UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TÍTULO DE LA TESIS:

Título: "Virtualización de una red LAN con servidores de código abierto para evaluar los niveles de seguridad"

Previa la obtención del Grado Académico de Magíster en Telecomunicaciones

ELABORADO POR:

CESAR LIBARDO ROSADO MUÑOZ

Guayaquil, Marzo2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Magíster Cesar Libardo Rosado Muñoz como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

Guayaquil, Marzo 2014

DIRECTOR DE TESIS

_____

Ing. Manuel Romero Paz, MSc.

REVISORES:

_____

Ing. Luis Córdova Rivadeneira, MSc.

_____

Ing. Orlando Philco Asqui, MSc.

DIRECTOR DEL PROGRAMA

_____

Ing. Manuel Romero Paz, MSc.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

DECLARACIÓN DE RESPONSABILIDAD

YO, CESAR LIBARDO ROSADO MUÑOZ

DECLARO QUE:

La tesis "**Virtualización de una red LAN con servidores de código abierto para evaluar los niveles de seguridad**", previa a la obtención del grado Académico de Magíster, ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico de la tesis del Grado Académico en mención.

Guayaquil, Marzo 2014

EL AUTOR

_____

CESAR LIBARDO ROSADO MUÑOZ

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

AUTORIZACIÓN

YO, CESAR LIBARDO ROSADO MUÑOZ

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución de la Tesis de Maestría titulada: "**Virtualización de una red LAN con servidores de código abierto para evaluar los niveles de seguridad**", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, Marzo 2014

EL AUTOR

_____

CESAR LIBARDO ROSADO MUÑOZ

DEDICATORIA

A Dios y a mis padres,

Ángel y Briceida

AGRADECIMIENTOS

A Dios por darme salud, bendiciones y una mente sana.

Al Ing. Manuel Romero Paz excelente persona pionero en emprender este reto por su apoyo total y constante, por su amistad desde el comienzo de mi carrera profesional.

Un agradecimiento muy especial merece la comprensión, paciencia y el ánimo recibido de mi familia.

A todos ellos, muchas gracias

Resumen

El presente trabajo muestra diferentes aspectos referidos a la seguridad en los sistemas informáticos con orientación a los sistemas de código abierto,se estudian varios tipos de amenazas, los sistemas de detección de intrusos (IDS), las paredes o cortinas de fuego (Firewall), entre otros mecanismos de protección perimetral de las redes de área local.

Mediante la herramienta VMWare se realiza una virtualización de una red conteniendo una Zona Desmilitarizada (DMZ), donde se ha implementado un Cortafuegos mediante IPtables al cual se le aplican cadenas para traslado de direcciones y filtrado de paquetes a conveniencia según un esquema determinado.

Palabras claves: Código abierto, Linux, Cortafuegos, Centos, IPtables.

Abstract

This paper shows different aspects related to security in computer systems. For greater accuracy,this paperfocuses on open source systems. Firstly general security issues are exposed including references to several types of threats.Mechanisms for protrcting local areas networks are also analyzed e.g. IDS, Firewalls, etc.

In de second part of this study it is shown the process to installing and configuring the open source operating system (Centos) and for the virtualization of a small network containing a DMZ using VMWare. The configuration of a Firewall (IPtables) is also shown and analized.

Keywords:Open Source, Linux, Firewall, Centos, IPtables.

Índice

Introducción

La Seguridad es un asunto que cada vez cobra mayor importancia y es ahora un requisito a tener en cuenta en todos los sistemas de comunicación ya que las comunicaciones globales son inherentemente inseguras. La detección de intrusos, de programas malignos y de aspectos que perjudiquen la seguridad de las redes es cada día uno de los temas que más preocupan a los operadores de redes. Por esta razón se puede entender como seguridad a las características que puede tener un sistema, que indique que este sea seguro, que esté fuera de peligro o algún tipo de daño. En la práctica es muy difícil tener un sistema totalmente fiable, solo se intenta tener la máxima seguridad posible.

Existen muchas formas de afectar a los sistemas de transmisión y redes de datos así como personal maligno cuya función se resume en hacer daño a los sistemas de información.Con todo ese flujo de información viajando por la gran infraestructura establecida actualmente (Internet) y los usuarios conectados a ella, la probabilidad de que ocurra un ataque es muy elevada. Si se le suma a esto la falta de establecimiento de un nivel elevado de seguridad tomando en cuenta la disponibilidad, muchos de los sistemas actuales tienen una alta brecha en su seguridad.

Con el desarrollo de los sistemas de cómputo, conexiones a redes, hardware y software se fueron mejorando conceptos sobre el tema así como herramientas con el fin de crear robustas técnicas y sistemas de seguridad. No obstante, los malware evolucionaron así como también lo hicieron sus creadores. Es una lucha constante por tratar de mantener la integridad de la información y los sistemas.

El fenómeno de seguridad es muy seguido y utilizado en el mundo y se pudiera decir que ha ahogado a toda la sociedad desde el punto de vista de las redes, la informática y las comunicaciones, por lo que es muy importante su estudio. Nuestro país no está alejado de dicha realidad al presentar numerosos sistemas de redes y estar conectado a la mayor de ellas, Internet.

Dentro de los caminos de estudio e investigación en las áreas de Telecomunicaciones y Electrónica, uno de los principales temas a tratar es la seguridad.Resulta necesario hacer un estudio profundo de sus aspectos y así crear un método óptimopara la comprobación de sus niveles. Dado a la rápida evolución de los sistemas de redes, software y hardware que los componen, y fundamentalmente la potencial amenaza existente, conllevan a plantear una problemática.

Problema de la investigación:lanecesidad de evaluar la seguridad en sistemas de redes con servidores de código abierto.

H**ipótesis:** si se virtualiza una red LAN mediante la herramienta *VMware* se permitiría la evaluación de políticas de Firewall en topologías de seguridad en un entorno controlado.

ObjetivoGeneral: La virtualización de una red LANmediante la configuración de máquinas virtuales con ayuda de la herramienta *VMware*.

Objetivos Específicos:

1. Estudiar el estado del arte de las políticas de seguridad en redes LAN.
2. Estudiar las herramientas de seguridad de código abierto como los firewalls, *IPtables*, sistemas de detección de intrusos, etc.
3. Implementar un Firewall (*IPtables*) y otros aspectos de seguridad.

Metodología del proyecto

Esta investigación busca establecer la posibilidad de realizar la virtualización de una red LAN con servidores de código abierto para evaluar los niveles de seguridad. Esto requiere un análisis del sistema, el tráfico que circula por él determinando todos los datos a enviar para calcular la capacidad de ese tráfico, ancho de banda empleado, jitter, retardo, entre otros parámetros, por lo tanto es una investigación de perfil explicativo, en razón de que se intenta valorar la técnica de virtualización para propagar datos en banda ancha. El paradigma correspondiente es el Empírico-Analítico, el trabajo presenta un enfoque cuantitativo y el diseño de la Investigación es no experimental transversal debido a que no se manejarán premeditadamente las variables de estudio y se realizará la observación directa del fenómeno como se produce en su entorno natural para posteriormente efectuar el análisis correspondiente.

Capítulo 1. Fundamentos Teóricos de Administración y Seguridad.

Hablar de seguridad es un tanto complejo, porque se tienen diferentes opiniones respecto al tema. Desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones, como principales ejecutores de la misma, y en los usuarios. En este proceso se aprecia que no se ha añadido ningún nuevo concepto, solo se han transformado otros ya existentes: llaves, cerradura, cajas fuertes, puertas blindadas, trampas, vigilancia, etc.

Este término es hoy en día una profesión compleja con funciones especializadas donde entran a jugar elementos como, protector, competidor y el valor como elemento a proteger. De esta manera se puede decir que el término en cuestión es la interrelación dinámica (competencia) entre el agresor y el protector para obtener o conservar el valor.(Escartín, 2005),(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Villalon, 2006).

El capítulo contiene términos y conceptos básicos orientados a varios aspectos que trata la seguridad, ya sea esta física o lógica.

1.1 Análisis y objetivo de la seguridad.

Para comenzar el análisis de seguridad se deben conocer características de lo que se va a proteger: la información. Para esto se define *Dato* como la unidad mínima con la cual se compone cierta información. La *Información* es un conjunto de datos que tiene un significado específico más allá de cada uno de estos.

Existen distintos tipos de información. Se hace referencia a que hay algunas que son públicas, las cuales pueden ser visualizadas por cualquier persona; y aquella que puede ser privada, solo será visualizada por un grupo selecto de personas que trabajan con ella. Esta última tiene algunos aspectos los cuales hay que llevar de la mano(Escartín, 2005)**,** (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Borghello, Linux Máxima seguridad, 2005)

- Es crítica: Es indispensable para garantizar la continuidad operativa.
- Es valiosa: Es un activo con valor en sí misma.
- Es sensitiva: Debe ser conocida por las personas que la procesan y solo por ellas.

Otros de los conceptos que hay que tener en cuenta son los siguientes:

- La *Integridad de la información:* Esta no en más que la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y estas modificaciones sean registradas para posteriores controles y auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos o modificaciones que se infiltren en el sistema.
- *Disponibilidad u Operatividad:* Es la capacidad de la información de estar siempre disponible para ser procesada para las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software correctamente funcionando y que se respeten los formatos para su recuperación en forma satisfactoria.
- La *Privacidad y confidencialidad:* Es la necesidad de que la información sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a los dueños de la misma. Un ejemplo de esto es el filtrado de datos importantes de proyectos empresariales a otras empresas competidoras.
- El *Control:* Este permite asegurar que sólo los usuarios autorizados pueden definir cómo y cuándo permitir el acceso a la información.
- *Autenticidad:* Permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad permite también definir el origen de la información, validando el emisor de la misma para evitar suplantación de identidades.(Escartín, 2005)**,** (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Villalon, 2006)

- La prevención (antes): Es un mecanismo que aumenta la seguridad o fiabilidad de un sistema durante su funcionamiento normal. Ejemplo, el cifrado de información para su posterior transmisión.
- La detección (durante): Son mecanismos orientados a revelar violaciones en la seguridad. Generalmente son programas de auditorías.
- La recuperación (después): Mecanismos que se aplican cuando la violación del sistema ya se ha detectado, para retomar este a su funcionamiento normal. Ejemplo, recuperación de las copias de seguridad.

Nota: hay que tener en cuenta que no existe sistema 100% seguro, sino que se trata de tener la máxima seguridad posible.(Escartín, 2005)**,** (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Villalon, 2006)

1.2 Defensa en profundidad.

Defensa en profundidad (*Defense in Depth*) es una iniciativa que pretende aislar en capas y dividir en diferentes áreas las instalaciones con el propósito de hacer más difícil el acceso al último bastión, es decir, los servidores donde se encuentra la información. (La defensa en profundidad aplicada a los sistemas de información, 2006), (Borghello, Linux Máxima seguridad, 2005).

La defensa en profundidad del sistema de información es una defensa global y dinámica, que coordina varias líneas de defensa que cubren toda la profundidad del sistema, sus funciones pueden observarse en la Tabla 1.1. El término profundidad debe entenderse en su sentido más amplio, es decir, en la organización del Sistema de Información (SI), en su implementación y, por último, en las tecnologías utilizadas. Se trata, por lo tanto, de permitir acciones de neutralización de los atentados contra la seguridad, al menor costo, mediante la gestión de los riesgos, un sistema de informes, la planificación de las reacciones y el enriquecimiento permanente gracias a la experiencia adquirida. Esta defensa en profundidad tiene una doble finalidad:

1. Reforzar la protección del sistema de información mediante un enfoque cualitativo que permita verificar la finalización y la calidad del dispositivo
2. Brindar un medio de comunicación que permita a los responsables de la toma de decisiones y a los usuarios tomar conciencia de la gravedad de los incidentes de seguridad. (La defensa en profundidad aplicada a los sistemas de información, 2006), (Borghello, Linux Máxima seguridad, 2005)

Tabla 1.1: Funciones de la Defensa en Profundidad.

Fuente: Autor

Función	Naturaleza
Globalidad	**La defensa debe ser global, lo que significa que engloba todas las dimensiones del sistema de información:** a) Aspectos organizacionales; b) aspectos técnicos; c) aspectos de implementación.
Coordinación	**La defensa debe ser coordinada, lo que significa que los medios implementados actúan:** a) gracias a una capacidad de alerta y difusión; b) tras una correlación de los incidentes.
Dinamismo	**La defensa debe ser dinámica, lo que significa que el SI dispone de una política de seguridad que identifica**: a) Una capacidad de reacción; b) una planificación de las acciones; c) una escala de gravedad.
Suficiencia	**La defensa debe ser suficiente, lo que significa que cada medio de protección (organizacional o técnico) debe contar con:** a) Una protección propia; b) un medio de detección; c) procedimientos de reacción.
Exhaustividad	**La defensa debe ser completa, lo que significa que:** a) Los bienes que deben protegerse se protegen en función de su criticidad; b) que cada uno de ellos está protegido, como mínimo, por tres líneas de defensa; c) se formaliza la difusión de la experiencia adquirida.

Demostración	**La defensa debe ser demostrada, lo que significa que:** a) Se califica a la defensa; b) existe una estrategia de homologación; c) la homologación acompaña al ciclo de vida del sistema de información.

1.2.1 Método para la defensa en profundidad.

El método permite al diseñador del proyecto integrar los principios de la defensa en profundidad. Aporta, en particular, la posibilidad de calificar un sistema y, en cierta forma, de medir su nivel de defensa. La clasificación por etapas, se puede definir dela siguiente forma:

1. Determinación de los bienes y de los objetivos de seguridad.
   Este está comprendido en la determinación de los bienes a defender y su criticidad, lo que permitirá realizar un análisis del valor de la seguridad.
2. Arquitectura general del sistema.
   Esta etapa apunta a determinar la profundidad del dispositivo y a realizar elecciones en cuanto a las organizaciones, las tecnologías y los procedimientos de seguridad.
3. Elaboración de la política de defensa.
   Esta etapa está compuesta por dos subetapas, la determinación de la defensa global y coordinada y la planificación. La defensa global viene determinada por algunos aspectos de seguridad como la protección la reacción y la detección, y la planificación por la determinación de nuevas configuraciones de red, la utilización de medios de respaldo, etc.
4. Clasificación de la defensa en profundidad.
   En esta etapa se trata de llevar a cabo la calificación del sistema, que resulta de dos enfoques: el primero es cualitativo mientras que el segundo es demostrativo y se lleva a cabo mediante el estudio de las situaciones aplicables.
   El enfoque cualitativo apunta a verificar el cumplimiento de los principios de la defensa en profundidad y el segundo enfoque se basa en los resultados producidos a lo largo de las distintas etapas.

5. Evaluación permanente y periódica.
   Como el nombre lo indica, se basa en la evaluación permanente y periódica del sistema, es decir, de forma sistemática.(La defensa en profundidad aplicada a los sistemas de información, 2006), (Borghello, Linux Máxima seguridad, 2005)

1.3 Políticas de seguridad.

Las políticas de seguridad surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de información. Esta es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales, que está o no está permitido en el sistema.(Escartín, 2005), (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Ardita, 2010), (Borghello, Linux Máxima seguridad, 2005).

La seguridad Informática no tiene una solución definitiva (no es al 100%), sino que es y será el resultado de la innovación tecnológica, a la par del avance tecnológico, por parte de aquellos que son responsables por los sistemas.

Todo esto porque a la hora de crear políticas de seguridad hay que enmarcarse a las condiciones reales del sistema sobre el cuál se trabaja. No se puede aplicar la misma política en Europa que en América, las condiciones reales son muy distintas. Ese fue tan solo un ejemplo, otro pudiera ser, una empresa con un gran comercio de sus productos, dependiente de las redes de datos y una escuela que tan solo necesita información para el desarrollo de los estudiantes.

Como ya se menciona, la política de seguridad es una serie de normas y medidas a seguir para mantener la seguridad del sistema. Pero ante todo esto es una forma de comunicarse con los usuarios. Siempre hay que tener en cuenta que la seguridad comienza y termina con las personas.

Cualquier política de seguridad ha de contemplar los elementos claves de la seguridad: Integridad, disponibilidad, privacidad, control, autenticidad y utilidad.

No debe tratarse nunca de una descripción técnica de mecanismos de seguridad sin utilidad alguna, ni una expresión legal que involucre sanciones a la conducta de los empleados. Es más bien una descripción de lo que desea proteger y el porqué de ello.(Escartín, 2005)**,** (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Ardita, 2010)**,** (Borghello, Linux Máxima seguridad, 2005)**.**

1.4 Hacking Ético.

Este tema consiste en descubrir las deficiencias relativas a seguridad y vulnerabilidades de los sistemas informáticos, analizarlas y calibrar su grado de riesgo y peligrosidad y recomendar las soluciones más apropiadas para cada una de ellas. (Escartín, 2005)

Un proyecto de este tipo consiste en la penetración a un sistema informático de una empresa de forma controlada, de la misma forma que lo haría un hacker o pirata informático, pero de forma ética, con previa autorización. El resultado es un informe sobre los sistemas a los cuales se ha logrado penetrar y la información secreta conseguida.(Escartín, 2005)

Existen diferentes tipos de Hacking Ético:

- Hacking Ético Externo Caja Blanca: Para este caso se facilita información para poder realizar la intrusión. Se analiza en profundidad y extensión todas las posibles brechas de seguridad al alcance de un atacante de los sistemas de comunicaciones sometidos a estudios. El resultado es un informe amplio de vulnerabilidades así como las recomendaciones para eliminar cada una de ellas.
- Hacking Ético Externo Caja Negra: Se realiza idénticamente igual al anterior, con la diferencia de que no se da información para la realización de la intrusión.
- Hacking Ético Interno: El ámbito de esta auditoría es la red interna de la empresa, para hacer frente a las amenazas de intrusión interna. Para esto es

necesaria la presencia del especialista en las instalaciones de la empresa ala cual se va a auditar. El resultado es un informe con los resultados obtenidos.

- Hacking Ético de Aplicaciones Web: Se simulan los intentos de ataques reales a las vulnerabilidades de una o varias aplicaciones determinadas, en las que se pueden encontrar, Sistemas de Comercio Electrónico, Sistemas de Información o Sistemas de Bases de datos. Al igual que en los casos anteriores, se realiza un informe con las incidencias recogidas.
- Hacking Ético de Sistemas de Comunicaciones: En esta auditoría se analiza la seguridad de las comunicaciones tales como, en las redes de datos, hardware de red, comunicaciones de voz, acceso no autorizado a Internet, redes de transmisión de datos por radio, etc.
- Hacking Ético de VoIP: Las empresas que están migrando a telefonía de VoIP por las múltiples ventajas que ofrece no deberían ignorar los riesgos de seguridad que aparecen cuando se migra las redes de datos. Los ataques que pueden sufrir estos sistemas son muchos. Al mismo tiempo, al modificar las redes de datos para brindar el servicio de VoIP, se pueden estar abriendo inadvertidamente vías de ataques a estos sistemas. Mediante los servicios de Hacking Ético de VoIP se pueden verificar las brechas de seguridad y dar solución a estos tipos de problemas.(Escartín, 2005), (Ardita, 2010), (Borghello, Linux Máxima seguridad, 2005).

1.5 Sistemas de detección de intrusos (IDS).

Un sistema de detección de intrusos o IDS (*Intrusion Detection System*) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers que usan herramientas automáticas.(Borghello, Linux Máxima seguridad, 2005).

El IDS suele tener sensores virtuales, por ejemplo, un *sniffer* de red con los que el núcleo del IDS puede obtener datos externos, generalmente sobre el tráfico de red. El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.(Ardita, 2010), (Chacón, 2009).

1.5.1 Funcionamiento de un IDS.

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Ardita, 2010), (Villalon, 2006), (Chacón, 2009).

Normalmente esta herramienta se integra con un firewall. El detector de intrusos es incapaz de detener los ataques por sí solo, excepto los que trabajan conjuntamente en un dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

Los IDS suelen disponer de una base de datos de (firmas) de ataques conocidos.Dichas firmas permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento, y entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.(Cristian, Seguridad Informática, sus implicaciones e implementación, 2008), (Ardita, 2010), (Villalon, 2006), (Chacón, 2009).

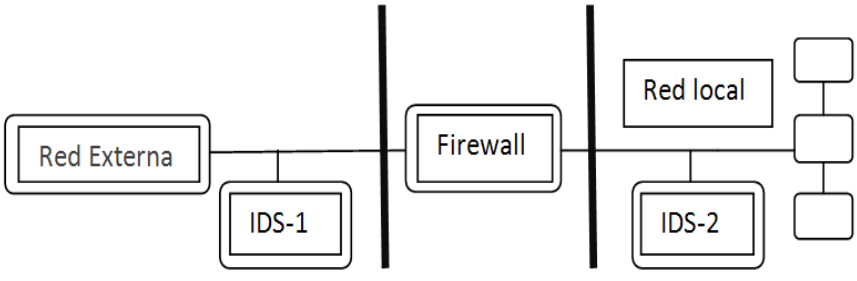

Figura 1.1: Ubicación de los IDS en la red.

Fuente:(Chacón, 2009)

1.5.2 Tipos de Sistemas de Detección de Intrusos.

Existen tres tipos de sistemas de detección de intrusos:

HIDS (HostIDS): el principio de funcionamiento de un HIDS, depende del éxito de los intrusos, que generalmente dejarán rastros de sus actividades en el equipo atacado, cuando intentan adueñarse del mismo, con propósito de llevar a cabo otras actividades.El HIDS intenta detectar tales modificaciones en el equipo afectado, y hacer un reporte de sus conclusiones.(Chacón, 2009)

NIDS (NetworkIDS): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.

DIDS (DistributedIDS): sistema basado en la arquitectura cliente-servidor compuesto por una serie de NIDS (IDS de redes) que actúan como sensores centralizando la información de posibles ataques en una unidad central que puede almacenar o recuperar los datos de una base de datos centralizada. La ventaja es que en cada NIDS se puede fijar unas reglas de control especializándose para cada segmento de red. Es la estructura habitual en redes privadas virtuales (VPN).(Chacón, 2009)

1.5.3 Detección de intrusos en tiempo real.

La seguridad se tiene que tratar en conjunto. Este viejo concepto es el que recuerda que si los sistemas son bien eficaces distan mucho de ser la protección ideal. De esta manera debe estar fuera de discusión la conveniencia de añadir elementos que controlen lo que ocurre dentro de la red(detrás de los Firewall).(Chacón, 2009), (Borghello, Linux Máxima seguridad, 2005).

Una de las formas de aplicación de esto son los IDSen tiempo real, los cuales:

- Monitorean el flujoen la red para determinarpotenciales ataques.

- Evalúan el peligro de las computadoras para determinar actos sospechosos.
- Conservan una base de datos con la situación precisa de los ficheros del sistema para determinar los cambios ocurridos.
- Controlan el núcleo del Sistema Operativo para detectar posibles infiltraciones en él.
- Avisan al administrador todo tipo de acciones malignas o amenazas.

Cada una de estas herramientas mantiene alejados a la mayoría de los intrusos normales. Otros con mayor experiencia y conocimiento pueden intentar voltear la seguridad de los sistemas, los cuales hay que estudiarlos para integrar una mejor política de seguridad. (Chacón, 2009), (Borghello, Linux Máxima seguridad, 2005).

1.5.4Sistemas de Prevención de Intrusos.

Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos. También es importante destacar que los IPS pueden actuar al nivel de equipo, para combatir actividades potencialmente maliciosas.(Borghello, Linux Máxima seguridad, 2005).

Un Sistema de Prevención de Intrusos, al igual que un Sistema de Detección de Intrusos, funciona por medio de módulos, pero la diferencia es que este último alerta al administrador ante la detección de un posible intruso (usuario que activó algún Sensor), mientras que un Sistema de Prevención de Intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque; se podría decir que un IPS protege al equipo

proactivamente y un IDS lo protege reactivamente.(Borghello, Linux Máxima seguridad, 2005).

1.6 Visión general de la seguridad en Sistemas de código abierto.

La seguridad es un tema amplio y sobre el cual hay que tomar el máximo de consideraciones para lograr tener un sistema lo más seguro y protegido posible. Seis de estas consideraciones de la arquitectura de seguridad de Linux son:

1. Cuentas de usuario.
2. Control de cuentas discrecional.
3. Control de acceso a la red.
4. Cifrado.
5. Conexión.
6. Detección de intrusos.

Todos estos mecanismos forman los componentes individuales de la compleja arquitectura de la seguridad de Linux. Uno a uno es posible que no parezcan tan extraordinarios, pero cuando se utilizan de forma compuesta constituyen un exhaustivo método global en lo relativo a la seguridad de redes. (***Ver Figura 1.2)***(Escartín, 2005), (Linux Security HOWTO, 2006), (Barrios, 2006), (Villalon, 2006)

1.6.1 Cuentas de usuario

En Linux, toda la potencia administrativa se confiere a una sola cuenta llamada root, que es el equivalente al Administrador de Windows. Con esta cuenta se controla todo, incluyendo, las cuentas de usuarios, los archivos y directorios y recursos de la red.

La cuenta *root* permite realizar cambios masivos en todos los recursos o cambios específicos en unos pocos. Esto ocurre así porque cada cuenta es una entidad independiente con un nombre, una contraseña y derechos de accesibilidad

independiente, lo que permite otorgar o denegar acceso a cualquier usuario, combinación de usuarios o a todos los usuarios. (***Ver Figura 1.3)***

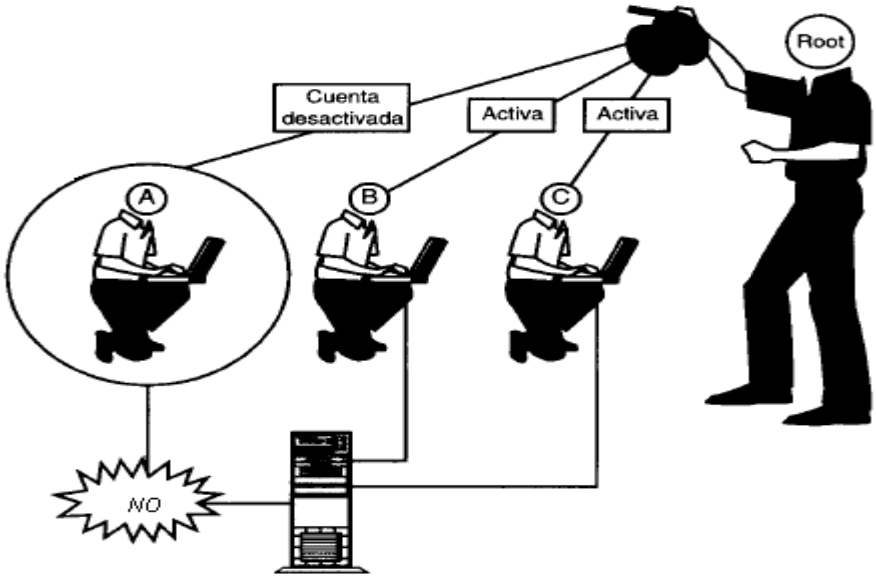

Figura 1.2: Control de root sobre cuentas de usuarios.

Fuente:(Linux Security HOWTO, 2006)

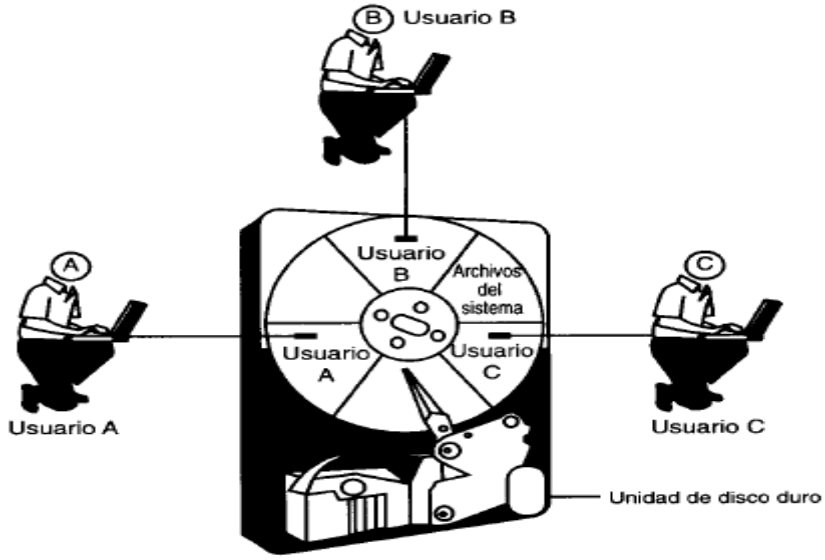

Figura 1.3: Distribución de los usuarios y a los archivos del sistema en el disco duro.

Fuente:(Linux Security HOWTO, 2006)

Como en todo sistema a medida que aumentan la cantidad de usuarios aumenta la complejidad ya que los usuarios generan sus propios archivos e instalan sus propios programas. Linux resuelve esto manteniendo aislados los directorios de los usuarios. Cada usuario recibe un directorio principal y un espacio en disco. Estas áreas son independientes del área del sistema y de las que ocupan los demás usuarios. Con esto se evita que las actividades de los usuarios afecten al sistema de archivos además de proporcionar privacidad. Ya que cada usuario tiene su propia cuenta, su propio espacio en disco sin que los demás lo interfieran o accedan a sus dominios.(***Ver Figura 1.4).***

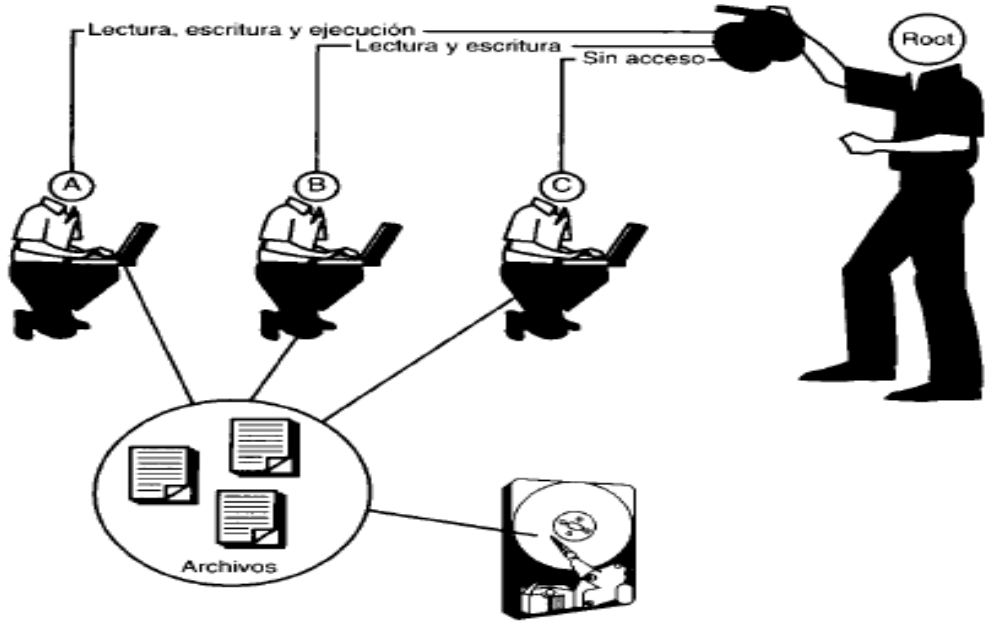

Figura 1.4: Control de privilegios a los usuarios.

Fuente:(Linux Security HOWTO, 2006)

Root además de controlar a los usuarios, también controla el lugar donde tienen almacenados sus archivos. Pero más que eso, controla a que recursos pueden acceder los usuarios y como se manifiesta dicho acceso. (Escartín, 2005), (Linux Security HOWTO, 2006), (Barrios, 2006), (Villalon, 2006).

1.6.2 Control de Acceso Discrecional (DAC).

Un tema central de Linux es el Control de Acceso Discrecional (DAC), Que permite controlar el grado de accesibilidad de los usuarios a los diferentes archivos y directorios.

Es decir, es posible declarar con exactitud la forma en que los usuarios acceden a los archivos.

Un ejemplo de esto es que un usuario tiene acceso a la escritura, lectura y ejecución, mientras que otro solamente tiene privilegios de lectura y escritura, y un tercero sin acceso a algún tipo de beneficio.

Dado que a menudo las organizaciones se dividen en departamentos y que varios usuarios de dichos departamentos tengan acceso a los mismos archivos, Linux permite agrupar a los usuarios. De esta forma cuando se definen permisos para determinados archivos y directorios, no es necesario hacerlo para todos y cada uno de los usuarios. En la mayoría de los casos cabe la posibilidad de definirlos por grupos. (***Ver Figura 1.5)***

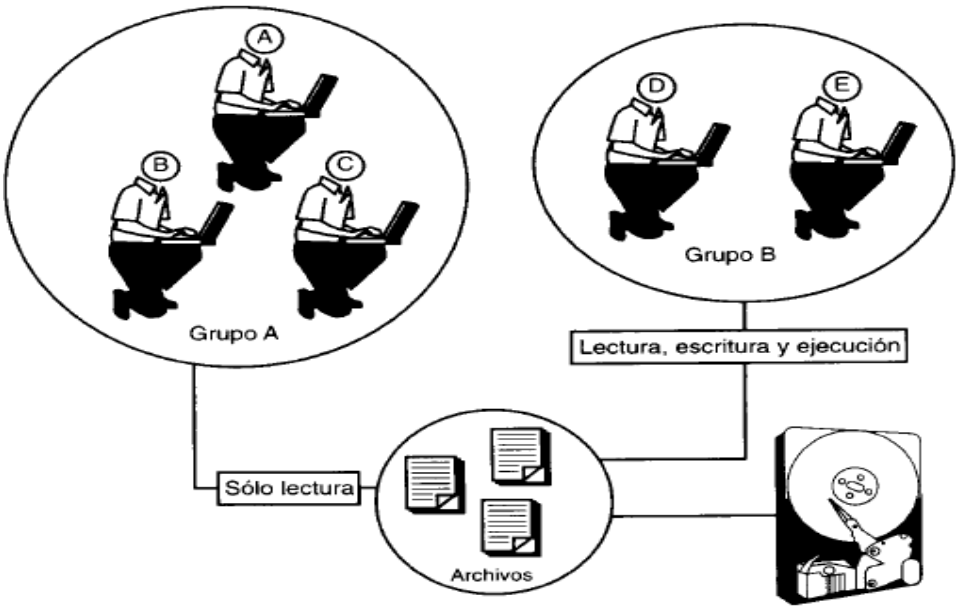

Figura 1.5: Accesos para diferentes grupos de usuarios.

Fuente:(Linux Security HOWTO, 2006)

De esta manera existen un conjunto de usuarios con privilegios de solo lectura mientras que un segundo grupo tienen acceso a la lectura, escritura y ejecución de funciones con respecto a los archivos. Dicha gestión a nivel de grupo resulta muy útil cuando hay muchos usuarios y varios subconjuntos de usuarios que necesitan privilegios idénticos o

parecidos. (Escartín, 2005), (Linux Security HOWTO, 2006), (Barrios, 2006), (Villalon, 2006).

1.6.3 Control de Acceso a la red.

El Sistema Operativo Linux también proporciona control de acceso a la red o la capacidad de permitir a los usuarios y *host* conectarse entre sí. Para esto es posible implantar reglas de acceso a la red muy refinadas.

Esta funcionalidad viene muy bien en los entornos de red o cuando el sistema Linux es un servidor de Internet. Por ejemplo, permite mantener solamente un servidor Web para los clientes de pago. La protección mediante contraseñas es una buena posibilidad, pero si se quiere mejor la seguridad lo mejor es que no se le permita la conexión a los *host* no autorizados. En Linux muchos servicios de red ofrecen esta función. (***Ver Figura 1.6).***(Escartín, 2005)**,** (Linux Security HOWTO, 2006)**,** (Barrios, 2006)**,** (Villalon, 2006)**.**

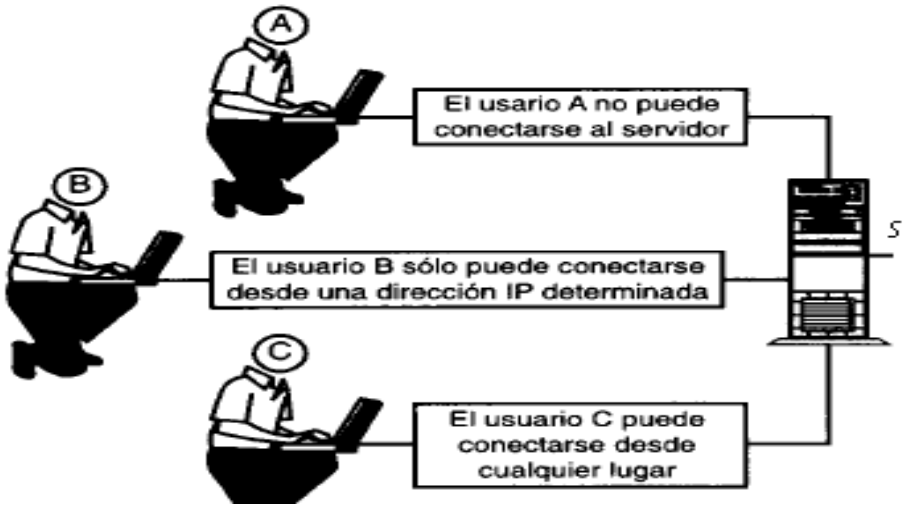

Figura 1.6: Conexiones autorizadas.

Fuente:(Linux Security HOWTO, 2006)

1.6.4 El cifrado.

El cifrado es el proceso de mezclar los datos para que no puedan leerlos los que no tengan autorización para ello. En la mayoría de los esquemas de cifrado es necesario tener una contraseña para organizar los datos de forma que puedan leerse. Este método se utiliza principalmente para mejorar la privacidad o la protección de datos importantes.

Linux ofrece varias opciones de cifrado punto a punto para proteger los datos que circulan. Habitualmente cuando se transmiten datos a través de Internet, atraviesan muchos *gateways*, los cuales en su camino,son vulnerables a escuchas. Linux cuenta con varias utilidades complementarias que permiten cifrar o codificar, para que si alguien los captura, solo vea una sintaxis de símbolos sin sentido e ininteligible. (Escartín, 2005), (Linux Security HOWTO, 2006), (Barrios, 2006), (Villalon, 2006).

1.6.5 La conexión.

Aunque se apliquen todos los controles de seguridad disponibles, en ocasiones se encuentran puntos vulnerables. Los intrusos rápidamente sacan partido de estas oportunidades mediante el ataque al mayor número de máquinas posible antes de que se arregle el agujero. Linux no puede predecir cuándo va sufrir algún ataque a un *host*, pero puede registrar el movimiento de la persona que realizó dicho ataque.(***Ver Figura 1.7).***

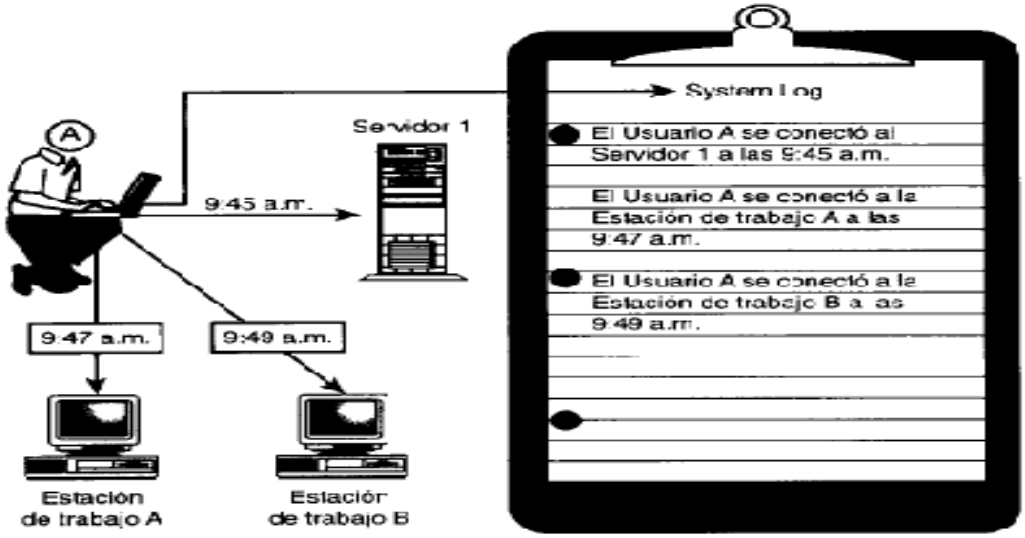

Figura 1.7: Registro de conexión.

Fuente:(Linux Security HOWTO, 2006)

Linux tiene exhaustivas capacidades de registro. Se detectará, marcará la hora y grabará las conexiones de la red. Esta información se redirige a los registros para su posterior análisis.

La capacidad de registro es un componente vital de la arquitectura de seguridad de Linux y proporciona la única evidencia real de que se ha producido un ataque.

Como existen un gran número de metodologías de ataques distintas, Linux graba registros a nivel de red, de *host* y de usuario.

Las funciones que realiza el Sistema Operativo son:

1. Registra todos los mensajes del sistema y del núcleo.
2. Registra todas las conexiones de la red, la dirección IP de donde parte cada una de ellas, su longitud y, en alguno de los casos el nombre de usuario y sistema operativo de la persona que realiza el ataque.
3. Registra los archivos que solicitan los usuarios remotos.
4. Puede registrar que procesos se encuentran bajo el control de cualquier usuario.
5. Puede registrar todos y cada uno de los comandos que ha emitido un usuario determinado.(Escartín, 2005)**,** (Linux Security HOWTO, 2006)**,** (Barrios, 2006)**,** (Villalon, 2006)**.**

1.7 Ubicación del servidor y el acceso físico a él.

Los aspectos más importantes para este tópico son, la disposición física del servidor, es decir el lugar donde se encuentre, y las personas que tienen acceso a él. Si múltiples usuarios tienen acceso a los servidores los controles de seguridad son inútiles.(Escartín, 2005)

Desde luego, un ataque puede significar muchas cosas en este contexto. Si por tan solo se dejara un usuario malintencionado por unos minutos en el local de servidores, es muy probable de que estos sufran daños significativos en ese intervalo de tiempo. El usuario podría realizar un rudimentario ataque de denegación de servicio desconectando cables, desconectando hardware de la red o reiniciando los servidores.(Villalon, 2006)

La mayor preocupación de estos actos son con los usuarios internos, y principalmente aquellos que tienen acceso de alguna forma a los servidores. Se ha estimado que el 80 % de los ataques provienen de personal interno al sistema. La cuestión es que este personal tiene acceso a información que los usuarios externos no tienen.

Pero esta no es la única ventaja de este personal. La confianza es otra ventaja potencial. Usualmente en las empresas el personal de confianza deambula por los pasillos y departamentos por lo que se hace muy difícil en este tipo de casos tener una máxima protección con respecto al personal interno.(Escartín, 2005)(Ardita, 2010)

Las agencias gubernamentales y los proveedores de servicios de Internet tienen una vasta experiencia en esta materia y merece la pena seguir su ejemplo. Se debe planificar un centro de operaciones de la red (NOC). (Escartín, 2005), (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Borghello, Linux Máxima seguridad, 2005), (Guia avanzada redes Linux con TCP/IP, 2004)

Un NOC es un área restringida donde se encuentran los servidores. Estos suelen estar asegurados con pernos fijados a bastidores o asegurados de alguna otra forma junto con el hardware de la red. Idealmente un NOC debería estar en un lugar donde tuviesen acceso pocas personas y éstas autorizadas por claves. Un buen ejemplo de claves es el uso de tarjetas de acceso y la firma del personal que entra y sale para tener constancia de su estancia física en el local.(Escartín, 2005), (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Borghello, Linux Máxima seguridad, 2005), (Guia avanzada redes Linux con TCP/IP, 2004).

El NOC requiere algunos requisitos para su establecimiento:

- Debe encontrarse en otro espacio de la oficina alejado del público; es preferible que no se encuentre en la planta baja.
- La sala y los pasillos que conducen a ella deben ser totalmente opacos: sin puertas de cristal.
- Las puertas de acceso deben tener un blindaje. Esto evita que fuercen la cerradura.
- Mantener los dispositivos de almacenamiento en un lugar seguro, y si se puede distinto.

Además como políticas de seguridad del sistema se debe promulgar estrictas normas escritas para los encargados del trabajo en el Centro de Operaciones y los usuarios. (Escartín, 2005), (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Borghello, Linux Máxima seguridad, 2005), (Guia avanzada redes Linux con TCP/IP, 2004)

1.8 Amenazas Lógicas.

Si se extrapola el concepto de entropía (en la química es el nivel de desorden de las partículas) a la seguridad, según los físicos todo sistema tiene una máxima entropía, resultaría que todo sistema tiende a su máxima inseguridad. Este principio supone decir que:(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Borghello, Linux Máxima seguridad, 2005)

- Existen agujeros en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.

Estos son solo algunos puntos de una lista que puede tener más que estos.

1.9.2 Identificación de las amenazas.

La identificación requiere conocer el tipo de ataque, el tipo de acceso, la forma operacional, y el objetivo del atacante. Las consecuencias podrían ser:

- La información que no contenía defectos pasa a tenerlas.
- Servicios que deberían estar disponibles no lo están.
- Los datos llegan a destinos erróneos.

Cualquier principiante sin tener grandes conocimientos pero con una potente herramienta de ataque, es capaz de dejar fuera de servicio a cualquier servidor de información de Internet, simplemente siguiendo las instrucciones de dicha herramienta.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Borghello, Linux Máxima seguridad, 2005)

1.9.3 Tipos de ataques.

Existen diferentes tipos de ataques perpetrados principalmente por hackers. Estos pueden ser realizados sobre cualquier tipio de red o sistema operativo utilizando diferentes medios:

- Caballos de Troya.
- Bombas de tiempo.
- Escáner.
- Puertas traseras.

Estos son solo algunos de una enorme lista de tipos de ataques, lo que es solo una idea de la cantidad y variabilidades existentes.

Otros tipos de ataques son los llamados *Ataques Remotos,* definido como el ataque iniciado por el atacante pero sin control físico de la víctima.

Varios de estos ataques son los mostrados a continuación:

- Ingeniería social.

Es la manipulación de las personas para convencerlas de ejecutar acciones o actos que normalmente no realizan para que revele todo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia necesaria, puede engañar fácilmente a un usuario en beneficio propio. Esta técnica es una de las más usadas y efectivas.

- Ataques de monitorización.

Consiste en espiar físicamente a los usuarios para obtener su *login* y *password* correspondiente. Este ataque también llamado *surfing* explota el error de los usuarios de dejar su *login* y *password* anotados cerca de la computadora. Otra vía es observar al usuario cuando teclea su *login* y *password*.

- El escanear conexiones TCP.

Esta es la forma básica de escanear puertos TCP. Si el puerto está escuchando enviará una respuesta de éxito: cualquier otro caso será que el puerto no está abierto o no puede establecer conexión con él.Este método tiene como desventaja que es fácilmente detectado por los administradores del sistema.

Existen otras formas de ataque como TCP SYN *Scanning*, *SnoopingDownloading*, por tan solo mencionar algunos.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Borghello, Linux Máxima seguridad, 2005)

1.9.4 Ataques de autentificación.

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y *password*. (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Borghello, Linux Máxima seguridad, 2005)

Entre estos están:

- *Spoofing Looping*: Lo cual puede traducirse como hacerse pasar por otro, y el objetivo está en hacerse pasar por otro usuario. Esto se usa mucho para tener acceso a un sistema y luego tener acceso a otro.
- *Spoofing*: este tipo de ataque suele implicar un buen conocimiento del protocolo en que se va a basar el ataque. Los ataques tipo *Spoofing* son básicamente conocidos como IP *Spoofing*, DNS *Spoofing*.
- IP *Ppoofing*: Con el IP *Spoofing* el atacante genera paquetes de Internet con una dirección de red falsa, pero que es aceptada por el destinatario. Su utilización más común es mandar los paquetes con una dirección de un tercero, de forma que la víctima ve un ataque de la red del tercero y no de la dirección real del intruso, un ejemplo de este caso se observa en la figura 1.8.

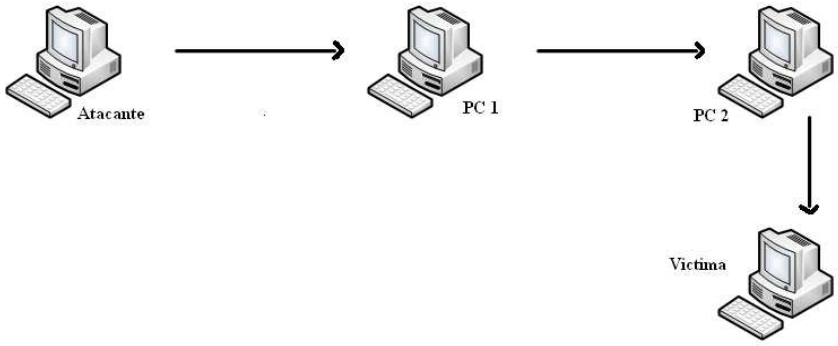

Figura 1.8: Ataque IP Spoofing.

Fuente:(Borghello, Seguridad Informática, sus implicaciones e implementación, 2008)

De esta manera la víctima nunca verá realmente de donde proviene el ataque. En la figura 1.2 se puede observar que la víctima si descubre el ataque solo podrá ver su origen desde la PC 2.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Borghello, Linux Máxima seguridad, 2005)

- Utilización de puertas traseras: Según el autor (Velasquez, 2011) sobre este aspecto, dice, las puertas traseras son trozos de código de un programa que permite a quien las conoce saltarse los métodos usuales de autenticación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar códigos en la fase de desarrollo.Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o

intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Borghello, Linux Máxima seguridad, 2005)**,** (Ramos, 2011)

- Uso de diccionarios: Los diccionarios son archivos con millones de palabras, las cuales pueden ser posibles *passwords* de los usuarios. Este archivo es utilizado para descubrir *passwords* de usuarios en pruebas de fuerza bruta. El programa encargado de probar cada una de estas palabras enmascara cada una de ellas mediante el algoritmo utilizado por el sistema atacado, y compara la palabra encriptada contra el archivo de *passwords* del sistema atacado (previamente obtenido). Si coinciden, entonces se ha encontrado la clave de acceso al sistema, mediante el usuario correspondiente de la clave hallada.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Borghello, Linux Máxima seguridad, 2005)

1.10 Administración de la seguridad.

Es posible dividir esta tarea en tres grupos:

- Autenticación: Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.
- Autorización: Es que el hecho de que las entidades que pueden tener acceso a los recursos de cómputo, lo tengan únicamente a las áreas de trabajo sobre las cuales ellas deben de tener dominio.
- Auditoria: Se refiere a la continua vigilancia de los servicios en producción. Entran en este grupo los inventarios de ingreso, de utilización y estrategias de entrada física a los medios.

Por regla general, las políticas son el primer paso de que dispone una organización para entrar en un ambiente de seguridad, puesto que reflejan su voluntad de hacer algo que permita detener un posible ataque antes de que este suceda. Esta es la llamada

proactividad.(Escartín, 2005)**,** (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Ardita, 2010)

Ejemplos de algunos métodos de seguridad:

1. Métodos de localización de extraños: según el autor de la página en línea http://ozdox.blogspot.com/, señala que se, permiten evaluar los archivos de las técnicas de investigación de esquemas de procedimiento o sucesos consideradosdudosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.
2. Métodosdirigidos a enlace de red: supervisan los enlaces que se trata de implantar en una red o dispositivo específico, siendo capaces de efectuar una acción sobre la base de parámetros como: origen y destino de la conexión, servicios solicitados, permisos, etc. Las acciones que pueden emprender pueden ir desde el rechazo de la conexión hasta el aviso al administrador. En esta categoría están los cortafuegos (*Firewalls*) y los *Wrappers*.
3. Sistemas de análisis de vulnerabilidades: Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La desventaja de estos sistemas es que lo pueden usar tanto personas autorizadas como aquellos que buscan acceso no autorizado al sistema.
4. Método de defensa de los datos: Son los que con claves o adiciones de confirmaciónpretenden certificar que no hay variacionesno deseadas en los datos a defender.
5. Método de defensa de la confidencialidad de los datos: instrumentos que usan claves para garantizar que los datos solo sonevidentes para alguienpermitido. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades. En los ejemplos de estas se pueden citar a *Pretty Good Privacy* (PGP), *Secure Sockets Layer* (SSL).

Un estándar de protecciónntiene que incluirvariadoselementos que puedan agregarsegradualmente al estándargeneral de la entidad.(Escartín, 2005)**,** (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Ardita, 2010)

1.11 Cortafuegos (*Firewalls*).

Uno de los elementos de más publicidad sin duda son los *Cortafuegos*. Aunque deben ser uno de los sistemas a los que más hay que prestarle atención, distan mucho de ser la solución real de los problemas de seguridad. De hecho estos elementos no tienen nada que hacer con técnicas como la ingeniería social.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Borghello, Linux Máxima seguridad, 2005)**,** (Guia avanzada redes Linux con TCP/IP, 2004)**,** (Ramos, 2011)

El Cortafuegos es un método o grupo de aquellos localizado entre dos mallas y que ejecuta una estrategia de protecciónінstaurada. Es el componentecuya función es resguardar una red segura de otra que no lo es,por ejemplo Internet.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Borghello, Linux Máxima seguridad, 2005)**,** (Ramos, 2011)**,** (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

Puede incluir diferentes elementos para alcanzar metas como:

1. Todo el flujo saliente y entrante tiene que pasar por él.
2. Únicamente el flujopermitido, establecido por la estrategiaespecífica de protección es autorizado.

Un ejemplo se muestra en la figura 1.9.

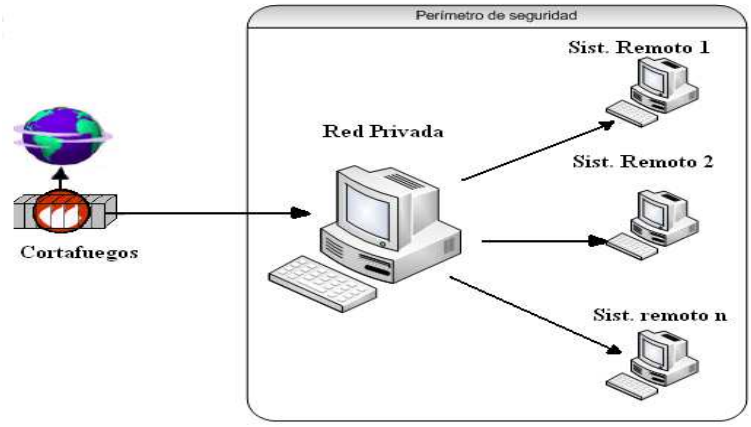

Figura 1.9: Estructura del Firewall (Cortafuegos).

Fuente:(Borghello, Seguridad Informática, sus implicaciones e implementación, 2008)

Algunos Firewall aprovechan la capacidad de que toda la información entre y salga por ellos para proveer servicios de seguridad adicionales, en los que están, la encriptación del tráfico de la red. Se entiende de que si el Cortafuegos está en el medio de dos redes, ambos lados deben hablar el mismo método de encriptación-desencriptación para entablar la comunicación. (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Ramos, 2011), (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

1.12 Tipos de Cortafuegos (*Firewalls*).

Existen varios tipos de cortafuegos (*firewall*), con características particulares según su función en la red. Pueden ser de filtrado de paquetes, de establecimiento de conexión o con los dos funcionamientos implícitos.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)

1.12.1 Filtrado de paquetes:

Se emplean filtros y normas fundamentadas en estrategias de registro de ingreso. El enrutadorfiltra los paquetes de acuerdo a los siguientes parámetros:

- Estándares empleados.
- Dirección IP de inicio y fin.
- Terminal TCP-UDP de inicio y fin.

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico. Restringiendo las comunicaciones entre dos computadoras (mediante direcciones IP) se permite establecer entre cuáles máquinas la comunicación está establecida(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Ramos, 2011)**,** (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

La filtración de paquetes por terminales y estándares, admitedeterminarlos servicios accesibles a los usuarios y en que terminales. Se puede establecer la navegación en la WWW (puerto 80 abierto), pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Ramos, 2011)**,** (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

Este tipo de aplicación tiene varias ventajas como la de ser económico, tener alto grado de desempeño y ser transparente a los usuarios conectados a la red. Pero como todo, también tiene sus desventajas:

- No son capaces de esconder la topología de las redes privadas, por lo que exponen las redes al entorno.
- La amplitud de sus auditoríaspueden ser delimitadas, así como los datos de acciones.

No sustentan estrategias de proteccióncomplicadas como certificación de usuarios y examen de ingresos con indicadoresdeterminados.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Ramos, 2011)**,** (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

1.12.2 Proxy-*Gateways* de utilidades:

Una forma de impedir las vulnerabilidades de la filtración de paquetes son los programas de aplicación para filtrar los enlaces. Estas utilidades se denominan*Servidores Proxy* y elequipoen que se hacees el *Gateway* de utilidad.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Ramos, 2011)**,** (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

El Proxy actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

Cuando un usuario desea algún servicio, lo hace a través del Proxy. Este realiza el pedido al servidor real y devuelve los resultados al cliente. Su función es la de analizar el tráfico de la red en busca de contenido que viole la seguridad de la misma. **Ver*Figura 1.10.***(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Ramos, 2011)**,** (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

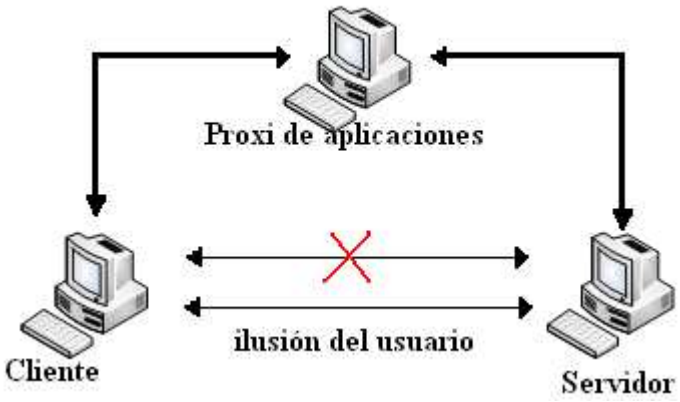

Figura 1.10: Servidor Proxy.

Fuente:(Borghello, Seguridad Informática, sus implicaciones e implementación, 2008)

1.12.3 Proxy de aplicaciones con el reenvío de paquetes desactivado(*Dual-Homed Host*).

Son equiposenlazados a los dos ámbitos (interno y externo) y no permiten el flujo de paquetes IP (como en la filtración de paquetes), es decir que opera con el IP-*Forwarding*inactivo.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Ramos, 2011)

Un usuario interior que desee hacer uso de un servidor exterior, deberá conectarse primeramente al *Firewall*, donde el *Proxy* entenderá su petición, y en función de la configuración impuesta en dicho *Firewall*, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Ramos, 2011)

Es decir que se utilizarán dos conexiones. Uno desde la máquina interior hasta el *Firewall* y el otro desde estahasta la máquina que albergue el servicio exterior. ***Ver Figura 1.11.***(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Ramos, 2011)**,** (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

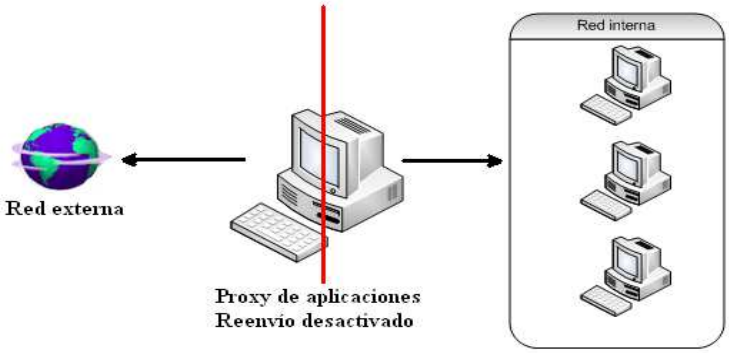

Figura 1.11: Reenvío de paquetes desactivado.

Fuente:(Borghello, Seguridad Informática, sus implicaciones e implementación, 2008)

1.12.5 *Iptables*.

Según el autor(Lopez, 2013) del artículo de "Gestión de redes de datos", comenta que, el *Netfilter* es un *framework* disponible en el núcleo Linux que permite interceptar y manipular paquetes de red. Dicho *framework* permite realizar el manejo de paquetes en diferentes estados del procesamiento. *Netfilter* es también el nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para cortafuegos basados en Linux.El componente más popular construido sobre *Netfilter* es*iptables*, una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para Ipv4 o mantener registros de log. El proyecto *Netfilter* no sólo ofrece componentes disponibles como módulos del núcleo sino que también ofrece herramientas de espacio de usuario y librerías. (Escartín, 2005), (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Ramos, 2011), (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

Iptables es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red. El nombre *iptables* se utiliza frecuentemente de forma errónea para referirse a toda la infraestructura ofrecida por el proyecto *Netfilter*. Sin embargo, el proyecto ofrece otros subsistemas independientes de *iptables* tales como el *connection tracking system* o sistema de seguimiento de conexiones, que permite encolar paquetes para que sean tratados desde espacio de usuario. *Iptables* es un software disponible en prácticamente todas las distribuciones de Linux actuales.(Escartín, 2005), (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Ramos, 2011), (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

1.12.6 Otros Cortafuegos (*firewall*).

Existen los de tipo *Inspección de Paquetes* que se fundamenta en el hecho de que cada paquete que transita por la red es examinado, igual su origen y objetivo. Generalmente se instalan cuando se requiere seguridad sensible y en aplicaciones muy complejas.

Otro de los Cortafuegos son los *Firewalls* Personales, que son herramientas para usuarios que quieren enlazarse a una red exteriorno segura y conservar su equipo libre deagresiones que puedan provocarles contaminaciones de virus o pérdida de los datos.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)

1.13 Políticas de diseño de un Cortafuegos (*Firewall*).

Las políticas de accesos en un *Firewall* se deben diseñar poniendo gran atención a sus debilidades o habilidades y además considerando los riesgos y fragilidades de la red exterior no segura. Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También se debe definir los usuarios contra los que se debe proteger cada recurso, ya que las medidas diferirán notablemente en función de esos usuarios.(Escartín, 2005), (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Borghello, Linux Máxima seguridad, 2005), (Arquitectura de

Sistemas Computarizados, Instalación de Firewall , 2012), (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

Generalmente se realizan algunas preguntas:

- ¿Qué se debe proteger? Se deberían proteger todos los elementos de la red interna (*hardware*, *software*, datos, etc.).
- ¿De quién protegerse? De cualquier acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan evitarse.

Sin embargo se pueden definir ciertos niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de servicios a otros.(Escartín, 2005), (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Borghello, Linux Máxima seguridad, 2005), (Arquitectura de Sistemas Computarizados, Instalación de Firewall , 2012), (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

- ¿Cómo protegerse? Esta es la pregunta más difícil y está orientada a establecer el nivel de monitorización, control y respuesta deseado en la organización. Puede optarse por las siguientes estrategias:

    1. Paradigma de seguridad.

    Se permiten servicios excepto aquellos expresamente prohibidos.

    Se prohíbe cualquier servicio excepto aquellos expresamente permitidos.

    2. Estrategias de seguridad.

    Paranoica: Se controla todo, no se permite nada.

    Prudente: Se controla y se conoce todo lo que sucede.

    Permisiva: Se controla pero se permite demasiado.

    Promiscua: No se controla o se hace muy poco, y se permite todo.

- ¿Cuánto costará? Estimando en función de lo que se desea proteger se debe decidir cuánto es conveniente invertir.(Escartín, 2005), (Borghello, Seguridad

Informática, sus implicaciones e implementación , 2008), (Borghello, Linux Máxima seguridad, 2005), (Arquitectura de Sistemas Computarizados, Instalación de Firewall , 2012), (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

1.14Zona Desmilitarizada.

- En este proyecto se pretendeincomunicarel equipo más agredido y sensible del *Firewall*, con este objetivo se implanta una Zona Desmilitarizada (DMZ) para que si un extrañoingresa a este equipo no tenga pasocompleto a la subred resguardada. En este proyecto se emplean dos enrutadores, uno externo y otro interno. El Enrutador exterior tiene la misión de bloquear el tráfico no deseado de ambos sentidos. El Enrutador interior hace lo mismo con la red interna y la DMZ (zona entre el *Router* externo y el interno). ***Ver Figura 1.12.***. (Escartín, 2005), (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Borghello, Linux Máxima seguridad, 2005), (Arquitectura de Sistemas Computarizados, Instalación de Firewall , 2012), (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

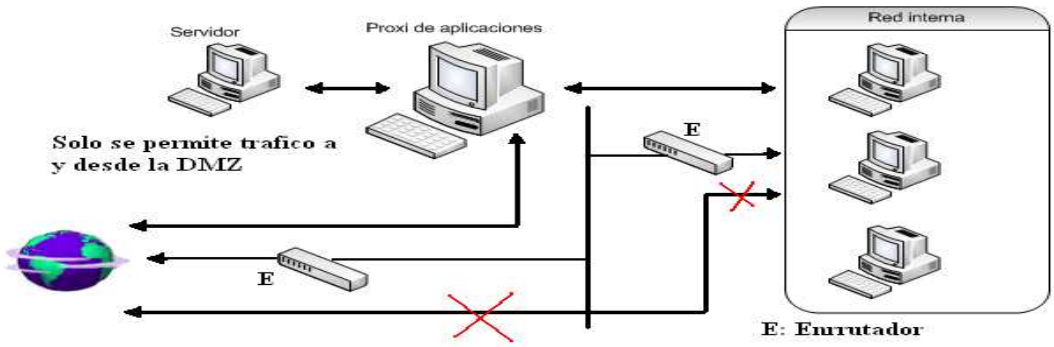

Figura 1.12: Zona desmilitarizada.

Fuente:(Borghello, Seguridad Informática, sus implicaciones e implementación, 2008)

Como puede apreciarse la Zona Desmilitarizada aísla físicamente los servicios internos, separados de los servicios públicos. Además no existe una conexión directa entre las dos redes(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)

Los Proxy de aplicaciones con el reenvío de paquetes desactivado y los sistemas con Zonas Desmilitarizadas podrían ser complejos para ordenar y probar, esto podría producirsignificativasaberturasen la defensa de la red. Por el contrario, si están bien ordenados y dirigidos, podrían dar un elevadonivel de seguridad y otras superioridades entre las que se encuentran: el ocultamiento de la información, registros de actividades y reglas de filtrado menos robustas.(Ardita, 2010), (Borghello, Linux Máxima seguridad, 2005), (Como instalar apache mysql y php en Ubuntu 5.4, 2012)

1.15 Seguridad en Protocolos y Servicios.

Se conoce diversos protocolos de comunicación en las redes de datos con servicios particulares. Como puede creerse, todos ellos tienen sus debilidades ya sea en su implementación o en su uso. A continuación se muestran algunos de ellos así como sus puertos, problemas de seguridad y sus formas de prevención.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008)**,** (Barrios, 2006)

- POP: El servicio Pop (puerto 109 y 110 en TCP) utilizados para que los usuarios puedan acceder a su correo sin necesidad de montar un sistema de archivos compartidos. Se trata de un servicio que podría ser peligroso, por lo que debería ser deshabilitado a no ser que sea estrictamente necesario ofrecerlo.Con POP se produce un flujo riesgoso de claves en la red. Hay tres clases de autenticación. Los usuarios suelen configurar sus clientes para que chequeen su buzón de correos cada pocos minutos, por lo que a intervalos muy cortos envían sus datos y puerto conocido de una máquina conocida. Al realizar toda esta comunicación en texto claro, un atacante no tiene más que interceptar la sesión POP para averiguar nombre de usuario y claves (aparte de leer el correo).
- FTP: Un inconvenientefundamental y peligroso de FTP (terminal 21 en TCP) es que fuecreado para brindar extremarapidez en el enlace, pero no para brindar protección. El tráfico de datos, desde la identificación y contraseña del usuario en la computadorahasta la transmisión de unfichero, se hace en contenido claro, así un agresor solo debe aprehender esos datos y conseguir así un acceso valido al servidor. Incluso puede ser una amenaza a la privacidad de los datos el hecho

de que ese atacante también pueda capturar y reproducir (modificar) los archivos transferidos.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Barrios, 2006), (Las diez vulnerabilidades de seguridad más críticas en aplicaciones web, 2005)

Para solucionar este problema es conveniente dar acceso FTP a pocos usuarios bien identificados y que necesiten utilizarlo, concientizándolos de la utilidad de aplicaciones que cifren todo el tráfico.

- SMTP: La mala configuración en los servidores SMTP (terminal 25 en TCP) empleado para transmitirmensajes electrónicos entre dispositivoslejanos puede provocar el *Mail Bombing* y el *Spam*reorientado.
- Usualmente se receptarámensajes de una cantidad no determinada de equipos sin poder impedirlaentrada a SMTP. En estas circunstancias se puede aplicar algunas medidas de seguridad simples, como realizar una consulta inversa a DNS para asegurarse de que solo máquinas registradas envían correo e impedir que el procesoreemitamensajes que no procedan de ubicaciones no definidas en su dominio.
- Servidores WWW: Hoy en día las conexiones en servidores Web son sin dudas las más extendidas entre usuarios de Internet. En la actualidad mueve a diario millones de dólares y es uno de los pilares fundamentales de muchas empresas. Es por tanto un objetivo muy atractivo para los intrusos.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Barrios, 2006), (Las diez vulnerabilidades de seguridad más críticas en aplicaciones web, 2005)

Los inconvenientes de protecciónrelacionados con la norma HTTP se clasifican en tres conjuntosde acuerdo a la información a la que pueden perturbar.

1. Protecciónal servidor: se debe certificar que los datos guardados en el servidor no puedan alterarse sin permiso, que esté utilizable y que solo puedan ingresar los usuarios autorizados.

2. Protecciónа la red: si un usuario se enlaza a un servidor Web se establece un tráfico de datos entre ellos; se debe certificar que la información receptada por el usuario del servidor sean los que se están transmitiendo y que los datos remitidos por el usuario al servidor no seanaprehendidos, arruinados o alterados por un agresor.
3. Protección al cliente: se debe certificar al usuario que baja datos de un servidor que no perjudique la seguridad de su equipo. Se deben evitar hechos maliciosos al acceder a una página, para que el usuario permanezca visitando el sitio. . (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Barrios, 2006), (Las diez vulnerabilidades de seguridad más críticas en aplicaciones web, 2005)

1.16 Criptografía y cifrado

Hoy en día la solidez del cifrado normalmente se mide por el tamaño de su clave. Independientemente de la solidez del algoritmo, los datos cifrados pueden estar sujetos a ataques por la fuerza en los que se prueban todas las combinaciones posibles de claves. Al final, el cifrado se puede romper. Para la mayoría de los códigos modernos con longitudes decentes, el tiempo para romper la clave a la fuerza se mide en milenios. Sin embargo, un fallo inadvertido en un algoritmo o el avance en la tecnología informática o en los métodos matemáticos pueden reducir este tiempo considerablemente.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Ardita, 2010), (Villalon, 2006)

Normalmente se cree que la longitud de la clave debe ajustarse para mantener seguros los datos durante una cantidad razonable de tiempo. Si el elemento es muy local, como las comunicaciones del campo de batalla o la información diaria sobre las acciones, un código que proteja estos datos durante semanas o meses está bien. Sin embargo, algo como número de tarjeta de crédito o los secretos de seguridad nacional tienen que mantenerse seguros durante un periodo de tiempo más prolongado y de forma eficaz para siempre. Por lo tanto, utilizar algoritmos de cifrado más débiles o longitudes de clave más cortas para algunas cosas está bien, siempre que la utilidad de la información

para un intruso expire en un breve periodo de tiempo.(Escartín, 2005), (Ardita, 2010), (Villalon, 2006)

1.16.1 Tipos de cifrado.

A continuación se detallan los diferentes tipos de cifrado:

- Criptografía simétrica:

El primer tipo de cifrado, denominado criptografía simétrica, o cifrado de secreto compartido, se ha estado utilizando desde la época de los antiguos egipcios. Esta forma de cifrado utiliza una clave secreta, denominada secreto compartido, para cifrar los datos en un galimatías inteligible. La persona que se encuentra en el otro extremo necesita la clave compartida para desbloquear los datos (el algoritmo de cifrado). Se puede cambiar la clave y los resultados del cifrado. Se denomina criptografía simétrica porque se utiliza la misma clave para ambos extremos tanto para cifrar como para descifrar los datos.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Ardita, 2010), (Villalon, 2006)

El problema que surge con este método es que se tiene que comunicar la clave secreta de una forma segura al destinatario pretendido. Si algún enemigo intercepta la clave, puede leer el mensaje.

- Criptografía asimétrica

La criptografía asimétrica utiliza un cifrado que divide la clave en dos claves más pequeñas. Una de las claves se hace pública y otra sigue siendo privada. El mensaje se cifra con la clave pública del destinatario. Éste puede descifrarla a continuación con su propia clave privada. La diferencia es que nadie necesita la clave privada de nadie para enviar un mensaje seguro.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Ardita, 2010), (Villalon, 2006)

Se utiliza la clave pública, que no tiene que mantenerse segura (de hecho, se publican en repositorios como si fueran una guía telefónica). Al utilizar la clave pública del destinatario, se sabe que sólo esa persona puede descifrarlo utilizando su propia clave privada. Este sistema permite que dos entidades se comuniquen con seguridad sin ningún intercambio anterior de claves.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Ardita, 2010), (Villalon, 2006)

Normalmente la criptografía asimétrica se implanta mediante el uso de funciones de un sentido. En términos matemáticos, éstas son funciones fáciles de calcular en una dirección pero muy difíciles de calcular a la inversa. De esta forma se puede publicar una clave pública, derivada a partir de la clave privada, una tarea muy difícil de llevar a cabo al revés para determinar la clave privada. Una función común de un sólo sentido utilizada actualmente, es la descomposición en factores de números primos grandes. Es fácil multiplicar dos números primos y obtener un producto. Sin embargo, determinar cuál de las muchas posibilidades son los dos factores de un producto es uno de los problemas matemáticos más complejos.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Ardita, 2010), (Villalon, 2006)

1.16.2 PGP (*Pretty Good Privacy*).

El proyecto de Seguridad Bastante Buena, que es la traducción de las siglas PGP, Se crea en 1991 por carencia de instrumentos cifrados simples, poderosos, de bajo precio y disponibles para cualquier usuario. Hoy PGP es elinstrumento más común y confiable para brindar protección enlas comunicaciones de simples usuarios o grandes organizaciones.(Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Borghello, Linux Máxima seguridad, 2005)

Operación de PGP:

- Anillos de códigos: Un anillo es un conjunto de códigosguardados en un fichero. Un usuario posee dos anillos: para códigos públicos y privados.

Cada una de las claves, además posee un identificador de usuario, Fecha de expiración, Versión de PGP y una huella digital única hexadecimal suficientemente corta que permita identificar la autenticidad de la clave.

- Codificación de mensajes: Como ya se sabe los algoritmos simétricos de cifrado son más rápidos que los asimétricos. Por esta razón PGP cifra primero el mensaje empleando un cifrado simétrico con una clave generada aleatoriamente y posteriormente codifica la clave haciendo uso de la llave pública del destinatario. Dicha clave es extraída convenientemente del anillo de claves públicas a partir del identificador suministrado por el usuario. Para que el mensaje pueda ser leído por varios usuarios solamente debe ser incluida en la cabecera cada una de las claves públicas correspondientes.
- Decodificación de mensajes: Cuando se trata de decodificar el mensaje, PGP simplemente busca en la cabecera las claves públicas con las que está codificado, pide una contraseña para abrir el anillo de claves privadas y comprueba si se tiene una clave que permita decodificar el mensaje. Cada vez que se quiera hacer uso de una clave privada, habrá que suministrar la contraseña correspondiente, o que si este anillo queda comprometido, el atacante debería averiguar dicha contraseña para descifrar los mensajes. No obstante, si el anillo de claves queda comprometido, es aconsejable revocar todas las claves almacenadas y generar otras nuevas.
- Compresión de ficheros: PGP usualmente comprime el contenido antes de codificar el correo para reducir el tiempo de encriptado y vigorizar la protección dela codificación ante el criptoanálisis que aprovechan las repeticiones del contenido. (Borghello, Seguridad Informática, sus implicaciones e implementación , 2008), (Ardita, 2010), (Borghello, Linux Máxima seguridad, 2005)

1.17 VMware. Creación de máquinas virtuales.

El VMware (VM de *Virtual Machine*) es una herramienta filial de EMC *Corporation* que proporciona la mayor parte del software de virtualización disponible para

ordenadores compatibles X86. Entre este software se incluyen VMware *Workstation*, y los gratuitos VMware *Server* y VMware *Player*. El software de VMware puede funcionar en Windows, Linux,y en otros sistemas operativos. ***Ver Figura 1.13***.(GNU/Linux CentOS , 2012), (Distribuciones libres de GNU/Linux , 2012)

Figura 1.13: Logo del Vmware Workstation.

Fuente:(GNU/Linux CentOS , 2012)

Este es un programa que simula un sistema físico con unas características de hardware determinadas. Cuando se ejecuta el programa (simulador), proporciona un ambiente de ejecución similar a todos los efectos a un computador físico (excepto en el puro acceso físico al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc(GNU/Linux CentOS , 2012), (Distribuciones libres de GNU/Linux , 2012)

Un virtualizador por software permite ejecutar varios computadores dentro de un mismo hardware de manera simultánea, permitiendo así el mayor aprovechamiento de los recursos. No obstante, y al ser una capa intermedia entre el sistema físico y el sistema operativo que funciona en el hardware emulado, la velocidad de ejecución de este último es menor, pero en la mayoría de los casos suficiente para usarse en entornos de producción(GNU/Linux CentOS , 2012), (Distribuciones libres de GNU/Linux , 2012)

El rendimiento del sistema virtual varía dependiendo de las características del sistema físico en el que se ejecute, y de los recursos virtuales (CPU, RAM, etc.) asignados al sistema virtual.(GNU/Linux CentOS , 2012), (Distribuciones libres de GNU/Linux , 2012)

Existen varias versiones de estos sistemas con funcionalidades similares. Varias de estas son:

1. VMware Player.
2. VMware Server
3. VMware ESX Server.

Este tipo de software es muy bueno para establecer todo tipo de aplicaciones desde el punto de vista virtual. Presenta la facilidad de crear conexiones de red, de establecer cortafuegos locales y la instalación de todo tipo de Sistemas Operativos. Con todas estas facilidades se pueden crear numerosas estrategias de seguridady disponibilidad de servicios en los sistemas. Es una herramienta robusta y de fácil utilidad(GNU/Linux CentOS , 2012), (Distribuciones libres de GNU/Linux , 2012)

1.18 Resumen del Capítulo.

Las vulnerabilidades existentes en un Sistema Informático tienen que ser de conocimiento del operador de redes del sistema, ya que existen numerosas amenazas que pueden traer severos daños físicos y lógicos. Los usuarios deben tomar partido sobre el caso porque son ellos los que reciben todos los servicios y por los cuales se trabaja y mantiene la disponibilidad y seguridad de la información con la cual operan. Para esto se crean políticas de seguridad en las cuales se implantan estrictas leyes a cumplir.

Además de establecer toda la seguridad física posible, creando Centro de Operaciones de la Red con toda la gama de elementos que esto conlleva, hay que establecer además elementos de seguridad (hardware y software) que garanticen el buen funcionamiento. Para esto existen los Cortafuegos y todas sus modalidades, Antivirus, Sistemas de Detección de intrusos, Sistemas de Protección de la Información, Encriptación, etc.

Se pudo observar la importancia de la seguridad en sistemas informáticos. El desarrollo dirigido hacia los Sistema Código abierto se hace evidente ya que la mayoría de los tópicos son en función de los servidores de Software Libres (Linux). La descripción de algunos términos de estos sistemas ha servido de base para realizar un mayor análisis sobre estos temas y poder citar nuevos elementos con mayor exactitud.

Capítulo 2. Virtualización del Sistema de Comprobación.

Para establecer un sistema de seguridad hay que tener numerosos aspectos en cuenta. Comenzando desde la seguridad física y concluyendo en la lógica. Muchos de estos temas se trataron en el capítulo anterior, realizando un análisis teórico para su posterior interpretación en el funcionamiento práctico.

El actual capítulo plantea el análisis de una pequeña red con la utilización de un cortafuego y el establecimiento de una DMZ. Plasma además las políticas para la configuración del cortafuego y para los servidores localizados en la DMZ.

Lo particular en la implementación de la arquitectura es que se realiza mediante la virtualización con la ayuda del VMware, para crear varias máquinas virtuales y establecer el entorno de red deseado.

CentOS toma el protagonismo como Sistema Operativo, ya que sobre él se establecen todas las configuraciones necesarias para el funcionamiento correcto del sistema.

2.1 VMware 7.0.0.20.3739. Utilidad para el proceso de virtualización.

Esta herramienta es de gran utilidad, gracias a su capacidad de virtualización de parámetros vistos en PCs físicas. Mediante su interfaz gráfica se hace muy factible su utilización e interpretación para la instalación de las PCs virtuales, además de presentar elementos gráficos de muy fácil manejo como: *play, stop, pause y reset*.***VerFigura 2.1***.

Con el *Virtual Network Editor*, que es una interfaz para la configuración de la red virtual, se pueden realizar conexiones de red mediante las diez interfaces que presenta. Además muestra especificidades en su conexión y función que estas pueden realizar.

La conexión puede ser de forma automática (DHCP) con un rango de direcciones definidos previamente, o establecerla de forma específica para una sola dirección IP. Se

puede establecer un NAT de direcciones IP mediante una de las interfaces y de esta forma lograr configuraciones de red a conveniencia.

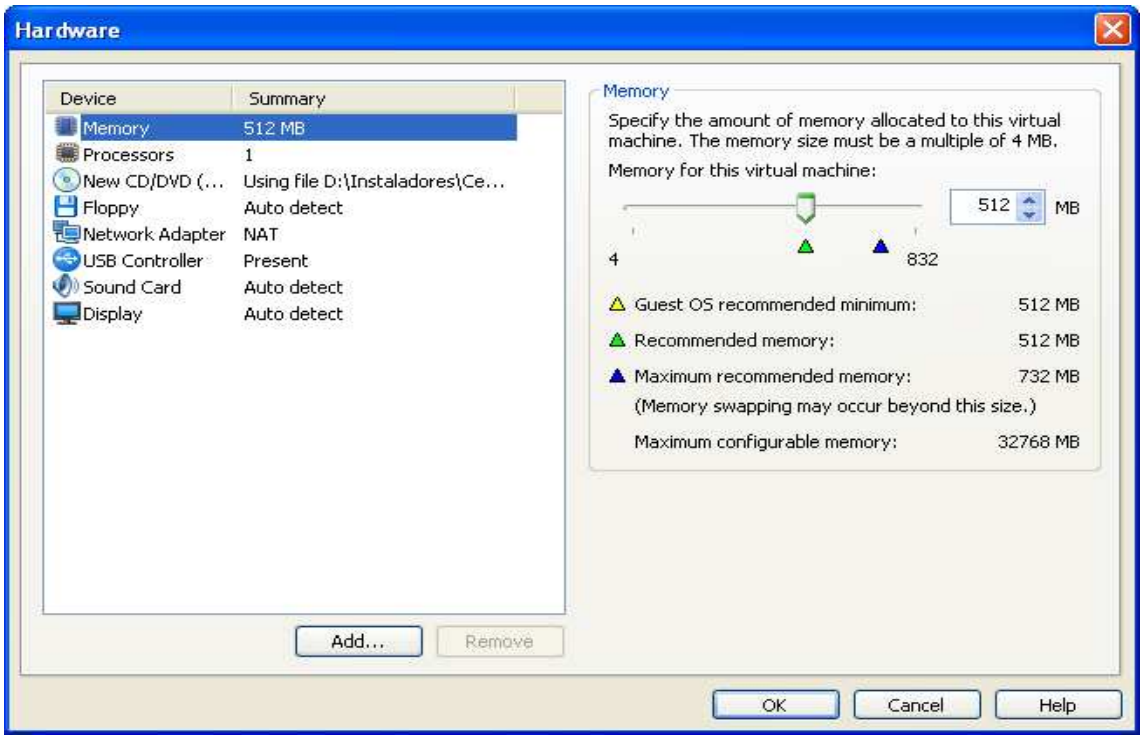

Figura 2.1: Interfaz de los elementos utilizados por cada Virtual Machines.

Fuente: CentOSVMware Workstation

En el caso particular de cada una de las *Virtual Machines*, se escoge la interfaz por donde va a trabajar dicha PC y en el *Virtual Network Editor* se configuran los elementos de red necesarios para la interfaz y así establecer una conexión de red virtual.

Además el entorno de red y la propia instalación de la PC virtual, ayudan a establecer todas las funciones de las PCs físicas y permite maniobrar los elementos indispensables de las mismas, como la RAM, disco duro, el control de usb.

2.2 Instalación de CentOS.

CentOS es una distribución de Linux basada en las fuentes libremente disponibles de *Red Hat Enterprise Linux*. Cada versión de CentOS es mantenida durante 7 años (por

medio de actualizaciones de seguridad). Las versiones nuevas son liberadas cada 2 años y actualizadas regularmente (cada 6 meses) para el soporte de hardware nuevo.

Para la implementación del sistema de seguridad se hace necesaria la instalación de Sistemas Operativos y la interconexión entre ellos. En el caso a mostrar, la versión CentOS 5.7 de Linux es el protagonista y representa las PCs virtuales. En base a esta versión se implementa el sistema de seguridad a mostrar montado sobre VMware.

2.2.1Creación de las PCs virtuales sobre el VMware.

El VMware permite la instalación y puesta en marcha de múltiples PCs en su entorno además de conectarlas a la red, ya sea esta una LAN local o una red virtual interna creada en la misma máquina física.

Para la puesta en marcha de este sistema primeramente se debe escoger el Sistema Operativo (SO) a instalar y desde el VMware crear un nuevo *Virtual Machine*. ***Ver figura 2.2***

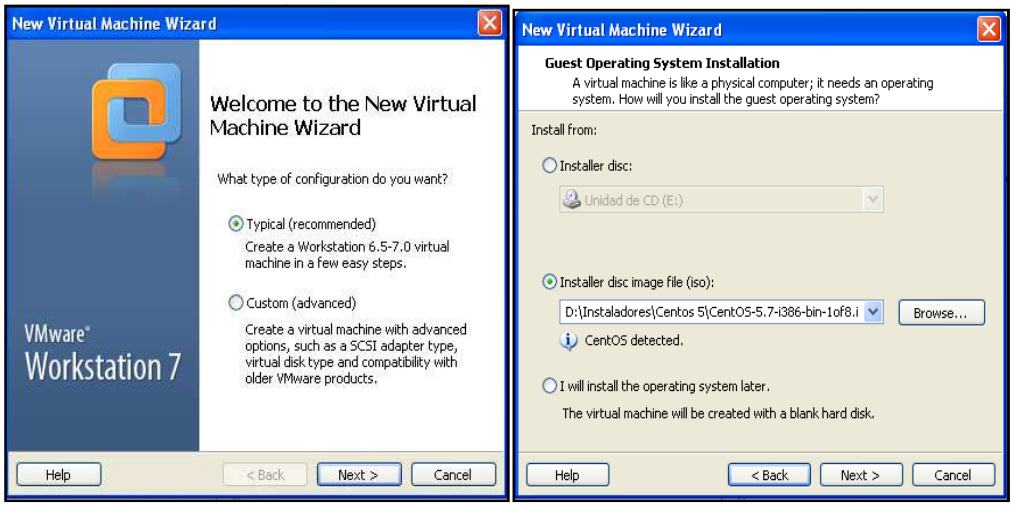

Figura 2.2 Creación de un nuevo VMware

Fuente: CentOSVMware Workstation

De esta manera se extraen los discos *.iso*del directorio donde estén almacenados y se sigue con la creación de la PC virtual. Se establece dónde se va a guardar la imagen, el

nombre con que la reconocerá posteriormente el VMware y se sigue con la creación de la misma. En todo el transcurso se pueden establecer o configurar el tamaño de la RAM y el disco duro, además de la red por la cual va a operar, entre otros aspectos (Figura 2.3).

Figura 2.3: Instalación de Centos 5 en el entorno del VMware.

Fuente: CentOSVMware Workstation

Ya creado el nuevo VMware, se pasa a la instalación del SO sobre la base virtual definida. Mediante el establecimiento se pide el idioma con el cual se va a trabajar durante la instalación. Otros de los aspectos a seguir es la partición del disco duro, que puede ser personalizada o predeterminada por el sistema. El entorno de la red es otro de los aspectos a configurar, aunque este se puede definir después de la instalación mediante el fichero de configuración **(/etc/sysconfig/network-scripts/ifcfg-eth0**). Este tipo de configuración pide la versión de IP, (IPv4) o (IPv6), además de la dirección IP, la máscara y la puerta de enlace.

El sistema horario es otro de los puntos que se configuran para el funcionamiento del sistema y luego la contraseña y la confirmación de la misma, con la cual se va a entrar

al sistema. Luego de todos estos procedimientos comienza la instalación de CentOS 5.7 cuyos discos son, CentOS-5.7-i386-bin-1of8.iso hasta el CentOS-5.7-i386-bin-8of8.iso.

Con la obtención de todos los discos de CentOS 5.7, se instalan todos los paquetes necesarios para el funcionamiento del (SO) y la posterior puesta en marcha de la arquitectura de red.

2.3 Topología de red implementada.

La topología de la red creada es sencilla, por lo que su funcionamiento se va a basar en la puesta en marcha de un sistema de seguridad. No es necesaria la creación de una gran arquitectura ya que con tan solo unos cuantos elementos se obtienen los resultados deseados.

Dicho diseño está constituido por un proveedor de servicios de Internet, un Firewall (IPtables) con políticas establecidas para realizar un NAT previamente definido entre las redes, y así prestar la mayor seguridad posible sin afectar la disponibilidad de la red. Existe una LAN local a la cual se le va a prestar servicios, y por último una Zona Desmilitarizada (DMZ), que es donde van a estarlas máquinas más atacadas de la red (Servidores).

Por su importancia esta zona requiere de seguridad adicional, ya que todo el tráfico de la red local pasará por ella, al igual que el que provenga del ISP. Además que el *IPtables* está para realizar el NAT entre las direcciones deseadas, y contiene un conjunto de reglas para el filtrado de paquetes, aperturas de puertos y conexiones, el reenvío de paquetes entre otras cadenas establecidas. La constitución de dicho sistema es de forma virtual con la utilización del *VMware*, por lo que carece de cableado, conectores e interfaces físicas. Otra de las particularidades que tiene esta red es la creación de dos interfaces virtuales dentro de la implementación del *Firewall* virtual, cuyas interfaces son las conectadas a las redes de la DMZ y la red local. La arquitectura de la red puede apreciarse en la figura 2.4.

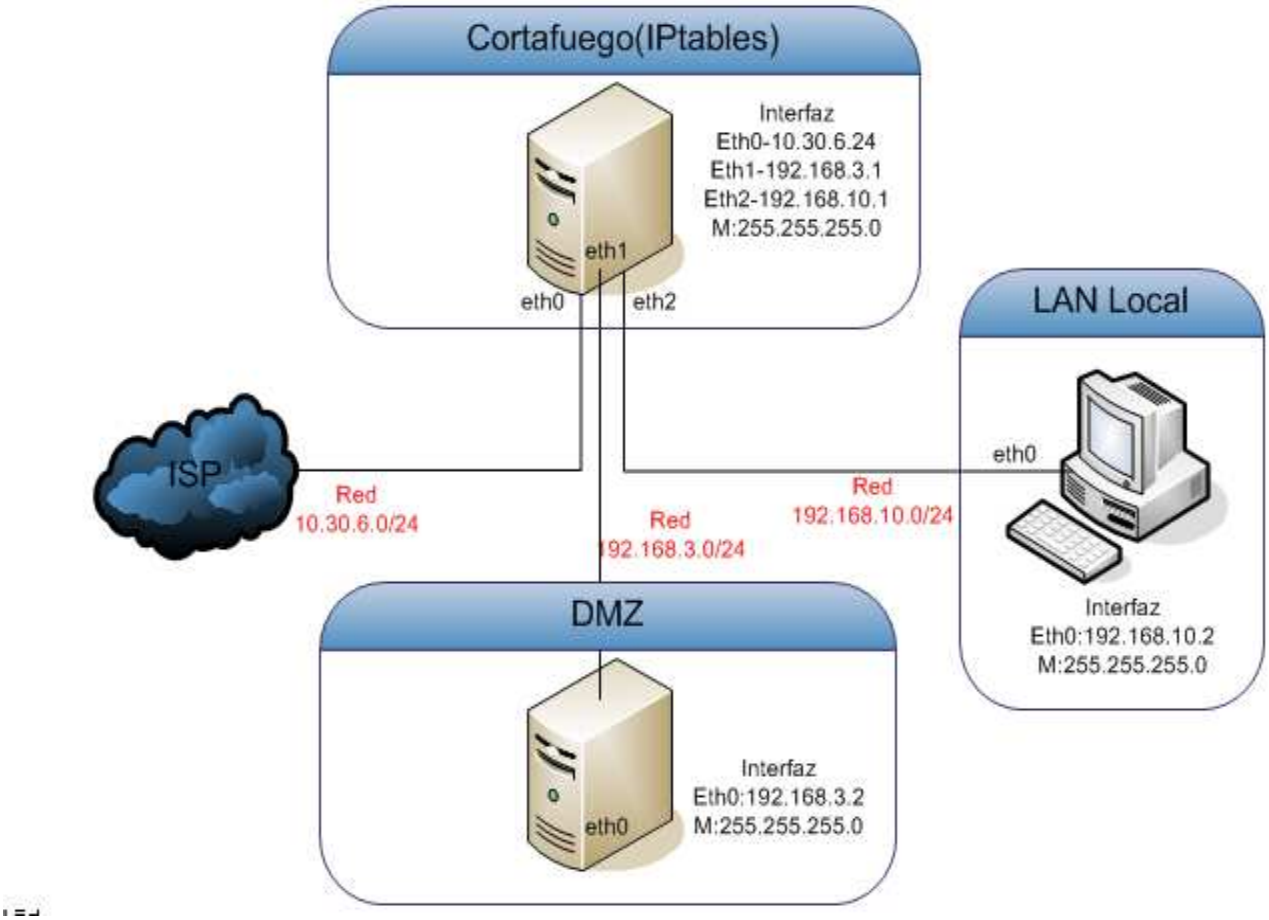

Figura 2.4: Diagrama de la arquitectura de la red.

Fuente: CentOSVMware Workstation

2.4 Configuración de las interfaces.

Para poder establecer la conexión de las PCs a la red deseada, primeramente se debe configurar la interfaz de red de cada uno de los dispositivos. Al tener una arquitectura sencilla, se hace maniobrable manejar pocas direcciones IP y su distribución en la red.

Al estar trabajando con máquinas virtuales, las interfaces que se utilizan son virtuales aunque se mantienen las mismas políticas de los dispositivos físicos. La mayoría de las PCs tienen una sola tarjeta de red, por lo que generalmente cuentan también con una sola interfaz física (eth0), y en el mejor de los casos, lo que trae como ejemplo en los Sistemas Linux, es la activación de interfaces virtuales sobre la interfaz física existente. Esta podría ser una solución al problema de las interfaces en el Cortafuegos. Pero el

VMware brinda una mejor opción. Por cada dispositivo instalado es capaz de agregarle varias interfaces de red, así como discos duros, puertos series, paralelos, etc.

De esta manera se le añaden dos interfaces más al servidor que realiza función de cortafuegoy mediante estas se establecen los caminos de comunicación hacia la Zona Desmilitarizada (DMZ) y la red localo el ISP.

2.4.1 Configuración de las interfaces eth0, eth1 y eth2 del Cortafuego.

Al tener una arquitectura de red como la mostrada anteriormente en la ***figura 2.4*** se hace necesario que el Cortafuego tenga presente tres interfaces de comunicación. Estas son eth0, eth1 y la eth2, por las cuales pasa todo el tráfico comprendido entre las redes implementadas.

Para el *VMware* o esta*Virtual Machine*, se configura la interfaz mediante el *Virtual Network Editor*. En esta herramienta del *VMware* se escogen una de las diez interfaces que brinda (Vmnet0) para la conexión de la interfaz eth0 del cortafuego y de ahí el tipo de conexión que se desea según las opciones que brinda este editor de redes virtual.

Para el caso se escoge "Host-only" si se desea conectarse a la máquina física o "*Bridget*" si es a la red externa. Para el caso de *Host-only*se establece la conexión de la misma mediante "*Connet a host virtual adapter to this network*". Hecho esto se le pasa la dirección de red(10.30.6.0/24) y la máscara de red(255.255.255.0). En la parte superior de la misma interfaz gráfica se debe visualizarlo siguiente (Ver figura 2.5):

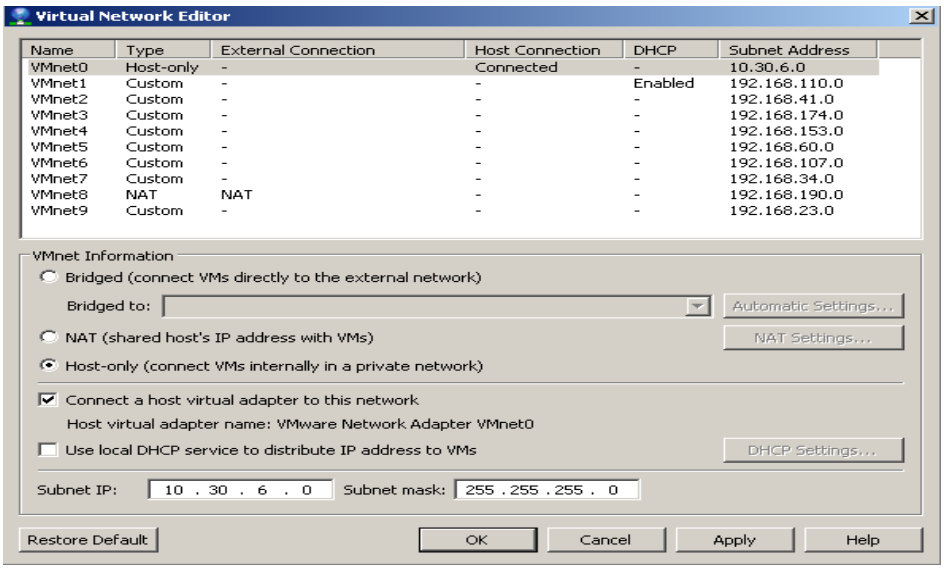

Figura 2.5: Configuración de la interfaz eth0 desde el VMware para el Cortafuego. Fuente: CentOSVMware Workstation

De esta forma queda configurada la interfaz eth0 desde el *VMware* y para los demás elementos virtuales ella está conectada a la red 10.30.6.0.

Para la conexión de las restantes interfaces con el *WMware* se utiliza el mismo editor de interfaces tal como muestra la ***figura 2.5,***a diferencia que se escogen los *Vmnet2* y *Vmnet4* para las redes 192.168.3.0 y 192.168.10.0 respectivamente.

Lo que brinda este editor (*Vmnet*) son conmutadores (*switch*) virtuales pertenecientes a la red especificada en dicho editor. Solamente quedaría asignar las máquinas de la red especificada a ese *switch* virtual. Esto se realiza mediante la configuración de red de cada máquina virtual en particular. ***Ver figura 2.6.***De esta manera para la red de la interfaz eth1 (192.168.3.0) se le asigna el *switch* virtual dos (*Vmnet2*), y para eth2 en la red (192.168.10.0) el *switch* virtual cuatro (*Vmnet4*).

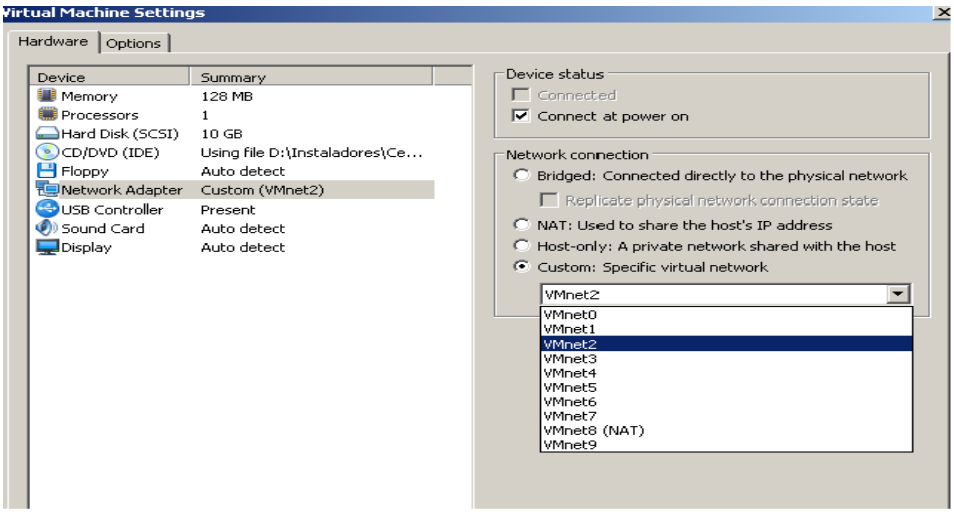

Figura 2.6: Configuración de la red desde el escenario de cada máquina virtual.

Fuente: CentOSVMware Workstation

La red también se configura desde la *Virtual Machine* creada. Desde el punto de vista del Sistema operativo (SO), este se hace mediante el comando ¨**/etc/sysconfig/network-scripts/ifcfg-eth0**¨, ver ***figura 2.7.*** En este archivo se configuran todos los parámetros de red necesarios para el funcionamiento del dispositivo en la red. Se hace algo parecido a lo explicado anteriormente con el *VMware*, pero la diferencia está en que como se trabaja con Linux modo texto, hay que entrar al archivo y copiar cada uno de los parámetros que se quiere configurar. En este caso la interfaz eth0 tiene como dirección IP (10.30.6.24) con Máscara (255.255.255.0).

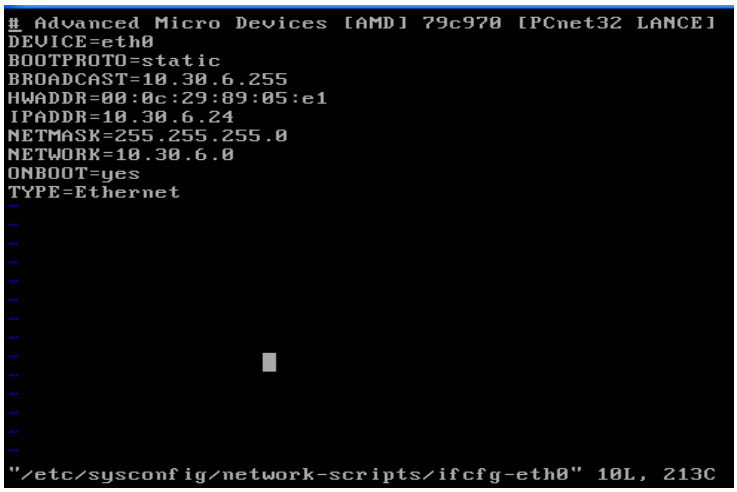

Figura 2.7: Configuración de eth0 del Firewall mediante el SO.

Fuente: CentOSVMware Workstation

De la misma forma se configuran las interfaces eth1 y eth2. Al igual que eth0, existe un archivo de configuración para cada una de estas interfaces, ¨**/etc/sysconfig/network-scripts-ifcfg-eth1**¨ para el terminal virtual eth1 y ¨**/etc/sysconfig/network-scripts-ifcfg-eth2**¨ para el tercer terminal virtual eth2. Para hacer activas estas interfaces solamente se les debe de poner la dirección IP de la red a la que va a pertenecer. En el caso de la DMZ con la interfaz eth1 la dirección IP es (192.168.3.1) y la Máscara de la red (255.255.255.0). El otro terminal eth1, perteneciente a la red local tiene como IP (192.168.10.1) con máscara (255.255.255.0). Cada una de estas direcciones pertenecen a las redes 192.168.3.0 y la Red 192.168.10.0 respectivamente.

Una vez realizados estos pasos, es necesario comenzar el servicio de red. Para esto se utiliza el ***service network start***. Esto se realiza cuando se comienza por primera vez el servicio de red. En otros casos ya iniciado el mismo, si se realiza algún cambio en estas configuraciones, entonces se plantea el ***service network restart,***o a la hora de detener el servicio sería de la forma ***service network stop***.

Para la comprobación de la existencia de estos terminales solamente se debe escribir, **ifconfig(la interfaz)** y salen todos los parámetros de la interfaz deseada o lo que es lo mismo **ifconfig** y salen todas las interfaces existentes y sus parámetros correspondientes.

2.4.2 Configuración de la interfaz eth0 del Servidor de la DMZ.

El servidor que se encuentra en la Zona Desmilitarizada (DMZ), es tan solo una representación de varios de los servidores que pueden estar presentes en dicha zona. Si ese fuera el caso se realizarían todas las configuraciones para cada una de las interfaces.

Para poder establecer los parámetros de red en el servidor ubicado en la DMZ, ocurre lo mismo que en *Firewall*. Lo que tiene como diferencia es que solamente se establecen los elementos de red del terminal eth0. No se establecen más terminales de red ya que la función a realizar con este servidor, es precisamente su función, prestar servicios.

Se reitera la utilización del *Virtual Network Editor* para configurar la interfaz eth0 de este nuevo elemento. A este terminal se le asigna desde el escenario de la máquina virtual del *VMware* la salida por el *VMnet2*. Es decir, este dispositivo pertenece ala red 192.168.3.0 al igual que una de las tarjetas de red de cortafuego. ***Verfigura 2.8.***

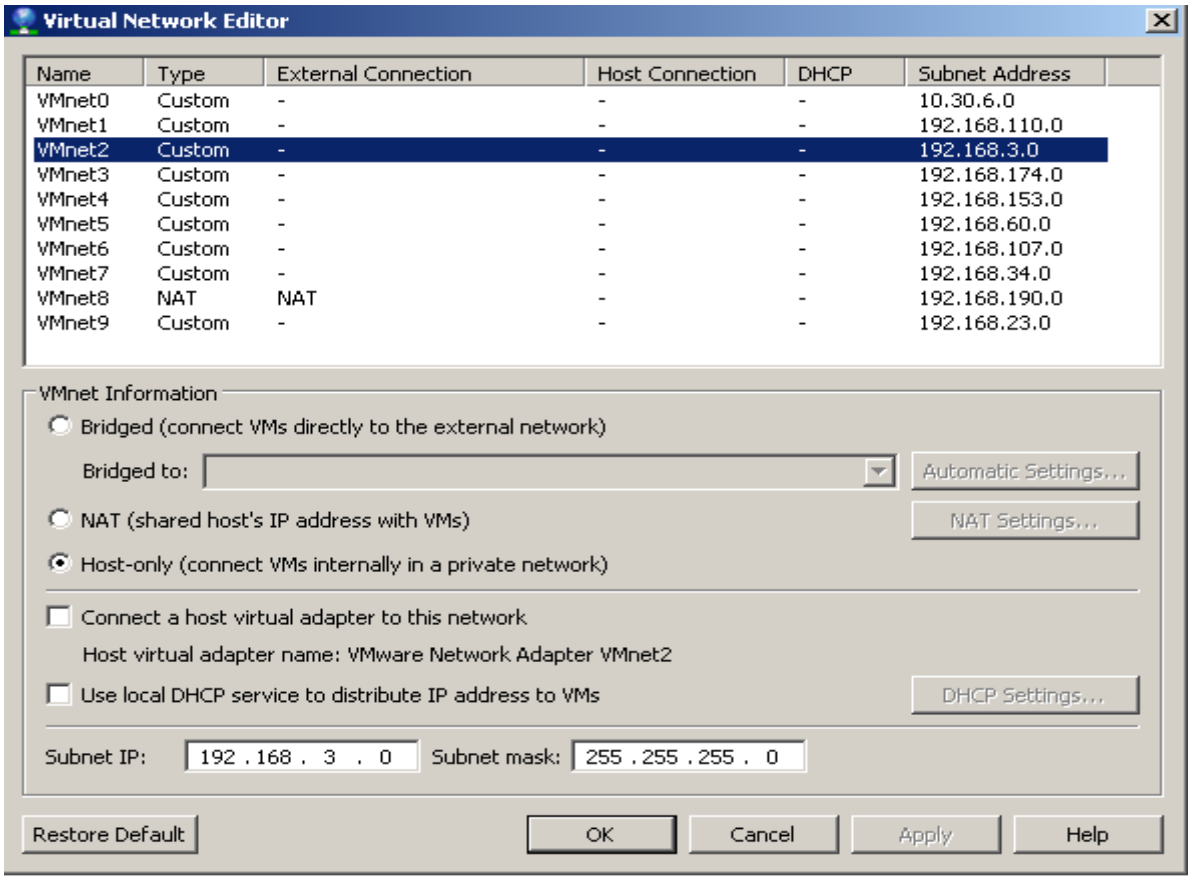

Figura 2.8: Configuración de la interfaz eth0 desde el VMware.

Fuente: CentOSVMware Workstation

En el caso del Servidor, las funciones son las mismas ya que se utiliza el mismo Sistema Operativo (SO) y versión. Se utiliza el ¨**vi**¨ como editor de configuración y para ello se establece la sintaxis, **/etc/sysconfig/network-scripts/ifcfg-eth0**. ***Verfigura 2.9.***

Una vez abierto el editor, se pasa a introducir todos los parámetros necesarios para el funcionamiento del dispositivo en la red.

Como se muestra en la figura 2.8, se establece la dirección IP (192.168.3.2), la red (192.168.3.0),la Máscara, el *Broadcast* y se le agrega un elemento nuevo que es el *Gateway* (192.168.3.1) o puerta de enlace del servidor.

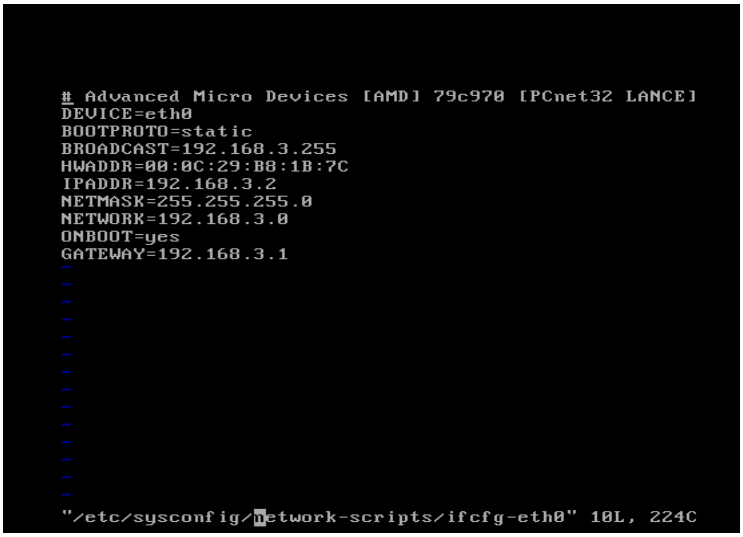

Figura 2.9: Configuración de eth0 del Servidor mediante CentOS.

Fuente: CentOSVMware Workstation

Con la ayuda del comando **ifconfig** se puede comprobar el establecimiento de esta interfaz (**ifconfig eth0**).

2.4.3 Configuración de la interfaz eth0 de la PC en la LAN.

La PC existente en la red local es la representación de un conjunto de máquinas que pueden existir en una LAN. Por las condiciones reales de la PC física solamente se pudo crear una máquina virtual en esa red. Pero esto no limita la disponibilidad de la red ni su funcionalidad. Con un elemento disponible se puede lograr todo tipo de comprobación y trabajo.

Para la configuración de los parámetros de red para la PC, se realizan pasos similares que en los casos anteriores. El *VMware* muestra nuevamente su utilidad para crear todo el entorno necesario en la creación de las *Virtual Machines* y el entorno de red.

El terminal eth0 está configurado tanto en el *Virtual Network Editor* como en el Sistema Operativo. En el *Virtual Network Editor* se escoge la interfaz por donde va a establecer conexión la PC (*VMnet4*). Este va a ser el *switch* virtual por donde va a comunicarse esta máquina y solamente quedaría establecer la conexión de este dispositivo a dicho *switch*. Como se mencionó anteriormente esta función se realiza por el escenario de la máquina virtual (*Virtual Machina Setting*). Ver ***figura 2.10***.

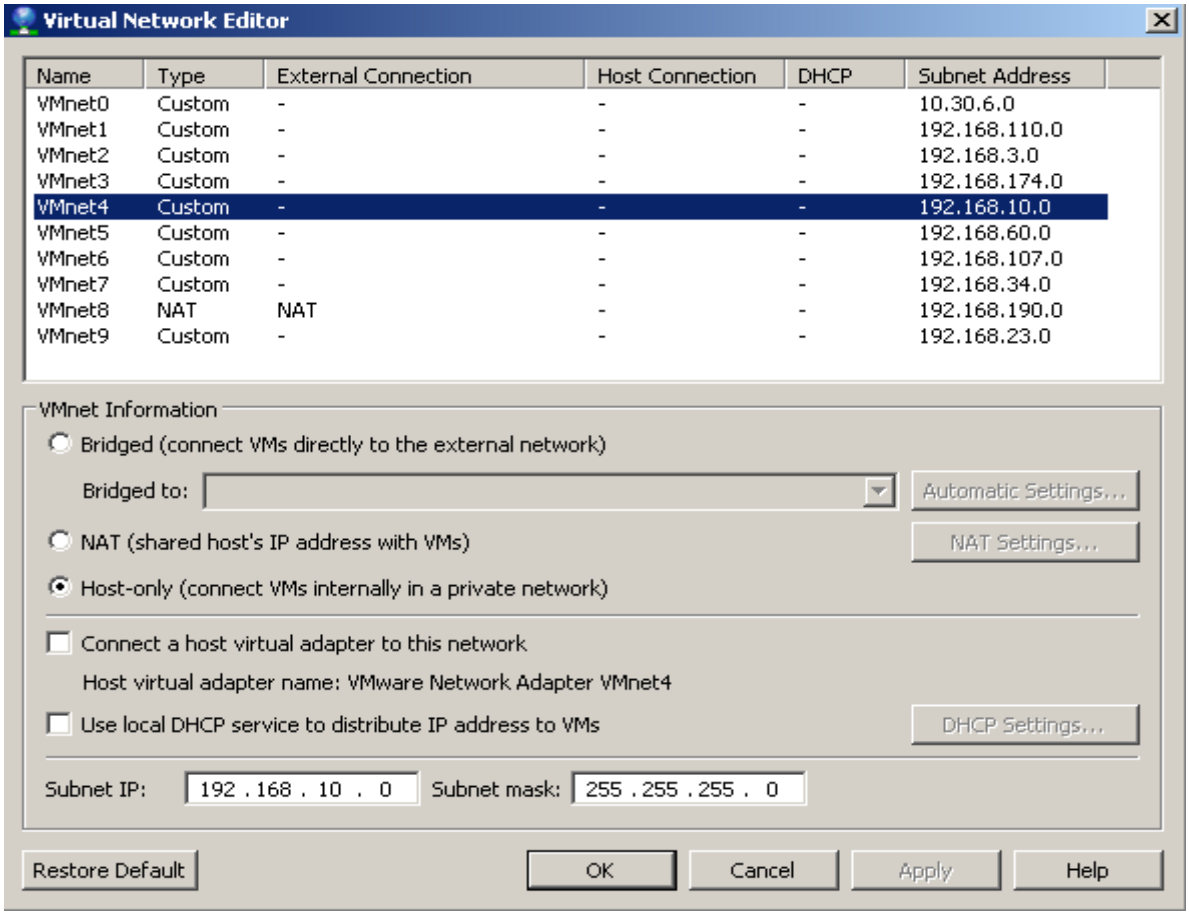

Figura 2.10: Configuración de la red para la PC de la red local desde el VMware.

Fuente: CentOSVMware Workstation

Este dispositivo realiza su conexión en el mismo *switch* al cual está conectada la tarjeta de red correspondiente a la interfaz eth2 del cortafuego, perteneciendo ambas a la misma red.

Estos pasos son similares a los realizados para los anteriores elementos de la red, se puede realizar también el llenado del archivo de configuración de la interfaz desde esta *Virtual Machine*. Ver ***figura 2.11.***

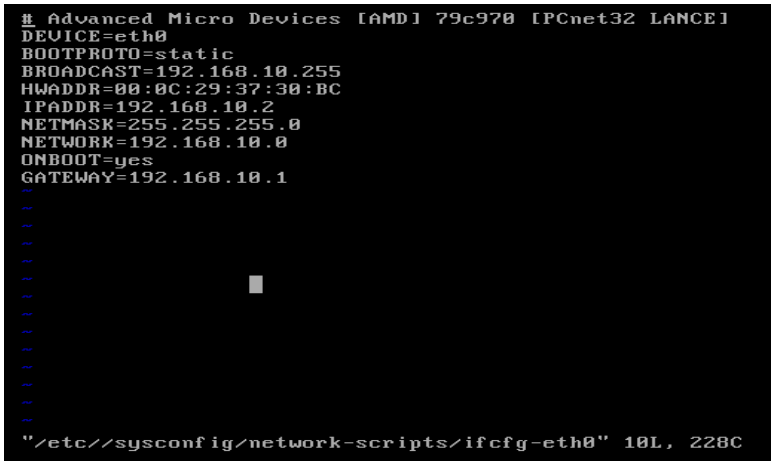

Figura 2.11: Configuración de la red eth0 de la PC local desde el Sistema Operativo.

Fuente: CentOSVMware Workstation

Nuevamente mediante el archivo ¨**/etc/sysconfig/network-scripts/ifcfg-eth0**¨ se pueden establecer los parámetros necesarios para el funcionamiento de la PC en su correspondiente red. De esta manera quedan configurados los elementos activos que constituyen la pequeña red y así queda conectada toda la estructura.***Ver figura 2.12.***

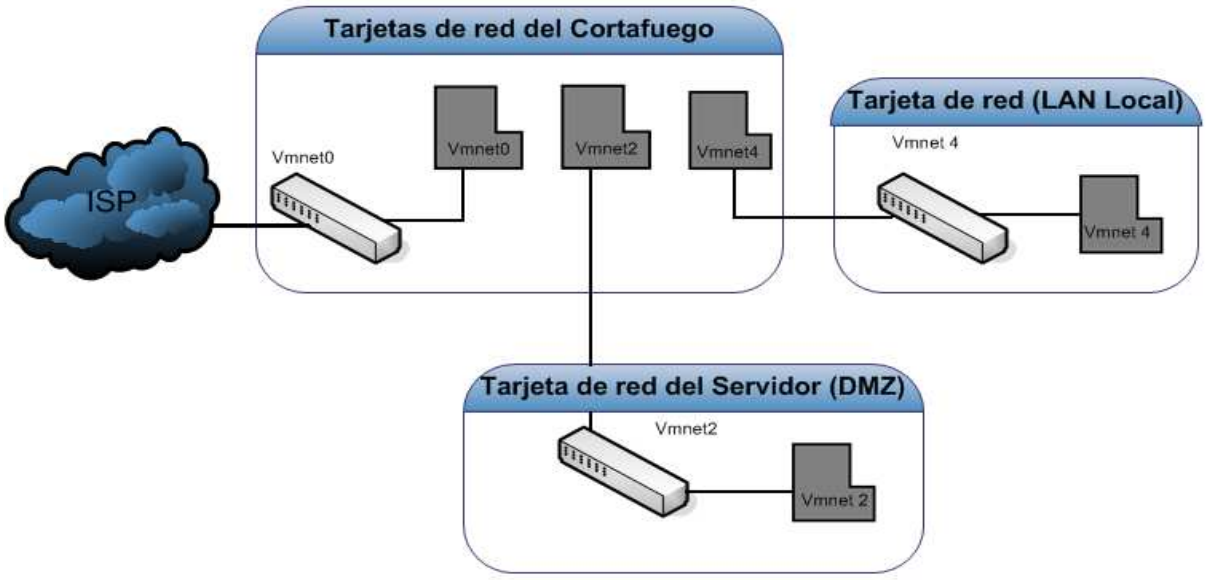

Figura 2.12: Esquema de la estructura con los conmutadores virtuales y las tarjetas de red.

Fuente: CentOSVMware Workstation

Cuando se concluyen todas las configuraciones de red realizadas, se pasa a la activación del servicio. Linux logra esto mediante el comando ***service network start***. Como se mencionó anteriormente, este servicio puede ser restablecido si existiera algún cambio, o detenido. Una vez guardados los cambios se pueden enviar todo tipo de paquetes de red.

Las conexiones después del cortafuego son de tipo "*Custom*". Este modo brinda conexión entre los dispositivos virtuales sin conectarse a la máquina física o tener salida hacia la red exterior. Por esa razón el *switch* virtual *Vmnet0de* la red 10.30.6.0 tiene conexión de tipo "*Host-only*" y los demás conmutadores de tipo *Custom*. Así se garantiza que la salida hacia el proveedor de servicios sea por una sola interfaz y las demás pertenezcan solamente a la red virtual.

2.4.4 Verificación de la conexión.

Para verificar el estado de la conexión se utilizan comandos conocidos para la comprobación de estado de conexión. El *ping* y el *traceroute* son los utilizados para este proceso.

Para Linux, a la hora de utilizar el *ping* se debe especificar la cantidad de paquetes que se van a transmitir. Un ejemplo de esto es ping -c4 192.168.10.1. Esta es la dirección del *Gateway* de la red local y de esta forma se puede ver si hay conexión o no y -c4 especifica la cantidad de elementos a transmitir.***Ver figura 2.13.***

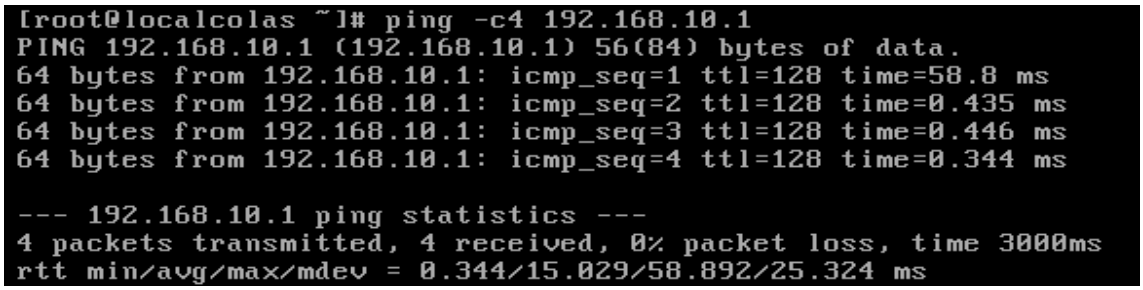

Figura 2.13: Ejemplo del estado de la conexión de la arquitectura de red.

Fuente: CentOSVMware Workstation

2.5 Variante de implementación del diseño de red.

Existe otra vía para la realización de dicho sistema. Este método tiene la particularidad de que la tarjeta de red de la máquina física se utiliza como puente para las comunicaciones de las PC virtuales. Las configuraciones de red implementadas en los Sistemas Operativos de cada una de las máquinas virtuales se hacen de la misma forma antes explicada, pues el principio y la estructura planteada en puntos anteriores son los mismos.

También se usan cinco conmutadores (*switch*) virtuales, cada uno de estos con conexión a una de las tarjetas de red virtuales existentes.

En el editor virtual de red del *VMware* se utilizan los *Vmnet0, Vnmet*y*Vmnet5*. De esta manera se establecen redes diferentes.

Para lograr el establecimiento del sistema se tienen que conectar cada una de las redes existentes de la forma "*Host-only*". La máquina física lo interpreta como la conexión entre dos máquinas de forma directa, es decir, con el cable de red cruzado. Así se pueden comunicar todas las redes con la PC física, pero, para establecer la conexión con las máquinas virtuales es necesario configurar la puerta de enlace a cada una de ellas.

La puerta de enlace (*gateway*)se configura tanto en el Sistema Operativo instalado como en los archivos de red que aparecen en la máquina física cuando se hace este tipo de conexión. Estos archivos son similares al existente en la PC física como conexión de área local, los cuales el sistema identifica como conexiones *Vmnet1*,2,3…etc.

Es necesario que a pesar de que existan varias redes diferentes trabajando, se debe especificar la puerta de enlace de cada una de ellas, de lo contrario no se puede ver ninguna de las redes, solamente se comunicarían con la PC física. ***Ver figura 2.14.***

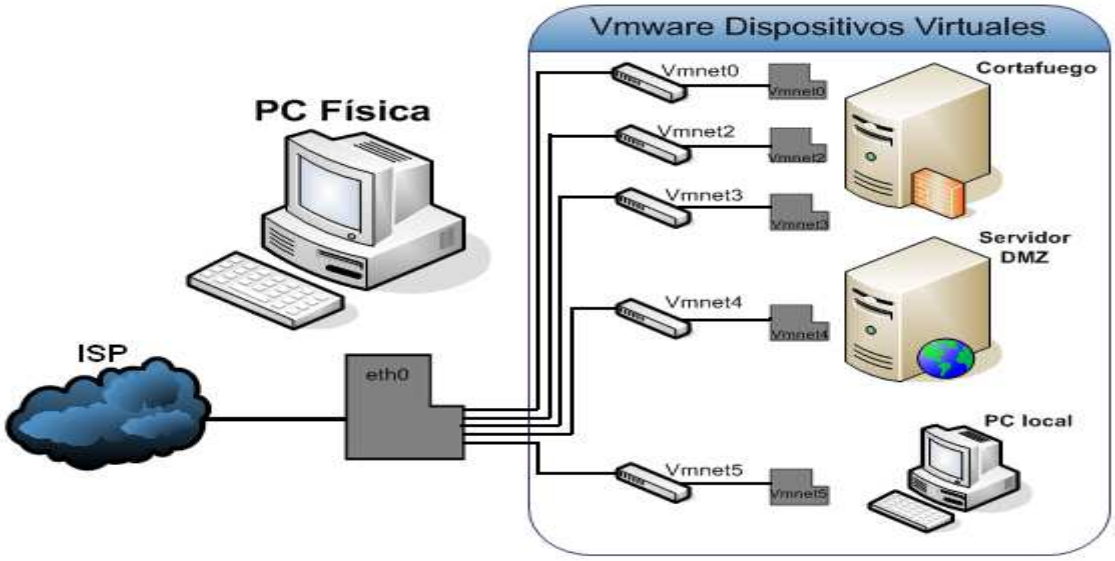

Figura 2.14: Configuración tipo "Host-only".

Fuente: CentOSVMware Workstation

Todas las máquinas están conectadas a la tarjeta de red física, aunque la *Vmnet0* se puede configurar como "*Bridged*" para tener acceso a la red exterior o como "*Host-only*" y probar con la PC física como ISP. Las redes empleadas son:

1. La red 10.30.6.0 para *Vmnet0*.
2. La red 192.168.3.0 para *Vmnet2*.
3. La red 192.168.10.0 para *Vmnet3*.
4. La red 192.168.4.0 para*Vmnet4*.
5. La red 192.168.11.0 para *Vmnet5*.

En este caso se mantienen las tres tarjetas de red en el cortafuego. Como ya se explicó anteriormente la conexión del *Vmnet0* puede ser a la PC física o a la red externa, mientras que a las demás interfaces de red se le especifica la puerta de enlace.En cuanto a la comunicación entre las redes 192.168.3.0 y 192.168.4.0, que es la comunicación del Cortafuego con la DMZ, se le establece como puerta de enlace de la red 192.168.3.0 la dirección 192.168.4.1, y a la red 192.168.4.0, la 192.168.3.1. En la comunicación del Cortafuego con la red localse establece la puerta de enlace de la red 192.168.10.0, la dirección 192.168.11.1, y a la red 192.168.11.0 la dirección 192.168.10.1. (Figura 2.15)

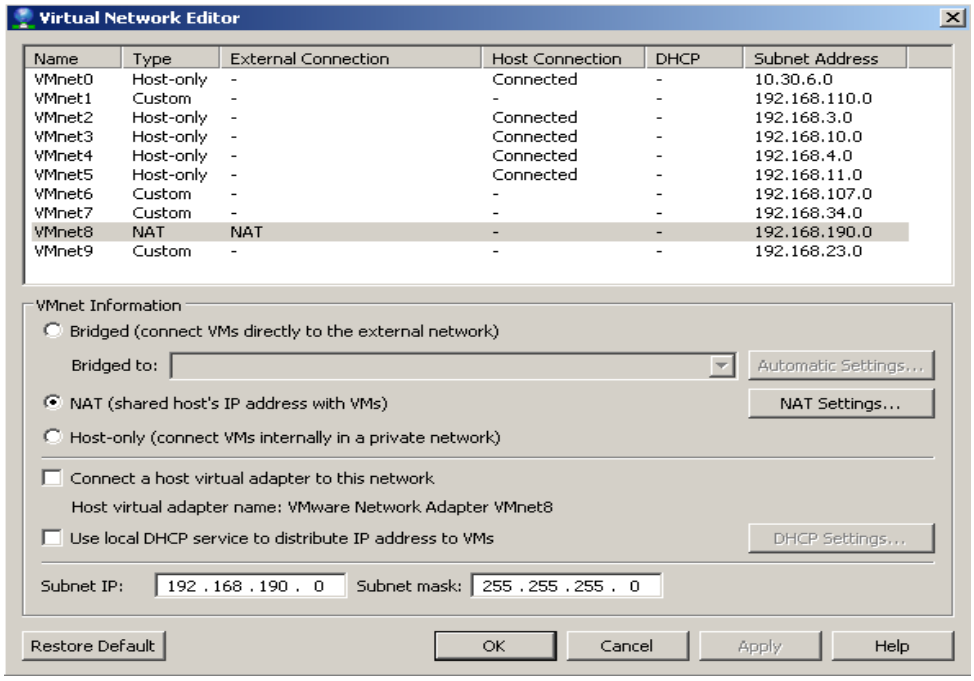

Figura 2.15: Configuración de la red desde el editor virtual de red del Vmware.

Fuente: CentOSVMware Workstation

Si en algún momento no se deseara la comunicación con la máquina física, solamente se debe especificar en una de las cadenas de *Iptables* del Cortafuego la denegación de tráfico de la dirección de dicha máquina.

2.6 Cortafuego. Conformación y configuración del *IPtables*.

Los Cortafuegos son poderosos y muy populares en las redes de datos al tenerse en cuenta cuando se habla de política de seguridad. El *IPtable* es una de las herramientas más utilizadas porque con ellas se realiza al NAT (*Network Adress Traslation*) deseado entre las redes escogidas y el filtrado de paquetes.

Para la red implementada las cadenas de *iptables*no son numerosas porque su arquitectura es sencilla. Las peculiaridades que presenta están en que el Cortafuego tiene tres interfaces y la política creada es establecer saltos (NAT) específicos.

Los saltos se realizan desde la zona externa hacia la DMZ, y de esta hacia la red local. Esto ocurre en los dos sentidos de transmisión, no siendo así en la conexión

directadesde el ISP con la red local. Así se protege la red interna, se controla todo el tráfico enviado y recibido, y mediante las cadenas de *iptables* implementadas se crean términos de seguridad con respecto a la Zona Desmilitarizada.***Ver figura2.16.***

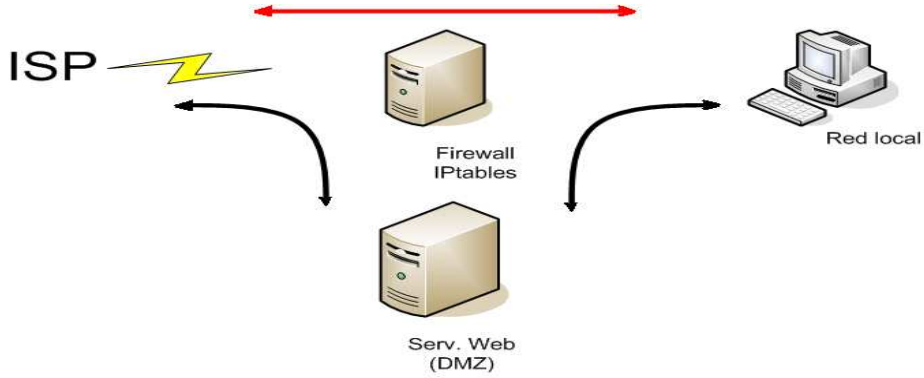

Figura 2.16: Sentido del NAT en el firewall.

Fuente:CentOSVMware Workstation

Para el buen funcionamiento del Cortafuego con los requerimientos deseados, es necesaria la implementación de algunas cadenas de *Iptables* en su fichero de configuración. Como en muchos de los casos en los servidores Linux, se realiza la instalación del paquete a utilizar mediante el "*yum*"**yum instal iptables**.

Yum es una herramienta sumamente útil para el manejo de paquetería RPM. Se hace alusión a esto ya que para las instalaciones y desinstalaciones de paquetes en los Sistemas de CódigoAbierto es muy usado y se hace muy sencilla esta operación mediante su utilización. Con el paquete *IPtable* instalado completamente se pasa a trabajar sobre él y así realizar los cambios pertinentes en el *firewall*.

Este elemento trae algunas políticas por defecto que en mucho de los casos no son las adecuadas para los operadores. Por esta razón las mismas deben ser borradas e implementar las nuevas reglas para el sistema.

Existen variables con las cuales se trabaja que especifican el tipo de cadena, interfaces, puertos, direcciones IP, etc. Las reglas a crear se configuran y quedan almacenadas en el fichero **/etc/sysconfig/iptables.** Una vez creadas estas reglas se arranca el servicio de

IPtables mediante el ***service iptables start***. Si se realizan modificaciones en el fichero de configuración, una vez establecido el servicio, entonces se realiza***service iptables restart***, para detener el mismo se usaría ***serviceiptables stop***. Otras de las habilidades que presenta el servicio de *Iptables* es que puede comenzar con el arranque del sistema, y para esto se usa***chkconfig iptables on.***Varias de las cadenas que se usan para el funcionamiento de *IPtables* implementados son:

Cadenas existentes en las tablas de salto y filtrado del IPtable:

- iptables −t nat −A PREROUTING −i eth0 −p tcp −−dport 80 −j DNAT −−to destination 192.168.3.2:80
- iptables −t nat −A PREROUTING −i eth1 −p tcp −−dport 80 −j DNAT −−to destination 10.30.6.23:80

Las cadenas anteriores muestran la forma y el sentido en el cual se realizan los saltos. Como se puede observar, -A abre una cadena de preenrutamiento (*PREROUTING*) para un tráfico desde la interfaz eth0, con un DNAT a la dirección de red 192.168.3.2. Se usa *(--to-destination*) para indicar el destino de dicho tráfico. Para una segunda cadena ocurre lo mismo pero en el sentido inverso. Ahora el tráfico de la interfaz eth1 realiza un DNAT hacia la dirección 10.30.6.23.

- iptables −A INPUT −s 192.168.10.0/24 −o eth1 −j ACCEPT

Esta cadena especifica la entrada de tráfico hacia la Zona Desmilitarizada desde la red militarizada. Indica la apertura de una cadena (-A) de entrada de tráfico (IMPUT) desde la dirección de red 192.168.10.0/24hacia la interfaz de salida (-i) eth1 aceptado (ACCEPT).

- iptables −t nat −A POSTROUTING −s 192.168.3.0/24 −o eth2 −j MASQUERADE
- iptables −t nat −A POSTROUTING −s 192.168.10.0/24 −o eth1 −j MASQUERADE

En este segundo caso, el NAT realizado es entre la DMZ y la red local (LAN) a diferencia del primer caso. La estructura de la cadena es similar desde el punto de vista del significado. Sólo cambian algunos aspectos como las direcciones IP. Otro de los aspectos nuevos es *MASQUERADE*, con el significado del enmascaramiento de la información hacia su destino. Es bueno aclarar la necesidad de establecer el reenvío de paquetes ipv4 para este sistema, de lo contrario, las cadenas de reenvío quedarían inutilizables.

- iptables −A FORWARD −s 192.168.3.0/24 −d 192.168.10.0/24 −j DROP

Ésta es otro tipo de cadenas, al igual que las que vienen a continuación. Son cadenas de denegación de tráfico (DROP). Esta cadena no permite reenviar tráfico desde la DMZ hacia la red militarizada.

- iptables −A FORWARD −s 192.168.10.0/24 −d 192.168.3.0/24 −j DROP

Ésta cadena evita el reenvío de paquetes ipv4 pero en el sentido contrario, desde la red local hacia la Zona Desmilitarizada.

- iptables −A INPUT −s 192.168.3.0/24 −i eth1 −j DROP

La sintaxis anterior muestra cómo se evita todo tipo de tráfico entrante al cortafuego por la interfaz eth1.

- iptables –A FORDWARD –s 192.168.10.0/24 –o eth0 –j DROP
- iptables –A FORDWARD –s 10.30.6.0/24 –o eth2 –j DROP

Estas dos últimas cadenas paran todo el tráfico entre las direcciones especificadas logrando de esta manera los saltos deseados.

Lo antes expuesto está organizado en el mismo orden que en el *firewall*. Este es un aspecto muy importante ya que el orden de estas cadenas son determinantes en el funcionamiento del *IPtables*. Esta herramienta comienza a leer las cadenas desde la línea 1 hasta la última. Por esta razón, las cadenas de denegación de tráfico están al final.

2.7 Activación del reenvío de paquetes de IPv4 y de rutas en las tarjetas de red en los Sistemas Operativos.

Para reenviar los paquetes en la red esnecesaria la activación de un servicio de reenvío de paquetes IPv4 en los dispositivos conectados. La puesta en marcha de este servicio es muy importante en el *Firewall* pues sus funciones están en el manejo de información de una dirección a otra en la red.

Para activar dicha función en Linux modo texto, solamente se debe ejecutar el archivo de configuración **/etc/sysctl.config**, y establecer 1 para activar el servicio o bien 0 para mantenerlo inactivo.

```
vim /etc/sysctl.conf
```

Y cambiando net.ipv4.ip_forward = 0 por net.ipv4.ip_forward = 1:

```
net.ipv4.ip_forward = 1
```

Otra vía de realizar esto sin necesidad de entrar al fichero de configuración es mediante **echo 1 > /proc/sys/net/ipv4/ip_forward.**Para aplicar el cambio, sin reiniciar el sistema, solo es necesario ejecutar lo siguiente:

```
sysctl -w net.ipv4.ip_forward=1
```

De esta manera queda configurado el reenvío de paquetes versión cuatro para el *Firewall* (*IPtables*), completando junto con las cadenas establecidas las reglas para el manejo de información en su funcionalidad.

En cuanto a las rutas, es necesario su establecimiento para poder encaminar el tráfico entre las diferentes direcciones.
En el cortafuego, con la existencia de más de una tarjeta de red y por su funcionalidad, hay que establecer rutas las cuales van a ser almacenadas en una tabla de rutas. Estas rutas van a estar dirigidas hacia la DMZ, la red local y el ISP. Para Linux existen varias formas de realizar esta función. Para el caso de CentOS se realiza de la forma mostrada a continuación:

- route add –net (dirección de red de destino) netmask (máscara de dicha dirección) gw (puerta de enlace de esa red)

Las rutas creadas son las siguientes:

- route add –net 192.168.3.0 netmask 255.255.255.0 gw 192.168.3.1 Esta sería la ruta por donde van a viajar los paquetes destinados a la DMZ.
- route add –net 192.168.10.0 netmask 255.255.255.0 gw 192.168.10.1 Esta es la ruta con destino a la red local.
- route add –net 10.30.6.0 netmask 255.255.255.0 gw 10.30.6.24 Esta última es la ruta para la salida hacia el proveedor de servicios.

Para CentOs esto se comprueba con **route -nL** lo que muestra las rutas establecidas en dicho sistema.

2.8 Instalación y configuración del Servidor Apache (www).

Como se menciona anteriormente en estos sistemas de código abierto, la utilización del "*yum*" es muy importante. Para la instalación del servidor Web, se utiliza esta herramienta, la cual se encarga de instalar todos los paquetes referidos a httpd.

2.8.1 Instalación del Servidor web Apache.

La instalación del servidor web apache es relativamente sencilla, sólo se debe teclear en el terminal el siguiente comando. Hay que recordar que esto se realiza como usuario *root* del sistema.

```
yum instal –y httpd
```

De esta manera queda instalada la paquetería correspondiente al servidor www, sólo faltaría lograr su configuración.

2.8.2 Configuración del Servidor Apache.

Una vez realizada la instalación de Apache se pasa a la configuración del mismo. La configuración de este servidor se realiza mediante dos ficheros de configuración distintos. Uno de configuración general del servidor web apache, y otro para indicarle al servidor apache los dominios virtuales que deben ser cargados al sistema.

La siguiente ruta contiene el fichero de configuración principal de Apache:

```
cd /etc/httpd/conf/
```

Siguiendo un orden para ver el archivo de configuración:

```
httpd.conf magic
```

La carpeta donde deberán ser añadidos los ficheros de configuración de los dominios virtuales es en la siguiente ruta:

```
vim httpd.conf
```

Al seguir estos pasos se puede observar el archivo de configuración de apache con todas sus directivas, las cuales serán modificadas si es necesario.Ver figura 2.17

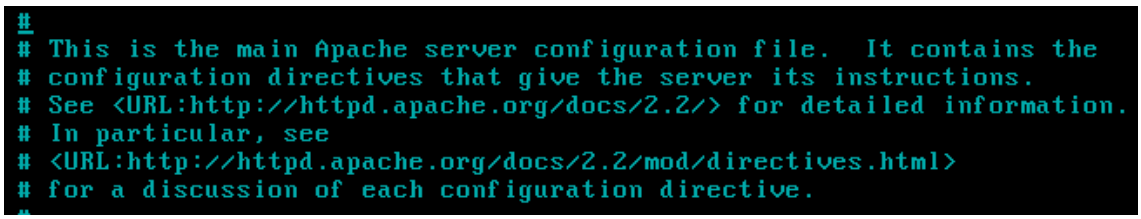

Figura 2.17: Encabezado del archivo de configuración de apache.

Fuente:(Como instalar apache mysql y php en Ubuntu 5.4, 2012)

Después de entrar al fichero de configuración, se pueden observar varias directivas las cuales influyen en el funcionamiento futuro del servidor. La lista comienza con:

- **ServerTokens:**

Esta directiva limita la cantidad de información que será mostrada por el servidor web apache como puede ser, la versión del servidor web apache que se tiene instalado o los servicios que corren paralelamente con apache como php o MySQL. Existen varias formas de configurar esta directiva con especificidades cada una de estas. Las formas en que se puede realizar están, ServerTokens ProductOnly, el Minimal, el Os, y el Full.

Para el caso del sistema instalado se escoge el *OS*, mostrando el tipo de servidor, la versión y el Sistema Operativo sobre el cual trabaja.

- **ServerRoot:**

Esta directiva le indica al servidor web la ubicación donde se almacenan los ficheros de configuración de apache:

ServerRoot “/etc/httpd”.

- **Directiva Timeout:**

Esta directiva indica el número de segundos antes de que se cancele una conexión por falta de respuesta. Su valor por defecto es 120 aunque puede variar de acuerdo a lo deseado por el administrador.

- **Directiva Listen:**

Listen permite asociar Apache a una dirección y/o puerto específico además del predeterminado.

```
Listen 192.168.3.2:80
Listen 80
```

- **Directiva User:**

Esta directiva especifica qué usuario es el que ejecuta los procesos del servidor web y en consecuencia los permisos de lectura y escritura que se aplican sobre los recursos

```
User apache
```

- **Directiva Group:**

Esta directiva especifica qué grupo es el que ejecuta los procesos del servidor web y en consecuencia los permisos de lectura y escritura que se aplican sobre los recursos.

```
Group apache
```

- **Directiva ServerAdmin:**

Esta directiva especifica la persona a la que se le debe notificar los problemas referentes al portal web, esto a través de su cuenta de correo.

```
ServerAdmin root@localhost
```

- **Directiva ServerName:**

Esta directiva especifica el nombre y puerto que el servidor utiliza para identificarse. Con una correcta configuración, este valor se puede determinar automáticamente, pero es recomendable especificarlo explícitamente para evitar problemas durante el arranque.

```
www.colasbas.com:80
```

2.8.3 Otras configuraciones.

Este tema hace alusión a otro tipo de configuraciones que pueden ser realizadas para el buen funcionamiento del servidor.

Una de estas es lograr enlazar la dirección IP con el dominio del servidor. Para poder crear esto se establece el comando:

```
vim /etc/hosts
```

Con esto se logra entrar a un ficheroen el cual se puede enlazar estos dos parámetros.

Otra de las cosas que se pueden realizar es la creación de paginas html para ver el correcto funcionamiento del servidor. Par esto se escribe:

```
cd /var/www/html/
```

Y siguiente a esto

```
vim hello.html
```

Con esto se pueden crear numerosas páginas html, después del *vim* nombre de la página¨. Para la prueba realizada se crea la siguiente página.

<-html>
<-head>title **las compras**
<-/head>
<-body>
todos los mercados
<-/body>
<-/html>

Para la comprobación de la misma solamente se debe poner:

```
wget www.colasbas.com/hello.html
```

La respuesta del servidor es la siguiente.***Ver figura 2.18***

Figura 2.18: Comprobación del funcionamiento del servidor apache.

Fuente: Fuente: CentOSVMware Workstation

2.9 Resumen del Capítulo.

Como se pudo observar, el capítulo muestra la instalación de un conjunto de máquinas mediante el *VMware*. Se instaló un servidor en la DMZ con funcionalidad web, un *IPtables* para realizar NAT y filtrado de paquetes entre tres zonas (ISP, DMZ, y una red local),y una PC para los clientes en la red militarizada. De esta manera se crea una

pequeña red con la cual se pueden hacer pruebas de seguridad desde un entorno virtual. En la figura 2.19 se muestra la respuesta del servidor Apache instalado.

Figura 2.19: Respuesta del Servidor Apache instalado.

Fuente: Fuente: CentOSVMware Workstation

Conclusiones.

Este trabajo culminó con el estudio de diversos temas de seguridad Informática. Al plasmar conceptos y métodos de control de acceso, autenticidad, disponibilidad, etc. Se ha logrado aumentar el conocimiento de los sistemas de control, supervisión y monitorización de hardware y software de *Open Source*. El estudio de las especificidades de Linux fue muy importante ya que ayuda a entender claramente elementos como los *IPtables* para la implementación de cortafuegos, y así brindar gran seguridad en redes privadas. También para establecer la seguridad del flujo de información de la red, con la utilización de programas de encriptación.

Para el sistema montado la creación de una Zona Desmilitarizada (DMZ) es de gran utilidad. Esto es debido al cortafuego implementado que separa el acceso de la red externa con las redes internas creadas. Esto brinda un alto nivel de seguridad para el acceso a los Servidores y a la red militarizada desde el punto de vista físico, y desde el punto de vista lógico, gracias a las reglas y políticas creadas y las que pueden implementarse a la hora de establecer las cadenas del *IPtables*.

- Se logra la puesta en marcha de una pequeña red con la capacidad de realizar pruebas de seguridad informática, sin afectar la red física.
- El análisis de los sistemas de código abierto fue muy importante para la implementación de la red.
- La herramienta *VMware* constituyó el centro de funcionamiento gracias a sus capacidades para la virtualización y conexión a lared.
- La puesta en marcha del Cortafuego (*IPtables*) crea gran nivel de seguridad a la arquitectura de red planteada.
- El análisis de seguridad estudiado e implementado, brinda un camino a seguir para mejorar dicha arquitectura en cuanto a su robustez y establecer mejorados niveles de seguridad en los sistemas de código abierto.

Recomendaciones

- Continuar el estudio de los métodos y herramientas de seguridad de código abierto dado a su importancia actual.
- Seguir el trabajo con el *VMware* para realizar este tipo de función.
- El perfeccionamiento de las políticas de **firewall** para la implementación de las cadenas de *IPtables*.

Ardita, J. (2010). *Aspectos prácticos de seguridad.* Recuperado el 5 de Julio de 2012, de http://ebookbrowse.com/aspectos-practicos-y-registro-confecoop-2010-pdf-d46054561

Arquitectura de Sistemas Computarizados, Instalación de Firewall . (2012). Recuperado el 15 de Agosto de 2012, de http://dns.bdat.net/documentos/cortafuegos/x235.html,

Ayuda instalar y configurar apache http y php 5 en Centos Creative Commons. (2009). Recuperado el 30 de Julio de 2012, de http://www.ecualug.org/2009/07/13/forums/ayuda_instalar_y_configurar_apache_http_y_php_5_en_centos.

Barrios, J. (2006). *Configuración de servidores GNU/Linux. Alcance libre.* Recuperado el 4 de Julio de 2012, de http://bakara.files.wordpress.com/2011/03/configuracion_servidores_linux-20110929-septiembre.pdf

Borghello, C. (2005). *Linux Máxima seguridad.*

Borghello, C. (2008). *Seguridad Informática, sus implicaciones e implementación* . Recuperado el 18 de Agosto de 2012, de http://www.informatica-juridica.com/trabajos/PRINCIPALES%20SUJETOS%20AGENTES%20EN%20EL%20UNDERGROUND.pdf

Chacón, D. (2009). *IDS/IPS.* Obtenido de Escuela Politécnica Nacional.

Commons, A. i. (2009). Recuperado el 30 de Julio de 2012, de http://www.ecualug.org/2009/07/13/forums/ayuda_instalar_y_configurar_apache_http_y_php_5_en_centos.

Como instalar apache mysql y php en Ubuntu 5.4. (2012). Recuperado el 23 de Julio de 2012, de TechnoBlog: http://www.technoblog.com.ar/index.php/2010/02/como-instalarapachemysqlphp-en-ubuntu-5-4/.

Creación de máquinas virtuales con VMware Workstation. (2012). Recuperado el 1 de Agosto de 2012, de http://www.vmware.com/files/pdf/dmz_virtualization_vmware_infra_wp.pdf,

Cristian, F. (2005). *Linux máxima seguridad.*

Cristian, F. (2008). *Seguridad Informática, sus implicaciones e implementación.*

Distribuciones libres de GNU/Linux . (2012). Recuperado el 20 de julio de 2012, de Creative Commons Atribución-SinDerivadas 3.0 Estados Unidos de América: http://www.gnu.org,

Echarri, W. (2008). *Guía de referencia Debian.*

Escartín, J. (2005). *Servidor Linux para conexiones seguras de una LAN a Internet.* Recuperado el 17 de Agosto de 2012, de http://www.computronixbras.com/cursos/RLP/redesdecomputadores/teseLinux/ManualdeUsuarioDebianSarge31-by-Jose%20Antonio%20Escartin.pdf

GNU/Linux CentOS . (2012). Recuperado el 10 de Agosto de 2012, de Comunidad de GNU/Linux CentOS Nicaragua: http://es.tldp.org/curso_linux/curso_linux.html

Guia avanzada redes Linux con TCP/IP. (2004). Madrid, España: PEARSON EDUCACION S.A.

Interfaces de red. (2012). Recuperado el 3 de Agosto de 2012, de http://es.kioskea.net/contents/detection/ids.php3

La defensa en profundidad aplicada a los sistemas de información. (2006).

Las diez vulnerabilidades de seguridad más críticas en aplicaciones web. (2005).

Linux Security HOWTO. (2006). Recuperado el 2 de Julio de 2012, de http://tldp.org/HOWTO/pdf/Security-HOWTO.pdf

Ovarzo, M. (2012). *Tabla mangle y rutas múltiples.* Recuperado el 12 de Agosto de 2012, de http://www.mail-archive.com/linux@listas.inf.utfsm.cl/msg17786.html.

Ramos, A. (2011). *Seguridad Perimetral.* Madrid, España.

Servidor virtual con VMware. (2012). Recuperado el 1 de Agosto de 2012, de http://vmware.com/web/vmware/downloads

Villalon, A. (2006). *Seguridad en UNIX y Redes. RedIRIS.* Recuperado el 10 de Julio de 2012, de http://www.rediris.es/cert/doc/unixsec/unixsec.pdf

Workstation, C. d. (2012). Recuperado el 1 de Agosto de 2012, de http://www.vmware.com/files/pdf/dmz_virtualization_vmware_infra_wp.pdf,

Zegarra, S. (2011). *Configuración de Apache.* Recuperado el 12 de Agosto de 2012, de Blog Sistemas Web: http://mitareaperu.blogspot.com/2011/05/clase-linux-configuracion-de-apache-en.html,

Glosario de términos

DMZ: Zona Desmilitarizada.

HTTP: Protocolo de Transporte de Ipertexto.

FTP: Protocolo de Transferencia de Archivos.

DAC: Control de Acceso Discrecional.

LAN: Red de Área Local.

Ipv4: Protocolo de Internet versión 4.

Ipv6 Protocolo de Internet versión 6.

SI: Sistema de Información.

VoIP: Voz sobre el Protocolo de Internet.

IDS: Sistema de Detección de Intrusos.

HIDS: Sistema de Detección de Intrusos en Terminales (HostIDS).

NIDS; Sistemas de Detección de Intrusos de Red.

DIDS: Sistema de Detección de Intrusos Distribuidos.

www: Extensa Red Mundial.

VPN: Redes Privadas Virtuales.

IPS: Sistemas de Prevención de Intrusos.

IP: Protocolo de Internet.

NOC: Centro de Operaciones de la Red.

SO: Sistema Operativo.

TCP: Protocolo de Control de Transporte.

UDP: Protocolo de Datagrama de Usuario.

DNS: Servidores de Nombre de Dominio.

PC: Máquinas Computadoras.

PGP: Elegante y Buena Privacidad.

SSL: Asegurar Niveles de Cuentas.

POP: Protocolo de Ofiscina de Correo.

SMTP: Protocolo de Simple Transferencia de Correo.

VM: Maquina Virtual (Virtual Machines).

EMC: Corporation que proporciona la mayor parte del software de virtualización disponible para ordenadores compatibles X86.

CPU: Unidad de Control y Proceso.

RAM: Memoria de Acceso Aleatorio.

USB: Puerto Serial Universal.

NAT: Traslado de Direcciones del Protocolo de Internet (IP).

DNAT Destinación del Traslado de Direcciones del Protocolo de Internet (IP).

Off: Apagado.

On: Encendido

HTML: Siglas de las PáginasWebEstáticas.

ISP: Proveedor de Servicios de Internet.