CAPITULO I

1. FUNDAMENTACIÓN TEÓRICA DE LAS MAQUINAS VIRTUALES Y LOS SISTEMAS OPERATIVOS

1.1. UTILIZACION DE MAQUINAS VIRTUALES

1.1.1. Introducción y Sinopsis

VMware Workstation es un poderoso software de máquina virtual para desarrolladores y administradores de sistemas que desean revolucionar el desarrollo, prueba e implementación de herramientas de software en su empresa. VMware Workstation, que se ha comercializado durante más de cinco años y ha sido ganador de más de una docena de importantes premios para productos, permite a los desarrolladores de software crear y probar las aplicaciones más complejas de tipo servidor en red que se ejecutan en Microsoft Windows, Linux o NetWare, todo desde un solo computador. Las características esenciales, como funcionamiento en red virtual, copias puntuales activas, funciones de arrastrar y soltar, carpetas compartidas y soporte para PXE convierten a VMware Workstation en una herramienta indispensable para los desarrolladores y administradores de sistemas de TI empresariales.

Con más de cinco años de éxito comprobado y millones de usuarios, VMware Workstation mejora la eficiencia, reduce los costos y aumenta la flexibilidad y la

capacidad de respuesta. Instalar VMware Workstation en el computador es el primer paso para transformar su infraestructura de TI en una infraestructura virtual. VMware Workstation se utiliza en la empresa para:

- Optimizar las operaciones de desarrollo y prueba de software.
- Acelerar las implementaciones de las aplicaciones.
- Garantizar la compatibilidad de las aplicaciones y realizar migraciones de sistemas operativos.

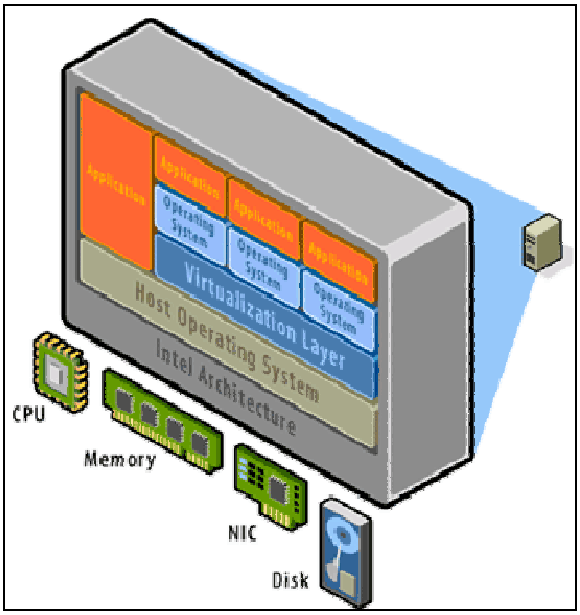

Figura 1.1: Distribución espacios en Maquinas Virtuales
Fuente: Grupo Investigador.(www.vmware.com)

VMware Workstation funciona al permitir que múltiples sistemas operativos y sus aplicaciones se ejecuten de manera simultánea en un solo equipo físico. Estos sistemas operativos y aplicaciones se aíslan en máquinas virtuales seguras que coexisten en una sola pieza de hardware. La capa de virtualización de VMware asigna los recursos de hardware físicos a los recursos de las máquinas virtuales, de modo que cada máquina virtual posee su propia CPU, memoria,

discos, dispositivos de I/O, etc. Las máquinas virtuales son el equivalente completo a un equipo x86 estándar.

VMware Workstation permite que los desarrolladores de software para empresas creen y prueben las aplicaciones más complejas de tipo servidor en red que se ejecutan en Windows, Linux o NetWare, todo desde un solo computador.
Crear redes complejas y desarrollar, probar e implementar nuevas aplicaciones, todo desde un único computador.

Aprovechar la capacidad de transporte de las máquinas virtuales para compartir fácilmente y sin riesgo los entornos de desarrollo y las configuraciones de prueba precargadas para sistemas operativos y aplicaciones.

Agregar o cambiar sistemas operativos sin necesidad de volver a particionar el disco ni reiniciar el computador.
Ejecutar sistemas operativos nuevos y aplicaciones antiguas en un mismo computador.

Desde su lanzamiento en 1999, VMware Workstation ha revolucionado la manera en que se desarrollan las herramientas de software y las infraestructuras de TI y se ha transformado en el estándar de facto para los desarrolladores y profesionales de TI en todo el mundo. Si su empresa está buscando una manera de simplificar y acelerar el desarrollo, las pruebas y la implementación de

software e infraestructuras de TI, VMware Workstation es esencial. Al implementar VMware Workstation en su entorno, usted podrá:

- Disminuir los ciclos de desarrollo.
- Disminuir el tiempo que tarda en resolver los problemas.
- Aumentar la productividad.
- Acelerar el tiempo de salida al mercado.
- Mejorar de la calidad de los proyectos.

1.1.2. Características de las Maquinas Virtuales

Las características más importantes del VMWare son sin lugar a dudas los 3 grandes grupos y de cada una de ellas se desprenden como realizar cada una de las características importantes:

- Optimizar el desarrollo y las pruebas de software
    - Crear múltiples entornos de desarrollo y pruebas en u único sistema
    - Aceleración de los ciclos de desarrollo y disminución del tiempo de salida al mercado.
    - Creara aplicaciones de misión critica basadas en Windows y/o Linux
    - Disminución de los costos de hardware entre un 50 y 60%.
    - Archivar entornos de prueba en file Server (Servidores de Archivos) y restaurarlos rápidamente, según sea necesario.
    - Disminución del costo o tiempo de configuración entre un 25 y 55% dejando tiempo para realizar las importantes tareas de desarrollo y prueba.

- Probar nuevas actualizaciones de aplicaciones, correcciones y service packs de sistemas operativos en un solo computador.
- Mejora de la calidad de los proyectos mediante pruebas más rigurosas.
- Eliminación de los costosos problemas de implementación y mantenimiento.

- Acelerar el desarrollo de las aplicaciones
  - Probar, configurar y realizar el aprovisionamiento de servidores de clase empresarial como máquinas virtuales de VMware Workstation y luego implementarlos en un servidor físico o en un servidor VMWare.
  - Mejora de la calidad de las implementaciones
  - Mejora de la productividad.
  - Crear una completa red de aplicaciones compuesta de múltiples computadores y switches de red en un conjunto de máquinas virtuales y probarlas sin afectar la red de producción.
  - Disminución del riesgo para las redes corporativas al crear redes virtuales complejas, seguras y aisladas que espejan las redes de las empresas.

1.1.3. Escenarios de las Maquinas Virtuales

Los escenarios que administran las Maquinas virtuales pueden ser muy variados, pero en el caso de la implementación de recursos propios de un Sistema Operativo debemos, detallar los tres más principales como son:

- Soporte para las aplicaciones heredadas.

- Soporte Técnico
- Quality Assurance(Aseguramiento de la Calidad)

Soporte para las aplicaciones heredadas

Gracias a VMWare las empresas pueden sacar provecho a los sistemas operativos nuevos al tiempo que siguen ofreciendo soporte para las aplicaciones heredadas que no son compatibles con ellos. Antiguamente, cuando una empresa tenía aplicaciones de misión crítica que no se podían ejecutar con sistemas operativos nuevos, las opciones que tenía la compañía eran aplazar la implementación hasta que los desarrolladores hubieses actualizado las aplicaciones heredadas u ofrecer a los usuarios de esas aplicaciones equipos independientes hasta que se dispusiese de las actualizaciones necesarias.

Ahora, se puede instalar VMWare en los ordenadores de usuarios que tienen que utilizar aplicaciones heredadas, de manera que pueden ejecutar la versión del sistema operativo con la que son compatibles las aplicaciones heredadas. Imaginemos por ejemplo que una empresa está realizando una migración a Linux, pero que el departamento contable utiliza un software que solo es compatible con Windows 98. Se puede instalar las maquinas virtuales en los equipos del departamento contable, y dejar instalado Windows 98 en una máquina virtual como sistema operativo invitado, con un software de contabilidad instalado sobre Windows 98. De este modo, esos usuarios pueden sacar el máximo partido a todos los beneficios que ofrece Linux pero seguir utilizando su software de contabilidad en las máquinas virtuales.

Soporte Técnico

VMWare puede convertirse en una herramienta esencial de ayuda en escritorio, recortando la frecuencia de llamadas, mejorando el tiempo de respuesta y reduciendo los costos derivados del soporte. Por lo general las ayudas de escritorio ofrecer soporte para diversos tipos de hardware y de configuraciones de software, versiones de aplicaciones, *Service Packs* y *hot fixes* entre otras cosas, lo que puede ser difícil de manejar. A menudo los técnicos de ayuda de escritorio tienen que mantener varios ordenadores o reiniciar sus equipos para ofrecer soporte a clientes que utilizan configuraciones de diversa índole. O bien puede que no tengan acceso a la gran variedad de tipos de configuración que utilizan los clientes.

Gracias a VMWare, el personal de ayuda de escritorio está mejor preparados para emular los entornos de los clientes que solicitan sus servicios, incluyendo sistemas operativos, aplicaciones *service packs* y otro tipo de variedades. Pueden crear estos entornos por adelantado y luego, cuando un usuarios se pone en contacto con ellos en busca de soporte, cargar el entorno en cuestión en segundos desde un servidor de archivos, un CD-ROM o incluso una red. Estas ventajas ofrecen una gran comodidad además de ahorrar tiempo. Por ejemplo, un técnico de ayuda de escritorio que utilice Windows XP puede seguir ofreciendo soporte a usuarios de Windows 98, Windows Me, Windows NT, Windows 2000, incluso Linux sin tener que utilizar varios ordenadores o reiniciar sus equipos con sistemas operativos distintos. Sin embargo, solo tienen que atender la llamada, iniciar una maquina virtual ya elaborada que se ajuste a las condiciones

del usuario y luego seguir atendiéndole.

Además, para ofrecer acceso inmediato a distintos tipos de configuraciones, VMWare ofrece a los técnicos de ayuda de escritorio la oportunidad de ofrecer soporte a los usuarios en entornos independientes y seguros. Por ejemplo, si el ordenador del técnico se averiara mientras estuviese comprobando los problemas de un usuario, la avería solo afectaría la máquina virtual, no a ninguna otra máquina virtual o al sistema operativo anfitrión.

Más aún, VMWare ofrece a los técnicos de ayuda de escritorio la posibilidad de empezar desde un entorno operativo limpio siempre que lo necesite. En lugar de tener que perder tiempo restableciendo una configuración para que adquiera el estado inicial, recargando un sistema operativo o instalando aplicaciones, los técnicos puede simplemente utilizar *Undo disk*, que siempre empieza con la misma configuración.

Quality Assurance(Aseguramiento de la Calidad)

Los ingenieros de Quality Assurance tienen que probar sus aplicaciones en una amplia gama de configuraciones. Por ejemplo, los desarrolladores de Windows a menudo diseñan el software de manera que pueda funcionar con diferentes idiomas las versiones de Windows 98, Windows Me, Windows NT, Windows 2000 y Windows XP. Ni siquiera las distintas combinaciones de sistemas operativos explican la gran variedad de hardware. Los ingenieros encargados de

las pruebas tienen que poner a prueba sus aplicaciones en todos los sistemas operativos para los que ofrecen soporte.

Tener que probar el software en todas las combinaciones posibles no es práctico Sin embargo, VMWare ofrece a los ingenieros de pruebas un método para verificar si el software funciona en varios sistemas operativos y en versiones con idiomas distintos. Pueden poner a prueba el software con mayor rapidez porque cada máquina virtual se inicia de forma prácticamente simultánea, y pueden pasar de una máquina a otra con tan solo un clic de ratón. Además, VMWare ofrece un entorno aislado para probar el software. Si el software se estropea, la avería no afecta al equipo real, y los ingenieros pueden reiniciar la máquina virtual rápidamente.

1.1.4. Sinopsis tecnológica y configuración

Virtualización del PC

Por lo general, un ordenador solo puede ejecutar un sistema operativo cada vez, con aplicaciones que se ejecutan sobre el mismo. El sistema operativo utiliza los controladores de dispositivos para abordar el hardware del ordenador. El hardware incluye el ratón y el teclado, el procesador, la memoria. Los discos y los controladores, las tarjetas de video, las tarjetas de red y otros dispositivos físicos. Es decir, un ordenador está compuesto por una serie de dispositivos, ejecuta un sistema operativo cada vez y dispone de una serie de aplicaciones en ese sistema operativo.

VMWare utiliza tecnología de máquina virtual para ejecutar dos o más sistemas operativos y las aplicaciones que incluyen al mismo tiempo. De hecho, solo los recursos del equipo como la memoria y el espacio del disco duro son los que limitan el número y variedad de sistemas operativos y programas que puede ejecutar el usuario. El número de sistemas operativos que el usuario puede utilizar al mismo tiempo viene dado por la memoria que hay disponible.

Las máquinas virtuales de VMWare dependen de hardware real y ficticio. VMWare simula el hardware de la máquina virtual en software. Los componentes de hardware simulados incluyen el controlador de interrupciones, controlador DMA, controlador IDE/ATA, Ram no volátil, reloj en tiempo real, controlador I/O, controlador de teclado, controlador de memoria, temporizador programable y hardware de gestión de potencial. Además, con VMWare se pueden utilizar diversos componentes de hardware real. Esto incluye el teclado, ratón, disquete, Puerto de juegos, lector de CD-ROM y procesador. Por ejemplo, VMWare depende del teclado para que los usuarios introduzcan información, dejando la información en la máquina virtual. Sin embargo, VMWare depende del sistema operativo anfitrión y del hardware par tareas como acceso al disco y a la red. Y para operaciones que exigen más resultados, VMWare obvia el sistema operativo para hacerse con el control del hardware, y devolviéndolo al sistema operativo tan pronto como sea posible. En cualquiera de los casos, todo lo que ven los usuarios es que los entornos de los sistemas operativos invitados y el anfitrión se están ejecutando de manera simultánea.

Actualización de VMWare para Windows

Los usuarios pueden actualizar a Microsoft VMWare si están utilizando Connectix VMWare para Windows 5.2. Aquellos que utilizan una versión más Antigua de Connectix VMWare para Windows tendrán que desinstalar esta versión primera y luego instalar VMWare.

El proceso de desinstalación de VMWare para Windows no altera o cambiar los discos duros virtuales, por lo que los usuarios pueden utilizar un disco duro virtual.

1.1.5. Requisitos del Sistema

La instalación y posterior configuración de las maquinas virtuales requiere de una serie de requisitos que son obligatorios al momento de su instalación, todo esto está dado por el numero de maquinas virtuales que se deseen configurar.

Es necesario aclarar que cada maquina virtual va a estar dado de igual manera por el sistema operativo que se seleccione, ya que no resulta igual la instalación de un Sistema Operativo como Linux o Solaris como la instalación de un Windows 95 o superior.

A continuación se recogen todos los requisitos del sistema mínimos para el equipo físico y el sistema operativo anfitrión.

- Un ordenador con procesador x86 de: la familia AMD Athlon/Duron o la familia Intel Celeron o Pentium II, III o 4; Un mínimo de 400 MHz, se recomienda 1.0 GHz o más rápido; Caché de nivel 2. Los usuarios pueden

ejecutar VMWare en un ordenador multiprocesador, pero el programa solo utilizará uno de ellos.

- Lector CD-ROM o DVD
- Pantalla Super VGA (800x600) o de resolución mayor
- Teclado y Microsoft *Mouse* o dispositivos señaladores compatibles
- Sistema operativo anfitrión: Windows XP Professional, Windows 2000 Professional o Windows XP Tablet PC Edition

Para la información sobre la memoria y espacio en el disco duro del equipo anfitrión debe estar dado por el numero de maquinas virtuales y el sistema operativo que se desea instalar en la maquina virtual. Estos requisitos son solo el punto de partida.

1.1.6. Evaluación de Maquinas Virtuales

Siendo está una herramienta de simulación de Plataformas de Sistemas Operativos podemos deducir que son de gran utilidad, ya que permiten a los usuarios de estos recursos experimentar nuevas y mejoradas experiencias, son un potencial si son explotadas en un alto porcentaje de rendimiento.

1.2. SISTEMAS DE DISTRIBUCION DE INTERNET (PROXY)

1.2.1. Definiciones de Proxy

El término en ingles **«Proxy»** tiene un significado muy general y al mismo tiempo ambiguo, aunque invariablemente se considera un sinónimo del concepto de **«Intermediario»**. Se suele traducir, en el sentido estricto, como **delegado** o **apoderado** (el que tiene el que poder sobre otro).

Un **Servidor Intermediario** (Proxy) se define como una computadora o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red. Durante el proceso ocurre lo siguiente:

- Cliente se conecta hacia un **Servidor Intermediario** (Proxy).
- Cliente solicita una conexión, fichero u otro recurso disponible en un servidor distinto
- **Servidor Intermediario** (Proxy) proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché.
- En algunos casos el **Servidor Intermediario** (Proxy) puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

Los **Servidores Intermediarios** (Proxies) generalmente se hacen trabajar simultáneamente como muro cortafuegos operando en el **Nivel de Red**, actuando como filtro de paquetes, como en el caso de **iptables**, o bien operando en el **Nivel de Aplicación**, controlando diversos servicios, como es el caso de **TCP**

Wrapper. Dependiendo del contexto, el muro cortafuegos también se conoce como **BPD** o **B**order **P**rotection **D**evice o simplemente **filtro de paquetes**.

Una aplicación común de los **Servidores Intermediarios** (Proxies) es funcionar como caché de contenido de Red (principalmente HTTP), proporcionando en la proximidad de los clientes un caché de páginas y ficheros disponibles a través de la Red en servidores HTTP remotos, permitiendo a los clientes de la red local acceder hacia éstos de forma más rápida y confiable.

Cuando se recibe una petición para un recurso de Red especificado en un **URL** (**U**niform **R**esource **L**ocator) el **Servidor Intermediario** busca el resultado del **URL** dentro del caché. Si éste es encontrado, el **Servidor Intermediario** responde al cliente proporcionado inmediatamente el contenido solicitado. Si el contenido solicitado no estuviera disponible en el caché, el **Servidor Intermediario** lo traerá desde servidor remoto, entregándolo al cliente que lo solicitó y guardando una copia en el caché. El contenido en el caché es eliminado luego a través de un algoritmo de expiración de acuerdo a la antigüedad, tamaño e historial de **respuestas a solicitudes** (hits) (ejemplos: **LRU**, **LFUDA** y **GDSF**).

Los **Servidores Intermediarios** para contenido de Red (Web Proxies) también pueden actuar como filtros del contenido servido, aplicando políticas de censura de acuerdo a criterios arbitrarios.

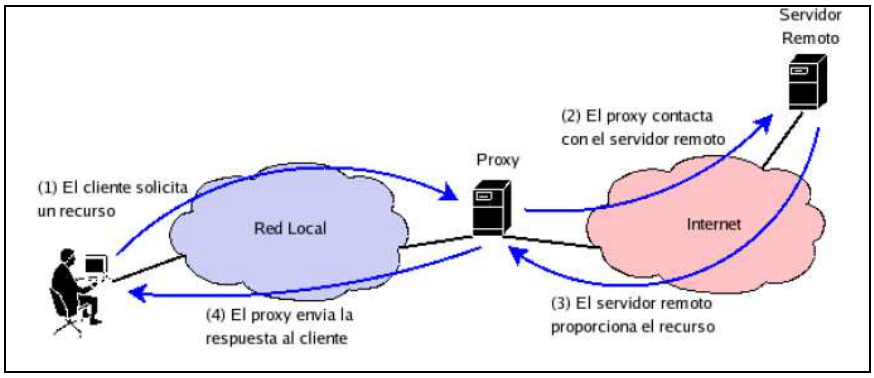

Figura 1.2: Diseño de un Proxy
Fuente: www.linuxparatodos.com

1.2.2. Tipos de Proxy

Dentro de los Proxy tenemos claramente identificados 3 tipos de servidores que son:

WEB PROXY CACHE

Se dice que un servidor esta actuado como Web Proxy cache cuando almacena en su disco duro las páginas Web descargadas de forma que, en próximas consultas, pueda acceder a ellas de forma muy rápida. De está forma estamos optimizando el canal de acceso a Internet de la organización del usuario en momentos de ocupación importante de la línea.

Este tipo de Proxy se suele usar en alguno de estos entornos:

- Cuando por motivos de seguridad, no deseas permitir acceso libre a Internet a los usuarios pero se desea proporcionarles acceso a la Web, se les proporciona a través del Proxy.

- Cunado se desea optimizar el ancho de banda y acelerar la navegación para los usuarios por ejemplo, una oficina con muchos trabajadores que sueles visitar frecuentemente las mismas páginas.

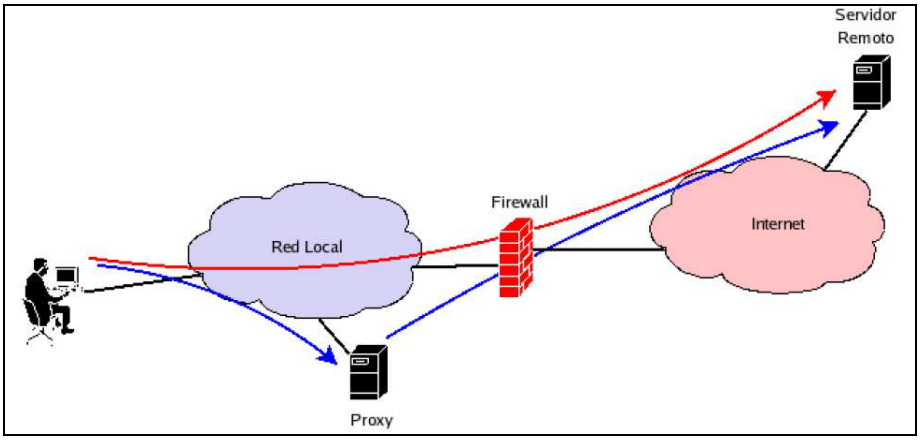

Figura 1.3: Diseño de un Web Proxy Cache
Fuente: www.linuxparatodos.com

Proxy Inverso

Un Proxy inverso (o *reverse Proxy*) es aquel que se sitúa cerca de uno o mas servidores Web, de forma que es el Proxy quien recibe las peticiones y las reenvía a los servidores Web. Este tipo de Proxy se suele usar en algunos de estos entornos:

- Para añadir seguridad a los servidores Web, en ningún momento se accede directamente a ellos sino al Proxy
- Para balancear la carga de los servidores: el servidor Proxy es el encargado de enviar las peticiones a aquellos a servidores que estén más descargados
- Para descargar a los servidores Web de contenido estático como imágenes o documentos
- En caso de sitios Web seguros se puede dejar al Proxy que haga el encriptado de los datos y descargar así a los servidores Web

PROXY TRANSPARENTE

Tal como hemos visto es posible usar un Proxy para aplicar políticas de control de acceso a Internet. Normalmente esa configuración no es transparente: es necesario modificar el cliente para que use el Proxy al acceder a Internet, de forma que es posible que un usuario modifique esa configuración.

Una configuración de Proxy transparente hace que no sea necesaria modificación alguna en las maquinas clientes, eliminando el riesgo de que un usuario modifique dicha configuración a su antojo. El uso de un Proxy transparente combina un servidor Proxy con NAT, de forma que todas las conexiones son encaminadas a través del Proxy sin la intervención de la maquina cliente.

1.2.3. Sistemas Operativos Soportados

1.2.3.1. Linux

Linux es probablemente el acontecimiento más importante del software gratuito desde el original Space War, o, más recientemente, Emacs. Se ha convertido en el sistema operativo para los negocios, educación, y provecho personal. Linux ya no es solo para gurus de UNIX que se sientan durante horas frente a la resplandeciente consola (aunque le aseguramos que un gran número de usuarios pertenece a esta categoría). Este libro le ayudara a sacarle el máximo partido.

Linux (pronunciado con una i corta, como en LIH-nucs) es un clonico del sistema operativo

UNIX que corre en ordenadores Intel 80386 y 80486. Soporta un amplio rango de software, desde TEX a X Windows al compilador GNU C/C++ a TCP/IP. Es una implementación de UNIX versátil, distribuida gratuitamente en los términos de la Licencia GNU.

Linux puede convertir cualquier PC 386 o 486 en una estación de trabajo. Le pondrá todo el poder de UNIX en la punta de sus dedos. En los negocios ya se instala Linux en redes enteras, usando el sistema operativo para manejar registros financieros y de hospitales, un entorno de usuario distribuido, telecomunicaciones, etc. Universidades de todo el mundo usan Linux para dar cursos de programación y diseño de sistemas operativos. Y, por supuesto, entusiastas de los ordenadores de todo el mundo están usando Linux en casa, para programar, entretenerse, y conocerlo a fondo.

Lo que hace a Linux tan diferente es que es una implementación gratuita de UNIX. Fue y aun es desarrollado por un grupo de voluntarios, principalmente en Internet, intercambiando código, comentando fallos, y arreglando los problemas en un entorno abierto. Cualquiera es bienvenido a sumarse al esfuerzo de desarrollo de Linux: todo lo que se pide es interés en producir un clónico gratuito de UNIX y algunos conocimientos de programación.

1.2.3.2. Windows 2003

Microsoft Windows (conocido simplemente como *Windows*) es un sistema operativo con interfaz gráfica para computadoras personales cuyo propietario es la empresa Microsoft. Las distintas versiones de Windows, las cuales ofrecen un entorno gráfico sencillo desde la versión Windows 95. Se ha convertido en el sistema operativo más utilizado en el mundo. Por ésta razón, la mayoría de las empresas fabricantes de hardware y software en el mundo tienden a desarrollar sus aplicaciones basadas en dicho sistema. El común uso de éste sistema operativo se debe a que la mayoría de las computadoras incluyen éste sistema instalado por defecto. Esto causa cierta controversia, ya que es visto por ciertas personas, como un método monopolista de Microsoft, ya que obliga al cliente a comprar una licencia de Microsoft, al mismo tiempo que compra la máquina.

Windows ha incorporado a través de sus diferentes versiones varias herramientas que se han convertido en estándares internacionales, como por ejemplo, el sistema de archivos FAT. Windows incorpora, entre otro software, herramientas como Internet Explorer y el Reproductor de Windows Media. Estas herramientas se han convertido con el tiempo en las más usadas, especialmente Internet Explorer, debido a que vienen instaladas por defecto en dicho sistema operativo.

Windows es utilizado principalmente en computadoras personales existiendo también diferentes versiones para servidores y dispositivos móviles.

1.2.3.3. Solaris

Solaris es un sistema operativo desarrollado por Sun Microsystems. Es un sistema certificado como una versión de UNIX. Aunque Solaris en sí mismo aún es software propietario, la parte principal del sistema operativo se ha liberado como un proyecto de software libre denominado *Opensolaris*. Solaris puede considerarse uno de los sistemas operativos más avanzados. Sun denomina así a su sistema operativo.

El primer sistema operativo de Sun nació en 1983 y se llamó inicialmente **SunOS**. Estaba basado en el sistema UNIX BSD, de la Universidad de Berkeley, del cual uno de los fundadores de la compañía fue programador en sus tiempos universitarios. Más adelante incorporó funcionalidades del System V, convirtiéndose prácticamente en un sistema operativo totalmente basado en System V.

Esta versión basada en System V fue publicada en 1992 y fue la primera en llamarse **Solaris**, más concretamente *Solaris 2*. Las anteriores fueron llamadas *Solaris 1* con efecto retroactivo. SunOS solo tendría sentido a partir de ese momento como núcleo de este nuevo entorno operativo Solaris. De esta forma Solaris 2 contenía SunOS 5.0. Desde ese momento se distingue entre el núcleo del sistema operativo (SunOS), y el entorno operativo en general (Solaris), añadiéndole otros paquetes como Apache o DTrace. Como ejemplo de esta función, Solaris 8 contiene SunOS 5.8.

Solaris usa una base de código común para las arquitecturas que soporta: SPARC y x86 (incluyendo AMD64/EM64T). También fue portado a la arquitectura PowerPC (en plataforma PReP) en la versión 2.5.1, pero el porte fue

cancelado casi tan pronto como fue liberado. En un tiempo se planeó soporte para el Itanium pero nunca se llevó al mercado. [1] Sun también tiene planes de implementar ABIs de Linux en Solaris 10, permitiendo la ejecución de código objeto Linux de forma nativa en la plataforma x86.

Solaris tiene una reputación de ser muy adecuado para el multiprocesamiento simétrico (SMP), soportando un gran número de CPUs. También ha incluido soporte para aplicaciones de 64 bits SPARC desde Solaris 7. Históricamente Solaris ha estado firmemente integrado con la plataforma hardware de Sun, SPARC, con la cual fue diseñado y promocionado como un paquete combinado. Esto proporcionaba frecuentemente unos sistemas más fiables pero con un coste más elevado que el del hardware de PC. De todas formas, también ha soportado sistemas x86 desde la versión Solaris 2.1 y la última versión, Solaris 10, ha sido diseñada con AMD64 en mente, permitiendo a Sun capitalizar en la disponibilidad de CPUs de 64 bits commodities basadas en la arquitectura AMD64. Sun ha promocionado intensamente Solaris con sus estaciones de trabajo de nivel de entrada basadas en AMD64, así como con servidores que en 2006 varían desde modelos dual-core hasta modelos a 16 cores.

El primer entorno de escritorio para Solaris fue OpenWindows. Fue reemplazado por CDE en la versión Solaris 2.5. El escritorio Java Desktop System, basado en GNOME, se incluye por defecto con Solaris 10.

El código fuente de Solaris (con unas pocas excepciones) [2] ha sido liberado bajo la licencia CDDL (**Licencia Común de Desarrollo y Distribución**) como un proyecto de software libre bajo el nombre **OpenSolaris**.

La licencia CDDL ha sido aprobada por la Open Source Initiative (OSI) como una licencia open source [3] y por la FSF como una licencia de software libre (aunque incompatible con la popular licencia GPL [4]).

La base de OpenSolaris fue alimentada el 14 de junio de 2005 a partir de la entonces actual base de desarrollo de código de Solaris. Es posible descargar y licenciar versiones tanto binarias como en forma de código fuente sin coste alguno. Además, se ha añadido al proyecto Open Solaris código para características venideras como soporte Xen. Sun ha anunciado que las versiones futuras de Solaris se derivarán a partir de OpenSolaris.

1.3. SISTEMA DE SEGURIDADES

1.3.1. Definición de Seguridad

Debido a la creciente confianza en computadoras de red poderosas para los negocios y en llevar un seguimiento de nuestra información personal, las industrias se forman considerando de antemano la práctica de seguridad de la computación y redes. Las corporaciones solicitan el conocimiento y habilidades de los expertos para auditar los sistemas y ajustar soluciones para satisfacer los requerimientos operativos de la organización. Puesto que la mayoría de las organizaciones son dinámicas por naturaleza, con trabajadores accesando los recursos informáticos de la organización local y remotamente, la necesidad de ambientes computacionales seguros se ha vuelto cada vez más relevante.

Desafortunadamente, la mayoría de las organizaciones (así como también usuarios individuales) dejan la seguridad como algo para resolver luego, un proceso que es ignorado en favor de mayor poder, mayor productividad y en las preocupaciones presupuestarias. La implementación adecuada de la seguridad es a menudo realizada *postmortem*. Después que ocurre una intrusión no autorizada. Los expertos de seguridad consideran que el establecimiento de medidas adecuadas antes de conectar un sitio a una red insegura tal como la Internet, es una forma efectiva de frustrar la mayoría de los intentos de intrusión.

La seguridad de computación es un término general que cubre una gran área de computación y procesamiento de la información. Las industrias que dependen de sistemas computarizados y redes para ejecutar sus operaciones y transacciones de negocios diarias, consideran sus datos como una parte importante de sus activos generales. Muchos términos y medidas se han incorporado a nuestro vocabulario diario en los negocios, tales como costo total de propiedad (total cost of ownership, TCO) y calidad de servicios (QoS). Con estas medidas, las industrias calculan aspectos tales como integridad de los datos y alta disponibilidad como parte de los costos de planificación y administración de procesos.

En algunas industrias, como el comercio electrónico, la disponibilidad y confianza de los datos pueden hacer la diferencia entre el éxito y el fracaso.

1.3.2. Tipos de Seguridades en Redes de telecomunicaciones

Después de implementar la seguridad en los componentes físicos de la red, el administrador necesita garantizar la seguridad en los recursos de la red, evitando

accesos no autorizados y daños accidentales o deliberados. Las políticas para la asignación de permisos y derechos a los recursos de la red constituyen el corazón de la seguridad de la red.

Se han desarrollado dos modelos de seguridad para garantizar la seguridad de los datos y recursos hardware:

- Compartición protegida por contraseña o seguridad a nivel de compartición
- Permisos de acceso o seguridad a nivel de usuario.

Compartición protegida por contraseña

La implementación de un esquema para compartir recursos protegidos por contraseñas requiere la asignación de una contraseña a cada recurso compartido. Se garantiza el acceso a un recurso compartido cuando el usuario introduce la contraseña correcta.

En muchos sistemas, se pueden compartir los recursos con diferentes tipos de permisos. Para ilustrar esto, utilizamos Windows 95 y 98 como ejemplos. Para estos sistemas operativos se pueden compartir los directorios como sólo lectura, total o depende de la contraseña.

- **Sólo lectura**. Si un recurso compartido se configura de sólo lectura, los usuarios que conocen la contraseña tienen acceso de lectura a los archivos de este directorio. Pueden visualizar los documentos, copiar a sus máquinas e imprimirlos, pero no pueden modificar los documentos originales.

- **Total**. Con el acceso total, los usuarios que conocen la contraseña tienen acceso completo a los archivos de este directorio. En otras palabras, pueden visualizar, modificar, añadir y borrar los archivos del directorio compartido.
- **Depende de la contraseña**. Depende de la contraseña implica configurar una compartición que utiliza dos niveles de contraseñas: **Contraseña de sólo lectura** y **Contraseña de acceso total.** Los usuarios que conocen la contraseña de sólo lectura tienen acceso de lectura y los usuarios que conocen la contraseña de acceso total tienen acceso completo

El esquema de compartir utilizando contraseña es un método de seguridad sencillo que permite a alguien que conozca la contraseña obtener el acceso a un recurso determinado.

Permisos de acceso

La seguridad basada en los permisos de acceso implica la asignación de ciertos derechos usuario por usuario. Un usuario escribe una contraseña cuando entra en la red. El servidor valida esta combinación de contraseña y nombre de usuario y la utiliza para asignar o denegar el acceso a los recursos compartidos, comprobando el acceso al recurso en una base de datos de accesos de usuarios en el servidor.

La seguridad de los permisos de acceso proporciona un alto nivel de control sobre los derechos de acceso. Es mucho más sencillo para una persona asignar a otra persona una contraseña para utilizar una impresora, como ocurre en la seguridad a nivel de compartición. Para esta persona es menos adecuado asignar una contraseña personal.

La seguridad a nivel de usuario es el modelo preferido en las grandes organizaciones, puesto que se trata de la seguridad más completa y permite determinar varios niveles de seguridad.

Seguridad de los recursos

Después de autenticar a un usuario y permitir su acceso a la red, el sistema de seguridad proporciona al usuario el acceso a los recursos apropiados.

Los usuarios tienen contraseñas, pero los recursos tienen permisos. En este sentido, cada recurso tiene una barrera de seguridad. La barrera tiene diferentes puertas mediante las cuales los usuarios pueden acceder al recurso. Determinadas puertas permiten a los usuarios realizar más operaciones sobre los recursos que otras puertas. En otras palabras, ciertas puertas permiten a los usuarios obtener más privilegios sobre el recurso.

El administrador determina qué usuarios tienen acceso a qué puertas. Una puerta asigna al usuario un acceso completo o control total sobre el recurso. Otra puerta asigna al usuario el acceso de sólo lectura.

Algunos de los permisos de acceso habituales asignados a los directorios o archivos compartidos son:

- **Lectura**: Leer y copiar los archivos de un directorio compartido
- **Ejecución:** Ejecutar los archivos del directorio
- **Escritura:** Crear nuevos archivos en el directorio
- **Borrado:** Borrar archivos del directorio.

- **Sin acceso:** Evita al usuario obtener el acceso a los directorios, archivos o recursos.

Diferentes sistemas operativos asignan distintos nombres a estos permisos

Permisos de grupo

El trabajo del administrador incluye la asignación a cada usuario de los permisos apropiados para cada recurso. La forma más eficiente de realizarlo es mediante la utilización de grupos, especialmente en una organización grande con muchos usuarios y recursos. Windows NT Server permite a los usuarios seleccionar el archivo o carpeta sobre la que se establecen los permisos de grupo.

Los permisos para los grupos funcionan de la misma forma que los permisos individuales. El administrador revisa los permisos que se requieren para cada cuenta y asigna las cuentas a los grupos apropiados. Éste es el método preferido de asignación de permisos, antes que asignar los permisos de cada cuenta de forma individual.

La asignación de usuarios a los grupos apropiados es más conveniente que asignar permisos, de forma separada, a cada usuario individualmente. Por ejemplo, puede que no sea conveniente la asignación al grupo *Todos* del control total sobre el directorio public. El acceso total permitiría a cualquiera borrar y modificar los contenidos de los archivos del directorio public.

El administrador podría crear un grupo denominado *Revisores,* asignar a este grupo permisos de control total sobre los archivos de los estudiantes e incorporar empleados al grupo *Revisores.* Otro grupo, denominado *Facultad,* tendría sólo

permisos de lectura sobre los archivos de los estudiantes. Los miembros de la facultad asignados al grupo *Facultad*, podrían leer los archivos de los estudiantes, pero no modificarlos.

Medidas de seguridad adicionales

El administrador de la red puede incrementar el nivel de seguridad de una red de diversas formas.

Cortafuegos *(Firewalls)*

Un *cortafuegos (firewalls)* es un sistema de seguridad, normalmente una combinación de hardware y software, que está destinado a proteger la red de una organización frente a amenazas externas que proceden de otra red, incluyendo Internet.

Los cortafuegos evitan que los equipos de red de una organización se comuniquen directamente con equipos externos a la red, y viceversa. En su lugar, todas las comunicaciones de entrada y salida se encaminan a través de un servidor Proxy que se encuentra fuera de la red de la organización. Además, los cortafuegos auditan la actividad de la red, registrando el volumen de tráfico y proporcionando información sobre los intentos no autorizados de acceder al sistema.

Un servidor Proxy es un cortafuego que gestiona el tráfico de Internet que se dirige y genera una red de área local (LAN). El servidor Proxy decide si es seguro permitir que un determinado mensaje pase a la red de la organización. Proporciona control de acceso a la red, filtrado y descarte de peticiones que el

propietario no considera apropiadas, incluyendo peticiones de accesos no autorizados sobre datos de propiedad

Auditoria

La revisión de los registros de eventos en el registro de seguridad de un servidor se denomina *auditoria.* Este proceso realiza un seguimiento de las actividades de la red por parte de las cuentas de usuario. La auditoria debería constituir un elemento de rutina de la seguridad de la red. Los registros de auditoria muestran los accesos por parte de los usuarios (o intentos de acceso) a recursos específicos. La auditoria ayuda a los administradores a identificar la actividad no autorizada. Además, puede proporcionar información muy útil para departamentos que facturan una cuota por determinados recursos de red disponibles y necesitan, de alguna forma, determinar el coste de estos recursos.

La auditoria permite realizar un seguimiento de las siguientes funciones:

- Intentos de entrada
- Conexiones y desconexiones de los recursos designados.
- Terminación de la conexión.
- Desactivación de cuentas.
- Apertura y cierre de archivos.
- Modificaciones realizadas en los archivos.
- Creación o borrado de directorios.
- Modificación de directorios.
- Eventos y modificaciones del servidor.
- Modificaciones de las contraseñas.

- Modificaciones de los parámetros de entrada.

Los registros de auditoria pueden indicar cómo se está utilizando la red. El administrador puede utilizar los registros de auditoria para generar informes que muestren las actividades con sus correspondientes fechas y rangos horarios. Por ejemplo, los intentos o esfuerzos de entrada fallidos durante horas extrañas pueden identificar que un usuario no autorizado está intentando acceder a la red.

1.3.3. Firewalls e IPSec

Red Hat Enterprise Linux es compatible con IPsec para la conexión entre hosts y redes remotos utilizando un túnel seguro en un transportador de red común tal como la Internet. IPsec se puede implementar usando una conexión host-a-host (una computadora a la otra) o de red-a-red (una LAN/WAN a la otra). La implementación IPsec en Red Hat Enterprise Linux utiliza el *Intercambio de llaves en Internet* (*IKE*), el cual es un protocolo implementado por el Internet Engineering Task Force (IETF), a ser usado para la autenticación mutua y asociaciones seguras entre sistemas conectándose. Una conexión IPsec se divide en dos fases lógicas. En la fase 1, un nodo IPsec inicializa la conexión con el nodo o red remota. El nodo/red remota verifica las credenciales del nodo solicitante y ambos lados negocian el método de autenticación para la conexión. En sistemas Red Hat Enterprise Linux, una conexión IPsec utiliza el método de *llave pre-compartida* o *pre-shared key* de autenticación de nodo IPsec.

La fase 2 de la conexión IPsec es donde se crea una *asociación de seguridad* SA) entre nodos IPsec.

Esta fase establece una base de datos SA con información de configuración, tal como el método de encriptación, parámetros de intercambio de llaves secretas y más. Esta fase maneja realmente la conexión IPsec entre nodos y redes.

La implementación de Red Hat Enterprise Linux de IPsec utiliza IKE para compartir las llaves entre hosts a través de la Internet. El demonio racoon de manejo de llaves se encarga de la distribución e intercambio de llaves IKE.

1.3.4. Protección Interna y Externa

La información es un recurso que, como el resto mide los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas a fin de garantizar a continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

La seguridad de la información se define aquí como la preservación de las siguientes características:

a) Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
b) Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

c) Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

La seguridad de la información se logra implementando un conjunto adecuado de controles que abarca políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software.

Se deben establecer estos controles para garantizar que se logre los objetivos específicos de seguridad de la organización.

La información y los procesos, sistemas y redes que le brindan apoyo constituyen importantes recursos de la empresa. LA confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Las organizaciones, sus redes y sistemas de información, se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los ataques mediante virus informáticos, “hacking” y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados.

La dependencia de las organizaciones respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a seguridad. La interconexión de las redes publicas y privadas, axial como el uso compartido de los recursos de información incrementa la dificultad de lograr el control para se seguros. La seguridad que puede

lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La identificación de los controles que deben implementarse requiere una cuidadosa planificación y atención a todos los detalles. La administración de la seguridad de la información, exige como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de proveedores, clientes y accionistas. Asimismo puede requerirse el asesoramiento experto de organizaciones externas. Los controles de seguridad de la información resultan considerablemente más económicos y eficaces si se incorporan en la etapa de especificación de requerimientos y diseño.