PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TITULO DE
MASTER EN REDES DE COMUNICACIÓN

"ESTUDIO COMPARATIVO DE LAS DISTRIBUCIONES LINUX ORIENTADO A LA SEGURIDAD DE REDES DE COMUNICACIÓN"

Ing. David Badillo Bernal

DIRECTOR: Dr. Gustavo Chafla A.

Quito – 2015

Agradecimiento

Agradezco a Dios por haberme guiado en este proceso de aprendizaje y brindarme los dones necesarios para culminar la maestría. Doy gracias a mis padres por el apoyo incondicional, a mis hermanos que han sabido darme ejemplo de trabajo y éxito profesional.

Debo reconocer el apoyo brindado por mi tío Paul Bernal, quien es mi guía profesional y me incursionó en el mundo de Linux.

Finalmente agradezco a mi esposa María Alexandra Salgado, por ser el soporte en mi vida y parte fundamental para poder terminar este estudio.

Dedicatoria

Dedico este trabajo de investigación a mi esposa e hijas, por ser el motor y razón de mi vida. A mis padres por brindarme su apoyo y ser parte de mi formación profesional. A mi familia y amigos que de alguna manera contribuyeron para la terminación de esta maestría. A toda la comunidad Linux.

Tabla de contenidos:

Índice de Figuras:

Índice de tablas:

CAPÍTULO 1. Introducción

Linux es un sistema operativo que tiene un gran desarrollo en los últimos años, motivo por el cual, empresas públicas como privadas en nuestro país han implementado soluciones informáticas con Linux, principalmente para brindar servicios de red como: Correo Electrónico, DNS, Web, VPN, DHCP, NTP, FTP, NFS y mucho más.

Cuando hablamos de Linux, no podemos referirnos a un solo sistema operativo, en realidad Linux se le define al núcleo (kernel[1]), que puede ser combinado con múltiples programas para así ofrecer diferentes opciones, a esto se lo conoce como Distribuciones Linux "distro" (El Rincón de Linux, 2014).

Existen más de cien distros Linux desarrolladas en diferentes partes del mundo y con diversas finalidades; por ejemplo, existen distros orientadas a: servidores, equipos de escritorio, dispositivos móviles, desarrollo, test de seguridad, educación infantil, entre otros. La gran variedad de distros se debe a que Linux es Software Libre, lo cual permite básicamente: copiar, distribuir, modificar, estudiar y usar el código fuente.

Los administradores de red que optan por usar Linux para la implementación de los servicios de red, tienen un problema al elegir qué distro utilizar, la solución que suelen tomar es instalar la distro más usada o de la que conocen ciertas características; sin embargo, muchas veces eligen soluciones no muy robustas ni estables que finalmente terminan generando problemas de seguridad y estabilidad en los servicios.

Este trabajo de investigación ofrece un estudio comparativo de las distribuciones Linux preparadas para ser servidores, podremos determinar las distros que tienen soporte mediante actualizaciones, parches de seguridad, etcétera; como también qué herramientas pueden incluirse: IDS/IPS, monitoreo de recursos, monitoreo de servicios, etcétera. Este estudio técnico determinará la distro que ofrezca las mejores opciones al momento de brindar servicios de red y a la vez sirva de guía para las empresas que deseen implementar Linux.

---

[1] **Kernel.** Es el núcleo del sistema operativo Linux, encargado de administrar el software y hardware de un equipo.

Un aporte adicional de este estudio, es entregar un documento-guía de instalación y aseguramiento de la distribución considerada como idónea, para la implementación de servicios en red.

La seguridad informática es el problema fundamental que hemos venido afrontando en los últimos tiempos, ya que cada día se incrementan los inconvenientes en los servidores publicados en Internet; la mayoría de estos son atacados por una mala configuración o desconocimiento de tareas básicas de seguridad. Mediante este estudio tendremos resultados relevantes para ayudar a los Administradores de red, a elegir la distribución Linux adecuada y guiarles a una implementación correcta de Linux como servidor.

1.1. Antecedentes

Richard Stallman en al año 1983 fundó el proyecto GNU, el mismo que tiene como objetivo fundamental el desarrollo de programas en Software Libre. Para finales de la década de los ochenta y principios de los noventa, GNU generó un sin número de programas y herramientas como para crear un sistema operativo, sin embargo, lo que hacía falta es el desarrollo del núcleo "kernel" (El sistema operativo GNU, 2014).

En 1991 el finlandés, Linus Tolvards, liberó la primera versión del núcleo (kernel) de Linux, que conjuntamente con varias herramientas elaboradas por el proyecto GNU, dan inicio a uno de los sistemas operativos más utilizados en el mundo para el manejo de servidores. Hoy en día, con un desarrollo de más de 20 años, Linux es usado típicamente para brindar servicios de red (Ciberaula, 2014).

La unión de herramientas GNU con el kernel de Linux, es lo que se conoce como GNU/Linux. Para poder suplir los requerimientos de los usuarios, se crearon las distribuciones Linux (distros); las cuales agrupan diferente tipo de software con el Kernel. Estas distros son soportadas comercialmente, por ejemplo: Red Hat, Fedora, Ubuntu, OpenSUSE; y, otras son mantenidas por comunidades informáticas como: Debian, CentOS, Gentoo entre otras. Las distribuciones tienen diferentes fines con distintos objetivos para satisfacer las necesidades de los usuarios; es así que existen una infinidad de variantes, desde Linux para servidores como Red Hat, hasta Linux para dispositivos móviles como ANDROID.

En gobiernos como Venezuela, gracias al apoyo gubernamental, se ha creado una distribución GNU/Linux; la cual es usada a nivel público, denominándose CANAIMA (CANAIMA, 2014). Existen otros países como Alemania, que han desarrollado varias distribuciones como: Gnoppix, LiMUx, OpenSUSE, Kanotix, Knoppix entre otras. Como podemos notar, Linux es un sistema operativo que no centra su desarrollo en una sola empresa, es un sistema que se aplica de diferentes maneras alrededor de todo mundo, algunos gobiernos de Europa como de Sudamérica, han incentivado el uso de Software libre y por ende el uso de Linux.

En nuestro país, gracias al Decreto presidencial de 10 de abril de 2008 (Correa Delgado, 2008); el cual promueve la utilización de Software libre en entidades del Estado; provocó que en instituciones del gobierno central como seccional, se realice la migración e instalación de sistemas informáticos basados en Linux.

El problema generado, es que en las entidades de gobierno se han instalado diferentes distribuciones Linux dependiendo de los responsables de cada entidad gubernamental, sin realizar un análisis técnico de ¿por qué usar una u otra distribución? Tal vez la solución no sea crear otra distribución como lo hizo el gobierno de Venezuela, pero si se puede estandarizar el uso de una distro, que preste las garantías necesarias para la implementación de servicios de red.

La presente investigación, pretende determinar mediante diferentes criterios, fundamentalmente de seguridad, la distribución Linux, que ofrezca una mayor facilidad al momento de implementar servicios de red; este estudio está principalmente direccionado para las instituciones del Estado, sin exceptuar a las empresas privadas, universidades u otros organismos que deseen hacer uso del mismo.

1.2. Justificación

En la actualidad muchas empresas públicas como privadas de nuestro país, hacen uso de Linux para brindar diferentes servicios para redes locales como en Internet, sin embargo, existe una problemática que es la seguridad. Por ejemplo mirando un reporte de los dominios con extensión .ec en el sitio Zone-H (Zone-H, 2015), podemos encontrar un sin número de ataques a sitios Web de nuestro país; no debemos sorprendernos al mirar en el informe, que la mayoría de sitios utilizan como sistema operativo Linux; de hecho esto

comprueba que en nuestro país, es uno de los sistemas operativos más usados al momento de brindar servicios en red. Esta es una prueba de la problemática de seguridad que existe en muchos sitios de Ecuador. Debemos tomar en cuenta que esta investigación se refiere solamente a páginas Web y no toma en cuenta a otros servicios como: correo electrónico, archivos, DNS, etcétera; que de igual manera podrían presentar problemas de seguridad.

Linux se puede presentar en varias formas mediante sus distros. Una distro está orientada a diferentes fines como: servidores, equipos de escritorio, dispositivos móviles, desarrollo, educación, salud, ciencia, etcétera. Muchos de los problemas de seguridad se derivan porque se elige la distribución equivocada para brindar servicios en la red, por un incorrecto asesoramiento o por afinidad a una distribución que normalmente no debería ser usada como servidor, ya que pueden estar diseñadas para otro fin.

El presente estudio comparativo de las distribuciones Linux orientadas a la seguridad de redes de comunicación, busca determinar la distro más óptima para brindar servicios en redes; ya que es indispensable que al momento de elegir Linux para implementar en un servidor, debemos tener siempre un criterio técnico adecuado para conocer que distro nos ofrece mayores ventajas en seguridad.

Dentro de las decenas de opciones Linux que se encuentran en el mercado, hay proyectos sólidos que ofrecen una gran cantidad de beneficios como: soporte por largo tiempo, desarrollo de nuevas tecnologías, mantenimiento de paquetes, etcétera; sin embargo, existen distros que no cumplen con las características fundamentales para ser implementadas como servidor y muchas veces, éstas son implementadas en empresas por que normalmente son cien por ciento gratuitas.

Otra problemática existente es que los administradores piensan que con el sólo hecho de instalar Linux, su servidor ya está seguro. Criterio totalmente errado, justamente por este hecho es que existen muchos eventos de problemas de seguridad en nuestro medio. Es evidente, que un servidor Linux bien implementado reduce al máximo los problemas de seguridad. Linux es un sistema operativo muy flexible, el cual permite personalizar al máximo las configuraciones, por eso es su gran acogida, pero sin un correcto aseguramiento, pondríamos en riesgo los datos que maneje el servidor.

Como aporte adicional de este estudio técnico estará el entregar un documento-guía de instalación y aseguramiento de la distribución Linux, determinada como la más adecuada

para brindar los servicios en redes de comunicación. Este manual tendrá los procedimientos más elementales que se deben realizar para instalar correctamente este sistema operativo y las consideraciones a tomar en cuenta para endurecer al sistema operativo contra ataques en la red.

Estamos seguros que al elegir la distribución Linux que nos brinde las mayores garantías para asegurar los servicios de red, se reducirán considerablemente los eventos de ataques, que mayormente se facilitan gracias al desconocimiento de los principios básicos de seguridad al momento de implementar este eficaz sistema operativo.

1.3. Alcance

El presente trabajo no realizará un estudio comparativo de todas las distribuciones Linux, ya que es muy difícil, casi imposible, por la cantidad de distros existentes, alrededor de 280 (DistroWatch, 2015); de hecho no existe un número exacto, muchas de las distros no son reportadas o publicadas. Se realizará el estudio comparativo con las distribuciones más usadas en nuestro medio, principalmente en entidades del Estado.

Se ofrecerán documentos-guías: De instalación de la distribución que se determine como la más óptima; de igual manera de aseguramiento de la distribución. Este estudio no incluye el aseguramiento de servicios especiales por ejemplo: Servidor Web, Correo electrónico, DNS, FTP, etcétera; esta investigación está centrada a nivel del aseguramiento del sistema operativo.

Dentro del documento-guía de aseguramiento, de la distribución Linux, se puede considerar el recomendar la instalación de ciertos programas que pueden ayudar al mantenimiento y detección de problemas de seguridad, este estudio no realizará una comparativa de estos software especiales. Se usarán los que se adapten a la distro determinada como óptima y las que sugieran los desarrolladores de la distribución Linux.

1.4. Objetivo General

Analizar las distribuciones Linux disponibles en nuestro medio bajo criterios de seguridad y así determinar la más óptima para brindar servicios en redes de comunicación.

1.5. Objetivos Específicos

1. Estudiar las distribuciones Linux orientadas al servicio en redes de comunicación y analizar las características de cada una.
2. Instalar las distribuciones Linux y documentar su procedimiento.
3. Diseñar los parámetros de evaluación, principalmente, con criterios de seguridad, para el análisis comparativo de las distros Linux orientadas a servicios en redes de comunicación.
4. Presentar un estudio comparativo de las distribuciones Linux en base a los parámetros de evaluación seleccionados.
5. Estudiar los modos de aseguramiento de la distribución Linux seleccionada como la más adecuada para brindar servicios de red.
6. Elaborar un documento-guía para la instalación de la distro Linux seleccionada.
7. Elaborar un documento-guía para el aseguramiento de la distro Linux seleccionada.

CAPÍTULO 2. Marco Teórico

Para poder realizar un estudio comparativo de las distribuciones Linux orientado a la seguridad de redes de comunicación, debemos contar con una base teórica que cuente con información, para ayudar al proceso de investigación.

En este capítulo vamos a revisar algunos conceptos enfocados al origen de Linux y la situación actual de este excelente sistema operativo. También analizaremos las características de las distribuciones Linux y su importancia para ser parte en las redes de comunicaciones.

Es necesario utilizar algunas herramientas disponibles en Internet y confirmar el uso de Linux para brindar servicios de red. Consultaremos algunos datos para determinar las distribuciones Linux más utilizadas a nivel mundial y local.

La información publicada en Internet es aproximada, por la cantidad de distribuciones y servidores que usan Linux, es virtualmente imposible obtener datos exactos; sin embargo para nuestro estudio es suficiente conocer las tendencias de uso de Linux.

Una vez que tengamos algunos datos importantes sobre el uso de las distribuciones y sus características fundamentales, podremos realizar el estudio comparativo.

2.1. Historia de Linux

Para poder comprender la historia de este excelente sistema operativo, debemos conocer sus inicios y que incentivaron a su creación. No podemos hablar de Linux sin referirnos a UNIX, GNU y Software Libre.

Linux es un sistema operativo que ha sido usado para equipos servidores, considerado uno de los más robustos y estables. Estas características que se lo asignan gracias a la gran variedad de opciones de desarrollo; Linux no depende de una compañía de software, este esta regado en todo el mundo y su desarrollo se basa a un sin número de comunidades que diariamente trabajan para su crecimiento. Existen grandes empresas de software que auspician a varios proyectos de código abierto los cuales son orientados a sistemas Linux, permitiendo que este sistema sea responsable de brindar servicios de red.

2.1.1. UNIX

Es un sistema operativo privativo que fue desarrollado en lenguaje C[2], el cual es portable, multitarea y multiusuario, dispone de un lenguaje de control llamado SHELL[3]. Tiene un sistema sofisticado en el manejo de procesos, permitiendo su interconexión. Unix maneja un sistema de archivos jerárquico el cual tiene la gran utilidad de proteger los ficheros, mediante un mecanismo de manejo de cuentas de usuario y procesos.

Unix se basa en el núcleo (kernel), el cual permanece en la memoria RAM, y es quien se encarga de atender a las llamadas del sistema, administrar el acceso a los archivos y maneja los procesos.

Existen varios sistemas operativos que se han basado en UNIX, por ejemplo: Linux, Solaris, MacOS; los cuales han heredado algunas de las funcionalidades importantes, principalmente a lo que se refiere a la administración mediante el uso de un SHELL.

Unix fue desarrollado en 1969 por el Instituto Tecnológico de Massachusetts, los Laboratorios Bell y General Electric (The UNIX® System, 2015), actualmente pertenece a Santa Cruz Operation, la cual comercializa la versión del Sistema llamado UnixWare (XinuOS, 2015).

---

2 **Lenguaje C.** Es un lenguaje de programación desarrollado en los Laboratorios Bell cuyo creador fue Dennis Ritchie, este lenguaje fue utilizado para la creación de varios sistemas operativos.

3 **Shell.** Es el término usado para el intérprete de comandos de los sistemas operativos basados en UNIX.

2.1.2. El Proyecto GNU

El proyecto GNU[4] fue fundado por Richard Stallman el 27 de septiembre de 1983, luego de que éste trabajara en el Instituto Tecnológico de Massachusetts, donde fue desarrollado el sistema UNIX. El objetivo fundamental del proyecto GNU, fue crear un sistema operativo que sea completamente libre. GNU creo una licencia para publicar sus productos, con el objetivo de garantizar los derechos del proyecto, esta licencia es lo que originó el Software Libre.

GNU significa “GNU is not Unix” y se refiere a que es un sistema basado en UNIX pero no privativo. Actualmente este proyecto tiene una gran variedad de paquetes de software, los cuales son usados en Linux y en algunos otros sistemas como Solaris, lo que busca es devolver el espíritu colaborativo que existía antes de que se formen los obstáculos creados por el software comercial.

Definitivamente es evidente la transformación en el desarrollo de software que generó este proyecto y la gran acogida que tiene, formando una gran comunidad que busca desarrollar programas de calidad y sin restricciones (GNU, 2015).

2.1.3. Software Libre

Para evitar confusiones, es necesario que nos refiramos a la definición exacta entregada por GNU el cual dice: ***“ «Software libre» es el software que respeta la libertad de los usuarios y la comunidad. En grandes líneas, significa que los usuarios tienen la libertad para ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, el «software libre» es una cuestión de libertad, no de precio. Para entender el concepto, piense en «libre» como en «libre expresión», no como en «barra libre».”*** (El sistema operativo GNU, 2015)

---

4 **GNU is not Unix.** Proyecto que ha fomentado el desarrollo del software Libre desde 1984

Dentro de este concepto, es fundamental aclarar que software libre no es lo mismo que software gratuito, muchos usuarios confunden estos conceptos y piensan que Linux es siempre gratis, creyendo que es una ventaja fundamental respecto al resto de sistemas operativos. Existen programas privativos que son gratis, por ejemplo el Internet Explorer o Skype, de igual manera existen programas en software libre que no son cien por ciento gratuitos y que tienen un costo por soporte técnico o distribución. Al software que sin importar si es libre o privativo pero que es gratuito, se lo conoce como Freeware.

Basados en este concepto se han generado un sin número de tipos de licencias para el manejo del software, unas que no entregan todas las libertades antes mencionadas u otras que las entregan bajo ciertas restricciones, a estas se las conoce como licencias mixtas. También existen empresas que lanzan versiones con licencia libre y versiones con licencia comercial.

La Licencia GPL[5] es la más representativa en Software Libre, muchos de los programas han sido liberados bajo este tipo de licenciamiento, sin embargo no es el único y en realidad existe un gran abanico de posibilidades en este aspecto.

2.1.4. Linux

Es el sistema operativo libre más popular, está basado en el sistema Unix, tiene las políticas y componentes del proyecto GNU, por lo que se lo denomina también como GNU/Linux.

Linus Torvalds, con 23 años de edad en 1991, propone hacer un sistema operativo basado en Unix para que funcione sobre cualquier arquitectura de hardware de una PC. Linus escribió el núcleo de Linux, el que en un principio solo permitía leer y escribir ficheros de un disquete; en octubre de 1991 Linus anuncia la primera versión de Linux el cual podía ejecutar algunas herramientas de GNU y de esta manera da inicio a uno de los sistemas operativos más populares cuando se trata de instalar servidores (The Linux Information Project, 2015).

---

5 **GPL**. General Public Licence

Actualmente Linux viene en diversos matices, que se los conoce como Distribuciones Linux, esto significa que existe una gran variedad de posibilidades para el uso de este sistema operativo.

2.2. Distribuciones Linux

Linux es básicamente el kernel (núcleo), el cual maneja todas las operaciones de entrada y salida, así mismo la memoria y la asignación de recursos del procesador. Dicho esto, debemos diferenciar en lo que es el kernel de Linux y lo que es una Distribución Linux.

Una Distribución Linux es una colección de paquetes recopilados por una empresa o comunidad informática, la cual agrupa el kernel de Linux con otros programas adicionales, por ejemplo los liberados por GNU u otras comunidades/empresas.

Las distribuciones Linux no sólo tienen programas de GNU, pueden contener otros proyectos dependiendo de la orientación que tenga dicha distribución, de hecho puede contener paquetes con diferentes tipos de licenciamiento: software libre como software comercial, pero la repartición de los paquetes es libre.

Las distribuciones Linux normalmente tienen un fin comercial, pueden basarse en cobrar por el costo de la venta de CD's o DVD's, por soporte técnico especializado o por capacitación.

Las distribuciones tienen como objetivo fundamental lograr un nivel de soporte, para ello realizan actualizaciones frecuentes de los paquetes, los cuales son publicados y como lo mencionamos anteriormente, estas pueden ser bajo un pago previo o no.

El tiempo de vida de una distribución depende de su promotor, existen algunas que ofrecen cambios constantes (versiones con tiempo de vida cortos) u otras que utilizan software probado y que son más estables.

2.2.1. Características de las distribuciones Linux

Existe una gran variedad de distribuciones Linux, de hecho no se conoce el número exacto de proyectos Linux existentes en el mundo, una de las razones fundamentales es que muchas distribuciones no son publicadas/conocidas.

Pese a la gran variedad todas tienes características comunes, entre las que podemos resaltar serían:

- **Agrupación de software.** La principal característica es que una distribución agrupa paquetes de software, los cuales pueden ser instalados posteriormente por los usuarios.

- **Sistema de Instalación:** Una distribución nos ofrece un sistema de instalación, el cual permite implementar en un computador el sistema operativo.

- **Orientación:** Las distribuciones tienen una orientación respecto al uso que se le dará al Linux, por ejemplo existen distribuciones para servidores, usuario final, dispositivos móviles, dispositivos de hardware, etc.

- **Soporte:** Las distribuciones nos ofrecen un soporte constante sobre los paquetes de software, esto es: actualizaciones constantes de paquetes, parches, corrección de errores, etcétera. Las distribuciones más grandes, nos brindan soluciones empresariales y soporte especializado, por ejemplo Red Hat, SUSE o Debian.

- **Manejo de paquetes.** Las distribuciones permiten el manejo de paquetes adecuado para evitar problemas de compatibilidad de software.

De seguro podremos encontrar más características, sin embargo consideramos que estas son las relevantes.

2.2.2. Componentes

Los componentes de una distribución son:

- **Núcleo.** Es el elemento más importante del sistema operativo y es obvio que el núcleo debe ser Linux para considerarle como distribución Linux.

- **Herramientas y librerías.** Normalmente las distribuciones nos brindan herramientas de configuración, por ejemplo: Yast en SUSE o System Config en Red Hat. Adicional también ofrecen librerías comunes que pueden ser utilizadas por diferentes programas.

- **Software Adicional.** Aparte de los elementos propios del sistema operativo, una distribución suele incluir en sus paquetes software adicional como: programas de ofimática, audio y video, gráficos, Internet, etcétera.

- **Documentación.** Las distribuciones también nos ofrecen documentación que permita guiar a los usuarios sobre el uso de algunos componentes, también suelen publicar foro de ayuda en los sitios web oficiales.

- **Entorno Gráfico.** Cuando queremos trabajar bajo un ambiente gráfico, las distribuciones nos deben ofrecer un gestor de ventanas y entorno de escritorio. Algunas distribuciones ofrecen varias alternativas como: KDE[6] o GNOME[7].

- **Gestor de paquetes.** Con el objetivo fundamental de evitar problemas con la instalación, mantenimiento y compatibilidad de software, las distribuciones Linux utilizan un gestor de paquetes de software. Los principales gestores de paquetes usados en Linux son: RPM[8] y DEB.[9]

2.3. Distribuciones Linux más populares

Existen grandes comunidades dentro del Software Libre que han logrado posicionar su marca a nivel mundial cuando hablamos de Linux. Dentro de las decenas de opciones que tenemos, resaltan siempre unas pocas.

Vamos analizar las distros más utilizadas a nivel mundial y local. No existe una herramienta que entregue información exacta, realizar un estudio global es virtualmente imposible, por la cantidad de usuarios y distros, sin embargo usaremos algunos utilitarios que están disponibles en Internet, estos nos ayudarán a obtener información de utilidad para conocer la tendencia en el uso de las distribuciones; esta será la base que utilizaremos para realizar el estudio comparativo.

---

6 **KDE:** Entrono de escritorio muy usado por sus características visuales.

7 **GNOME:** Entorno de escritorio de GNU, muy usado en distribuciones para servidores.

8 **RPM:** Red Hat Package Manager. Se utiliza en todas las distribuciones basadas en Red Hat.

9 **DEB:** Manejado de paquetes propio de Debian, existen varias distribuciones que utilizan esta herramienta.

2.3.1. Distribuciones más usadas a nivel mundial.

Es difícil determinar valores exactos para conocer que distribución Linux es la más usada, sin embargo existe un sitio web que se ha dedicado a entregar datos importantes (DistroWatch, 2015). Dentro de la información que podemos encontrar, tenemos una estadística de las distribuciones más utilizadas mediante el uso de voto en línea; debemos recalcar que no son datos cien por ciento exactos, el propio autor del sitio, indica que el sistema de votación tiene algunos problemas; por ejemplo no puede evitar el voto múltiple.

No encontramos otros sistemas que pueda ayudar a conocer la tendencia de las distribuciones Linux a nivel mundial.

A continuación la tabla de las distribuciones Linux más utilizadas en los últimos 6 meses. Los datos fueron tomados el día miércoles 19 de agosto del 2015

Puesto	**Distribución**	***H.D.P.**
1	Mint	3116
2	Debian	1694
3	Ubuntu	1633
4	Open SUSE	1200
5	Fedora	1150
6	Mageia	1023
7	CentOS	989
8	Manjaro	935
9	LXLE	786
10	Arch	775
11	Elementary	773
12	Android-x86	690
13	PCLinuxOS	602

14	Kali	571
15	Puppy	570
16	Lubuntu	569
17	Zorin	553
18	Simplicity	514
19	Lite	496
20	Deepin	469
21	Bodhi	457
22	SteamOS	427
23	Xubuntu	424
24	AntiX	423
25	Makulu Linux	421
26	FreeBSD	410
27	Ubuntu Mate	400
28	KaOS	399
29	Robolinux	392
30	Black Lab	390
***H.D.P. Número de visitas diarias**		

Tabla 1: Lista de Distribuciones Linux más visitadas

La mayoría de las distribuciones citadas en esta estadística, no están orientadas a ser servidores, más bien son orientadas a usuario final.

2.3.2. Distribuciones más usadas en nuestro medio.

Linux también es muy usado en nuestro país, por ejemplo realizando un monitoreo de algunos sitios web, podemos determinar que la gran mayoría están bajo un servidor Linux.

Utilizando la herramienta NetCraft (NetCraft, 2015), la cual permite determinar qué sistema operativo utiliza un sitio web, podemos analizar algunas pertenecientes a Ecuador.

Dirección Web	Sistema Operativo	Servidor Web
www.presidencia.gob.ec	Linux	Apache
www.vicepresidencia.gob.ec	Linux	Apache
www.administracionpublica.gob.ec	Linux	Apache
www.comunicacion.gob.ec	Linux	Apache
www.politica.gob.ec	Linux	Apache
www.planificacion.gob.ec	Linux	Apache
www.agua.gob.ec	Linux	Apache
www.desarrolloamazonico.gob.ec	Linux	Apache
www.educacionsuperior.gob.ec	Linux	Apache
www.educacionderiesgos.gob.ec	Linux	Apache
www.desarrollosocial.gob.ec	Linux	Apache
www.cne.gob.ec	Linux	Apache
www.institutocne.gob.ec	Linux	Apache
www.quito.gob.ec	Linux	Apache
www.pichincha.com	Solaris	Apache
www.bancodelpacifico.com	Windows	IIS
www.bancoguayaquil.com	Linux	Apache
www.produbanco.com	Windows	IIS
www.bancointernacional.com.ec	Linux	IBM_HTTP
www.elcomercio.com	Linux	Apache
www.lahora.com.ec	Linux	Apache

www.ecuadorinmediato.com	Linux	Apache
www.ecuadorenvivo.com	Linux	Apache
www.guayaquil.gob.ec	Windows	Apache
www.cuenca.gob.ec	Windows	Apache

Tabla 2: Muestra de sitios web de Ecuador para determinar el uso de Linux.

Como podemos analizar de la *Tabla No. 2*, determinamos que la mayoría de los sitios están bajo Linux; para esta pequeña muestra, hemos tomado sitios de gobierno, periódicos, bancos entre otros.

Es necesario conocer qué distribuciones Linux son las más utilizadas en Ecuador; por las estadísticas generadas del CEDIA[10], podemos determinar cuáles han sido descargadas desde el repositorio general de varias distribuciones; estas son:

- CentOS
- Fedora
- Debian
- Ubuntu
- ZeroShell
- ArchLinux
- Mint
- Open SUSE
- Slackware
- Kali Linux
- Scientific Linux

10 CEDIA. Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado.

- Trisquel Linux
- Mageia
- Blackarch Linux
- Nova

De esta lista de distribuciones podemos revisar cuales son las más visitadas, a continuación la estadística del mes de Julio del 2015.

Distribución	**Hits**[11]
Kali Linux	226971
Fedora	295430
CentOS	153212
ArchLinux	81515
Ubuntu	16215
Open SUSE	11899
Debian	10358

Tabla 3: Estadística mes de agosto 2015 repositorio CEDIA

Las estadísticas detalladas en la *Tabla 3* fueron obtenidas del sistema webalizer[12], el cual presenta las visitas detalladas por diferentes criterios. En nuestro caso se obtuvo los datos de acceso a las imágenes ISO de las distribuciones analizadas.

Como podemos observar Kali Linux es la distribución que más descargas presenta en la estadística, este no termina de ser un dato curioso, al estar por encima de CentOS, Fedora,

---

11 **Hits.** Es una unidad para sacar la estadística de visitas web. Se contabiliza un hit cuando se abre un archivo. Normalmente se abre un archivo web el cual varios hits por los ficheros dependientes que son parte del contenido Web.

12 **Webalizer.** Es una aplicación que genera una estadística de visitas de un sitio web usando registros (logs) del servidor Web. Esta herramienta está bajo licencia GPL.

Debian y Ubuntu. Kali Linux es una distribución orientada a la auditoría y seguridad informática; esta no está diseñada para brindar servicios de red.

También debemos recalcar que al repositorio del CEDIA no acceden solamente equipos desde el Ecuador, al estar publicado en Internet estos pueden ser accedidos desde cualquier parte del mundo, sin embargo utilizando la misma herramienta estadística, esta nos indica que la mayoría de accesos son desde el Ecuador.

La parte fundamental de la recolección de estos datos es tener una idea de cuales distribuciones son usadas y aunque es un tema bastante subjetivo, tenemos algunos datos importantes en que basarnos, para continuar con nuestro estudio.

2.3.3. Estadística de sitios ecuatorianos atacados.

Es importante señalar que muchos sitios ecuatorianos con Linux, son atacados diariamente. Hemos capturado los datos presentados por Zone-h para analizar que la mayoría de sitios atacados, tienen a Linux como sistema operativo. (Ver Figura 1).

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Time	Notifier	H	M	R	L	Domain	OS	View
2015/11/21	ProtoWave Reloaded			R		www.liceonaval.mil.ec/webpages...	F5 Big-IP	mirror
2015/09/30	Drac-101code					www.gobiernogalapagos.gob.ec/x...	Linux	mirror
2015/09/20	Lopht Crews			R		www.munjoyasachas.gob.ec//imag...	Linux	mirror
2015/09/15	Matrix Dz	H				normaspdf.inen.gob.ec	Linux	mirror
2015/08/23	Black Worm			R		www.bomberoselempalme.gob.ec/n...	Linux	mirror
2015/08/23	SaMi1					bomberosvalencia.gob.ec/leydet...	Linux	mirror
2015/08/23	SaMi1			R		bomberossalitre.gob.ec/leydetr...	Linux	mirror
2015/08/23	SaMi1					bomberosquinsaloma.gob.ec/leyd...	Linux	mirror
2015/08/23	SaMi1			R		bomberospuebloviejo.gob.ec/ley...	Linux	mirror
2015/08/23	SaMi1	H				bomberospalenque.gob.ec	Linux	mirror
2015/08/22	SaMi1					bomberosbaba.gob.ec/leytranspa...	Linux	mirror
2015/08/20	RuLing					www.bomberospedrocarbo.gob.ec/...	Linux	mirror
2015/08/18	RuLing					www.bomberosdesantalucia.gob.e...	Linux	mirror
2015/08/18	MiguelCity					bomberosvinces.gob.ec/panel_le...	Linux	mirror
2015/08/15	Abdellah Elmaghribi	H				www.zonaiq.aeropuertoquito.gob.ec	Linux	mirror
2015/08/05	Error 7rB	H				www.cuerpodeingenierosdelejerc...	Linux	mirror
2015/08/05	./MrJ					www.cncine.gob.ec/blogosfera/s...	Linux	mirror
2015/07/31	Fayzoun Hacker			R		www.preinversion.gob.ec/gestio...	Linux	mirror
2015/07/18	rooterror			R		www.patate.gob.ec/noticias/g_n...	Linux	mirror

Figura 1: Estadística sitios ecuatorianos vulnerados.

Fuente: Zone-h . Consulta 26 de noviembre de 2015.

CAPITULO 3. Estado del arte, endurecimiento y administración de servidores Linux para brindar servicios de red.

Hemos realizado varias búsquedas en Internet con el fin de encontrar información referente a las características de seguridad de las distribuciones Linux. No se hallaron datos relevantes que puedan ayudar a determinar qué componentes mínimos se requieren, para ayudar a la seguridad de un servidor y la red.

Luego de analizar las características de seguridad sugeridas en documentación oficial de las distribuciones Linux, podemos señalar varios criterios importantes y básicos, que deben tomar en cuenta los administradores de red para reducir la probabilidad de problemas de seguridad.

En este capítulo, bajo nuestra experiencia e investigación, señalaremos algunos aspectos de seguridad que a nuestro criterio deben ser aplicados en una red de comunicación.

3.1. Endurecimiento de las distribuciones Linux.

No solamente con instalar Linux se ofrece una seguridad absoluta, una buena configuración permite endurecer el sistema.

Para poder realizar un estudio comparativo de las distribuciones Linux orientadas a la seguridad, debemos conocer ciertos criterios comunes, Dentro de los principales fundamentos tenemos:

- Instalación personalizada
- Bajar servicios innecesarios
- Actualización del sistema operativo
- Configuración del Firewall
- Activación de SELinux

- Protección para accesos remotos
- Uso de protocolos seguros (https, ssh, vpn, sftp etc.)
- Herramientas de monitoreo de servicios y recursos
- Sistema de detección/prevención de intrusos (IDS/IPS)
- Sistema para el escaneo de vulnerabilidades.
- Implementación de AIDE[13]
- Sistema de aseguramiento Bastille

3.1.1. Instalación personalizada

Antes de instalar cualquier distribución Linux, debemos considerar algunos aspectos comunes entre las distribuciones. Lo primero que debemos preguntarnos es: ¿qué propósito tiene el equipo a instalar? Por ejemplo: difiere realizar una instalación para un equipo de escritorio, que realizar una instalación para un equipo servidor.

Este estudio está orientado a equipos servidores, para ello debemos tomar en cuenta algunos aspectos importantes dentro de la instalación:

- Creación de particiones de disco.
- Contraseña del super usuario root.
- Contraseña del gestor de arranque.
- Elección de paquetes.

Un servidor Linux bien instalado puede ser muy robusto cuando hablamos de la seguridad, en cambio si al momento de cargar el sistema no lo configuramos correctamente, posteriormente se pueden producir problemas de seguridad que afecten a los servicios de red que esté brindando el servidor.

---

[13] AIDE. (Advanced Intrusion Detection Enviroment). Herramienta que permite determinar cambios en archivos producto de una intrusión.

Los criterios son sencillos, sin embargo muchos administradores pasas por alto las recomendaciones efectuadas por los desarrolladores de las distribuciones, esto ocasiona tener varios sistemas para contrarrestar problemas de seguridad, pero sin uso. A continuación detallamos los pasos importantes de la instalación de cualquier Linux.

3.1.1.1. Creación de particiones de disco.

A nuestro criterio, lo más importante del proceso de instalación de Linux, es la creación de las particiones de disco, no existe un patrón definido para todo tipo de instalación, depende de algunas variables como el destino del equipo. El diseño de particiones no es lo mismo para un equipo de escritorio que para un servidor. Así mismo el diseño de particiones no es lo mismo para un servidor de archivos que para un servidor de correo o servidor de base de datos.

Con estos criterios, se debe realizar un análisis previo para crear la estructura de particiones. Dentro de Linux existen directorios que guardan información específica y depende de ésta para crear el diseño de particiones (Pérez Estévez, 2015). Dentro de los directorios más importantes y para los cuales debemos crear particiones tenemos:

- **Directorio usr (/usr).** Es el directorio que guarda los programas instalados en el equipo, contiene archivos ejecutables.
- **Directorio var (/var).** Es el directorio que guarda los archivos de contenido variable, es decir que los archivos cambian frecuentemente, por ejemplo: buzones de correo electrónico, registros del sistema (logs), bases de datos, etcétera.
- **Directorio home (/home).** Es el directorio que guarda los archivos de los usuarios del sistema. Cada usuario a excepción de root posee un directorio en el cual se guarda toda su información.
- **Directorio boot (/boot)**. Es el directorio que guarda todo lo necesario para que arranque el sistema operativo, fundamentalmente alberga las imágenes del kernel.
- **Directorio raíz (/).** Es el directorio por defecto, es donde se guarda todo lo que no se almacena en los directorios anteriormente señalados.

Adicional a estos directorios que representan particiones de disco, debemos crear la partición para la memoria virtual SWAP, obviamente esta no tiene un directorio como punto de montaje.

Los tamaños de las particiones como lo señalamos anteriormente, dependen de cuál será el destino del equipo, sin embargo pondremos dos ejemplos:

- Disco de 1 Tb destinado a un servidor de base de datos donde la mayor carga de información se la guarda en la partición /var, podría tener el siguiente diseño de particiones:
    - 500Mb para /boot
    - 30Gb para /usr
    - 30Gb para /home
    - 1Gb para swap
    - 30 Gb para /
    - 908.50 Gb para /var
- Disco de 1 Tb destinado a un servidor de archivos donde la mayor carga de archivos tiene la partición /home, podría tener el siguiente diseño de particiones:
    - 500Mb para /boot
    - 30Gb para /usr
    - 908.50 Gb para /home
    - 1Gb para swap
    - 30 Gb para /
    - 30 Gb para /var

Es recomendable se use LVM (Logical Volumen Manager) si está disponible en la distribución a instalar, esta tecnología facilita el trabajo de re-dimensionar las particiones y administración de las mismas.

La mayoría de distribuciones brindan la opción de cifrar las particiones que contienen datos importantes, estas pueden ser /var y /home, según sea el tipo de instalación que realicemos. Para encriptar nos pedirán determinemos una contraseña de cifrado, la cual no la podemos olvidar; sin la contraseña no podremos arrancar el servidor y no hay manera de recuperarla.

3.1.1.2. Contraseña de super usuario (root).

El super usuario root es el administrador del sistema, por ende puede hacer prácticamente cualquier cosa, es por esta razón que debemos proteger esta cuenta con una contraseña muy segura. Puntualicemos algunos aspectos al momento de definir la contraseña de root:

- No utilice palabras simples o de diccionario que sean fáciles de descifrar.
- No utilicen nombres, fechas de nacimiento, placas de autos, etcétera, que puedan ser adivinadas por un atacante que conozca la identidad del administrador del sistema.
- La longitud de la contraseña debe ser mayor a los 8 caracteres.
- Para la creación de la contraseña, utilizar una combinación entre letras mayúsculas, letras minúsculas, números y caracteres especiales (?¿!¡ etc.).
- Cambiar periódicamente cada trimestre la contraseña de root.

3.1.1.3. Contraseña del gestor de arranque.

Toda distribución Linux posee un gestor de arranque, el cual permite entre otras cosas, elegir el núcleo para arrancar el sistema o enviar parámetros para el inicio. Para proteger nuestro sistema es necesario que asignemos una contraseña al gestor de arranque, para evitar que sea arrancado de manera incorrecta o con el objetivo de violentar la seguridad del servidor (Geekland, 2015).

Para establecer la contraseña se recomienda utilizar los mismos criterios señalados en el punto anterior.

El gestor de arranque comúnmente utilizado por las distribuciones es el GRUB, el cual permite determinar una contraseña para editar los parámetros al momento de arrancar el sistema.

Debemos recalcar que existen maneras para violentar la clave del GRUB, para ello se requiere el acceso físico al equipo y tener un tiempo considerable.

A nuestro entender, un servidor con acceso físico pierde todo criterio de seguridad, un atacante puede dañar directamente el equipo, desconectar cables, sustraerse el hardware, etcétera.

3.1.1.4. Elección de paquetes.

Como se ha explicado en este documento las distribuciones aparte de usar el kernel de Linux, provee de un sin número de paquetes adicionales, los cuales nos permiten mantener completamente operativo a nuestro equipo informático, por ejemplo: En una distribución orientada a servidor, este nos ofrece los paquetes necesarios para implementar los servicios de: correo electrónico, archivos, DNS, NTP, DHCP, etcétera; sin embargo no siempre tendremos estos servicios activos.

Al realizar la instalación de Linux, normalmente debemos elegir la opción para escoger el tipo de instalación, según lo que nosotros necesitemos. Lo recomendable es realizar una instalación mínima del sistema y posteriormente ir agregando los paquetes que requiramos, ya que un servicio inactivo puede ocasionar una brecha de seguridad.

Cuando instalamos Linux, no se aplica el refrán “Preferible que sobre a que falte”, ya que como explicamos, lo que sobre nos puede ocasionar serios problemas de seguridad, es aconsejable instalar lo estrictamente necesario.

3.1.2. Bajar servicios innecesarios

Como lo explicamos en el punto anterior, un servicio inutilizado que esté escuchando un puerto determinado puede ser un gran peligro para la seguridad del servidor, por esta razón, debemos apagar los servicios que no estemos utilizando.

De igual manera al apagar servicios no utilizados, optimizamos los recursos del sistema, reduciendo el consumo de la CPU y memoria RAM.

Dependiendo de la distribución que usemos, tendremos la manera de encender y apagar los demonios[14] en tiempo de ejecución, como desactivar el arranque de los servicios al inicio del sistema. Debemos consultar en la documentación de la distribución la forma de realizar este trabajo. Como parte de este documento, detallaremos este procedimiento de acuerdo a la distribución que se determine la más idónea para ser instalada como servidor, según los criterios de seguridad.

3.1.3. Actualización del sistema operativo.

Las distribuciones Linux al publicar una versión estable, dependiendo el tiempo de soporte, ofrecen la actualización de paquetes. El tener un servidor actualizado reduce considerablemente los problemas de seguridad, la razón fundamental es que las distribuciones Linux siempre estarán publicando parches a paquetes en los cuales se han detectado problemas de seguridad.

Debemos recalcar que lo recomendable es siempre utilizar los repositorios oficiales para realizar cualquier actualización, el instalar paquetes desde repositorios no oficiales, aumenta el riesgo de que se presenten problemas.

3.1.4. Configuración del Firewall

El firewall de Linux es denominado como **iptables,** este está incluido en el kernel desde la versión 2.4. Este firewall está basado en reglas, las cuales se las pueden configurar en tiempo de ejecución mediante el comando iptables (Netfilter, 2015).

Existe la confusión de que iptables es un servicio al cual podemos arrancar o detener, como ya lo indicamos anteriormente el iptables está integrado al kernel.

---

14 Demonio. Denominación de servicio en Linux.

La configuración del firewall no es sencilla, ya que mediante el comando antes indicado, se debe configurar las reglas para determinar el comportamiento de este sistema.

El firewall de Linux tiene tres funciones principales determinadas en tablas donde se almacenan las reglas, estas son:

- **FILTER.** Se determinan las reglas para el filtrado de paquetes, se puede inspeccionar los datos de entrada INPUT, salida OUTPUT y redirección FORWARD.
- **NAT.** Se determinan las reglas para implementar NAT[15] o DNAT, maneja las cadenas PREROUTING, OUTPUT y POSTROUTING.
- **MANGLE.** Se determinan reglas para modificar los paquetes, son reglas poco usadas y conocidas.

Las distribuciones para facilitar el manejo del firewall, normalmente han creado un servicio el cual maneja las reglas del iptables. Cuando arrancamos el demonio, se aplican las reglas al kernel, cuando paramos el servicio, se limpian las tablas antes mencionadas.

Existen algunos servicios de firewall para ser instalados en Linux, a continuación citamos los más populares.

- Shortwall
- rc-firewall
- APF[16]
- CSF[17]

Estos paquetes de software, permiten realizar configuraciones seguras sin mayor trabajo, pues traen ya una gran cantidad de reglas que permiten asegurar a un servidor por defecto.

---

15 **NAT (Network Address Translation).** Perimte principalmente compartir una IP pública, con muchos equipos.

16 **APF.** Advanced Policy Firewall

17 **CSF.** ConfigServer Security & Firewall

3.1.5. Activación de SELinux

La Agencia de Seguridad Nacional de los Estados Unidos de América[18] en conjunto con la comunidad SELinux[19] creó una arquitectura de seguridad, el cual está integrado al kernel de Linux desde la versión 2.6.x. (Red Hat, 2015)

SELinux se basa en un sistema de control de acceso obligatorio llamado MAC por sus siglas en inglés[20], el cual tiene como objetivo fundamental, el proteger al sistema operativo de software malicioso.

Para equipos de escritorio este sistema es muy útil, de hecho prácticamente es invisible para los usuarios finales. Para equipos que son destinados a servidor, SELinux puede provocar conflictos, para lo cual el administrador del sistema, tiene que implementar políticas para el correcto funcionamiento de los servicios instalados.

Para entender de mejor manera el funcionamiento de SELinux, podemos poner como ejemplo: Cuando una aplicación quiere acceder a un archivo, SELinux verifica si dicha aplicación tiene permiso hacia este, según la política registrada en la caché de vector de acceso[21], de esta manera permite o deniega el acceso. El detalle de esta operación es escrita en el registro del sistema /var/log/message.

3.1.5.1. Estados posibles de SELinux

SELinux se lo puede configurar de tres maneras:

- **Enforcing.** Está en modo impositivo por lo cual se impone las políticas de seguridad de SELinux.

---

18 **NSA (Natiotal Security Agency).** Agencia de Seguridad Nacional de los Estados Unidos.

19 **SELinux (Security-Enhanced Linux).** Seguridad Mejorada de Linux.

20 **MAC (Mandatory Access Control)**. Control de acceso obligatorio.

21 **AVC (Access Vector Cache).** Caché de vector de acceso.

- **Permissive.** Está en estado permisivo, en este caso, SELinux notifica pero no impone las políticas. Se utiliza este estado para proceso de depuración, así conocemos cual sería el comportamiento de SELinux bajo algunas acciones que realicemos en el sistema.

- **Disabled.** Este estado es inhabilitado, esto quiere decir que SELinux no aplicará ninguna política, tampoco la registrará.

Para configurar el estado de SELinux, debemos abrir el archivo /etc/selinux/config, el cual tiene el siguiente contenido:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

En este caso de ejemplo, vemos que el sistema está en modo impositivo según lo determinado en el parámetro SELINUX=enforcing.

3.1.6. Protección de acceso remoto

Es muy común que se administren los servidores Linux de manera remota, es por esta razón, que debemos aplicar algunas medidas para evitar ataques.

3.1.6.1. Deshabilitar el acceso remoto al usuario root

El protocolo usado para acceder a un servidor Linux de manera remota es el SSH[22], el cual permite abrir una consola de administración del sistema.

Como ya lo hemos indicado, el super administrador se llama *root*, el cual tiene todos los privilegios sobre el sistema operativo. Si por alguna razón un atacante accede con este usuario porque descubrió su contraseña, este podría afectar enormemente al Linux, por esta razón recomendamos deshabilitar el acceso remoto para el usuario root de manera directa (Linux Total, 2015).

La pregunta que surge es: ¿Si deshabilito el acceso mediante el usuario root, como administro mi servidor remotamente?

La respuesta es sencilla, debemos acceder con un usuario común, cuyo nombre seguramente no es conocido y una vez adentro del sistema procedemos a cambiarnos de usuario mediante el comando ***su -*** . De esta manera podremos administrar nuestro servidor normalmente.

Para desactivar el acceso remoto con el usuario root, debemos entrar al archivo de configuración del servicio SSH, este es /etc/ssh/sshd_config, buscamos el parámetro *PermitRootLogin* y le ponemos No, debe quedar así:

PermitRootLogin no

Se reinicia el servicio para que surtan efecto los cambios realizados en la configuración.

3.1.6.2. Cambiar el puerto por defecto del servicio SSH

Muchos administradores aplican el cambio del puerto 22 el cual está configurado por defecto para el servicio SSH, por otro puerto no conocido, para de esta manera despistar a los atacantes.

---

22 SSH (Secure SHell), Intérprete de órdenes seguras, reemplaza al viejo protocolo RSH (Remote SHell).

Al cambiar el puerto 22 por otro, no se oculta el servicio, si usamos una herramienta para escaneo de puertos como nmap[23], este nos informará cual es el puerto que se está usando para el servicio SSH.

En todo caso si se requiere cambiar el puerto por defecto, se lo puede hacer en el archivo de configuración /etc/ssh/sshd_config, buscamos el parámetro Port, por ejemplo:

Port 2222

Esto quiere decir que el servicio SSH va a escuchar el puerto 2222 el cual será usado para los accesos remotos (Desde Linux, 2015).

3.1.6.3. Configuración del Firewall para regular los accesos remotos.

Según lo explicado en el punto 2.4.4., el iptables permite crear reglas para el filtrado de paquetes, es buen hábito filtrar los accesos por el puerto 22 o el configurado para el servicio SSH para determinas direcciones IP públicas. Esto quiere decir que por ejemplo podemos activar el acceso al puerto 22 desde una IP pública conocida y para el resto de direcciones IP denegar el acceso, de esta manera se reduce considerablemente un posible ataque mediante el uso de este protocolo.

Como recomendación es importante que la IP pública que tendrá acceso al servidor no cambie, en el caso de que esta cambie, nos quedaremos sin acceso remoto al servidor. Es muy frecuente que en conexiones de Internet para hogares, las direcciones IP públicas cambien constantemente.

3.1.7. Uso de protocolos seguros

Cualquier servidor expuesto al Internet está en peligro, este medio es muy inseguro, por esta razón, se hace necesario el uso de protocolos seguros, ¿qué son los protocolos seguros?.

---

23 **Nmap.** Es un programa de código abierto, el cual realiza un escaneo de puertos de comunicación.

Los protocolos tradicionales suelen trasmitir información de tal manera que esta pueda ser interceptada por un atacante dentro de la red, los protocolos seguros lo que hacen es aplicar varios mecanismos criptográficos, que impidan descifrar la información transmitida dentro de una red.

Existen protocolos seguros para el manejo de: confidencialidad de la información, autenticación, autorización, integridad, no repudio, etcétera.

En el caso específico de Linux, tenemos algunos protocolos de utilidad, por ejemplo:

SSH. (Secure Shell). Es un protocolo que permite crear conexiones seguras entre dos equipos, sobre redes no seguras.

Con SSH (Safari, 2015) podemos reemplazar a protocolos inseguros como: telnet[24], FTP[25], RLOGIN[26], RSH[27], y RCP[28], usando: SFTP[29], y SCP[30].

SSL. (Secure Socket Layer). Es un protocolo que permite el uso de certificados digitales para establecer comunicación segura entre dos equipos remotos. Permite asegurar varios servicios que funcionan en Internet, por ejemplo: Web (HTTPS), correo electrónico entre otros (GlobalSign, 2015).

TLS. (Trasport Layer Security). Protocolo criptográfico sucesor de SSL, el cual permite asegurar la comunicación entre dos puntos dentro de Internet.

---

24 **TELNET**. (Teletype Network). Es un protocolo que permite manejar remotamente a un equipo, ocupando el puerto

25 **FTP.** (File Transfer Protocolo). Protocolo que permite la transferencia de archivos utiliza el puerto 21 por defecto

26 **RLOGIN**. (Remote Login) Protocolo basado en TCP/IP para acceso de sesión remoto.

27 **RSH.** (Remote Shell) Usa RLOGIN para acceso remoto de una consola SHELL.

28 **RCP.** (Remote Copy). Protocolo que permite realizar copias de archivos entre equipos remotos.

29 **SFTP.** (Secure File Transfere Protocol). Protocolo separado que aprovecha una conexión vía SSH para realizar la transferencia de archivos.

30 **SCP** (Secure Copy). Permite realizar copia remota de archivos bajo SSH.

VPN. (Virtual Private Network). Es un conjunto de protocolos, que permiten la extensión de una red privada sobre una red pública (Internet). Mediante esta tecnología, es posible realizar enlaces dedicados entre puntos geográficamente lejanos a muy bajo costo. Es recomendable el uso de esta tecnología para tener accesos remotos a una red.

3.2. Herramientas de monitoreo de servicios y recursos

Podemos tener un sistema instalado y funcionando, sin embargo pueden ocurrir problemas de seguridad que afecten al servidor o a los servicios de red brindados; es fundamental que los administradores de red, conozcan las herramientas de monitoreo.

Linux proporciona varios comandos que permiten determinar problemas en el rendimiento de un servidor, adicional también tenemos disponible algunas herramientas gráficas que ayudan a conocer el estado de nuestro sistema.

3.2.1. Herramientas de monitoreo bajo consola

Existe una gran variedad de comandos que informan sobre el estado del sistema operativo, a continuación detallamos los que consideramos muy importantes. La salida de los comandos está referidos en el **Anexo A** de este documento.

3.2.1.1. Comando free

El comando free (rm-rf.es, 2015), permite conocer el consumo de memoria RAM, tanto la memoria real como de la virtual. Normalmente cuando vemos que el consumo de memoria es alto, el administrador piensa en aumentar la capacidad para mejorar el rendimiento del equipo; muchas veces esta no es la solución, ya que pueden existir procesos que están consumiendo memoria innecesariamente, esto ocasiona que se utilice la memoria virtual.

Es una alerta que un servidor consuma memoria virtual, debemos analizar el comportamiento del servidor y determinar las causas. Si luego de un estudio profundo de los procesos, se determina que por el normal uso del servidor justifica el consumo, se debe proceder aumentar la memoria real si el hardware lo permite.

Podemos crear un script Shell que verifique el consumo de memoria y nos alerte en el caso de que este sea exagerado.

3.2.1.2. Comando top

Muestra de manera dinámica los programas que se están ejecutando en orden de los procesos que más recursos están consumiendo en el sistema. Presenta también información importante como:

- Hora actual
- Tiempo en el cual el sistema está funcionando
- Número de usuarios registrados
- La carga promedio[31]
- Número de tareas
- Número de procesos corriendo, dormidos y en estado zombie
- Consumo de la CPU
- Consumo de la memoria física
- Consumo de la memoria virtual (swap)

Los procesos son detallados con la siguiente información:

- **PID.** Identificador del proceso
- **USER.** Usuario quien ejecutó el proceso
- **PR.** Prioridad del proceso.
- **NI.** Asignación de prioridad por parte del usuario
- **VIRT.** Consumo de memoria virtual por parte del proceso.

---

31 **Carga del Servidor Promedio** (Load Average). Son tres valores que determinan el trabajo del CPU, en periodos de tiempo de 1, 5 y 15 minutos. Permite determinar si el CPU está subutiliado o sobreutilizado.

- **RES.** Consumo de la memoria física por parte del proceso.
- **SHR.** Memoria compartida
- **%CPU.** Porcentaje de consumo de procesador/es
- **%MEM.** Porcentaje de consumo de la memoria física
- **TIME+.** El tiempo que lleva ejecutándose el proceso
- **COMMAND.** El comando que se está ejecutando dueño del proceso.

Para un administrador, este comando es de gran utilidad para determinar los proceso que están consumiendo excesivamente recurso del sistema, por eso lo recomendamos el uso (CCM, 2015).

3.2.1.3. Comando htop

Este comando no viene instalado por defecto, pero recomendamos lo carguen en el sistema ya que es muy similar al top, la ventaja de htop (hipertextual, 2015) es que podemos interactuar para el manejo de procesos, permite por ejemplo:

- Buscar un proceso (Presionar F3)
- Filtrar por nombre de los procesos (Presionar F4)
- Presenta el árbol de procesos (Presionar F5)
- Permite ordenar los procesos por: (Presionar F6)
    - Número de proceso
    - Usuario
    - Prioridad
    - Consumo de memoria
    - Consumo de procesador
- Estado

- Disminuir la prioridad (Presionar F7)
- Aumentar la prioridad (Presionar F8)
- Enviar señales a los procesos (Presionar F9)

3.2.1.4. Comando ps

Este comando enlista todos los procesos que están corriendo en el servidor, es muy útil para determinar si un programa se está ejecutando o no (HScripts.com, 2015).

Esta herramienta tiene una gran variedad de opciones que facilitan analizar a los procesos del sistema. Las opciones comunes son “aux”, las cuales presentan todos los procesos y sus detalles.

Dentro de la información que presenta ps, podemos destacar:

- Usuario dueño del proceso
- Identificador del Proceso (PID)
- Los archivos binarios abiertos para que se ejecute el proceso.

Con esta información es fácil administrar los procesos y detectar ataques o código malicioso que se esté ejecutando en el sistema.

3.2.1.5. Comando df

Presenta la información de las particiones de disco y su consumo (HScripts.com, 2015). Es muy útil para determinar particiones que se quedan sin espacio, lo que puede ocasionar problemas con el rendimiento del servidor.

Como lo indicamos anteriormente, al momento de instalar el servidor se deber realizar un análisis previo para realizar una repartición de espacio adecuado, así reducimos el desperdicio y optimizamos al máximo el uso de disco. Bajo esta herramienta determinamos el consumo exacto de espacio en disco.

3.2.1.6. Comando w

Presenta información sobre los usuarios registrados en el sistema, también indica la carga promedio (Linux y Software Libre en Colombia, 2015). Es útil para conocer la salud del servidor y que usuarios se encuentran activos.

En el tema de seguridad, con este comando podemos detectar usuarios registrados que pueden estar ejecutando acciones no permitidas en el sistema. También nos entrega un resumen del consumo de recursos para determinar problemas de rendimiento en el servidor.

Cuando existen usuarios remotos registrados, podremos conocer la dirección IP desde donde han realizado la conexión.

Con la información resumida pero importante, podremos detectar usuarios desconocidos registrados en el sistema, lo que están haciendo y desde donde se conectan.

3.2.1.7. Comando isof

Este comando presenta los archivos que se encuentran abiertos cuando se ejecuta un proceso en el sistema (NexoLinux, 2015). Con la opción -p, permite conocer los archivos que abre un determinado proceso.

Cuando detectamos un proceso no conocido, podemos examinarlo con el uso de esta herramienta, así sabremos exactamente donde están ubicados los archivos ejecutables y que comportamiento tiene un determinado proceso.

Es común que los atacantes coloquen código malicioso en la carpeta temporal del sistema /tmp, con este comando lo podríamos detectar inmediatamente.

3.2.1.8. Comando ifstat

Este comando presenta estadísticas de actividad, de todas las interfaces de red que tiene el servidor (Linux Hispano, 2015).

Para nosotros es un comando muy útil y sencillo, se puede analizar el número de paquetes de entrada/salida procesados por el equipo, de igual manera la cantidad de información entrante/saliente. Además presenta la cantidad de errores ocurridos al trasmitir o recibir información.

Si implementamos un servidor de comunicaciones con Linux, podremos determinar problemas de consumo de red por cada interface.

Una variante interesante de este comando es cuando lo usamos con la opción –t, la cual permite entregar las estadísticas en un periodo de tiempo determinado en segundos; esto puede ayudar a determinar problemas en tiempo real.

3.2.1.9. Comando netstat

Sirve para realizar un monitoreo de la red (Alcance Libre, 2015), fundamentalmente es capaz de entregar información referente a las conexiones de red.

Mediante este comando podemos determinar puertos abiertos del servidor y detectar demonios que se encuentren levantados innecesariamente. Con la opción –a muestra todas las conexiones de red establecidas en el servidor tanto TCP como UDP, al ser muy extensa la salida en pantalla, lo podemos paginar de la siguiente manera:

#netstat –a | less

Más útil puede resultar utilizando la opción –p (muestra el nombre de los programas), combinando la salida en pantalla con el comando grep (permite buscar un patrón de texto), de la siguiente manera:

#netstat –ap | grep httpd.

Buscará si el programa httpd (servicio web), tiene conexiones activas.

3.2.1.10. Comando pmap

Presenta un detalle del consumo de memoria RAM de un proceso. Informa sobre los archivos abiertos y su respectivo consumo (die.net, 2015).

Es un complemento del comando *ps* anteriormente analizado, este último presenta los identificadores de los procesos (PID), mediante pmap podremos conocer el detalle en memoria RAM de los procesos consultados.

Para determinar problemas con los procesos de un programa, este comando es muy útil al presentar una radiografía de los procesos. Se requiere ciertos conocimientos avanzados sobre la administración de procesos, sin embargo debemos señalar que es muy útil.

3.2.1.11. Comando tcpdump

Permite mostrar en tiempo real el tráfico de la red a la cual está conectado el computador desde el que se ejecuta este comando (TCPDUMP & LIBCAP, 2015).

Es muy útil y completo para la captura de paquetes que transitan por la red, utiliza la librería libcap, prácticamente es un sniffer.

Las opciones más útiles de este comando son:

- **-i.** Determinar que interface de red usaremos para capturar los paquetes.
- **-w.** Si requerimos que la salida del comando se guarde en un archivo de texto plano.
- **-D.** Presenta las interfaces disponibles.
- **tcp.** Captura solo tráfico bajo TCP.
- **udp.** Captura solo tráfico bajo UDP.
- **icmp.** Captura solo tráfico bajo ICMP.
- **port.** Captura el tráfico por un puerto determinado.
- **src.** Capturar el tráfico de una IP de origen específica.
- **dst.** Captura el tráfico de una IP de destino específica.
- **-A.** Vuelca el contenido de un paquete en código ASCII

Como podemos analizar brinda un sin número de opciones de gran utilidad, si implementamos a Linux como un servidor de comunicaciones, podremos estudiar el tráfico de entrada y salida hacia nuestra red privada. La utilidad de este comando es muy grande.

3.2.1.12. Comando vmstat

Muestra la estadística de la memoria y a su vez proporciona información sobre los eventos del sistema (Ubuntu manuals, 2015). Se usa con algunas opciones útiles, estas son:

- **-s.** Muestra el número de eventos que se produjeron desde la última vez que se inició el sistema.
- **-S.** Muestra las estadísticas de intercambio de memoria física y swap
- **-i.** Muestra las interrupciones por dispositivo

Para analizar la salud de un servidor, este comando suele ser muy útil, recomendamos su uso permanente para determinar problemas en rendimiento del equipo con Linux.

3.2.2. Herramientas gráficas de monitoreo

Como se puedo analizar, existen comandos bajo consola muy útiles para determinar la salud de un servidor, sin embargo puede ser interesante instalar herramientas que manejen un historial y generen estadísticas de consumo de recursos. Es importante conocer el comportamiento de un servidor con el uso de comandos como lo analizamos en el punto anterior o con herramientas gráficas de monitoreo.

Existe una gran variedad de herramientas que presentan de forma gráfica el estado de un servidor, la mayoría de programas se basan en la lectura de los archivos de registro (logs[32]), los cuales almacenan los datos generados por los diferentes servicios que corren en el equipo. Mediante el uso de fórmulas y gráficos estadísticos podemos acceder a la información y determinar los problemas en el rendimiento de los servidores. Se recomienda instalar herramientas gráficas para que el administrador pueda tener los recursos necesarios para realizar un monitoreo constante. Los programas de monitoreo gráfico son muy intuitivos, por lo que no se requiere un tiempo considerable para aprender su manejo. A continuación enlistaremos algunas herramientas gráficas que están disponibles para la mayoría de las distribuciones Linux:

---

32 Logs. Registro del sistema generados por el servicio rsyslog, el cual guarda la información en archivos de texto plano.

3.2.2.1. Munin

Es una de las herramientas gráficas más usadas para el monitoreo de recursos en ambientes UNIX, está construido bajo tecnología web y presenta las estadísticas de consumo de recursos, lo que permite detectar con facilidad los problemas de rendimiento (Munin, 2015). Munin está basado en RRDtool[33] para el manejo de datos. Se puede obtener información por día, semana o mes; así podemos conocer el comportamiento de nuestro servidor y determinar las horas pico de mayor trabajo. (Ver Figura 2).

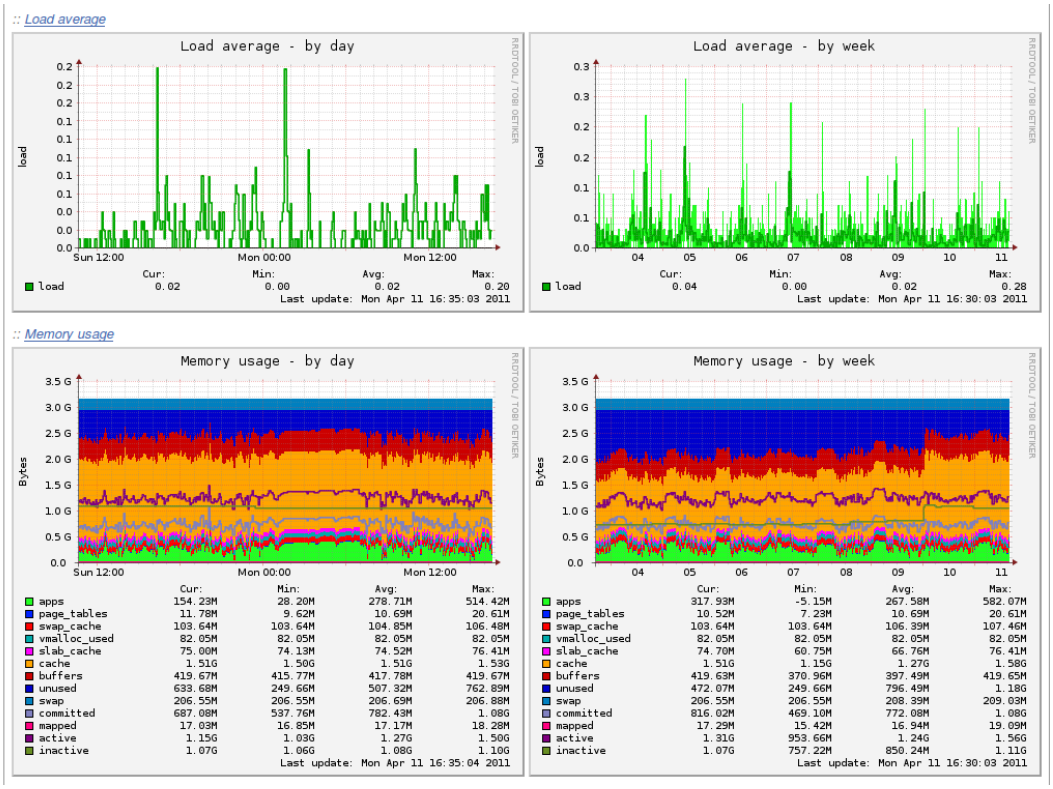

Figura 2: Captura de pantalla de estadísticas Munin

33 **RRDtool**. Es una herramienta que guarda información en una base de datos, con el objetivo de luego presentar una estadística detallada, es muy utilizado para el manejo de datos temporales y datos seriales como, el uso de procesador, memoria, tráfico de una red.

Para el tema de seguridad, Munin puede colaborar en detectar problemas de rendimiento del servidor por ejemplo, si analizamos el consumo de recursos de hardware, se puede detectar si está corriendo algún tipo de código malicioso.

3.2.2.2. Cacti

Al igual que Munin, es una herramienta web que usa RRDtool, la diferencia principal es que Cacti (Cacti, 2015) puede hacer uso del protocolo SNMP[34]. (Ver Figura 3).

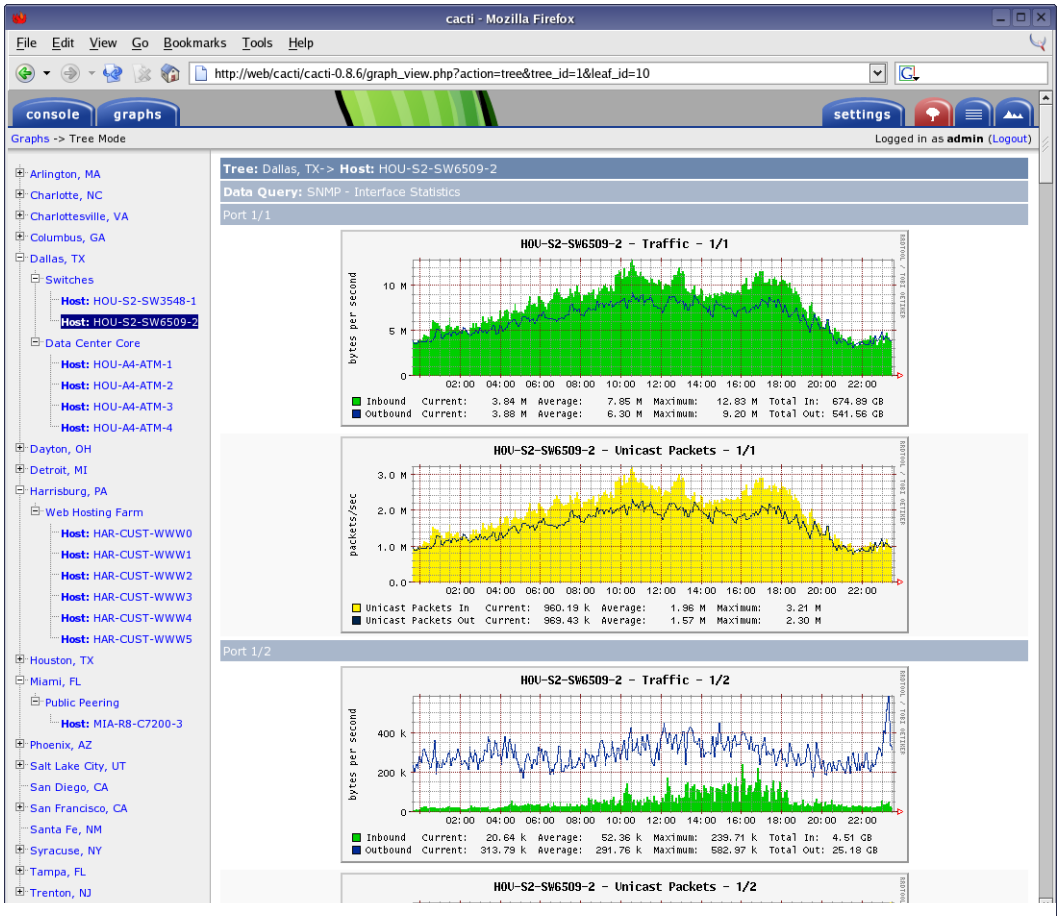

Figura 3: Captura de pantalla estadística Cacti

34 **SNMP. (Simple Network Management Protocol)**. Es un protocolo que permite el intercambio de información de administración entre dispositivos de red.

Para el funcionamiento de esta herramienta se requiere la instalación de un servidor Web como Apache o Lighttpd[35], base de datos MySQL y lenguaje de programación PHP. La información recopilada mediante el protocolo SNMP, es guardada en la base de datos, para posteriormente ser analizada con el uso de gráficos estadísticos.

Es otra opción muy útil a l igual que Munin, para monitorear los recursos de un servidor, adiciona es multiplataforma, se puede también instalar en equipos con sistema operativo Windows.

3.2.2.3. Nagios

Es una herramienta que permite el monitoreo de servicios como: HTTP, SMTP, POP3, ICMP, NNTP y SNMP. También puede analizar los recursos del sistema como: carga del servidor, lectura y escritura de discos y registros de log (Nagios, 2015).

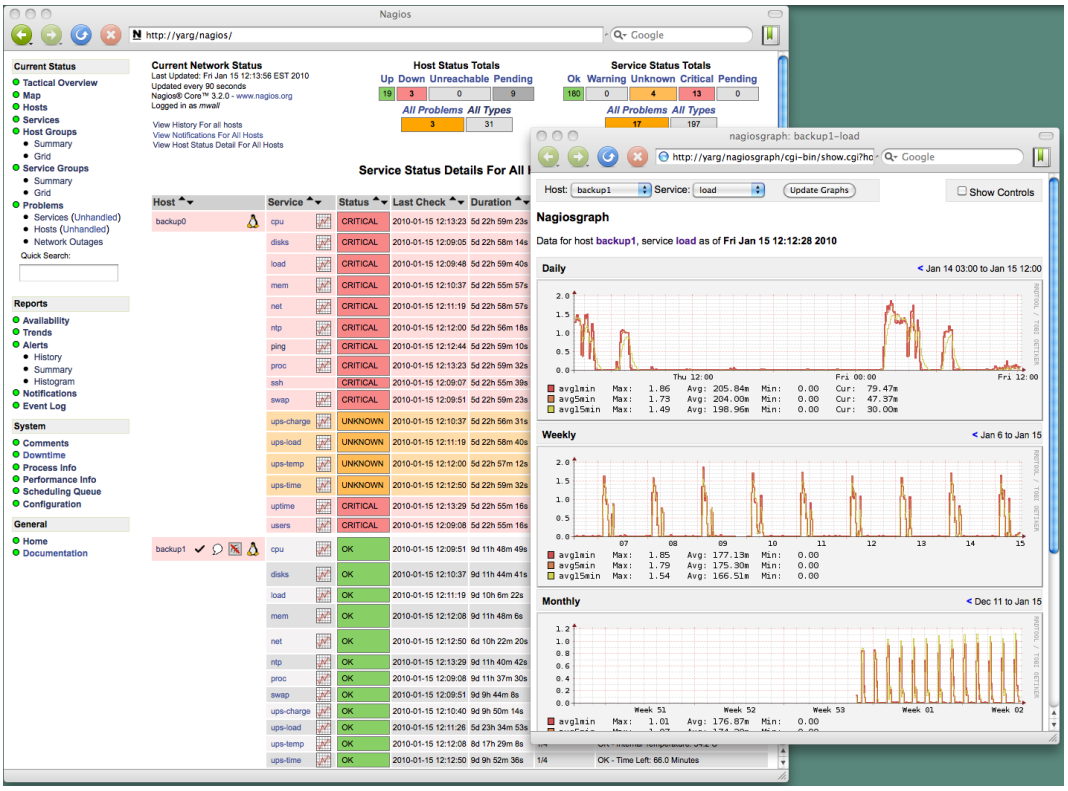

Figura 4: Estadísticas de Nagios

35 **Lighttpd.** Servidor web para lLinux, muy ligero.

Permite notificaciones por varias vías: correo electrónico, mensajes de texto, plugins de navegadores, entre otras. (Ver Figura 4). Se debe tomar en cuenta que el monitoreo es remoto.

3.3. Sistema de detección/prevención de intrusos (IDS/IPS)

Como parte de las herramientas de seguridad para las redes de comunicación, tenemos a los IDS[36] y a los IPS[37], estos se encuentras disponibles también para sistemas Linux.

Los IDS tienen como objetivo fundamental el detectar eventos que comprometen la seguridad de un sistema informático, en cambio los IPS tienen como objetivo la prevención de intrusiones en un sistema informático.

En Linux existen varias soluciones que funcionan como IDS o IPS, sin embargo en el presente documento, citaremos dos herramientas muy usadas en ambientes Unix.

3.3.1. Snort

Figura 5: Logotipo de Snort

Snort es un detector de intrusiones orientado al monitoreo de una red, se basa en el escaneo de puertos para identificar cualquier anomalía en el sistema (Snort FAQ, 2015).

Al momento de instalar Snort, este trae reglas predefinidas, sin embargo el juego de reglas complejas tienen costo.

---

36 IDS (Intrusion Detection System). Sistema de detección de intrusiones.

37 IPS (Intrusion Prevention System). Sistema de prevención de intrusiones

Snort puede trabajar también como IPS, luego de la detección de una intrusión, este es capaz de bloquear el ataque y de esta manera evitar un problema de seguridad en el servidor. Es evidente que el uso de esta herramienta, reduce considerablemente los eventos por ataques a sistemas informáticos. (Ver Figura 6).

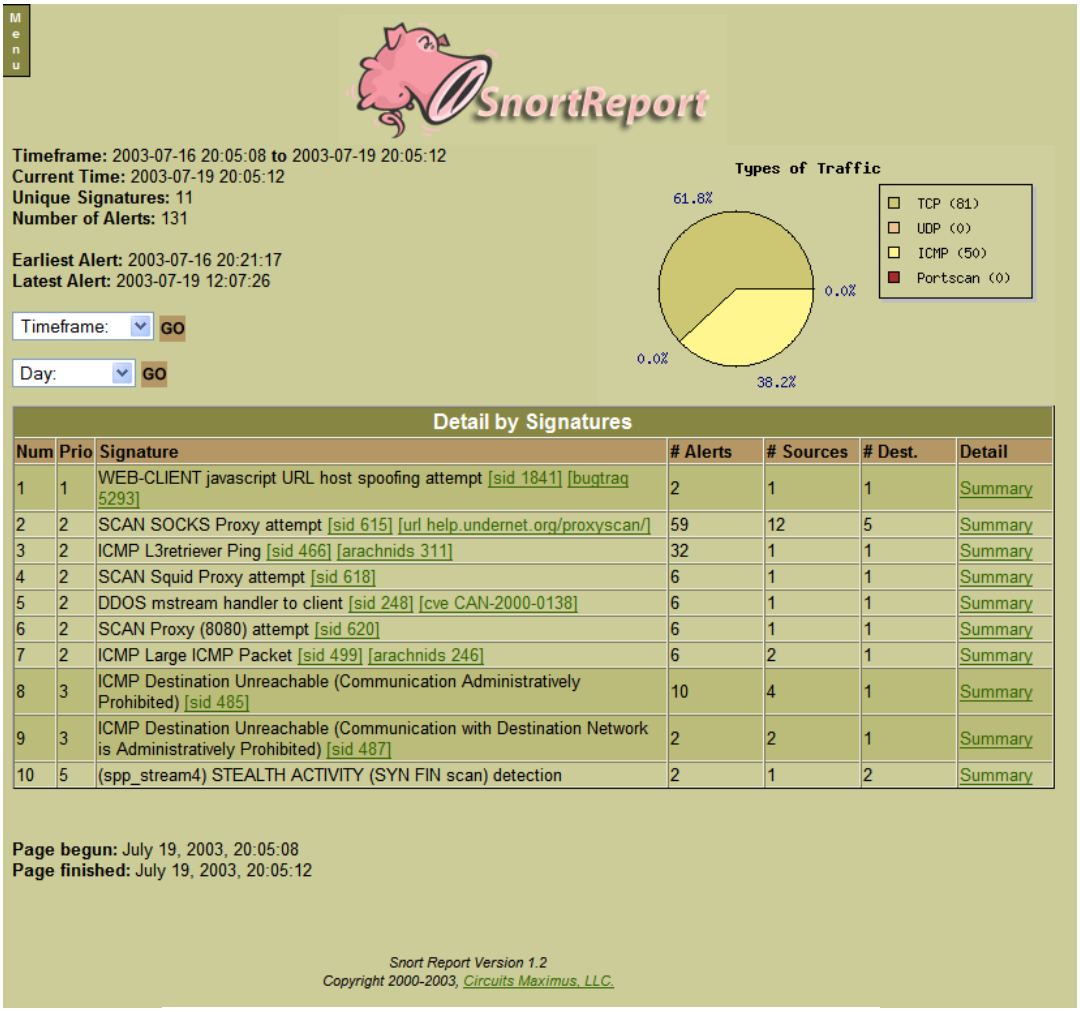

Figura 6: Reporte generado por Snort

Snort se puede instalar en cualquier distribución Linux, sin embargo en algunas es un trabajo difícil y se requiere conocimientos avanzados.

3.3.2. Suricata

Herramienta desarrollada por Open Information Security Foundation en el 2009, el cual trabaja como IDS e IPS al igual que Snort (Suricata, 2015).

Permite la ejecución de varios procesos y subprocesos de manera simultánea, lo que facilita el procesar una gran cantidad de paquetes para ser escaneados.

Está basado en reglas para la detección de intrusiones y es compatible con las reglas desarrolladas para Snort.

Esta herramienta presenta la información por consola, es decir que no se requiere tener una interfaz gráfica para su uso. (Ver Figura 7).

Finalmente, debemos indicar que su popularidad es menor a la que tiene Snort que se ha convertido en el programa preferido para utilizarlo como IDS/IPS en ambientes Linux.

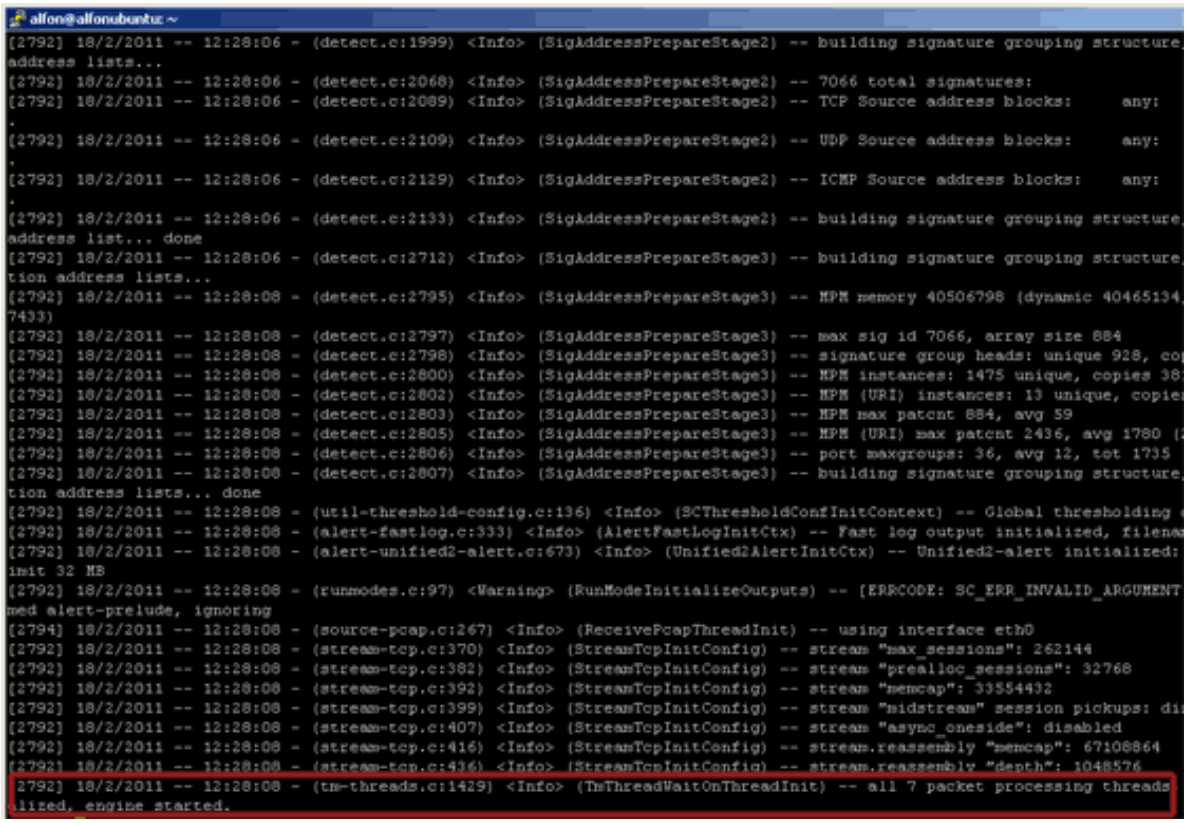

Figura 7: Reporte por consola generado por Suricata

3.4. Sistemas para escaneo de vulnerabilidades

Los escáneres de vulnerabilidades son herramientas que permiten verificar mediante el uso de reglas la existencia de brechas de seguridad en un sistema operativo o red. Estos programas utilizan una serie de protocolos y mecanismos internos para la detección de problemas.

El sistema más conocido es Nessus, sin embargo existen otras alternativas, por ejemplo OpenVAS, Nexpose entre otros.

3.4.1. Nessus

Contiene un demonio que realiza el escaneo de vulnerabilidades, para ello utiliza una serie de plugins y mediante el uso de reglas, realiza la verificación de un equipo o red. Esta herramienta tiene una interfaz web amigable, además que es multiplataforma.

Figura 8: Captura de pantalla de Nessus

Nessus tiene una versión home la cual es gratuita, para soluciones más avanzadas tiene las versiones: Nessus professional, Nessus Manager y Nessus Cloud, las cuales son pagadas (Tenable Network Security, 2015).

La instalación de esta herramienta es muy amigable y en la versión actual es muy completa para el manejo de vulnerabilidades ofreciendo un sin número de herramientas que permiten encontrar problemas en el sistema operativo, servicios, sistemas de archivos, manejo de usuarios, etcétera. (Ver Figura 8).

3.4.2. OpenVAS

OpenVAS, es un sistema para escanear vulnerabilidades liberado bajo licencia GPL, al inicio del proyecto se lo denominó GNessus ya que el equipo desarrollador de esta herramienta, anteriormente trabajó para Nessus (OpenVAS, 2015).

Utiliza interfaz web y no solamente realiza un escaneo de puertos, al igual que Nessus mediante el uso de reglas verifica las vulnerabilidades de un equipo. Por el tiempo de desarrollo menor que Nessus, esta herramienta cuenta con menos puntos de inspección, sin embargo por ser un proyecto en software libre, su desarrollo es muy acelerado.

(Ver Figura 9)

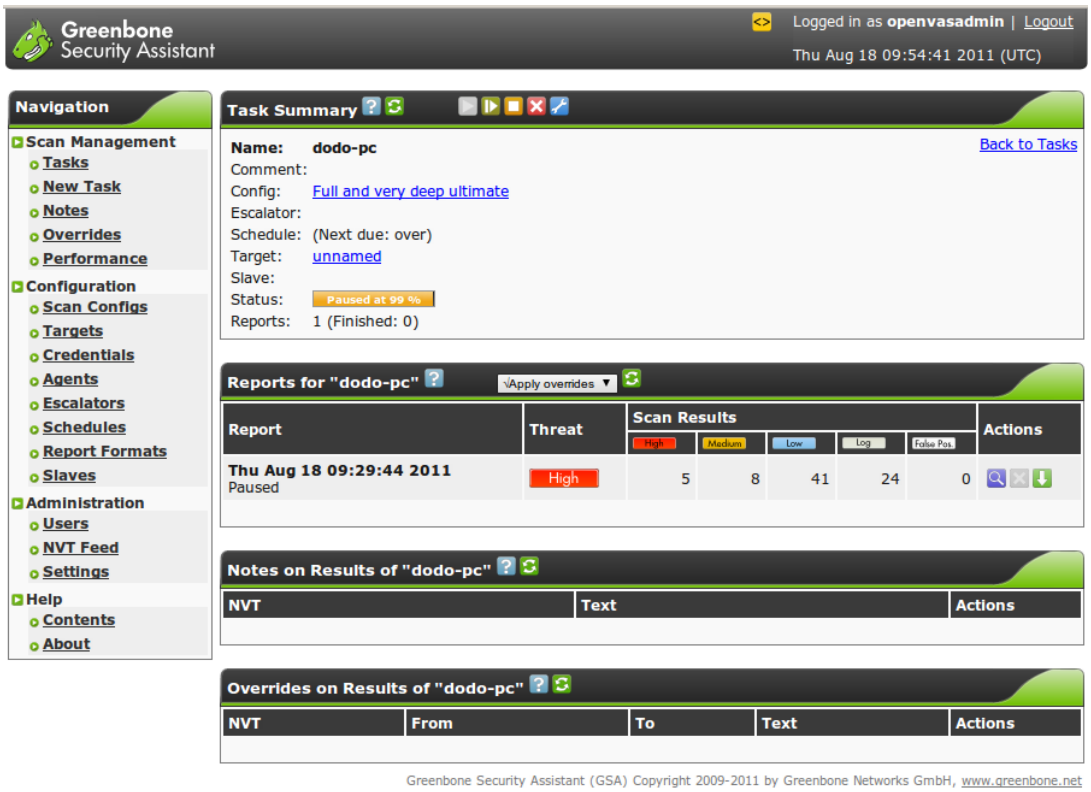

Figura 9: Captura de pantalla de OpenVAS

3.4.3. NeXpose

NeXpose es una herramienta de escaneo de monitoreo de la empresa Rapid7 la cual provee de otros sistemas para el manejo de seguridad como Metasploit[38] (Rapid 7, 2015).

Brinda una interfaz web para realizar un escaneo de vulnerabilidades de un equipo o red que pueden ser encontradas en el sistema operativo, base de datos, sistema de archivo. NeXpose detecta software malicioso y es multiplataforma. (Ver Figura 10).

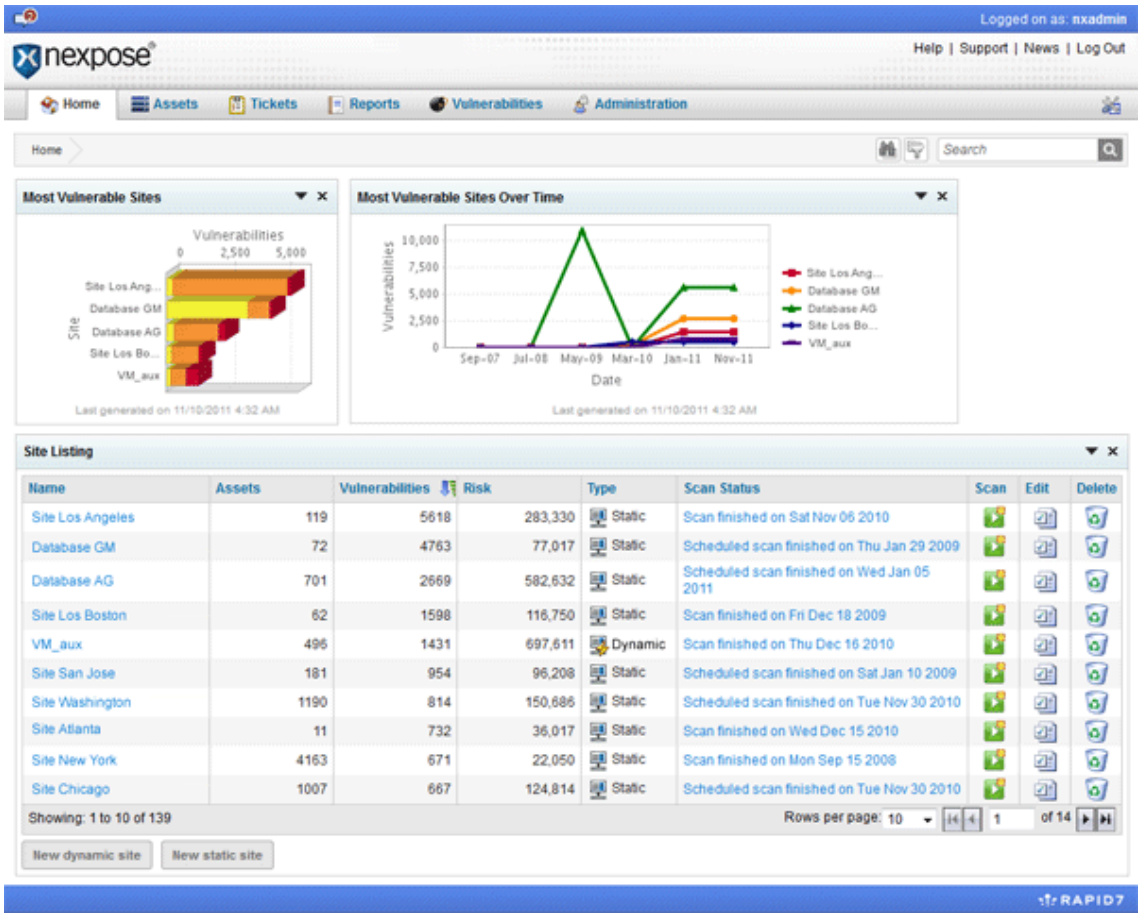

Figura 10: Captura de pantalla de Nexpose

38 Metasploit. Es una herramienta para realizar pruebas de penetración para equipos de seguridad.

3.5. Implementación de AIDE

AIDE[39] es un sistema que permite detectar intrusiones a través de alteraciones, en el sistema de archivos (AIDE, 2015).

Esta herramienta toma una radiografía del sistema de archivos, para luego identificar las modificaciones que se hayan realizado y así descubrir intrusiones.

Para poder analizar la integridad del sistema de archivos, AIDE utiliza a mhash[40], librería que maneja varios algoritmos de encriptación.

La implementación de esta herramienta es muy sencilla y útil para identificar cambios en archivos que sean evidencia de una intrusión o alteración del Linux.

3.6. Sistema de aseguramiento Bastille

Bastille es una herramienta que permite endurecer a Linux mediante el cambio de varias configuraciones en el sistema.

Para usuarios sin mayor experiencia en Linux, esta herramienta puede ser de gran utilidad, mediante un conjunto de preguntas, Bastille configura al sistema como el administrador desea (Linux Zone, 2015).

Dentro de las consideraciones de seguridad que toma en cuenta esta herramienta son:

- Desactivar programas innecesarios.
- Auditar las configuraciones de algunos servicios instalados.
- Verifica los permisos y listas de archivos de control de acceso.
- Analiza configuraciones de la red.
- Realiza una revisión de la configuración del gestor de arranque.
- Entre otros.

---

39 AIDE (Advanced Instruction Detection Environment). Herramienta que permite detectar intrusiones al determinar alteraciones en el sistema de archivos.

40 MHASH. Librería que provee una interface para el uso de algoritmos de encriptación.

3.7. Repositorios

Un repositorio es un lugar dentro de Internet que almacena todo el software publicado por una distribución Linux. Existe al menos un repositorio oficial por cada distro (Ovtoaster, 2015).

Los repositorios permiten la descarga de paquetes de versiones base, actualizaciones y paquetes extra para una distro, al tener todo disponible en Internet, es muy fácil el instalar paquetes de software.

Cada distribución Linux trabaja con un gestor de paquetes, el cual se comunica con los repositorios instalados en el sistema para la instalación o actualización de paquetes de software. (Ver Figura 11).

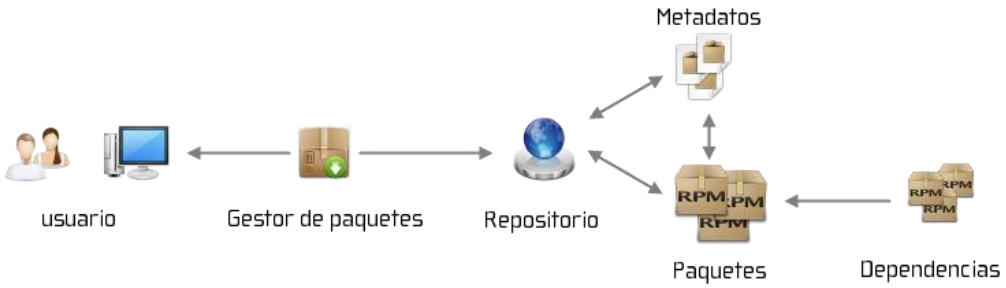

Figura 11: Diagrama que representa la estructura de un repositorio

3.7.1. Características de los Repositorios

Dentro de las características principales de un repositorio tenemos:

- Son de acceso público, al estar disponibles en Internet.
- Proveen los paquetes de software de una distribución Linux.
- Están bajo un sistema de espejos alrededor de todo el mundo para su mayor disponibilidad.
- Son accedidos mediante el gestor de paquetes proveído por la distribución Linux.

- Para su acceso se utilizan típicamente los protocolos: HTTP, FTP, RSYNC.

Se debe recalcar que existen repositorios oficiales y no oficiales disponibles para las distribuciones, por ejemplo:

RedHat tiene sus repositorios oficiales, sin embargo existen: EPEL, RPMFORGE, ANKU, entre otros, que pueden ser instalados en un sistema RHEL, los cuales permiten agregar paquetes de software que no ofrece la distribución.

3.7.2. Actualizaciones en Linux

Mediante el uso de los repositorios, las actualizaciones de las distribuciones se lo hacen de manera muy simple, sin embargo debemos considerar algunos aspectos que pueden afectar a nuestro sistema.

Si tenemos instalados repositorios que no son oficiales y ejecutamos una actualización, puede ser que algunos paquetes entren en conflicto y ocasionen inconvenientes. Los repositorios extras suelen traen versiones más actuales de las que provee el repositorio oficial. Se recomienda el uso de repositorios adicionales, sin embargo al momento de actualizar el sistema, estos deben estar deshabilitados.

Debemos considerar al momento de instalar un repositorio, que este pertenezca a la versión de la distribución instalada, si utilizamos una versión diferente, ocasiona problemas graves al momento de actualizar el sistema.

Se recomienda revisar de manera permanente la existencia de actualizaciones de paquetes, estos muchas veces proveen parches sobre paquetes a los cuales se les ha detectado errores. Es importante escoger una distribución Linux que se comprometa a distribuir actualizaciones para versiones anteriores, como lo hemos indicado, es de suma importancia tener nuestro sistema actualizado.

CAPÍTULO 4: ESTUDIO COMPARATIVO DE LAS DISTRIBUCIONES LINUX.

Luego de analizar varios criterios de seguridad se debe realizar la comparación de las distribuciones Linux orientado a la seguridad de las redes de comunicación.

En base a la información recopilada y documentada en los capítulos anteriores, vamos a realizar la comparación de las distribuciones Linux de acuerdo a parámetros generales y de seguridad. Los criterios considerados para determinar los parámetros a evaluar, se basan a las recomendaciones entregadas por las distribuciones y bajo la experiencia que tenemos en la administración de sistemas Linux.

Para poder obtener datos exactos basados en la práctica, se crearán escenarios de prueba, utilizando un servidor de virtualización. Se instalarán las distribuciones Linux a estudiar para verificar el cumplimiento o no de los parámetros diseñados.

Posteriormente se pondera los parámetros de acuerdo a la importancia y se analiza cada distribución evaluando su cumplimiento.

Para la presentación de resultados se crea una matriz con las calificaciones finales según cada característica analizada, se determinará la distribución que más cumple con los criterios de seguridad.

Debemos recalcar que las distribuciones estudiadas son las orientadas a brindar servicios de red, no se tomó en cuenta las distribuciones diseñadas para usuario final u otros fines diferentes a las redes de comunicaciones.

4.1. Determinación de las distribuciones Linux a estudiar.

Como lo hemos explicado anteriormente existen alrededor de 280 distribuciones Linux conocidas, no es factible realizar un estudio comparativo de todas ellas, por esta razón, se realizó una investigación de las distro Linux más utilizadas para determinar cuál es la mejor opción en seguridad. Según el reporte detallado en el punto 2.3.1 y 2.3.2, las distribuciones más usadas a nivel mundial y en nuestro medio son:

1. Kali
2. Fedora
3. CentOS (Red Hat)
4. Arch
5. Ubuntu
6. Open Suse
7. Debian
8. Mint
9. Mageia
10. Zorin
11. Elementary
12. Lubuntu
13. LXLE
14. Puppy
15. Bodhi
16. PCLinuxOS
17. Deepin
18. Manjaro
19. Ultimate Edition
20. Xubuntu

Debemos señalar que dentro de esta lista no se encuentra una de las distribuciones Linux más importantes como es *Red Hat*, la cual ha desarrollado muchas herramientas útiles y definitivamente aporta en gran magnitud el desarrollo de Linux en todo el mundo. La principal causa por la cual no se encuentra instalada en un gran número de equipos, se basa a que esta tiene costo por soporte (Red Hat, 2015).

El hecho de tener costo no implica que esta distribución no sea software libre, ya que está liberada bajo licencia GPL en su gran mayoría.

Dentro del estudio tenemos a CentOS que es una distribución Linux clon de Red Hat, esto quiere decir que técnicamente son distribuciones idénticas a excepción de la imagen corporativa; Red Hat lo maneja bajo derechos reservados de la marca.

Para el presente trabajo al estudiar a CentOS, estamos comparando a Red Hat, por lo antes expuesto.

4.1.1 Características generales de las distribuciones Linux.

En este punto analizaremos las características generales de las distribuciones Linux a estudiar, con el objetivo de conocer los datos que permitirán posteriormente realizar la respectiva comparación.

El detalle del análisis de las distribuciones está disponible en el **Anexo B**, pueden encontrar información de las características generales de cada una de ellas.

De las veinte distribuciones estudiadas, una está orientada a hackeo ético, trece a usuario final y seis a brindar servicios de red. CentOS/Red Hat y Debian, son las únicas distribuciones cien por ciento orientadas a servidores; Ubuntu, Open SUSE, ArchLinux y Mageia, son distribuciones para usuario final, pero tienen versiones para servidores.

4.2. Creación de escenarios de prueba

Es fundamental que podamos constatar las características de seguridad en equipos instalados con cada distribución, por esta razón debemos crear escenarios de prueba.

La virtualización permite crear máquinas virtuales independientes, así podremos instalar todas las distribuciones a estudiar y realizar las pruebas necesarias.

Para virtualizar utilizaremos un servidor con KVM[41] bajo un equipo instalado con Linux Fedora 22.

Luego de analizadas las características básicas de las distribuciones, crearemos los escenarios de prueba para las siguientes:

- CentOS
- ArchLinux
- Ubuntu Server
- Open Suse
- Debian
- Mageia

4.2.1. Instalación y configuración de KVM

Para la creación de máquinas virtuales debemos tener un computador con procesador que soporte virtualización; podemos buscar en las especificaciones del procesador la bandera "vmx"[42] o "svm[43]". En Linux debemos ejecutar lo siguiente:

```
[root@pruebas~]# cat /proc/cpuinfo | egrep "vmx|svm
```

Una vez comprobado el soporte procedemos a instalar lo necesario, estas acciones la debemos hacer con el super usuario "root".

```
[root@pruebas~]# yum install qemu-kvm qemu-img virt-manager libvirt libvirt-python python-virtinst libvirt-client virt-install virt-viewer
```

Los componentes son:

---

41 **KVM (Kernel-based Virtual Machine)**. Es un módulo del núcleo de Linux que permite implementar virtualización completa.

42 **vmx.** Bandera del CPU para determinar soporte de virtualización en procesadores Intel.

43 **svm.** Bandera del CPU para determinar soporte de virtualización en procesadores AMD.

- **qemu-kvm.** Emulador de procesadores
- **qemu-img.** Gestor de imágenes de disco
- **virt-manager.** Gestor gráfico de máquinas virtuales
- **libvirt.** Demonio para manejar máquinas virtuales
- **libvirt-client.** Provee la API para acceder al servicio brindado por libvirt.
- **virt-install.** Herramienta en línea de comandos para crear máquinas virtuales.
- **virt-viwer.** Consola gráfica

A través del virt-manager podemos realizar la creación de las máquinas virtuales, también administrar las mismas bajo un entorno gráfico.

4.2.2. Instalación de máquinas virtuales

Utilizando el virt-manager, procedemos a crear e instalar las máquinas virtuales, para correr esta herramienta, debemos ejecutar el siguiente comando: (Ver Figura 12).

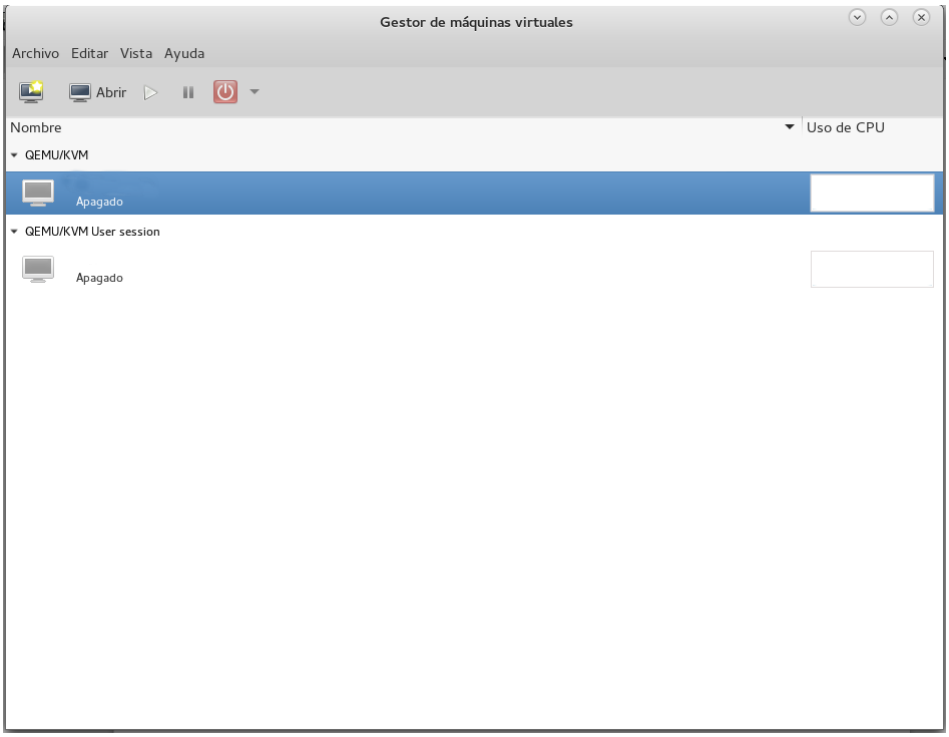

Figura 12: Captura de pantalla del gestor de máquinas virtuales.

```
[root@pruebas~]# virt-manager
```

Una vez cargada la herramienta, procedemos a dar clic en “nueva máquina”.

En la primera etapa debemos indicar el medio que utilizaremos para instalar el sistema operativo de la máquina virtual, en nuestro caso usaremos la primera opción “Medio de instalación local (imagen ISO ó CDROM)”. Previamente hemos descargado las diferentes imágenes ISO de las distribuciones a usar; los enlaces donde encontramos las imágenes de los instaladores son: (Ver Figura 13).

- **CentOS:** http://mirror.cedia.org.ec/centos/7.1.1503/isos/x86_64/
- **ArchiLinux:** http://mirror.cedia.org.ec/archlinux/iso/2015.06.01/
- **Ubuntu Server:** http://www.ubuntu.com/download/server
- **Open SUSE:** http://mirror.cedia.org.ec/opensuse/distribution/13.2/iso/
- **Debian:** http://mirror.cedia.org.ec/debian-cd/8.1.0/
- **Mageia:** https://www.mageia.org/en/downloads/

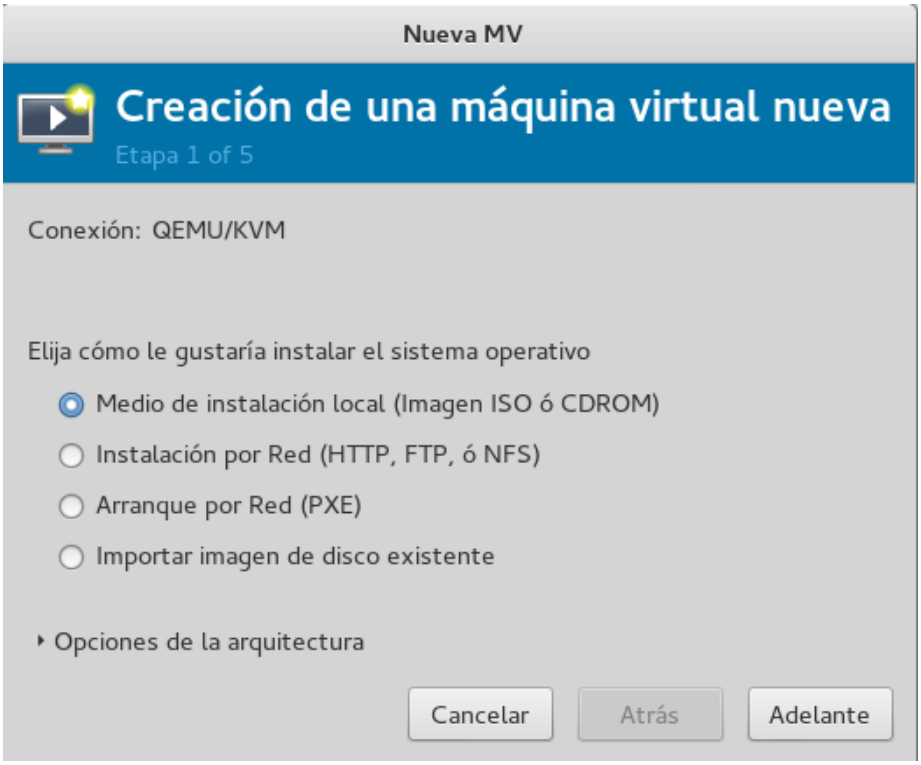

Figura 13: Captura de pantalla de la Etapa 1 para la creación de una máquina virtual.

En los casos de CentOS, ArchLinux, Open SUSE y Debian, se hace referencia al repositorio montado por el Consorcio Ecuatoriano para el Desarrollo del Internet Avanzado (CEDIA).

Para continuar con la instalación, debemos dar clic en el botón “Adelante”.

En la segunda etapa elegimos la opción “Utilizar imagen ISO”, luego examinamos la imagen ISO grabada en el disco local, la misma que se utilizará para el comienzo del proceso de instalación. Damos clic en el botón “Adelante” para entrar a la siguiente etapa. (Ver Figura 14)

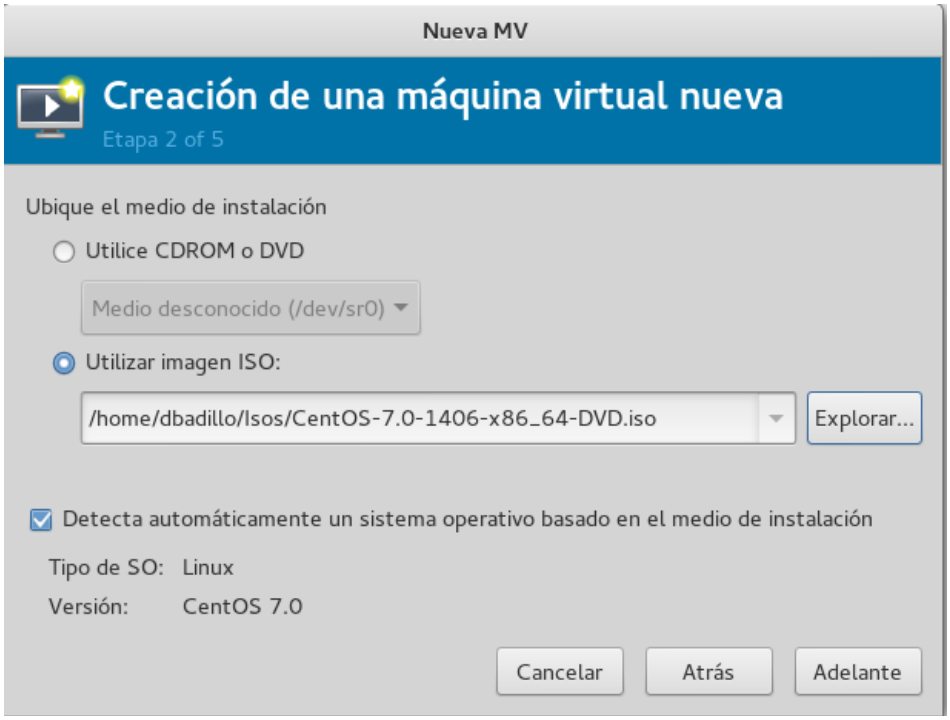

Figura 14: Captura de pantalla de la Etapa 2 para la creación de una máquina virtual.

En la tercera etapa debemos indicar la cantidad de memoria RAM que le asignaremos a la máquina virtual, también el número de procesadores (en el caso que tenga más de uno el equipo).Dependiendo el tipo de sistema operativo a instalar en la máquina virtual, se debe asignar la cantidad de memoria RAM, para ello debemos consultar en los requerimientos mínimos entregados por el desarrollador de la distribución. Damos clic en el botón “Adelante” para entrar a la siguiente etapa. (Ver Figura 15).

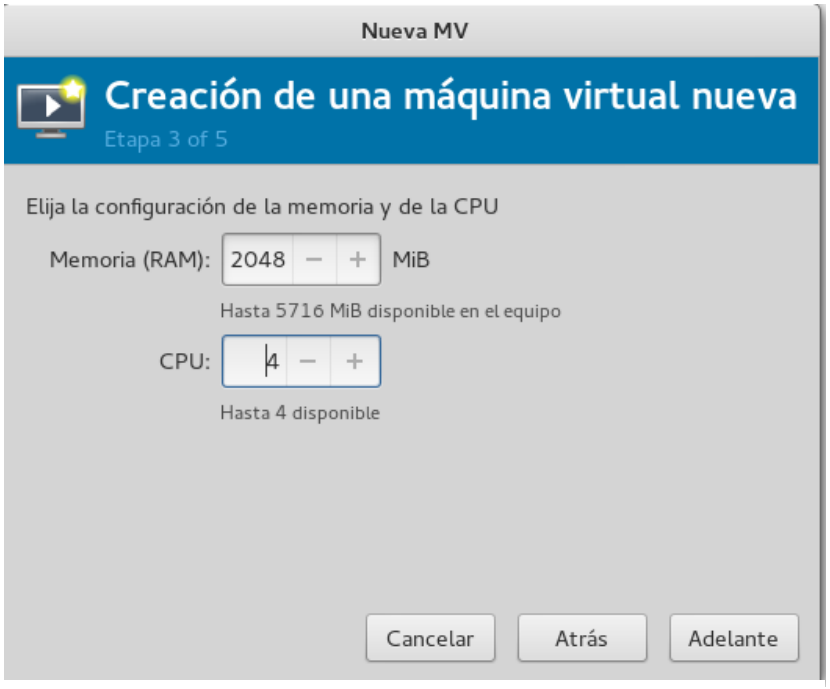

Figura 15: Captura de pantalla etapa3, Asignación memoria RAM y CPU

En la cuarta etapa seleccionamos la unidad de almacenamiento a usar para la máquina virtual. Escogeremos la opción *"Elija administrarlo, o algún otro tipo de almacenamiento existente"*, le damos clic en el botón "Explorar". (Ver Figura 16).

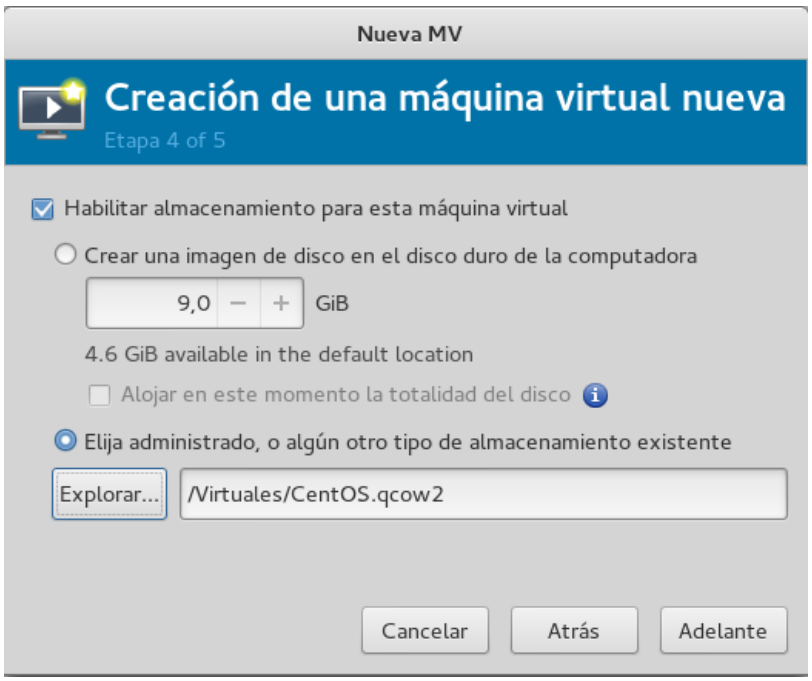

Figura 16: Captura de pantalla etapa 4, Elección almacenamiento

En esta pantalla nos muestra los volúmenes de almacenamiento disponibles, al lado derecho se encuentra la opción ”Virtuales”, la cual representa al directorio donde se guardan los discos. (Ver Figura 17).

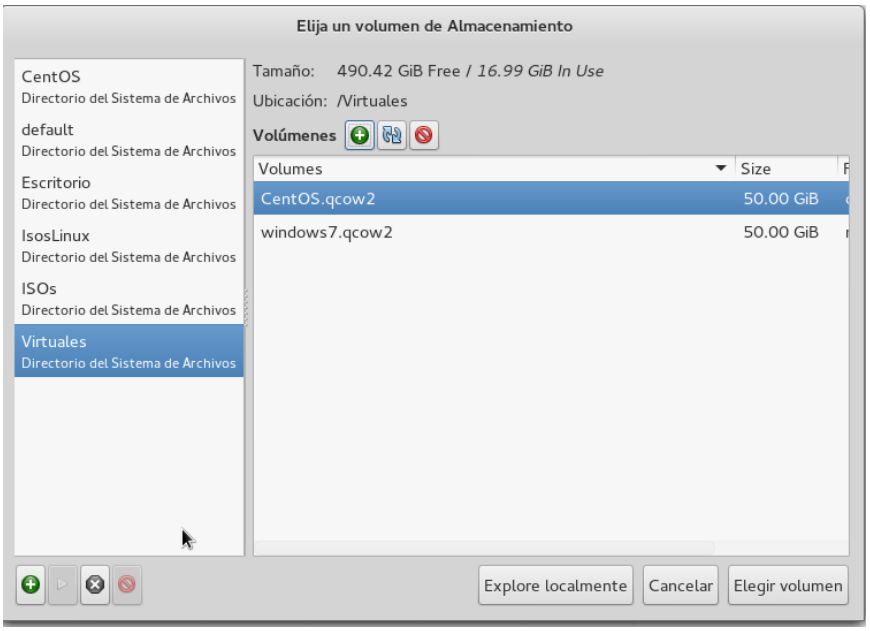

Figura 17: Captura de pantalla, volumen de almacenamiento

Le damos clic en el botón con el signo de más (+) y pasaremos a la pantalla para crear un nuevo volumen de almacenamiento. (Ver Figura 18).

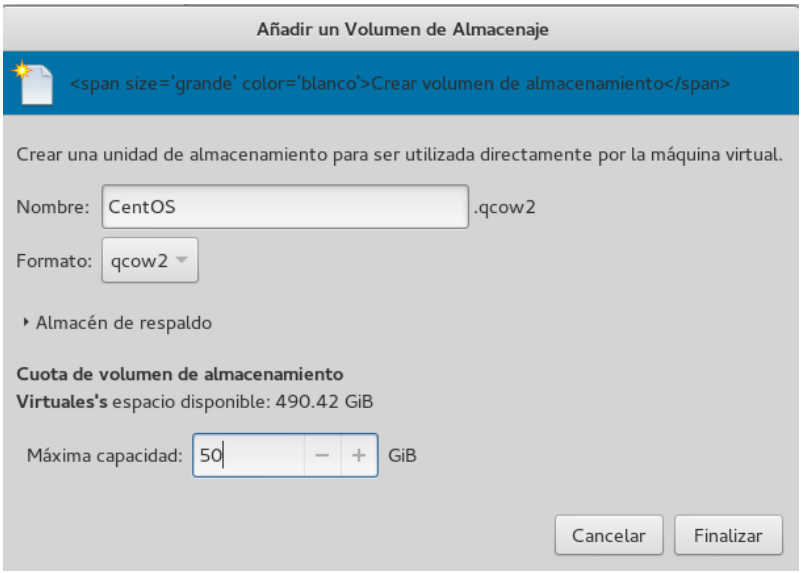

Figura 18: Captura de pantalla, Añadir un volumen de almacenamiento

Debemos determinar el nombre de disco virtual, en formato seleccionamos la extensión qcow2[44]. Hay que tomar en cuenta que podemos elegir diferentes tipos de volúmenes, sin embargo es recomendable utilizar el tipo de disco qcow2 propio de KVM. Asignamos la capacidad del disco virtual, en nuestro caso 50GB por cada máquina creada. Finalmente presionamos el botón “Finalizar”.

En la quinta etapa, se presenta un resumen de las características seleccionadas en las etapas anteriores, adicionalmente tenemos la opción de configurar la red, elegimos “Red virtual ‘default’: NAT”. Le damos clic en “Finalizar” lo que permite la creación de la máquina y el arranque del instalador Linux. (Ver Figura 19).

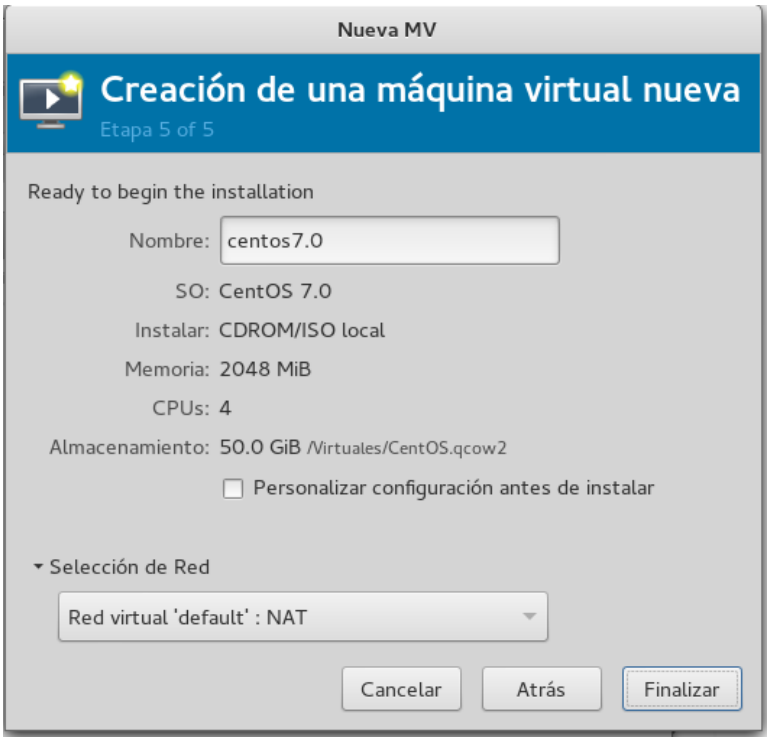

Figura 19: Captura de pantalla etapa 5, selección de red.

Una vez creada la máquina virtual se procede a cargar cada distribución. El detalle de la instalación realizada está documentado en el **Anexo C.**

Con los escenarios de prueba, procedemos a diseñar los parámetros a evaluar, posteriormente debemos definir si cada distribución cumple o no con cada uno de ellos.

---

44 **qcow2.** Es un formato de archivo que representa a imágenes de disco usados por QUEMU

4.3. Diseño de los parámetros de evaluación.

Para realizar el estudio comparativo, se requiere determinar los parámetros a evaluar de cada distribución. Para obtener los resultados de manera detallada se dividió en dos grupos de parámetros, estos son:

1. Parámetros generales
2. Parámetros de seguridad

Los parámetros generales se refieren a las características comunes que tienen las distribuciones Linux, por ejemplo la complejidad en la instalación, herramientas de configuración, etcétera.

Los parámetros de seguridad están orientados al objetivo de este estudio y con estos buscamos determinar la distribución Linux que brinde facilidades en la implementación de seguridades.

4.3.1. Diseño de parámetros generales para la comparación

Dentro de los parámetros generales para la evaluación de las distribuciones Linux tenemos:

Proceso de instalación amigable.

Es importante que la distribución Linux sea accesible para un gran número de usuarios, para ello el gestor de instalación debe tener una interfaz amigable y debe contener información de ayuda para facilitar la instalación.

Soporte técnico.

Al existir un gran número de distribuciones Linux con diferentes características, si una empresa opta por instalar a Linux, es importante que existan profesionales o empresas que se dediquen a dar soporte técnico especializado dentro de la ciudad/país. Se realiza una investigación por Internet, para conocer empresas que ofertan soporte técnico Linux.

Pueden existir empresas grandes que requieran soporte directo de la distribución, eso también tomaremos en cuenta dentro de este parámetro de evaluación.

Manejo de actualizaciones en línea.

Es importante que el sistema operativo se encuentre actualizado todo el tiempo, no solamente por obtener las últimas versiones de los paquetes de software, los cuales pueden presentar nuevas funcionalidades/mejoras normalmente las actualizaciones traen parches de seguridad. La mayoría de distros proporcionan actualizaciones mediante el uso de repositorios.

Opciones de entornos gráficos.

Si bien es cierto existen un gran número de usuarios Linux que administran al sistema mediante la línea de comando, también encontramos un gran número de usuarios que dependen de la interfaz gráfica. Es necesario conocer las opciones de entornos gráficos que ofertan las distribuciones Linux, para poder adaptarse a las necesidades gráficas de los usuarios.

Soporte de varias arquitecturas.

Las distribuciones Linux deben ser compatibles con diferentes arquitecturas de hardware, por ejemplo i386, x86_64, ia64, s390, s390x, ppc, sparc, entre otras.

Documentación.

Para facilidad de los usuarios, es importante que las distribuciones oferten documentación para el manejo del sistema, por ejemplo: manuales de instalación, usuario, guías para realizar configuraciones de servicios, manejo de herramientas, etcétera.

Soporte de varios idiomas.

Aunque el estudio está orientado al Ecuador, es importante que una distribución Linux tenga soporte en diferentes idiomas para ser más global y adaptarse a cualquier tipo de usuario. Aunque todas las distros vienen con soporte de inglés también deben tener soporte de Español.

Requerimientos de hardware.

Con la finalidad que se pueda instalar en un mayor número de computadores; las distros deben pensar en funcionar con equipos de cualquier característica y no solamente en máquinas construidas con tecnología de punta, con este parámetro queremos conocer que tan demandante de recursos son las distribuciones Linux.

Herramientas gráficas de configuración.

Normalmente las configuraciones se las puede hacer mediante la consola de comandos, editando archivos de texto plano. Para usuarios no muy experimentados puede ser de gran utilidad el uso de herramientas gráficas. Existen distribuciones que poseen poderosas herramientas de configuración, que facilitan enormemente esta tarea.

Sistemas de archivos soportados.

A diferencia de otros sistemas operativos, Linux tiene diferentes opciones para sistemas de archivos, es importante que las distros ofrezcan una variedad de sistemas para que el usuario decida según sus necesidades o preferencias.

Gestor de paquetes.

La administración de software es fundamental en cualquier sistema operativo, es básico que las distribuciones Linux cuenten con un gestor de paquetes, que permita disminuir los conflictos generados por librerías sueltas, diferencia de versiones, etcétera.

4.3.2. Diseño de parámetros de seguridad para la comparación

Dentro de los parámetros de seguridad para la evaluación de las distribuciones Linux tenemos:

Opciones de cortafuegos (Firewall).

Para la seguridad de un equipo es fundamental contar con unos cortafuegos; existen distribuciones Linux que ofrecen algunas opciones de firewalls para ser instalados.

Opciones de antivirus.

Aunque en Linux es poco frecuente la presencia de virus, es importante que las distros cuenten con un antivirus y así aumentar el nivel de seguridad del sistema operativo.

Soporte de SELinux.

SELinux es una arquitectura de seguridad integrada al kernel, usando módulos de seguridad que controlan diferentes elementos del sistema. Es importante para la seguridad que las distribuciones tengan soporte de SELinux.

Soporte de herramienta para evaluar vulnerabilidades.

Evaluar las vulnerabilidades que tiene un equipo servidor, es fundamental para valorar los peligros y tomar acciones correctivas. Existen algunas herramientas como Nessus, OpenVAS, Retina CS, entre otras. Con este parámetro evaluaremos si la distribución soporta de manera nativa alguna de estas herramientas.

Soporte de herramienta IDS/IPS.

Tener instalado un sistema para detección de intrusiones puede ayudar a descubrir intentos de vulnerar a nuestro equipo, es importante que dentro de las herramientas en software libre para este fin, tengan instaladores para las distribuciones en estudio.

No basta con detectar si un equipo fue vulnerado o no, podemos utilizar herramientas para prevenir que ingresen a nuestro equipo de manera ilegal mediante el uso de reglas.

Soporte de herramienta para determinar y forzar contraseñas débiles.

Un gran número de problemas de seguridad se originan cuando los usuarios determinan claves de seguridad débiles, es importante contar con una herramienta que busque contraseñas poco seguras y así obligar a los usuarios a cambiarla por una robusta.

Algunas distribuciones bloquean el uso de contraseñas débiles, esto ayuda a la seguridad de los equipos, por esta razón evaluaremos esta característica.

Tiempo de soporte.

El tiempo de soporte es una característica fundamental para este estudio, es importante conocer cuántos años la distro está comprometida en publicar actualizaciones de seguridad en los paquetes instalados. Mientras más tiempo de soporte, tendremos más seguridad para apostar a un proyecto a largo plazo.

Soporte para cifrado de las particiones del disco duro.

La protección de los datos es fundamental dentro de un servidor, es importante que las distribuciones tengan soporte para cifrar las particiones mediante el uso de una contraseña de paso. No es necesario cifrar todas las particiones, por ejemplo: /boot o /usr; pero si las que contienen datos delicados como: /home o /var.

Soporte para herramientas de monitoreo de recursos.

Tener herramientas de monitoreo de recursos y consumo de red, pueden ayudar a detectar problemas y realizar correcciones a tiempo. Si bien es cierto existen herramientas por

consola, las gráficas son de gran ayuda, gracias a la presentación de datos e imágenes estadísticas. También mediante el uso de estos utilitarios podemos detectar intrusiones o software malicioso, los que consumen recursos del sistema.

4.4. Evaluación de las distribuciones Linux

Una vez determinados los parámetros de evaluación, procedemos a documentar los resultados obtenidos de las pruebas e investigación, para determinar si las distribuciones cumplen o no con las características y a qué nivel.

La metodología de calificación que usaremos, está basada en asignar una nota sobre diez puntos por cada parámetro de evaluación. La distro que más cumple con el parámetro tendrá la calificación de 10 y en base a esta nota se irán evaluando al resto de distribuciones.

4.4.1. Evaluación de parámetros generales.

Es importante conocer el cumplimiento de los parámetros generales de las distribuciones para determinar similitudes. Estos parámetros no serán determinantes para la evaluación de seguridad, sin embargo brindarán información valiosa.

4.4.1.1. Evaluación - proceso de instalación amigable.

Como lo especificamos en el **Anexo C**, la distribución más simple de instalar es Mageia, gráficamente es muy amigable e intuitivo.

ArchLinux es la distribución más compleja para instalar, el proceso está basado en texto y se requiere de conocimientos intermedios sobre Linux.

Debemos señalar que las distribuciones evaluadas a excepción de ArchLinux, cuentan con sistemas de instalación intuitivos, algunos de ellos permiten mayor personalización, para esto se requiere conocimientos de Linux.

Proceso de instalación amigable (G1)		
Distribución	**Calificación**	**Observaciones**
CentOS	9/10	Se requiere conocimientos básicos para la instalación
ArchLinux	5/10	Se requiere conocimientos intermedios para la instalación
Ubuntu Server	9/10	Se requiere conocimientos básicos para la instalación
Open SUSE	8/10	Se requiere conocimientos básicos para la instalación
Debian	7/10	Se requiere conocimientos básicos para la instalación
Mageia	10/10	Se requiere conocimientos básicos para la instalación

Tabla 4: Evaluación general - Proceso de instalación amigable.

4.4.1.2. Evaluación – soporte técnico.

Se investigó en algunas empresas nacionales sobre el soporte a Linux, prácticamente todas brindan servicios para CentOS, en menor escala Ubuntu y Debian. Para el resto de distribuciones no se tiene una oferta específica.

A nivel internacional existen empresas que brindan soporte técnico para todas las distribuciones, sin embargo en Latinoamérica es un mercado no explotado.

Soporte técnico (G2)		
Distribución	**Calificación**	**Observaciones**
CentOS	10/10	Existen varias empresas locales de soporte para esta distribución.
ArchLinux	6/10	Casi nulo el soporte local.
Ubuntu Server	8/10	La mayoría de soporte local es para la versión Desktop, no Server.
Open SUSE	7/10	Existen pocas empresas con soporte local

Debian	7/10	Existen pocas empresas con soporte local.
Mageia	4/10	No encontramos empresas que den soporte local

Tabla 5: Evaluación general - Soporte técnico.

4.4.1.3. Evaluación – manejo de actualizaciones en línea.

Los sistemas operativos modernos brindan el servicio de actualizaciones mediante el Internet, es importante que la distribución permita una actualización semiautomática para tener siempre al sistema actualizado. Después de la evaluación se determinó que todas las distribuciones cuentan con un sistema de actualizaciones en línea, mediante el uso de repositorios.

Manejo de actualizaciones en línea (G3)		
Distribución	**Calificación**	**Observaciones**
CentOS	10/10	Usa repositorios en línea
ArchLinux	10/10	Usa repositorios en línea
Ubuntu Server	10/10	Usa repositorios en línea
Open SUSE	10/10	Usa repositorios en línea
Debian	10/10	Usa repositorios en línea
Mageia	10/10	Usa repositorios en línea

Tabla 6: Evaluación general - Manejo de actualizaciones en línea.

4.4.1.4. Evaluación – opciones de entornos gráficos.

Los administradores avanzados suelen prescindir del entorno gráfico, sin embargo varios usuarios lo requieren. De las distribuciones analizadas Debian y Mageia cuentan con soporte a un sin número de escritorios remotos, se los puede cargar al momento de la instalación.

Ubuntu cuenta con su propio escritorio y aunque se puede instalar algún otro entorno, este no tiene la opción directa para hacerlo.

Opciones de entornos gráficos (G4)		
Distribución	**Calificación**	**Observaciones**
CentOS	6/10	Soporta GNOME, KDE
ArchLinux	7/10	Soporta Cinnamon, GNOME, KDE, LXDE
Ubuntu Server	3/10	Soporta Unity
Open SUSE	9/10	Soporta Blackbox, GNOME, KDE, LXDE, Openbox
Debian	10/10	Soporta GNOME, KDE, LXDE, MATE, Openbox, Cinnamon
Mageia	10/10	Soporta Cinnamon, GNOME, KDE, LXDE, Openbox

Tabla 7: Evaluación general - Opciones de entornos gráficos.

4.4.1.5. Evaluación – soporte varias arquitecturas.

Luego de analizar a las distribuciones nos encontramos que Debian soporta una gran cantidad de arquitecturas de hardware, el resto de distribuciones fundamentalmente cuentan con las arquitecturas más utilizadas, estas son: i386 y x86_64.

Soporte de varias arquitecturas (G5)		
Distribución	**Calificación**	**Observaciones**
CentOS	7/10	Soporta i386, x86_64
ArchLinux	6/10	Soporta arm, i686, x86_64
Ubuntu Server	7/10	Soporta i686, x86_64, armhf, powerpc
Open SUSE	5/10	Soporta i586, x86_64
Debian	10/10	Soporta i386, x86_64, arm64, s390x, mips, mipsel,armhf

Mageia	5/10	Soporta i586, x86_64

Tabla 8: Evaluación general - Soporte de varias arquitecturas.

4.4.1.6. Evaluación – documentación.

Se realizó la investigación de documentación oficial ofertados por cada distribución, también algunos sitios no oficiales que brindan escritos de varias distribuciones.

Para Debian y CentOS existe gran cantidad de información, referente a la instalación del sistema, configuración de servicios, foros de ayuda para problemas, etcétera.

Aparte del sitio oficial ArchLinux no cuenta con documentación, sin embargo debemos señalar que los escritos brindados por esta distribución, están muy bien elaborados.

Documentación (G6)		
Distribución	**Calificación**	**Observaciones**
CentOS	10/10	Tiene documentación en línea https://wiki.centos.org/es
ArchLinux	7/10	Tiene documentación en línea https://wiki.archlinux.org
Ubuntu Server	8/10	Tiene documentación en línea https://help.ubuntu.com/
Open SUSE	9/10	Tiene documentación en línea https://es.opensuse.org/
Debian	10/10	Tiene documentación en línea https://www.debian.org/doc/
Mageia	9/10	Tiene documentación en línea https://wiki.mageia.org

Tabla 9: Evaluación general - Documentación.

4.4.1.7. Evaluación – soporte varios idiomas.

La mayoría de las distribuciones evaluadas, a excepción de ArchLinux, soportan un sin número de idiomas. En nuestro caso particular, se requiere que soporte al menos inglés y español.

Soporte de varios idiomas (G7)		
Distribución	**Calificación**	**Observaciones**
CentOS	10/10	Soporte varios idiomas incluido inglés y español
ArchLinux	5/10	No tiene soporte de varios idiomas
Ubuntu Server	10/10	Soporte varios idiomas incluido inglés y español
Open SUSE	10/10	Soporte varios idiomas incluido inglés y español
Debian	10/10	Soporte varios idiomas incluido inglés y español
Mageia	10/10	Soporte varios idiomas incluido inglés y español

Tabla 10: Evaluación general - Soporte de varios idiomas

4.4.1.8. Evaluación – requerimientos de hardware.

Linux es un sistema operativo caracterizado por el bajo consumo de recursos, sin embargo existen distribuciones que priorizan el entorno gráfico como Mageia, esto puede ocasionar mayor consumo de hardware. Las distribuciones que no requieren de mayor equipamiento son: CentOS, ArchLinux y Debian.

Las distribuciones que consumen más recursos son: Ubuntu y Mageia. Esto se debe a los entornos gráficos utilizados.

Requerimientos de hardware (G8)		
Distribución	**Calificación**	**Observaciones**
CentOS	10/10	Es muy poco consumidor de recursos
ArchLinux	10/10	Es muy poco consumidor de recursos
Ubuntu Server	6/10	Consume recursos por su entorno gráfico Unity
Open SUSE	8/10	Consume recursos por su herramienta gráfica de configuración
Debian	10/10	Es poco consumidor de recursos

Mageia	8/10	Por su llamativa interfaz gráfica, consume recursos.

Tabla 11: Evaluación general - Requerimientos de hardware.

4.4.1.9. Evaluación – herramientas gráficas de configuración.

Para usuarios principiantes e intermedios, es muy útil la utilización de herramientas gráficas de configuración. Open SUSE brinda una excelente herramienta llamada YAST, la cual es intuitiva y fácil de utilizar. El resto de distribuciones provee algunas herramientas genéricas o propias.

Herramientas gráficas de configuración (G9)		
Distribución	**Calificación**	**Observaciones**
CentOS	8/10	Utiliza varias herramientas de configuración con system-config
ArchLinux	5/10	No cuenta con una herramienta gráfica de configuración
Ubuntu Server	8/10	Utiliza varias herramientas de configuración
Open SUSE	10/10	Utiliza YAST un sistema completo de administración
Debian	7/10	Utiliza varias herramientas de configuración
Mageia	9/10	Utiliza varias herramientas gráficas de calidad

Tabla 12: Evaluación general - Herramientas gráficas de configuración.

4.4.1.9. Evaluación – sistema de archivos soportados.

Dentro de un servidor Linux se puede utilizar diferentes sistemas de archivos dependiendo las necesidades específicas. Todas las distribuciones cuentan con el soporte a varios sistemas de archivos; CentOS en este aspecto, ofrece soporte de los sistemas de archivos más conocidos y utilizados en entornos Linux.

Sistemas de archivos soportados (G10)		
Distribución	**Calificación**	**Observaciones**
CentOS	9/10	Soporta ext4, XFS,VFAT
ArchLinux	10/10	Soporta ext4, JFS, ReiserFS, XFS, Btrfs
Ubuntu Server	10/10	Soporta ext4, JFS, ReiserFS, XFS, Btrfs
Open SUSE	10/10	Soporta ext4, JFS, ReiserFS, XFS, Btrfs
Debian	10/10	Soporta ext4, JFS, ReiserFS, XFS, Btrfs
Mageia	10/10	Soporta ext4, JFS, ReiserFS, XFS, Btrfs

Tabla 13: Evaluación general - sistemas de archivos soportados.

4.4.1.9. Evaluación – gestor de paquetes.

Todas las distribuciones evaluadas cuentan con un gestor de paquetes adecuado. Esto permite garantizar la instalación y administración de software.

Gestor de paquetes (G11)		
Distribución	**Calificación**	**Observaciones**
CentOS	10/10	Soporta RPM
ArchLinux	10/10	Soporta Pacman
Ubuntu Server	10/10	Soporta DEB
Open SUSE	10/10	Soporta RPM
Debian	10/10	Soporta DEB
Mageia	10/10	Soporta RPM

Tabla 14: Evaluación general - Gestor de paquetes.

4.4.2 Evaluación de parámetros de seguridad.

Los parámetros evaluados a continuación permitirán conocer a la distribución que cuente con las mayores prestaciones de seguridad.

Debemos señalar que muchos de los parámetros se cumplen por parte de todas las distro, en este aspecto se evaluará el nivel de complejidad de las herramientas, complejidad de implementación, problemas reportados, etcétera.

4.4.2.1. Evaluación – opciones de cortafuegos (firewall).

Todas las distros traen un firewall por defecto, sin embargo en mucho de los casos estos son difíciles de configurar o no permiten crear reglas personalizadas. La mayoría de distribuciones, permiten la instalación de varios cortafuegos desarrollados por terceros, estos son muy eficientes al momento de asegurar un servidor.

Opciones de cortafuegos (Firewall) (S1)

Distribución	Calificación	Observaciones
CentOS	10/10	Shortwall, RC-Firewall,APF,CFS, UFW, Iptables service y más...
ArchLinux	10/10	Arno's firewall, Ferm, Firehol, Firetable, Shorwall, UFW, y más...
Ubuntu Server	10/10	Shortwall, Firestarter,Fwbuilder,Arno-iptables-firewall, y más...
Open SUSE	8/10	SuSeFirewall2, apf, CFS, Shortwall
Debian	10/10	Shortwall, Firestarter,Fwbuilder,Arno-iptables-firewall, y más...
Mageia	7/10	Drakfirewall, Shortwall, APF.

Tabla 15: Evaluación de seguridad - Opciones de cortafuegos (Firewall)

4.4.2.2. Evaluación – opciones de antivirus.

Por diferentes motivos es poco frecuente que un equipo Linux sea infectado por un virus, sin embargo se recomienda la instalación de un antivirus para proteger a nuestro equipo. Debian, Ubuntu y CentOS; ofrecen varias opciones de anti virus, las otras distribuciones no tienen mayor flexibilidad en este parámetro.

Opciones de antivirus (S2)

Distribución	Calificación	Observaciones
CentOS	10/10	ClamAV, Comodo, Avast,Clamtk
ArchLinux	6/10	ClamAV, Comodo
Ubuntu Server	10/10	ClamAV, Comodo, Avast,Clamtk
Open SUSE	8/10	ClamAV, Comodo, Avast
Debian	10/10	ClamAV, Comodo, Avast,Clamtk
Mageia	5/10	ClamAV

Tabla 16: Evaluación de seguridad - Opciones de antivirus

4.4.2.3. Evaluación – SELinux.

La mayoría de distribuciones soportan a SELinux. Debemos recalcar que ArchLinux, Ubuntu, Open SUSE y Debian, soportan también AppArmor, este cumple las mismas funciones que SELinux. CentOS soporta nativamente no soporta AppArmor..

Soporte de SELinux (S3)

Distribución	Calificación	Observaciones
CentOS	8/10	Si lo soporta
ArchLinux	10/10	Si lo soporta y AppArmor

Ubuntu Server	10/10	Si lo soporta y AppArmor
Open SUSE	10/10	Si lo soporta y AppArmor
Debian	10/10	Si lo soporta y AppArmor
Mageia	3/10	No lo trae por defecto

Tabla 17: Evaluación de seguridad - Soporte de SELinux

4.4.2.4. Evaluación – soporte de herramientas para evaluar vulnerabilidades.

Las principales herramientas para evaluar vulnerabilidades como: Nessus, OpenVAS, NeXpose, etcétera; brindar instaladores para CentOS, Ubuntu y Debian. En el resto de distribuciones se los puede instalar, pero se requiere de conocimientos Linux intermedios o avanzados.

Soporte de herramienta para evaluar vulnerabilidades (S4)

Distribución	Calificación	Observaciones
CentOS	10/10	Nessus, OpenVAS, NeXpose
ArchLinux	0/10	No se encontró soporte directo
Ubuntu Server	10/10	Nessus, OpenVAS, NeXpose
Open SUSE	7/10	Nessus, NeXpose
Debian	10/10	Nessus, OpenVAS, NeXpose
Mageia	0/10	No se encontró soporte directo

Tabla 18: Evaluación de seguridad - Soporte de herramientas para evaluar vulnerabilidades.

4.4.2.5. Evaluación – soporte de herramientas IDS/IPS.

Existen dos sistemas IDS/IPS para Linux, estos son: snort y suricata. El primero brinda soporte directo a CentOS, para el resto entrega el código fuente. El segundo entrega el código fuente y se debe efectuar una instalación a mano en todas las distribuciones.

Soporte de herramienta IDS/IPS (S5)

Distribución	Calificación	Observaciones
CentOS	10/10	Snort
ArchLinux	5/10	Sin soporte directo de Snort
Ubuntu Server	5/10	Sin soporte directo de Snort
Open SUSE	5/10	Sin soporte directo de Snort
Debian	5/10	Sin soporte directo de Snort
Mageia	5/10	Sin soporte directo de Snort

Tabla 19: Evaluación de seguridad - Soporte de herramienta IDS/IPS

4.4.2.6. Evaluación – soporte de herramientas para determinar y forzar contraseñas débiles.

A excepción de Mageia, todas cuentan con un programa para forzar contraseñas débiles. Se debe señalar que la mayoría de las distribuciones, cuentan con un sistema para evaluar la complejidad de las contraseñas.

Soporte herramienta para determinar y forzar contraseñas débiles (S6)

Distribución	Calificación	Observaciones
CentOS	10/10	John the Ripper
ArchLinux	10/10	John the Ripper
Ubuntu Server	10/10	John the Ripper

Open SUSE	10/10	John the Ripper
Debian	10/10	John the Ripper
Mageia	0/10	No se encontró ninguna herramienta

Tabla 20: Evaluación de seguridad - Soporte herramienta para determinar y forzar contraseñas débiles

4.4.2.7. Evaluación – tiempo de soporte.

CentOS es la distribución que brinda mayor tiempo de soporte, esto garantiza poder establecer proyectos de software a largo plazo, sin depender de cambios en el sistema base. El resto de distribuciones cuentan con soporte hasta de 5 años, los cambios son frecuentas, lo que ocasiona mayor probabilidad de fallo en el software.

Tiempo de soporte (S7)

Distribución	Calificación	Observaciones
CentOS	10/10	10 años
ArchLinux	1/10	No determinado, cambios frecuentes
Ubuntu Server	5/10	5 años en su versión LTS
Open SUSE	2/10	2 años, no define el ciclo de vida de las últimas versiones
Debian	5/10	4 años aproximadamente
Mageia	1.5/10	1 año y medio

Tabla 21: Evaluación de seguridad - Tiempo de soporte

4.4.2.8. Evaluación – soporte para cifrado de las particiones del disco duro

Todas las distribuciones evaluadas, cuenta con soporte para cifrar las particiones de disco duro, por ende todas obtienen la mayor calificación en este parámetro-

Soporte para cifrado de las particiones del disco duro (S8)		
Distribución	**Calificación**	**Observaciones**
CentOS	10/10	Si soporta
ArchLinux	10/10	Si soporta
Ubuntu Server	10/10	Si soporta
Open SUSE	10/10	Si soporta
Debian	10/10	Si soporta
Mageia	10/10	Si soporta

Tabla 22: Evaluación de seguridad - Soporte para cifrado de las particiones del disco duro

4.4.2.9. Evaluación – soporte para herramientas de monitoreo de recursos.

Todas las distribuciones evaluadas cuentan con soporte para instalar Munin, la mayoría de distros se puede instalar a Cacti.

Soporte para herramientas de monitoreo de recursos (S9)		
Distribución	**Calificación**	**Observaciones**
CentOS	10/10	Munin, Cacti
ArchLinux	10/10	Munin, Cacti
Ubuntu Server	10/10	Munin, Cacti
Open SUSE	10/10	Munin, Cacti
Debian	10/10	Munin, Cacti
Mageia	5/10	Munin,

Tabla 23: Evaluación de seguridad - Soporte para herramientas de monitoreo de recursos

4.4. Presentación de resultados

Una vez evaluadas a las distribuciones con los parámetros generales y de seguridad, presentaremos dos matrices con los puntos totales alcanzados por cada distro, para ello debemos asignar un peso a cada parámetro, el cual será multiplicado por la calificación sobre 10.

Se determinará la distribución que cumple de mejor manera con los parámetros generales y la distribución que cumple de la mejor manera con los parámetros de seguridad. Al final se analizará las matrices para especificar que distribución brinda mayores prestaciones de seguridad.

4.4.1. Resultados según parámetros generales

Para mejor manejo de la matriz vamos asignar un código a cada parámetro, también asignaremos un peso según la importancia de cada característica. Se analizó según el nivel de importancia cada uno de los parámetros.

Parámetro	Código	Peso
Proceso de instalación amigable.	G1	9
Soporte técnico.	G2	10
Manejo de actualizaciones en línea.	G3	8
Opciones de entornos gráficos.	G4	8
Soporte de varias arquitecturas.	G5	8
Documentación.	G6	12
Soporte de varios idiomas.	G7	8
Requerimientos de hardware.	G8	9
Herramientas gráficas de configuración.	G9	11
Sistemas de archivos soportados.	G10	8
Gestor de paquetes.	G11	9

TOTAL	100

Tabla 24: Determinación de pesos para parámetros generales

Una vez que tenemos la codificación de los parámetros y la determinación de los pesos respectivos, procedemos a elaborar la matriz con los resultados finales.

Código	Peso	CentOS		Arch Linux		Ubuntu Server		Open SUSE		Debian		Mageia	
		C	T	C	T	C	T	C	T	C	T	C	T
G1	9	9	81	5	45	9	81	8	72	7	63	10	90
G2	10	10	100	6	60	8	80	7	70	7	70	4	40
G3	8	10	80	10	80	10	80	10	80	10	80	10	80
G4	8	6	48	7	56	3	24	9	72	10	80	10	80
G5	8	7	56	6	48	7	56	5	40	10	80	5	40
G6	12	10	120	7	84	8	96	9	108	10	120	9	108
G7	8	10	80	5	40	10	80	10	80	10	80	10	80
G8	9	10	90	10	90	6	54	8	72	10	90	8	72
G9	11	8	88	5	55	8	88	10	110	7	77	9	99
G10	8	9	72	10	80	10	80	10	80	10	80	10	80
G11	9	10	90	10	90	10	90	10	90	10	90	10	90
TOTALES			**905**		**728**		**809**		**874**		**910**		**859**

Tabla 25: Matriz resultados finales - Parámetros generales

C = Calificación, T = Total

Como podemos analizar en la matriz, existen dos distribuciones Linux que están por encima del resto con más de novecientos puntos sobre mil. Debian es la Distribución que mejor cumple con las características generales, seguido de CentOS/RedHat.

4.4.2. Resultados según parámetros de seguridad

Al igual que los parámetros generales debemos determinar un peso según la importancia y se le asignará un código para mejor manejo de la matriz.

Parámetro	Código	Peso
Opciones de cortafuegos (Firewall).	S1	9
Opciones de antivirus.	S2	9
Soporte de SELinux.	S3	9
Soporte de herramienta para evaluar vulnerabilidades.	S4	14
Soporte de herramienta IDS/IPS.	S5	14
Soporte herramienta para determinar y forzar contraseñas débiles.	S6	10
Tiempo de soporte.	S7	14
Soporte para cifrado de las particiones del disco duro.	S8	10
Soporte para herramientas de monitoreo de recursos.	S9	11
TOTAL		**100**

Tabla 26: Determinación de pesos para parámetros de seguridad

Luego de la determinación de los pesos y códigos, elaboramos la matriz para calcular los puntos totales por cada distribución.

Código	Peso	CentOS		ArchLinux		Ubuntu Server		Open SUSE		Debian		Mageia	
		C	T	C	T	C	T	C	T	C	T	C	T
S1	9	10	90	10	90	10	90	8	72	10	90	7	63
S2	9	10	90	6	54	10	90	8	72	10	90	5	45
S3	9	8	72	10	90	10	90	10	90	10	90	3	27
S4	14	10	140	0	0	10	140	70	98	10	140	0	0
S5	14	10	140	5	70	5	70	5	70	5	70	5	70

S6	10	10	100	10	100	10	100	10	100	10	100	0	0
S7	14	10	140	1	14	5	70	2	28	5	70	1.5	21
S8	10	10	100	10	100	10	100	10	100	10	100	10	100
S9	11	10	110	10	110	10	110	10	110	10	110	5	55
TOTALES			**982**		**628**		**860**		**740**		**860**		**381**

Tabla 27: Matriz resultados finales - Parámetros de seguridad

C = Calificación, T = Total

Analizando la matriz, la distribución que brinda mayores características de seguridad es CentOS con novecientos ochenta y dos puntos sobre mil.

Con estos resultados no podemos asegurar que las otras distribuciones son inseguras, pues en su mayoría cuentan con las herramientas necesarias para poder blindar correctamente a un servidor, sin embargo, puede ser que se requiera más esfuerzo o conocimiento del sistema para hacerlo.

Una vez que hemos determinado que CentOS es la distribución que mayores prestaciones de seguridad nos brinda; como aporte para este estudio elaboramos los siguientes documentos guías:

- Instalación de CentOS 7 **(Anexo D**)
- Aseguramiento de Linux CentOS 7 **(Anexo E**)

CAPÍTULO 5: Conclusiones y Recomendaciones

5.1. Conclusiones

Al finalizar la investigación, podemos llegar a las siguientes conclusiones:

- Del análisis de varios sitios Web ecuatorianos (Referencia Tabla 2), se evidencia que en su mayoría están bajo el sistema operativo Linux, sin embargo, muchos de ellos han sido vulnerados de alguna manera.
- Luego de analizar las estadísticas (Referencia Figura 1), se colige una mala instalación y configuración de Linux, lo cual genera problemas de seguridad; por lo que se requiere aplicar varios criterios para endurecer al sistema operativo.
- Mediante el uso de estadísticas en línea (Referencia Tabla 1), se determina las distribuciones Linux más utilizadas a nivel mundial y local; esta información sirvió de base para realizar el estudio comparativo. La mayoría de las distribuciones analizadas están orientadas a usuarios finales, dejando a un lado el criterio general de que Linux solamente es utilizado para equipos servidores.
- Podemos demostrar que Linux tiene varios programas que ayudan a blindar la red o un servidor, que en su mayoría son de código abierto. Por ejemplo: Snort, OpenVAS, Nessus, NeXpose, AIDE, SELinux, AppArmor, Clamav, Bastille, entre otros.
- Determinamos a CentOS como la distribución que se ajusta de mejor manera con las características de seguridad para implementar servicios de red. Debemos recalcar que Debian, Open SUSE y Ubuntu Server también son opciones válidas. Lo que no ocurre con: Fedora, Mint, Mageia, Manjaro, Arch Linux y Zorin.
- Como resultado de la investigación y bajo los criterios expuestos, se elaboraron documentos-guía para la instalación de CentOS 7 (Anexo D) y otro para endurecer al sistema Linux base (Anexo E). Los conceptos detallados en estos documentos están justificados con la información producto de éste estudio y por la experiencia profesional.

- Los conocimientos adquiridos en la Maestría, en el Seminario de Seguridad, dictado por el Ing. Francisco Rodríguez; fueron base fundamental para realizar este estudio.
- La presente investigación está orientada para todos los profesionales o público en general, que deseen utilizar a Linux como servidor. Mediante las guías de instalación y aseguramiento, brindando algunas directrices para implementar a Linux, como sistema operativo base para ofrecer servicios de red.

5.2. Recomendaciones

- Luego del análisis de los problemas de seguridad que puede presentar un servidor Linux, se sugiere seguir las directrices presentadas en este trabajo mediante los documentos guía (Referencia Anexo D y E), para reducir la incidencia de vulnerabilidades.
- Se recomienda no usar para brindar servicios de red, a las distribuciones Linux que estén orientadas a equipos de escritorio u otros propósitos.
- Se sugiere implementar las herramientas de seguridad que brinda Linux como: Firewall, antivirus, escáner de vulnerabilidades e IDS/IPS.
- Este trabajo realiza una comparación de las distribuciones Linux, determinando las que son aptas para implementar servicios de red; recomendamos se analicen las consideraciones de seguridad específicas por cada servicio a ser instalado.
- A nivel de Gobierno se debe normar para que todas las instituciones utilicen una misma distribución Linux, con el objetivo de estandarizar los procesos informáticos comunes en las entidades del Estado.
- Es fundamental que los administradores de Linux tengan los conocimientos necesarios para asegurar al servidor. Se recomienda que se capaciten en temas de seguridad y se mantenga un estudio constante, sobre los riesgos que presenta un equipo que tiene instalado a Linux.
- Según el decreto presidencial 1014 del 10 de abril del 2008, las entidades del Estado deben utilizar sistemas bajo Software Libre. Se recomienda realizar un estudio comparativo de las distribuciones Linux orientadas a equipos de escritorio, para determinar qué sistema brinda las mejores características que se adapten a

nuestro medio. Es necesario se tomen en cuenta también los parámetros de seguridad.

- Linux permite en una distribución orientada a usuarios finales, montar servicios de red; esto puede servir para realizar pruebas o desarrollo de programas, sin embargo, no se recomienda bajo ningún concepto utilizar a estos sistemas para equipos de producción.

Bibliografía

AIDE. (18 de Septiembre de 2015). Obtenido de About AIDE: http://aide.sourceforge.net/

Alcance Libre. (03 de Mayo de 2015). Obtenido de Uso de Netstat: http://www.alcancelibre.org/staticpages/index.php/como-netstat

Cacti. (17 de Mayo de 2015). Obtenido de About Cacti: http://www.cacti.net/

CANAIMA. (06 de Noviembre de 2014). Obtenido de http://canaima.softwarelibre.gob.ve/

CCM. (03 de Mayo de 2015). Obtenido de Linux - Comandos para monitorear el sistema: http://es.ccm.net/faq/3435-linux-comandos-para-monitorear-el-sistema

Ciberaula. (02 de Noviembre de 2014). Obtenido de http://linux.ciberaula.com/articulo/que_es_linux/

Correa Delgado, R. (10 de Abril de 2008). Decreto 1014. *Decreto Ejecutivo 1014*, 1. Quito, Pichincha, Ecuador.

Desde Linux. (20 de Abril de 2015). Obtenido de Configurar SSH por otro puerto y no por el 22: http://blog.desdelinux.net/configurar-ssh-por-otro-puerto-y-no-por-el-22/

die.net. (03 de Mayo de 2015). Obtenido de pmap(1) - Linux man page: http://linux.die.net/man/1/pmap

DistroWatch. (06 de Abril de 2015). Obtenido de http://distrowatch.com/dwres.php?resource=popularity

DistroWatch. (19 de Agosto de 2015). Obtenido de Las más visitadas: http://distrowatch.com/

El Rincón de Linux. (05 de Noviembre de 2014). Obtenido de http://www.linux-es.org/distribuciones

El sistema operativo GNU. (05 de Noviembre de 2014). Obtenido de http://www.gnu.org/gnu/gnu-history.es.html

El sistema operativo GNU. (16 de Marzo de 2015). Obtenido de Definición de software libre: https://www.gnu.org/philosophy/free-sw.es.html

Geekland. (20 de Julio de 2015). Obtenido de Proteger el GRUB con contraseña: http://geekland.eu/proteger-el-grub-con-contrasena/

GlobalSign. (03 de Mayo de 2015). Obtenido de ¿Qué es SSL?: https://www.globalsign.es/centro-informacion-ssl/que-es-ssl.html

GNU. (15 de Febrero de 2015). Obtenido de Qué es GNU: https://www.gnu.org/home.es.html

hipertextual. (03 de Mayo de 2015). Obtenido de Comando Linux htop: administra interactivamente los procesos del sistema: http://hipertextual.com/archivo/2010/03/comando-linux-htop-administra-interactivamente-los-procesos-del-sistema/

HScripts.com. (15 de Mayo de 2015). Obtenido de Comandos Linux ps: https://www.hscripts.com/es/tutoriales/linux-commands/ps.html

HScripts.com. (03 de Mayo de 2015). Obtenido de Comandos Linux df: https://www.hscripts.com/es/tutoriales/linux-commands/df.html

Linux Hispano. (03 de Mayo de 2015). Obtenido de Monitorizar en tiempo real el tráfico de red. Instalar ifstat: http://www.linuxhispano.net/2011/12/16/monitorizar-en-tiempo-real-el-trafico-de-red-instalar-ifstat/

Linux Total. (20 de Abril de 2015). Obtenido de Asegurando SSH: http://www.linuxtotal.com.mx/index.php?cont=info_seyre_004

Linux y Software Libre en Colombia. (03 de Mayo de 2015). Obtenido de Comando w Linux: http://cosaslibres.com.co/ayuda-en-linux/man-comandos-linux/comando-w-linux/

Linux Zone. (10 de Octubre de 2015). Obtenido de Asegurar el sistema operativo con Bastille: http://linuxzone.es/asegurar-el-sistema-operativo-con-bastille/

Munin. (17 de Mayo de 2015). Obtenido de About Munin: http://munin-monitoring.org/

Nagios. (17 de Mayo de 2015). Obtenido de Nagios Core: https://www.nagios.org/projects/nagios-core/

NetCraft. (20 de Julio de 2015). Obtenido de NetCraft Site Report: http://toolbar.netcraft.com/site_report

Netfilter. (23 de Junio de 2015). Obtenido de What is netfilter: http://www.netfilter.org/

NexoLinux. (03 de Mayo de 2015). Obtenido de Comando lsof: http://www.nexolinux.com/comando-lsof-comprobar-ficheros-abiertos/

OpenVAS. (04 de Junio de 2015). Obtenido de About OpenVAS: http://www.openvas.org/about.html

Ovtoaster. (04 de Junio de 2015). Obtenido de ¿Qué son los repositorios en Linux?: http://ovtoaster.com/repositorios-linux/

Pérez Estévez, E. (18 de Abril de 2015). *CSIRT CEDIA*. Obtenido de Correcto Particionamiento: http://csirt.cedia.org.ec/how-to/instalacion/instalacion/correcto-particionamiento/

Rapid 7. (04 de Junio de 2015). Obtenido de Nexpose: Reduce your risk of a breach: http://www.rapid7.com/products/nexpose/

Red Hat. (20 de Abril de 2015). Obtenido de SELinux - Main Configuration File: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security-Enhanced_Linux/

Red Hat. (13 de Junio de 2015). Obtenido de Featured Products: https://www.redhat.com/wapps/store/catalog.html

rm-rf.es. (03 de Mayo de 2015). Obtenido de El comando Free: http://rm-rf.es/el-comando-free/

Safari. (03 de Mayo de 2015). Obtenido de Replacing r-Commands with SSH: https://www.safaribooksonline.com/library/view/ssh-the-secure/0596008953/ch04s05.html

Snort FAQ. (04 de Junio de 2015). Obtenido de What is Snort: https://www.snort.org/faq/what-is-snort

Suricata. (04 de Junio de 2015). Obtenido de What is Suricata: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/What_is_Suricata

TCPDUMP & LIBCAP. (10 de Mayo de 2015). Obtenido de TCPDUMP: http://www.tcpdump.org/tcpdump_man.html

Tenable Network Security. (04 de Junio de 2015). Obtenido de Nessus: http://www.tenable.com/products/nessus-vulnerability-scanner

The Linux Information Project. (18 de Marzo de 2015). Obtenido de Linus Torvalds: A Very Brief and Completely Unauthorizes Biography: http://www.linfo.org/linus.html

The UNIX® System. (08 de Febrero de 2015). Obtenido de What is UNIX®?: http://www.unix.org/what_is_unix.html

Ubuntu manuals. (10 de Mayo de 2015). Obtenido de vmstat - proporciona datos sobre la memoria virtual: http://manpages.ubuntu.com/manpages/hardy/es/man8/vmstat.8.html

XinuOS. (09 de Febrero de 2015). Obtenido de Unix Ware : http://www.sco.com/products/unixware714/

Zone-H. (04 de Febrero de 2015). Obtenido de http://www.zone-h.com/archive

GLOSARIO DE TÉRMINOS

ANACONDA. Gestor de instalación desarrollado por Red Hat.

AIDE. Advanced Intrusion Detection Environment.

APF. Advanced Policy Firewall.

BIOS. Basic Input Output System.

C. Lenguaje de programación popular desarrollado en los Laboratorios Bell.

CEDIA. Consorcio Ecuatoriano de Internet Avanzado.

CD. Compact Disc.

CPU. Central Processing Unit.

CSF. Config Server Firewall.

DISQUETTE. Disco flexible de almacenamiento de datos de tipo magnético.

DISTRO. Nombre alternativo para una distribución GNU/Linux.

DNS. Domain Name System o Domain Name Server.

DVD. Digital Versatile Disc.

FREE. Comando Linux que despliega el consumo de memoria RAM.

FREEWARE. Se refiere a software gratuito.

FTP. File Transfer Protocol. Protocolo para transferir dicheros.

GUI. Graphical User Interface

GNOME. Entorno de escritorio para sistemas Unix desarrollado por GNU.

GNU. GNU is not Unix. Proyecto que fomenta el software libre.

GPL. General Public License

GRUB. GNU Grand Unified Bootloader. Gestor de arranque para Linux.

HTOP. Comando que despliega los procesos más consumidores y permite administrarlos.

HTTP. Hypertext Transfer Protocol.

ICMP. Internet Control Message Protocol.

IDS. Intrusion Detection System.

ISO. International Organization for Standardization.

IP. Internet Protocol.

IPS. Intrusion Prevention System

IPTABLES. Herramienta de cortafuegos disponible en el núcleo de Linux.

KDE. Entorno de escritorio para Linux.

KVM. Kernel-based Virtual Machine

LOGS. Resgitros del sistema almacenados en archivos de texto plano

LTS. Long Term Support

LVM. Logical Volume Manager

LXDE. Lightweight X11 Desktop Environment. Entorno de escritorio para Linux muy ligero.

MIDORI. Navegador Web de Elementary OS.

NETCRAFT. Compañía que brinda servicios de internet basados en el análisis de servidores y alojamiento web.

NMAP. Network Mapper. Software que permite escanear puertos de un equipo.

NNTP. The Network News Transfer Protocol

NTP. Network Time Protocol

PACMAN. Gestor de paquetes de software para Arch Linux.

PANTHEON. Entorno de escritorio para Linux, desarrollado por Elementary OS.

PC. Personal Computer.

PLUG-IN. Aplicación que se relaciona con otra, para agregarle una función nueva.

POP3. Post Office Protocol.

PS. Comando Linux que despliega los procesos que se están ejecutando en el sistema

PYMES. Pequeñas y medianas empresas.

RAM. Random Access Memory

RCP. Se basa en RLOGIN para realizar copias remotas entre ordenadores.

RLOGIN. Remote Login. Permite abrir una sesión remota.

RPM. Red Hat Package Manager. Gestor de paquetes de software desarrollado por Red Hat.

RRDTOOL. Round Robin Database Tool.

RSH. Remote Shell. Programa de consola para ejecutar comandos en un equipo remote.

RSYNC. Programa que permite transferir archivos rápidamente y de manera incremental.

SANDBOX. Entorno para pruebas de software.

SCRATCH. Editor de archivos de Elementary Linux.

SCP. Secure Copy. Programa que permite transferir archivos remotamente bajo el protocolo SSH.

SFTP. SSH File Transfer Protocol.

SHELL. Programa que provee una interfaz para la interpretación de comandos en Linux.

SMTP. Simple Mail Transfer Protocol.

SNMP. Simple Network Management Protocol.

SSH. Secure Shell. Protocolo que permite conexiones remotas seguras para el uso de SHELL.

SSL. Secure Sockets Layer

SWAP. Espacio de memoria para intercambio de disco, conocida también como memoria virtual.

TELNET. Telecommunication Network. Permite accede remotamente a un equipo.

TLS. Transport Layer Security

TOP. Comando Linux que despliega los procesos más consumidores de recursos.

UNITY. Entorno de escritorio desarrollado por Ubuntu.

UNIX. Sistema operativo comercial multiusuario y multitarea, desarrollado por los Laboratorios Bell, actualmente pertenece a la empresa Novell.

UNIXWARE. Sistema operativo comercial de la familia Unix, desarrollado por SCO Group.

URPMI. Gestor de paquetes basado en RPM utilizado por Mageia Linux

VPN. Virtual Private Network

YAST. Yet Another Setup Tool. Herramientas que facilitan la administración de los sistemas Open SUSE y SUSE Linux.

WEBALIZER. Programa que genera estadísticas de acceso Web, a través de la lectura de logs.

WINE. Wine is not an Emulator. Programa que permite la ejecución de programas diseñados para Microsoft Windows.