soporte (o entorno) del Sistema de Información, se refiere a activos físicos, tangibles como por ejemplo personal, edificaciones.

  - El sistema de información propio del Dominio (hardware, redes, software, aplicaciones)

  - La información que requiere, soporta o produce el sistema de información (datos, claves, códigos).

  - Las funciones que justifican la existencia del sistema de información, incluye tanto objetivos de organización o sistema como personal.

  - Otros Activos, hace referencia a diversos activos con diferentes naturalezas, como imagen de la empresa o sistema, confiabilidad del mismo.

- Riesgo: El riesgo se define como la probabilidad de que una amenaza se materialice.

- Amenaza: Una amenaza es un evento que puede ser causante de un incidente con consecuencias que se pueden reflejar en daños materiales o inmateriales. Estas amenazas pueden ser:

  - [N] Desastres naturales
  - [I] De origen industrial
  - [E] Errores y fallos no intencionados
  - [A] Ataques intencionados

[8]ESQUEMA NACIONAL DE SEGURIDAD. MAGERIT: versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid – España. 2012 [En línea] [consultado el 23 de noviembre de 2017]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

La metodología Magerit categoriza y califica la probabilidad de ocurrencia, el impacto y el nivel de riesgo de los posibles incidentes para establecer medidas para controlar los riesgos o asumirlos. Esa clasificación se puede observar en las tablas 1, 2 y 3.

Tabla 1. Magerit: Impacto

CALIFICACIÓN NUMÉRICA	GRAVEDAD (IMPACTO)
5	Muy grave
4	Importante
3	Moderado
2	Leve
1	Marginal

Fuente: autor

Tabla 2. Magerit: Probabilidad

CALIFICACIÓN NUMÉRICA	PROBABILIDAD
5	Muy frecuente
4	Frecuente
3	Normal
2	Poco frecuente
1	Muy poco frecuente

Fuente**:** autor

El establecimiento del nivel de riesgo se realizará de forma cuantitativa, realizando una multiplicación entre los valores numéricos de probabilidad e impacto, se clasificarán en rangos y se les asignará un nivel de riesgo de la siguiente forma:

Tabla 3. Magerit: Nivel de Riesgo

RANGO	CALIFICACIÓN DE RIESGO
21-25	CATASTRÓFICO
16-20	MAYOR
10-15	MODERADO
5-9	MENOR
1-4	INSIGNIFICANTE

Fuente: Autor

Según lo anterior la calificación del riesgo en una matriz quedaría de la siguiente manera:

Tabla 4. Magerit: Matriz de Riesgo

PROBABILIDAD						
	5	**5**	**10**	**15**	**20**	**25**
	4	**4**	**8**	**12**	**16**	**20**
	3	**3**	**6**	**9**	**12**	**15**
	2	**2**	**4**	**6**	**8**	**10**
	1	**1**	**2**	**3**	**4**	**5**
	0	**1**	**2**	**3**	**4**	**5**
		IMPACTO				

Fuente: autor

4.3 MARCO LEGAL

Teniendo en cuenta que el proyecto consiste en auditar un servidor, se podría tomar a modo general como un proceso de hardening a un servidor Ubuntu 14.04 en cuanto a sus configuraciones por defecto que pueden ser más vulnerables. Para lo anterior no se requiere abarcar a gran profundidad un marco legal, se requiere conocer principalmente normatividad colombiana en cuanto a derechos de autor:

- **Decisión 351 de la C.A.N.** busca proporcionar protección a los autores y titulares de derechos, de las obras desarrolladas en distintos campos.

- **Ley 23 de 1982**: Norma colombiana que contienen las disposiciones en cuanto a la regulación del derecho de autor**.** Esta norma sirve como fundamento para que se inicie la regulación de software y a partir de ella se emiten algunas circulares ajustando y reglamentando la protección judicial o jurídica del software por parte de la Dirección Nacional del Derecho de Autor. Teniendo en cuenta esta norma cabe aclarar que el software utilizado para la ejecución de las diferentes pruebas es libre.

4.4 MARCO CONCEPTUAL

Activo: En el contexto de seguridad de la información hace referencia a información o cualquier elemento que tenga alguna relación con el tratamiento de esta (Sistemas, personas, etc), y que represente algún valor para la organización.

Amenaza: En el ámbito de seguridad informática, se refiere a la potencial causa de incidentes que pueden representar daños en la organización o en los sistemas de información.

Análisis de riesgo: Se refiere al proceso por el cual se realiza un análisis de las posibles causas de las amenazas, teniendo en cuenta los riesgos encontrados para clasificarlos y establecer medidas para mitigarlos.

Control: Son medidas que se generan para mitigar un riesgo encontrado.

Hardening: Proceso de aseguramiento de un sistema mediante la aplicación de controles para mitigar el nivel de exposición en el que dicho sistema se encuentra.

Magerit: es una metodología de interés para personas que trabajan con sistemas de información. La información como activo tiene un valor muy alto, esta metodología permite conocer el nivel de exposición en el que se encuentra y ayudará a protegerlo. Conocer el riesgo en el que se encuentra un sistema es fundamental para su correcta gestión, Magerit impulsa un enfoque metódico completo sin dejar lugar para improvisar

PHVA: proporciona una consecución de procesos claros a implementar para desarrollar de una manera correcta, ordenada y eficiente un trabajo (auditoría), se compone de cuatro fases:

- Planear
- Hacer
- Verificar
- Actuar

Riesgo: Es la probabilidad de una ocurrencia de un incidente en base a una vulnerabilidad.

Vulnerabilidad: Se refiere a la capacidad, condiciones y/o características que posee un sistema y lo hacen susceptible a ser víctima de una amenaza.

5. DISEÑO METODOLÓGICO

Es un proyecto de investigación (monografía), no se ejecutará en ninguna organización, pero se realizarán y/o documentarán las pruebas necesarias para lograr cumplir con los objetivos propuestos.

El proyecto de análisis de seguridad informática aplicado a distribución de Linux Ubuntu 14.04 para controlar vulnerabilidades en configuración por defecto, es una investigación descriptiva ya que se analizarán y se establecerán controles necesarios para satisfacer los niveles de seguridad de un servidor en sus configuraciones iniciales.

5.1 ALCANCE

Se busca analizar la distribución Linux Ubuntu 14.04 en su estado de configuraciones por defecto para lograr determinar vulnerabilidades presentes en las configuraciones iniciales del sistema operativo, es de tener en cuenta que se busca analizar en cuanto a seguridad únicamente las configuraciones, por lo cual el análisis de riesgo y los controles a establecer tendrán en cuenta únicamente estos parámetros.

Para detectar las vulnerabilidades presentes en las configuraciones por defecto del sistema operativo se utilizará el software Lynis, el cual permite realizar un escaneo y análisis de parámetros de configuración para identificar vulnerabilidades presentes en las mismas.

La distribución Linux Ubuntu 14.04 se ejecutará en una máquina virtual para documentar los procesos necesarios para plasmarlos en el presente documento.

5.2 RESTRICCIONES

El sistema operativo será virtualizado en una máquina virtual, este no hace parte de ninguna organización.

Los aspectos a analizar abarcan solamente variables de configuración, no se ahondará en vulnerabilidades que puedan presentarse por ausencia de hardware u otros servicios que pueden hacer parte de un servidor pero que no son los básicos.

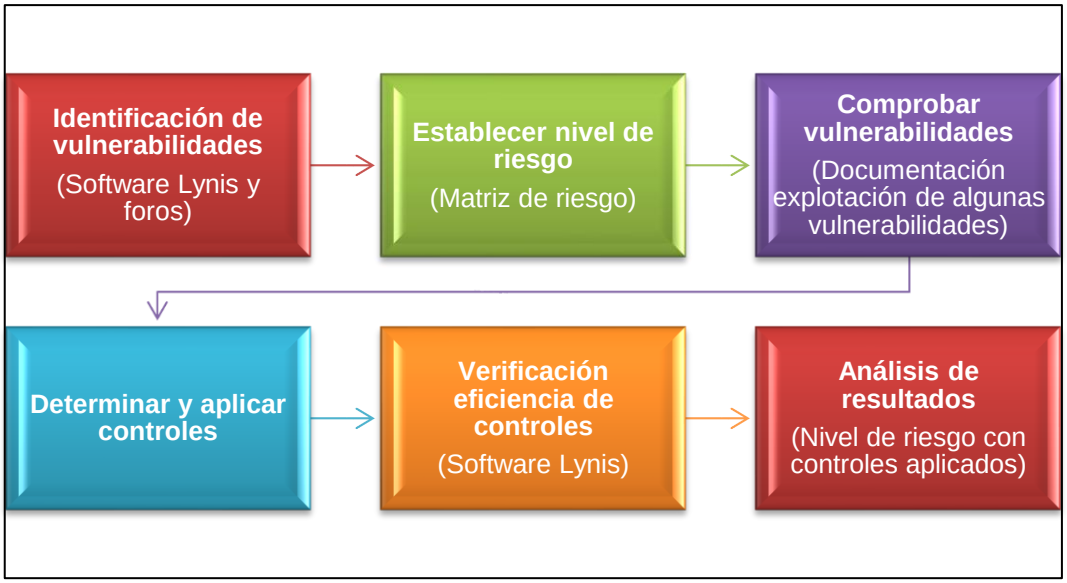
5.3 MÉTODO DE TRABAJO

Para desarrollar este proyecto se ha optado referenciarse en el ciclo PHVA (Planear, Hacer, Verificar, Actuar), ya que permite de una manera clara y consecuente establecer los procesos y actividades a llevar a cabo para lograr dar cumplimiento a los objetivos establecidos en este trabajo de grado y del mismo modo definir indicadores que corroboren que cada uno de ellos se alcanzó a cabalidad para posteriormente llevar a la práctica cada proceso y actividad planificadas, luego se ha de verificar si se han cumplido los objetivos, para en última instancia realizar las correcciones o adecuaciones necesarias.

Es importante aclarar que lo que se busca realizar es una auditoria en seguridad informática aplicada específicamente a las configuraciones del servidor, es decir, que el análisis de riesgo y los procesos siempre se centrarán en configuraciones.

Los procesos a realizar en resumen para el desarrollo de este trabajo se pueden observar en la figura 2, iniciando con la identificación de vulnerabilidades para posteriormente establecer el nivel de riesgo en el que se encuentra el servidor, posteriormente se documenta la explotación de algunas vulnerabilidades encontradas. Teniendo claridad del nivel de riesgo se procede a determinar y aplicar controles necesarios para reducir o subsanar las vulnerabilidades encontradas, luego de aplicar los controles se verificará la eficiencia de los mismos y se realizará el correspondiente análisis de resultados.

Figura 2. Esquema de trabajo



Fuente: autor

5.3.1 Planear. Conociendo que el objetivo del proyecto es brindar una serie de recomendaciones en cuanto a las vulnerabilidades y los controles necesarios para establecer un nivel de riesgo aceptable en un servidor Ubuntu 14.04,se hará uso de software especializado en auditar los parámetros de configuración del servidor para así lograr establecer que parámetros del mismo representan una vulnerabilidad y además de esto se indagará en portales reconocidos de soporte al sistema Ubuntu, para mejorar la detección e identificación de vulnerabilidades presentes en dicho servidor.

Luego de haber identificado las vulnerabilidades se realizará la respectiva matriz de riesgo para determinar el nivel de exposición en el cual se encuentra el sistema, para esto se tendrán en cuenta las calificaciones de impacto, probabilidad y riesgo establecidas en las tablas 1, 2 y 3 respectivamente.

Teniendo en cuenta las vulnerabilidades a las que está expuesto el servidor Ubuntu 14.04 en sus configuraciones por defecto se han de establecer controles que permitan una reducción significativa del riesgo que se tiene, para posteriormente verificar que los procedimientos de fortalecimiento de la seguridad han sido eficientes.

5.3.2 Hacer. En esta etapa se utilizará el software Lynis para detectar vulnerabilidades en el servidor y conocer algunas recomendaciones que Lynis realiza para mejorar el nivel de seguridad, al finalizar la ejecución del software se revisarán los resultados arrojados por el escaneo realizado y se documentaran algunas explotaciones de las vulnerabilidades identificadas en las configuraciones por defecto del servidor, adicionalmente serán de gran apoyo los foros dedicados a exponer las diversas vulnerabilidades de este sistema operativo, así como los controles a tomar.

Habiendo identificado las vulnerabilidades se procederá a realizar una clasificación del riesgo de exposición en el que se encuentra el sistema para con ello proceder con la determinación de controles pertinentes para reducir el nivel de riesgo.

En síntesis, se podría decir que esta etapa se compone de cuatro procesos:

- Identificación de vulnerabilidades
- Documentación de algunas posibles explotaciones de vulnerabilidades encontradas
- Generación de matriz de riesgo
- Determinación y aplicación de controles pertinentes

5.3.3 Verificar. Se busca valorar la veracidad de las vulnerabilidades encontradas y la efectividad de los controles aplicados para reducir el nivel de exposición a las posibles amenazas, para realizar la verificación de la eficiencia de los controles aplicados se ejecutará nuevamente el software Lynis después de haber implementado los controles establecidos. Habiendo realizado dicha verificación se procederá con el análisis de resultados para determinar el nivel de exposición en el que se encuentra el sistema luego de haber aplicado los controles establecidos.

5.3.4 Actuar. Habiendo realizado la verificación de la eficiencia de los controles establecidos se procederá con el análisis de resultados para determinar el nivel de exposición en el que se encuentra el sistema luego de haber aplicado los controles pertinentes para reducir el nivel de riesgo.

6. DESARROLLO DEL PROYECTO

6.1 INSTALACION BÁSICA DE UBUNTU SERVER 14.04

Lo primero que se realiza es la instalación básica del servidor Ubuntu 14.04 con el objetivo de contar con un sistema de fábrica. Para este proyecto el sistema operativo se va a instalar en una máquina virtual. La imagen ISO de la distribución se encuentra disponible para descargar en el siguiente Link: http://old-releases.ubuntu.com/releases/14.04.4/

Para proceder con la instalación se llevaran a cabo los siguientes pasos (cabe aclarar que solo se mostrarán las opciones más relevantes, para tener mayor información sobre el paso a paso para instalar Linux Ubuntu server 14.04 se puede consultar el siguiente link :https://www.youtube.com/watch?v=ApdFjKlRdfI

- Al iniciar la instalación, en la primera imagen que se muestra seleccionar la opción Instalar Ubuntu Server tal como se muestra en la figura 3.

Figura 3. Instalar Ubuntu Server 14.04

Fuente: autor

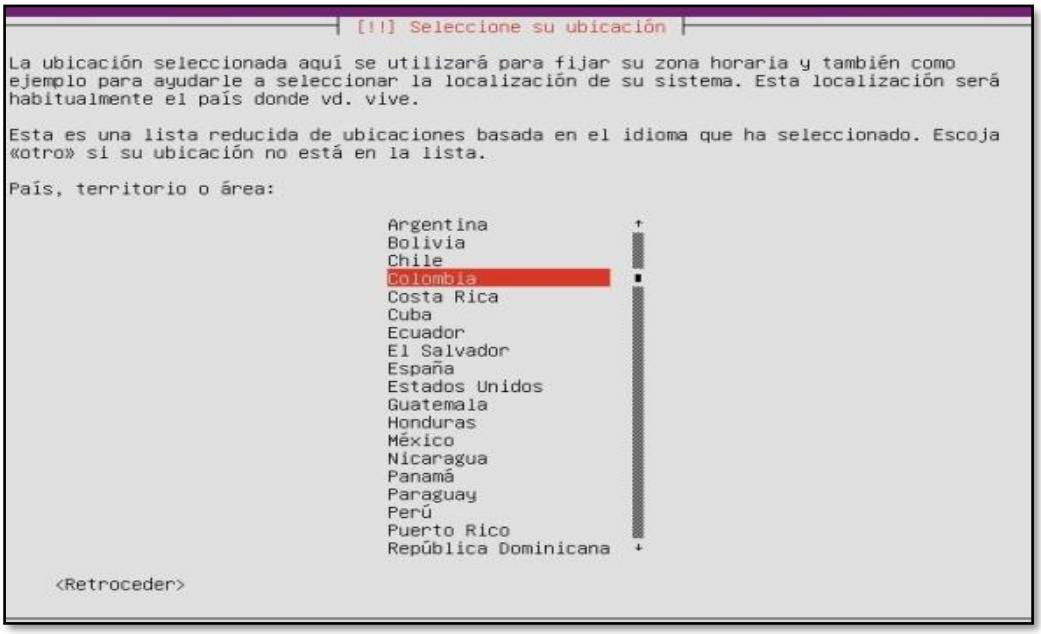
- En la figura 4 se muestra el siguiente paso a seguir, se debe seleccionar el idioma de instalación del servidor, en este caso Español.

Figura 4. Selección de idioma de instalación

Fuente: autor

- Posteriormente se debe elegir la ubicación donde se está instalando el servidor, para esta instalación el país seleccionado es Colombia como se puede observar en la figura 5.

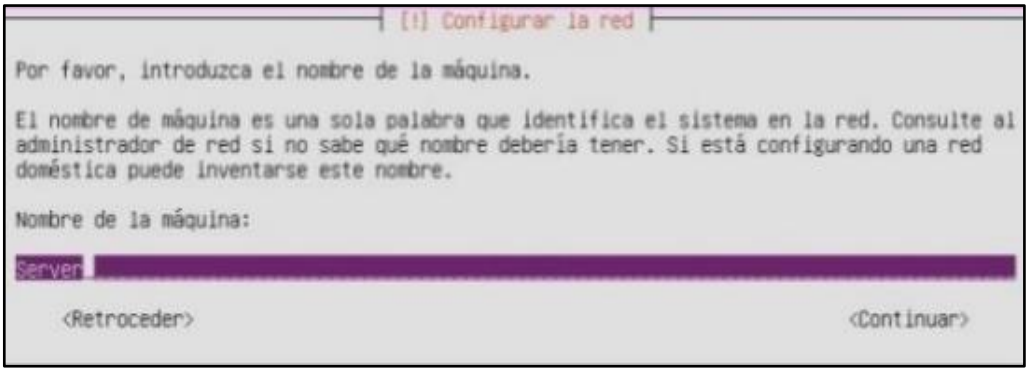
Figura 5. Ubicación del Sistema



Fuente: autor

- Las figuras 6, 7 y 8 muestran las opciones de nombre de la máquina, nombre real del usuario y nombre de usuario para la cuenta respectivamente. El nombre de la maquina se refiere a la identificación del sistema en la red.

Figura 6. Nombre de la máquina

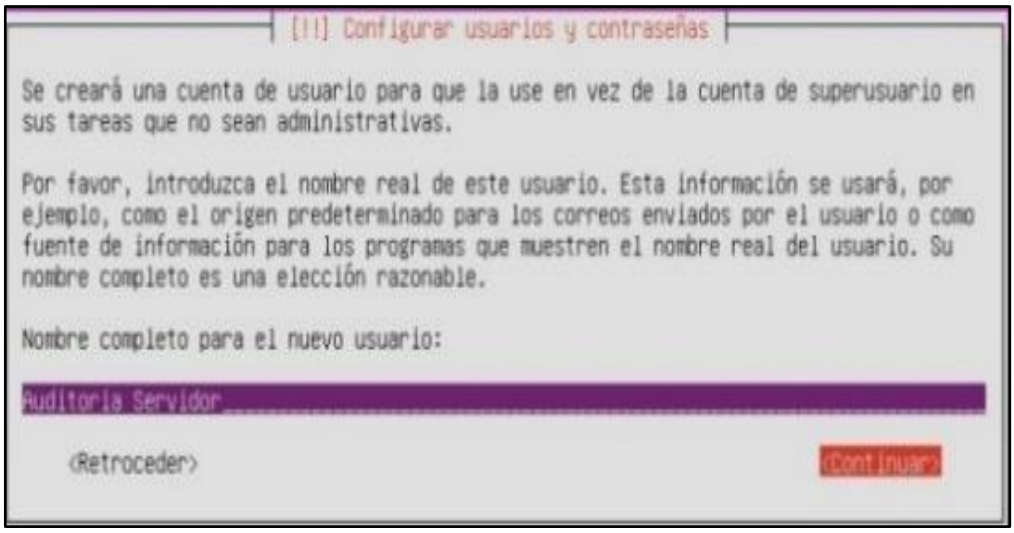


Fuente: autor

El nombre de la maquina seleccionado fue “Server”.

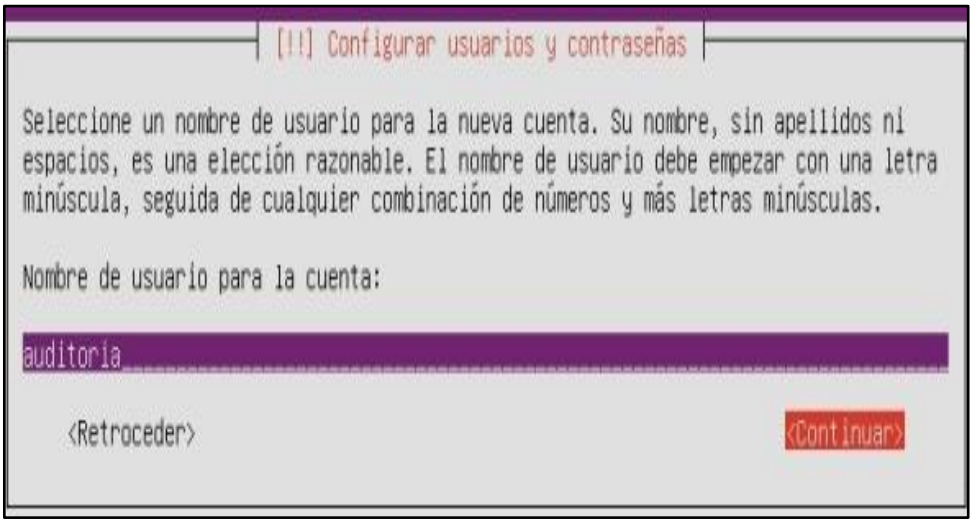
El nombre real del usuario es “Auditoria servidor”. Este nombre se refiere a la identificación que se le dará al usuario para realizar tareas que no sean administrativas, este usuario es diferente del usuario root. Una recomendación que el mismo sistema ofrece es el nombre completo de la persona que está realizando la instalación y que vaya a utilizar normalmente el sistema.

Figura 7. Nombre real del usuario



Fuente: autor

Figura 8. Nombre de usuario para la cuenta

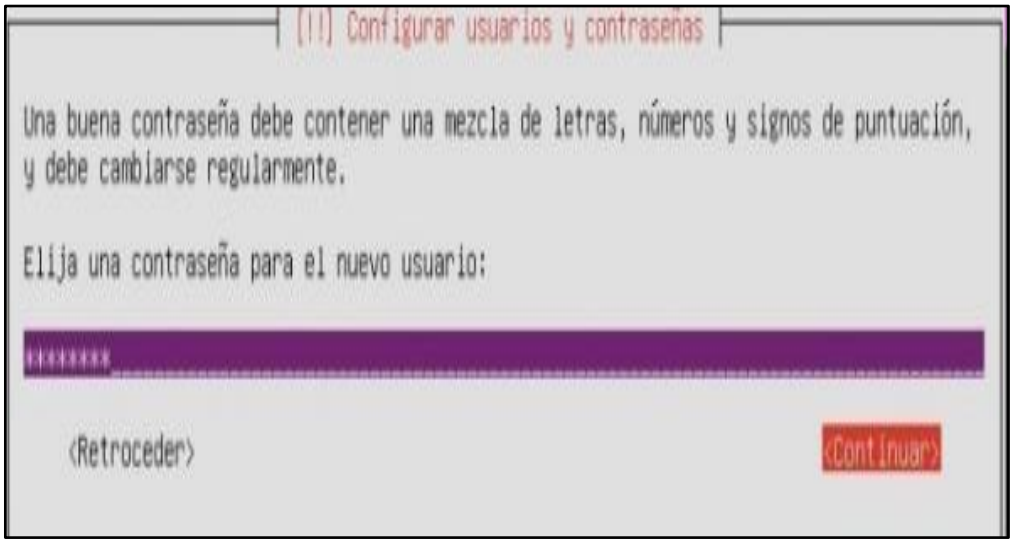


Fuente: autor

El nombre de usuario para la cuenta es “auditoria”. El sistema solicita que el nombre de la cuenta inicie con una letra minúscula, y posteriormente se realice la combinación de números y letras deseados.

- Luego de asignar los respectivos nombres o identidades se procede a establecer una clave de usuario. Esta contraseña se recomienda que contenga por lo menos una letra en mayúscula y combinaciones de letras, números y caracteres especiales. En la figura 9 se puede visualizar la configuración que se muestra en el instalador del servidor para contraseña de usuario.

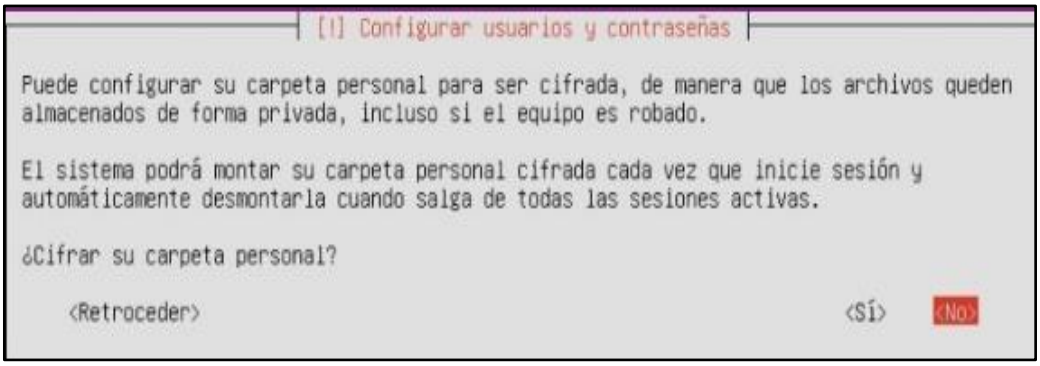
Figura 9. Contraseña de usuario



Fuente: autor

- La próxima opción que aparece es cifrar la carpeta personal como se muestra en la figura 10, teniendo en cuenta que se busca una configuración básica y por defecto, no se elegirá esta opción. Cabe aclarar que esta opción habilitada es considerada como una buena práctica teniendo en cuenta que brinda la información de nuestro sistema con un nivel más robusto de seguridad.

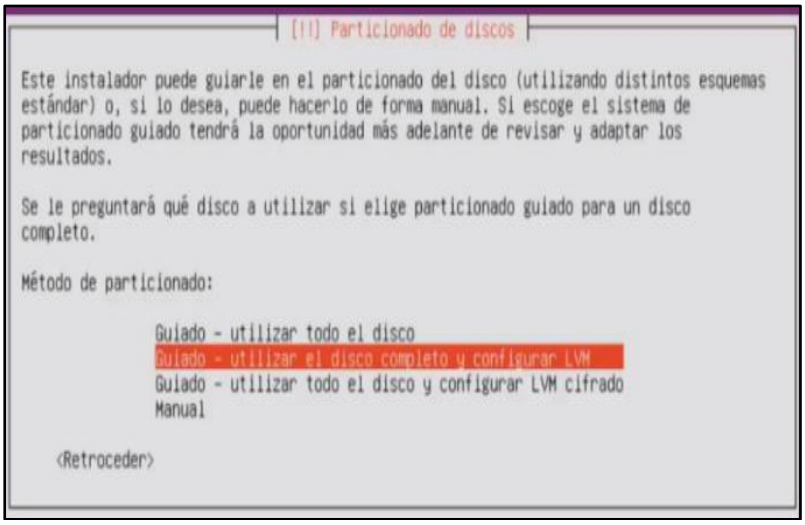
Figura 10. Cifrar carpeta personal



Fuente: autor

- En la figura 11, se debe elegir un método de particionado para la instalación del servidor, el método más básico es “Guiado, utilizar todo el disco” y por ende es el método seleccionado.

Figura 11. Método de particionado



Fuente: autor

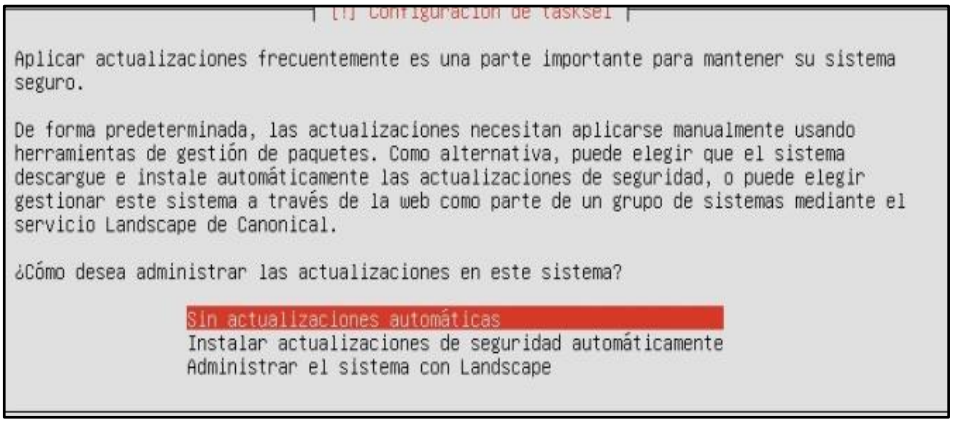
- El siguiente figura (12) paso que es escribir la información del proxy, por defecto no se usa ninguno, así que se deja en blanco. En caso de requerir un proxy para acceder a la red se debe ingresar en el formato: *<<http:///[usuario] [:contraseña]] [servidor][:puerto]/>>*

Figura 12. Uso de Proxy

Fuente: autor

- La siguiente opción es determinar cómo se administrarán las actualizaciones, en este caso se elegirá la opción sin actualizaciones automáticas, esta opción se puede ver en la figura 13. Cabe aclarar que de forma predeterminada Ubuntu requiere que las actualizaciones se realicen de forma manual aunque se recomienda para mejorar la seguridad que algunas actualizaciones se realicen automáticamente, ya que constantemente se desarrollan actualizaciones para corregir vulnerabilidades y/o errores identificados en el sistema.

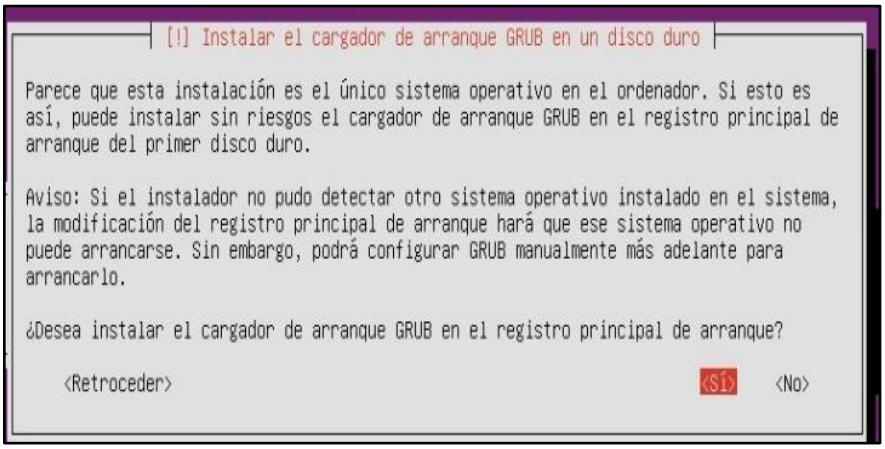
Figura 13. Administración de actualizaciones



Fuente: autor

- En la figura 14 se puede observar el siguiente paso, que consiste en la instalación del cargador de arranque GRUB, el cual permite arranque dos o más sistemas operativos que hayan sido instalados en el equipo.

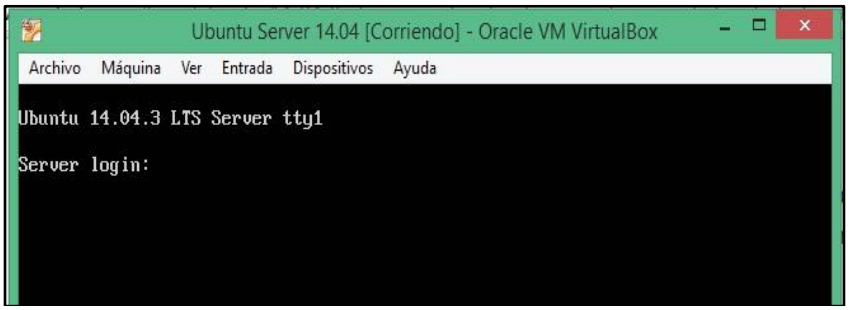
Figura 14. Cargador de arranque



Fuente: autor

A continuación en la figura 15 se puede observar el servidor Ubuntu 14.04 instalado.

Figura 15. Servidor instalado



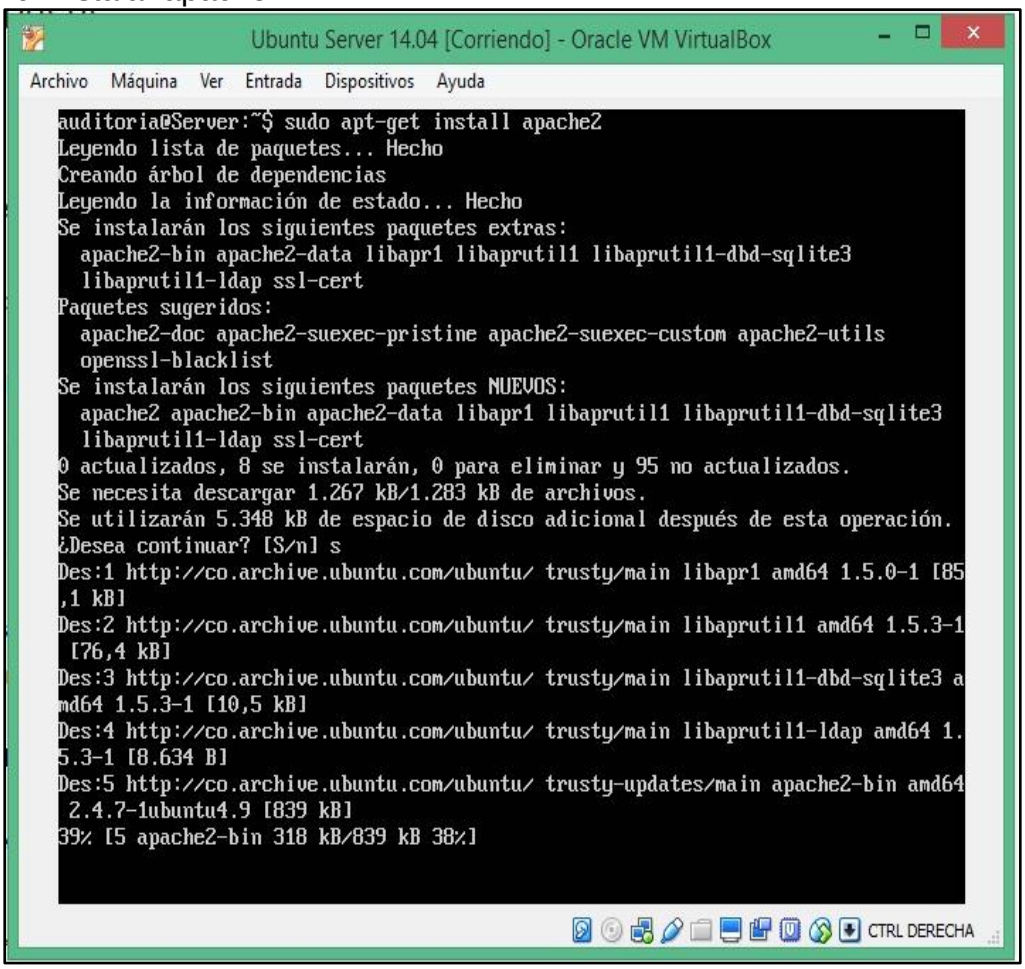
Fuente: autor

Como software básico de un servidor se instalan programas que permiten alojar aplicaciones y sitios web en el mismo, en este caso se instalará el servidor web Apache, sistema gestor de bases de datos Mysql y PHP.

6.1.1 Instalación Apache. Para la instalación de Apache desde el gestor de paquetes de Ubuntu, se utiliza el código
sudo apt -get install apache2

Esta instalación se puede observar en la figura 16.

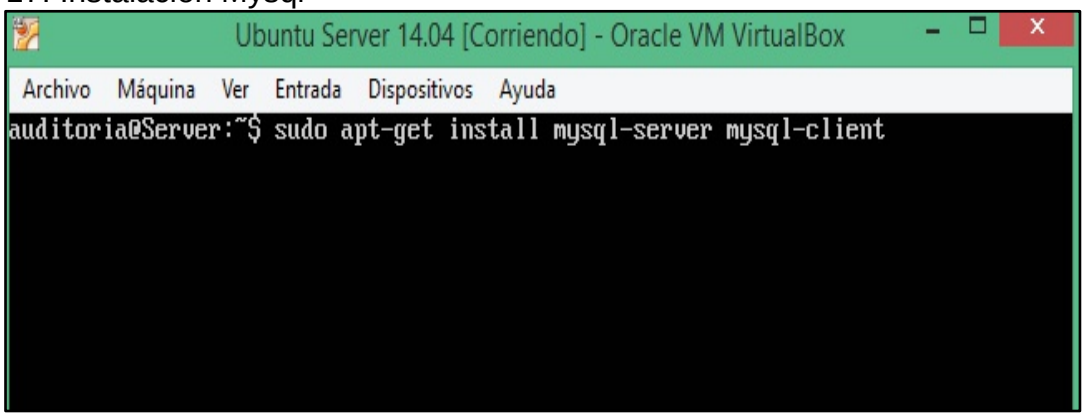
Figura 16. Instalar apache



Fuente: autor

6.1.2. Instalación Mysql. Para la instalación del gestor de bases de datos Mysql *se* utiliza el siguiente código:
sudo apt-get install mysql-server mysql-client (Ver figura 17)

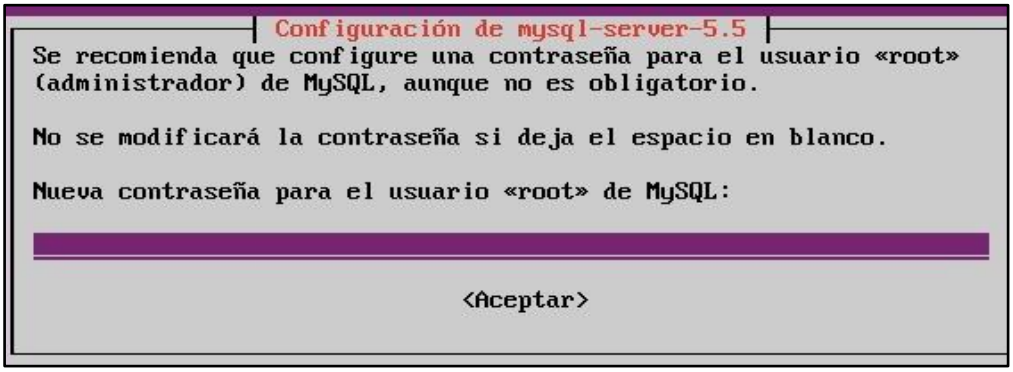
Figura 17. Instalación Mysql



Fuente: autor

Posteriormente se requerirá definir una contraseña para el usuario *root mysql*, estas opciones se pueden visualizar en la figura 18.

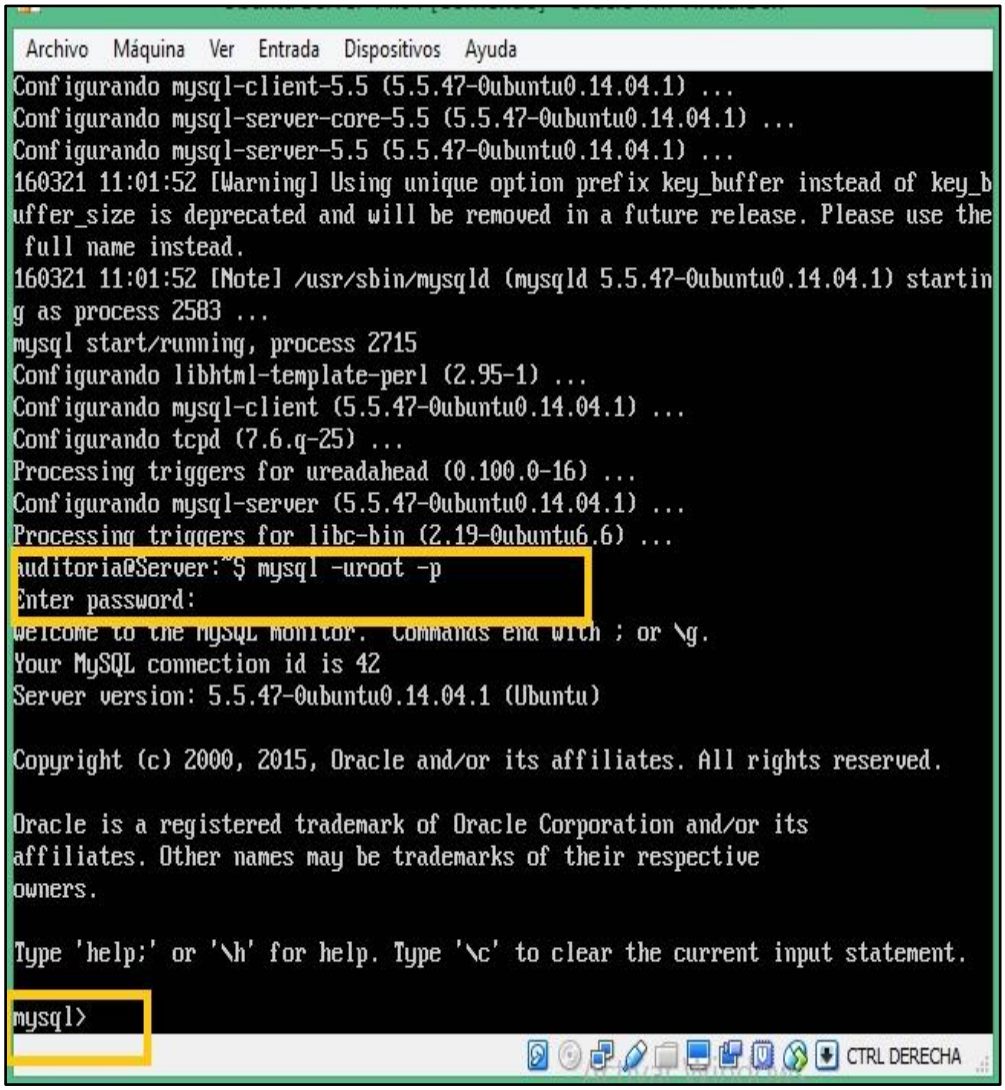
Figura 18. Contraseña *root Mysql*



Fuente: autor

Luego de los anteriores pasos quedará Mysql instalado, para ingresar es necesario el código: *mysql –uroot –p* y escribir la contraseña de usuario *root* cuando sea solicitada (ver figura 19).

Figura 19. Ingreso Mysql



Fuente: autor

6.1.3 Instalación PHP. Para la Instalación de PHP se utiliza el código*: Sudo apt-get install PHP5*

La instalación de PHP se puede ver en la figura 20.

Figura 20. Instalación PHP

Fuente: autor

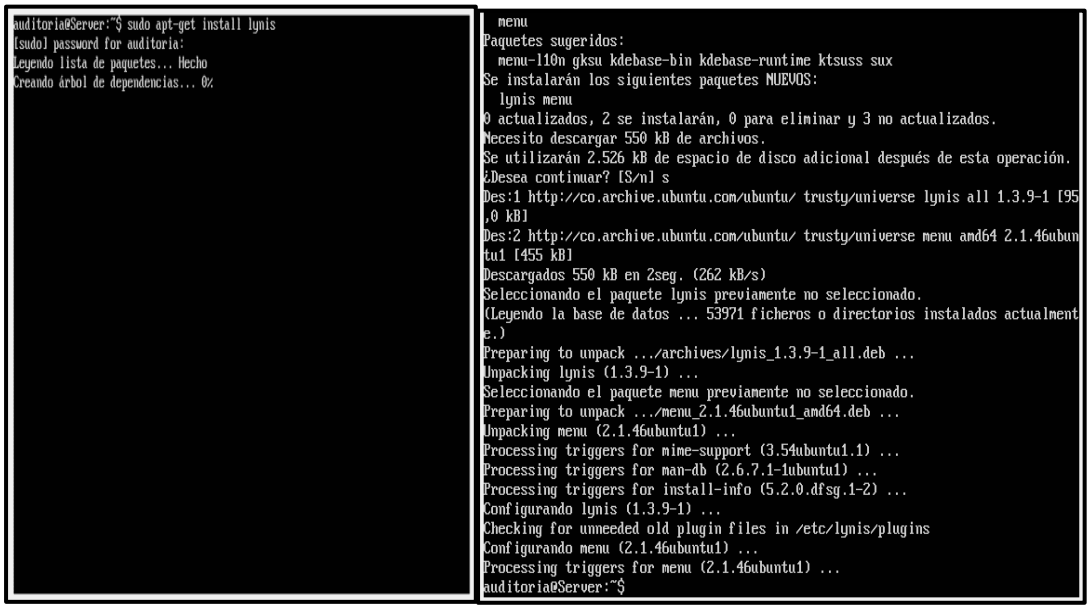
6.2 AUDITORIA A CONFIGURACIÓN DE SERVIDOR UBUNTU 14.04

Para realizar la auditoria de seguridad informática enfocada a las configuraciones por defecto del servidor Ubuntu 14.04 se utilizará la herramienta de seguridad Lynis la cual se caracteriza por realizar auditorías completas a sistemas Linux, analizando el software instalado en cada sistema para lograr identificar inconvenientes de seguridad, mostrará los peligros o principales fallos de seguridad y también mostrará sugerencias para reducir el riesgo. Esta herramienta mostrará las configuraciones que se tienen en el servidor, posteriormente conociendo las configuraciones por defecto se establecerá una matriz de riesgo utilizando el método Magerit para identificar los principales problemas en seguridad y proceder a determinar controles aplicables para mitigar los riesgos identificados.

6.2.1 Escaneo Lynis. Para realizar la instalación de la herramienta Lynis se utiliza el siguiente comando *Sudo apt-get install lynis*

La figura 21 muestra la instalación de Lynis en el servidor.

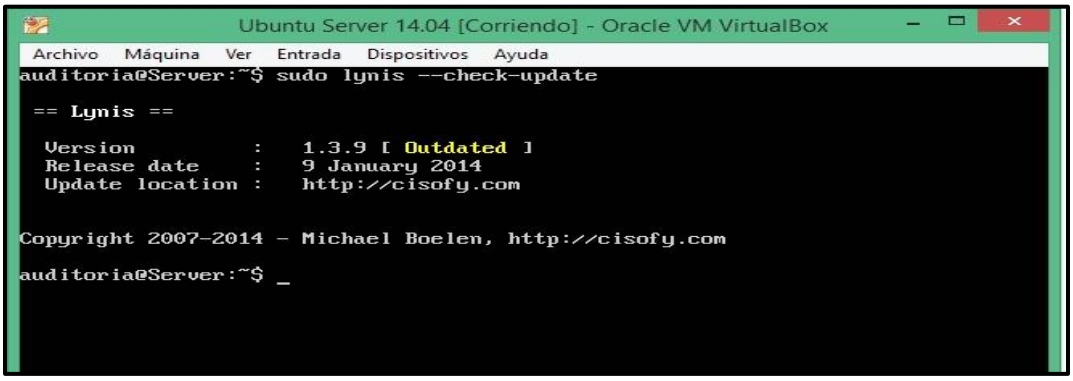
Figura 21. Instalar Lynis



Fuente: autor

Luego de instalar es necesario actualizar lynis con el *comando sudo lynis --check-update* (figura 22)

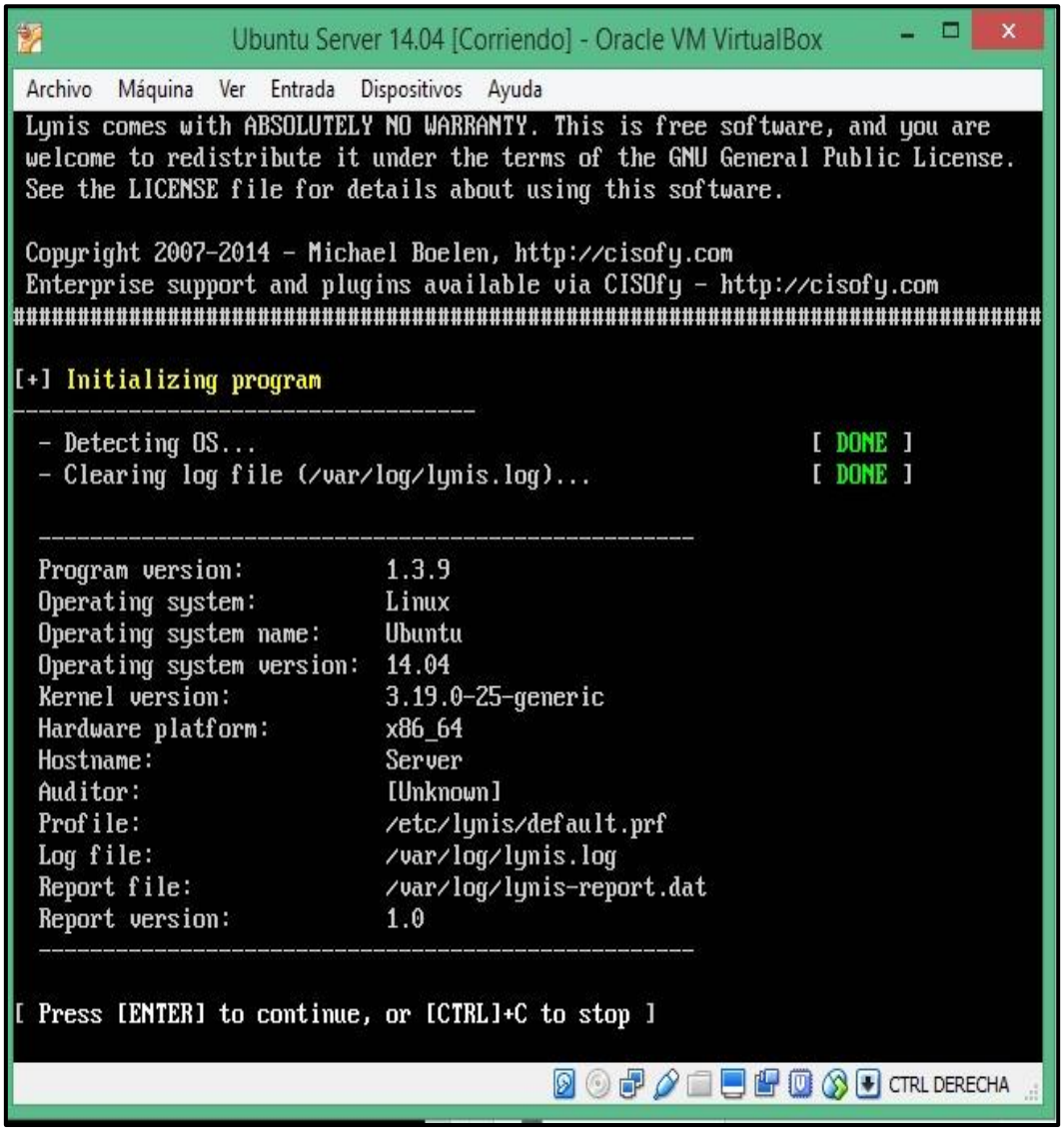
Figura 22. Actualizar Lynis



Fuente: autor

En la figura 23, después de tener actualizada la herramienta *Lynis* se ejecuta un código para iniciar el análisis del servidor Ubuntu 14.04 instalado mediante el código *sudo lynis* –c

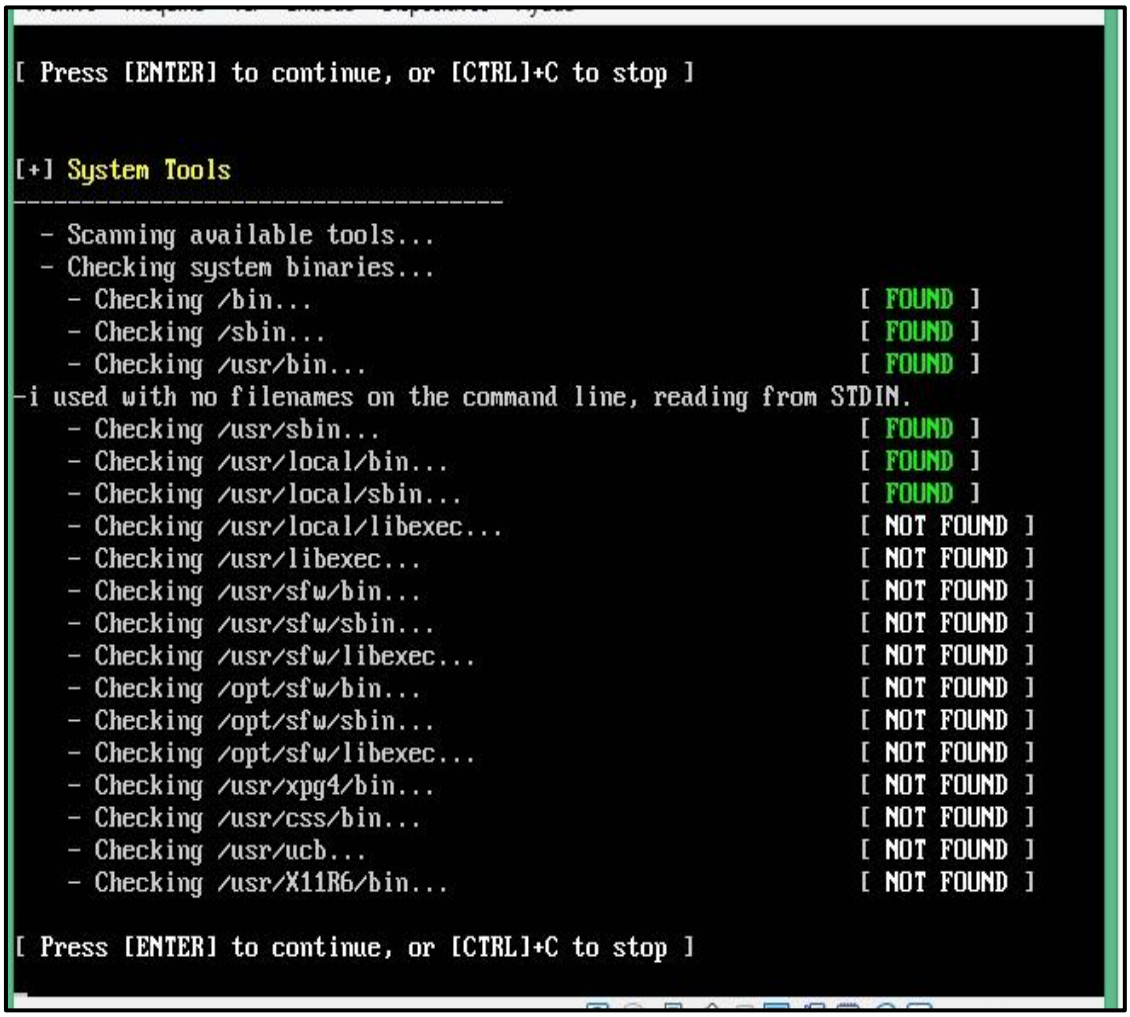
Figura 23. Ejecución de Lynis



Fuente: autor

Como se puede observar en la anterior figura, el programa inicia mostrando las características principales del sistema que se va a analizar.

Figura 24. Escaneo Lynis: Herramientas del sistema



Fuente: autor

El primer análisis que se realiza muestra las herramientas del sistema que están instaladas, la figura 24 muestra dichas herramientas.

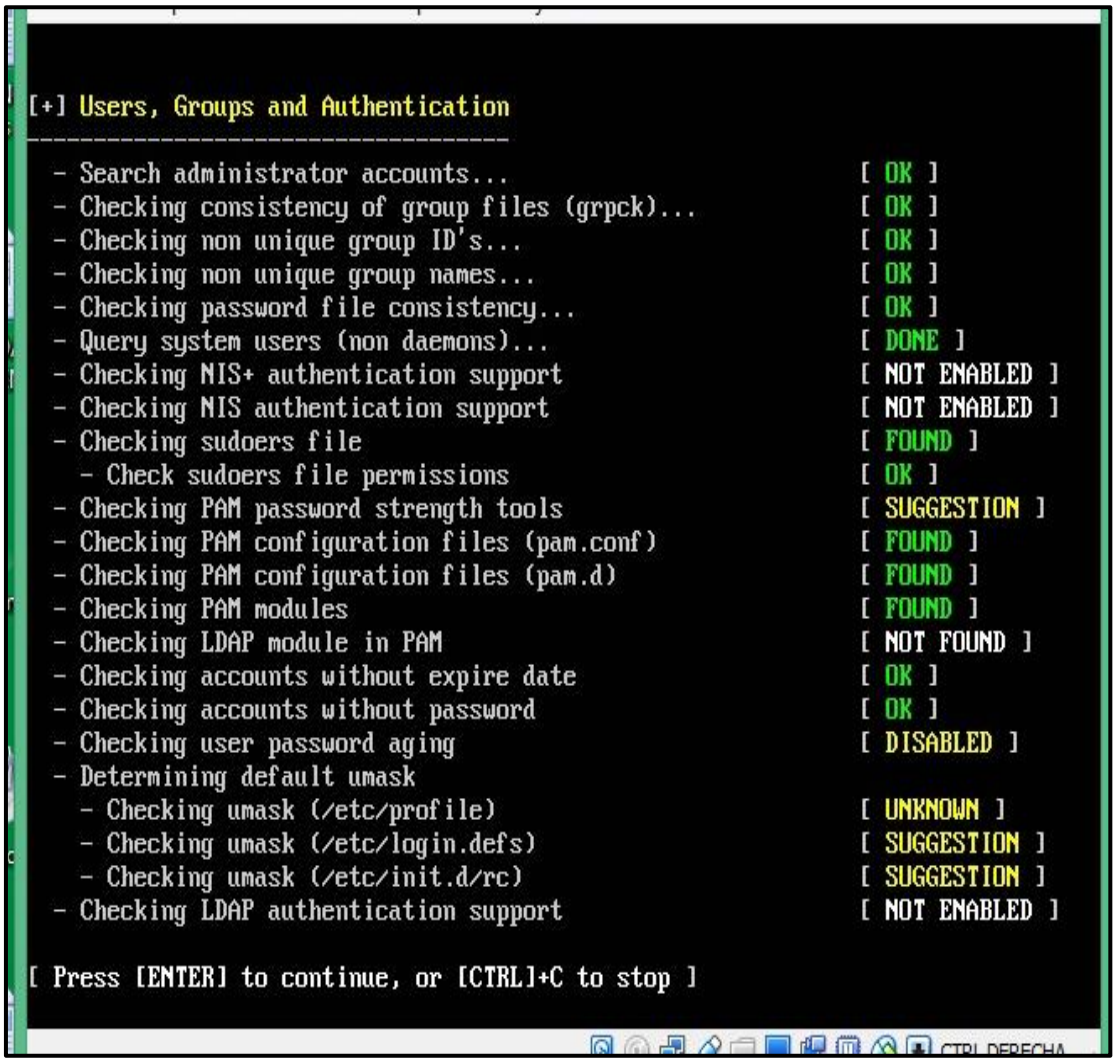
En la figura 25, el paso siguiente es analizar el gestor de arranque que se detecta en el sistema, los servicios que se inician y el *kerne*l

Figura 25. Escaneo Lynis: Gestor de arranque y Kernel

Fuente: autor

El siguiente aspecto por analizar se muestra en la figura 26 y es todo lo relacionado con usuarios, grupos y autenticación.

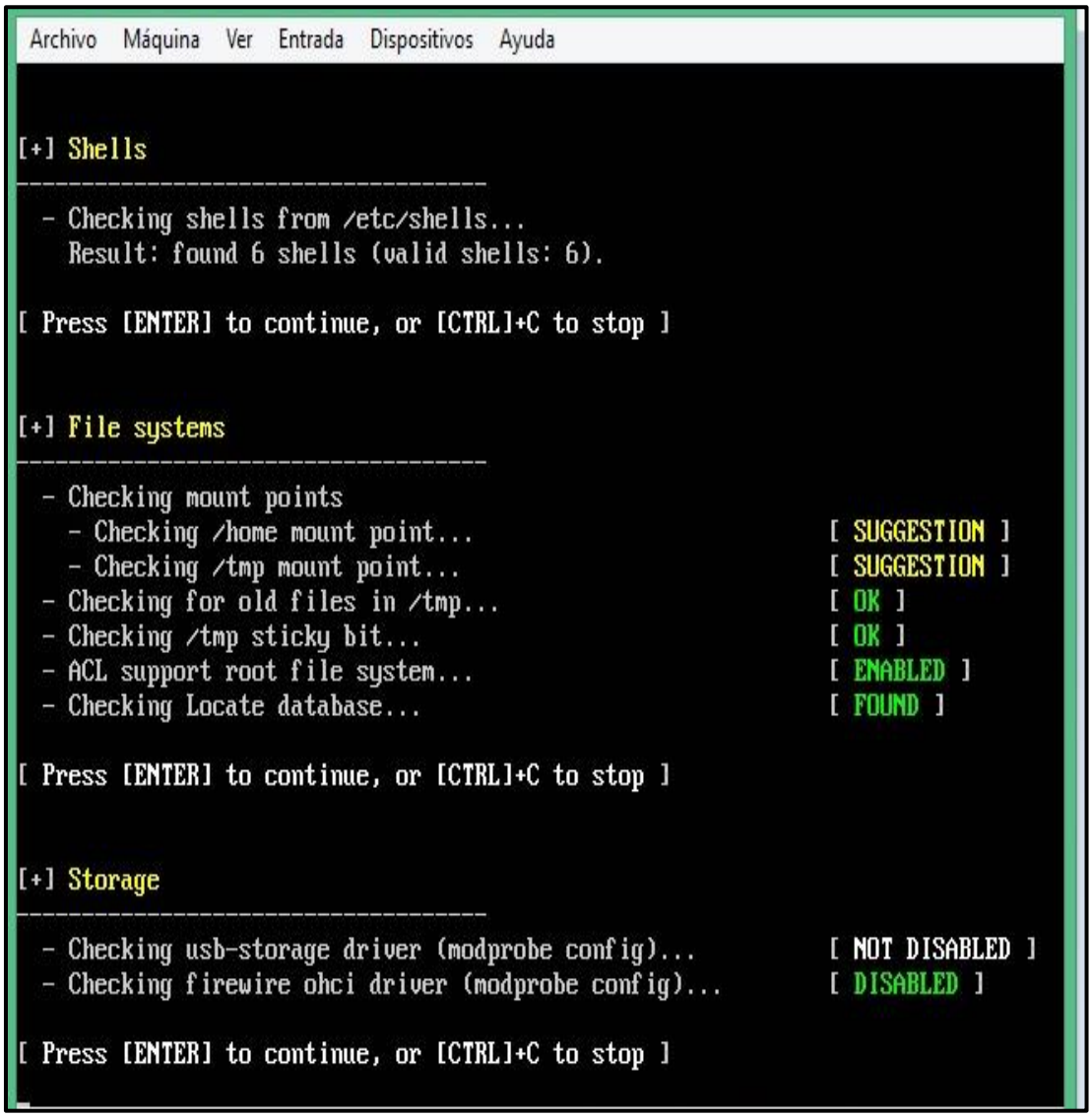
Figura 26. Escaneo Lynis: Usuarios, grupos y autenticación



Fuente: autor

Posteriormente en la figura 27 se escanea el escudo del sistema, el sistema de archivos y el soporte para almacenamiento masivo.

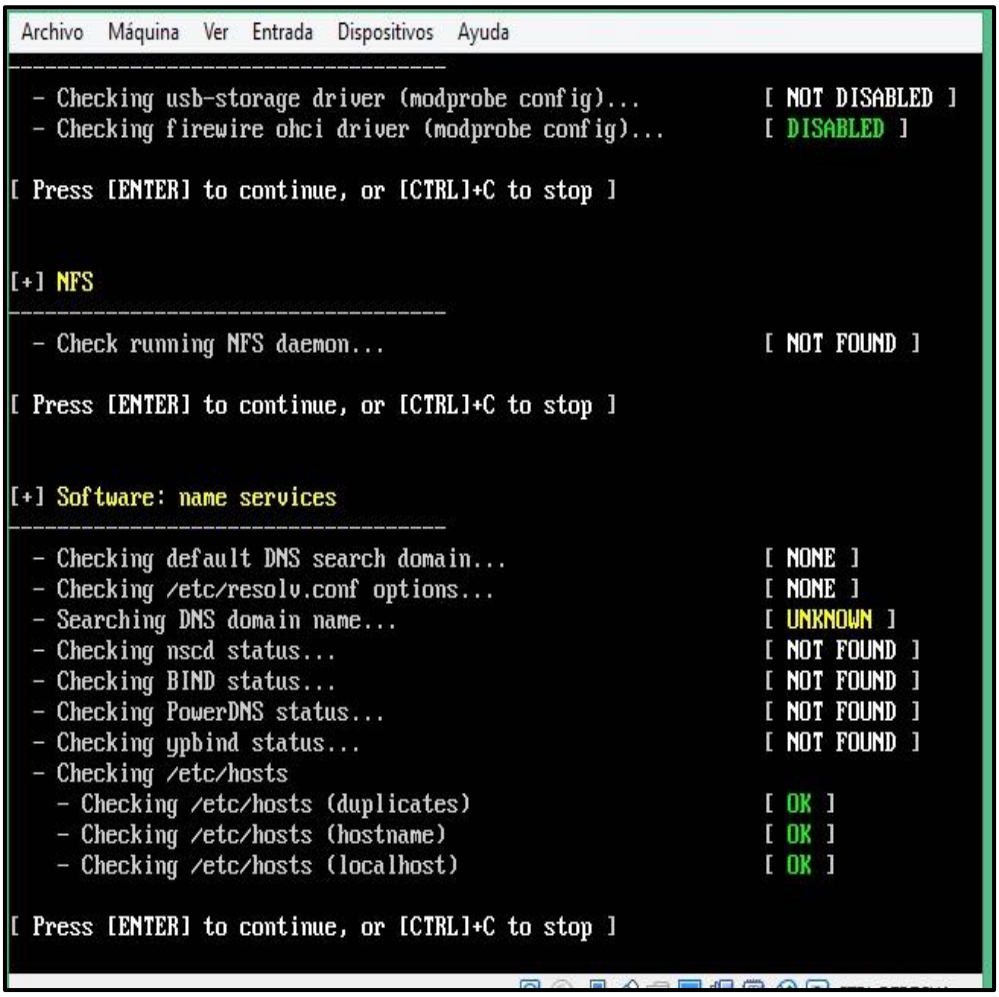
Figura 27. Scaneo Lynis: *Shells*, sistema de archivos, almacenamiento



Fuente: autor

El siguiente análisis el cual se puede observar en la figura 28 es el sistema de archivos de red y el servicio de nombres de servicios.

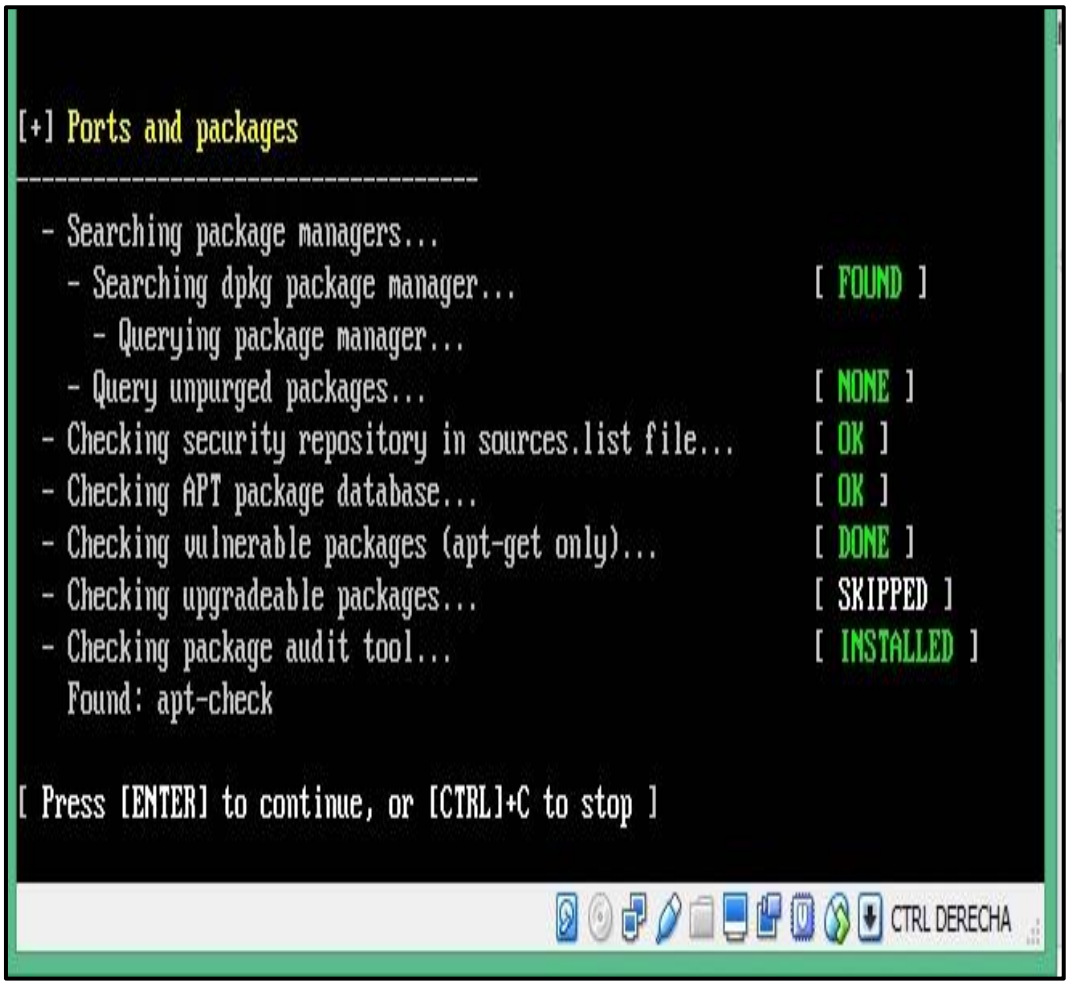
Figura 28. Escaneo Lynis: NFS, Software: nombre de servicios



Fuente: autor

El siguiente análisis corresponde al gestor de paquetes de distribución mostrado en la figura 29.

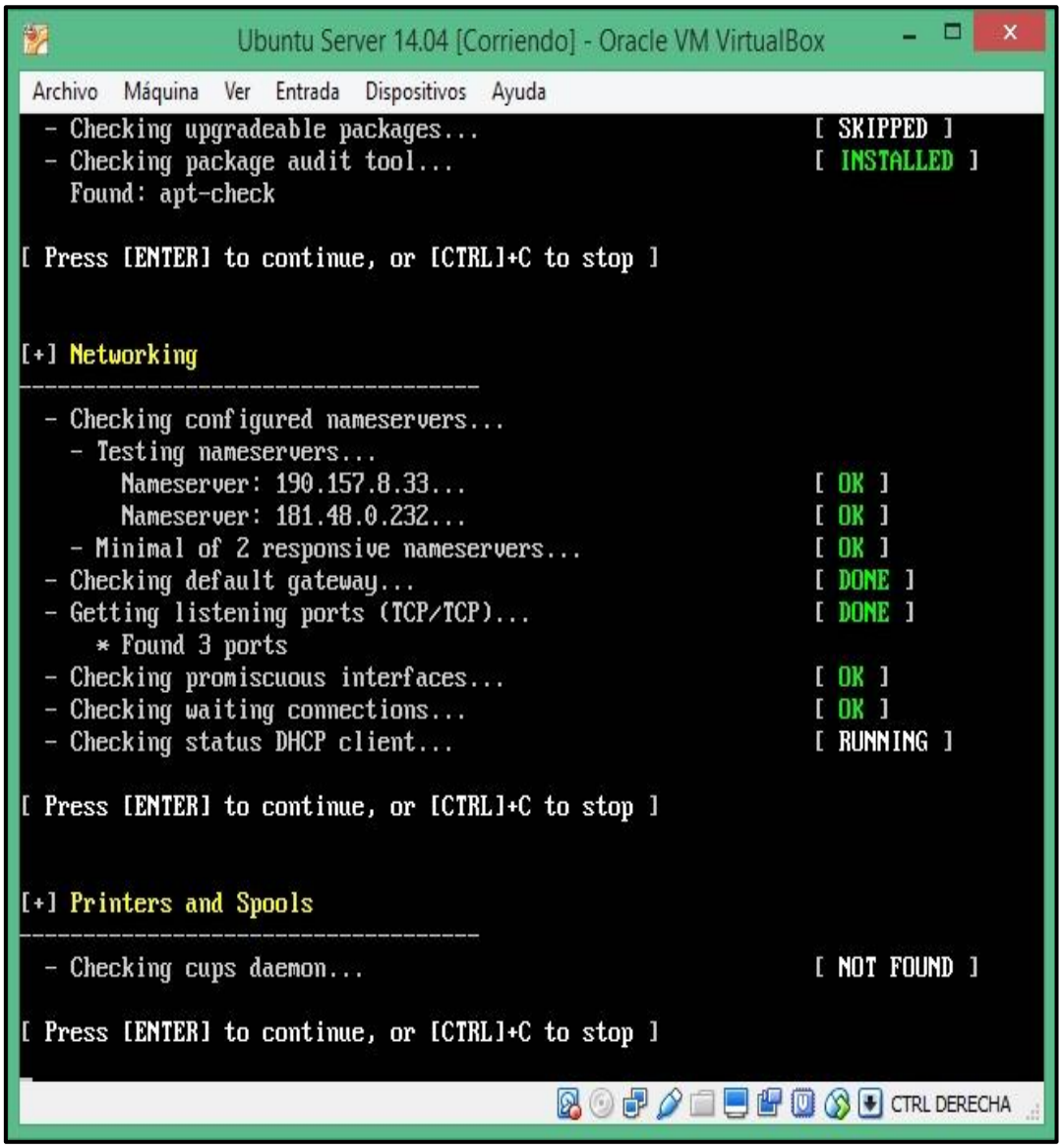
Figura 29. Escaneo Lynis: Puertos y Paquetes



Fuente: autor

En la figura 30 se muestra el análisis de redes realizado por *Lynis.*

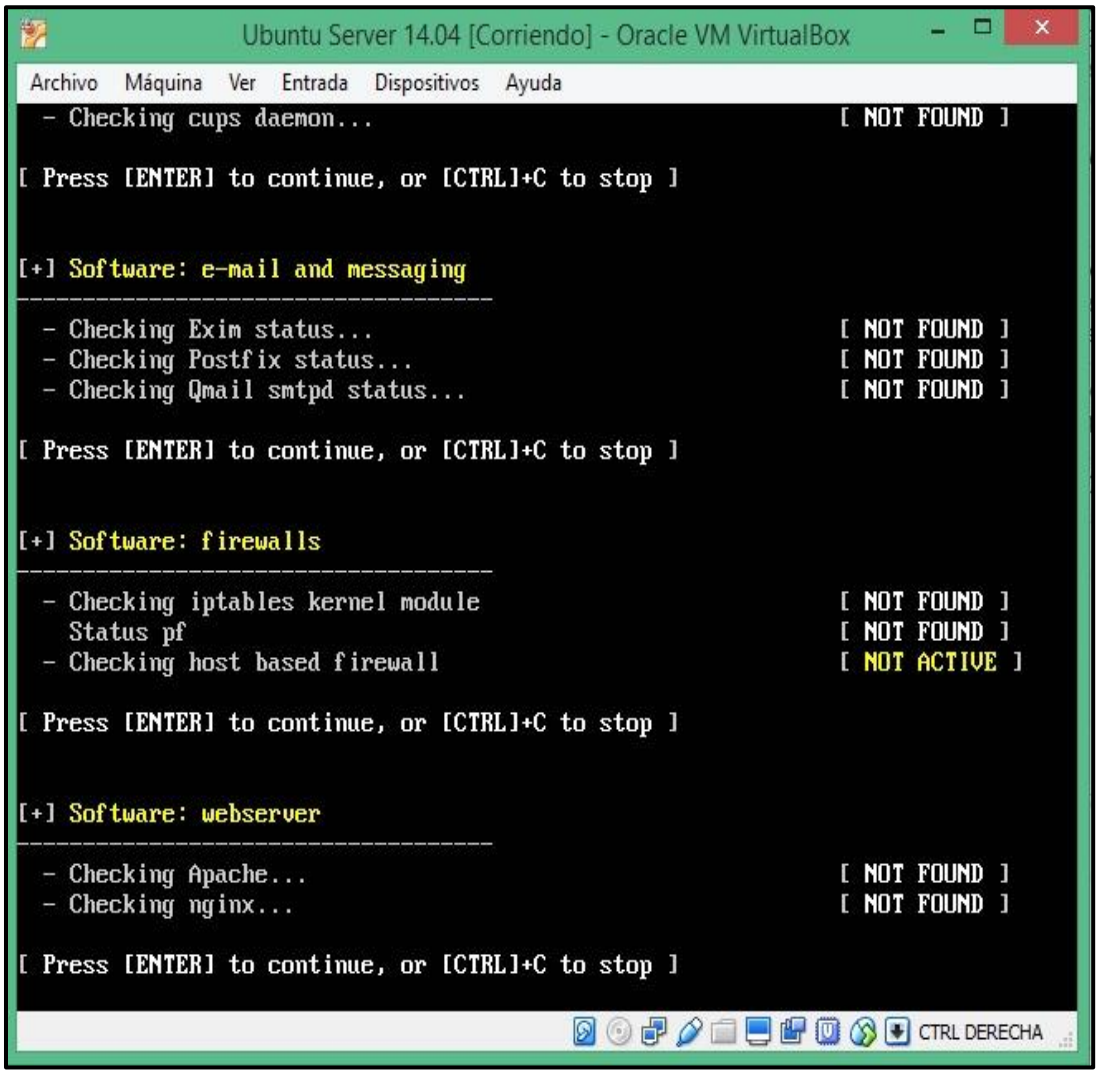
Figura 30. Escaneo Lynis: Networking, Printers and Spools



Fuente: autor

La figura 31 revela los resultados del análisis del servidor de correo y del firewall.

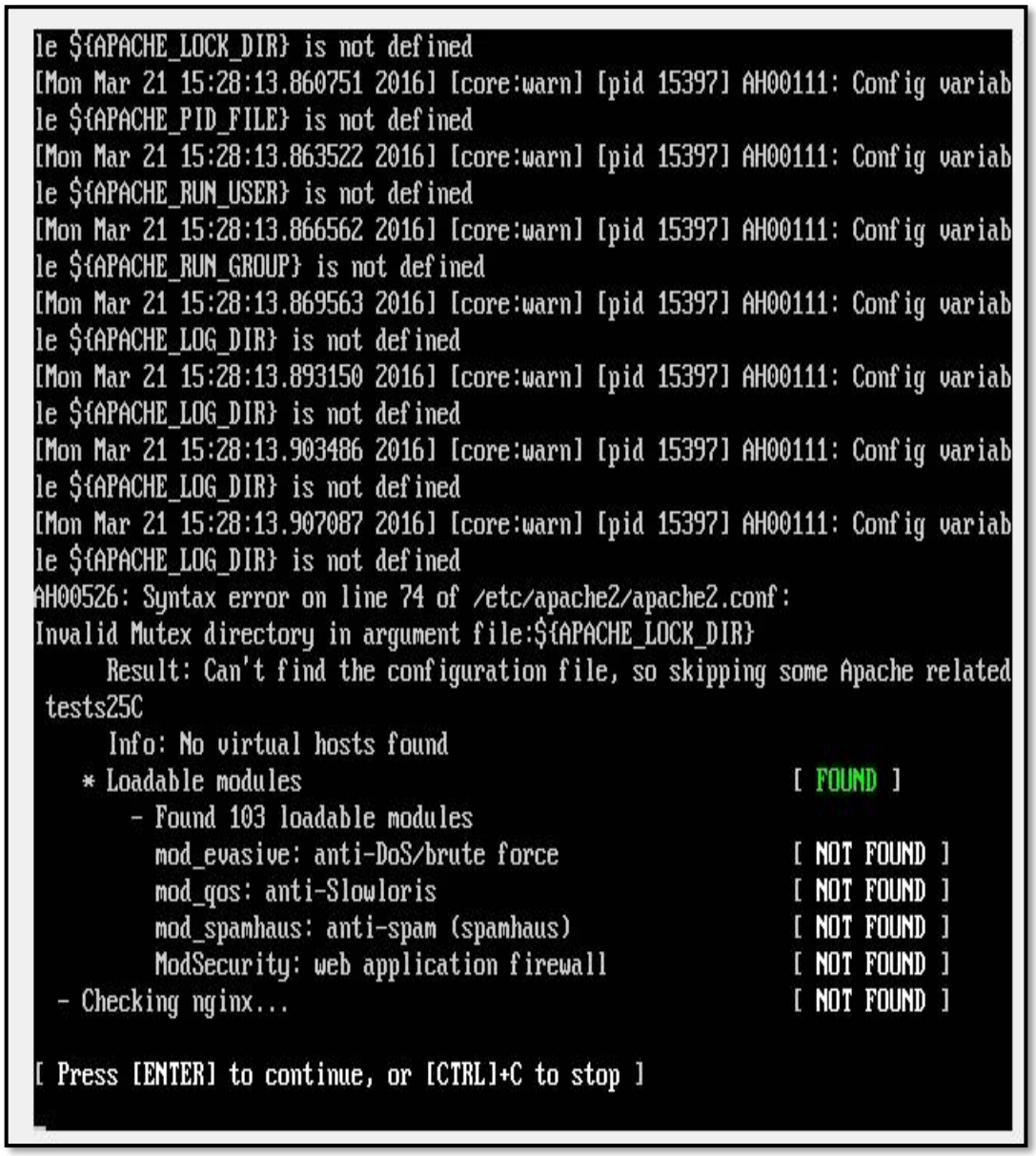
Figura 31. Escaneo Lynis: e-mail, firewalls



Fuente: autor

Seguidamente se analizará el servidor Web como se observa en la figura 32.

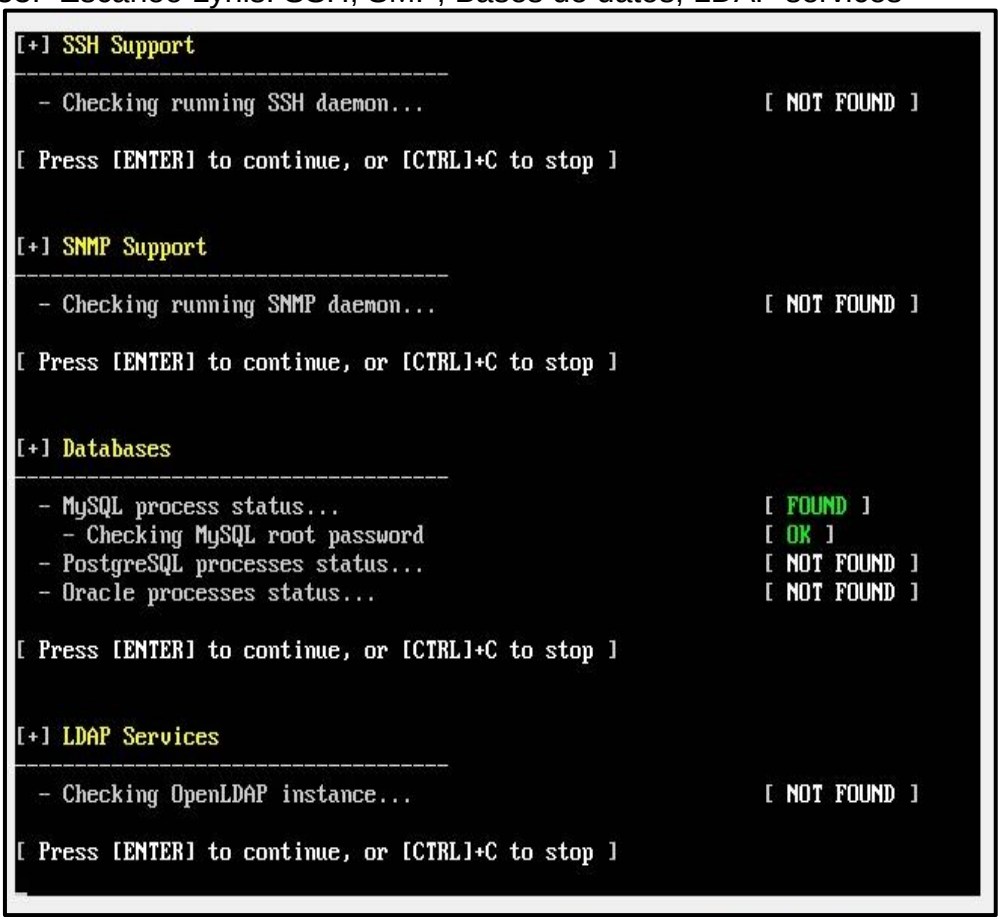
Figura 32. Escaneo Lynis: Web server



Fuente: autor

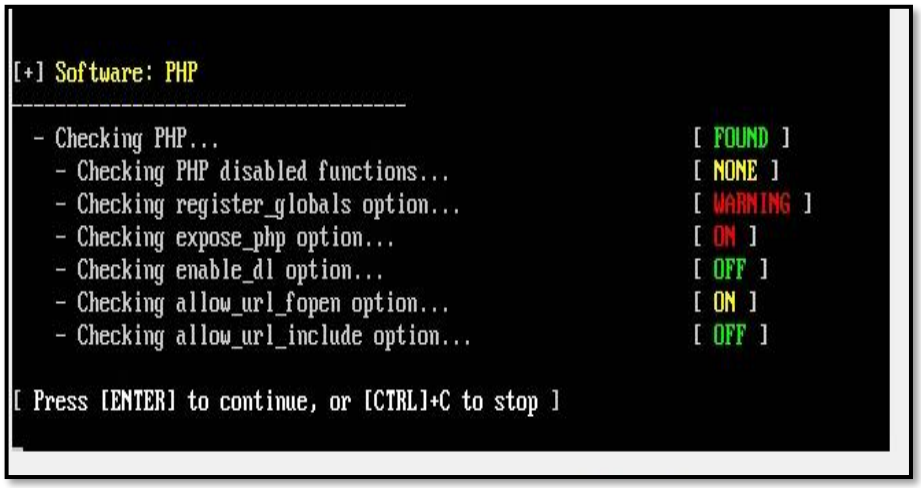
Continua el software Lynis realizando el análisis con los servicios SSH, SMP, Bases de Datos, LDAP y PHP, estos resultados se muestran en las figuras 33 y 34.

Figura 33. Escaneo Lynis: SSH, SMP, Bases de datos, LDAP services



Fuente**:** autor

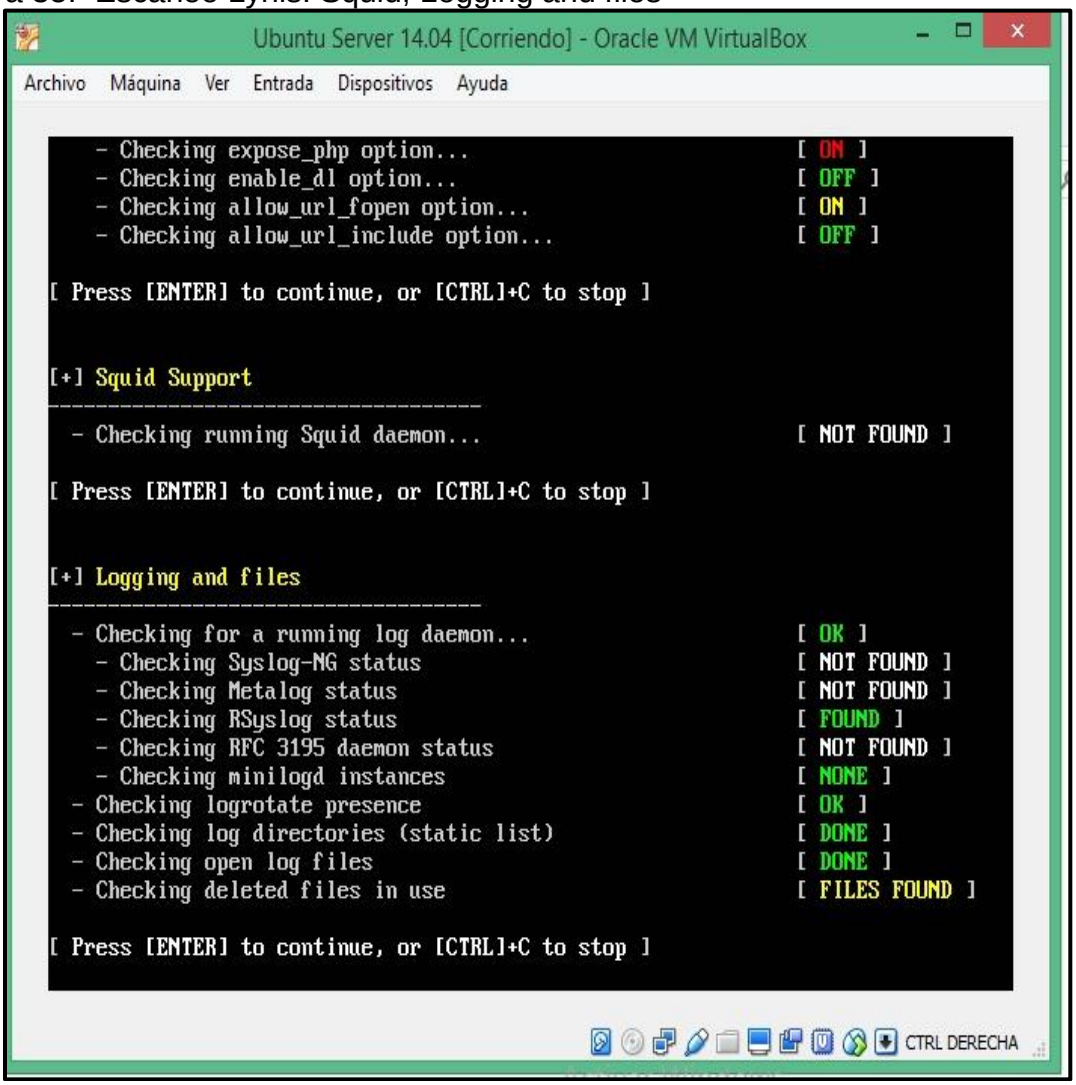
Figura 34. Escaneo Lynis: PHP



Fuente: autor

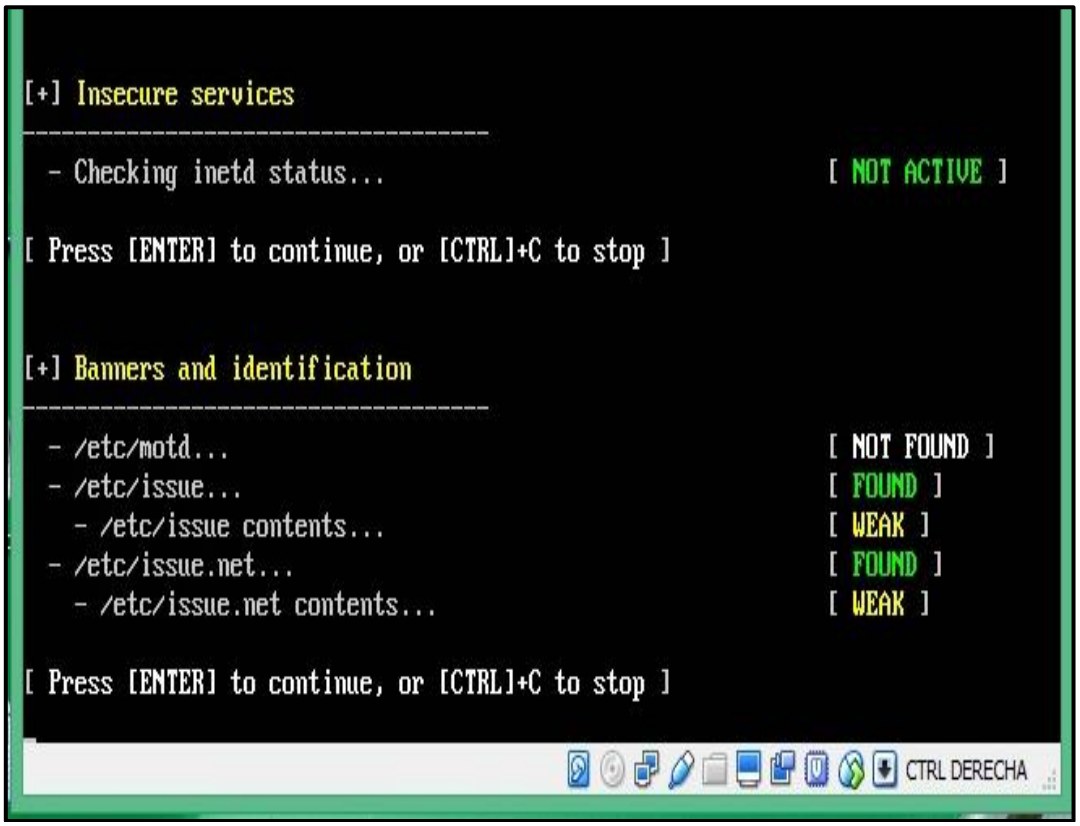
Seguidamente se analiza el servidor *Squid* y logs del sistema (figura 35), posteriormente se continúa con los servicios inseguros, Banners e identificación tal como se muestra en la figura 36.

Figura 35. Escaneo Lynis: Squid, Logging and files



Fuente: autor

Figura 36. Servicios Inseguros, Banners e identificación



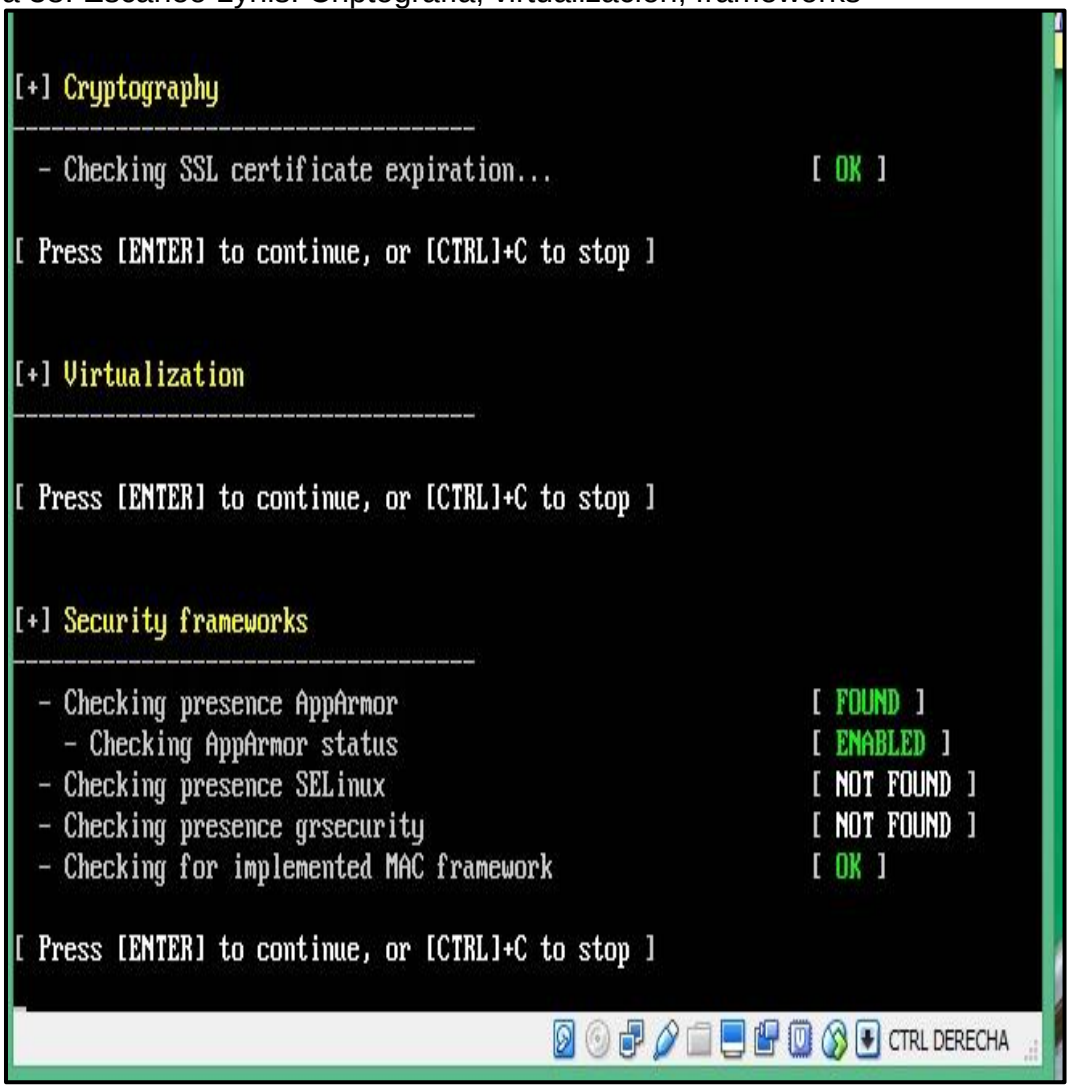
Fuente: autor

A continuación, se analizan las tareas programadas, la información de la cuenta, el estado del servidor de hora y sincronización Prosigue el análisis de la criptografía del sistema y los aspectos relacionados con la virtualización y seguridad de *frameworks*. Los resultados generados por los análisis realizados se plasman en las figuras 37 y 38 respectivamente.

Figura 37. Escaneo Lynis: Scheduled tasks, Accounting, Tiempo de sincronización

Fuente: autor

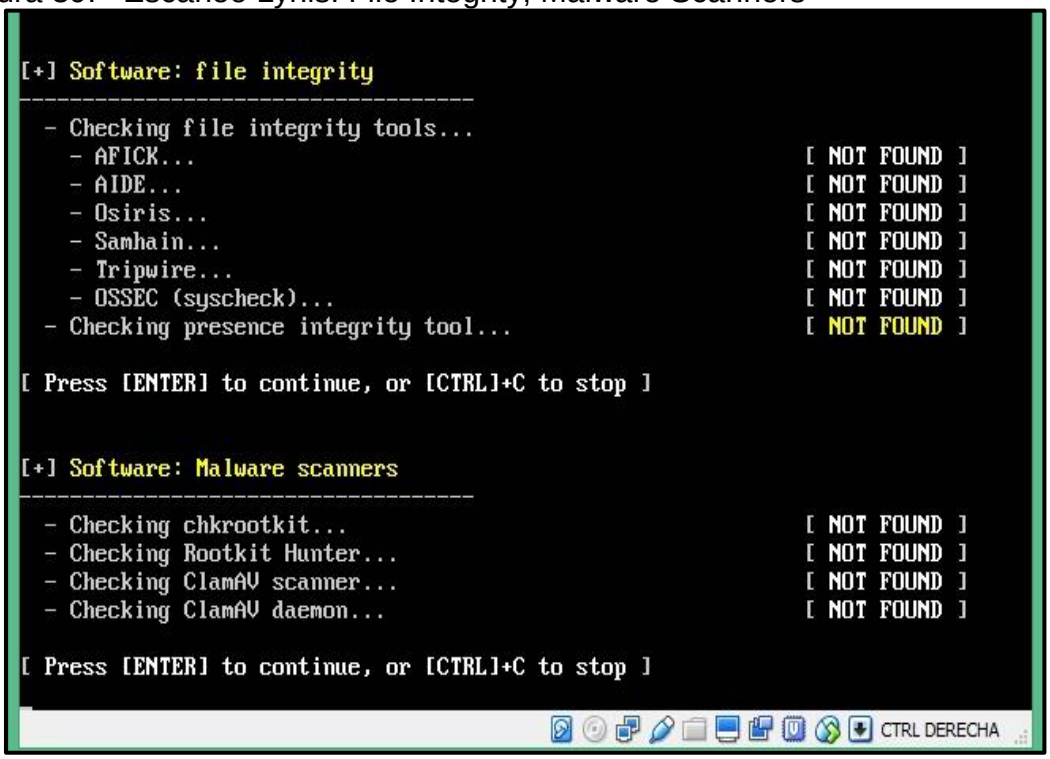
Figura 38. Escaneo Lynis: Criptografía, virtualización, frameworks



Fuente: autor

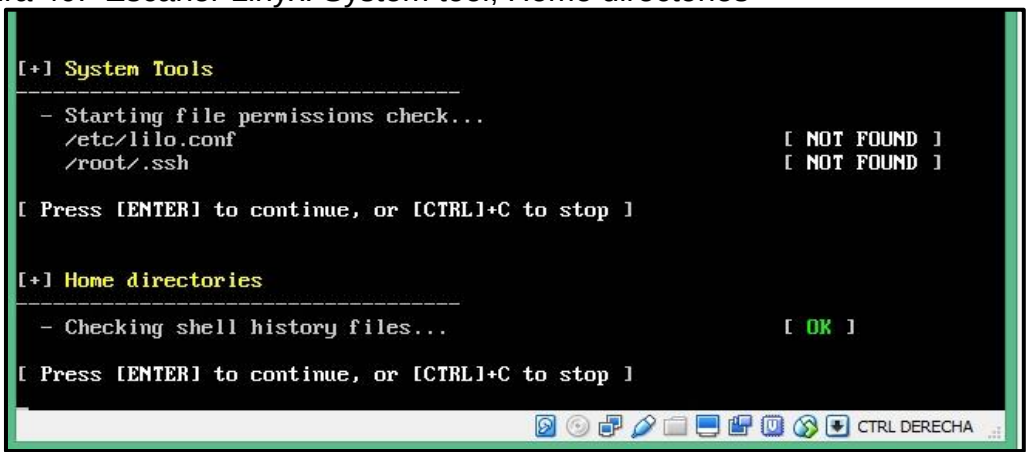
El análisis continúa con la integridad de archivos y el escáner de malware (si está instalado) (ver figura 39), posteriormente las herramientas del sistema y los directorios también son escaneados (ver figura 40).

Figura 39. Escaneo Lynis: File Integrity, Malware Scanners



Fuente: autor

Figura 40. Escaner Linyx: System tool, Home directories



Fuente: autor

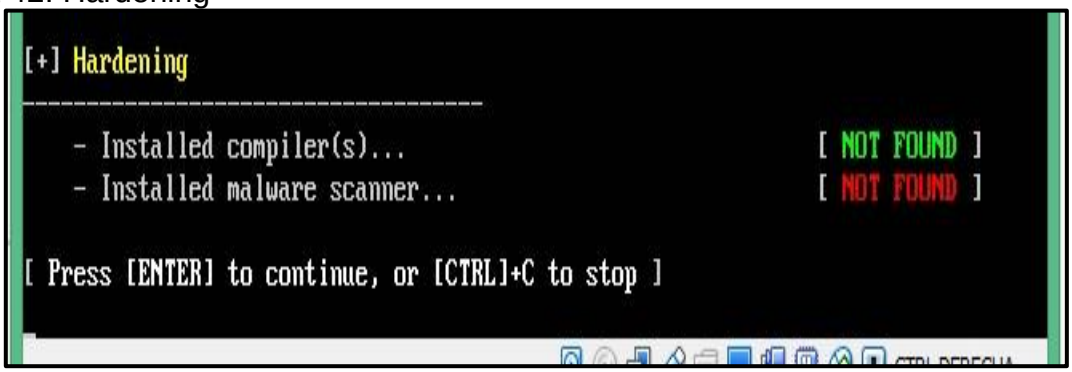
Finalmente se realiza un escáner del *kernel*, en el cual se verifica que existan herramientas o configuraciones que permitan mayor seguridad en el mismo (Figura 41) y programas o procesos adicionales de hardening (Figura 42). Por último, se

presenta un resumen de las vulnerabilidades encontradas, y se muestra la ubicación de los reportes generados (Figura 43).

Figura 41. Escaneo Lynis: Kernel Hardening

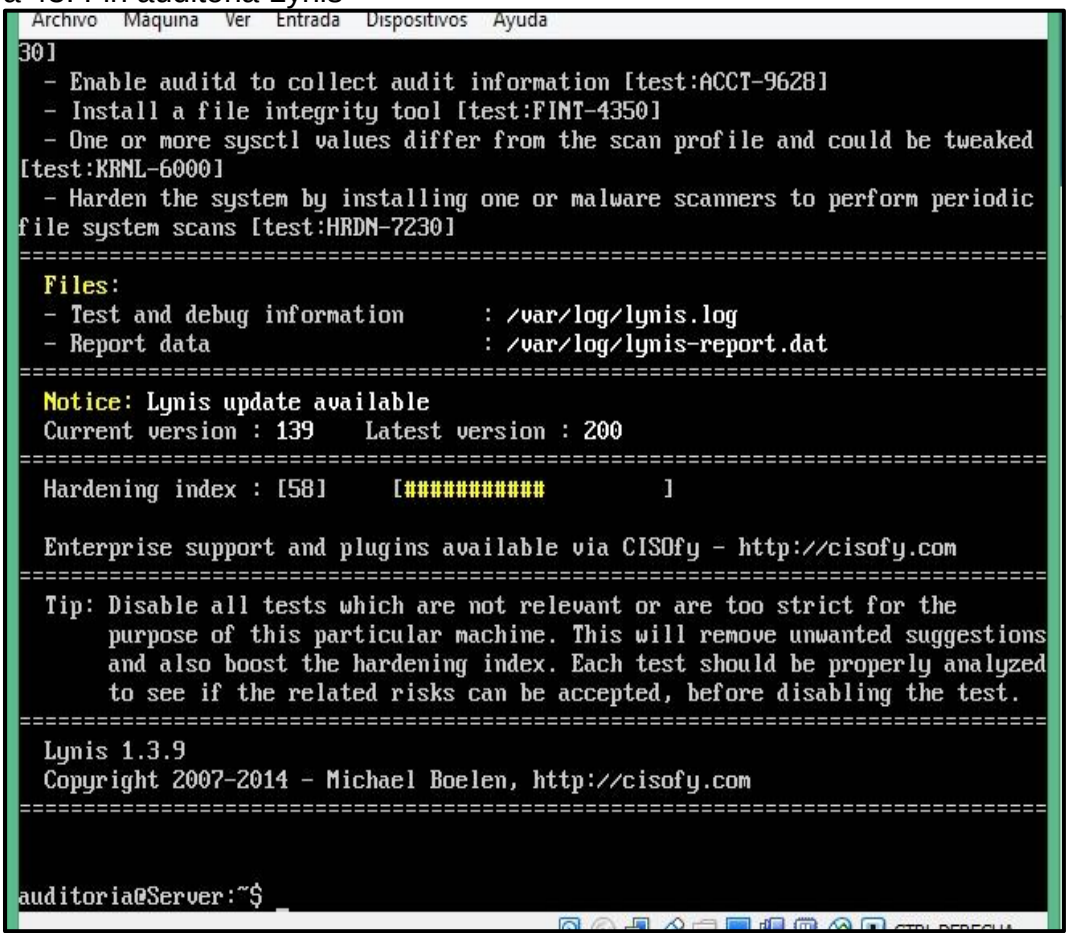
Fuente: autor

Figura 42. Hardening



Fuente: autor

Figura 43. Fin auditoria Lynis



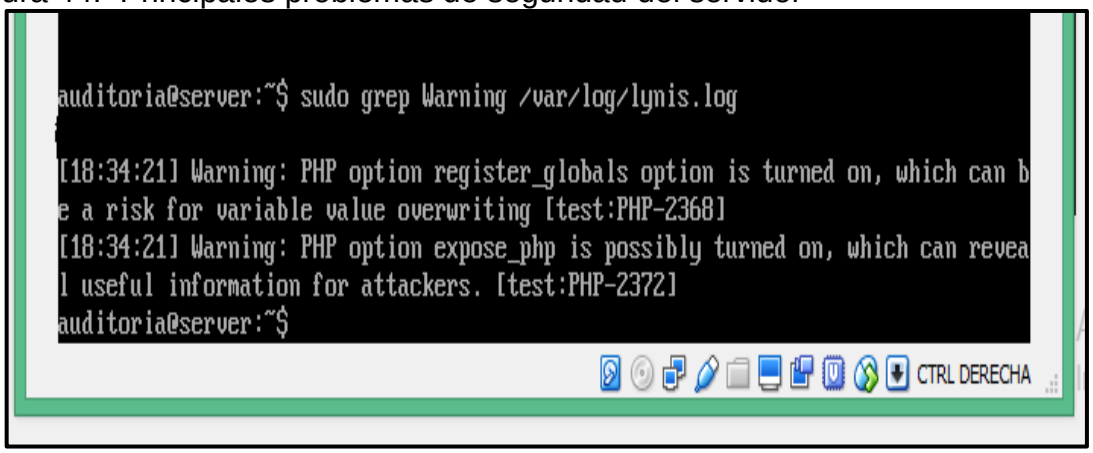
Fuente: autor

6.3 VULNERABILIDADES DETECTADAS POR LINYS.

Teniendo los resultados de la auditoría realizada a la configuración del servidor Ubuntu 14.04, se procede a establecer una matriz de riesgo basada en la metodología Magerit, ya conociendo las configuraciones por defecto presentes en el servidor, cabe resaltar que el objetivo de este proyecto son las configuraciones del servidor, por lo cual el análisis de riesgo solamente se realizará en base a sus configuraciones que representan alguna vulnerabilidad.

Para visualizar las principales fallas de seguridad halladas por linys se usa el siguiente código *Sudo grep Warning /var/log/lynis.log*. (Figura 44):

Figura 44. Principales problemas de seguridad del servidor



Fuente: autor

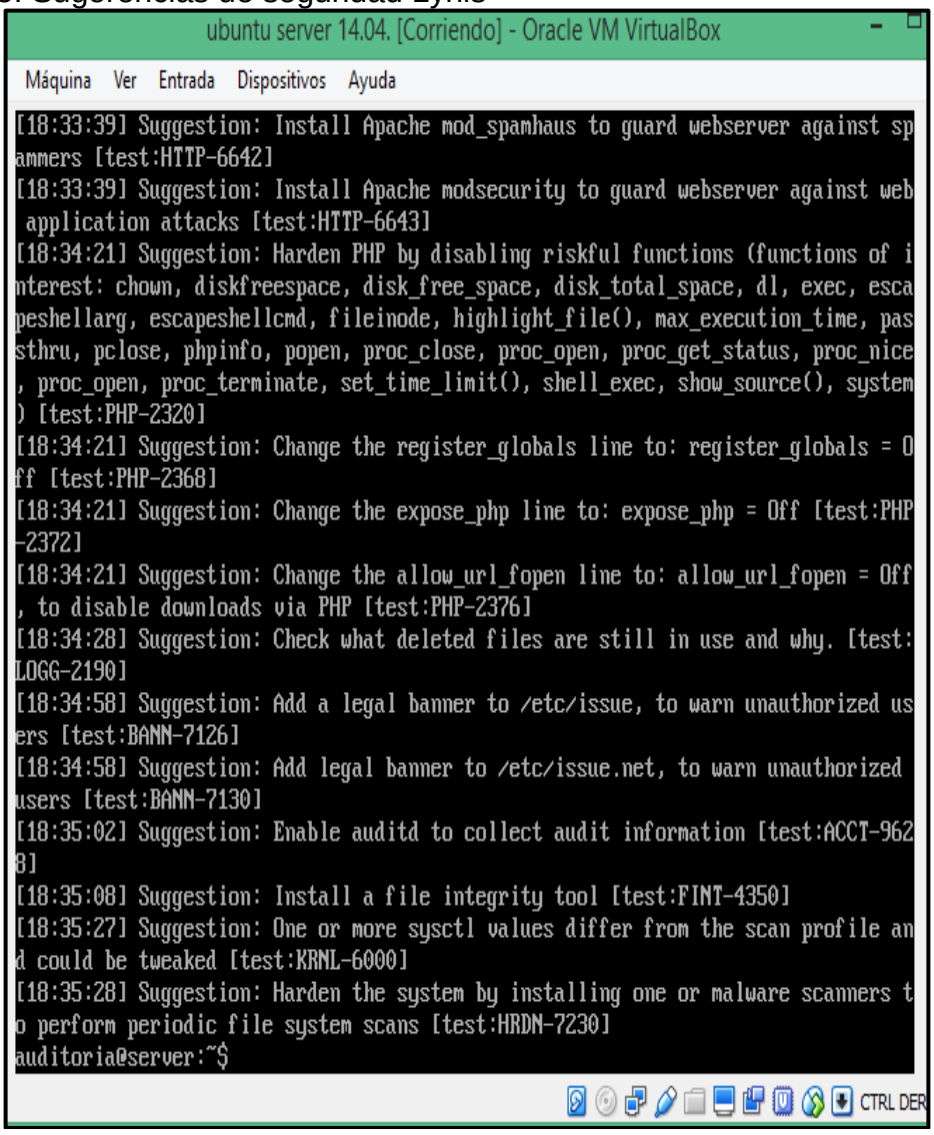
Los dos principales problemas de seguridad identificados son:

- Opción global opción de registro activada, que puede ser un riesgo para el valor variable de sobreescritura.

- Opción *expose_PHP* esta activada, puede revelar información útil para los atacantes.

Para visualizar las recomendaciones de seguridad que proporciona lynis se usa el siguiente código *Sudo grep Suggestion /var/log/lynis.log*. (Figura 45):

Figura 45. Sugerencias de seguridad Lynis



Fuente: autor

Teniendo en cuenta que el objetivo del proyecto es identificar las principales vulnerabilidades del servidor Ubuntu 14.04 no se ahondará en las sugerencias de seguridad, ya que si bien son un aspecto que puede tomar importancia para mejorar el nivel de seguridad, no todas las sugerencias se realizan por causa de una vulnerabilidad, algunas solo buscan fortalecer aún más la seguridad. Por lo anterior solo se han tenido en cuenta las recomendaciones que traducen la ausencia de alguna herramienta de seguridad como lo son:

- Firewall desactivado
- No presencia de antimalware

6.4 VULNERABILIDADES DE UBUNTU SERVER 14.04 IDENTIFICADAS EN FOROS WEB

En este apartado se ha consultado en las principales páginas y/o foros donde se informan las distintas vulnerabilidades que tienen las versiones de los sistemas Ubuntu, esto con el objetivo de complementar la detección de vulnerabilidades en las configuraciones por defecto del servidor Ubuntu, ya que según los resultados encontrados algunas vulnerabilidades vienen inmersas como un error de configuración del sistema y no como una debilidad.

Las configuraciones por defecto que representan algún riesgo en la seguridad del servidor Ubuntu debido principalmente a errores presenten en el servidor son:

6.4.1 *Kernel*. El *kernel* del servidor no limita el espacio que puede ocupar el archivo en el cual se guardan los registros y se está expuesto a una denegación de servicio.

6.4.2 Usuarios, grupos y autenticación. Debido a un error en el controlador multisistema, un usuario local puede llegar a tener acceso a información privada escalando privilegios.

Además de los problemas de seguridad por defecto anteriormente mencionados, se han encontrado algunos otros errores, los cuales se solucionan solamente actualizando el sistema con los códigos:

- *sudo apt-get-update*
- *sudo apt-get upgrade*

6.5 ANÁLISIS DE RIESGO MAGERIT

Conociendo las vulnerabilidades presentes en las configuraciones por defecto del servidor Ubuntu 14.04 se procede a realizar una matriz de riesgo para analizar los riesgos a los que se está expuesto, cabe reiterar que este proyecto está enfocado solamente en las configuraciones por defecto del servidor, por lo cual solamente se tendrá en cuenta esto para realizar la matriz. Posteriormente con el análisis de los resultados se establecerán los controles pertinentes, los cuales hacen parte del producto a entregar, es decir, los controles se documentarán y se identificarán como los lineamientos adicionales a tener en cuenta al momento de auditar un servidor de esta distribución y versión.

Se utilizará como referencia la metodología de análisis de riesgo Magerit en cuanto sea pertinente, teniendo en cuenta que el proceso va desde el análisis hasta el tratamiento (controles a ejecutar) de los riesgos. Como punto de partida es necesario establecer el contexto del análisis.

6.5.1 Determinación del contexto. Es algo difícil especificar un contexto en este caso debido al objeto del proyecto, lo que se busca es identificar y controlar los riesgos de la configuración por defecto de un servidor, por lo cual es algo muy general ya que cambiará dependiendo del sistema en el cual se encuentre implementado, para este caso el contexto es un servidor que no tiene mayores servicios instalados, solamente los servicios elementales (Apache, Mysql, PHP) en sus configuraciones por defecto, el cual requiere que su configuración básica ofrezca un nivel de riesgo bajo.

6.5.2 Análisis de riesgo. Antes de realizar la matriz de riesgo es necesario establecer los parámetros o los niveles asignados a la probabilidad, impacto y riesgo, para este caso se tomarán como referencia los datos asignados en las tablas 5, 6 y 7.

Tabla 5. Análisis de riesgo metodología Magerit a configuraciones por defecto de Servidor Ubuntu 14.04

ÍTEM	ACTIVO	CLASE DE ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
1	Kernel	Software	Ataques de denegación de servicio	FRECUENTE	IMPORTANTE	MAYOR
2	Usuarios, grupos y autenticación Sistema de archivos	Software	Acceso a información confidencial	NORMAL	IMPORTANTE	MODERADO
			Ejecución de Procesos no autorizados	NORMAL	MUY GRAVE	MODERADO
3	PHP (variables globales)	Software	Ejecución remota de código	FRECUENTE	MUY GRAVE	MAYOR
4	PHP (expose_PHP)	Software	Acceso a información sobre la versión de PHP (facilita un ataque)	MUY FRECUENTE	MODERADO	MODERADO
5	Firewall (Desactivado)	Software	Acceso de intrusos a la red	NORMAL	IMPORTANTE	MODERADO
6	Inexistencia de Malware	Software	Presencia de programas malintencionados	POCO FRECUENTE	MODERADO	MENOR

Fuente: autor

En la tabla 6 se puede observar el análisis de riesgo, con calificaciones cuantitativas:

Tabla 6. Análisis de riesgo cuantitativo

ÍTEM	ACTIVO	CLASE DE ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
1	Kernel	Software	Ataques de denegación de servicio	4	4	16
2	Usuarios, grupos y autenticación	Software	Acceso a información confidencial	3	4	12
	Sistema de archivos		Ejecución de Procesos no autorizados	3	5	15
3	PHP (variables globales)	Software	Ejecución remota de código	4	5	20
4	PHP (expose_PHP)	Software	Acceso a información sobre la versión de PHP (facilita un ataque)	5	3	12
5	Firewall (Desactivado)	Software	Acceso de intrusos a la red	3	4	12
6	Inexistencia de Malware	Software	Presencia de programas malintencionados	2	3	6

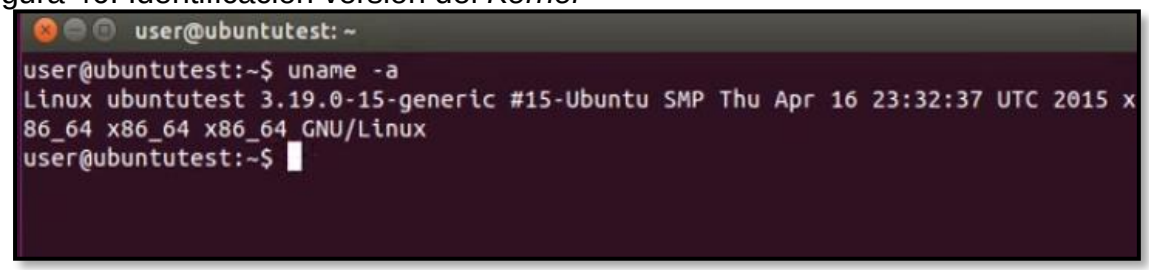
Fuente: autor

Antes de establecer los controles pertinentes ante cada riesgo, se documentarán pruebas que corroboren algunas de las vulnerabilidades detectadas.

6.5.3 Escalamiento de privilegios. Se ha comprobado la veracidad de esta vulnerabilidad, trata de un error en la comprobación de permisos, por lo cual un usuario local puede escalar privilegios.

En la figura 46 se muestra el primer paso, el cual es comprobar la versión del *kerne*l, para ello se usa el código: Uname –a

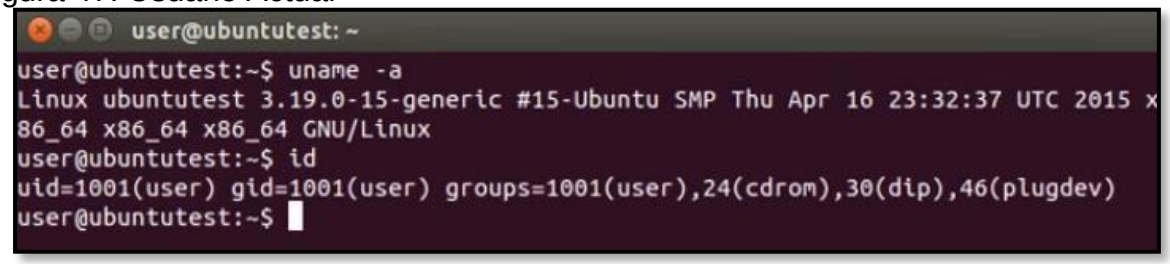
Figura 46. Identificación versión del *Kernel*



Fuente: https://www.youtube.com/watch?v=LcdgzeXmJz4

Ahora se verifica el usuario actual (figura 47), en este caso es un usuario distinto al *root*.

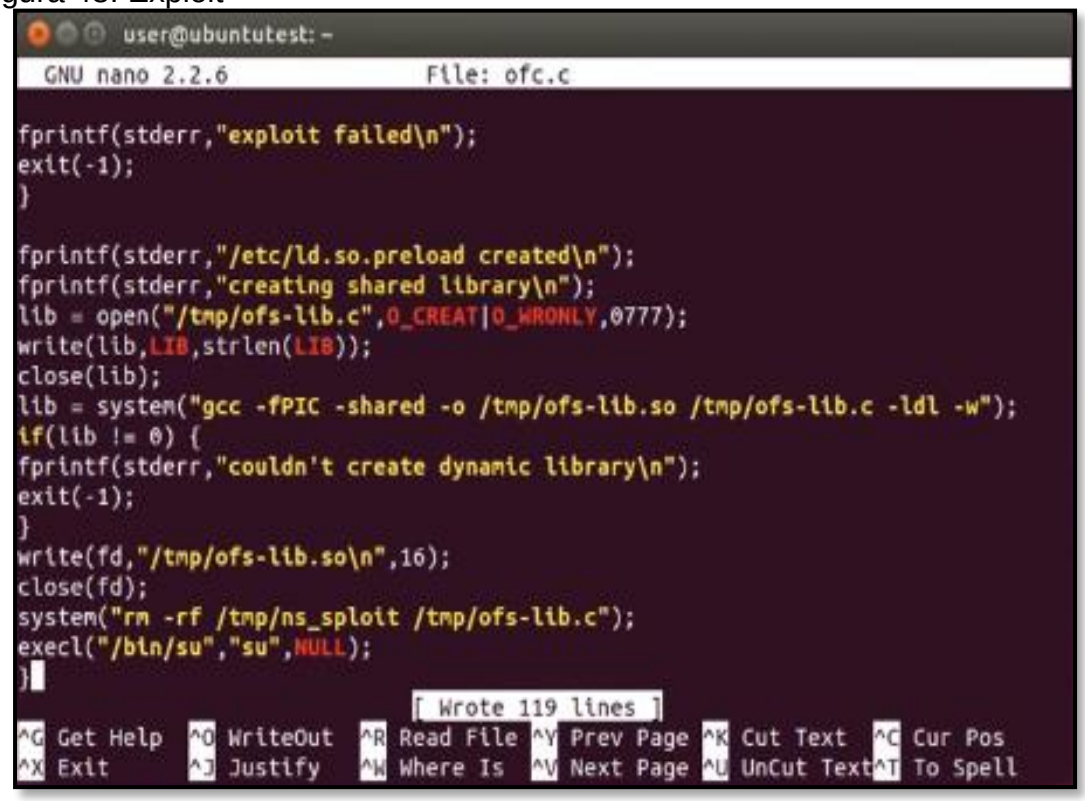
Figura 47. Usuario Actual



Fuente: https://www.youtube.com/watch?v=LcdgzeXmJz4

Posteriormente se crea un *exploit* para realizar el ataque (Figura 48), en este caso llamado ofc.

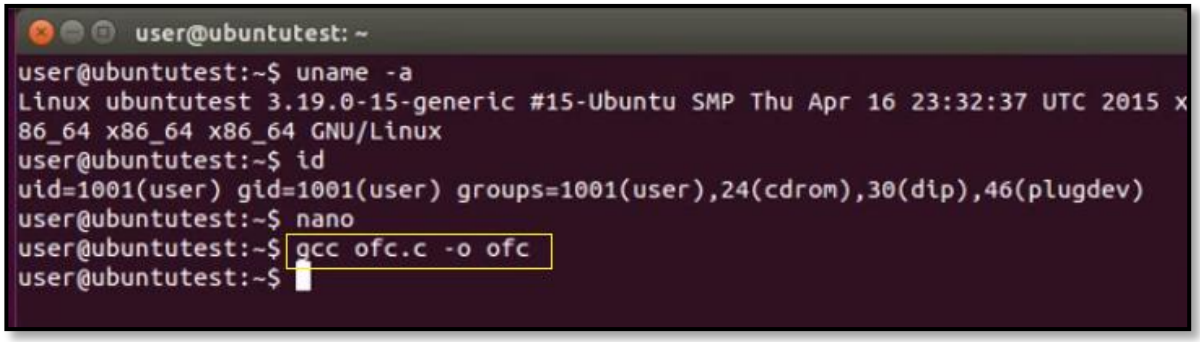
Figura 48. Exploit



Fuente: https://www.youtube.com/watch?v=LcdgzeXmJz4

Habiendo guardado el exploit creado, se compila el mismo (figura 49), utilizando el código: *Gcc ofc.c –o ofc*

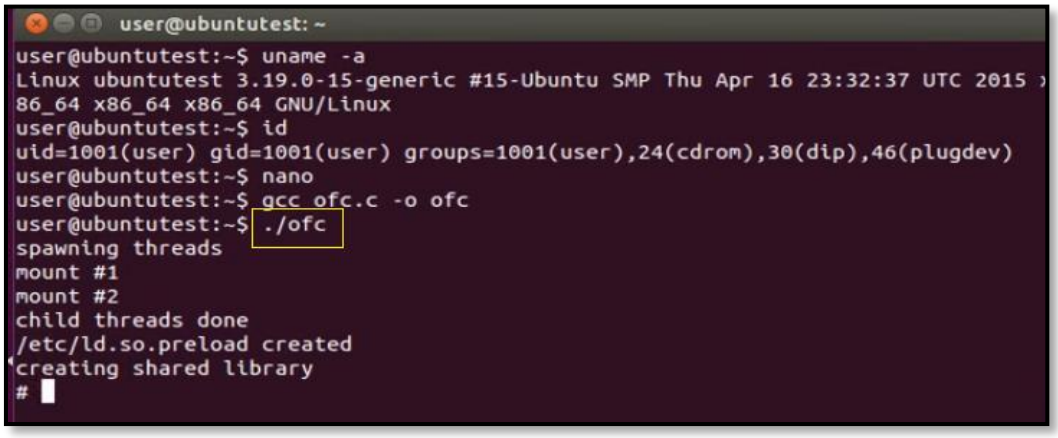
Figura 49. Compilación del *exploit*



Fuente: https://www.youtube.com/watch?v=LcdgzeXmJz4

El siguiente paso consiste en ejecutar el programa compilado (figura 50).

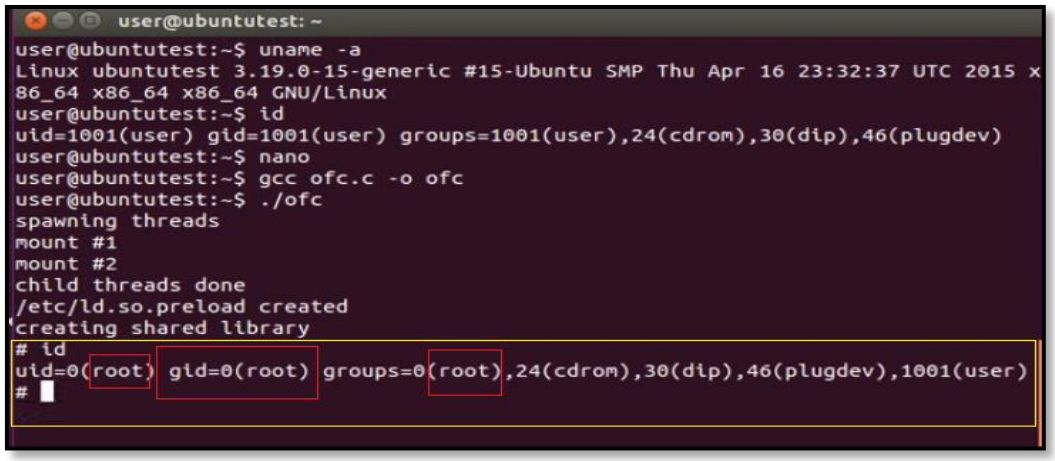
Figura 50. Ejecución del Exploit



Fuente: https://www.youtube.com/watch?v=LcdgzeXmJz4

Por último, se vuelve a verificar el usuario actual, y se puede observar que ahora el usuario es *root* (figura 51).

Figura 51. Escalamiento de Privilegios

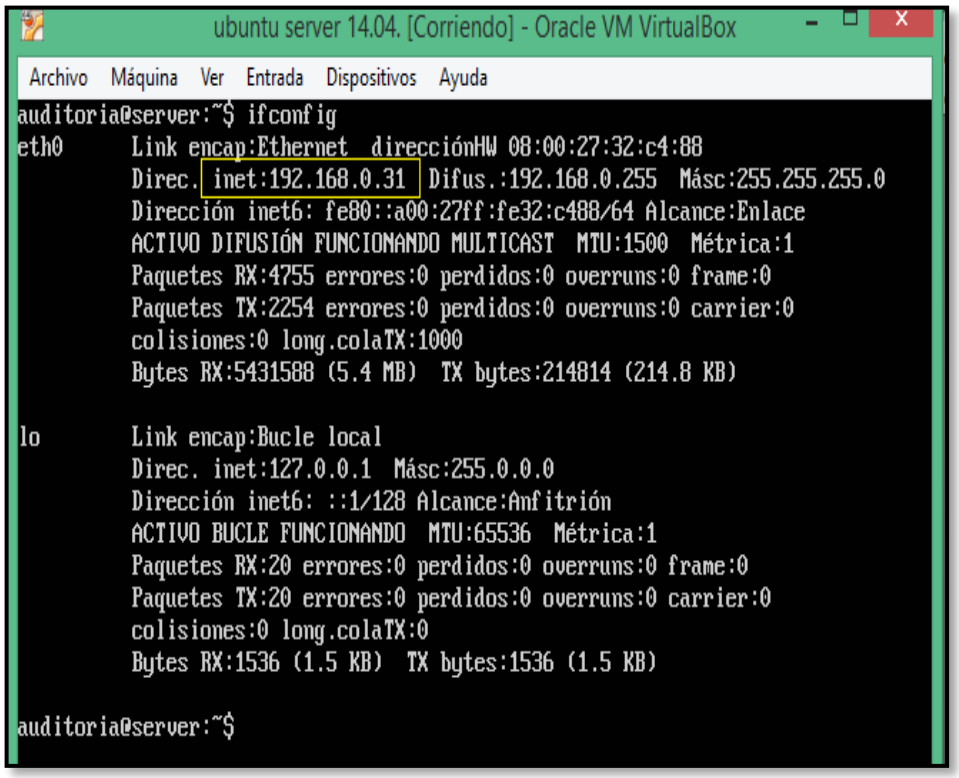


Fuente: https://www.youtube.com/watch?v=LcdgzeXmJz4

6.5.4 Cabeceras HTML. Esta vulnerabilidad consiste en que la opción *expose_PHP* se encuentra por defecto activada, lo cual permitirá para cualquier persona ver la versión del servidor web, solo es necesario tener la dirección IP del mismo.

El primer paso es verificar la IP del servidor, para ello en Ubuntu Server 14.04 digitamos: *Ifconfig*

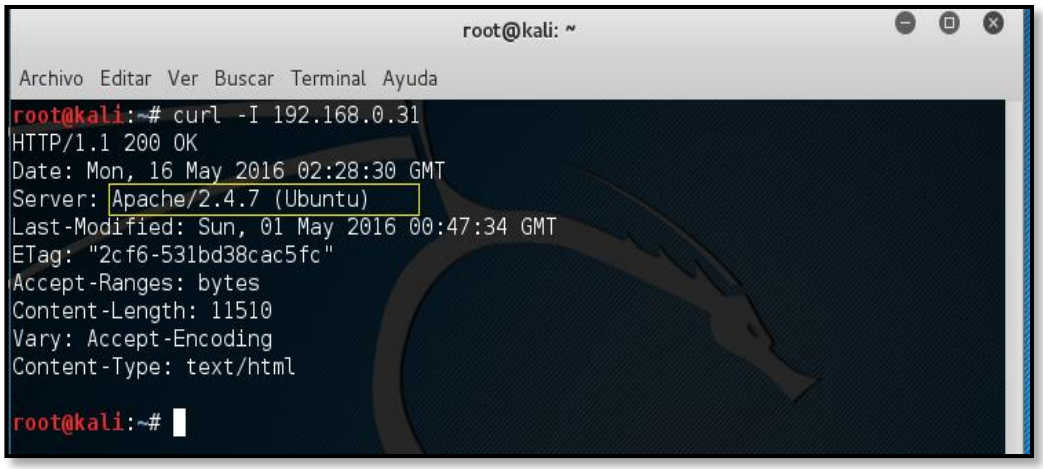
Figura 52. IP del Servidor



Fuente: autor

Conociendo la dirección IP del servidor, se procede en otro sistema a visualizar la cabecera HTML con el código: *curl –I 192.168.0.31*

Figura 53. Cabecera HTML



Fuente: autor

Se puede observar en la figura anterior la versión del servidor, esto puede representar una ventaja para el atacante para estudiar las vulnerabilidades de las versiones y sistemas operativos.

6.6 INFORME DE AUDITORIA

6.6.1 Presentación de la auditoria. Se realizó un análisis de seguridad en cuanto a las configuraciones por defecto de la distribución Linux Ubuntu 14.04 mediante un software especializado en auditar el software y las configuraciones presente en determinado sistema, además de esto también se indagó en foros relacionados a problemas de seguridad identificados en el sistema operativo analizado.

6.6.2 Objetivo general auditoría. Establecer nivel de riesgo al que se encuentra la distribución Linux Ubuntu 14.04 en sus configuraciones por defecto.

6.6.3 Objetivos específicos auditoría

- Identificar vulnerabilidades presentes en configuraciones por defecto de Ubuntu 14.04

- Determinar nivel de riesgo al que se encuentra expuesta la distribución Linux Ubuntu 14.04 en sus configuraciones por defecto

6.6.4 Alcance auditoría. El análisis de seguridad realizado a la distribución Linux Ubuntu 14.04 está enfocado en las configuraciones por defecto con las cuales se instala dicho sistema, para determinar los riesgos presentes en estas se recurrió a foros y un software de auditoría.

Al realizar el análisis de riesgo se identificaron seis activos que presentan vulnerabilidades y se establecieron cinco distintos controles para mitigar el riesgo. Teniendo esto en cuenta se tienen las siguientes conclusiones:

6.6.4 Conclusiones auditoría. En cuanto a los riesgos identificados por causa de las configuraciones por defecto, se encontraron seis parámetros que aumentan la exposición a:

- Ataques de denegación de servicio
- Remotamente se puede cambiar el valor de algunas variables
- Un usuario podría tener permisos para realizar acciones no autorizadas

- Pueden existir intrusos en la red sin que sean identificados
- Se está revelando información de versiones y sistema
- Algunos programas malintencionados no se podrían detectar

Las configuraciones por defecto de Ubuntu 14.04 contienen algunos parámetros que aumentan el riesgo de ser víctima de algún tipo de ataque que podría generar la caída del servicio ofrecido o la alteración de información propia por parte de un agente externo.

6.6.5 Recomendaciones. Se recomienda establecer una periodicidad de actualización del sistema para garantizar que el sistema utilizado se encuentre al día en cuanto a parches de seguridad desarrollados continuamente por la comunidad canonical de Ubuntu.

La desactivación de algunas configuraciones que por defecto vienen activas en los servicios instalados de la distribución Linux Ubuntu 14.04 permitiría reducir la exposición del sistema, por lo cual se debe garantizar que las características activas sean las necesarias y no aumenten el nivel de exposición al riesgo.

Se recomienda utilizar software de seguridad que permita detectar la presencia en la red o en el equipo de programas o personas no autorizados.

6.7 TRATAMIENTO DE RIESGOS

Teniendo en cuenta la matriz de riesgos realizada se han de determinar controles pertinentes según lo amerite el nivel en el que se ubique cada riesgo, en este caso todos los riesgos se mitigarán, ninguno se va a aceptar, ya que no representan costo alguno, por lo cual es poco probable que alguna entidad prefiera asumir el riesgo conociendo que los controles pertinentes se pueden implementar con una serie de configuraciones y/o software libre.

Tomando como base la matriz de riesgos elaborada, se complementará con el control necesario para mitigar el riesgo tratado.

Tabla 7. Establecimiento de controles

ÍTEM	ACTIVO	AMENAZA	RIESGO	CONTROL
1	Kernel	Ataques de denegación de servicio	MAYOR	Actualizar el sistema para que se instale el parche que corrige esta vulnerabilidad, el paquete es inux-image-3.13.0-65 PowerPC-e500 3.13.0-65.106
2	Usuarios, grupos y autenticación	Acceso a información confidencial	MODERADO	
	Sistema de archivos	Ejecución de Procesos no autorizados	MODERADO	
3	PHP (variables globales)	Ejecución remota de código	MAYOR	Desactivar la opción de variables globales
4	PHP (expose_PHP)	Acceso a nformación sobre l versión de PHP (facilita un ataque)	MODERADO	Desactivarla opción expose_PHP
5	Firewall (Desactivado)	Acceso de intrusos la red	MODERADO	Activar firewall
6	Inexistencia de Malware	Presencia de programas malintencionados	MENOR	Instalación de Rkhunter

Fuente: autor

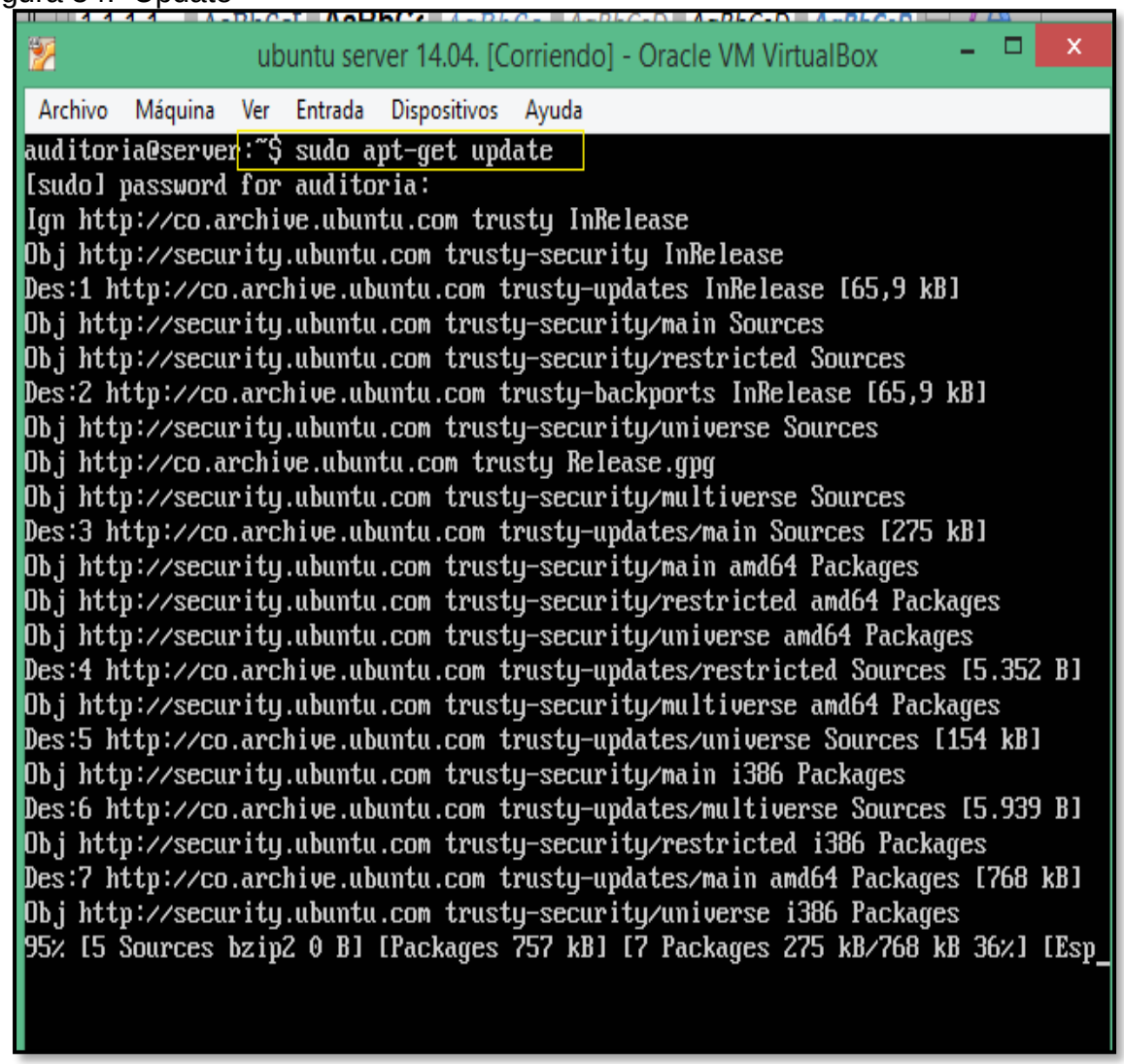
6.7.1 Actualización del sistema. Actualizando el sistema se resuelven los problemas del kernel del servidor y con ello el problema de autenticación que permitía escalamiento de privilegios. Además de esto se debe configurar el servidor para que se actualice automáticamente.

Para realizar la actualización del sistema se usan los siguientes códigos:

- *Sudo apt-get update (*ver figura 54)

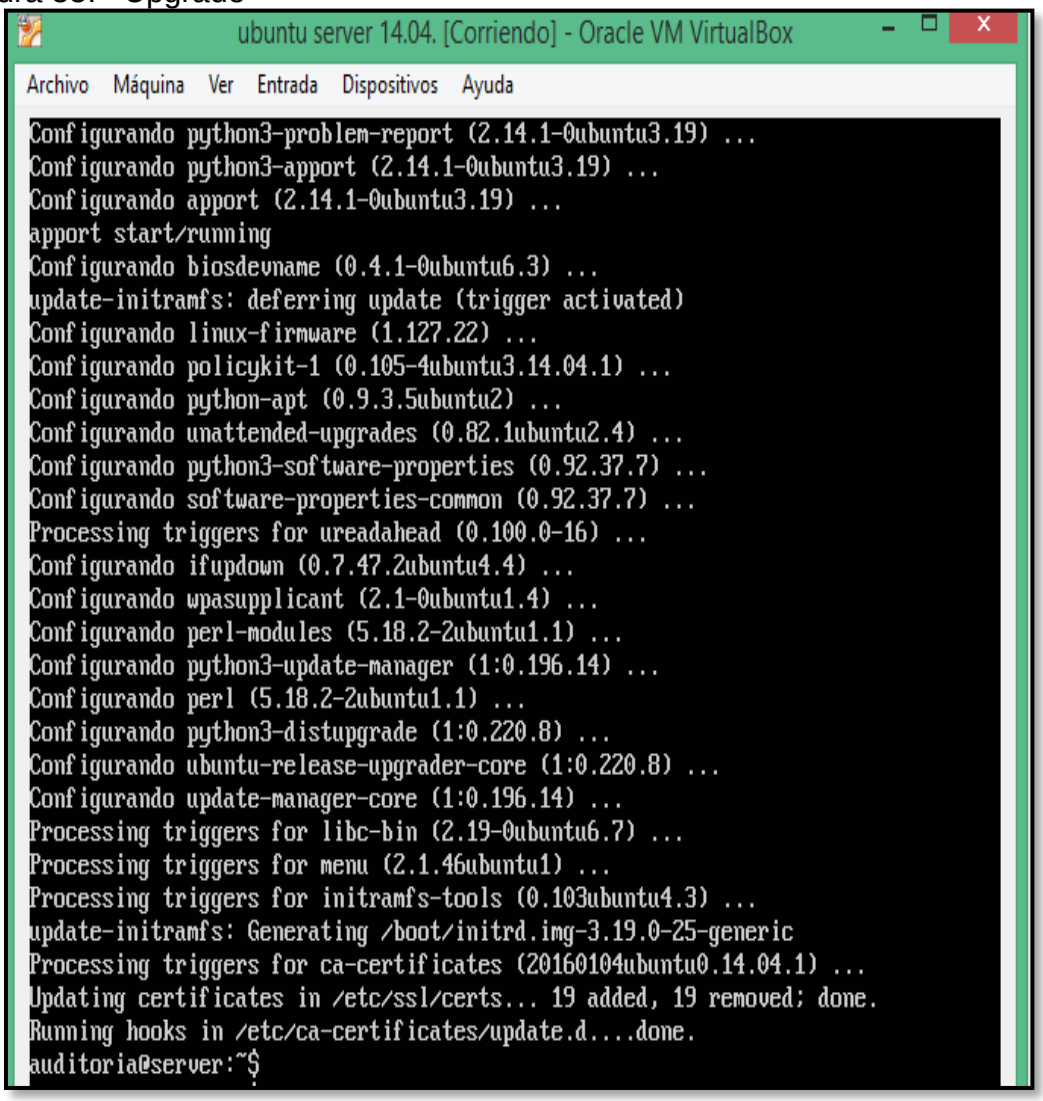
- *Sudo apt-get upgrade* (ver figura 55)

Figura 54. Update



Fuente: autor

Figura 55. Upgrade

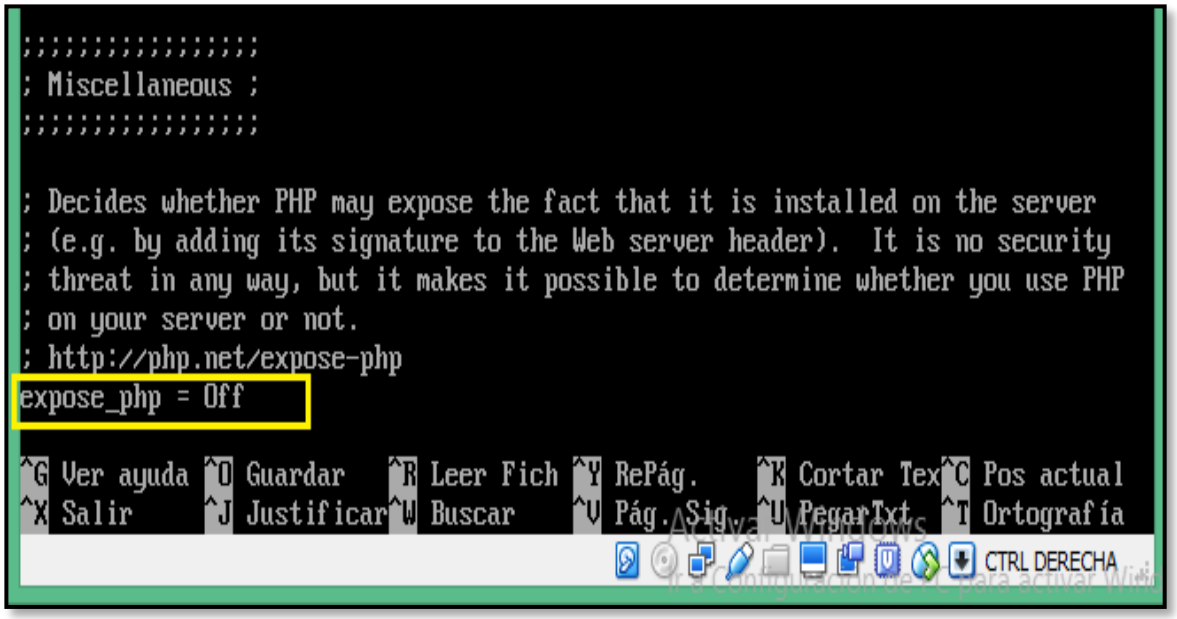


Fuente: autor

6.7.2 Desactivación de registros globales y expose_php. Para desactivar estas opciones basta con ingresar al archivo php.ini y modificar sus estados de on a off, esta configuración se muestra en la figura 56. Para ingresar al archivo se escribe el siguiente código:

Sudo nano /etc/php5/apache2/php.ini

Figura 56. Desactivación de registros globales y expose_php

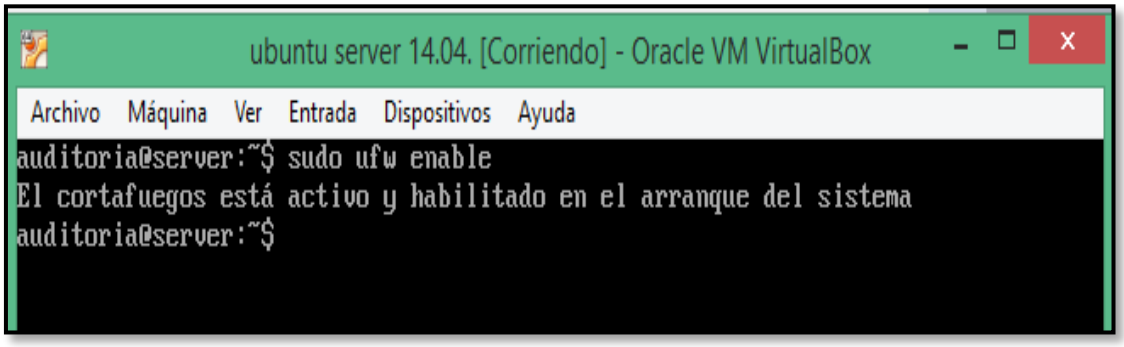


Fuente: autor

Es de aclarar que, para realizar la desactivación de registros globales en caso de no tener acceso a esta opción, es necesario realizar la solicitud de esta configuración al administrador del hosting.

6.7.3 Activación del firewall. En la figura 57 se muestra la activación del firewall, para habilitar el firewall se usa el siguiente código:
Sudo ufw enable

Figura 57. Activación del firewall



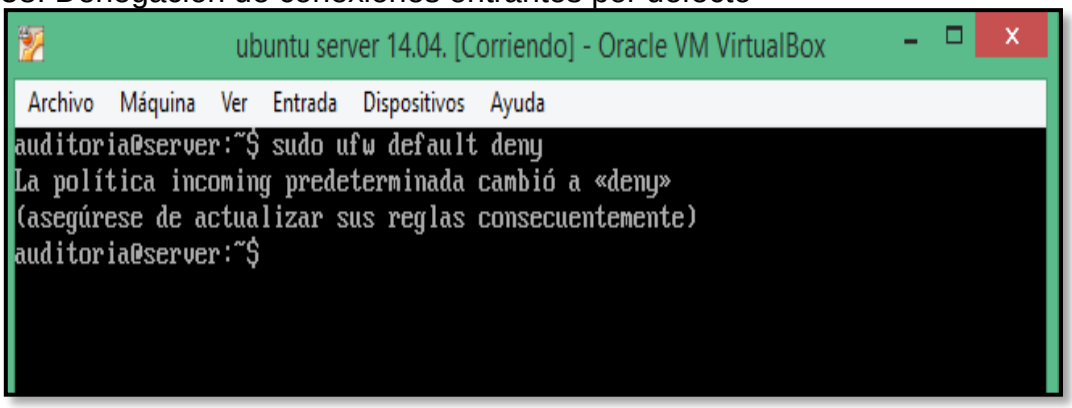
Fuente: autor

Una ventaja del servidor Ubuntu es que por defecto los puertos se encuentran cerrados, por lo cual no es necesario como en la mayoría de servidores comenzar a verificar puertos que no se estén utilizando para cerrarlos.

Luego de tener activo el firewall se considera como una buena práctica denegar todas las conexiones entrantes por defecto tal como se muestra en la figura 58, para ello se utiliza el código:

sudo ufw default deny

Figura 58. Denegación de conexiones entrantes por defecto



Fuente: autor

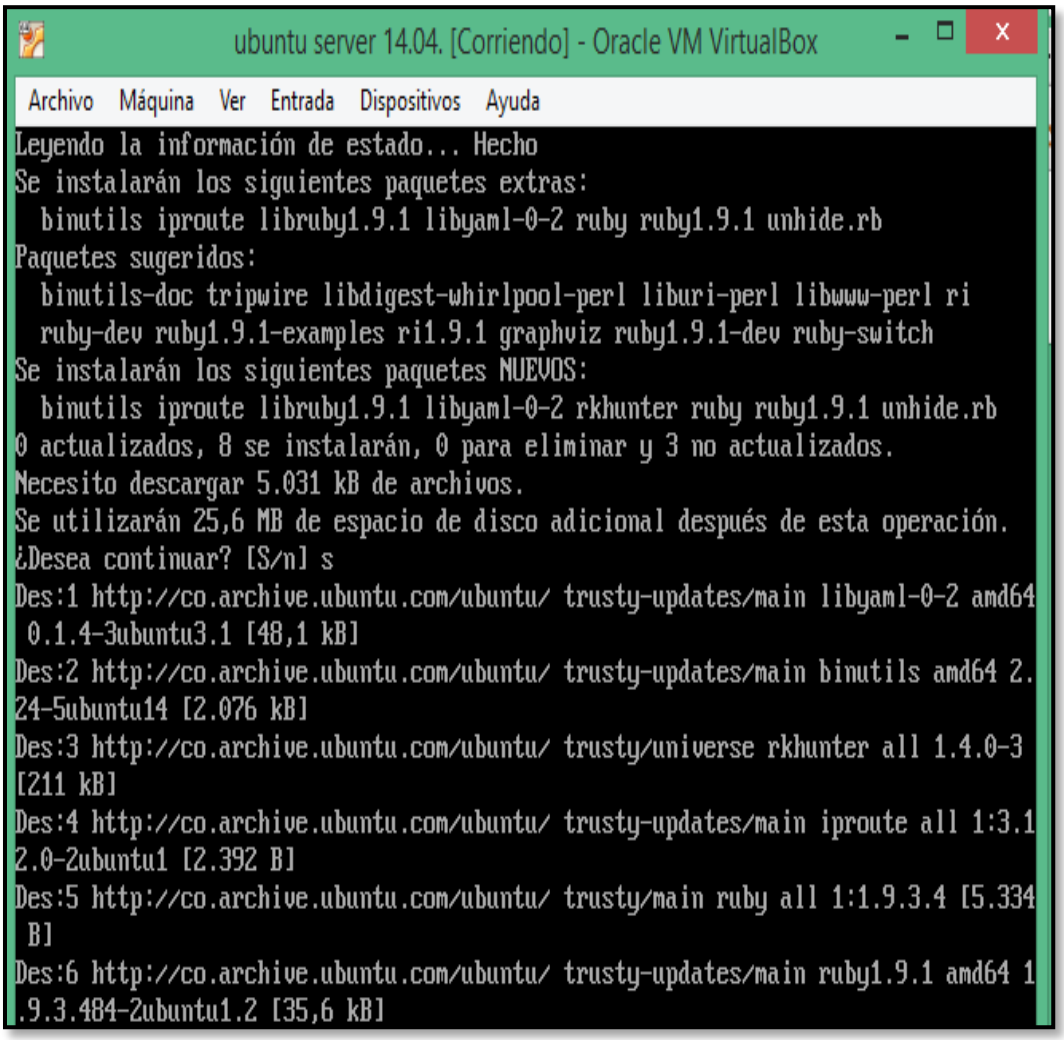
Posteriormente se deben habilitar los puertos que se requieran, es recomendable no utilizar los puertos que por defecto se utilizan con los principales servicios. Para habilitar un puerto se utiliza el siguiente código: *sudo ufw allow <número de puerto>*

Solo es cuestión de agregar el número de puerto requerido.

6.7.4 Instalación de Rkhunter. Para instalar este antimalware se usa el código:

*Sudo apt-get install rkhunter (*ver figura 59)

Figura 59. Instalación de Rkhunter



Fuente: autor

7. ANÁLISIS DE RESULTADOS

Estableciendo los controles descritos anteriormente se lograron corregir vulnerabilidades presentes en el servidor Ubuntu 14.04, lo cual permite un aporte significativo al momento de realizar auditorías internas en un sistema que contenga este tipo de servidor, ya que además de las consideraciones que se han de tener normalmente en las auditorias, se han lograron establecer los puntos importantes en materia de seguridad de la información.

A continuación (tabla 8), se presenta el resultado de los controles implementados en el servidor (riesgos residuales):

Tabla 8. Riesgo residual

ÍTEM	ACTIVO	CLASE DE ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
1	Kernel	Software	Ataques de denegación de servicio	MUY POCO FRECUENTE	MODERADO	INSIGNIFICANTE
2	Usuarios, grupos y autenticación	Software	Acceso a información confidencial	MUY POCO FRECUENTE	MODERADO	INSIGNIFICANTE
	Sistema de archivos		Ejecución de Procesos no autorizados	MUY POCO FRECUENTE	IMPORTANTE	INSIGNIFICANTE
3	PHP (variables globales)	Software	Ejecución remota de código	MUY POCO FRECUENTE	MUY GRAVE	MENOR
4	PHP (expose_PHP)	Software	Acceso a información sobre la versión de PHP (facilita un ataque)	MUY POCO FRECUENTE	MODERADO	INSIGNIFICANTE
5	Firewall (Desactivado)	Software	Acceso de intrusos a la red	MUY POCO FRECUENTE	IMPORTANTE	MENOR
6	Inexistencia de Malware	Software	Presencia de programas malintencionados	MUY POCO FRECUENTE	MODERADO	INSIGNIFICANTE

Fuente: autor

Como se puede observar en la tabla anterior, los riesgos se han minimizado considerablemente, en base a ella podemos deducir que los controles en riesgos por configuraciones tienen un nivel de eficiencia bastante alto.

En la tabla 9 se observa el resultado de los controles establecidos para tratar los riesgos en las configuraciones por defecto del servidor Ubuntu 14.04.

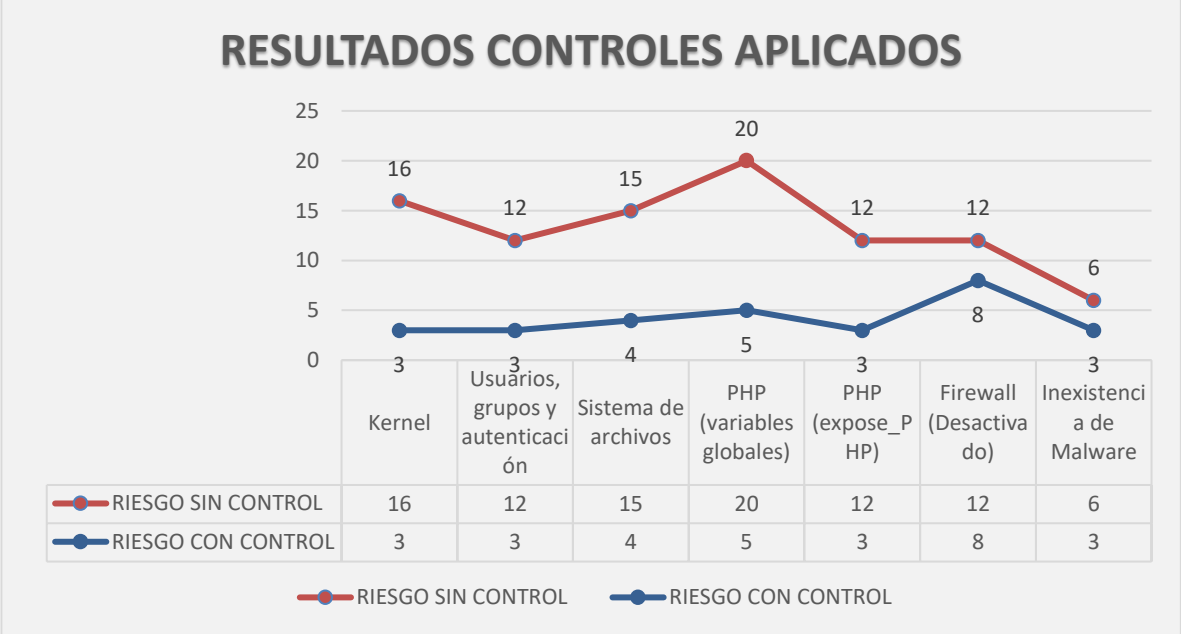
Tabla 9. Resultados controles aplicados

ÍTEM	ACTIVO	RIESGO SIN CONTROL	RIESGO CON CONTROL
1	Kernel	16	3
2	Usuarios, grupos y autenticación	12	3
	Sistema de archivos	15	4
3	PHP (variables globales)	20	5
4	PHP (expose_PHP)	12	3
5	Firewall (Desactivado)	12	8
6	Inexistencia de Malware	6	3

Fuente: autor

La siguiente figura (60) muestra de manera gráfica los resultados de los controles aplicados.

Figura 60. Resultados controles aplicados



Fuente: autor

El riesgo presente en las configuraciones por defecto que fueron detectadas y controladas en este proyecto representa en general un impacto considerable a tener en cuenta, y deben ser tratados de una manera prioritaria, teniendo en cuenta que este puede ser el punto de partida para el aseguramiento de un sistema.

8. DIVULGACIÓN

Teniendo en cuenta que no es un proyecto aplicado directamente en una organización, se ha decidido dejar este trabajo a disposición de la Universidad Nacional Abierta y a Distancia como un aporte al conocimiento, este documento estará alojado en el repositorio institucional con la correspondiente cesión de derechos en cuanto a publicación del mismo.

9. CONCLUSIONES

Se realizó una auditoria a las configuraciones por defecto de la distribución Linux Ubuntu 14.04 y una consulta en distintos foros y páginas encontrando vulnerabilidades en:

- Kernel: Debido a que el servidor no limita el espacio que puede ocupar el archivo en el cual se guardan los registros, por lo cual se puede estar expuesto a una denegación de servicio.

- Usuarios, grupos y autenticación: Se ha detectado un error en el controlador multisistema, por lo cual un usuario local puede llegar a tener acceso a información privada escalando privilegios.

- PHP (variables globales):Se podría presentar ejecución remota de código teniendo en cuenta que por defecto esta opción viene activada lo cual permitiría alterar el valor de las variables desde la url.

- Expose_PHP activado: Puede revelar información sobre la versión de PHP que se maneja, lo cual permitiría a un atacante conocer determinadas características para realizar un ataque.

- Firewall desactivado: Podría facilitar el ingreso de intrusos a la red ya que no serían identificados.

- Inexistencia de antimalware: No se detectaría la presencia de programas malintencionados

Al realizar el análisis de riesgo se determinó la vulnerabilidad del *kernel* y las variables globales (PHP) como los dos factores con mayor nivel de riesgo, debido a su probabilidad de ocurrencia y su impacto.

Considerando los riesgos identificados y las pruebas documentadas sobre la explotación de algunas vulnerabilidades en las configuraciones por defecto de la distribución Linux Ubuntu 14.04 se determinaron los controles necesarios para mitigar los riesgos:

- Actualización del sistema para que se instale el paquete es inux-image-3.13.0-65 PowerPC-e500 3.13.0-65.106, el cual subsana la vulnerabilidad del *kernel* reduciendo la exposición ante un ataque de denegación de servicio, también corrige el error en el controlador multisistema que permite a un usuario local escalar privilegios.

- Desactivación de variables globales: Con esto se reduce el riesgo de ejecución remota de código para modificar el valor de alguna variable, teniendo en cuenta que las variables ya no serían globales.

- Desactivación expose PHP: Realizando esta acción no se brinda información en la cabecera HTTP de la versión de PHP utilizada, lo cual en cierto modo evita revelar información que permita detectar la versión utilizada.

- Activar firewall: Teniendo en cuenta que Ubuntu maneja por defecto los puertos cerrados, al activar el firewall se requiere habilitar los puertos a utilizar, estos se recomiendan no sean los convencionalmente utilizados.

- Instalar antimalware: Con esto se evita la presencia de programas mal intencionados.

La descripción realizada sobre el paso a paso de la aplicación de los controles determinados para tratar los riesgos identificados (Cap. 6.7), proporciona una guía para reducir el nivel de riesgo que presenta en sus configuraciones por defecto el servidor Ubuntu 14.04.

Teniendo en cuenta los resultados obtenidos se ha detectado que la efectividad de los controles es bastante alta cuando se trata de errores de configuración.

10. OBSERVACIONES Y RECOMENDACIONES

Se recomienda estar siempre actualizados en los foros que ofrece la comunidad canonical de Ubuntu, en la cual se desarrollan permanentemente soluciones a los problemas de seguridad encontrados en las distintas distribuciones.

BIBLIOGRAFÍA

ALBERT M.C. (2011) Enabling Process Accounting on Linux HOWTO.[En linea], [consultado]. Disponible en: http://www.tldp.org/HOWTO/text/Process-Accounting

AZPE. Detectadas nuevas vulnerabilidades en Ubuntu. Linuxadictos. 30 de Septiembre del 2015. [En linea]. [consultado el 23 de octubre de 2017] Disponible en: http://www.linuxadictos.com/detectadas-nuevas-vulnerabilidades-en-ubuntu.html

BOWEN RONDA. (2013). ¿Qué es el plan PHVA?. [En línea], [consultado el 13 de julio de 2017]. Disponible en: http://www. brighthubpm.com/methods-strategies/73268-what-is-plan-do-check-act/

CANONICAL. USN-2761-1: la vulnerabilidad del núcleo de Linux. 5 DE Octubre del 2015 [En línea], [consultado el 5 de octubre de 2017]. Disponible en: http://www.ubuntu.com/usn/usn-2761-1/

ESQUEMA NACIONAL DE SEGURIDAD. MAGERIT: versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid – España. 2012 [En línea] [consultado el 23 de noviembre de 2017]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

GÓMEZ LABRADOR, Ramón M. Administración de servidores Linux (Ubuntu/Fedora/Centos). Universidad de Sevilla. Sevilla-España. 2014. [En línea], [consultado el 23 de enero de 2018]. Disponible en: https://www.informatica.us.es/~ramon/articulos/AdminServidoresLinux.pdf

HESS KENETH. Ubuntu Server: The Linux Server Operating Systems Dark Horse. [En línea], [consultado el 23 de enero de 2018]. Disponible en: http://www.serverwatch.com/trends/article. php/3870141/Ubuntu-Server-The-Linux-Server-Operating-Systems-Dark-Horse.htm

INCIBE. Vulnerabilidad en la configuración por defecto para CURL y libcurl (CVE-2015-3153). 21 de enero del 2016. España. [En Línea]. Gobierno de España. [consultado el 23 de enero de 2018]. Disponible en: https://www.incibe.es/ vulnDetail/CERT/Alerta_Temprana/Actualidad_Vulnerabilidades/detalle_ vulnerabilidad/ CVE-2015-3153

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACION ICONTEC. Presentación de tesis, trabajos de grado y otros trabajos de

investigación. Colombia. 2008. [En línea], [consultado el 23 de enero de 2018]. Disponible en: http://66.165.175.235/campus18_20151/file.php/85/entorno_ de_ conocimiento/NTC 14862008.pdf

JARAMILLO CASTILLO C.M && RIOFRIO HERRERA J.C. Metodología para realizar la evaluación, detección de riesgos, vulnerabilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la editorial Don Bosco, mediante un test de intrusión de caja blanca. Universidad Politécnica Salesiana Ecuador: Sede Cuenca,. 2015. [En línea], [consultado el 23 de enero de 2018]. Disponible en: http://dspace.ups.edu.ec/handle/123456789/7910

MARTÍNEZ J.E, GIRALDO C.A. Auditoria de seguridad informática. Password S.A. [En línea], [consultado el 23 de enero de 2018]. Disponible en: http://artemisa.unicauca.edu.co/~ecaldon/ docs/audit/ponencia_PASSWORD_siti2004.pdf

METALBYTE. Debian sigue siendo la número uno en servidores. MuyLinux. 2013. [En línea], [consultado el 23 de enero de 2018].Disponible en: http://www.muylinux.com/2013/10/25/debian-sigue-numero-uno-en-servidores

NIXCRAFT. ¿Qué es Umask y Cómo configurar por defecto umask con Linux? [en linea]. [consultado el 23 de enero de 2018]. Disponible en: http://www.cyberciti. biz/tips/understanding-linux-unix-umask-value-usage.html

RIESGO Y CONTROL INFORMÁTICO. Estándar Magerit para Análisis de Riesgos Informático. Universidad Nacional Abierta y a Distancia. [en linea]. [consultado el 23 de enero de 2018]. Disponible en: http://datateca.unad. edu.co/ contenidos/233004/riesgos/leccin_8_estndar_magerit_para_anlisis_de_riesgos_informticos.html

SAYS Alex. Lynis: auditoría, hardening y seguridad de sistemas. 2 de Noviembre del 2014. [En Línea], [consultado el 23 de enero de 2018]. Disponible en: http://rm-rf.es/lynis-auditoria-hardening-seguridad-sistemas/

TABASSUM, M. Análisis de la evolución del software de Linux OS (Ubuntu). Ciencias de la Computación y Tecnología (ICCST). Editorial: IEEE. 28 Agosto del 2014. Kota Kinabalu–Malasia. [En línea], [consultado el 23 de enero de 2018].Disponible en: http://ieeexplore.ieee.org/xpl/article Details .jsp? arnumber=7045194

UBUNTU. Avisos de seguridad Ubuntu. Ubuntu. Disponible en: http://www.ubuntu.com/usn/

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. riesgo y control informático. Estándar Magerit para Análisis de Riesgos Informático. [en línea]. [consultado el 2 de diciembre de 2017]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_8_estndar_ magerit_ para_anlisis_de_riesgos_informticos.html

VELASCO Rubén. Canonical parchea una vulnerabilidad grave en Ubuntu. 6 de octubre del 2016. [En línea]. Redes Zone. [consultado el 23 de enero de 2018]. Disponible en: http://www.redeszone.net/2015/10/06/canonical-parchea-una-vulnerabilidad-grave-en-ubuntu/

_____. Nuevas vulnerabilidades críticas en el Kernel de Linux. 26 de Marzo del 2015. [En linea]. [consultado el 23 de enero de 2018]. Disponible en: http://www.redeszone.net/2015/03/26/nuevas-vulnerabilidades-criticas-en-el-kernel-de-linux/

ANEXOS

Anexo A. LINEAMIENTOS A TENER EN CUENTA EN CUANTO A SEGURIDAD EN CONFIGURACIONES POR DEFECTO DE UN SERVIDOR UBUNTU 14.04

Los sistemas Ubuntu a modo general representan un nivel de confiabilidad bueno, no se pueden encontrar muchas vulnerabilidades en sus configuraciones por defecto, lo cual indica que hay que prestar mayor atención a los aspectos generales establecidos por las normas legisladores de las auditorias en seguridad de la información (ISO 27001:2013).

El principal aspecto a tener en cuenta además de sus actualizaciones constantes son las configuraciones de PHP, ya que esto puede representar un nivel de riesgo considerable, teniendo en cuenta que algunas personas por ejemplo consideran conveniente habilitar las variables globales y se sienten cómodos con ellas, pero es un aspecto que representa un nivel de riesgo que es mejor mitigar.

Otro aspecto importante a tener en cuenta es la gestión de riesgo, si bien la norma establece de una manera muy completa las técnicas de identificar, evaluar y tratar los riesgos, se hace énfasis en esta parte porque es la columna vertebral de una auditoría, una minuciosa gestión de riesgo garantiza una excelente base para los demás puntos.

Las vulnerabilidades en configuraciones por defecto en el servidor Ubuntu 14.04 corregidas, no tienen mayor riesgo, ya que la eficiencia de los controles es bastante alta.

Anexo B. RAE

TITULO DEL PROYECTO	ANÁLISIS DE SEGURIDAD INFORMÁTICA APLICADO A DISTRIBUCIÓN DE LINUX UBUNTU 14.04 PARA CONTROLAR VULNERABILIDADES EN CONFIGURACIÓN POR DEFECTO
AUTOR	CABEZA SEGURA, JEISON SNEIDER
REFERENCIA APA	RIESGO Y CONTROL INFORMÁTICO. Estándar Magerit para Análisis de Riesgos Informático. Universidad Nacional Abierta y a Distancia. [En linea]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_8_estndar_magerit_para_anlisis_de_riesgos_informticos.html
	CANONICAL. USN-2761-1: la vulnerabilidad del núcleo de Linux. 5 DE Octubre del 2015 [en línea]. Ubuntu. Disponible en: http://www.ubuntu.com/usn/usn-2761-1/
	VELASCO Rubén. Canonical parchea una vulnerabilidad grave en Ubuntu. 6 de octubre del 2016. [En línea]. Redes Zone. Disponible en: http://www.redeszone.net/2015/10/06/canonical-parchea-una-vulnerabilidad-grave-en-ubuntu/
	SAYS Alex. Lynis: auditoría, hardening y seguridad de sistemas. 2 de Noviembre del 2014. [En Línea]. Disponible en: http://rm-rf.es/lynis-auditoria-hardening-seguridad-sistemas/
	INCIBE. Vulnerabilidad en la configuración por defecto para cURL y libcurl (CVE-2015-3153). 21 DE Enero del 2016. España. [En Línea]. Gobierno de España. Disponible en: https://www.incibe.es/vulnDetail/CERT/Alerta_Temprana/Actualidad_Vulnerabilidades/detalle_vulnerabilidad/CVE-2015-3153
PALABRAS CLAVES	Hardening, Ubuntu Server, Vulnerabilidades, Auditoría., Gestión de riesgos
TEMA CENTRAL	Gestión de riesgos de seguridad informática

PROBLEMAS Y PREGUNTAS QUE ABORDA EL TEXTO	Vulnerabilidades en configuraciones por defecto en servidor Ubuntu 14.04. Controles necesarios para mitigar los riesgos encontrados. Principales aspectos a tener en cuenta en una auditoría a estos servidores.
RESUMEN DE CONTENIDOS	El proyecto cuenta con un fundamento teórico para establecer los conceptos base para llevar a cabo el mismo. Posteriormente se realiza la gestión de los riesgos presente en las vulnerabilidades presentes en las configuraciones por defecto de un servidor Ubuntu 14.04. Luego de esto se muestran ejemplos de ataques realizados para finalizar esta apartado con los controles necesarios para mitigar los riesgos identificados. El proyecto culmina con el análisis de los resultados, observaciones y recomendaciones en cuanto a los lineamientos a tener en cuenta al momento de realizar una auditoría a estos servidores.
PRINCIPALES REFERENTES TEÓRICOS Y CONCEPTUALES	Servidor Ubuntu 14.04, sus características y configuraciones por defecto. Gestión y tratamiento de riesgos
METODOLOGÍA DE LA INVESTIGACIÓN	Se estableció el ciclo PHVA para la ejecución del proyecto, y para la gestión de riesgos se referencia la metodología Magerit
RESULTADOS Y CONCLUSIONES	Se realizó una auditoria a las configuraciones por defecto de la distribución Linux Ubuntu 14.04 y una consulta en distintos foros y páginas encontrando vulnerabilidades en: • Kernel: Debido a que el servidor no limita el espacio que puede ocupar el archivo en el cual se guardan los registros, por lo cual se puede estar expuesto a una denegación de servicio. • Usuarios, grupos y autenticación: Se ha detectado un error en el controlador multisistema, por lo cual un usuario local puede llegar a tener acceso a información privada escalando privilegios. • PHP (variables globales):Se podría presentar ejecución remota de código teniendo en cuenta que por defecto esta opción viene activada lo cual permitiría alterar el valor de las variables desde la url.

	• Expose_PHP activado: Puede revelar información sobre la versión de PHP que se maneja, lo cual permitiría a un atacante conocer determinadas características para realizar un ataque. • Firewall desactivado: Podría facilitar el ingreso de intrusos a la red ya que no serían identificados. • Inexistencia de antimalware: No se detectaría la presencia de programas malintencionados Al realizar el análisis de riesgo se determinó la vulnerabilidad del *kernel* y las variables globales (PHP) como los dos factores con mayor nivel de riesgo, debido a su probabilidad de ocurrencia y su impacto. Considerando los riesgos identificados y las pruebas documentadas sobre la explotación de algunas vulnerabilidades en las configuraciones por defecto de la distribución Linux Ubuntu 14.04 se determinaron los controles necesarios para mitigar los riesgos: • Actualización del sistema para que se instale el paquete es inux-image-3.13.0-65 PowerPC-e500 3.13.0-65.106, el cual subsana la vulnerabilidad del *kernel* reduciendo la exposición ante un ataque de denegación de servicio, también corrige el error en el controlador multisistema que permite a un usuario local escalar privilegios. • Desactivación de variables globales: Con esto se reduce el riesgo de ejecución remota de código para modificar el valor de alguna variable, teniendo en cuenta que las variables ya no serían globales. • Desactivación expose PHP: Realizando esta acción no se brinda información en la cabecera HTTP de la versión de PHP utilizada, lo cual en cierto modo evita revelar información que permita detectar la versión utilizada. • Activar firewall: Teniendo en cuenta que Ubuntu maneja por defecto los puertos cerrados, al activar el firewall se requiere habilitar los puertos a utilizar, estos se recomiendan no sean los convencionalmente utilizados.

	• Instalar antimalware: Con esto se evita la presencia de programas mal intencionados. La descripción realizada sobre el paso a paso de la aplicación de los controles determinados para tratar los riesgos identificados (Cap. 6.7), proporciona una guía para reducir el nivel de riesgo que presenta en sus configuraciones por defecto el servidor Ubuntu 14.04. Teniendo en cuenta los resultados obtenidos se ha detectado que la efectividad de los controles es bastante alta cuando se trata de errores de configuración. Se ha encontrado que el servidor Ubuntu 14.04 no presenta muchas configuraciones que representen riesgos inherentes a ellas, las vulnerabilidades detectadas representan riesgos considerables, con un impacto importante en un sistema. Se han establecido los lineamientos teniendo en cuenta que la norma ISO 27000 abarca prácticamente todo el tema de auditoría en seguridad de la información, por lo cual se han dado recomendaciones de acuerdo a los riesgos tratados en el proyecto.
COMENTARIOS	Los resultados encontrados corroboran la confiabilidad y la mayor demanda que ha tenido Ubuntu en los últimos años
ELABORADO POR	CABEZA SEGURA, JEISON SNEIDER
FECHA DE ELABORACIÓN	MARZO DEL 2018