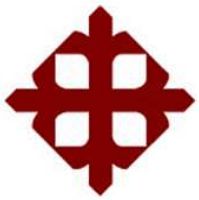


UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TÌTULO:VULNERABILIDADES Y SEGURIDAD EN REDES TCP/IP

AUTORES:
HENRY CRISTHIAN MANCHENO TORRES
IVETTE LORENA ROBLES CORONEL

TUTOR:
MARIA LUSMILA RUILOVA AGUIRRE

Guayaquil, Ecuador
2013

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por **Henry Cristhian Mancheno Torres e Ivette Lorena Robles Coronel**, como requerimiento parcial para la obtención del Título de **Ingeniero (a) telecomunicaciones.**

TUTOR (A)

_____
ING. MARIA LUSMILA RUILOVA AGUIRRE

REVISOR(ES)

_____
ING. LUIS PINZON BARRIGA

_____
ING. CARLOS ROMERO ROSERO

DIRECTOR DE LA CARRERA

_____
ING. ARMANDO HERAS SANCHEZ

Guayaquil, a los 3 del mes de Octubre del año 2013

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Nosotros,

DECLARAMOS QUE:

El Trabajo de Titulación **Vulnerabilidad y seguridad en redes Tcp/Ip.** Previa a la obtención del Título **de Ingeniero (a) telecomunicaciones con Mención en Gestión Empresarial en Telecomunicaciones** derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, a los 3 del mes de Octubre del año 2013

AUTOR (ES)

_____
HENRY CRISTHIAN MANCHENO TORRES

_____
IVETTE LORENA ROBLES CORONEL

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGFENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Nosotros,

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la **publicación** en la biblioteca de la institución del Trabajo de Titulación: **Vulnerabilidad y seguridad en redes Tcp/Ip**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 3 del mes de Octubre del año 2013

AUTOR (ES):

_____
HENRY CRISTHIAN MANCHENO TORRES

_____
IVETTE LORENA ROBLES CORONEL

AGRADECIMIENTO

A nuestro Padre Celestial por darnos vida, fuerza e iluminarnos en cada uno de los pasos emprendidos para culminar nuestra carrera universitaria.

A nuestros padres y familiares por su apoyo incondicional en todas las metas que nos hemos propuesto y por sus sabios consejos para superar cualquier adversidad que se nos ha presentado en este trayecto.

A nuestro Decano, el Ing. Manuel Romero Paz, que con su experiencia y paciencia nos condujo en el desarrollo de nuestro proyecto de tesis, siempre pendiente en cualquier detalle durante la implementación y revisión del mismo.

A todos nuestros profesores que en el transcurso de nuestra carrera supieron brindarnos sus conocimientos para finalmente ponerlos en práctica en nuestra vida profesional.

A nuestros compañeros por compartir con nosotros alegrías, tristezas, experiencias y oportunidades durante todo nuestro ciclo universitario.

HENRY CRISTHIAN MANCHENO TORRES
IVETTE LORENA ROBLES CORONEL

DEDICATORIA

Dedicamos este trabajo a todas las personas que nos han apoyado directa e indirectamente y en especial a nuestros padres, que con su ejemplo de amor y constancia, han influido en nuestras personalidades para poner el entusiasmo, dedicación y esfuerzo, para llegar a la culminación de nuestros logros profesionales

HENRY CRISTHIAN MANCHENO TORRES
IVETTE LORENA ROBLES CORONEL

ÍNDICE GENERAL

ÍNDICE DE GRÁFICOS

RESUMEN

El siguiente trabajo trata acerca del estudio de la VULNERABILIDADES Y SEGURIDAD EN REDES TCP/IP mediante la creación de un entorno virtual de red creado con ayuda del software VMWare, para la evaluación de diferentes políticas de seguridad implementadas en los cortafuegos de una zona desmilitarizada (DMZ). Se abordan conceptos generales tales como : la seguridad en las redes informáticas, los diferentes tipos de ataques que pueden ocurrir en un sistema, algunos de los métodos que existen para detectar y evitar estos ataques, además trata sobre las zonas desmilitarizadas y conceptos relacionados con estas. También se presenta la implementación de una topología de red mediante su virtualización. Se explica la configuración de un servidor Web, la configuración del cortafuego y las políticas establecidas en el mismo. Las máquinas virtuales de los servidores y clientes corren sobre CentOS como sistema operativo escogido. Finalmente se tratan algunas técnicas para de realizar test de penetración a la red protegida, y se explica cómo se ejecutó el test en la red de máquinas virtuales.

Palabras Claves:VULNERABILIDADES Y SEGURIDAD EN REDES TCP/IP,Zonas Desmilitarizadas, DMZ, cortafuegos, hacking ético, máquinas virtuales, VMWare.

ABSTRACT

The following work deals with the creation of a network virtual environment created with the help of VMWare software for evaluating different security policies implemented in the firewall demilitarized zone (DMZ). It addresses general concepts such as: security in computer networks, the different types of attacks that can occur in a system, some of the methods that exist to detect and prevent these attacks, and discusses the demilitarized zones and concepts related to these. It also presents the implementation of a network topology through its virtualization. It explains the setup of a Web server, firewall settings and policies set out therein. Virtual machines servers and clients running on CentOS operating system chosen. Finally, try some techniques for performing penetration testing to the protected network, and explain how you ran the test on the virtual machine network.

Key words: Network security,demilitarized zones, DMZ, firewalls, ethical hacking, virtual machines, VMWare.

CAPÍTULO No1.

INTRODUCCIÓN

En la actualidad las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte por mínimo que sea puede llegar a comprometer la continuidad de sus operaciones. La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez, es mayor el número de atacantes, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

En el mundo siempre cambiante de las comunicaciones globales, conexiones baratas a Internet y desarrollo rápido de software tiene un tema clave a tratar, la seguridad. Este es un requisito básico ya que las comunicaciones globales son 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, no necesariamente informático 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.

El mayor por ciento de la información mundial de los mensajes viajan por las redes de datos, por lo cual no está exenta de ataques piratas. Existen muchas formas de afectar a los sistemas de transmisión y redes de datos así como personal maligno (hacker) cuya función se resume en hacer daño a los sistemas de información.

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 técnicas más robustas y sistemas de seguridad más fiables. No obstante, los programas malignos (malware) evolucionaron así como también lo hicieron sus creadores.

La seguridad de la información, es un aspecto vital en la sociedad de la información, donde dicha información ya alcanza un rol protagónico entre los activos con que

cuentan las organizaciones para el normal desempeño de su gestión. De modo que proteger la información como un activo de tan elevada importancia, se convierte cada vez más un proceso con grandes retos y exigencias por parte de los especialistas. En este sentido, es cada vez más importante, adoptar estrategias y métodos, que permitan implantar políticas que permitan elevar los niveles de seguridad en las redes informáticas ya que por ellas circula la mayor parte de la información de las organizaciones, y su pérdida o alteración pueden acarrear consecuencias nefastas para las mismas.

Evaluar la seguridad de las redes, puede comprometer, en determinados escenarios la integridad y confidencialidad de la información de una organización, ya que la misma puede quedar expuesta a usuarios no autorizados o ser modificada por la ocurrencia de un error de ejecución de un especialista. Por otro lado, en entornos de aprendizaje o entrenamiento, no se debería exponer la información resguardada en servidores de una red para demostrar la validez o efectividad de una determinada política de seguridad.

Todo esto justifica el planteamiento del siguiente problema de investigación:

1.1 Problema de la investigación

Necesidad de estudiar de forma segura la efectividad de las diferentes políticas de seguridad en los cortafuegos de redes desmilitarizadas o DMZ.

1.2 Hipótesis

Si se virtualiza un entorno de red con una zona desmilitarizada mediante la herramienta VMware se permitiría el estudio de políticas de seguridad en los cortafuegos sin riesgos de perder o modificar la información.

1.3 Objetivo general

Creación mediante la herramienta VMware de una topología de red de máquinas virtuales, donde se puedan implementar políticas de seguridad perimetral en el cortafuego de una zona DMZ y que permita el estudio de su efectividad mediante técnicas de hacking ético.

1.4 Objetivos específicos

- El estudio de las tendencias actuales de las técnicas de seguridad informática.

- Selección del software para la virtualización de los servidores y estaciones de trabajo de la red LAN y la DMZ.
- Configuración de la red para crear la topología deseada y las pruebas de conexión.
- Elección del cortafuego y configuración del mismo, según las políticas seleccionadas para asegurar la DMZ.
- Selección de técnicas de hacking ético para estudiar la robustez del cortafuego.

1.5 Metodología de Investigación

1.5.1 Métodos Teóricos:

1. **Histórico-Lógicos:**Para el análisis del objeto de estudio y sus antecedentes históricos, y las tendencias al desarrollo de la aplicación con tecnología que se propone.
2. **Análisis-Síntesis**: Para analizar y sintetizar toda la información relacionada con el tema de la investigación y en la determinación de los hechos que han servido de base para fundamentar la necesidad del sistema que se propone.
3. **Hipotético Deductivo:** Para la elaboración de la hipótesisy deducir de ella consecuencias directamente verificables en la realidad.
4. **Modelación:** Elaborar una aplicación con tecnología de programación Web que permita el seguimiento y evaluación de proyectos de telecomunicaciones.

1.5.2 Métodos empíricos:

1. **Observación**: Para diagnosticar la situación actual que presenta el seguimiento y evaluación de proyectos de telecomunicaciones.
2. **Encuestas y Entrevistas**: Realizadas para el diagnóstico y la validación por criterio de los especialistas.
3. **Análisis documental**: Para la caracterización y desarrollo de la tesis y la elaboración de la Aplicación.

CAPÍTULO No2.

FUNDAMENTOS TEÓRICOS DE LA SEGURIDAD.

Borghello, C. (2005):

> Para comenzar el análisis de seguridad primeramente se debe conocer lo que se debe proteger: la información. De esta manera se define dato como la unidad mínima con la cual se compone cierta información. Mientras que la información es un conjunto de datos que tiene un significado específico más allá de cada uno de estos. Existen distintos tipos de información: las públicas y las privadas. Las públicasson aquellas que pueden ser visualizadas por cualquier persona, mientras que las privadas serán visualizadas solamente por un grupo determinado de personas autorizadas que trabajan con ella.

2.1 Fundamentos de la seguridad de la información.

Un concepto primordial para la comprensión del tema es el de “integridad de la información” la cual no es 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.

Para Borghello, C. (2001):

> Otro concepto importante es la “disponibilidad u operatividad” que es la capacidad de la información de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y software correctamente funcionando y que se respeten los formatos para su recuperación en forma satisfactoria.

Segu.Info (s.f.):

> “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 [5].

Para Escartín, V. (2005):

> "El control" permite asegurar que sólo los usuarios autorizados pueden definir cómo y cuándo permitir el acceso a la información. Por otro lado, la "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**.**

2.2 Vulnerar para proteger.

Para Luna, D. & Solís, E. (2002:8) los intrusos:

> Utilizan diversas técnicas para quebrar los sistemas de seguridad de una red. Básicamente buscan los puntos débiles del sistema para poder filtrarse en ella. El trabajo de los administradores y testersno difiere mucho de esto. En lo que sí se diferencian y por completo, es en los objetivos: un intruso penetra en las redes de computadoras para distintos fines (investigación, daño, robo, etc.) mientras que un administrador lo hace para poder mejorar los sistemas de seguridad.

Comentario [f1]: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDUQFjAB&url=http%3A%2F%2Frepositorio.pucesa.edu.ec%2Fjspui%2Fbitstream%2F123456789%2F80%2F1%2F75205.pdf&ei=gTFCUvGpDIro8gT_0oCwCg&usg=AFQjCNEw9Q6biXLLtz4AjhO4ad3e01xrUQ&sig2=W_jDXV9ANd0TRM_5CRvtVg

Los intrusos cuentan con grandes herramientas como los escaneadores de puertos, robo de contraseñas, software de análisis de vulnerabilidades, un administrador cuenta con todas ellas empleadas para bien, además de los sistemas de detección de intrusos y los sistemas de rastreo de intrusiones.

Para Callegari, O. (s.f.:198):

> Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se lo conoce como test de penetración, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces contra los intrusos.

Comentario [f2]: http://cdigital.udem.edu.co/TESIS/CD-ROM28692008/13.Capitulo7.pdf

http://www.segu-info.com.ar/proteccion/proteccion.htm

http://www.rnds.com.ar/articulos/034/RNDS_198W.pdf

Cabaleiro, J. (s.f.):

> Un test está totalmente relacionado con el tipo de información que se maneja en cada organización. Por consiguiente, según la información que deba ser protegida, se determinan la estructura y las herramientas de seguridad; no a la inversa.

El software y el hardware utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina "políticas de seguridad internas" que cadaorganización (y usuario) debe generar e implementar.

2.3 Políticas de seguridad interna.

Para Ardita, J. (2008) las políticas de seguridad interna:

> Surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información. Esta es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales, que está o no permitido en el sistema.

Comentario [f3]: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDQQFjAB&url=http%3A%2F%2Fwww.quadernsdigitals.net%2Findex.php%3FaccionMenu%3Dsecciones.DescargaArticuloSeccionIU.descarga%26articuloSeccion_id%3D1559%26fichero_id%3D447&ei=1zVCUpLSK5LM9gSRzICgCQ&usg=AFQjCNE00XiqdafwPwrdcrH9y5vPIqGEdQ&sig2=qSadXS0bx9SX-i6XG8rSiA

http://repository.ean.edu.co/bitstream/10882/2361/1/AegriaMaria2012.pdf

Borghello, C.(2008):

> A la hora de crear políticas de seguridad hay que enmarcarse en las condiciones reales del sistema sobre el cual se trabaja. No se puede aplicar la misma política de seguridad en 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.

La política de seguridad no es más que una serie de normas y medidas a seguir para mantener la seguridad del sistema. Siempre hay que tener en cuenta que la seguridad comienza y termina con las personas.

Para Escartín, V. (2005) 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 conducta de los

empleados. Es más bien una descripción de lo que desea proteger y el porqué de ello.

Comentario [f4]: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDYQFjAB&url=http%3A%2F%2Fwww.quadernsdigitals.net%2Findex.php%3FaccionMenu%3Dsecciones.DescargaArticuloSeccionIU.descarga%26articuloSeccion_id%3D1559%26fichero_id%3D447&ei=3DZCUqbUFJPO9ASPv4DoBw&usg=AFQjCNE00XiqdafwPwrdcrH9y5vPIqGEdQ&sig2=aCPZAKQwIel9gcK4QLhWvw

2.4 Seguridad lógica.

Para Cabaleiro, J. (s.f.):

> La mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada. La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Comentario [f5]: http://www.segu-info.com.ar/logica/seguridadlogica.htm

http://redes6h1.blogspot.com/2010_04_01_archive.html

http://www.monografias.com/trabajos88/seguridad-e-integridad-sistemas/seguridad-e-integridad-sistemas.shtml

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CEoQFjAD&url=http%3A%2F%2Fsistemascompensar.wikispaces.com%2Ffile%2Fview%2FSEGURIDAD.doc&ei=kjdCUsrdC4W48wThuIGQCg&usg=AFQjCNE8gbgb-hw8InmvUpjdQ67o2wAVvQ&sig2=EZQ6zGyg5-xljsD1Z9S6-Q

Para Villalón, A. (2006):

> La seguridad lógica involucra todas aquellas medidas establecidas por la administración-usuarios y administradores de recursos de tecnología de información para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información.

Los objetivos que la seguridad lógica debe cumplir son los siguientes:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
6. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Comentario [f6]: http://vicentesanchez90.files.wordpress.com/2012/10/seguridad-lc3b3gica.pdf

http://prezi.com/leibxpz3vqrr/seguridad-informatica/

Comentario [f7]: http://www.segu-info.com.ar/logica/seguridadlogica.htm

Para Seguridad Lógica (s.f.):

> También hay que tener en cuenta otras consideraciones, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si

corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

Algunos de los requisitos de seguridad que un sistema debe tener en cuenta son:

1. Identificación y autentificación de roles:es el acceso a la información, también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder del proyecto, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

Para Cabaleiro, J. (s.f.):

2. Limitaciones a los servicios: estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

3. Control de acceso interno y externo: estos controles pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario. Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Comentario [f8]: http://www.segu-info.com.ar/logica/seguridadlogica.htm

2.5 Mecanismos para proporcionar seguridad en las redes informáticas.

Existen múltiples mecanismos para brindar seguridad en las redes informáticas, y evitar el robo de información, la suplantación de usuarios, la modificación de la misma. Entre los más empleados se encuentran:

2.5.1 Cortafuegos (firewall).

Para Cabaleiro, J. (s.f.):

> Un cortafuego o firewall es un sistema (o conjunto de ellos) ubicado entre dos redes, que ejerce una política de seguridad determinada. Este mantiene separada la red interna (de la cual se tiene control) de diferentes tipos de redes externas (de las cual no se tiene control). Es el encargado de proteger una red confiable de una que no lo es (por ejemplo Internet). Permite habilitar el acceso a usuarios y servicios aprobados.

Un cortafuego es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra a través de él y en función de lo que el usuario necesite permite o deniega su paso, protegiendo así la red de intromisiones indeseadas. Su función es, ser una sólida barrera entre la red local y la red exterior.

Para Teuno. (s.f.):

> Permitir o denegar una comunicación, el cortafuegos examina el tipo de servicio al que corresponde, como pueden ser Web, correo o FTP, dependiendo del servicio, este decide si lo permite o no. Además examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

Para Cabaleiro, J. (s.f.):

> En general un cortafuegos es un elemento de hardware o software que se utiliza en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su ubicación habitual es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet, de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna. Un cortafuego puede

Comentario [f9]: http://www.teuno.com/index.php?id=61

http://redcin.blogspot.com/p/firewall.html

Comentario [f10]: http://dspace.ups.edu.ec/bitstream/123456789/205/7/Anexos.pdf

http://www.slideshare.net/marcoslmori/vision-generalinstalacion20121206es

http://www.safavirtual.com/mod/glossary/print.php?id=2917&mode=author&hook=M&sortkey=LASTNAME&sortorder=desc&offset=120

http://www.amesis.org.mx/gt.html

http://modeloosiyprotocolos.galeon.com/

Comentario [f11]: http://geneura.ugr.es/~gustavo/cortafuegos/introduccion.html

https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&ved=0CDQQFjAB&url=http%3A%2F%2Fwww.itescam.edu.mx%2Fprincipal%2Fsylabus%2Fpdb%2Frecursos%2Fr68954.DOCX&ei=CGRCUvfOD4e69gTw0oCgAw&usg=AFQjCNFcWH0tfPpGokfEyN9CDzGLVFMEPw&sig2=Y2eubkZN1-bXtyMcmWalZg

http://ti.uqroo.mx/indexp.php?id=24

http://goc.networktech.com.ar/knowledgebase/19/iQue-es-un-Firewall.html

http://informaticaellacuria.wikispaces.com/Seguridad+en+la+red

permitir desde una red local hacia Internet servicios como Web, correo y FTP, pero no restringe tráfico que puede ser innecesario para nuestro trabajo. También se pueden configurar los accesos que se hagan desde Internet hacia la red local y se pueden denegar todos o permitir algunos servicios como el de Web, DNS, FTP, etc. Dependiendo del cortafuego que tenga también se podrá permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local. Este logra el balance óptimo entre seguridad y accesibilidad.

Los cortafuegos manejan la conectividad por zonas (seguras o no) o por niveles de seguridad, los cuales los establece el responsable de la red, según el grado de permisividad que le imponga al equipo.

Para Zapata, R. (2012):

> Estos sólo deben configurarse según las necesidades o gustos del responsable de la red, cosa que no termina con la instalación. Después de esta, una vez que el usuario se conecta a Internet (o aún antes) comienza a trabajar el programa. Los primeros días de uso pueden ser un tanto engorrosos, ya que tanto el administrador de la red como el programa "aprenden" mutuamente.

Comentario [f12]: http://dspace.espoch.edu.ec/bitstream/123456789/2548/1/18T00524.pdf

Para Morales, H. (s.f.):

> Este aprende las funciones y el programa qué cosas debe dejar pasar, qué bloquear y qué programas dejar conectar, por eso al principio son puras preguntas, hasta que se van conformando las reglas de uso en la medida que el usuario haga determinadas acciones con las alarmas. Con este tipo de aviso el programa pide que se defina la regla que se va a aplicar.

Para Semeria, C. (s.f.):

> Una vez que se determina qué hacer con esa acción (por ejemplo permitir que un programa se conecte siempre a Internet), con cada cartel de alerta se van configurando las reglas ya que luego ese aviso no va a volver a aparecer. Con el tiempo estos avisos se reducen al mínimo. Por cada acción crean un

registro de la actividad (log) para el posterior análisis del administrador de la red.

Entre los beneficios de los cortafuegosestá en que el acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet y si no existieran, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.

También permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y a la información que le sean estrictamente permitidas (García, M. s.f).

Otra causa que ha hecho que el uso de los cortafuegos se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un “traductor de direcciones” o NAT, el cual puede alojarse en el cortafuego [5].

Para Morales, H. (s.f.):

> También son importantes los cortafuegos para llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Más peligroso aún es que ese intruso deje puertas traseras (back doors), abriendo un puerto diferente y borre las pruebas o indicios del ataque original.

El cortafuego no puede proteger a la red de las amenazas a las que está sometido por ataques internos o usuarios negligentes, ni protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen en Internet [5].

Comentario [f13]: http://www.infospyware.com/articulos/firewall-cortafuegos/

http://www.cosmosvideo.net/prensa/firewall/

http://dspace.espoch.edu.ec/bitstream/123456789/2548/1/18T00524.pdf

http://intercambiosos.org/archive/index.php/t-26383.html

http://infosimple.blogspot.com/2006_11_01_archive.html

http://dra19401.blogspot.com/2011_09_01_archive.html

Comentario [f14]: http://mgarciafelipe.files.wordpress.com/2012/02/ud-4-instalacic3b3n-y-configuracic3b3n-de-cortafuegos-miguelangelgarcia.pdf

Comentario [f15]: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

http://computersecurityagents.blogspot.com/p/firewalls.html

http://seguridadinformaticaconsitio.pbworks.com/w/page/52117817/firewall

http://tremoto.jimdo.com/motivaciones/

Comentario [f16]: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

http://www.slideshare.net/montillaelwuin/firewall-y-vpn

http://www.uv.es/~montanan/redes/trabajos/Firewalls.pdf

http://biblioteca.usac.edu.gt/tesis/08/08_0236_EO.pdf

http://biblioteca.usac.edu.gt/tesis/08/08_0236_EO.pdf

Comentario [f17]: http://www.slideshare.net/lalex20/historia-de-los-cortafuegos

http://rsvlk.blogspot.com/2010_06_01_archive.html

http://jgdasir2.files.wordpress.com/2012/02/ut04-instalacion-y-configuracion-de-cortafuegos.pdf

Para Semeria, C.(s.f.):

> Este no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (diskettes, memorias, etc.) y sustraerlas del edificio. No tienen defensa alguna contra técnicas como la ingeniería social y el ataque de insiders. No pueden proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.

Algunos de las prestaciones que brindan los cortafuegos son:

- Previene que usuarios no autorizados obtengan acceso a la red.
- Provee acceso transparente hacia Internet a los usuarios habilitados.
- Asegura que los datos privados sean transferidos en forma segura por la red pública.
- Ayuda a los administradores a buscar y reparar problemas de seguridad.
- Provee un amplio sistema de alarmas advirtiendo intentos de intromisión a la red.

2.5.2 Tipos de cortafuegos según el nivel OSI y nivel TCP/IP.

Existen muchos tipos de cortafuegos, no obstante la clasificación más clara quizás sería la que los diferencia según la forma de implementar las políticas de seguridad de la organización atendiendo al nivel de la capa OSI en la que se implementan dichas políticas de seguridad.

Ventura L. (s.f.):

> En primer lugar existen los cortafuegos de nivel 3 de la capa OSI, esto es, de nivel de red o lo que es lo mismo nivel IP en redes TCP/IP como Internet. Estos cortafuegos pueden ser considerados como filtros de paquetes ya que lo que realizan a fin de cuentas es un filtrado de los intentos de conexión atendiendo a direcciones IP origen y destino y puerto de destino de los paquetes IP.

Comentario [f18]: http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)

http://www.etapa.net.ec/Telecomunicaciones/bib_telecom_doc/antivirus/Cortafuegos%20o%20Firewall.pdf

http://www.slideshare.net/astrologia/cortafuegos-jprl

http://carloseduca.byethost11.com/PCPI/MANTENIMIENTO/ut2/cortafuegos.html

http://will4864.tripod.com/software/id25.html

http://rsvlk.blogspot.com/

http://prezi.com/u2wziyrl6s0i/untitled-prezi/

http://www.laminfo.com/blog/archivos/__6_unidad_VI_Seguridad_perimetro_Firewalling_Accesos_remotos_VPNs_tuneles.pdf

https://sites.google.com/site/raul12abc/raul123abc

Comentario [f19]: http://redesysegu.blogspot.com/p/tipos-de-proteccion-para-una-red.html

http://clubensayos.com/Tecnolog%C3%ADa/Manual-De-Redes-De-Internet/936149.html

http://prezi.com/8uyekfuuihcj/untitled-prezi/

http://www.buenastareas.com/ensayos/Proteccion-Vs-Amenazas-Al-Software-y/4164288.html

http://infosegura.tripod.com/firewall.html

https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=0CHwQFjAJ&url=http%3A%2F%2Fwww.hacienda.go.cr%2Fcentro%2Fdatos%2FArticulo%2FSeguridad%2520Inform%25C3%25A1tica.%2520Hackers.doc&ei=RL1CUsrHAcWj4AOf6oDADA&usg=AFQjCNHHndkZZ_o_mlTvHGqobjPe0lFI_w&sig2=LXDoKzil8RZawsqCOde7Nw

También se puede especificar desde qué direcciones IP origen se dará acceso a los servidores públicos. Este tipo de cortafuegos vienen implementados en la mayoría de los enrutadores comerciales (Analuisa, R. 2012).

Comentario [f21]: http://dspace.espoch.edu.ec/bitstream/123456789/2548/1/18T00524.pdf

Otra posibilidad de implementación de cortafuegos es a nivel 4 de OSI, esto es a nivel de transporte o TCP en redes TCP/IP. En este nivel ya se puede atender a aspectos de sí los paquetes son de inicio de conexión o se corresponden con paquetes cuyas conexiones están ya establecidas. A grandes rasgos los cortafuegos a nivel de circuitos ya tratan con números de secuencias de paquetes TCP/IP. Si los paquetes pertenecen a una conexión o si no se corresponden con ninguna conexión establecida. Por último los cortafuegos a nivel de aplicación (capa 7 del modelo OSI, capa 4 de la pila de protocolos TCP/IP) actúan a modo de proxy para las distintas aplicaciones que van a controlar. Con estos cortafuegos no será posible dejar pasar todos los protocolos [11].

2.5.2.1 Filtrado de paquetes .

Para Ramos, A. (s.f.):

> Se utilizan filtros y reglas basadas en políticas de control de acceso. Funciona a nivel de red (capa 3 del modelo OSI, capa 2 de la pila de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. También en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI) como el puerto origen y destino.

Para Barrios, J. (2012):

> 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.El filtrado de paquetes mediante puertos y protocolos, permite establecer que servicios están disponibles a los usuarios y por cuáles puertos. Se puede establecer la navegación en la Web (puerto 80 abierto), pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).

Comentario [f22]: http://datateca.unad.edu.co/contenidos/233015/233015Exe/leccin_4_firewalls.html

http://repositorio.espe.edu.ec/bitstream/21000/3494/1/T-ESPEL-0014.pdf

http://seguridadasir.files.wordpress.com/2012/02/tema_4.pdf

http://cdigital.uv.mx/bitstream/123456789/32009/1/cervantesruiz.pdf

http://dspace.espoch.edu.ec/bitstream/123456789/325/1/18T00406.pdf

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.

Para Moyano, C. & Villa, V. (2010):

- No son capaces de esconder la topología de las redes privadas, por lo que exponen las redes al mundo exterior.
- Sus capacidades de auditorías suelen ser limitadas, al igual que el registro de actividades.
- No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

2.5.2.2 Proxy-pasarela de aplicaciones.

Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como servidores proxy y la máquina donde se ejecuta recibe el nombre de pasarela de aplicación.

Para KiosKea. (s.f.):

> El filtrado de aplicaciones permite la destrucción de los encabezados que preceden los mensajes de aplicaciones, lo cual proporciona una mayor seguridad. Este tipo de cortafuegos es muy efectivo y, si se ejecuta correctamente, asegura una buena protección de la red. Por otra parte, el análisis detallado de los datos de la aplicación requiere una gran capacidad de procesamiento, lo que a menudo implica demora en las comunicaciones, ya que cada paquete debe analizarse minuciosamente. Además, el proxy debe interpretar una gran variedad de protocolos y conocer las vulnerabilidades relacionadas para ser efectivo.

Para Tonato, B. & Viracocha, P. (2003):

> 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.

Comentario [f23]: http://cdigital.uv.mx/bitstream/123456789/32009/1/cervantesruiz.pdf

http://dspace.espoch.edu.ec/bitstream/123456789/325/1/18T00406.pdf

Comentario [f24]: http://www.segu-info.com.ar/firewall/proxygateways.htm

http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

http://plataforma.edu.pe/pluginfile.php/145786/mod_resource/content/1/4taSEM-VIE%20-%20Tema%203%20-%20Control%20de%20Acceso.pptx

http://prezi.com/ib-dqocbci6a/untitled-prezi/

http://seguridad-infomatica.blogspot.com/2012/11/proteccion.html

http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/Seguridad_de_Internet-El_Futuro_de_TCP-IP.pdf

http://www.slideshare.net/Niver/firewall-presentacion-niver

http://www.slideshare.net/krmn35/seguridad-en-internet-13322989

Comentario [f25]: http://es.kioskea.net/contents/590-firewall

http://www.slideshare.net/LILILILILILI/firewall-total-2501494?nomobile=true

Comentario [f26]: http://www.segu-info.com.ar/firewall/proxygateways.htm

http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/Seguridad_de_Internet-El_Futuro_de_TCP-IP.pdf

http://repositorio.espe.edu.ec/bitstream/21000/3494/1/T-ESPEL-0014.pdf

http://ticobegogarcia.wordpress.com/category/informatica/

Trabaja en el nivel de aplicación (nivel 7 modelo OSI y capa 4 Pila de protocolos TCP/IP) de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP se pueden realizar filtrados según la URL a la que se está intentando acceder, de manera que si cumple con las políticas establecidas la deja pasar sino la bloquea. Su función es la de analizar el tráfico de la red en busca de contenido que viole la seguridad de la misma (Ver Fig.1.1).

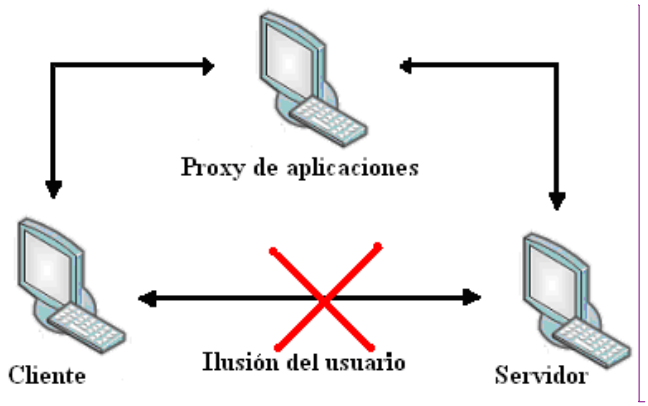


Fig. 2.1: Servidor Proxy. (Creada por el autor).

Comentario [f27]: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CD4QFjAC&url=http%3A%2F%2Frepositorio.utn.edu.ec%2Fbitstream%2F123456789%2F561%2F4%2FC%2520A%2520P%2520I%2520T%2520U%2520L%2520O%2520%2520IV.doc&ei=pT5DUpb-K5Ho8QS5_YDQCw&usg=AFQjCNET3BW3YUi6eeH408k7XwL1BOO1tQ&sig2=lsj-gv98Ol4EcuVL0KdeUw

2.5.2.3 Proxy de aplicaciones con el reenvío de paquetes desactivado.

Estos son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso de filtrado de paquetes), por lo que se dice que actúa con el IP-forwarding desactivado (Callegari, O. s.f.).

Comentario [f28]: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

http://www.rnds.com.ar/articulos/036/RNDS_180W.pdf

http://prezi.com/55jxlwarwiba/untitled-prezi/

Un usuario interior que desee hacer uso de un servidor exterior, deberá conectarse primeramente al cortafuego, donde el proxy entenderá su petición, y en función de la configuración impuesta en dicho cortafuego, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario. Es decir que se utilizarán dos conexiones. Uno desde la máquina interior hasta el cortafuego y el otro desde este hasta la máquina que albergue el servicio exterior (Ver Fig. 1.2).

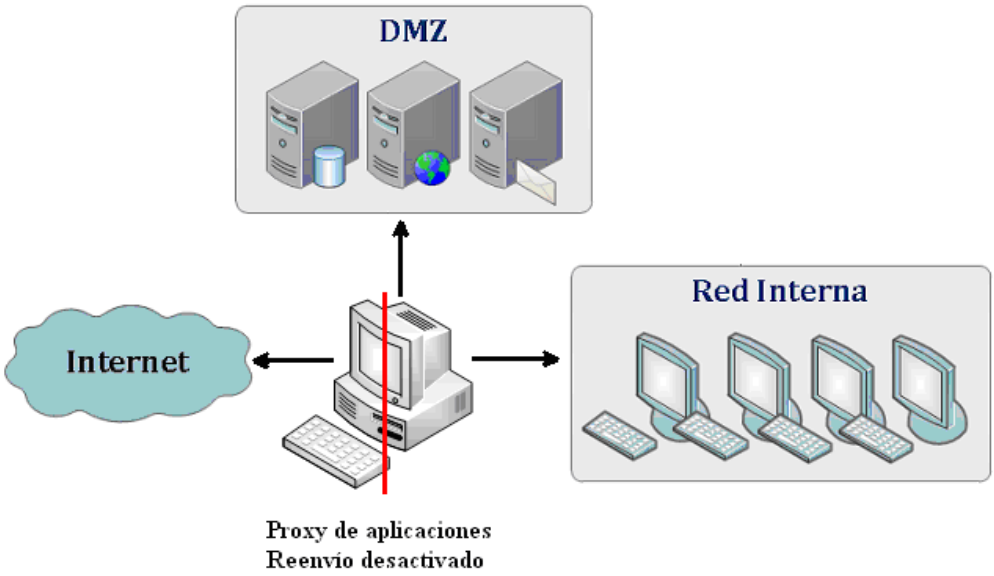


Fig. 2.2. Reenvío de paquetes desactivado. (Creada por el autor)**.**

2.5.2.4 IPtables

Chacón, D. (2009):

> El núcleo de Linux presenta un subsistema de redes muy poderoso llamado Netfilter (filtro de red). Este permite interceptar y manipular paquetes de red, proporciona un filtrado de paquetes con vigilancia continua o sin ella, así como también NAT y servicios de enmascaramiento IP. Netfilter también tiene la habilidad de quitar la información IP de cabecera para un enrutamiento avanzado y gestión del estado de la conexión.

Para Barrios, J.(s.f.):

> El poder y flexibilidad de Netfilter es implementado y controlado a través de la interfaz de IPtables (herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red). Este utiliza el subsistema Netfilter para mejorar la conexión de la red, inspección y procesamiento, presenta funcionalidades como: registro avanzado, acciones previas y posteriores al enrutamiento, traducción de

direcciones de red y reenvío de puertos. Está disponible en prácticamente todas las distribuciones de Linux actuales.

2.5.3 Políticas de diseño de un cortafuegos.

Para Borghello, C. (2005):

> Las políticas de acceso en un cortafuego se deben diseñar poniendo gran atención a sus limitaciones o capacidades, pero también pensando en las amenazas y vulnerabilidades de una red externa insegura. 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.

Cabaleiro, J. (s.f.):

> Sin embargo los cortafuegos pueden definir niveles de seguridad, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros.

Para Barrios, J. (2012):

Generalmente se realizan las siguientes preguntas:

- ¿Qué se debe proteger? Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).
- ¿De quién debe 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.
- ¿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.

2.5.4 Wrappers

Para Cabaleiro, J. (s.f.):

> Un wrapper es un programa que controla el acceso a un segundo programa. El wrapper literalmente cubre la identidad de este segundo programa, obteniendo con esto un más alto nivel de seguridad. Los wrappers son usados dentro de la seguridad en sistemas UNIXs. Estos programas nacieron por la necesidad de modificar el comportamiento del sistema operativo sin tener que modificar su funcionamiento.

Los wrappers son ampliamente utilizados, y han llegado a formar parte de herramientas de seguridad por las siguientes razones:

- Debido a que la seguridad lógica está concentrada en un solo programa, los wrappers son fáciles y simples de validar.
- Debido a que el programa protegido se mantiene como una entidad separada, éste puede ser actualizado sin necesidad de cambiar el wrapper.
- Debido a que los wrappers llaman al programa protegido mediante llamadas estándar al sistema, se puede usar un solo wrapper para controlar el acceso a diversos programas que se necesiten proteger.
- Permite un control de accesos exhaustivo de los servicios de comunicaciones, además de buena capacidad de registros (logs) y auditorias de peticiones a dichos servicios, ya sean autorizados o no.

Para Seguridad de la Información. (s.f.):

> El paquete wrapper más ampliamente utilizado es el TCP-wrappers, el cual es un conjunto de utilidades de distribución libre. Consiste en un programa que

es ejecutado cuando llega una petición a un puerto específico, una vez comprobada la dirección de origen de la petición, la verifica contra las reglas almacenadas, y en función de ellas, decide o no dar paso al servicio. Adicionalmente, registra estas actividades del sistema, su petición y su resolución.

Para Cabaleiro, J. (s.f.):

Algunas configuraciones avanzadas de este paquete, permiten también ejecutar comandos en el propio sistema operativo, en función de la resolución de la petición. Por ejemplo, es posible que interese detectar una posible máquina atacante, en el caso de un intento de conexión, para tener más datos a la hora de una posible investigación. Puede pensarse que los wrappers son cortafuegos ya que muchos de los servicios brindados son los mismos o causan los mismos efectos, usando wrappers se puede controlar el acceso a cada máquina y los servicios accedidos.

1.5.5 Sistemas de detección de intrusos (IDS).

Borghello, C. (2005):

Un sistema de detección de intrusos (IDS Intrusion Detection System) es un programa usado para detectar accesos no autorizados a una computadora o a una red. Estos accesos pueden ser ataques de habilidosos hackers que usan herramientas automáticas.

Ardita, J. (2008):

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**.**

Chacón D. (2009):

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.

Para Villalón, A. (2006):

Normalmente esta herramienta se integra con un cortafuego. 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 cortafuego, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del cortafuego, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

Chacón D. (2009):

Los IDS suelen disponer de una base de datos de firmas de ataques conocidos.Estas permiten al IDS distinguir entre el uso normal de la máquina 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 (Ver Fig. 1.3)**.**

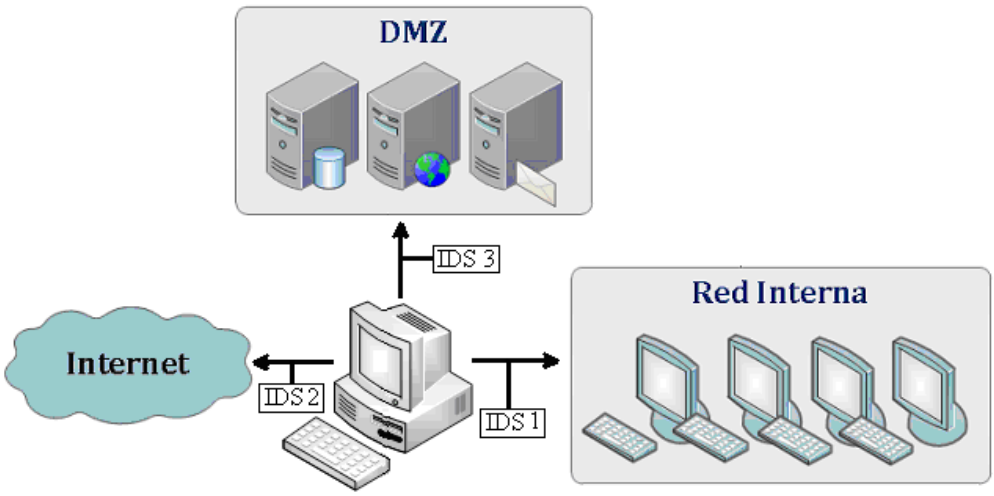


Fig. 2.3 Ubicación de los IDS en la red. (Creada por el autor)

Para Chacón, D. (2009) Existen tres tipos de sistemas de detección de intrusos:

1- HIDS (Host IDS): el principio de funcionamiento de un HIDS, depende del éxito de los intrusos, que generalmente dejaran 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.

2- NIDS **(**Network IDS): 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.

3- DIDS (Distributed IDS): 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).

Comentario [f29]: http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&ved=0CD4QFjAC&url=http%3A%2F%2Fuagrm-components-design.googlecode.com%2Fsvn%2Ftrunk%2Fmodule10%2FVoIp%2FVoIp%2520-%2520proyecto%2520de%2520seguridad%2520snort%2520en%2520fedora%252017.docx&ei=4EBDUqiHKI709gTeroGgCg&usg=AFQjCNEwm_XqBTJToRS8wLnN6i9wKU5CbA&sig2=ttg8IwJBmhLX99ijUfBnfw

http://es.scribd.com/doc/56255979/Sistema-de-deteccion-de-intruso1

http://elsitiodejosejisaid.files.wordpress.com/2011/09/ud-3-implantacic3b3n-de-tc3a9cnicas-de-acceso-remoto-seguridad-perimetral.pdf

Comentario [f30]: http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos

Comentario [f31]: http://bibing.us.es/proyectos/abreproy/11499/fichero/05+-+Seguridad+en+la+red+en+GNU-Linux.pdf

http://es.scribd.com/doc/44258805/In-for-Me

2.5.6 IDS en tiempo real.

Es muy conveniente añadir elementos que controlen el tráfico detrás de los cortafuegos (dentro de la red local), uno de estos elementos son los IDS en tiempo real los cuales deben de:

- Inspeccionar el tráfico de la red buscando posibles ataques.
- Controlar el riesgo de los servidores para detectar acciones sospechosas.
- Mantener una base de datos con los estados exactos de cada uno de los archivos del sistema para detectar la modificación de los mismos.
- Controlar el núcleo del sistema operativo para detectar posibles infiltraciones en el.
- Avisar al administrador de todo tipo de acciones malignas o amenazas.

Para Chacón D. (2009):

> 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.

2.5.7 Sistemas de prevención de intrusos.

Para Borghello, C. (2005):

> 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.
>
> 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 pro-activamente y un IDS lo protege re-activamente.

2.5.8 Sistemas anti–sniffers

Para Seguridad de la Información. (s.f.):

> Esta técnica consiste en detectar sniffers en el sistema. Generalmente estos programas se basan en verificar el estado de la placa de red, para detectar el modo en el cual está actuando (los sniffer la colocan en modo promiscuo para capturar todo el tráfico que pasa por la red).

Comentario [f32]: http://es.wikipedia.org/wiki/Sistema_de_prevenci%C3%B3n_de_intrusos

http://kalilinux.foroactivo.com/t54-tutorial-ua-tester-para-kali-linux

Comentario [f33]: http://ditech.com.co/soluciones-integrales/seguridad-informatica-en-redes/revencion-de-intrusos-ips/

http://admonredescesarlopera4453.wikispaces.com/Glosario+videos

http://bashingnet.wordpress.com/2012/10/19/patriot-ngidsipsesen/

Comentario [f34]: http://es.wikipedia.org/wiki/Sistema_de_prevenci%C3%B3n_de_intrusos

http://kalilinux.foroactivo.com/t54-tutorial-ua-tester-para-kali-linux

http://books.google.com.ec/books?id=xb3mzBE-yIoC&pg=PA145&lpg=PA145&dq=Los+IPS+presentan+una+mejora+importante+sobre+las+tecnolog%C3%ADas+de+cortafuegos+tradicionales,+al+tomar+decisiones+de+control+de+acceso+basados+en+los+contenidos+del+tr%C3%A1fico,+en+lugar+de+direcciones+IP+o+puertos.+Tambi%C3%A9n+es+importante+destacar+que+los+IPS+pueden+actuar+al+nivel+de+equipo,+para+combatir+actividades+potencialmente+maliciosas+%5B1%5D.&source=bl&ots=I7CK-gND3C&sig=-8_FHFA01vFaZe1ghRDbIsRO8vk&hl=en&sa=X&ei=a0ZDUpnVOI-C9QTn-IDABA&redir_esc=y#v=onepage&q&f=false

http://evidenciasdelsena.over-blog.net/article-cortafuegos-informatica-59355393.html

http://redes1-nelly.blogspot.com/

Comentario [f35]: http://es.wikipedia.org/wiki/Sistema_de_prevenci%C3%B3n_de_intrusos

http://www.trendcorp.com.pe/intrusos.html

http://www.buenastareas.com/ensayos/Foro-3-Redes-y-Seguridad/31547092.html

http://www.grupotemel.net/lineas-de-negocio/soluciones/seguridad-corporativa-y-proteccion-de-datos/ips-ids/

http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/6747/1/SISTPREVENTOR.pdf

http://prezi.com/agmms-t5qqaz/idsips/

2.6 Niveles de seguridad informática.

El estándar de niveles de seguridad más utilizado internacionalmente es el TCSEC Orange Book (2), desarrollado de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.
Los niveles describen diferentes tipos de seguridad del sistema operativo y se enumeran desde el mínimo grado de seguridad al máximo. Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).

Cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.

Seguridad Lógica (s.f.):

- Nivel D: Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS y System 7.0 de Macintosh.
- Nivel C1 protección discrecional: Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

  Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "súper usuario" quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización se encuentren dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se muestran los requerimientos mínimos que debe cumplir la clase C1:

- Acceso de control discrecional: distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.
- Identificación y Autentificación: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

- Nivel C2 protección de acceso controlado: Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización. Requiere que se audite el sistema. Esta auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoria requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos. Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.
- Nivel B1 seguridad etiquetada: Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultra-secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.). Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos

asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

- Nivel B2 protección estructurada: Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La protección estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios. El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.
- Nivel B3 dominios de seguridad: Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad.Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y test ante posibles violaciones. Este nivel requiere que la Terminal del usuario se conecte al sistema por medio de una conexión segura. Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.
- Nivel A protección verificada: Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema. Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

2.7 Seguridad en sistemas de código abierto.

Hay que tomar el máximo de consideraciones para lograr tener un sistema lo más protegido posible. Algunas de estas consideraciones de la arquitectura de seguridad de Linux son:

- Control de acceso a la red.
- Conexión.
- Detección de intrusos.

2.7.1 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 máquinas conectarse entre sí. Para esto es posible implantar reglas de acceso a la red muy refinadas (Howto, 2006).

Para Villalón, A. (2006):

> 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 las computadoras no autorizadas. En Linux muchos servicios de red ofrecen esta función. Anexo 1.

2.7.2 Conexión.

Para Villalón, A. (2006):

> 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 una computadora, pero puede registrar el movimiento de la persona que realizó dicho ataque.

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. (Barrios, J. 2012)

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

Para Escartín, J. (2005):

> 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. Puede registrar todos y cada uno de los comandos que ha emitido un usuario determinado.

Para Barrios, J. (2012):

> 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.

2.8 Hacking ético.

Hacking ético no es más que descubrir las deficiencias relacionadas con la seguridad y vulnerabilidades de los sistemas informáticos, analizarlas y calibrar su grado de riesgo y peligrosidad, además de recomendar las soluciones más apropiadas para cada una de ellas.

2.8.1 Diferentes tipos de hacking ético.

Borghello, C. (2005):

> 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.

Comentario [f36]: http://www.palentino.es/blog/que-es-el-hacking-etico/

http://letysystem.wordpress.com/2011/01/29/ethical-hackers/

http://sycg.wordpress.com/category/compiladores/

Hackingético externo caja negra**:** Se realiza idénticamente al anterior, con la diferencia de que no se da información para la realización de la intrusión (Ardita, J. 2008).

Para Ardita, J. (2008):

> Hackingético 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.

Comentario [f37]: http://taliahaker.blogspot.com/

Para Escartín, J. (2005):

> Hackingético 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.

Comentario [f38]: http://www.palentino.es/blog/que-es-el-hacking-etico/

2.9 Generalidades de las DMZ.

Para Sanjuan, L. (s.f.):

> Cuando algunas máquinas de la red interna deben ser accesibles desde una red externa es necesario crear una nueva interfaz hacia una red separada a la que se pueda acceder tanto desde la red interna como por la red externa sin correr el riesgo de comprometer la seguridad de la red interna.

Comentario [f39]: http://manglar.uninorte.edu.co/bitstream/10584/2203/2/Panorama%20general%20de%20la%20seguridad%20inform%C3%A1tica.pdf

http://drexlerr2corporation.files.wordpress.com/2012/01/teoria-ud3.pdf

> El término "zona desmilitarizada" o DMZ hace referencia a esta zona aislada que posee aplicaciones disponibles para el público. La DMZ es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet, la cual actúa como una "zona de búfer" entre la red que necesita protección y la red hostil.

Comentario [f40]: http://dra19401.blogspot.com/2011_09_01_archive.html

http://dra19401.blogspot.com/

Primo, A. (2012):

> Una DMZ se crea a menudo a través de las opciones de configuración del cortafuego, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall). Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando traducción de direcciones depuertos(PAT).
>
> Esta red contiene servidores que proporcionan dos grupos básicos de servicios: El primero es el servicio Web de aplicaciones para el usuario, formado por servidores en los que se ejecuta Internet Information Server (IIS). Este grupo ofrece los servicios Web fundamentales y se comunica con los clientes de Internet a través de los protocolos de transporte estándar de Internet, como HTTP o HTTPS. Estos servidores se reúnen en clústeres con el servicio equilibrio de la carga en la red.

Para Velásquez, F. (2011):

El segundo grupo de servidores proporciona servicios de red como el sistema de nombres de dominio (DNS, Domain Naming System). Todos los servidores de la red DMZ también pueden comunicarse con recursos internos, como los servidores de bases de datos y otros componentes adicionales que formen parte de la red interna.

Para Semeria, C. (s.f.):

> El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, los equipos en la DMZ no pueden conectarse con la red interna. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. Para ello se emplean dos enrutadores (routers), uno exterior, el cual tiene como objetivo bloquear el tráfico no deseado de ambos sentidos y otro interior, este realiza la misma función en la red interna y la DMZ (zona entre el enrutador externo y el interno). Para cualquiera de la red

Comentario [f41]: http://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica)

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDUQFjAB&url=http%3A%2F%2Fvicentesanchez90.files.wordpress.com%2F2013%2F01%2Fpoliticas-de-defensa-en-profundidad.pptx&ei=oklDUqXhN4XO8wTP7IDwCg&usg=AFQjCNF5SvTUHRxlIIv6IxPcJqB8w2d5DQ&sig2=Fr_dM1MGE0sl_lDsAKIk5w

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&ved=0CD4QFjAC&url=http%3A%2F%2Fseguridadasir.files.wordpress.com%2F2012%2F01%2Ftema_3.docx&ei=oklDUqXhN4XO8wTP7IDwCg&usg=AFQjCNG2fYzvzp_Tj1dLt-PyHyXIlD1zXA&sig2=nB_l5rxYd4juZlGUH4Qsew

http://esperanza7989.files.wordpress.com/2012/01/tema3_seguridad.pdf

http://lalesespecial.files.wordpress.com/2011/09/tema-3-sad-implantacic3b3n-de-tc3a9cnicas-de-acceso-remoto-seguridad-perimetral.pdf

http://alvaroprimoguijarro.files.wordpress.com/2012/01/ud03_sad_alvaroprimoguijarro.pdf

Comentario [f42]: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCsQFjAA&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2Fb%2F9%2Fc%2Fb9c5fcd7-db63-4858-9871-a9bd515bb5ea%2FRAG01.doc&ei=IEpDUs7aPIqC9QTwh4GQCw&usg=AFQjCNF6cb1HK2qmCq0JHmpnqi0gX-SEnA&sig2=jAFxvVcs92yZ4n0mhwxdjQ

externa que quiera conectarse sin autorización a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

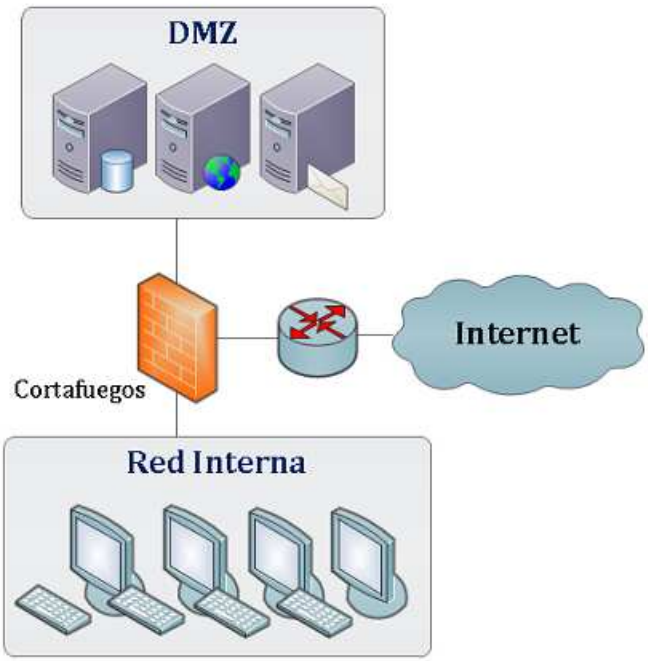


Fig.2.4. Diagrama de una red típica que usa una DMZ con un cortafuego en trípode. (Tomada de [17])

Los servidores en la DMZ se denominan "anfitriones bastión" ya que actúan como un puesto de avanzada en la red de la compañía.

Por lo general, la política de seguridad para la DMZ es la siguiente:

- El tráfico de la red externa a la DMZ está autorizado.
- El tráfico de la red externa a la red interna está prohibido.
- El tráfico de la red interna a la DMZ está autorizado.
- El tráfico de la red interna a la red externa está autorizado.
- El tráfico de la DMZ a la red interna está prohibido.
- El tráfico de la DMZ a la red externa está denegado.

De esta manera, la DMZ posee un nivel de seguridad intermedio, el cual no es lo suficientemente alto para almacenar datos imprescindibles. Es posible instalar las

DMZ en forma interna para aislar la red interna con niveles de protección variados y así evitar intrusiones internas.

2.10 Características de una zona desmilitarizada.

Las zonas desmilitarizadas tienen varias características importantes, entre las que se encuentran: Filtrado de paquetes a cualquier zona, NAT, mapeo bidireccional, colas de tráfico y prioridad, salidas redundantes / balanceo de carga, filtrado de contenido (Web-cache), monitoreo de tráfico en interfases vía netflow.

2.10.1 Filtrado de paquetes a cualquier zona.

Para Semeria, C. (s.f.):

> La acción de filtrar paquetes es bloquear o permitir el paso a los paquetes de datos de forma selectiva, según van llegando a una interfaz de red. Los criterios que usa filtrado de paquetes para inspeccionar los mismos los toma de la información existente en la capa 3 (IPv4 e IPv6) y en la capa 4 (TCP, UDP, ICMP, e ICMPv6) de las cabeceras de los paquetes. Los criterios que más se utilizan son los de la dirección de origen y de destino, el puerto de origen y de destino, y el protocolo. Las reglas de filtrado especifican los criterios con los que debe concordar un paquete y la acción a seguir, bien sea bloquearlo o permitir que pase, que se toma cuando se encuentra una concordancia. Las reglas de filtrado se evalúan por orden de secuencia, de la primera a la última. A menos que el paquete concuerde con una regla que contenga la clave quick, se evaluará el paquete comparándolo con todas las reglas de filtrado antes de decidir una acción final. La última regla que concuerde será la que dictamine qué acción se tomará con el paquete. Al principio del grupo de reglas de filtrado hay un pasa todo implícito que indica que si algún paquete no concuerda con ninguna de las reglas de filtrado, la acción a seguir será permitirle el paso.

2.10.2 NAT, mapeo bidireccional.

La traducción de direcciones de red (NAT Network Address Translation), se utiliza para asignar una red completa (o varias redes) a una sola dirección IP. El NAT es necesario cuando la cantidad de direcciones IP que haya asignado el proveedor de

Internet a la red sea inferior a la cantidad de ordenadores que se quieran que accedan a Internet. Este permite aprovechar los bloques de direcciones reservadas que se describen en el RFC 1918. Generalmente, una red interna se suele configurar para que use uno o más de estos bloques de red.

Los bloques son:

10.0.0.0/8 (10.0.0.0 - 10.255.255.255)

172.16.0.0/12 (172.16.0.0 - 172.31.255.255)

192.168.0.0/16 (192.168.0.0 - 192.168.255.255)

Cuando los paquetes pasan a través de la pasarela de NAT, son modificados para que parezca que se han originado y provienen de la misma pasarela de NAT. La pasarela de NAT registra los cambios que realiza en su tabla de estado, para así poder:

- Invertir los cambios en los paquetes devueltos.
- Asegurarse de que los paquetes devueltos pasen a través del cortafuego y no sean bloqueados.

Para Semeria, C. (s.f.):

> Se puede establecer una asignación de tipo bidireccional usando la regla binat. La cual establece una asignación de uno por uno entre la dirección IP interna y la dirección IP externa. Esto puede ser útil, por ejemplo, para colocar un servidor Web en la red interna con su propia dirección IP externa. Las conexiones desde Internet hacia la dirección externa se traducirán a la dirección interna, y las conexiones desde el servidor Web como los requerimientos de DNS se traducirán a la dirección externa.

2.10.3 Colas de tráfico y prioridad.

Semeria, C. (s.f.):

> Poner algo en cola es almacenarlo en orden, a la espera de ser procesado. En una red de computadoras, cuando se envían paquetes desde un servidor entran en un sistema de colas en el que permanecen hasta ser procesados por el sistema operativo. Entonces el sistema operativo decide qué cola debe

Comentario [f43]: http://www.cudi.edu.mx/primavera_2006/presentaciones/wireless02_mario_farias.pdf

http://es.scribd.com/doc/95620139/Zonas-Militarizadas-y-Desmilitarizadas

procesar y qué paquete o paquetes de dicha cola. El orden en el que el sistema operativo selecciona los paquetes que va a procesar puede afectar al rendimiento de la red, por ejemplo un usuario que estuviera ejecutando dos aplicaciones de red: SSH y FTP. Lo ideal sería procesar los paquetes de SSH antes que los de FTP, por la propia naturaleza de SSH; cuando se pulsa una tecla en el cliente SSH se espera obtener una respuesta inmediata, mientras que un retraso de unos pocos segundos en una transferencia por FTP pasa casi inadvertido. Pero, ¿qué ocurriría si el enrutador que maneja estas conexiones procesara una gran parte de paquetes de la conexión de FTP antes de procesar la conexión de SSH? Los paquetes de la conexión de SSH se quedarían en la cola (o incluso serían rechazados por el enrutador si la cola no fuera lo suficientemente grande como para mantener todos los paquetes) y podría parecer que hay retrasos en la sesión de SSH, o que va muy lenta. Al modificar la estrategia de la cola en uso, las diversas aplicaciones, usuarios y ordenadores pueden compartir bastante bien el ancho de banda de la red.

El programador (scheduler) es el que decide qué colas hay que procesar y en qué orden deben ser procesadas. Por definición, OpenBSD usa un programador tipo FIFO (el primero en entrar es el primero en salir). Una cola FIFO, como su nombre lo indica lo primero que entra en la cola es lo primero que se procesa. Según van llegando nuevos paquetes, éstos se van añadiendo al final de la cola. Si la cola se llena, los nuevos paquetes que vayan llegando van siendo bloqueados. Esto se conoce como “tail-drop”.

Comentario [f44]: http://www.openbsd.org/faq/pf/es/queueing.html

http://www.linguee.es/aleman-espanol/traduccion/unverz%FCgliche+antwort.html

Comentario [f45]: http://www.openbsd.org/faq/pf/es/queueing.html

http://www.cudi.edu.mx/primavera_2006/presentaciones/wireless02_mario_farias.pdf

http://es.scribd.com/doc/51853861/DMZ-1

http://es.scribd.com/doc/95620139/Zonas-Militarizadas-y-Desmilitarizadas

Comentario [f46]: http://www.cudi.edu.mx/primavera_2006/presentaciones/wireless02_mario_farias.pdf

Comentario [f47]: http://openbsd.groupbsd.org/faq/pf/es/queueing.html

2.10.4 Salidas redundantes / balanceo de carga.

Para Zárate, J. (2006):

Una reserva de direcciones es un grupo de dos o más direcciones cuyo uso comparten un grupo de usuarios. Una reserva de direcciones puede aparecer como la dirección de redirección en las reglas rdr, como la dirección de traducción en las reglas NAT y como la dirección de destino en las opciones route-to, reply-to, y dup-to de las reglas de filtrado de paquetes.

2.10.5 Filtrado de contenido (Web-cache).

Semeria, C. (s.f.):

> Web-cache consiste en que cuando varios clientes solicitan el mismo objeto, este puede proporcionárseles desde el caché de disco. De este modo, los clientes obtiene los datos mucho más rápidamente que si lo hicieran desde Internet y se reduce al mismo tiempo el volumen de transferencias en red. Además del caching, Squid ofrece múltiples prestaciones tales como la definición de jerarquías de servidores proxy para distribuir la carga del sistema, establecer estrictas reglas de control de acceso para los clientes que quieran acceder al proxy, permitir o denegar el acceso a determinadas páginas Web con ayuda de aplicaciones adicionales o producir estadísticas sobre las páginas Web más visitadas y por tanto sobre los hábitos de navegación del usuario.

Comentario [f48]: http://es.scribd.com/doc/51853861/DMZ-1

http://es.scribd.com/doc/95620139/Zonas-Militarizadas-y-Desmilitarizadas

Comentario [f49]: http://www.cudi.edu.mx/primavera_2006/presentaciones/wireless02_mario_farias.pdf

http://es.scribd.com/doc/51853861/DMZ-1

http://es.scribd.com/doc/95620139/Zonas-Militarizadas-y-Desmilitarizadas

2.10.6 Monitoreo de tráfico en interfases vía netflow.

Inicialmente fue diseñado para las rutas en los conmutadores. Netflow es ahora la tecnología más utilizada para llevar la contabilidad de red. Contesta las preguntas del tráfico:

¿Quién?, ¿Qué?, ¿Cómo?, ¿Cuando?, y ¿Donde?

Define llaves únicas como son:

Dirección IP origen, dirección IP destino, puerto origen, puerto destino, tipo de protocolo, interfases lógicas.

Para Primo, A. (2012):

> Problemas que se pueden generar: Esta topología de cortafuegos elimina los puntos únicos de fallo presentes en las anteriores, antes de llegar al bastión (por definición, el sistema más vulnerable) un atacante ha de saltarse las medidas de seguridad impuestas por el enrutador externo.

Comentario [f50]: https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC0QFjAA&url=http%3A%2F%2Fvicentesanchez90.files.wordpress.com%2F2013%2F03%2Fcortafuegos.pptx&ei=VE5DUs-JPJL89gTY-IHYAQ&usg=AFQjCNG2y2hKMzpTuWGoED2w-4HnDegn9g&sig2=BUHtkJyqoahDExMG5xdRdA&bvm=bv.53077864,d.eWU

http://alvaroprimoguijarro.files.wordpress.com/2012/01/ud03_sad_alvaroprimoguijarro.pdf

http://alvaroprimoguijarro.files.wordpress.com/2012/01/ud03_sad_alvaroprimoguijarro.pdf

Si lo consigue, como se ha aislado la máquina bastión en una subred se está reduciendo el impacto de un atacante que logre controlarlo, ya que antes de llegar a la red interna ha de comprometer también la seguridad del segundo enrutador.

Morales, V. (2012):

> Por supuesto, en cualquiera de los tres casos (compromiso del enrutador externo, del host bastión, o del enrutador interno) las actividades de un pirata pueden violar nuestra seguridad, pero de forma parcial: por ejemplo, simplemente accediendo al primer enrutador puede aislar toda la organización del exterior, creando una negación de servicio importante, pero esto suele ser menos grave que si lograra acceso a la red protegida.

Para Semeria, C. (s.f.):

> La topología DMZ es la que mayores niveles de seguridad puede proporcionar. Evidentemente existen problemas relacionados con este modelo: por ejemplo, se puede utilizar el cortafuego para que los servicios fiables pasen directamente sin acceder al host bastión, lo que puede dar lugar a un incumplimiento de la política de la organización. Un segundo problema, quizás más grave, es que la mayor parte de la seguridad reside en los enrutadores utilizados; las reglas de filtrado sobre estos elementos pueden ser complicados de configurar y comprobar, lo que puede dar lugar a errores que abran importantes brechas de seguridad en nuestro sistema.

Soluciones que se pueden proponer: En la actualidad hay empresas que proporcionan una solución y una topología innovadoras como es: DdMZ (Distributed dedicated Militarized Zones). Esta asocia dos conjuntos de soluciones para asegurar una protección de red reforzada:

- Una protección completa de los servidores y de las redes, mediante un software innovador para proteger cada servidor individualmente, además de los tradicionales cortafuegos.

- Un motor de administración de procesos de negocio, que permiten utilizar los cortafuegos y los servidores para dividir la red interna de la compañía en diferentes zonas de seguridad: marketing, financiero, etc.

2.11DMZ host.

En una topología de seguridad con DMZ, se denomina DMZ host al ordenador que situado en la DMZ está expuesto a los riesgos de acceso desde Internet. Es por ello un ordenador de sacrificio, pues en caso de ataque está más expuesto a riesgos. Normalmente el DMZ host está separado de Internet a través de un enrutador o un cortafuegos. Es aconsejable que en el cortafuegos se abran al exterior únicamente los puertos de los servicios que se pretende ofrecer con el DMZ host. En una topología de seguridad más simple el enrutador estaría conectado, por un lado a la red externa (usualmente Internet), por otra parte a la red interna, y en una tercera conexión estaría la DMZ, donde se sitúa el DMZ host [20].

2.11.1 Entorno doméstico.

Para Semeria, C. (s.f.):

> En el caso de un enrutador de uso doméstico, el DMZ host se refiere a la dirección IP que tiene una computadora para la que un enrutador deje todos los puertos abiertos, excepto aquellos que estén explícitamente definidos en la sección NAT del enrutador. Es configurable en varios enrutadores y se puede habilitar y deshabilitar. Con ello se persigue conseguir superar limitaciones para conectarse con programas, aunque es un riesgo muy grande de seguridad que conviene tener solucionado instalando un cortafuego por software en el ordenador que tiene dicha IP en modo DMZ. Para evitar riesgos es mejor no habilitar esta opción y usar las tablas NAT del enrutador y abrir únicamente los puertos que son necesarios.

Los sistemas con zonas desmilitarizadas pueden ser complicados de configurar y comprobar, lo que puede dar lugar a importantes agujeros de seguridad en toda la red. En cambio sí se encuentran bien configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas en las que se encuentran, el ocultamiento de la información, registros de actividades y reglas de filtrado menos robustas.

CAPÍTULO No 3.

VIRTUALIZACIÓN DE UNA TOPOLOGÍA DE RED LAN CON UNA ZONA DESMILITARIZADA.

Para Colás, A. (s.f.):

> Una máquina virtual es un sistema operativo que funciona de forma simulada, es decir, son simulaciones de otros ordenadores pero en modo software, es decir, el programa simula que tiene conexiones de red, CD, puertos, discos duros, etc., pero todo de forma simulada. En estas máquinas se pueden instalar cualquier sistema operativo, incluso diferentes al sistema operativo real, por ejemplo, suponiendo que se tiene instalado Windows XP, dentro de ese XP se puede tener un Linux, un Windows 2003 Server, un Windows Vista, etc.

Para Som, G. (2007):

> Cuando se instala un sistema operativo en una máquina virtual es como si se instalara el sistema operativo desde cero, incluso se puede formatear un disco, crear particiones, etc., todo igual que si fuera un ordenador normal. Con las máquinas virtuales no es necesario tener más discos duros ni más CD o DVD, ya que todo es simulado, se pueden crear discos duros virtuales que en realidad son también simulados, ya que en realidad son ficheros que el programa crea, donde instala todo lo que se quiera instalar. Además de los discos simulados (o virtuales), también se puede usar interfases y dispositivos que ya tiene el equipo, por ejemplo, un CD o un DVD, la impresora, otro disco duro "real", tarjeta de red etc. Pero también se puede "simular" cosas que no tiene, por ejemplo una disquetera.

Para Colás, A. (s.f.):

> La ventaja de usar los CD o DVD simulados es que se puede trabajar con "imágenes" como si fueran discos compactos reales. Esas imágenes son las que los propios programas de grabación crean, y que suelen tener extensiones como .iso o .img. Cuando se indica la memoria a usar, siempre se debe disponer de esa memoria, además por supuesto de la que el

programa "simulador" requiera, por regla general el programa "virtualizador" indica la capacidad de memoria mínima (recomendable) que hay que asignarle.

3.1 Ventajas de trabajar con máquinas virtuales.

Colás, A. (s.f.):

> Con las máquinas virtuales se puede tener varios sistemas operativos sin necesidad de crear particiones o tener más discos duros, esto permitirá poder tener sistemas operativos para pruebas. Por ejemplo, sale una versión beta y no se quiere instalar en el sistema operativo de la máquina física debido a que las betas son pruebas y pueden dejar el sistema operativo inestable. De esta forma siempre se puede probar esos programas beta sin que afecte a las cosas que están instaladas, ni que obligue a formatear y volver a instalar de nuevo todo lo que tiene el equipo físico.

Para Som, G. (2007):

> Las ventajas de trabajar con las máquinas virtuales, es que se puede estar trabajando con varias betas y máquinas virtuales a la vez, aunque no tiene por qué ser al mismo tiempo, ya que cuando se trabaja con máquinas virtuales se necesita tener recursos en el equipo para que le den vida a estas. Por ejemplo, si el equipo tiene un giga de memoria RAM, la máquina virtual no puede simular que tiene más, porque una de las cosas que no se simulan es la memoria, ya que la memoria que se usa en la máquina virtual es la memoria física, es decir, memoria real. La ventaja de los discos duros virtuales frente a la memoria es que se puede indicar la capacidad que usara el disco duro, por ejemplo, 20 Gigas, pero ese espacio no se usa completo, sino que las máquinas virtuales permiten que ese espacio vaya creciendo con forme haga falta, hasta el tamaño máximo que se halla indicado.

Colás, A. (s.f.):

> Otra cosa que se necesita es que el procesador sea rápido, ya que la máquina virtual trabajará dentro del sistema operativo de la máquina física y ese sistema operativo también tendrá que seguir trabajando, además de que

el programa tiene que simular por software todo lo que un sistema operativo necesita. El procesador entre más rápido sea es mejor, se necesita tener bastante espacio libre en el disco, sobre todo si se va a trabajar con varias máquinas virtuales y los discos usados van a necesitar bastante espacio (en algunos casos de 5 a 8 gigas para cada máquina virtual, todo dependiendo de lo que se instale). También se necesita de una suficiente memoria RAM, siempre será mejor 1 GB que 512 MB o 2 GB que 1 GB, todo dependerá de cuanta memoria se quiera que tengan esas máquinas virtuales, pero en la mayoría de los casos, con 256 ó 384 MB trabajan bien, por tanto se necesitará como mínimo 1 GB para trabajar más o menos cómodo.

3.2 Software empleado en la virtualización. VMware Workstation 7.0.0.20.3739.

Entre el software que se emplean para la creación de topologías de redes virtuales se encuentran: VMware Server, VMware Player y VMware ESX Server, VirtualBox, VMware Workstation.

Howto, (2006):

VMware Workstation 7.0.0.20.3739 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 una máquina física (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.

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 seguridad y disponibilidad de servicios en los sistemas. Es una herramienta robusta y de fácil utilidad.

Para Colás, A. (s.f.):

> Esta herramienta es de gran ayuda gracias a su capacidad de virtualización de parámetros vistos en las máquinas físicas. Mediante su interfaz gráfica se hace muy factible su utilización e interpretación para la instalación de las máquinas virtuales, además de presentar elementos gráficos de muy fácil manejo como:play, stop, pause y reset. Con el Virtual Network Editor, que es una interfaz para la configuración de la red virtual, se pueden realizar conexiones de red mediante las interfases que presenta. Además muestra especificidades en su conexión y función que estas pueden realizar.
>
> La conexión puede ser de forma automática (mediante asignación dinámica de direcciones IP por 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 interfases y de esta forma lograr configuraciones de red a conveniencia. En el caso particular de cada una de las máquinas virtuales, se escoge la interfaz por donde va a trabajar 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 del entorno de red y la propia instalación de la máquina virtual, ayuda a establecer todas las funciones de las máquinas físicas y permite maniobrar los elementos indispensables de las mismas, como la RAM, disco duro, el control de USB, etc.

3.3 Instalación de CentOS.

Para Colás, A. (s.f.):

> 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. La versión CentOS 5.7 de Linux es el

sistema operativo escogido. En base a esta versión se implementa el sistema de seguridad montado sobre VMware.

3.3.1 Creación de las máquinas virtuales.

El VMware permite la instalación y puesta en marcha de múltiples máquinas 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 una nueva máquina virtual (Ver Fig. 2.1).

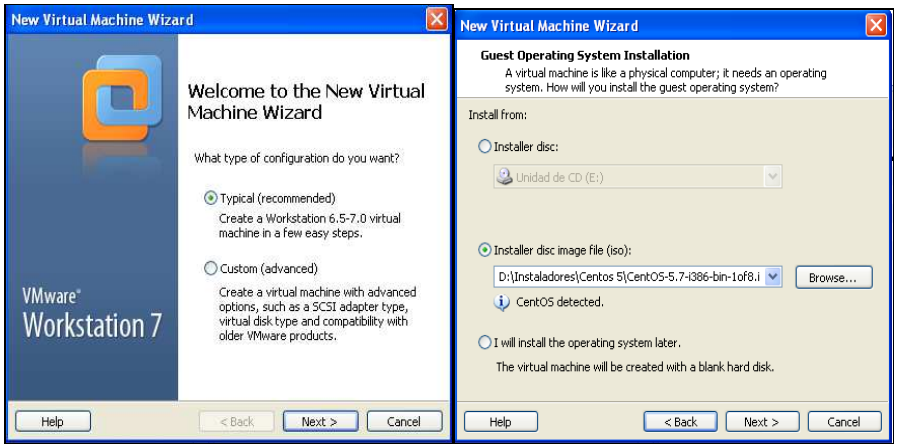


Fig. 3.1 Creación de una nueva máquina virtual. (Creada por el autor.)

De esta manera se extraen los discos .isodel directorio donde estén almacenados y se sigue con la creación de la máquina virtual. Se establece donde 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.

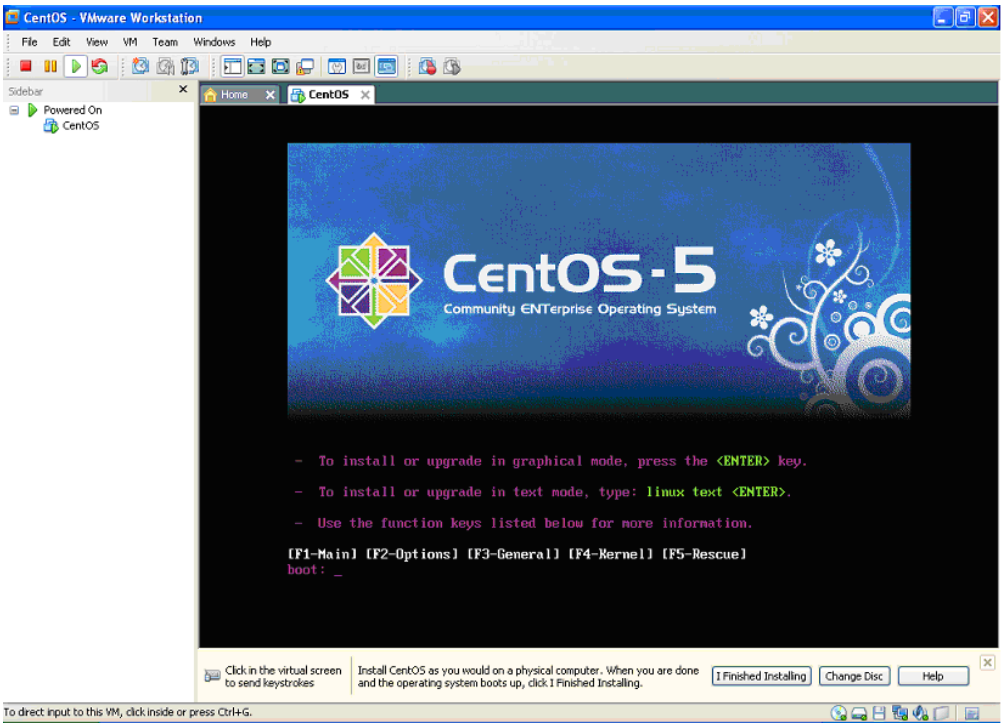


Fig. 3.2. Instalación de CentOS 5 en el entorno del VMware. (Creada por el autor).

Ya creado el nuevo VMware, se pasa a la instalación del sistema operativo 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 (América-Habana), y luego la contraseña y la confirmación de la misma, con la cual se va a entrar al sistema. Luego de todos estos procedimientos pues comienza la instalación de CentOS 5.7 cuyos discos son, CentOS-5.7-i386-bin-1of2.iso y el CentOS-5.7-i386-bin-2of2.iso.

Con la obtención de los discos de CentOS 5.7, se instalan todos los paquetes necesarios para el funcionamiento del sistema operativo y la posterior puesta en marcha de la topología de red.

3.4 Topología de la 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 topología ya que con tan solo varios elementos se obtienen los resultados deseados. Dicho diseño está constituido por un proveedor de servicios de Internet (ISP), un cortafuego (IPtables) con políticas establecidas para prestar la mayor seguridad posible sin afectar la disponibilidad de la red. Existe una red LAN local a la cual se le va a prestar servicios, y por último una zona desmilitarizada (DMZ) la cual esta constituida por un servidor Web, que son las máquinas más atacadas de la red.

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 o red externa. 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, 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 interfases físicas. Otras de las particularidades que tiene esta red es la creación de dos interfases virtuales dentro de la implementación del cortafuego virtual, cuyas interfases son las conectadas a las redes de la DMZ y la red local (Ver Fig. 2.3.)

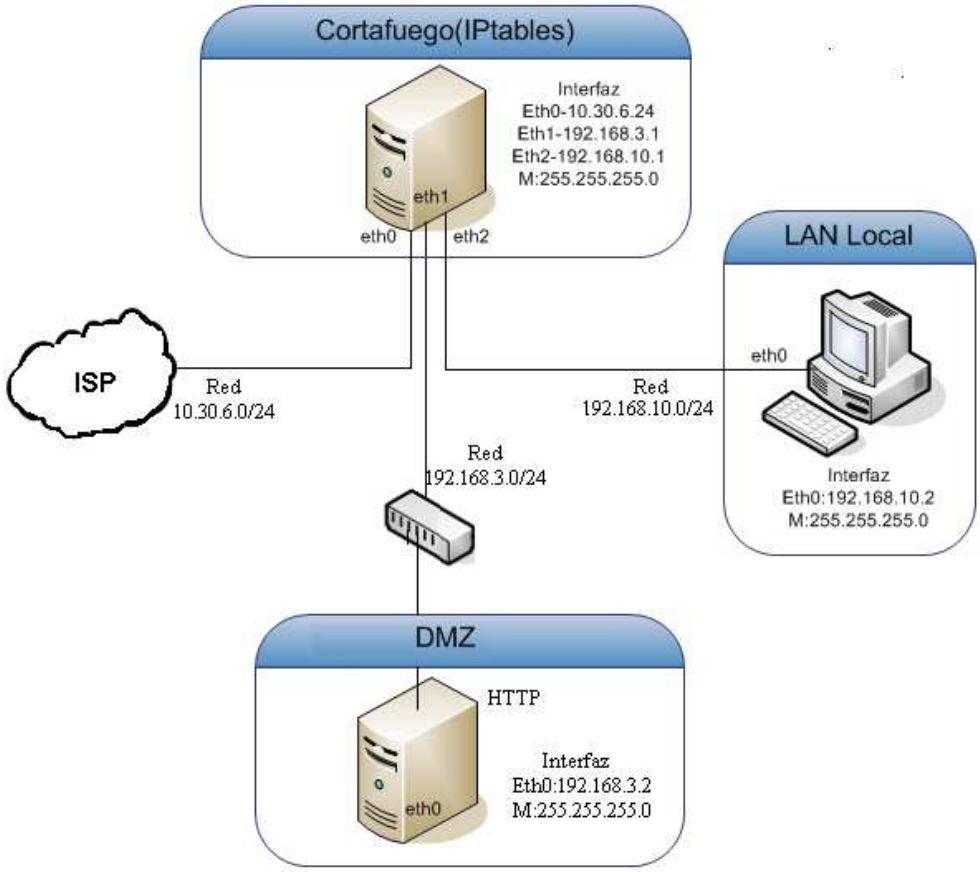


Fig. 3.3. Diagrama de la topología de la red. (Creada por el autor).

3.5 Configuración de las interfases.

Para poder establecer la conexión de las máquinas viruales a la red deseada, primeramente se debe configurar la interfaz de red de cada uno de los dispositivos. Al estar trabajando con máquinas virtuales, las interfases que se utilizan son virtuales aunque se mantienen las mismas políticas de los dispositivos físicos. La mayoría de las máquinas 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, por ejemplo en los sistemas Linux, es la activación de interfases virtuales sobre la interfaz física existente. Este podría ser una solución al problema de las interfases en el cortafuego. Pero el VMware brinda una mejor opción, por cada dispositivo instalado es capaz de agregarle varias interfases de red, así como discos duros, puertos series, paralelos, etc. De esta manera se le añaden dos interfases más a la

máquina virtual que realiza función de cortafuego y mediante estas se establecen los caminos de comunicación hacia la zona desmilitarizada (DMZ), la red local y el ISP.

3.5.1 Configuración de las interfases eth0, eth1 y eth2 del cortafuego.

Al tener una topología de red como la mostrada anteriormente en la Fig. 2.3 se hace necesario que el cortafuego tenga presente tres interfases 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 máquina virtual se configuran las interfases mediante el Virtual Network Editor. Con esta herramienta del VMware se escogen una de las interfases 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 en que se quiera conectar la máquina virtual a la red física se escoge “Bridged” o “Host-only” si se desea conectar a la máquina física. Para este trabajo se escogió la conexión Bridged (Ver Fig. 2.4)

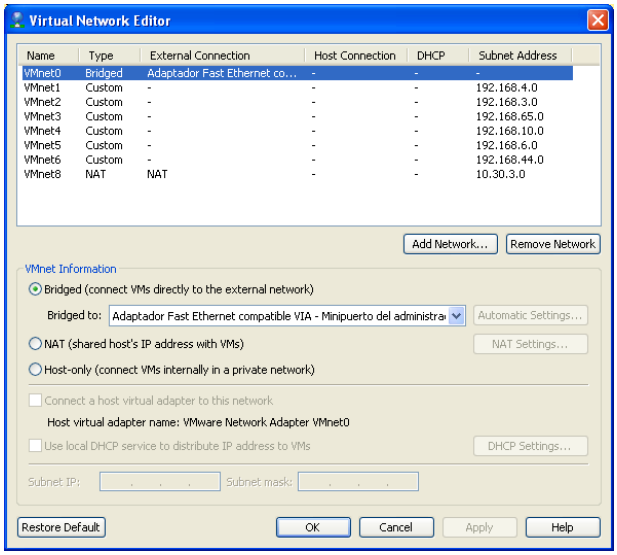


Fig. 3.4. Configuración de la interfaz eth0 del cortafuego. (Creada por el autor)

De esta forma queda configurada la interfaz eth0 desde el Virtual Network Editor.

Para la conexión de las restantes interfases con el VMware se utiliza el mismo editor de interfases tal como muestra la Fig. 2.4, 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 virtuales pertenecientes a la red especificada en dicho editor. Solamente quedaría asignar las máquinas virtuales de la red especificada a ese conmutador virtual. Esto se realiza mediante la configuración de red de cada máquina virtual en particular (Ver Fig. 2.5).

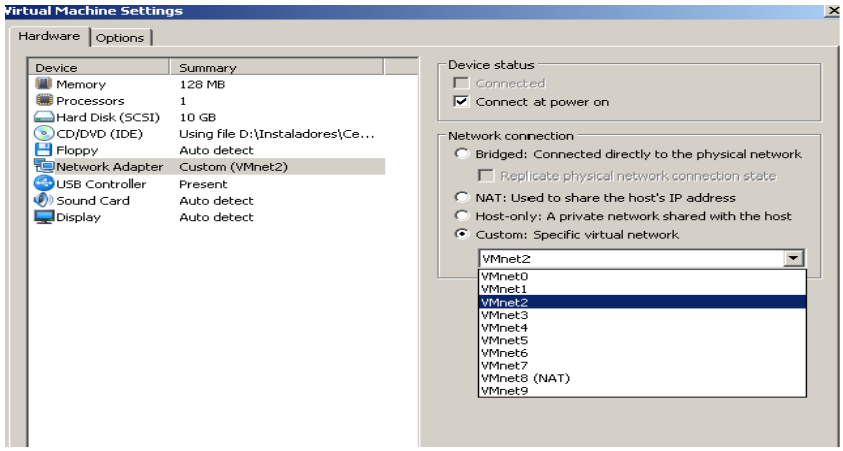


Fig. 3.5. Configuración de la red desde el escenario de cada máquina virtual. (Creada por el autor).

La red también se configura desde la máquina virtual creada. Desde el punto de vista del Terminal, este se hace mediante el comando ¨**nano /etc/sysconfig/network-scripts/ifcfg-eth0/**¨. Ver Fig. 2.6. En este archivo se configuran todos los parámetros de red necesarios para el buen funcionamiento del dispositivo en la misma. Se hace algo parecido a lo explicado anteriormente con el VMware, 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 y la es pasarela 10.30.6.254.

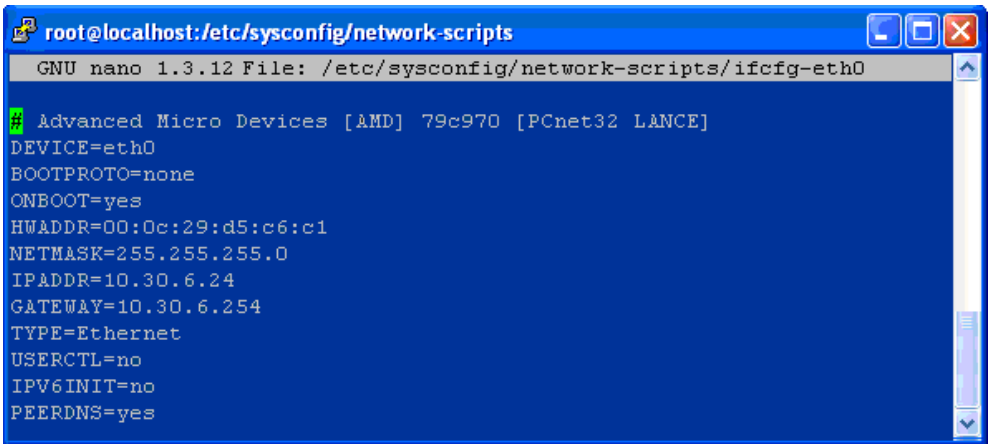


Fig. 3.6. Configuración de eth0 del cortafuego mediante el Terminal. (Creada por el autor)

De al misma forma se configuran las interfases eth1 y eth2. Al igual que eth0, existe un archivo de configuración para cada una de estas interfases, ¨**nano /etc/sysconfig/network-scripts/ifcfg-eth1**¨ para el terminal virtual eth1 y ¨**nano /etc/sysconfig/network-scripts/ifcfg-eth2**¨ para el tercer terminal virtual eth2.

Para hacer activas estas interfases solamente se les debe de poner la dirección IP de la red a la que va a pertenecer. En el caso de la interfaz perteneciente a la DMZ (eth1) la dirección IP es 192.168.3.1 y la máscara de la red 255.255.255.0. El otro terminal eth2, el cual pertenece a la red local tiene como dirección IP 192.168.10.1 con máscara 255.255.255.0. Cada una de estas direcciones perteneciendo a las redes 192.168.3.0 (DMZ) y a la red 192.168.10.0 (red interna).

Para la comprobación de la existencia de estos terminales solamente se debe escribir, por ejemplo, **ifconfig eth0** para la interfaz eth0 y salen todos los parámetros de dicha interfaz o lo que es lo mismo **ifconfig** y salen todas las interfases existentes y sus parámetros correspondientes (Ver Fig. 2.7).

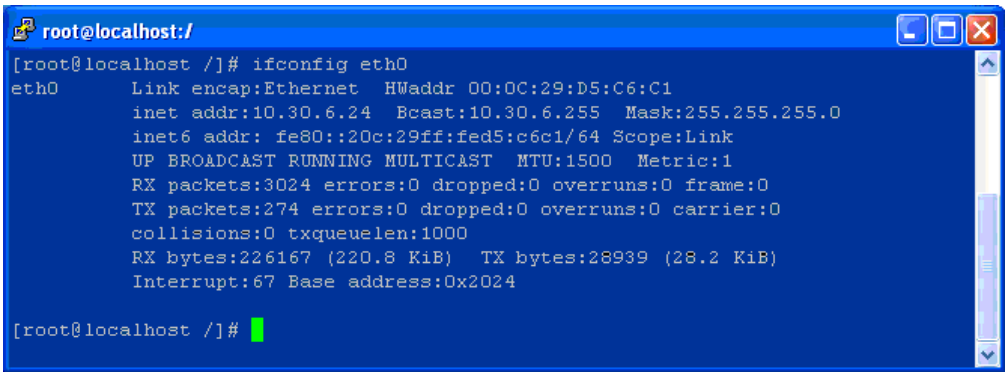


Fig. 3.7. Verificación de la interfaz eth0 del cortafuego. (Creada por el autor**)**

3.5.2 Configuración de la interfaz eth0 del servidor Web ubicado en la DMZ.

El servidor que se encuentra en la zona desmilitarizada (DMZ), es una representación de varios de los servidores que pueden prestar servicios en dicha zona. Si ese fuera el caso se realizarían todas las configuraciones para cada una de las interfases. Para poder establecer los parámetros de red en los servidores ubicados en la DMZ ocurre lo mismo que en el cortafuego. Lo que tiene como diferencia que solamente se establecen los elementos de red del terminal eth0.

Se utiliza el Virtual Network Editor para configurar la interfaz eth0 de estos nuevos elementos. A este terminal se le asigna desde el escenario de la máquina virtual del VMware la salida por el VMnet2. Es decir, estos dispositivos pertenecen a la red 192.168.3.0 al igual que una de las tarjetas de red del cortafuego. (Ver Fig. 2.8).

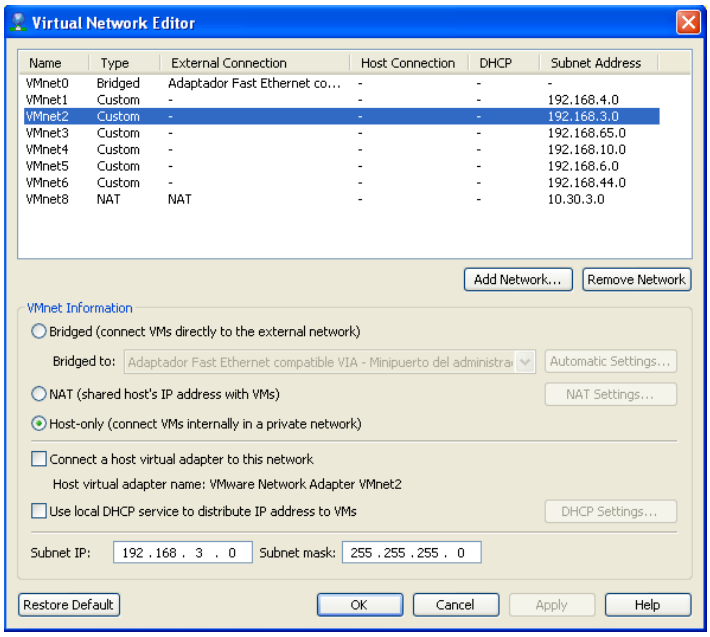


Fig. 3.8. Configuración de la interfaz eth0 de la DMZ. (Creada por el autor)

En el caso de los servidores, las funciones son las mismas ya que se utiliza el mismo sistema operativo y versión. Se utiliza ¨**nano**¨ como editor de configuración y para ello se establece la sintaxis, **"nano /etc/sysconfig/network-scripts/ifcfg-eth0"** (Ver Fig. 2.9).

Una vez abierto el editor, se pasa a introducir todos los parámetros necesarios para el funcionamiento de cada uno de los dispositivos en la red.

Como se muestra en la Fig. 2.9 se establece la dirección IP 192.168.3.2, la red 192.168.3.0, la máscara 255.255.255.0, y por último se le agrega la pasarela 192.168.3.1 o puerta de enlace del servidor Web.

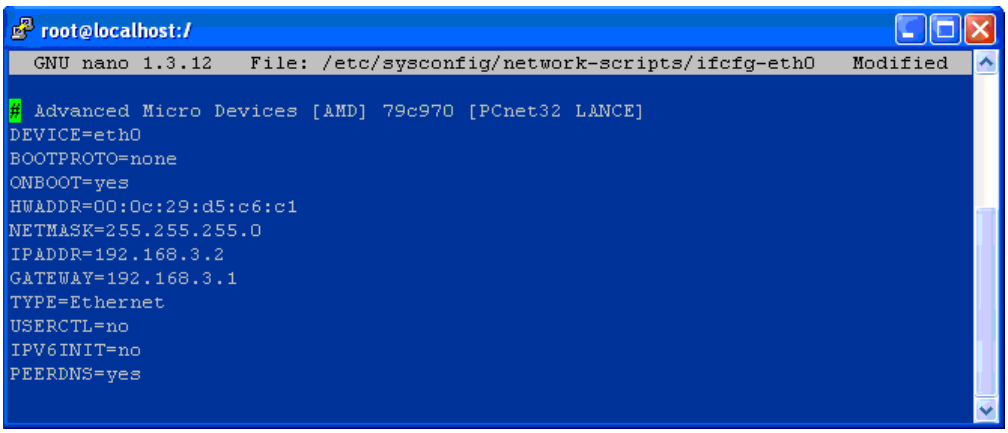


Fig. 3.9 Configuración de eth0 del servidor mediante el Terminal. (Creada por el autor)

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

3.5.3 Configuración de la interfaz eth0 de la máquina en la red interna.

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

Para la configuración de los parámetros de red para la máquina, se realizan pasos similares que en los casos anteriores. 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 máquina (VMnet4). Este va a ser el conmutador virtual por donde va a comunicarse esta máquina y solamente quedaría establecer la conexión de este dispositivo a dicho conmutador. Como se menciona anteriormente esta función se realiza por el escenario de la máquina virtual (Virtual Machine Setting) (Ver Fig. 2.10).

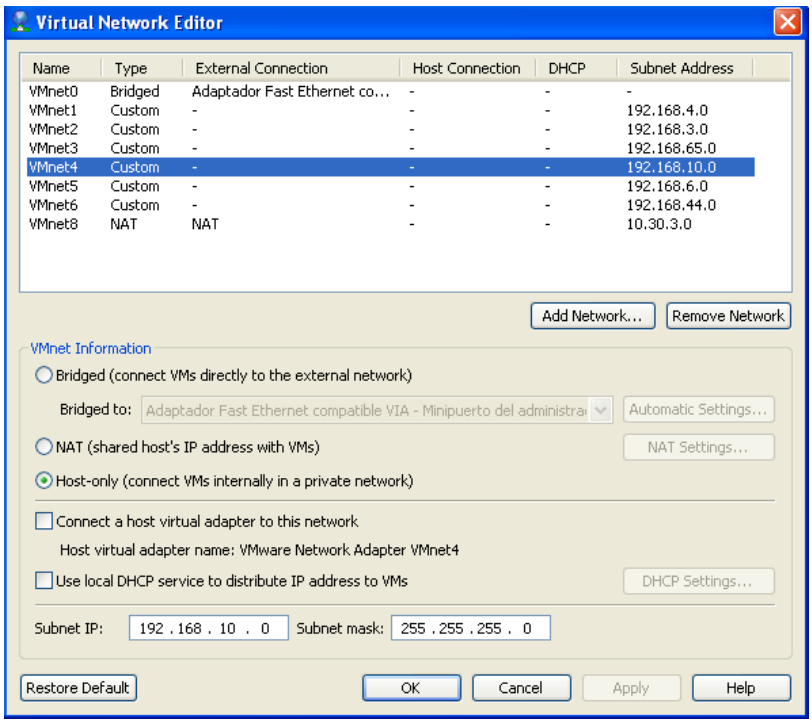


Fig. 3.10. Configuración de la máquina virtual de la red local. (Creada por el autor).

Solo queda mencionar que esta máquina realiza su conexión en el mismo conmutador que la tarjeta de red correspondiente a eth2 del cortafuego, perteneciendo a la misma red que la máquina en la red local.

Nuevamente mediante el archivo ¨**nano /etc/sysconfig/network-scripts/ifcfg-eth0**¨ se pueden establecer los parámetros necesarios para el buen funcionamiento de la máquina virtual 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 Fig. 2.11).

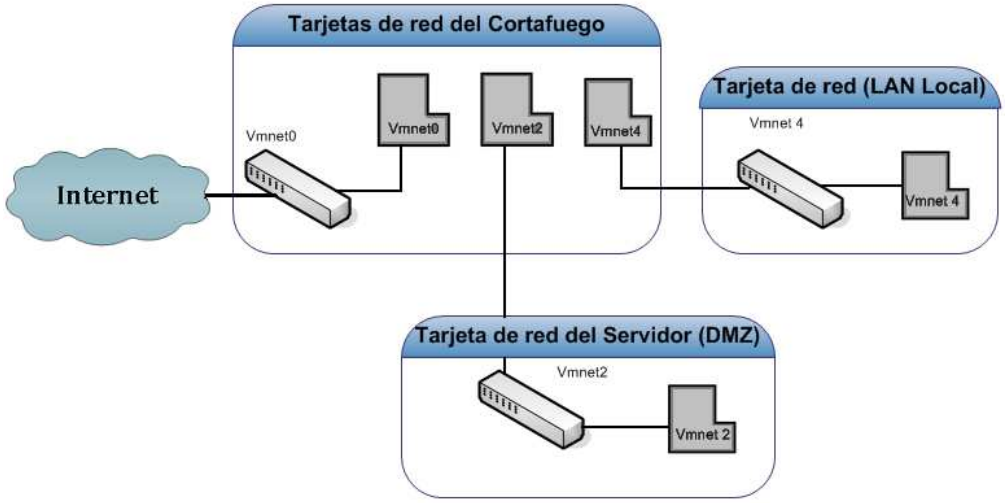


Fig. 3.11. Configuración de las tarjetas de red de las máquinas virtuales. (Creada por el autor)

Una vez que se concluyen todas las configuraciones de red necesarias se pasa a la activación del servicio, CentOS logra esto mediante el comando 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 se utiliza el comando service network restart**,** o a la hora de detener el servicio se emplea el comando service network stop. Una vez guardado los cambios se pueden enviar todo tipo de paquetes de red.

Hay algo muy importante que no se puede dejar de mencionar, y es que todas las conexiones excepto VMnet0 perteneciente al cortafuego son de tipo “Custom”. Este brinda conexión entre los dispositivos virtuales sin conectarse a la máquina física o tener salida hacia la red exterior. Por esa razón el conmutador virtual VMnet0 de la red 10.30.6.0 tiene conexión de tipo “Bridged” y los demás conmutadores de tipo Custom. Así se garantiza que la salida hacia el proveedor de servicios de Internet (ISP) sea por una sola interfaz y las demás pertenezcan solamente a la red virtual.

3.6 Verificación de la conexión.

Para verificar el estado de la conexión se utilizan comandos como el ping y el traceroute. Para CentOS a la hora de utilizar el ping se debe especificar la cantidad

de paquetes que se van a transmitir, en caso de que no se especifique, se estará mandado paquetes hasta que se aborte la operación, para esto se utiliza la combinación de teclas Ctrl + c. Un ejemplo de esto es **ping -c5 10.30.1.3**, donde 10.30.1.3 es la dirección de la máquina física y de esta forma se puede ver si hay conexión o no y –c5 especifica la cantidad de paquetes a transmitir (Ver Fig. 2.12).

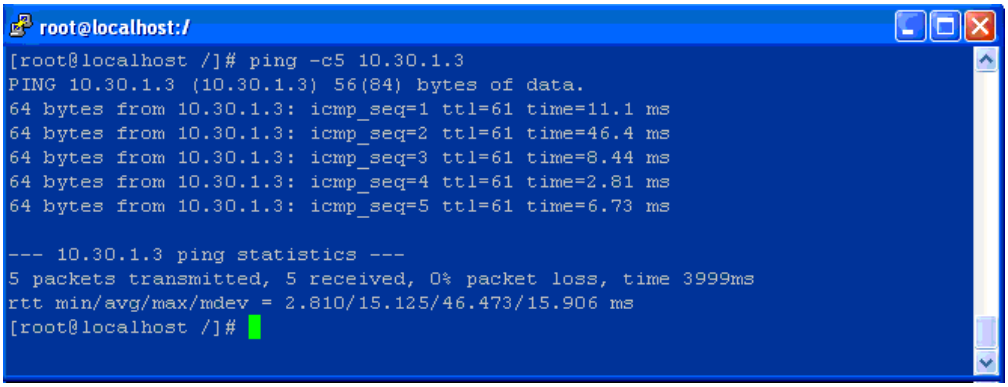


Fig. 3.12 Verificación de la conexión entre una máquina virtual y una máquina física. (Creada por el autor).

3.7 Instalación y configuración del cortafuego IPtables.

Los cortafuegos son poderosos y muy populares en las redes de datos cuando se habla de seguridad. El IPtables es una de las herramientas más utilizadas ya que con su uso se realiza el NAT (Traducción de Dirección de Red) deseado entre las redes escogidas. Además de esto se pueden realizar filtrados de paquetes.

Para la red implementada las cadenas de IPtablesno son numerosas ya que la topología es pequeña. Las peculiaridades que presenta están en que el cortafuego tiene tres interfases 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 ambos sentidos de transmisión, no siendo así en la conexión directa desde el ISP con la red local. De esta manera se protege la red interna, se controla todo el tráfico enviado y recibido, y mediante las cadenas de IPtablesimplementadas se crean términos de seguridad con respecto a la zona desmilitarizada (Ver Fig. 2.13).

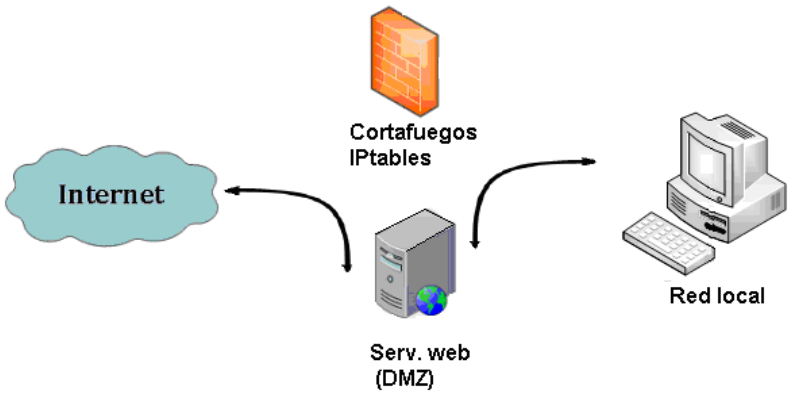


Fig. 3.13 Sentido del NAT en el cortafuego. (Creada por el autor).

Lo primero que se debe hacer para la instalación del cortafuego es descargar los paquetes necesarios para el buen funcionamiento de este, los cuales se encuentran en los repositorios de CentOS esto se hace mediante el comando:

[root@httpd]# yum install iptables.

Yum es una herramienta muy importante para el manejo de paquetería rpm. Se hace alusión a esto ya que para las instalaciones y desinstalaciones de paquetes en los sistemas de código abierto es muy usado y se hace muy simple esta operación mediante su utilización. Con el paquete IPtables instalado completamente se pasa a trabajar sobre él y así realizar los cambios necesarios en el cortafuego.

Este elemento trae algunas políticas por defecto que en mucho de los casos no son las adecuadas para mantener la red segura. Por esta razón se deben borrar las reglas existentes para el tráfico entrante, tráfico reenviado y tráfico saliente así como el NAT e implementar las nuevas reglas para el sistema, esto se logra de la siguiente manera:.

iptables -F INPUT.

iptables -F FORWARD.

iptables -F OUTPUT.

iptables -F -t nat.

Existen varias variables con las cuales se trabaja, que especifican el tipo de cadena, interfases, puertos, direcciones IP, etc. Las reglas a crear se configuran y quedan almacenadas en el fichero **/etc/sysconfig/iptables.**

Las cadenas que se utilizaron en el IPtables implementado son:

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.3.2:80.

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 10.30.6.24:80.

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 pre-enrutamiento (PREROUTING) para un tráfico desde la interfaz eth0, con un DNAT a la dirección IP 192.168.3.2. Se usa (--to destino) para indicar el destino de dicho tráfico. Para una segunda cadena ocurre lo mismo lo que en el sentido inverso. Ahora el tráfico de la interfaz eth1 se le realiza un DNAT hacia la dirección 10.30.6.24.

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 53 -j DNAT --to 192.168.3.2:53.

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 53 -j DNAT --to 10.30.6.24:53.

Las cadenas anteriores abren el puerto correspondiente al servicio de nombre de dominio para ambas redes.

iptables -A INPUT -i eth1 -s 192.168.10.0/24 -j ACCEPT.

Esta cadena específica la entrada de tráfico hacia la zona desmilitarizada desde la red local. Indica la apertura de una cadena (-A) de entrada de tráfico (INPUT) desde la dirección de red 192.168.10.0/24 hacia 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.

Como mismo ocurre en el primer punto, sucede en este segundo caso, lo que el NAT realizado es ahora entre la DMZ y la red local. La estructura de la cadena es similar desde el punto de vista del significado. Solo cambian algunos aspectos como las direcciones IP del origen y destino del tráfico, el cual sale por las interfases virtuales previamente creadas. 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 INPUT -p tcp -s 10.30.6.19/24 -d 10.30.6.24/24 --destination-port 22 -j ACCEPT

La cadena anterior abre la conexión para tener acceso al cortafuego mediante el protocolo SSH solamente desde la máquina con dirección IP 10.30.6.19.

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

Esta 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 local.

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

Al igual que la cadena anterior, esta evita el reenvío de paquetes ipv4 pero en el sentido contrario, desde la red local hacia la zona desmilitarizada.

iptables -A FORWARD -s 192.168.10.0/24 -o eth0 -j DROP.

iptables -A FORWARD -s 10.30.6.0/24 -o eth2 -j DROP.

Estas dos últimas cadenas paran todo el tráfico directo entre la red local y el proveedor de servicios de Internet logrando de esta manera los saltos deseados.

Para verificar las reglas configuradas en el cortafuego se hace mediante el comando **iptables-nL.**

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 ya establecido el servicio, entonces se realiza **service iptables restart**. En el caso de parar el mismo se usaría **service iptables stop**. Otras de las habilidades que presenta el servicio de IPtables es que puede comenzar con el arranque del sistema mediante **chkconfig iptables on**.

Lo antes expuesto está organizado en el mismo orden que en el cortafuego. 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.

Para verificar los puertos abiertos se utiliza el comando **nmap**con la sintaxis siguiente:

nmap IP remoto

[root@localhost]# nmap 10.30.6.24

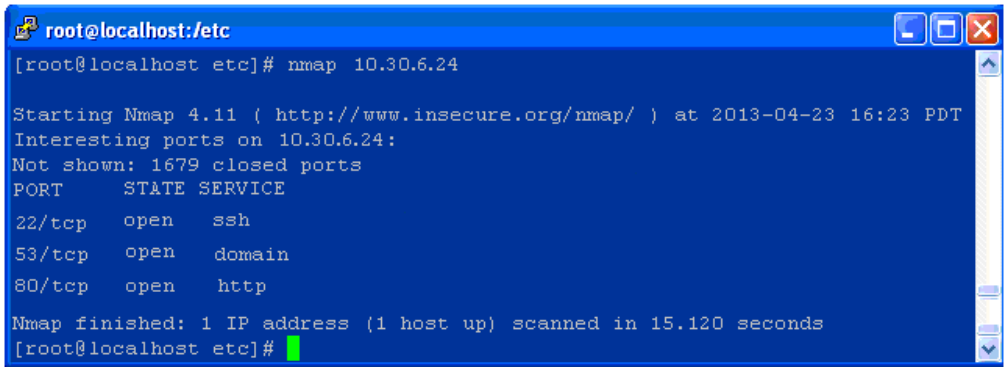


Fig. 3.14 Puertos abiertos en la interfaz del cortafuego con el servidor. (Creada por el autor**)**

2.8 Activación del reenvío de paquetes IPv4 y de rutas en las tarjetas de red en los sistemas operativos.

Para poder realizar el reenvió de paquetes en la red se hace necesario 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 cortafuego ya que sus funciones están en el manejo de información de una dirección a otra en la red.

Para activar dicha función solamente se debe ejecutar el archivo de configuración **/etc/sysctl.config**, y establecer 1 para activar el servicio ó 0 para mantenerlo inactivo.

Para modificarlo se ejecuta:

nano /etc/sysctl.conf.

Y se cambia **net.ipv4.ip_forward = 0** por **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 Ipv4 para el cortafuego (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 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.

En CentOS para comprobar las rutas establecidas en dicho sistema se realiza mediante el comando **route -v** como se muestra en la Fig. 2.15.

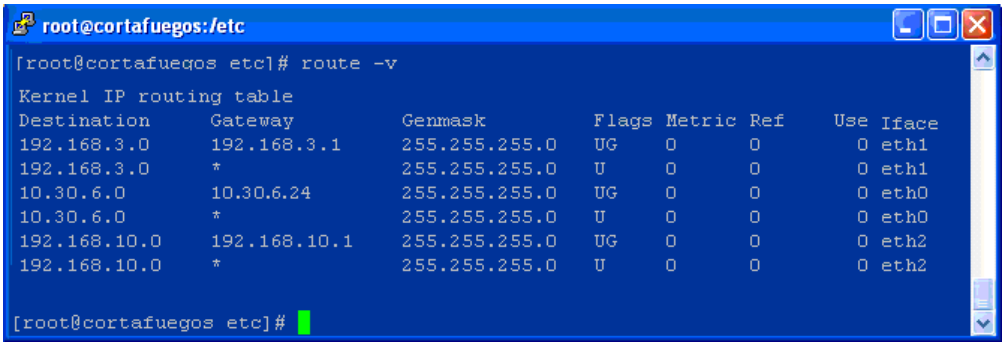


Fig. 3.15. Rutas creadas en el cortafuego. (Creada por el autor)

2.9 Instalación y configuración del servidor Web Apache**.**

Para Som, G. (s.f.):

> Apache es un servidor Web HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual, el servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Fundation, fundación creada para dar soporte a los proyectos de software bajo la denominación Apache. Este es el servidor Web más utilizado con más de un 50%.

Instalación del servidor Web Apache: Para la puesta en marcha del servidor web se cuenta con la instalación de un servidor DNS para realizar la traducción del nombre de dominio funcionando en la misma máquina donde se instalará dicho servidor. El

primer paso que se debe seguir es instalar el servidor, este está en los repositorios de CentOS y se puede descargar como httpd a través del comando:

[root@httpd]# yum install httpd

Luego se va a la carpeta donde está ubicado uno de los archivos de configuración del Apache. Esto se realiza de la siguiente manera:

[root@httpd]# cd /etc/httpd/conf/

Si se lista se puede ver el archivo httpd.conf el cual se procederá a modificar con cualquier editor de textos instalado, en este caso se usó el nano.

[root@httpd conf]# ls

httpd.conf magic

[root@httpd conf]# nano httpd.conf

Lo primero será buscar la línea que dice **NameVirtualHost *:80** y descomentarla para habilitar los Hosting Virtuales.

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:

Para AyZSoluciones. (s.f.):

> ServerTokens:Esta directiva limita la cantidad de información que será mostrada por el servidor Web Apache como puede ser, la versión del servidor Web 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.

Comentario [f51]: http://es.scribd.com/doc/65987341/Servicio-Web-en-Centos

http://ayzsoluciones.blogspot.com/p/blog-page_6.html

http://bunchtech.wordpress.com/2011/01/page/7/

Para el caso del sistema instalado se escoge la versión y el sistema operativo sobre el cual trabaja.

DocumentRoot: La ruta donde estará ubicado el documento de la página Web.

Directory:El mismo DocumentRoot

DirectoryIndex:El archivo index de la página Web

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

ServerRoot "**/etc/httpd".**

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.

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

Listen 192.168.3.2:80

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 (http://dns.bdat.net/).

User apache

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 (Tejada, M. 2011)

Group apache

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

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.prueba.com:80(Amaya, C. 2011)

Luego se busca en la línea final de este archivo y se añadirá el texto **"Include/etc/httpd/conf.d/prueba.com"**esta línea lo que hace es incluir en este archivo de configuración, el archivo **"prueba.com"** el cual es un archivo que aún no se ha creado pero en este se crearan los host virtuales.

Comentario [f52]: http://dns.bdat.net/blog/index.php/administracion/6-apache/18-configuracion-del-servidor-principa?showall=1&limitstart=

http://dns.bdat.net/documentos/entorno_publicacion_web/x677.html

http://www.monografias.com/trabajos-pdf4/instalar-servidor-apache-php-mysql/instalar-servidor-apache-php-mysql.pdf

Comentario [f53]: http://dns.bdat.net/documentos/entorno_publicacion_web/x677.html

http://www.monografias.com/trabajos-pdf4/instalar-servidor-apache-php-mysql/instalar-servidor-apache-php-mysql.pdf

http://mauricio-tejeda.blogspot.com/2011/10/apache-en-centos.html

Comentario [f54]: http://sistemasligth.blogspot.com/2012/11/servior-web-apache-en-centos.html

http://es.scribd.com/doc/65987341/Servicio-Web-en-Centos

Luego de guardar los cambios en el archivo, se cierra, entonces se va a la ruta indicada para crear este archivo.

[root@httpd conf]# cd /etc/httpd/conf.d/

Si se lista se puede ver que el archivo **"prueba.com"** no existe. Por lo que se procederá a crearlo y modificarlo con el editor de textos utilizado (Ver Fig. 2.16).

[root@httpd conf.d]#nano prueba.com

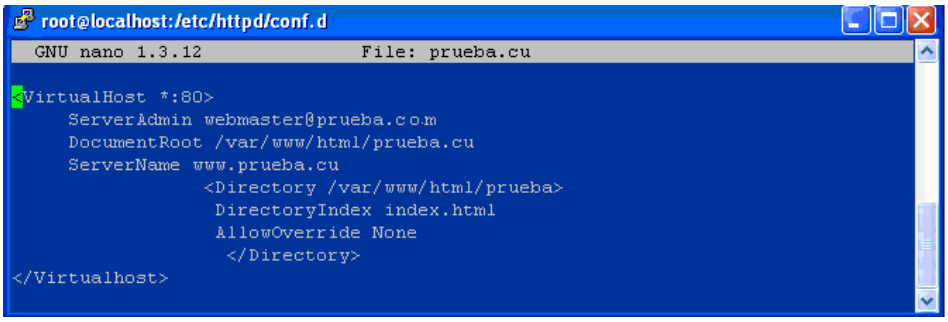


Fig. 3.16: Archivo prueba.com. (Creada por el autor)

Los DirectoryIndex y el DocumentRoot no han sido creados por lo que se procederá a crearlos, además si se quisiera alojar varias páginas Web en el servidor simplemente bastaría con ponerlas debajo de esta de la misma manera con los parámetros adecuados. Ahora se creará el DocumentRoot, primero se va a la carpeta html ubicada en la dirección **/var/www/html**.

[root@httpd conf]# cd /var/www/html.

Si se lista se puede observar que esta carpeta no contiene nada.

Entonces se creará el DocumentRoot tal y como se declaró en el archivo anterior.

[root@httpd html]# mkdir prueba

Y ahora se creará el DirectoryIndex con el editor de texto nano, con el nombre igual al declarado en el archivo de virtualhosts.

[root@httpd html]# nano prueba/index.html

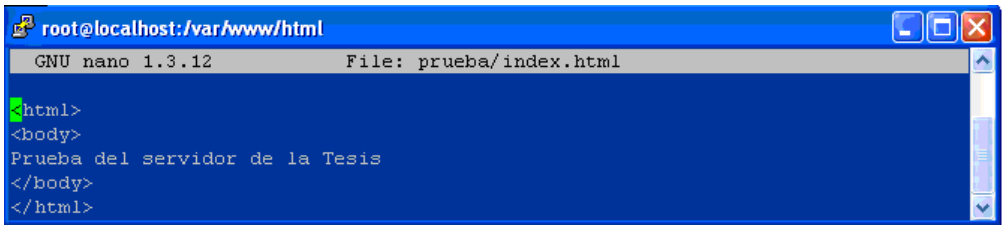


Fig. 3.17 Archivo DirectoryIndex. (Creada por el autor).

Finalizado el index de prueba se reinicia el servidor Apache, con el comando **/etc/init.d/httpdrestart**

Y se verifica que el servidor DNS este resolviendo por el ServerNameque se declaró en el virtualhost, mediante el comando:

[root@httpd conf]# nslookup www.prueba.com

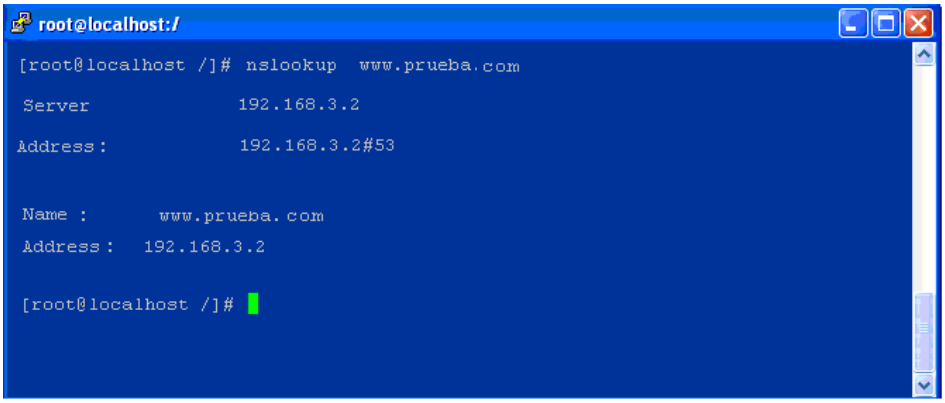


Fig. 3.18 Verificación del servidor DNS. (Creada por el autor).

Por último se verifica que el servidor este funcionando correctamente desde un cliente que esté en esta misma subred.

Fig. 3.19 Verificación del servidor Web Apache. (Creada por el autor).

Y como se puede observar el servidor Web Apache funciona perfectamente.

2.10 Conclusiones del capítulo

Como se pudo observar, el capítulo muestra la instalación de un conjunto de máquinas mediante el VMware, es decir, se crearon máquinas virtuales, con las cuales se creó un pequeño sistema con un elemento importante para cualquier institución, un cortafuego. Este es un IPtables y se configuró para realizar NAT y filtrado de paquetes entre tres zonas (ISP, DMZ, y una red interna), también se instaló un servidor con funcionalidad Web Apache situado en la zona desmilitarizada. Existe un tercer elemento que es una máquina la cual hace referencia a una red local. Se les configuró la red, comprobando su conectividad.

CAPÍTULO No4.
EVALUACIÓN DE LA SEGURIDAD

4.1 Test de penetración:

Portantier, F. (2011):

> A través del test de penetración es posible detectar el nivel de seguridad interno de los sistemas de información de una red, determinando el grado de acceso que tendría un atacante con intenciones maliciosas. Además, el servicio chequea las vulnerabilidades que pueden ser vistas y explotadas por individuos no autorizados, "crackers", agentes de información, ladrones, antiguos empleados, competidores, etc. 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.

4.2 Los servicios del test de penetración permiten.

- Evaluar vulnerabilidades por medio de la identificación de debilidades de configuración.
- Analizar y categorizar las debilidades explotables basadas en el impacto y posibilidad de ocurrencia.
- Proveer recomendaciones priorizadas para mitigar y eliminar las debilidades.

Objetivo:

- Vulnerar la seguridad de los mecanismos implantados para conseguir accesos no autorizados a la organización, obtener información sensible, interrumpir un servicio. Dependerá del alcance concreto del test realizado.
- Tratar de eliminar las vulnerabilidades detectadas.

4.3 Tipos de test de penetración:

Borja, M. (s.f.):

White box pentest: Se tiene un amplio conocimiento de la organización (estructura, departamentos, responsabilidades) y de la red (topología, dispositivos, S.O., bases de datos, IDS, cortafuegos.) Se cuenta con colaboración del personal y con acceso a los recursos de la empresa.

Para Ribadas, F. (2010):

Black box pentest: No hay conocimiento previo de la organización o la red, sólo se dispone de información públicamente accesible. Pocas personas de la organización saben que esta será atacada. Simulación más realista de un ataque auténtico. Puede ser muy costoso (tiempo [recopilación información] + personal entrenado).

Grey box pentest (combina los anteriores): Usa técnicas de un atacante real (black box) con conocimiento del sistema analizado (white box) (Borja, M. s.f.)

Comentario [f55]: http://ccia.ei.uvigo.es/docencia/SSI/1112/apuntes/pentest.pdf

http://ccia.ei.uvigo.es/dojo/pentest/Dojo.pdf

4.4 Fases y tareas típicas de un test de penetración.

4.4.1 Recopilación de información.

Etapa 1 Recolección de información: Obtener información del sistema / organización / red/ máquina bajo análisis como nombres de dominio, direcciones IP, nombres de usuarios, responsables, bases de datos públicas: whois, RIPE, DNS.

Buscadores:

1. **Genéricos:** Google hacking, bing hacking.
2. **Específicos:** Goolag (http://www.goolag.org), KartOO (http://kartoo.org)
3. **Herramientas genéricas de gestión de red:** dig, nslookup.

Etapa 2 exploración: Analizar el sistema objetivo para identificar servicios activos, máquinas disponibles, recursos/dispositivos de red (enrutadores, cortafuegos.), sistema operativo.

Herramientas genéricas de gestión de red: ping, traceroute.

Herramientas específicas escáneres de puertos: nmap, hping3, xprobe.

Para Ribadas, F. (2010):

Etapa 3 enumeración: Pruebas y test para identificar recursos específicos y sus características concretas. Identificar el sistema operativo., sus versiones y parches de seguridad (service packs, etc.), versiones concretas de servicios/aplicaciones, cuentas de usuario válidas.

Comentario [f56]: http://ccia.ei.uvigo.es/docencia/SSI/1112/apuntes/pentest.pdf

Herramientas específicas:

- Escáner de puertos e identificadores de servicios: nmap, xprobe.
- Escáner de vulnerabilidades: nessus, openvas.
- Escáner de vulnerabilidades específicos: w3af (escáner de vulnerabilidades Web)

Etapa 4 accesos: Obtener un acceso no autorizado o no previsto a algunos de los recursos o servicios identificados en el sistema objetivo.

Rotura de contraseñas: Por fuerza bruta, ataques de diccionario (Rainbow tables), prueba de contraseñas por defecto o contraseñas débiles

Herramientas: THC hydra, John the Ripper, Abel and Cain.

Sniffing, escucha de contraseñas o datos sensibles: wireshark, tcpdump, ettercap.

Inyección de tráfico: ettercap, dnsniff, sslsniff.

Explotación de vulnerabilidades específicas de las versiones concretas de los servicios/recursos identificados.

Exploits específicos: http://milw0rm.com

Herramientas automatización exploits: Metasploit, CORE Impact, SAINTexploit

Uso de valores de entrada no previstos fuzzers: exploraciones exhaustiva automatizada de los posibles datos de entrada, buscando (a ciegas) situaciones no previstas

Etapa 5 escaladas de privilegios: Obtener control completo del sistema, adquiriendo y manteniendo permisos, credenciales y privilegios propios de los administradores.

Objetivos:

- Validar si para el supuesto atacante sería posible adquirir privilegios que le permitieran ejecutar acciones maliciosas o acceder a datos restringidos.

- Suele requerir incluir código específico en el sistema objetivo (payload) que permitan realizar determinadas acciones.
- Normalmente ofrecen algún tipo de acceso remoto al mismo (habilitan puertas traseras): abrir shells del sistema con privilegios (bash), habilitar conexiones de escritorio remoto (VNC).

Herramientas automatización exploits: Metasploit, Core Impact

Puertas traseras: BackOrifice, LCP 5.0

Etapa 6 daño: Valorar y evaluar la capacidad del atacante que ha "escalado" privilegios de realizar acciones maliciosas que causen daño:

Daños posibles: Acceso a datos confidenciales.

Robo de información:

- **Alteración de información:** datos protegidos, páginas Web.
- **Denegación de servicio (DoS):** Imposibilitar el acceso o uso de determinados componentes del sistema a sus usuarios legítimos.

Extensión del ataque:Evaluar la posibilidad de usar el sistema controlado como punto de partida para iniciar ataques a otras partes del propio sistema objetivo o a sistemas ajenos.

Etapa 7 borrado de huellas: Verificar hasta que punto el potencial atacante tendría capacidad de eliminar el rastro de sus acciones maliciosas y mantener su control del sistema de forma permanente sin ser detectado.

Comentario [f57]: http://ccia.ei.uvigo.es/docencia/SSI/1112/apuntes/pentest.pdf

Objetivo: Eliminación de los registros y logs que contengan información que revele la existencia del ataque y que pudiera ser de utilidad en un análisis forense o una auditoria de seguridad.

Etapa 8 informe final del test.

Informe técnico: Resumen del proceso realizado, clasificación de las vulnerabilidades encontradas y su nivel (alto, medio, bajo), propuesta de correcciones y sugerencia de buenas prácticas

4.5 Informe del test realizado a la DMZ

Para este caso se va a realizar un test de penetración del tipo Black-Box Externo (atacando desde la red externa, y sólo conociendo el nombre del servidor que se le va a realizar el test).

Etapa 1 recolección de información:

- Nombre del servidor.

- Datos de los servidores DNS para ese dominio.

Lo primero que se hace es utilizar el comando '**dig**' para obtener la información acerca de los servidores DNS asociados a dicho dominio.

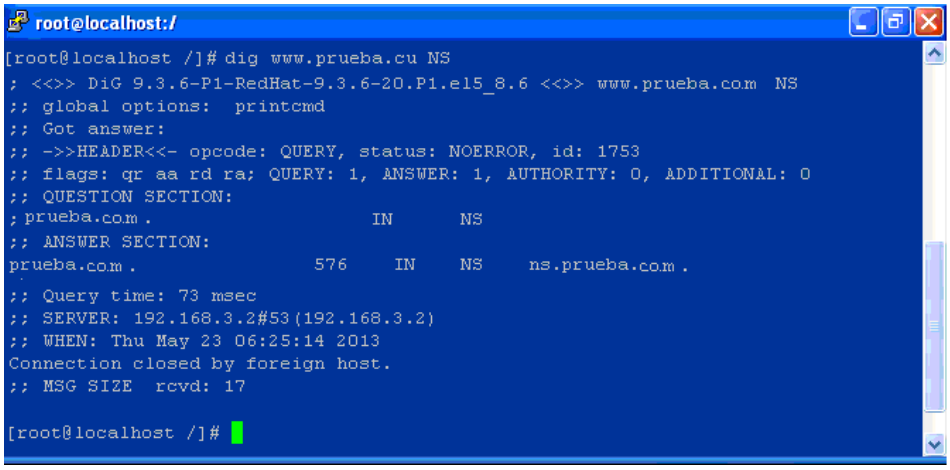


Fig. 4.1 Información sobre el servidor DNS. (Creada por el autor).

De aquí se puede ver que el servidor ns.prueba.com es el encargado del DNS de este dominio.

Ya con esto se puede utilizar el comando '**fpdns**' para obtener más información acerca del servidor de DNS:

Fig. 4.2 Respuesta del comando fpdns. (Creada por el autor).

Con esto ya se sabe que el servidor DNS es un**CentOS**.

Etapa 2: exploración:

También se puede utilizar la herramienta **nmap** para obtener más información del servidor, (se utiliza sudo porque las pruebas **-O** y -**sV** necesitan permisos de **root**)

Fig. 4.5 Servicios, versiones y puertos abiertos del servidor. (Creada por el autor).

De este reporte se puede ver que, además de estar corriendo un servidor Apache 2.2.3, el sistema operativo es un **CentOS Linux**.

Las pruebas con **nmap** también se pueden hacer contra los servidores DNS, para recabar más datos aún. Y tener más información para encontrar vulnerabilidades asociadas al software del equipo.

Etapa 3: enumeración:

El siguiente paso será analizar el servidor Web, como el servidor Web es **www.prueba.com**, se hace un **telnet** al puerto 80 para obtener alguna que otra información básica.

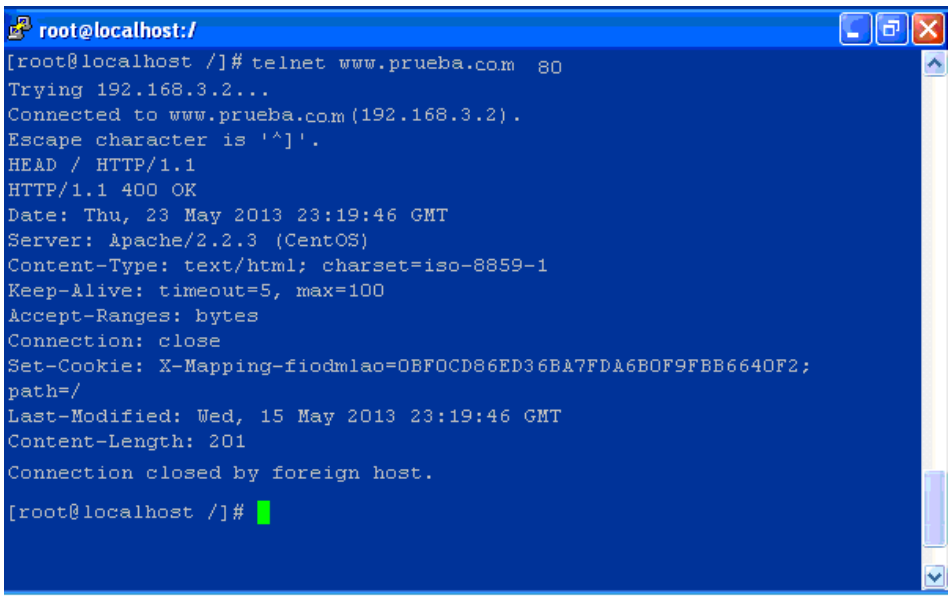


Fig. 4.3 Información del servidor web. (Creada por el autor)

Aquí se puede ver la información básica del servidor Web (Apache/2.2.3 (CentOS)).

Etapa 4 acceso:

Para obtener información sobre posibles vulnerabilidades en el mismo, se utiliza la herramienta especializada, **nikto.**

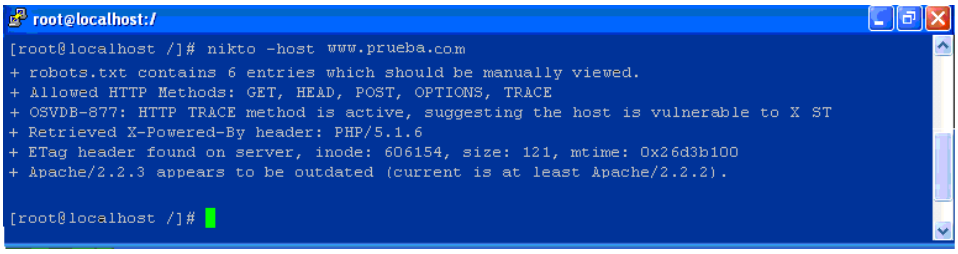


Fig. 4.4 Posibles vulnerabilidades (Creada por el autor)

Con lo cual, se puede determinar que los siguientes pasos serán:

- Analizar el archivo **'robots.txt'** y buscar anormalidades.

- Verificar si se podría explotar el método '**TRACE**' para atacar el servidor.

- Buscar vulnerabilidades en la versión de **PHP** instalada (5.1.6).

- Buscar vulnerabilidades en la versión de Apache instalada (2.2.3).

Con todos estos datos ya se puede armar un mapa de los servicios básicos que está brindando prueba.com. En base a esto se puede obtener algunos otros datos adicionales, con algunas herramientas como:

Nessus, OpenVAS, Metasploit.

4.6 Conclusiones del capítulo

No se pudo conectar desde la red externa a ningún puerto cerrado del servidor Web, pero si se pudo obtener información muy importante sobre él. Lo que quiere decir que la seguridad de una red no depende solamente de la configuración de un cortafuego, sino que los servicios que estén corriendo en los diferentes servidores localizados en la DMZ estén actualizados con la última versión que haya salido, para que esas vulnerabilidades sean parcheadas, debido a que cuando los hacker encuentra una vulnerabilidad en el mismo la publican y crean exploit para explotarlas para su propio beneficio, es decir, el bloqueo de un determinado servidor, pidiendo dinero a cambio para desbloquearlo etc.

CONCLUSIONES

Este trabajo culminó con el estudio de diversos temas de seguridad informática al plasmar conceptos y métodos de control de acceso. Se logró virtualizar una topología de red pequeña donde se pudieron evaluar las diferentes políticas de seguridad implementadas en el cortafuego.

El estudio de las especificidades de Linux fue muy importante ya que ayuda a entender elementos como los IPtables para la implementación de cortafuegos, y así brindar gran seguridad en redes privadas.

Se demostró la efectividad de la DMZ, esto es debido a que el cortafuego implementado separa el acceso de la red externa con la red interna. Esto brinda un alto nivel de seguridad para el acceso a los servidores y a la red militarizada desde el punto de vista lógico, gracias a las políticas creadas, las que pueden implementarse a la hora de establecer las reglas del cortafuego.

La herramienta VMware constituyó el centro de funcionamiento gracias a sus capacidades para la virtualización y conexión a la red y permitió la realización de las pruebas de penetración para evaluar la efectividad de las políticas seleccionadas en el cortafuego.

Mediante el test de penetración se evidenció la robustez de los cortafuegos IPtables, ya que no se pudo penetrar al servidor por otro puerto diferente al 80, ni acceder a la red interna. También demostró que los servidores deben de estar actualizados con la última versión del sistema operativo y de los servicios que corren sobre él, debido a que las actualizaciones eliminan las vulnerabilidades existentes en las versiones anteriores.

RECOMENDACIONES

- Continuar el estudio de los métodos y herramientas de seguridad de código abierto para implementar otros métodos de seguridad como por ejemplo un sistema de detección de intrusos (IDS).
- Seguir el trabajo con el VMware para realizar este tipo de experiencias de laboratorio con la utilización de programas malignos reales del tipo exploits, puertas traseras, bombas de tiempos, troyanos, etc.
- Capacitar a los estudiantes y docentes sobre los métodos y herramientas de seguridad física y lógica.
- Realizar prácticas de laboratorio en las asignaturas correspondientes sobre seguridad.

REFERENCIAS

Ardita, J.(2008). Aspectos Prácticos de Seguridad.

Barrios, D. (2012). Configuración De Servidores Con GNU/Linux.

Barrios, D. (s.f.). Introducción a IPTABLES. Recuperado 10 de abril 2013, de http://www.alcancelibre.org/introducción-a-iptables

Borghello, C.(2005). Linux máxima Seguridad.

Borghello, C. (2008). Seguridad Informática, Sus Implicaciones e Implementación.

Borja, M. PENTEST: RECOLECCIÓN DE INFORMACIÓN (INFORMATION GATHERING).

Cabaleiro, J. (s.f.). Seguridad informática.

Coletti, D. (s.f.).Entendiendo IPtables. Recuperado 10 de marzo 2012, de http://www.danielcoletti.com.ar/Documentos/Tech/Iptables/iptables/node15.html

Colás, C. (s.f.). Virtualización de una red LAN con servidores de código abierto para evaluar los niveles de seguridad.

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

DMZ (Zona desmilitarizada). (s.f.). Recuperado 10 de marzo 2012, de http://es.kioskea.net/contents/protect/dmz-cloisonnement.php3

Escartín, V. (2005). Servidor Linux para conexiones seguras de una LAN a Internet.

Firewall. (s.f). recuperado 6 de abril 2013, de http://es.kioskea.net/contents/protect/firewall

FIREWALL. (2008). Recuperado 3 de mayo 2013, de http://carolavega.blogspot.com/2008/08/firewall.html

Instalación de un servidor Web Apache en CentOS. (s.f.). Recuperado 7 de enero 2013, de http://gnunick.blogspot.com/2011/03/instalando-un-servidor-web-en-centos.html

Morales, R. (s.f.). Diseño de aseguramiento de redes utilizando DMZ'S

Portantier, F. (2011) ¿Cómo realizar un Penetration Test?

Protección. (s.f.). Recuperado 7 de enero 2012, dehttp://www.segu-info.com.ar/proteccion/proteccion.htm

Ramos, F. (2011). Seguridad Perimetral.

Seguridad Lógica. (s.f). Recuperado 5 de enero 2012, de http://www.segu-info.com.ar/logica/seguridadlogica.htm

Semeria, C. (s.f.). Firewalls y seguridad en Internet: Recuperado 15 de abril 2012, de http://www.monografias.com/trabajos3/firewalls/firewalls.shtml

Som, G. (2007). Máquinas virtuales. Recuperado 5 de enero 2012, de http://www.elguille.info/sistema/máquinas_virtuales.htm

Tipos de cortafuegos según el nivel OSI: (s.f.). Recuperado 3 de mayo 2013, de http://www.elprisma.com/apuntes/ingenieria_de_sistemas/cortafuegos/default5.asp

Linux Security HOWTO. (Documento PDF) 25 Abril 2006

Villalón, H. (2006). Seguridad en Linux y Redes.

Zona desmilitarizada (informática). (s.f.). Recuperado 5 de enero 2012, de http://www.danielcoletti.com.ar/Documentos/Tech/Iptables/iptables/node15.html

OTRAS BIBLIOGRAFIAS CONSULTADAS.

Borja, Merino. PENTEST: RECOLECCIÓN DE INFORMACIÓN (INFORMATION GATHERING). (Documento PDF).

Borghello Cristian Fabián. Linux máxima Seguridad. Marzo 2005.

Borghello Cristian Fabián. Seguridad Informática, Sus Implicaciones e Implementación. A.S.S. Septiembre 2008

Barrios Dueña, Joel. Alcance Libre. Configuración de Servidores GNU/Linux. Edición Enero 2012.

Barrios Dueñas, Joel. Introducción a IPTABLES: Consultado 10 de abril 2013.

Disponible en: http://www.alcancelibre.org/introducción-a-iptables

Cabaleiro, Juan M. Seguridad informática.

C Ardita, Julio. Aspectos Prácticos de Seguridad. 26 de noviembre 2008.

Colás Cámbara, Ángel M. Virtualización de una red LAN con servidores de código abierto para evaluar los niveles de seguridad.

Coletti, Daniel E.Entendiendo iptables. Disponible en:

http://www.danielcoletti.com.ar/Documentos/Tech/Iptables/iptables/node15.html

DMZ (Zona desmilitarizada). Disponible en:

http://es.kioskea.net/contents/protect/dmz-cloisonnement.php3

FIREWALL. 18 de agosto de 2008. (Página Web). (Consultado 3 de mayo 2013). Disponible en: http://carolavega.blogspot.com/2008/08/firewall.html

Linux Security HOWTO. 25 Abril 2006

Escartín Vigo, José Antonio. Servidor Linux para conexiones seguras de una LAN a Internet. Junio de 2005

IDS/IPS. Escuela Politécnica Nacional Diego Jefferson Chacón Herrera. Diciembre 2009.

Instalación de un servidor Web Apache en CentOS: (Consultado 7 de enero 2013). Disponible en: http://gnunick.blogspot.com/2011/03/instalando-un-servidor-web-en-centos.html

Morales Rabanales, Héctor Rodolfo. Diseño de aseguramiento de redes utilizando DMZ'S

Protección. Disponible en: http://www.segu-info.com.ar/proteccion/proteccion.htm

Portantier, Fabian. ¿Cómo realizar un Penetration Test? 2 de mayo de 201. (Documento PDF)

Ramos Fraile, Alejandro. Seguridad Perimetral. Febrero 2011.

Semeria, Chuck. Firewalls y seguridad en Internet: Disponible en:

http://www.monografias.com/trabajos3/firewalls/firewalls.shtml

Seguridad Lógica. Disponible en: http://www.segu-info.com.ar/logica/seguridadlogica.htm

Som, Guillermo. Máquinas virtuales. 25 de Febrero 2007. Disponible en:

http://www.elguille.info/sistema/máquinas_virtuales.htm

Tipos de cortafuegos según el nivel OSI: (Página Web). Consultado 3 de mayo 2013. Disponible en:

http://www.elprisma.com/apuntes/ingenieria_de_sistemas/cortafuegos/default5.asp

Villalón Huerta, Antonio. Seguridad en Linux y Redes. Julio 2006.

Zona desmilitarizada (informática). Disponible en:http://www.danielcoletti.com.ar/Documentos/Tech/Iptables/iptables/node15.html

GLOSARIO

DMZ (demilitarized zone) Zona Desmilitarizada

PAT (Port Address Translation) Traducción De Direcciones De Puertos

NAT (Network Address Translation) Traducción De Direcciones De Red

IDS (IntrusionDetectionSystem) Sistema De Detección De Intrusos

DNS (ServerDomainName) Servidor De Nombre De Dominios

LAN (LocalArea Network) Red De Área Local

FTP (File Transfer Protocol) Protocolo De Transferencia De Ficheros

HTTP (Hypertext Transfer Protocol) Protocolo De Transferencia De Hipertexto

OSI (Open Systems Interconnection) Interconexión De Sistemas Abiertos

TCP/IP (ControlProtocolconnection / Internet Protocol) Protocolo de Control de la Conexión /Protocolo De Internet

IDS (Intrusion Detection System) Sistema De Detección De Intrusos

HIDS (Intrusion Detection System) Sistema De Detección De Intrusos

NIDS (Intrusion Detection System) Sistema De Detección De Intrusos Basados En Red

DIDS (Intrusion Detection System) Sistema De Detección De Intrusos

VPN (Virtual Private Network) Red Virtual Privada

IPS (Intrusion Prevention System) Sistema De Prevención De Intrusos

DdMZ (Distributed dedicated Militarized Zones) Zonas Militarizadas DedicadasDistribuidas

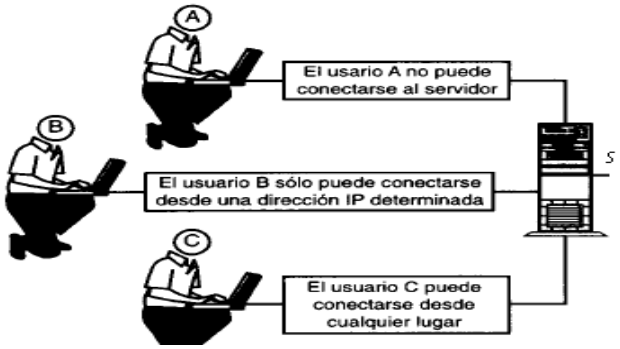
RAM (Random Access Memory) Memoria De Acceso Aleatorio

ISP (Internet Service Provider) Proveedor De Servicio De Internet

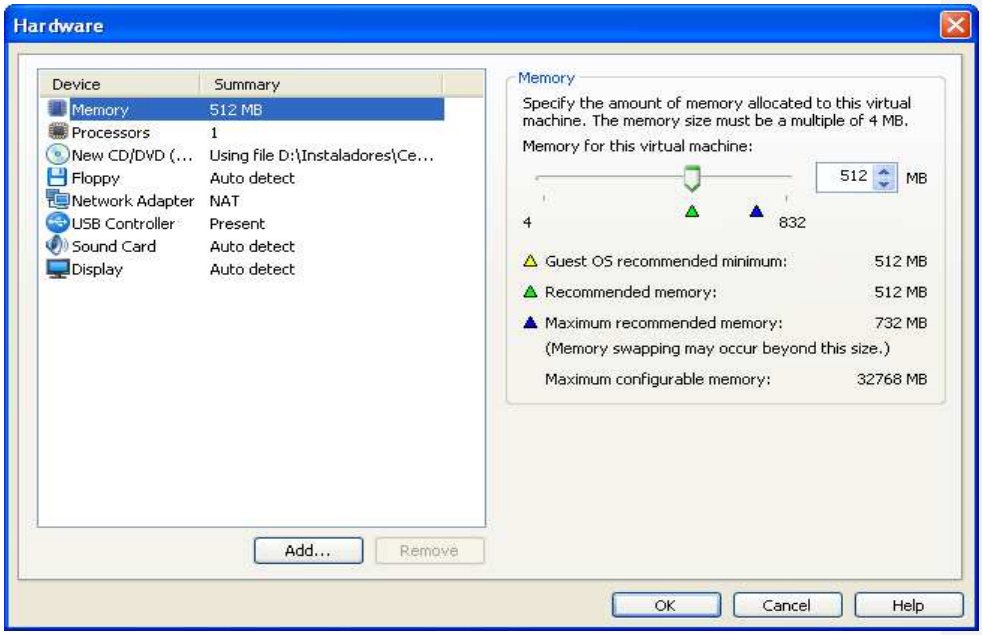
DNAT (Network Address Translation Dynamic) Traducción De Direcciones De Red Dinámica

Dos (Denial of Service) Denegación De Servicio

ANEXOS



Anexo 1: Conexiones autorizadas.



Anexo2: Interfaz de los elementos utilizados por cada Virtual Machines.